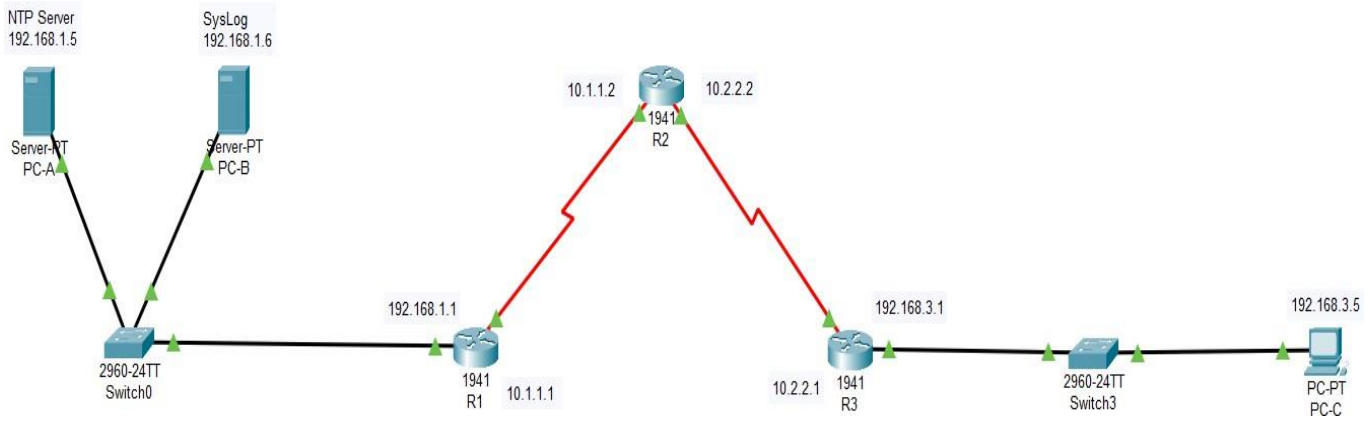
Practical-1

Aim : Configure Cisco Routers for OSPF & MD5, NTP, Syslog, and SSH Operations

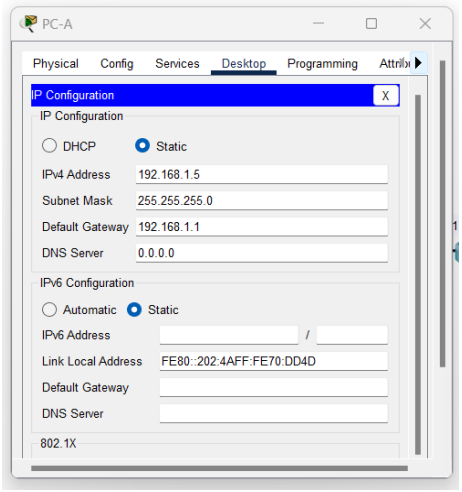
Topology:

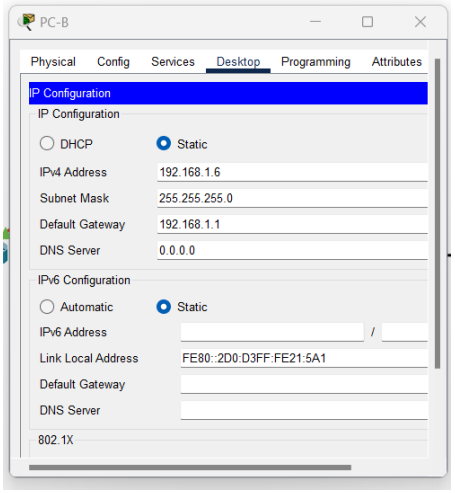


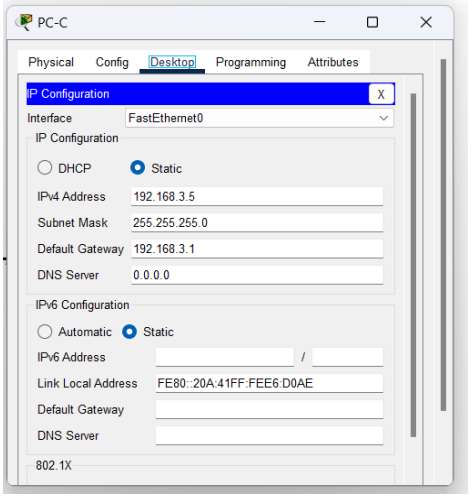
Addressing Table:

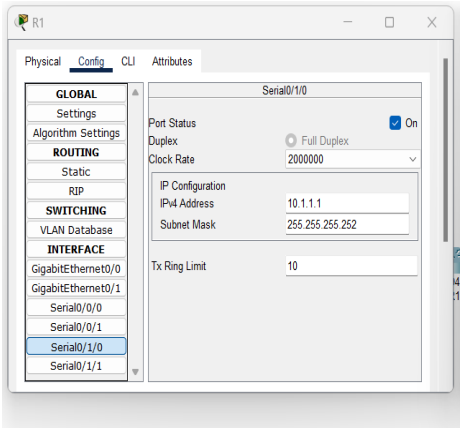
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	-
	S0/1/0	10.1.1.1	255.255.255.252	-
R2	S0/1/0	10.1.1.2	255.255.255.252	-
	S0/1/1	10.2.2.2	255.255.255.252	-
R3	G0/0	192.168.3.1	255.255.255.0	-
	S0/1/0	10.2.2.1	255.255.255.252	-
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1

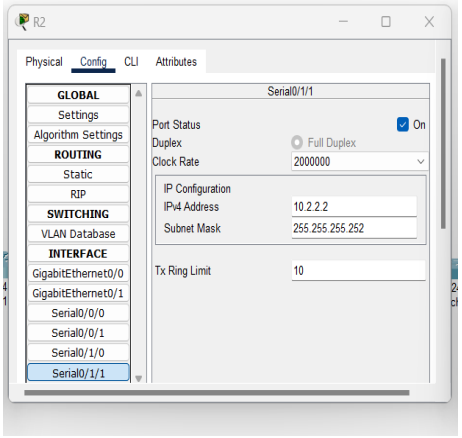
Configurations:

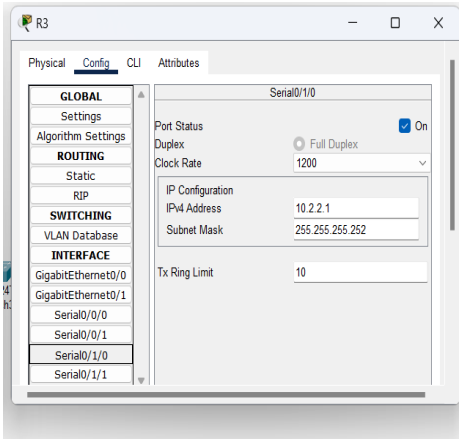


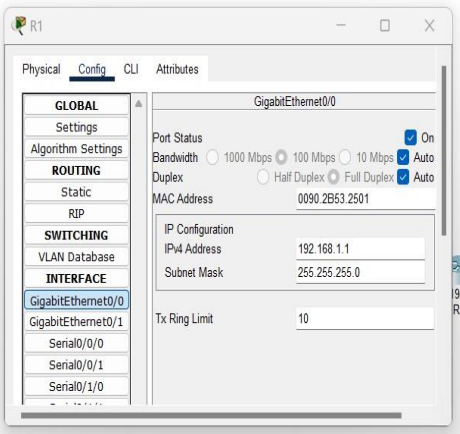


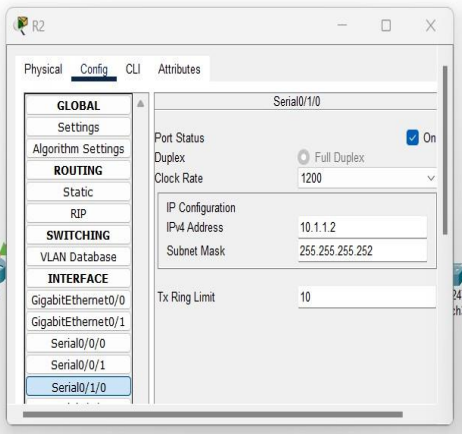


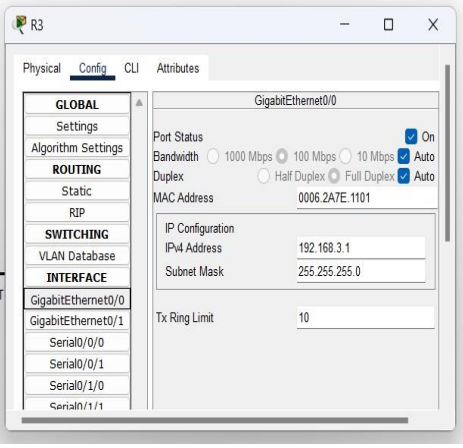




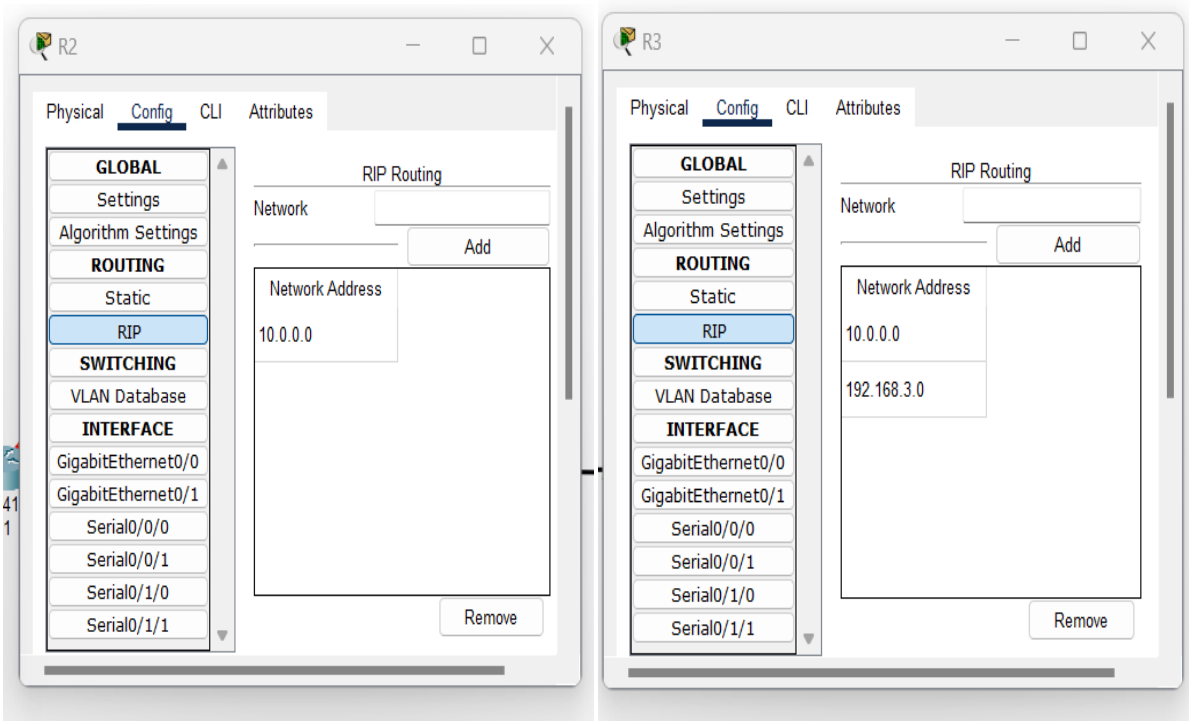








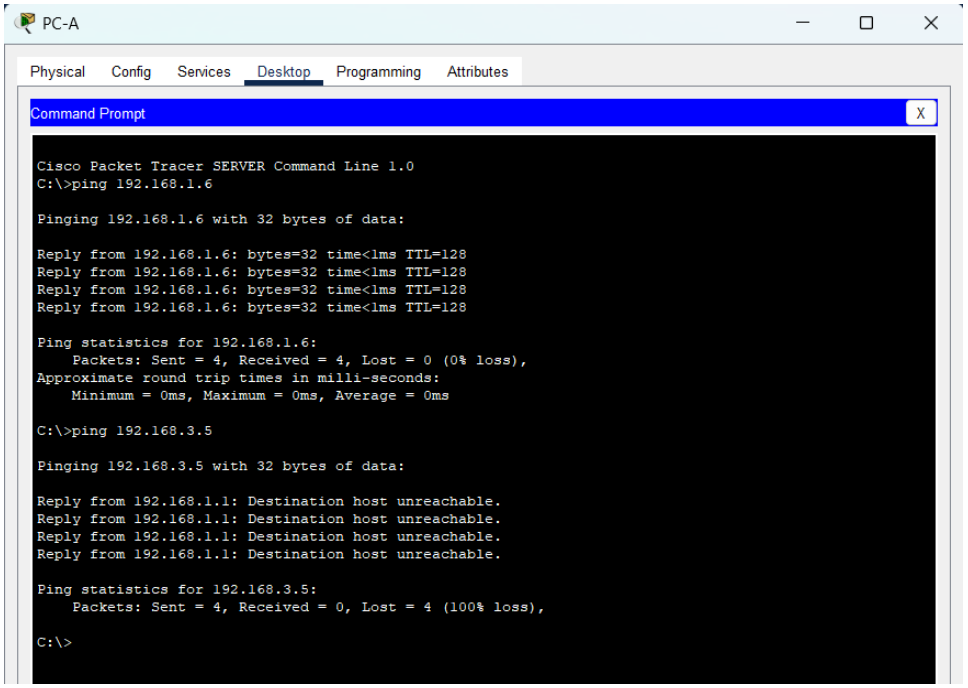
RIP Routing:


R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
10.0.0.0
Remove
R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
10.0.0.0
192.168.3.0
Remove

Part 1: Configure OSPF MD5 Authentication

Step 1: Test connectivity. All devices should be able to ping all other IP addresses.

- Click on NTP server → Click on Desktop → Click on Command Prompt and Enter following:



Step 2: Configure OSPF MD5 authentication for all the routers in area 0. Configure OSPF MD5 authentication
for all the routers in area 0.

- For R1

```
Router(config-if)#exit
Router(config)#
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#
00:22:13: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Router(config-router)#router ospf 1
Router(config-router)#area 0 authentication message-digest
Router(config-router)#
```

Copy Paste

- For R2

```
Router(config-router)#router ospf 2
Router(config-router)#area 0 authentication message-digest
Router(config-router)#
00:32:22: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL, Loading
Done
```

Copy Paste

- For R3

```
Router(config-router)#router ospf 3
Router(config-router)#area 0 authentication message-digest
Router(config-router)#
```

Copy Paste

Step 3: Configure the MD5 key for all the routers in area 0. Configure an MD5 key on the serial interfaces
on R1, R2 and R3. Use the password MD5pa55 for key 1.

For R1

```
R1(config)#interface s0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R1(config-if)#
```

Copy Paste

For R2

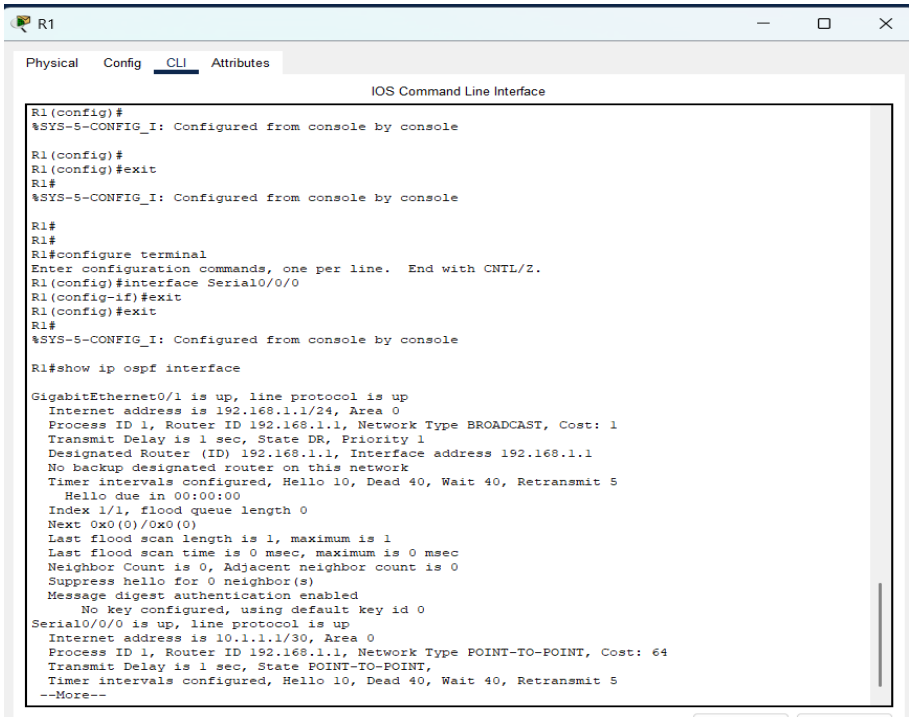
```
R2(config)#interface s0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#interface s0/0/1
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#
```

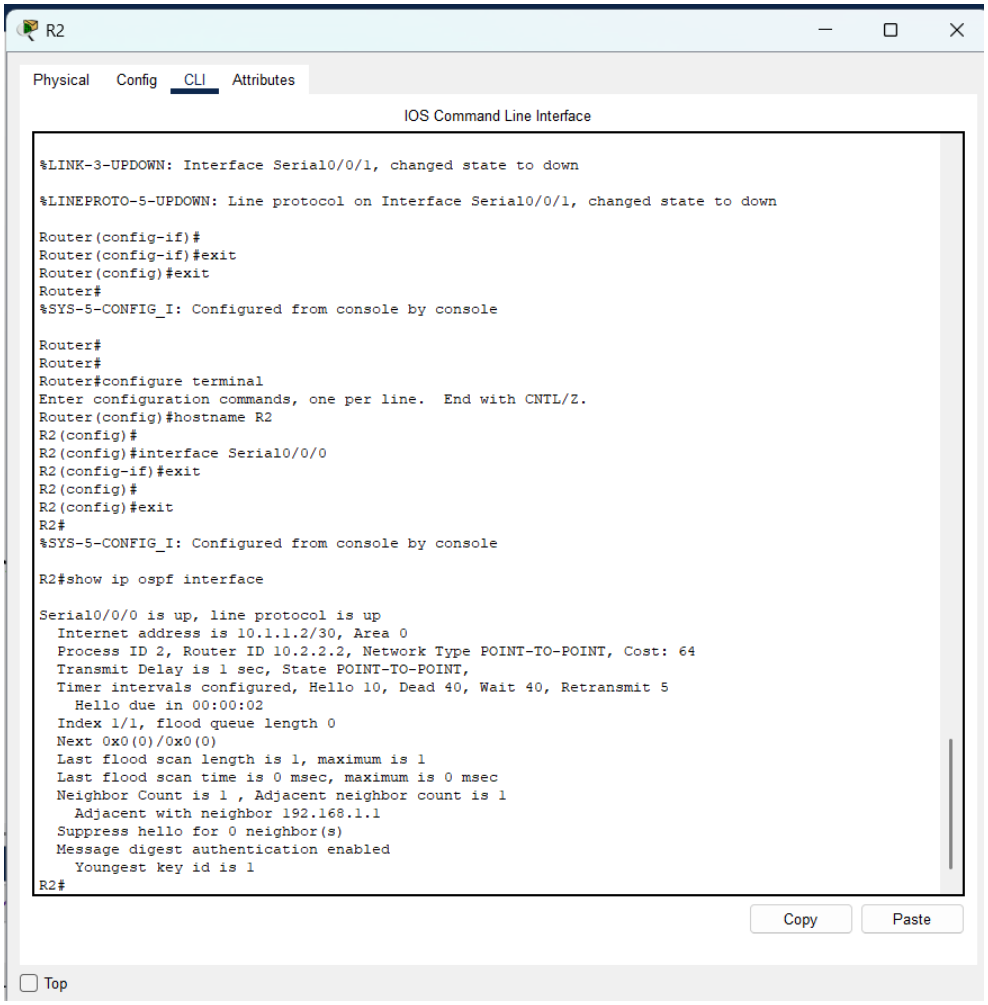
For R3

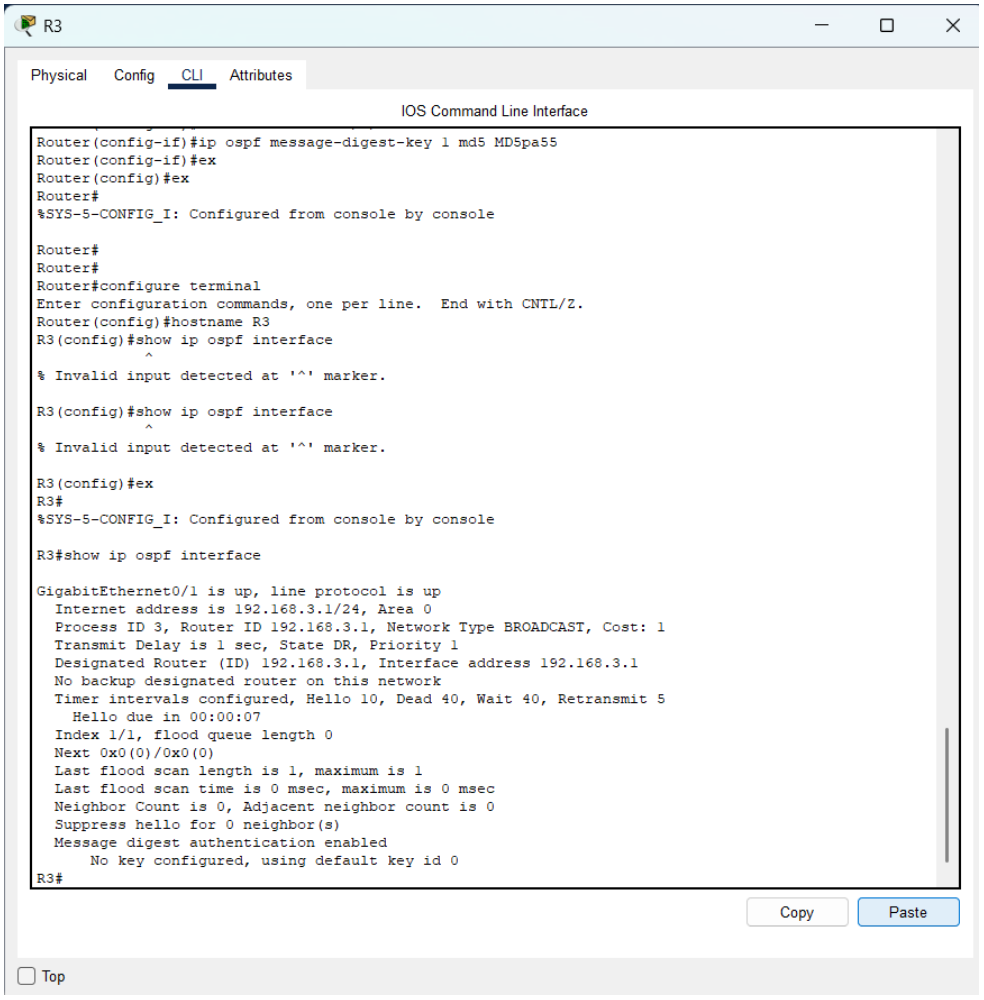
```
R3(config)#interface s0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R3(config-if)#
```

Step 4: Verify configurations.

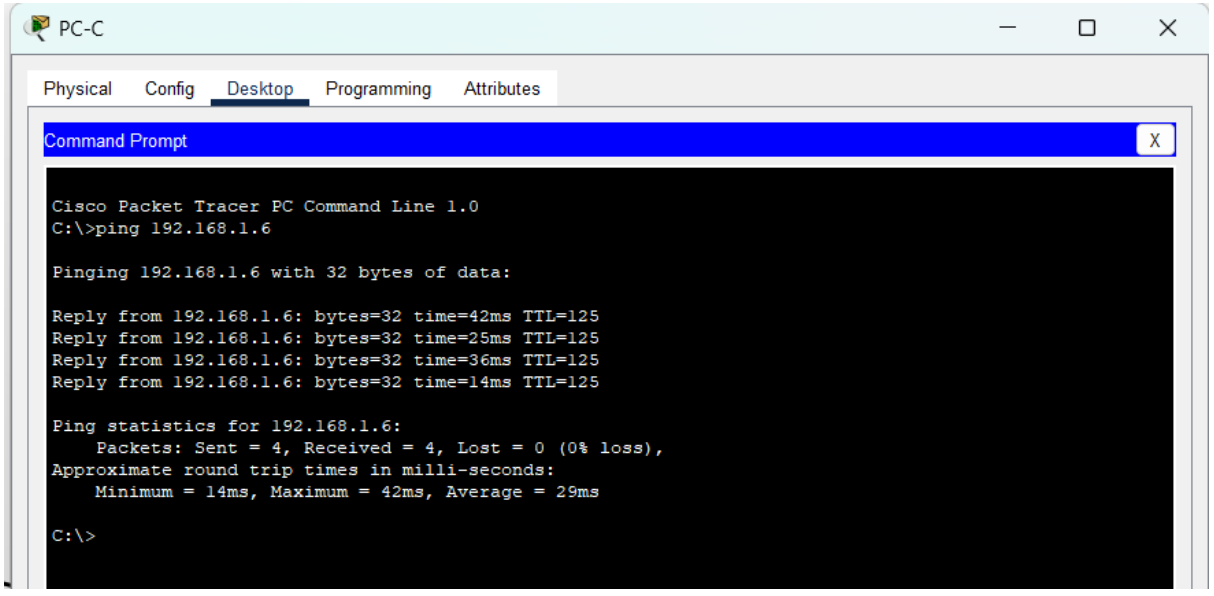
a. Verify the MD5 authentication configurations using the commands show ip ospf interface.


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1(config)#
%SYS-5-CONFIG_I: Configured from console by console
R1(config)#
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Serial0/0/0
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip ospf interface
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
No key configured, using default key id 0
Serial0/0/0 is up, line protocol is up
Internet address is 10.1.1.1/30, Area 0
Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
--More--


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-3-UPDOWN: Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
R2(config)#interface Serial0/0/0
R2(config-if)#exit
R2(config)#
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#show ip ospf interface
Serial0/0/0 is up, line protocol is up
Internet address is 10.1.1.2/30, Area 0
Process ID 2, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 192.168.1.1
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
R2#
Copy
Paste
Top

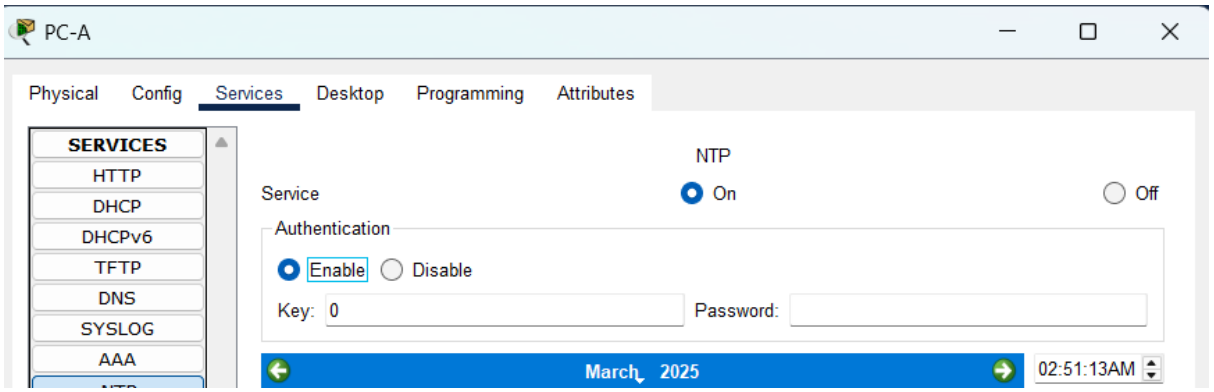


b. Verify end-to-end connectivity.

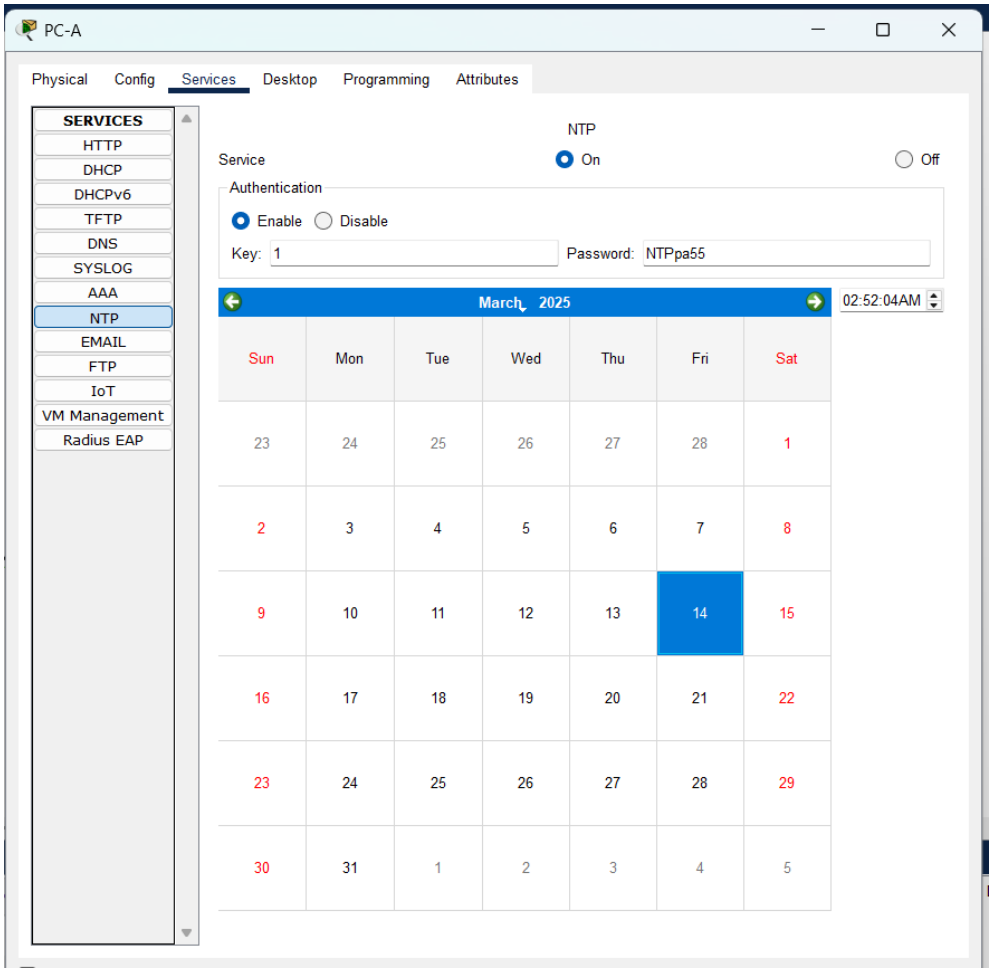


Part 2: Configure NTP

Step 1:
Enable NTP authentication on PC-A.
a. On PC-A, click NTP under the Services tab to verify NTP service is enabled.



c. To configure NTP authentication, click Enable under Authentication. Use key 1 and password NTPpa55 for authentication.



Step 2: Configure R1, R2, and R3 as NTP clients.

Step 3: Configure routers to update hardware clock. Configure R1, R2, and R3 to periodically update the hardware clock with the time learned from NTP.

R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
R1(config)#
```

Copy Paste

R2

```
R2>
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#ntp update-calendar
R2(config)#
```

Copy Paste

R3

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ntp server 192.168.1.5
R3(config)#ntp update-calendar
R3(config)#
```

Copy Paste

Step 4: Configure NTP authentication on the routers. Configure NTP authentication on R1, R2, and R3 using key 1 and password NTPpa55.

Step 5: Configure routers to timestamp log messages.

R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp authentication-key 1 md5 NTPpa55
R1(config)#service timestamps log datetime msec
```

Copy Paste

R2

```
R2>
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#ntp update-calendar
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authentication-key 1 md5 NTPpa55
R2(config)#service timestamps log datetime msec
```

Copy Paste

R3

```
R1(config)#service timestamps log datetime msec
R1(config)#ex
R1#
*Mar 14, 03:03:55.033: SYS-5-CONFIG_I: Configured from console by console
R1#show clock
3:4:7.399 UTC Fri Mar 14 2025
R1#show clock
3:5:32.602 UTC Fri Mar 14 2025
R1#
```

Copy Paste

Part 3: Configure Routers to Log Messages to the Syslog Server

Step 1: Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.

R1

```
R1(config)#logging host 192.168.1.6
R1(config)#ex
R1#
*Mar 14, 03:14:10.1414: SYS-5-CONFIG_I: Configured from console by console
*Mar 14, 03:14:10.1414:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514 started
- CLI initiated
R1#
```

Copy Paste

R2

```
R2(config)#logging host 192.168.1.6
R2(config)#ex
```

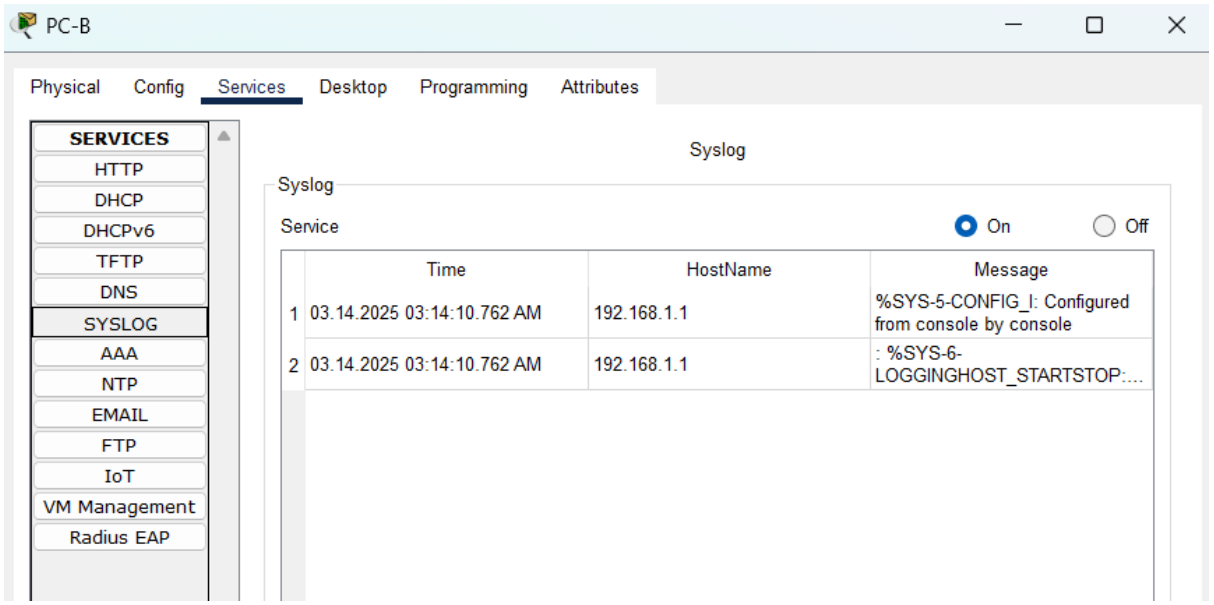
R3

```
R3(config)#logging host 192.168.1.6
R3(config)#
```

Step 2: Verify logging configuration. Use the command show logging to verify logging has been enabled.

Step 3: Examine logs of the Syslog Server. From the Services tab of the Syslog Server's dialogue box, select the Syslog services button. Observe the logging messages received from the routers.

PC-B Syslog Server



Part 4: Configure R3 to Support SSH Connections

Step 1: Configure a domain name. Configure a domain name of ccnasecurity.com on R3. R3(config)# ip domain-name ccnasecurity.com

Step 2: Configure users for login to the SSH server on R3. Create a user ID of SSHadmin with the highest possible privilege level and a secret password of ciscosshpa55. R3(config)# username SSHadmin privilege 15 secret ciscosshpa55

Step 3: Configure the incoming vty lines on R3. Use the local user accounts for mandatory login and validation. Accept only SSH connections. R3(config)# line vty 0 4 R3(config-line)# login local R3(config-line)# transport input ssh

Step 4: Erase existing key pairs on R3. Any existing RSA key pairs should be erased on the router. R3(config)# crypto key zeroize rsa

Step 5: Generate the RSA encryption key pair for R3.

R3 (RSA Encryption)

```
R3>
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip domain-name ccnasecurity.com
R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#crcex
% Ambiguous command: "ex"
R3(config-line)#en
% Ambiguous command: "en"
R3(config)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

R3(config)#crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.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]
```

Step 6: Verify the SSH configuration

R3

```
%SYS-5-CONFIG_I: Configured from console by console
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514 started - CLI initiated

R3#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R3#
```

Copy Paste

Step 7: Configure SSH timeouts and authentication parameters.

R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
R3(config)# ip ssh version 2

Step 8: Attempt to connect to R3 via Telnet from PC-C

PC-C

```
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open

[Connection to 192.168.3.1 closed by foreign host]
C:\>
```

Step 9: Connect to R3 using SSH on PC-C.

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

Password:



R3#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
R3#
```

Step 10: Connect to R3 using SSH on R2.

R2# ssh –v 2 –l SSHadmin 10.2.2.1

R3

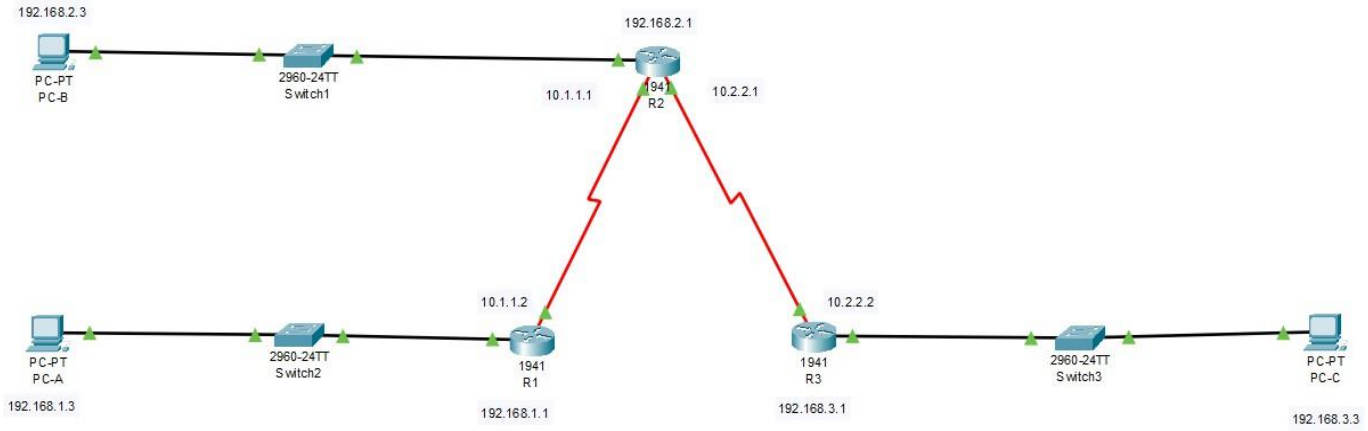
```
R2#ssh -v 2 -l SSHadmin 10.2.2.1

Password:



R3#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
R3#
```

Copy Paste

Practical-2

Aim:- Configure AAA Authentication on Cisco Routers.

Topology:

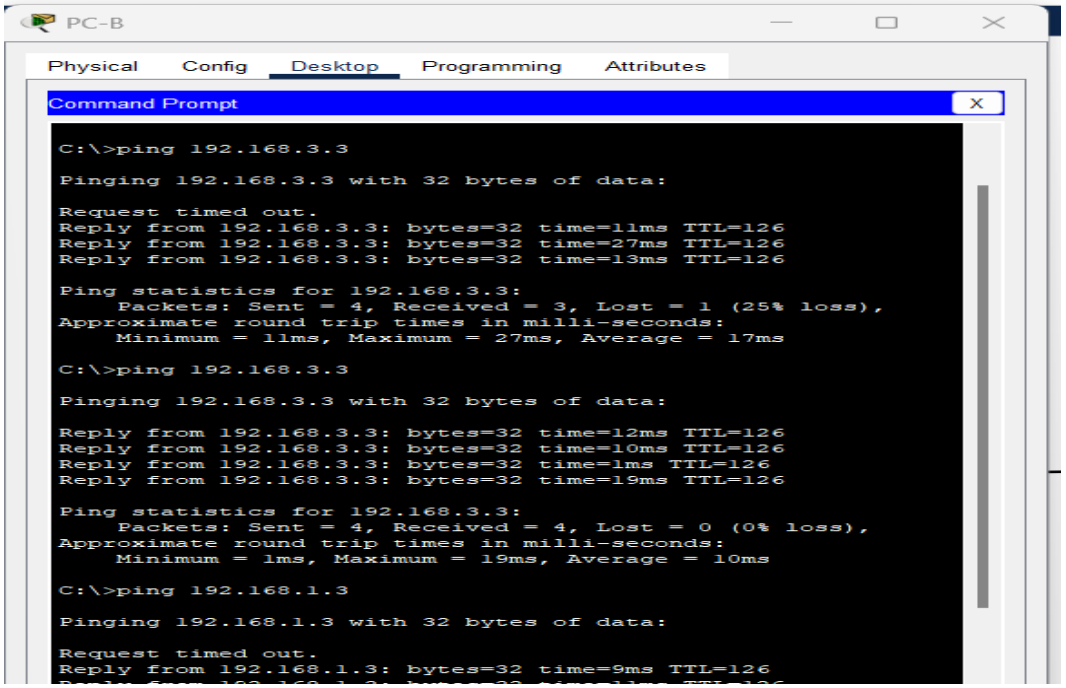


Addressing Table:

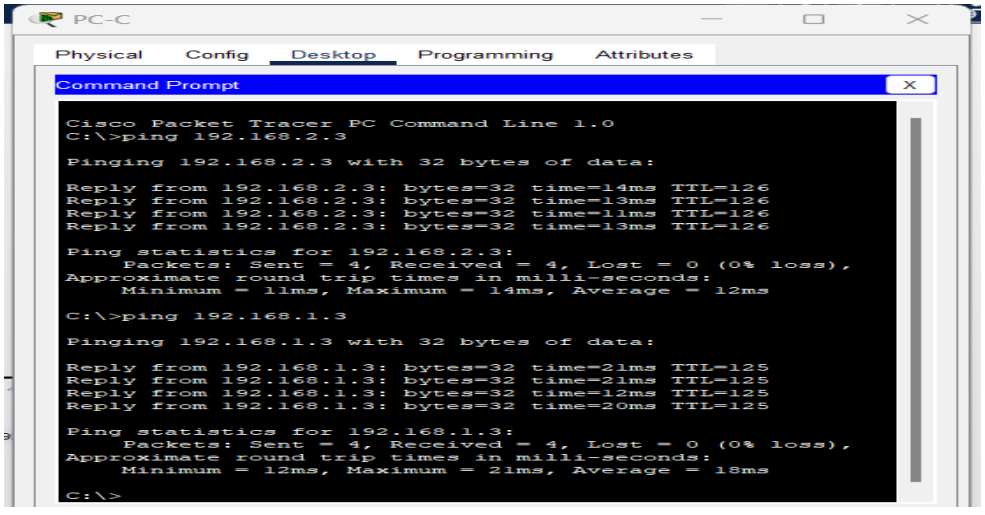
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	-
	S0/1/0	10.1.1.2	255.255.255.252	-
R2	S0/1/0	10.1.1.1	255.255.255.252	-
	S0/1/1	10.2.2.1	255.255.255.252	-
	G0/0	192.168.2.1	255.255.255.0	-
R3	G0/0	192.168.3.1	255.255.255.0	-
	S0/1/0	10.2.2.2	255.255.255.252	-
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Part 1: Configure Local AAA Authentication for Console Access on R1

Step 1: Test connectivity.
• Ping from PC-A to PC-B.
• Ping from PC-A to PC-C.



• Ping from PC-B to PC-C.



Step 2: Configure a local username on R1. Configure a username of Admin1 with a secret password of admin1pa55.
R1(config)# username Admin1 secret admin1pa55

Step 3: Configure local AAA authentication for console access on R1. Enable AAA on R1 and configure AAA authentication for the console login to use the local database.
R1(config)# aaa new-model

Step 4: Configure the line console to use the defined AAA authentication method. Enable AAA on R1 and configure AAA authentication for the console login to use the default method list.
R1(config)# line console 0 R1(config-line)# login authentication default

Step 5: Verify the AAA authentication method. Verify the user EXEC login using the local database.
R1(config-line)# end %SYS-5-CONFIG_I: Configured from console by console
R1# exit
Username: **Admin1**
Password: **admin1pa55**

R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# username Admin1 secret admin1pa55
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)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

```
R1 con0 is now available
```

```
Username: Admin1
Password:
R1>
```

Part 2: Configure Local AAA Authentication for vty Lines on R1

Step 1: Configure domain name and crypto key for use with SSH.

a) Use ccnasecurity.com as the domain name on R1
b) Create an RSA crypto key using 1024 bits.

R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name ccnasecurity.com
R1(config)# crypto key generate rsa
The name for the keys will be: R1.ccnasecurity.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)#
```

Copy Paste

Step 2: Configure a named list AAA authentication method for the vty lines on R1.
Configure a named list called SSH-LOGIN to authenticate logins using local AAA.

R1

```
R1(config)# aaa authentication login SSH-LOGIN local
*Mar 1 0:54:7.901: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
```

Step 3: Configure the vty lines to use the defined AAA authentication method.
Configure the vty lines to use the named AAA method and only allow SSH for remote access.

R1

```
R1(config)# line vty 0 4
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

Step 4: Verify the AAA authentication method.
Verify the SSH configuration SSH to R1 from the command prompt of PC-A.

```
C:\> ssh -l Admin1 192.168.1.1

Password:
R1>
```

Part 3: Configure Server-Based AAA Authentication Using TACACS+ on R2

Step 1: Configure a backup local database entry called Admin.
For backup purposes, configure a local username of Admin2 and a secret password of admin2pa55.

R2

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# username Admin2 secret admin2pa55
R2(config)#
```

Step 2: Verify the TACACS+ Server configuration.
Click the TACACS+ Server.On the Services tab, click AAA. Notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

Step 3: Configure the TACACS+ server specifics on R2.
Configure the AAA TACACS server IP address and secret key on R2.
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55

Step 4: Configure AAA login authentication for console access on R2.
Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server. If it is not available, then use the local database.
R2(config)# aaa new-model
R2(config)# aaa authentication login default group tacacs+ local

Step 5: Configure the line console to use the defined AAA authentication method. Configure AAA authentication for console login to use the default AAA authentication method.
R2(config)# line console 0
R2(config-line)# login authentication default

Step 6: Verify the AAA authentication method.
R2(config-line)# end
R2# exit
Username: **Admin2**
Password: **admin2pa55**

R2

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username Admin2 secret admin2pa55
R2(config)#tacacs-server host 192.168.2.2
R2(config)#tacacs-server key tacacspa55
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#ine console 0
           ^
% Invalid input detected at '^' marker.

R2(config)#line console 0
R2(config-line)# login authentication default
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit




R2 con0 is now available
```

Part 4: Configure Server-Based AAA Authentication Using RADIUS on R3

Step 1: Configure a backup local database entry called Admin. For backup purposes, configure a local username of Admin3 and a secret password of admin3pa55.
R3(config)# username Admin3 secret admin3pa55

Step 2: Verify the RADIUS Server configuration. Click the RADIUS Server. On the Services tab, click AAA. Notice that there is a Network configuration entry for R3 and a User Setup entry for Admin3.

Step 3: Configure the TACACS+ server specifics on R2. Configure the AAA TACACS server IP address and secret key on R2.
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55

Step 4: Configure AAA login authentication for console access on R3.
Enable AAA on R3 and configure all logins to authenticate using the AAA RADIUS server. If it is not available, then use the local database.
R3(config)# aaa new-model
R3(config)# aaa authentication login default group radius local

Step 5: Configure the line console to use the defined AAA authentication method. Configure AAA authentication for console login to use the default AAA authentication method.
R3(config)# line console 0
R3(config-line)# login authentication default

Step 6: Verify the AAA authentication method. Verify the user EXEC login using the AAA RADIUS server.
R3(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R3# exit

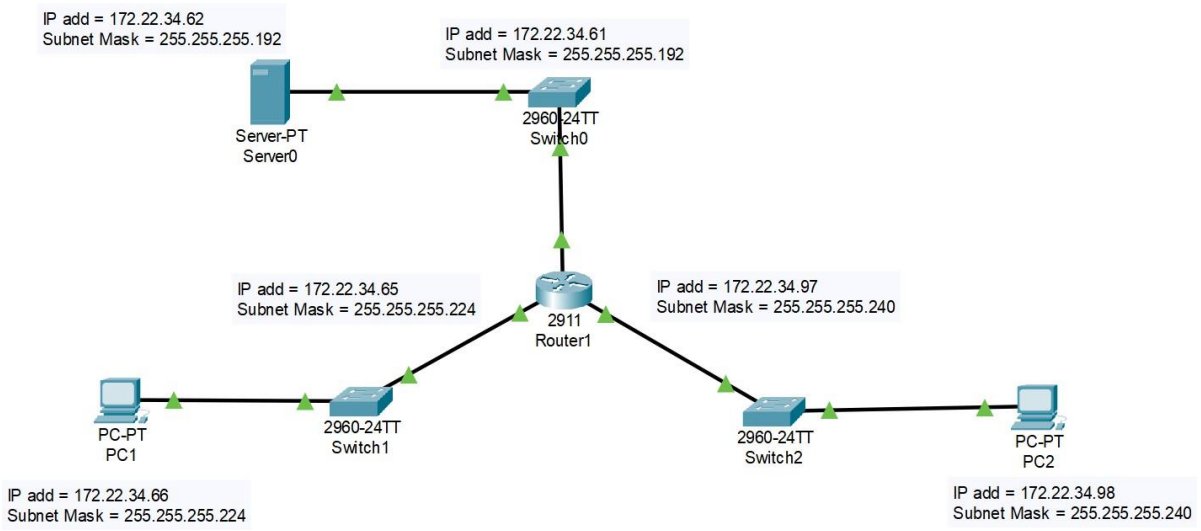
```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username Admin3 secret admin3pa55
R3(config)#radius-server host 192.168.3.2
R3(config)#radius-server key radiuspa55
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit




R3 con0 is now available
```

```
User Access Verification

Username: Admin3
Password:




Press RETURN to get started!

R3>
```

Practical-3

Aim: Configuring Extended Access Control Lists (ACLs)

Topology:



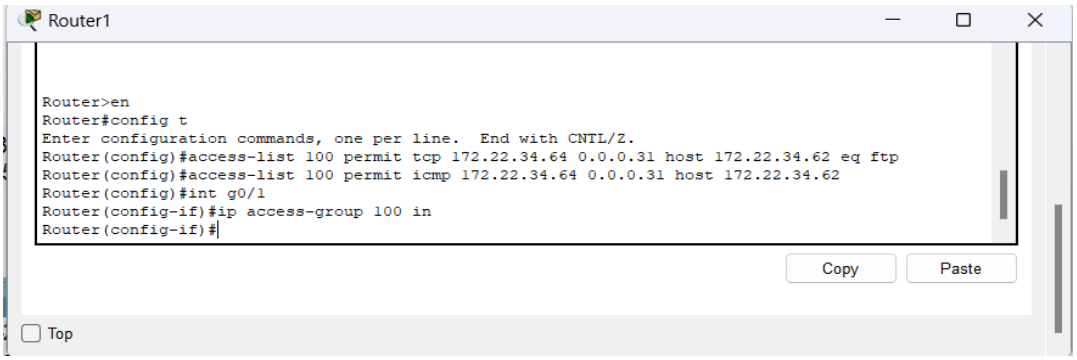
Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router	G0/0	172.22.34.61	255.255.255.192	-
	G0/1	172.22.34.65	255.255.255.224	-
	G0/2	172.22.34.97	255.255.255.240	-
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.61
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.224	172.22.34.97

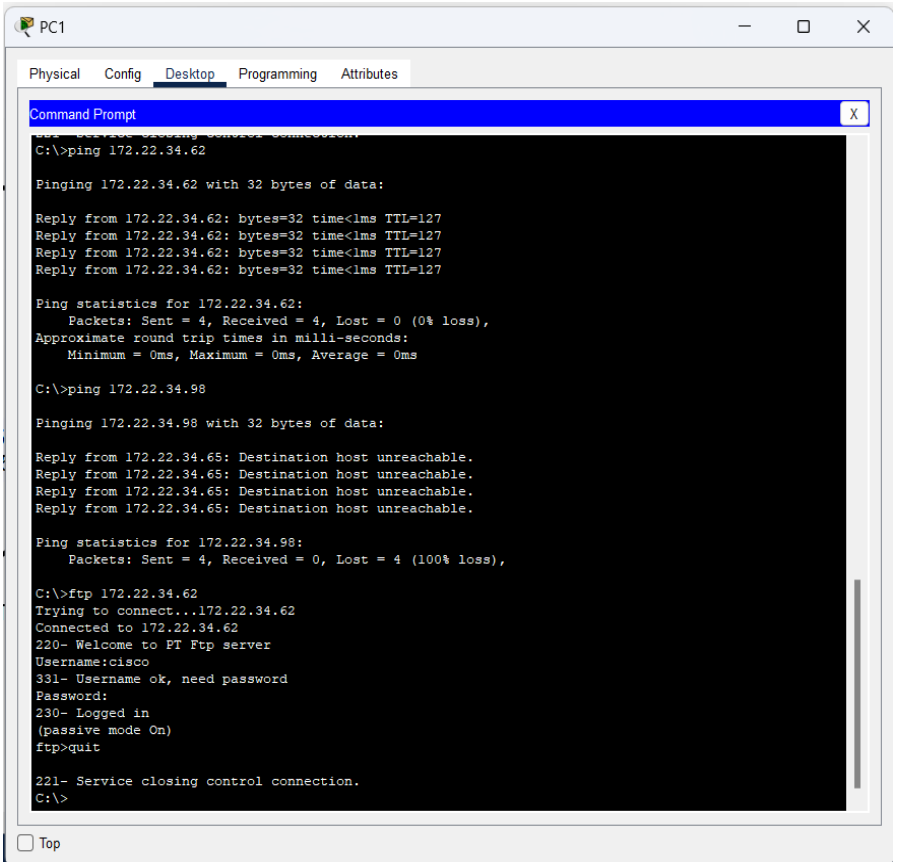
(NOTE: After applying the RIP, check with the ping command from multiple devices to verify successful connection.)

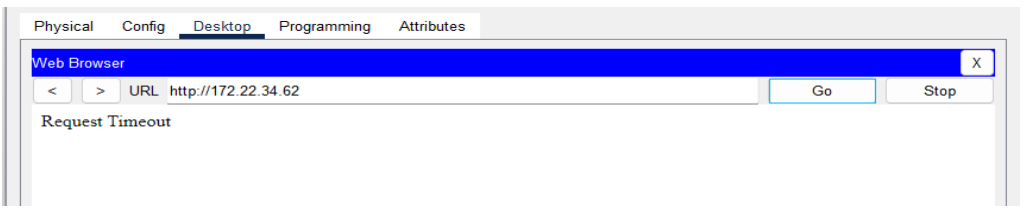
Part-1 : Configuring an ACL to permit FTP and ICMP to PC1.

R1

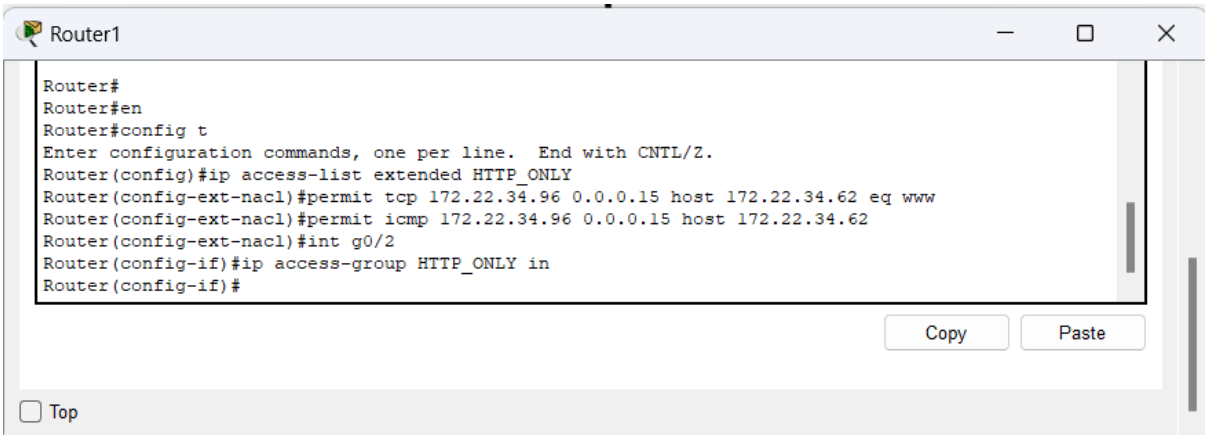


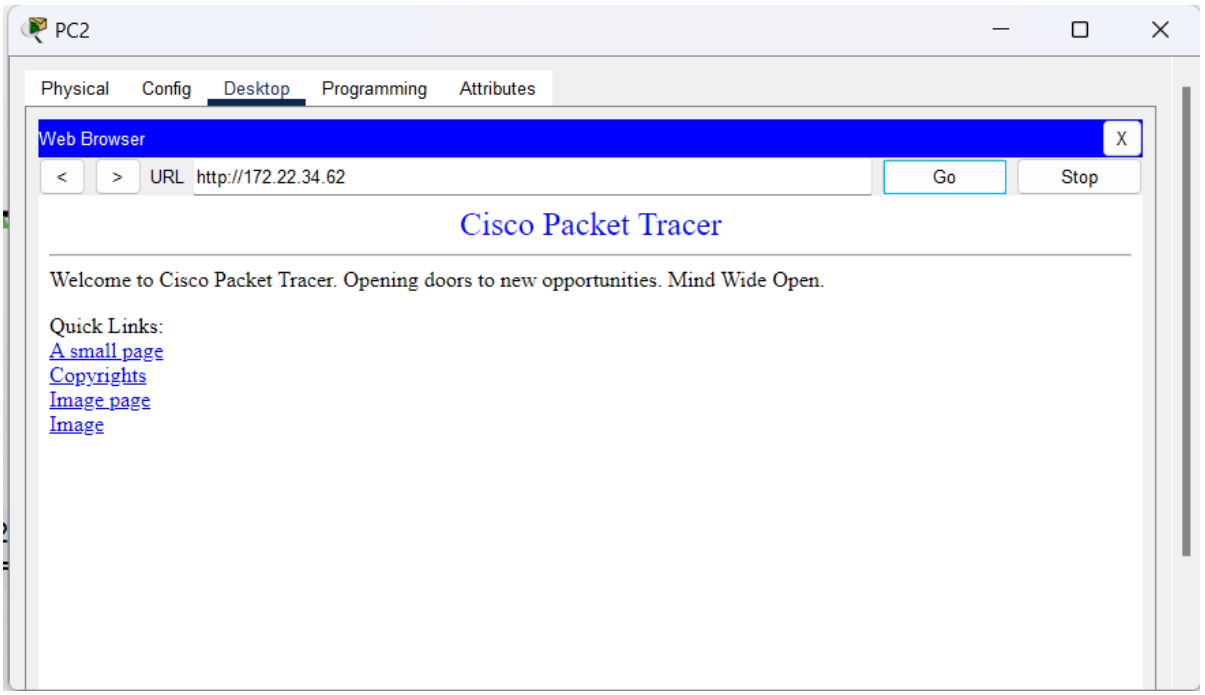
PC 1

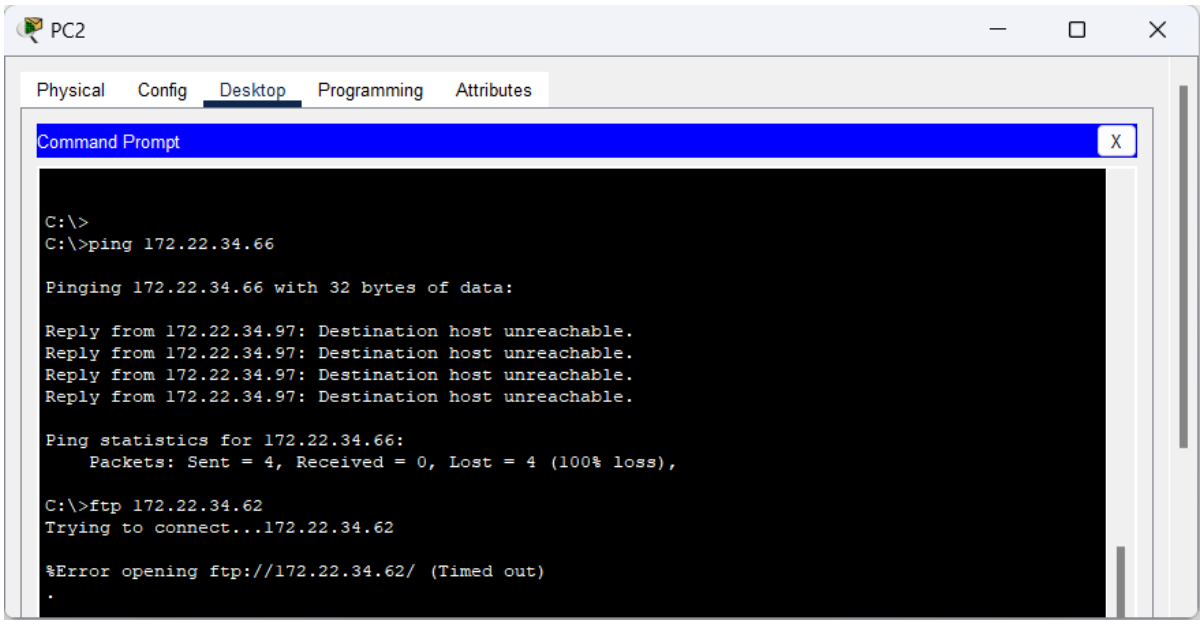




Part-2 : Configure, Apply and Verify an Extended Named ACL



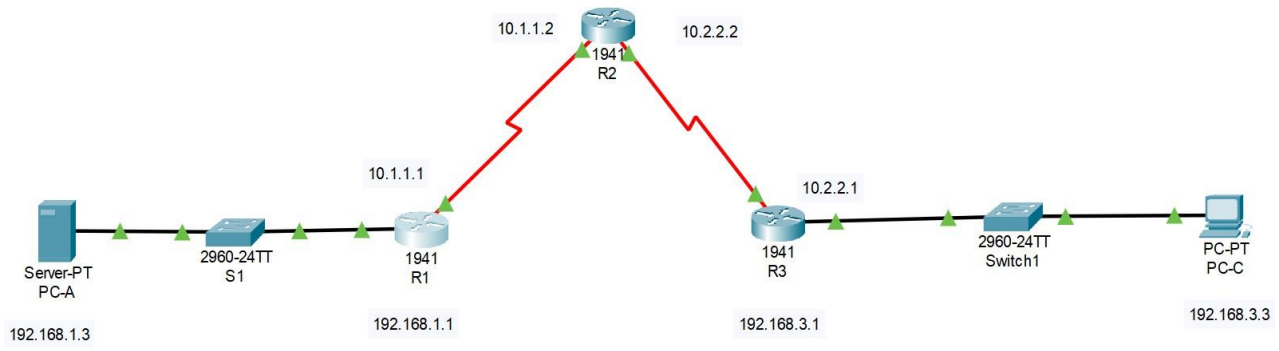




Practical-4

Aim : Configure IP ACLs to Mitigate Attacks.

Topology:

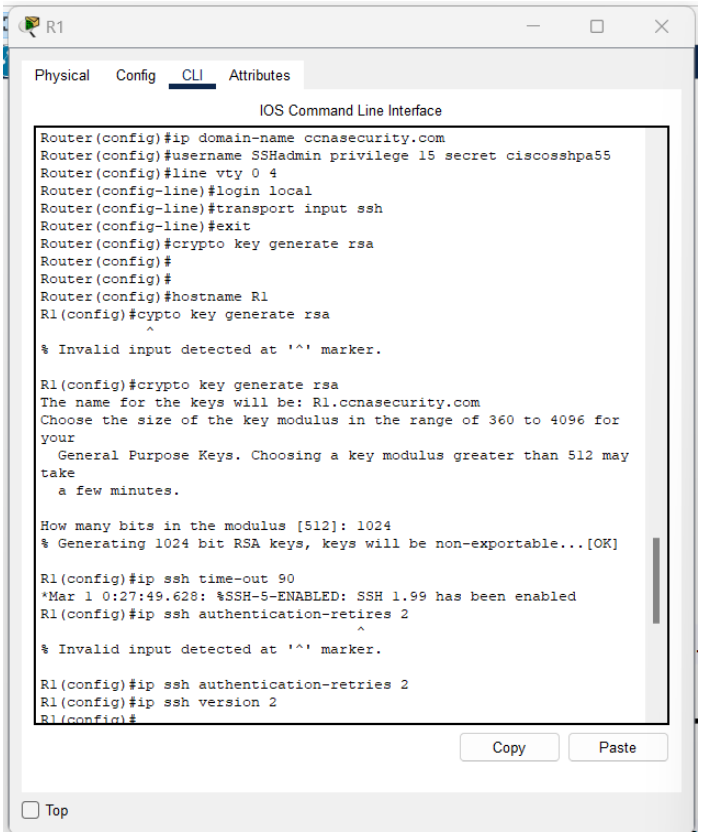


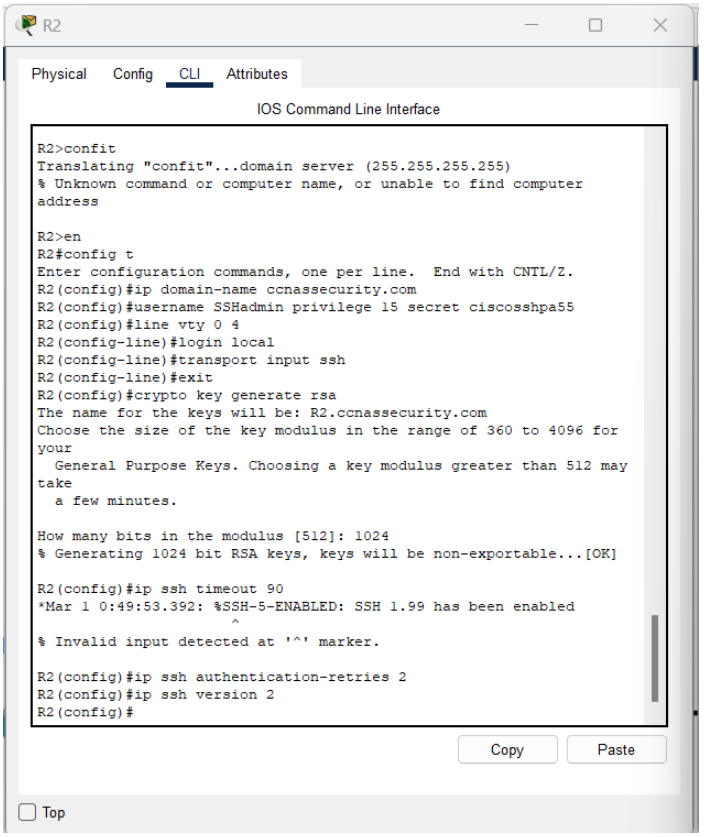
Addressing Table:

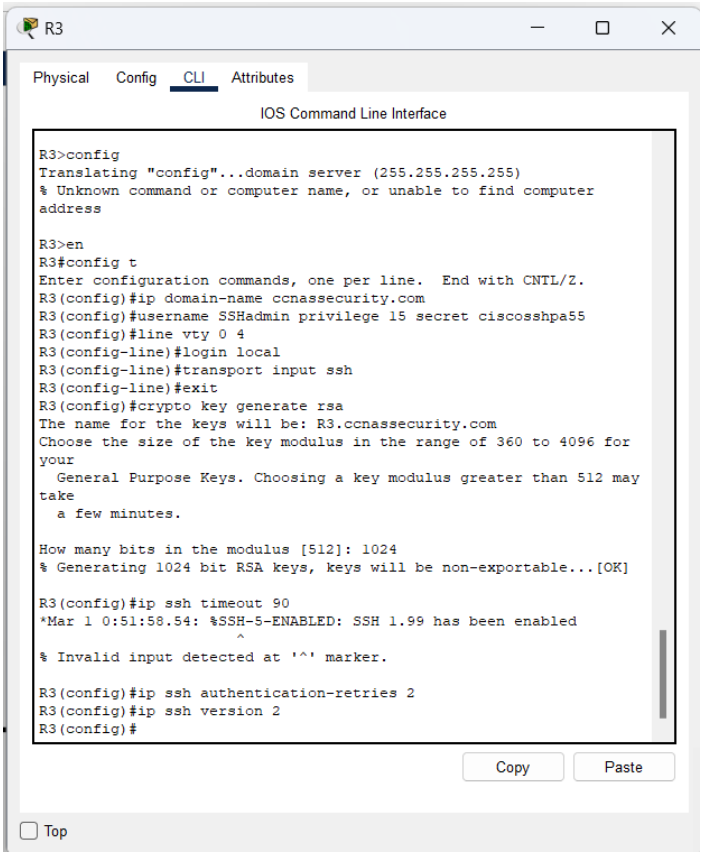
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	-
	S0/1/0	10.1.1.1	255.255.255.252	-
R2	S0/1/0	10.1.1.2	255.255.255.252	-
	S0/1/1	10.2.2.2	255.255.255.252	-
R3	G0/0	192.168.3.1	255.255.255.0	-
	S0/1/0	10.2.2.1	255.255.255.252	-
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

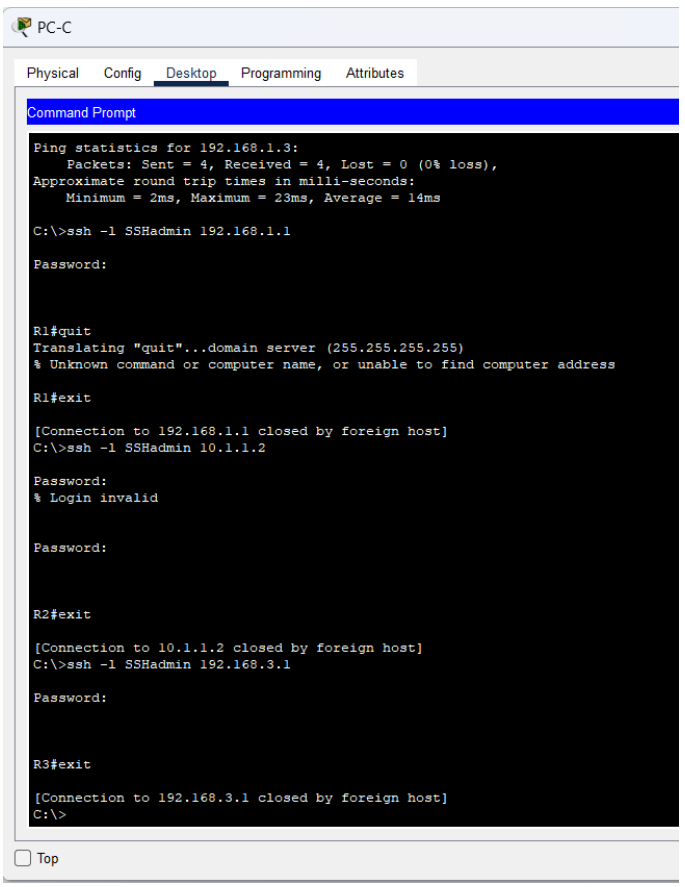
(NOTE: After applying the RIP, check with the ping command from multiple devices to verify successful connection.)

Part - 1 : SSH enabling and checking

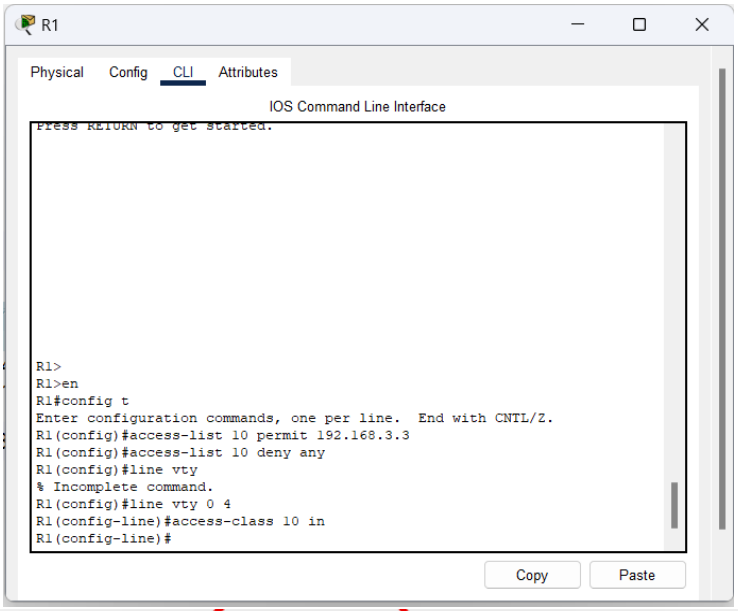


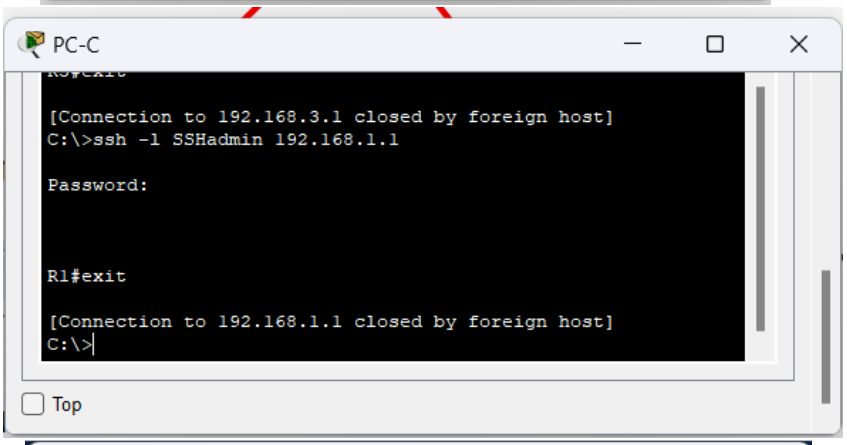


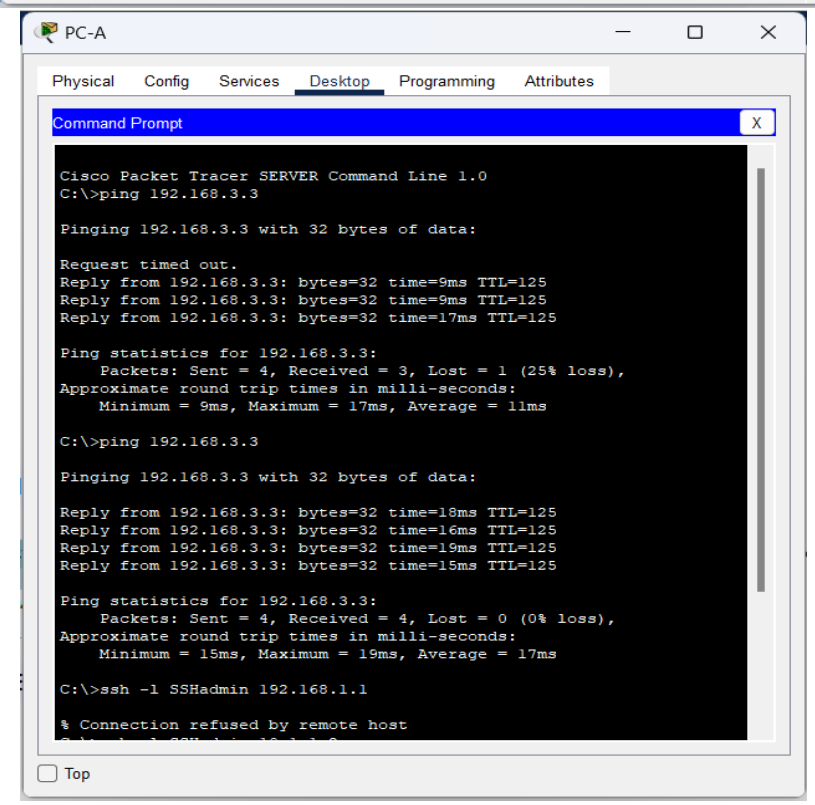




Part - 2 : Block all remote access to router except PC-C

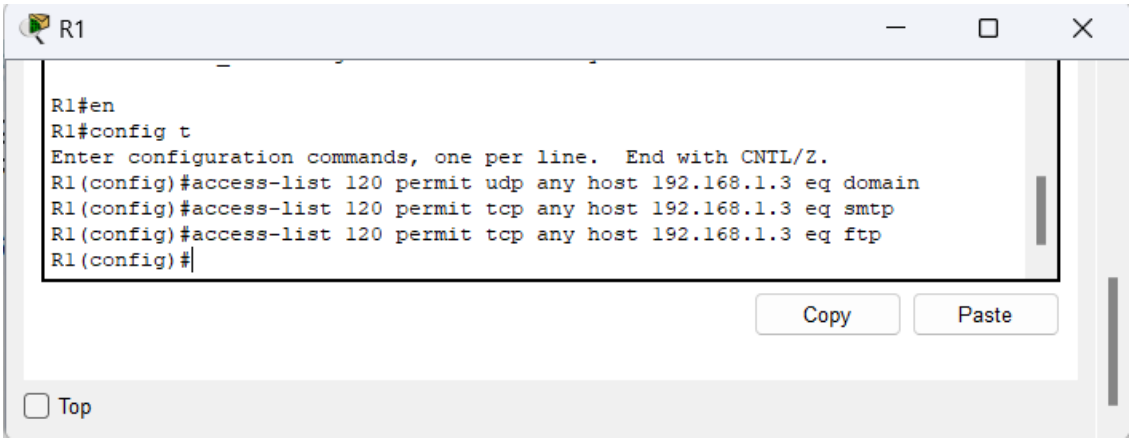




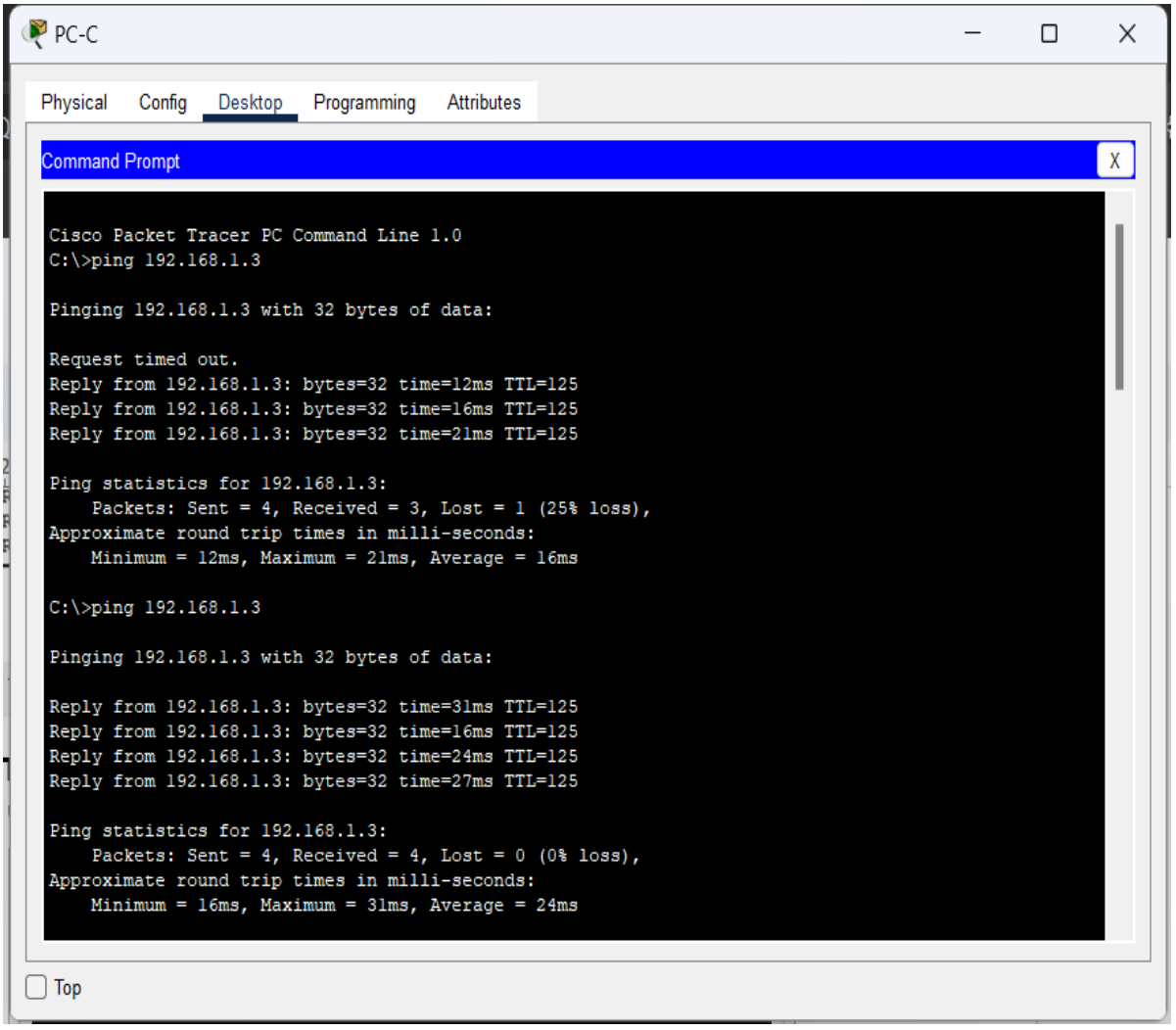


Part - 3 :

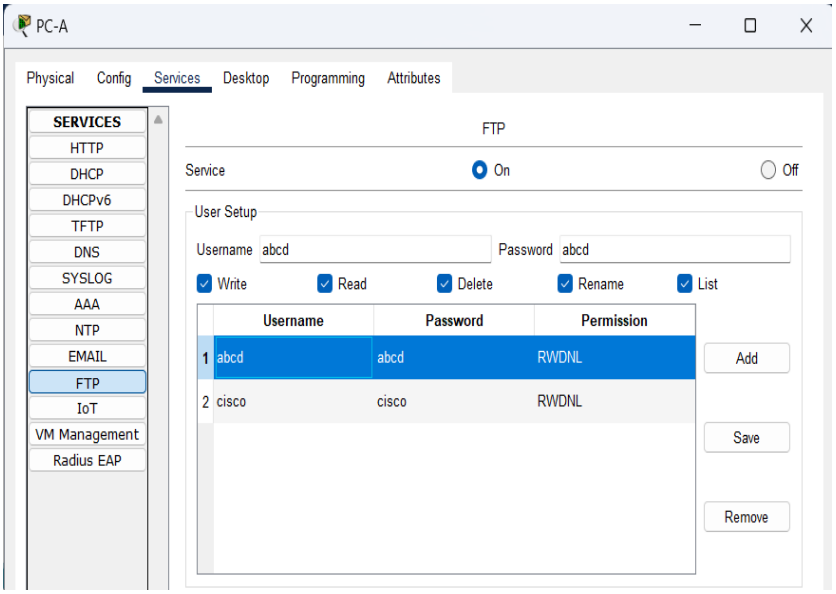
Part - 3.1 : IP ACL 120 to permit any to access DNS,SMTP and FTP on Server

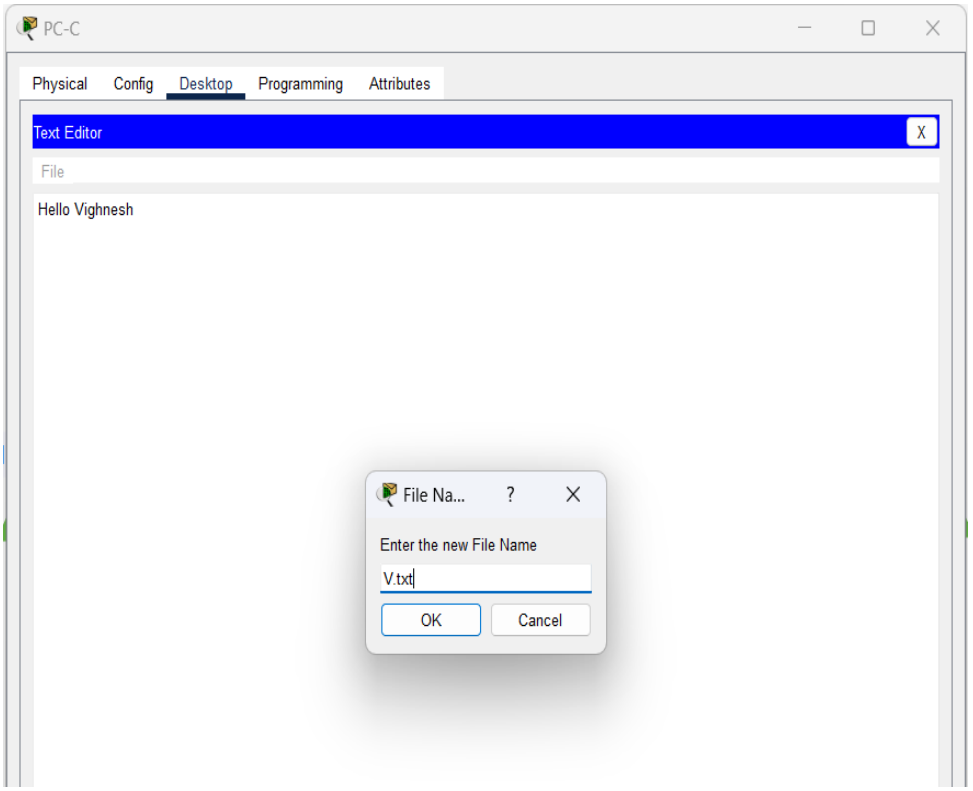


SMTP:

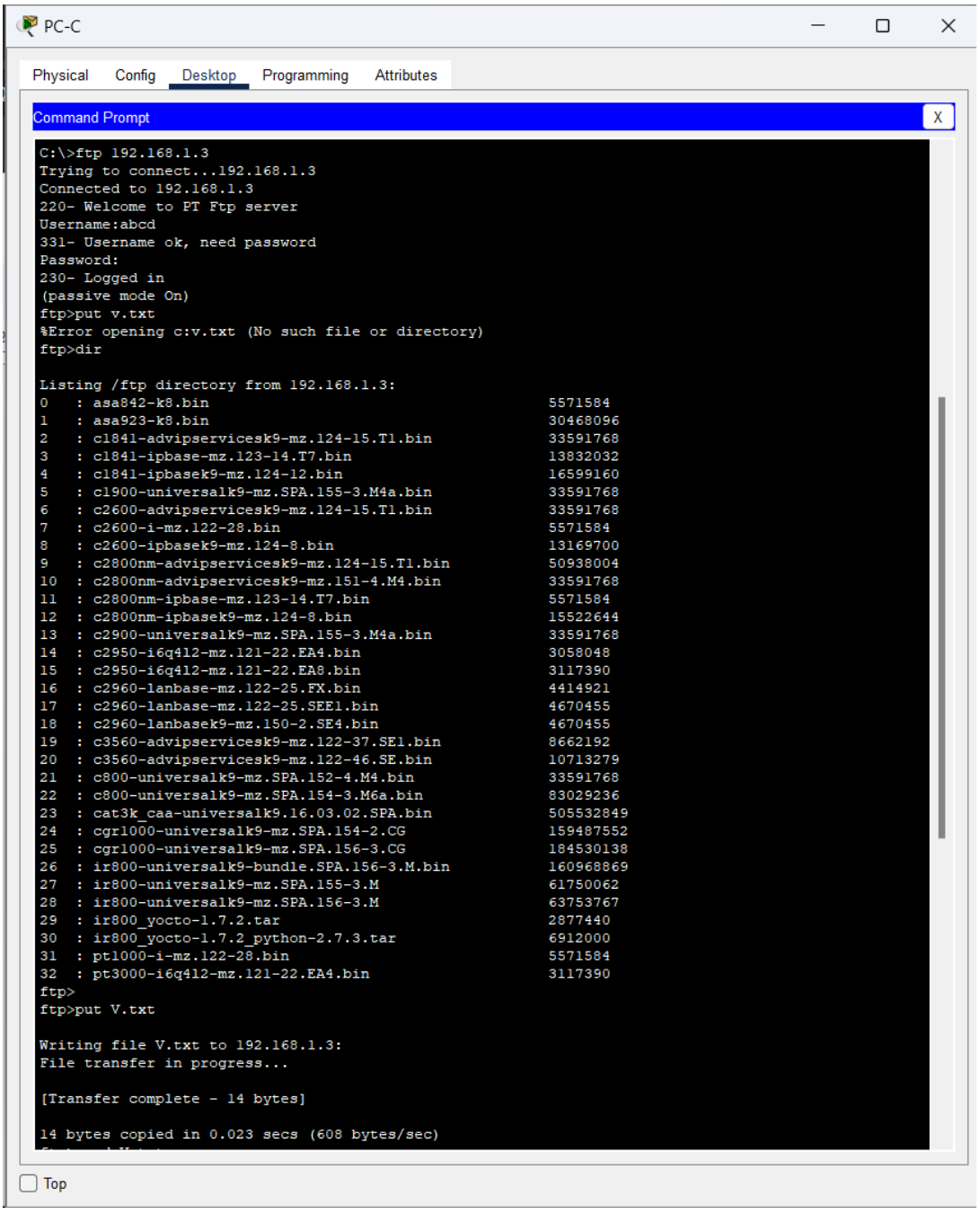


FTP:


PC-A
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
FTP
Service
On
Off
User Setup
Username abcd
Password abcd
Write
Read
Delete
Rename
List
Username
Password
Permission
1 abcd abcd RWDNL
2 cisco cisco RWDNL
Add
Save
Remove

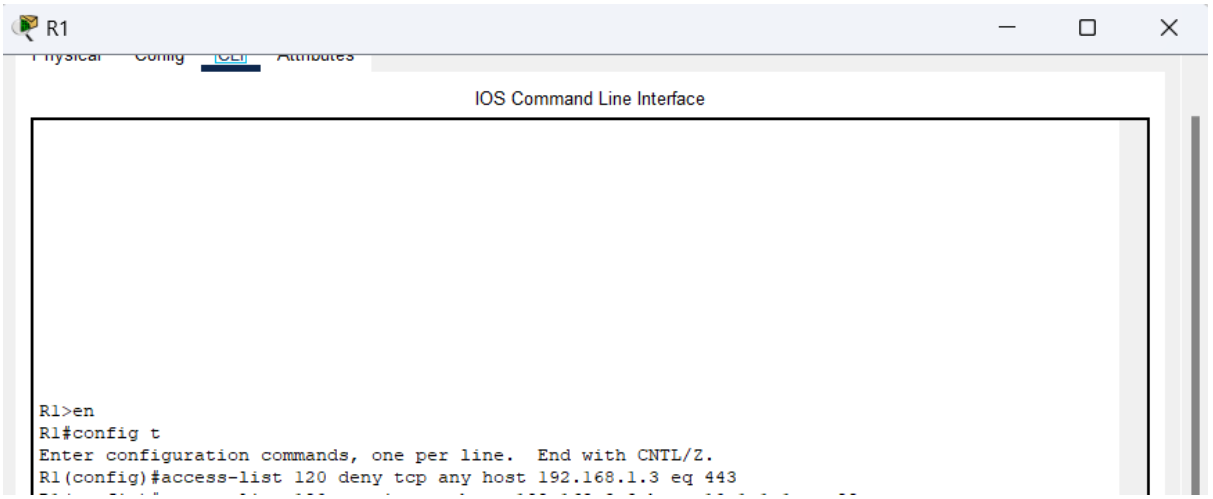

PC-C
Physical
Config
Desktop
Programming
Attributes
Text Editor
File
Hello Vighnesh
File Na...
Enter the new File Name
V.txt
OK
Cancel

PC-C

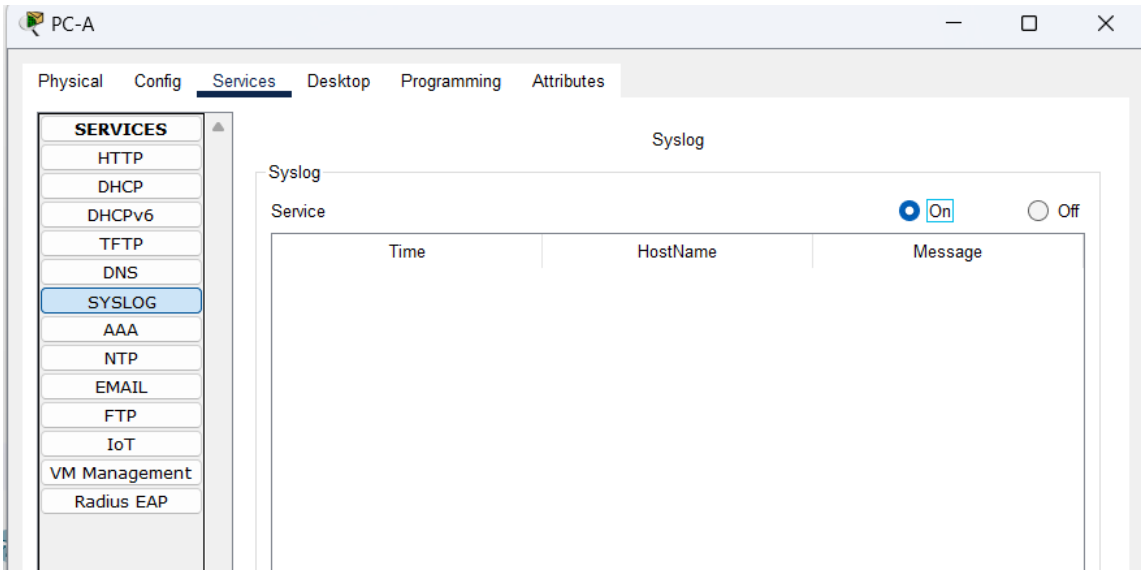

PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ftp 192.168.1.3
Trying to connect...192.168.1.3
Connected to 192.168.1.3
220- Welcome to PT Ftp server
Username:abcd
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put v.txt
%Error opening c:v.txt (No such file or directory)
ftp>dir
Listing /ftp directory from 192.168.1.3:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>
ftp>put V.txt
Writing file V.txt to 192.168.1.3:
File transfer in progress...
[Transfer complete - 14 bytes]
14 bytes copied in 0.023 secs (608 bytes/sec)
Top

Part - 3.2 : Deny Access to HTTPS on PC-A

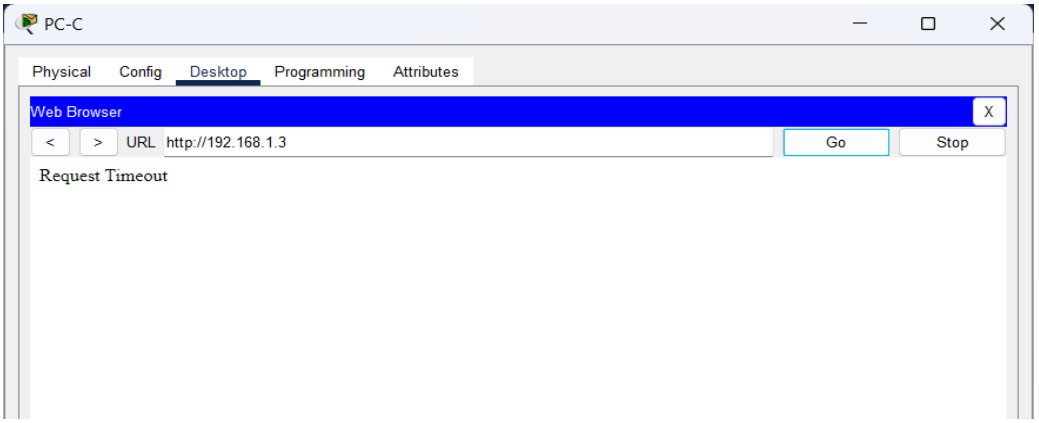
R1



PC-A

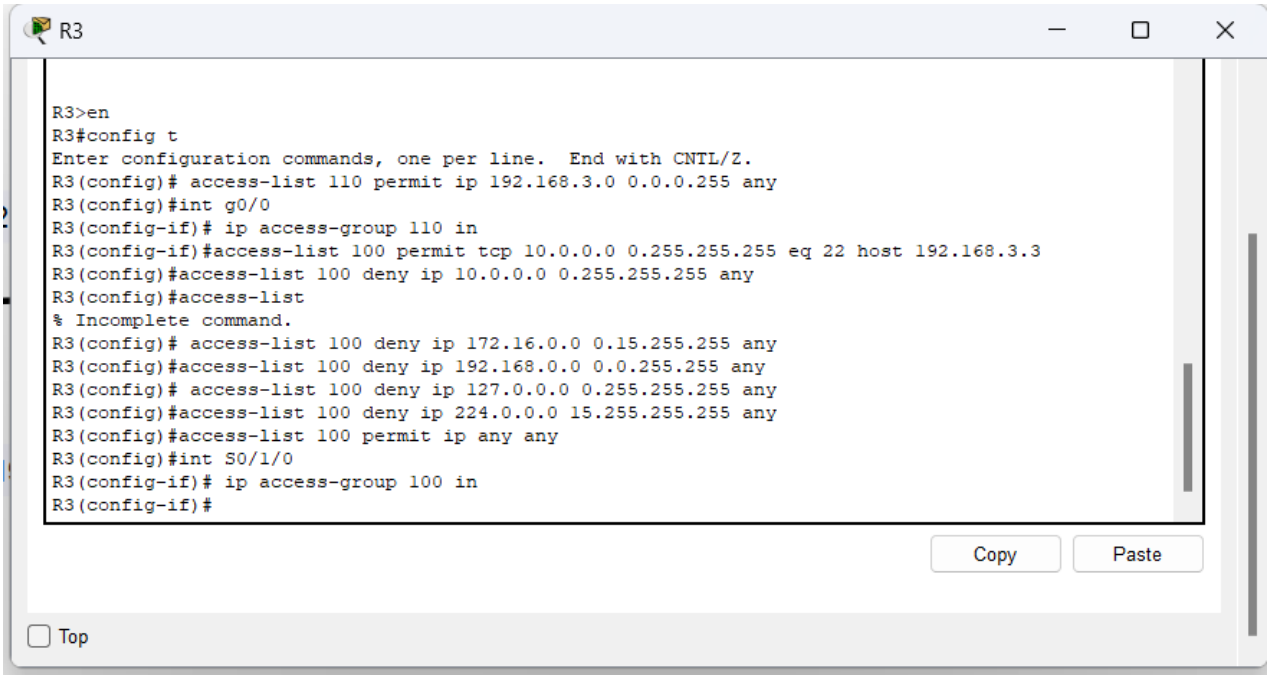


PC-C



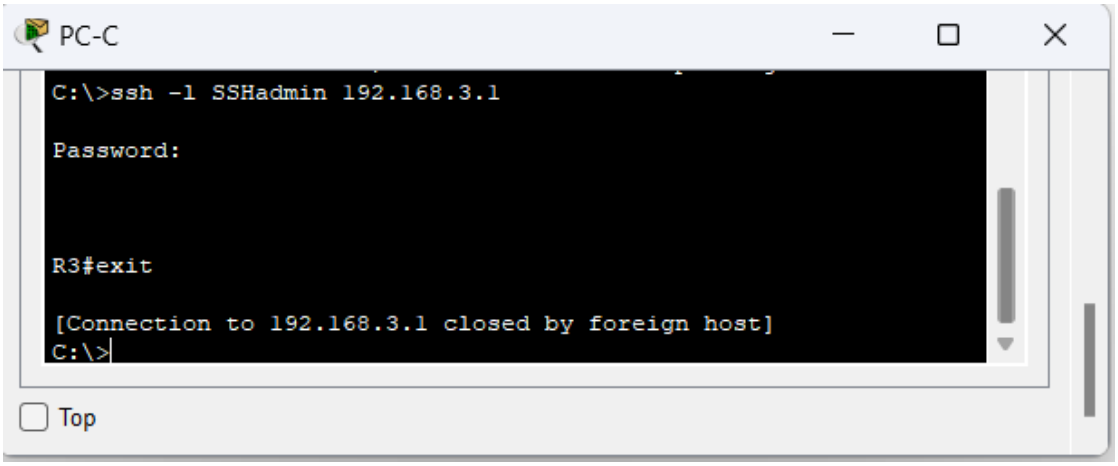
Part - 3.3 : Permit PC-C to access R3 via ssh

R3



(PC-C getting SSH access via R3)

PC-C

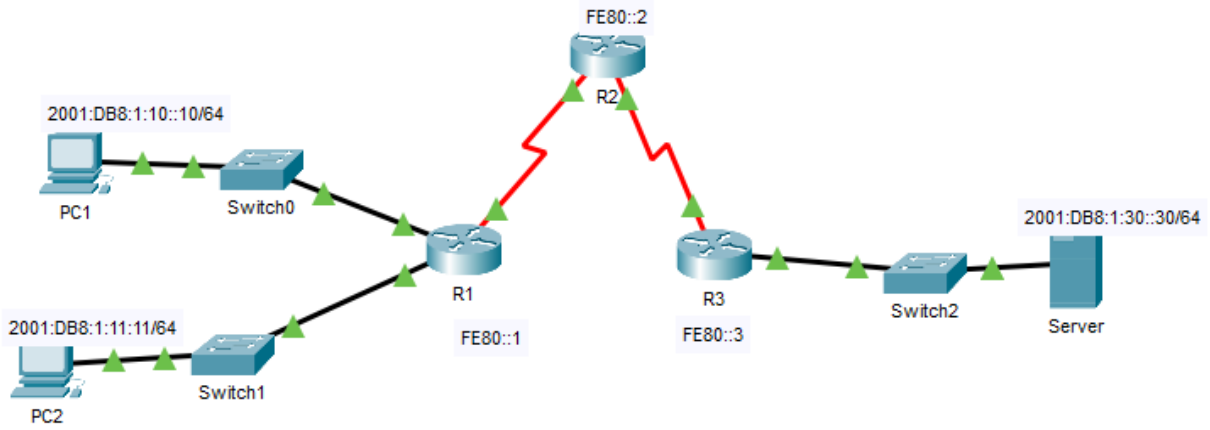


Configuring IPv6 ACLs

Configure IPv6 ACLs (Active Control Lists) to allow access to authorized communication in case of IPv6 environment.
PART 1: Configure an IPv6 ACL that will block HTTP and HTTPS access.
PART 2: Configure an IPv6 ACL that will block ICMP.
Procedure:

PART 0: Build the topology and verify the connectivity.

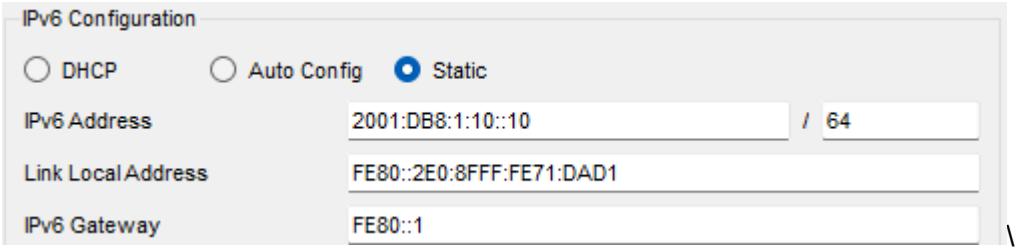
1. Open Cisco packet tracer and create a topology as shown in diagram



2. Use following Addressing table to assign IP addresses to various interfaces ad end-points. Also change the display name and Hostname of each device using 'Config" tab under 'Settings'.

Device	Interface	IPv6 Address/Prefix	Default Gateway
PC1	NIC	2001:DB8:1:10::10/64	FE80::1
PC2	NIC	2001:DB8:1:11::11/64	FE80::1
R1	gig0/0	2001:DB8:1:10::1/64	FE80::1
	gig0/1	2001:DB8:1:11::1/64	FE80::1
	se0/1/0	2001:DB8:1:1::1/64	FE80::1
R2	se0/1/0	2001:DB8:1:1::2/64	FE80::2
	se0/1/1	2001:DB8:1:2::2/64	FE80::2
R3	gig0/0	2001:DB8:1:30::1/64	FE80::3
	se0/1/0	2001:DB8:1:2::1/64	FE80::3
Server	NIC	2001:DB8:1:30::30/64	FE80::3

A) Assign IPv6 addresses to PC1, PC2 and Server under Desktop -> IP configuration -> IPv6 configuration.
For PC1



Similarly, assign to PC2 and Server.

B) Assign IPv6 addresses to various interfaces of Routers R1, R2 and R3 using CLI.
For interfaces of R1,

```
R1(config)#ipv6 unicast-routing
R1(config)#int g0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:10::1/64
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R1(config-if)#int g0/1
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:11::1/64
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)#int s0/1/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
R1(config-if)#ipv6 add FE80::1 link-local
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#
```

For interfaces of R2

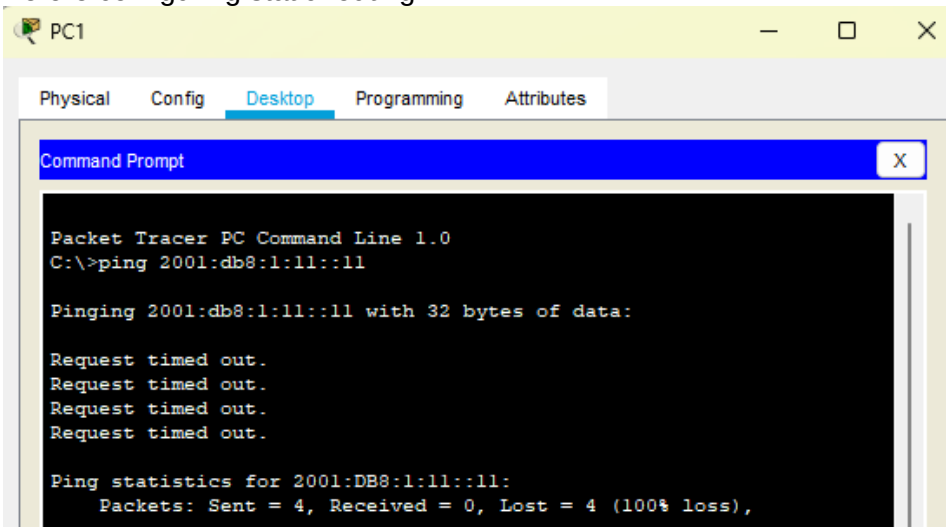
```
R2(config)#ipv6 unicast-routing
R2(config)#int s0/1/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:1::2/64
R2(config-if)#ipv6 add FE80::2 link-local
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

R2(config-if)#int
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up
R2(config-if)#int s0/1/1
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:2::2/64
R2(config-if)#ipv6 add FE80::2 link-local
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R2(config-if)#
```

For interfaces of R3

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#int g0/0
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2001:DB8:1:30::1/64
R3(config-if)#ipv6 add FE80::3 link-local
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

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

R3(config-if)#int s0/1/0
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2001:DB8:1:2::1/64
R3(config-if)#ipv6 add FE80::3 link-local
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

3. Configure static routing for R1

Before configuring static routing

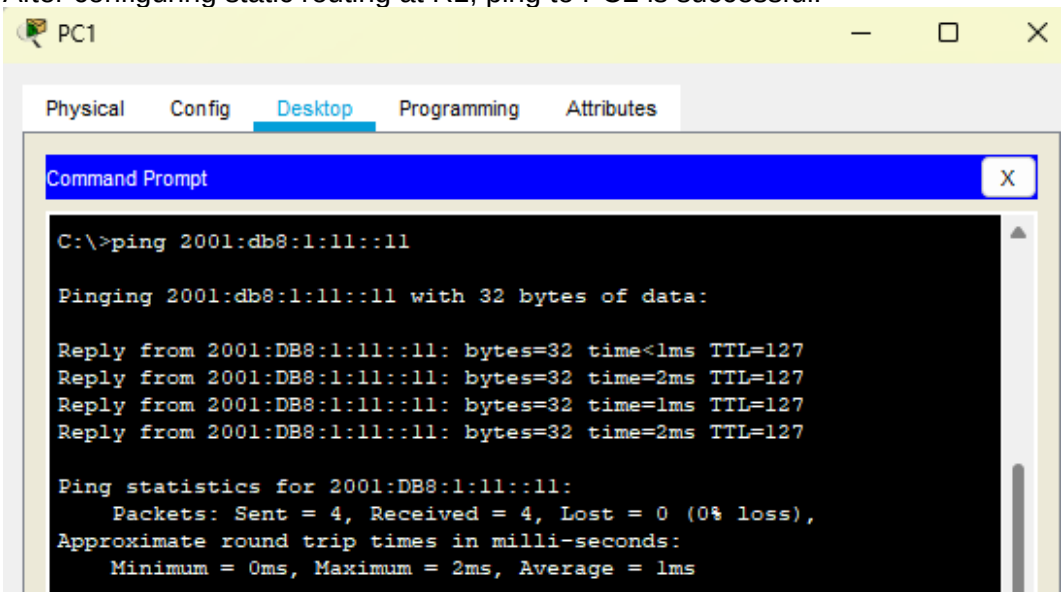


COMMAND FORMAT is - ipv6 route <network address that R1 doesn't know> <next hop>. The router R1 doesn't have established the neighbor-ship with the network between R2 and R3 (2001:DB8:1:1:), and the network between R3 and server (2001:DB8:1:30::). These both networks are accessible to R1 through the interface s0/1/0 of R2. Its IPv6 address is 2001:DB8:1:1::2.

A) Configure static routing for R1

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 route 2001:DB8:1:2::/64 2001:DB8:1:1::2
R1(config)#ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:1::2
```

After configuring static routing at R1, ping to PC2 is successful.

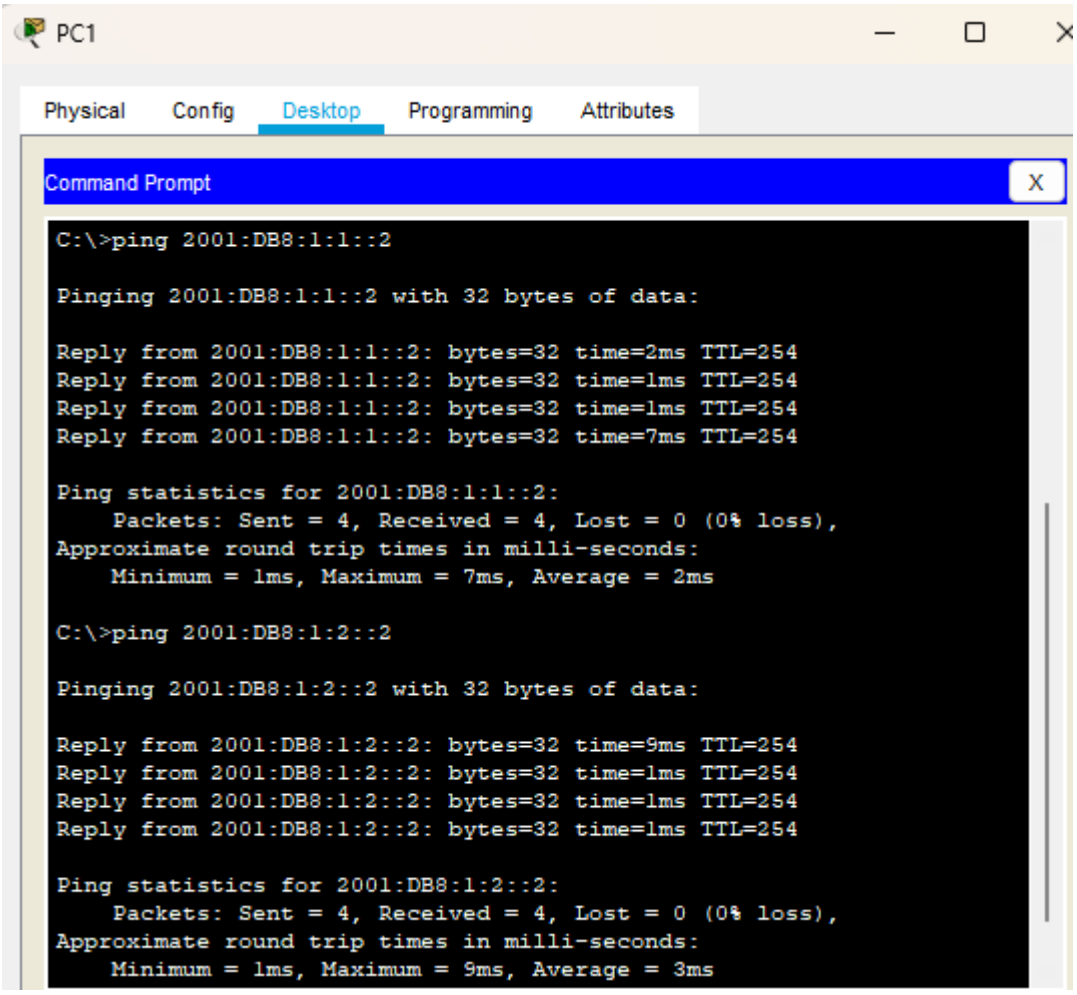


B) Configure static routing at R2.

The router R2 doesn't have established the neighbor-ship with the network between R1 and PC1 (2001:DB8:1:10::) and between R1 and PC2 (2001:DB8:1:11:), and the network between R3 and server (2001:DB8:1:30::). These both networks are accessible to R2 through the interfaces s0/1/0 of R1 and through interface s0/1/0 of R3. Its IPv6 address is 2001:DB8:1:1::1 and 2001:DB8:1:2::1.

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:1::1
R2(config)#ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:1::1
R2(config)#ipv6 route 2001:DB8:1:30::/64 2001:DB8:1:2::1
R2(config)#
```

After configuring static routing at R2,

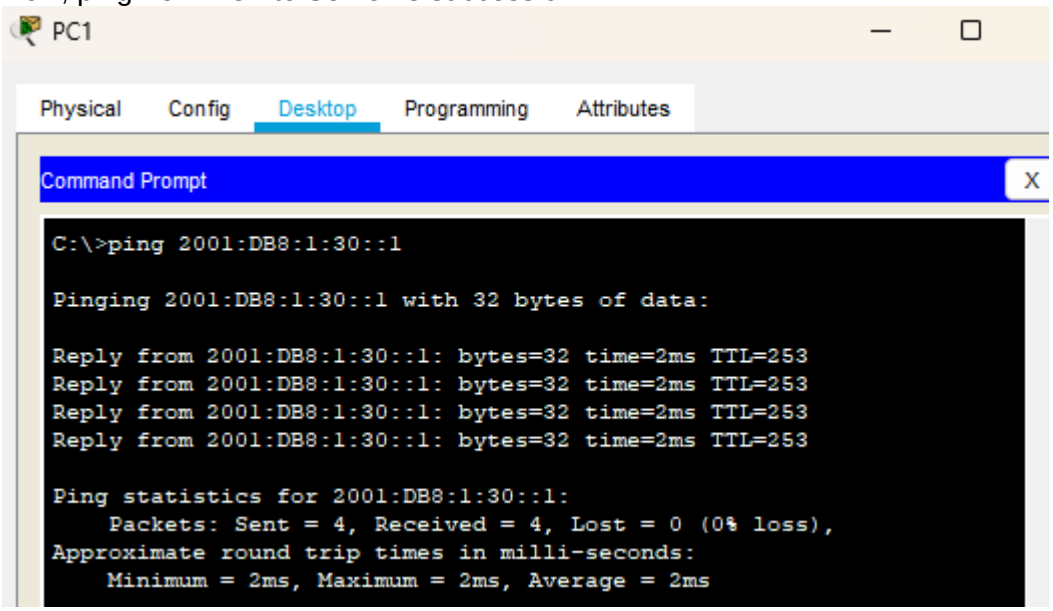


Ping from PC1 to R3 is successful

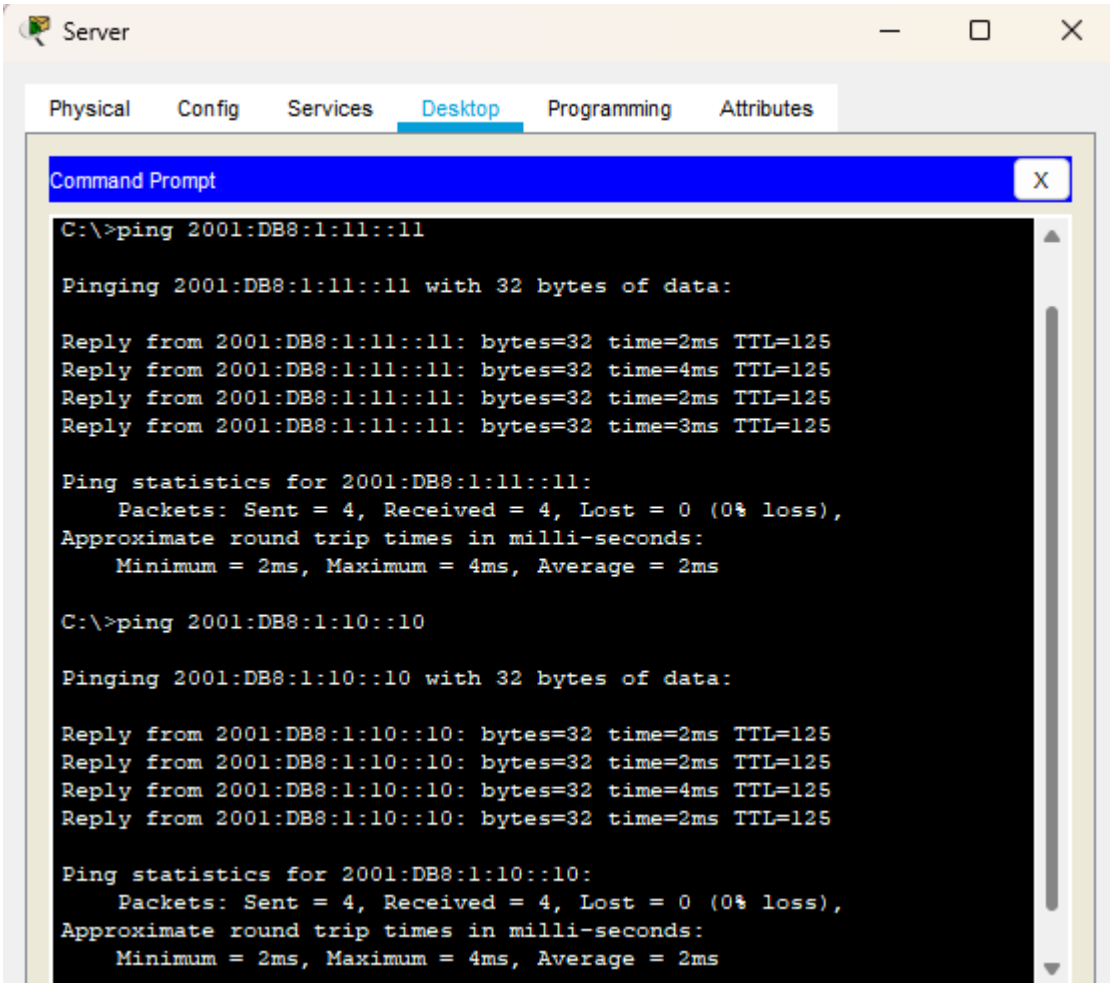
C) Similarly, configure static routing at R3.

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 route 2001:DB8:1:10::/64 2001:DB8:1:2::2
R3(config)#ipv6 route 2001:DB8:1:11::/64 2001:DB8:1:2::2
R3(config)#ipv6 route 2001:DB8:1:1::/64 2001:DB8:1:2::2
R3(config)#
```

Now, ping from PC1 to Server is successful.

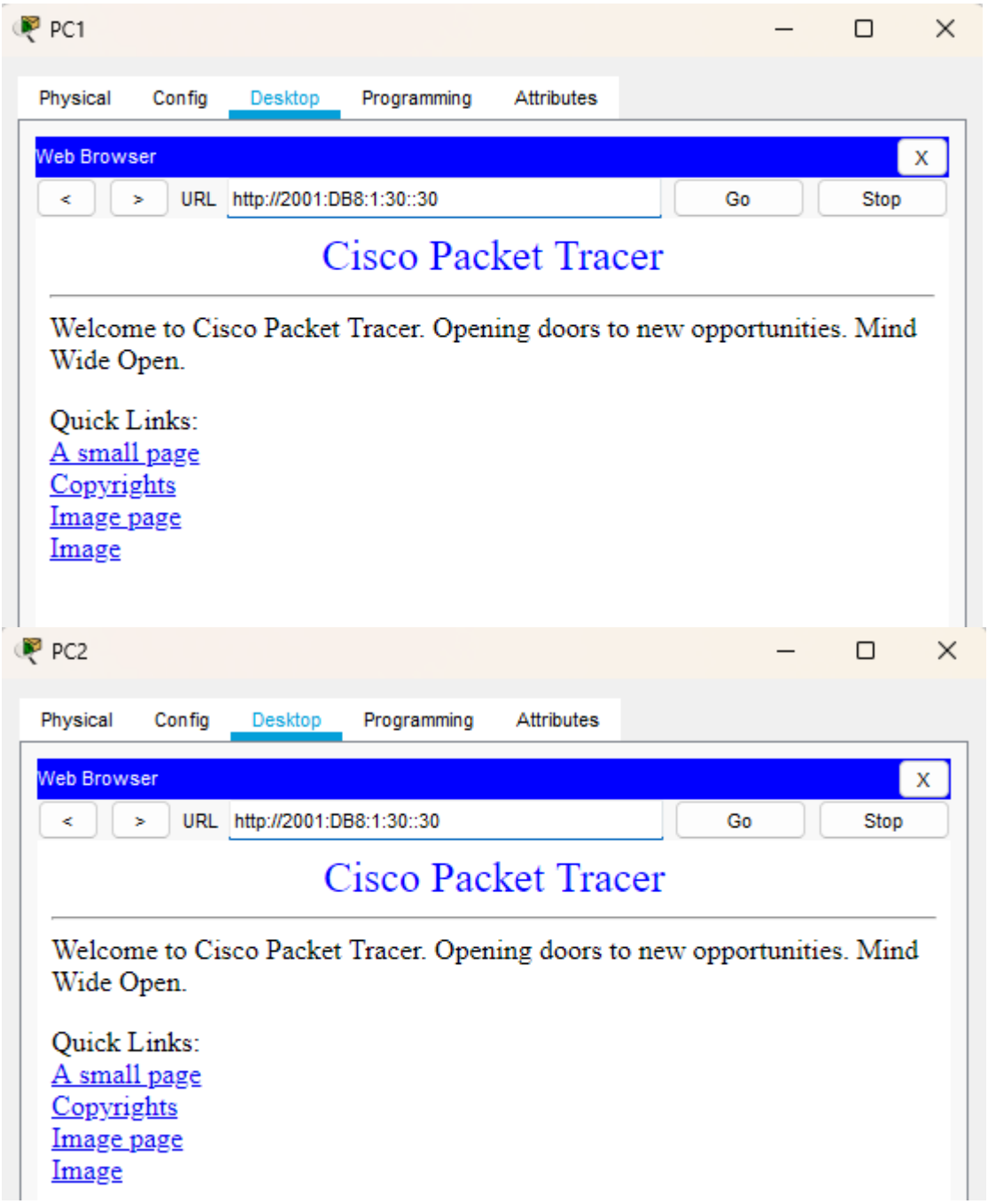


Also ping from Server to PC1 and PC2 is successful.



PART 1: Configure an IPv6 ACL that will block HTTP and HTTPS access.

Logs indicate that a computer on the 2001:DB8:1:11::0/64 network is repeatedly refreshing web page. This is causing a Denial-of-Service (DoS) attack against Server3. Until the client can be identified and cleaned, you must block HTTP and HTTPS access to that network with an access list .Before configuring ACL at R1 to block HTTP and HTTPS access to Server, the website hosted by Server is appe aring on both PC1 and PC2.



Step 1: Configure an ACL that will block HTTP and HTTPS access from PC2.

```
R1(config)#ipv6 access-list BLOCK_HTTP
R1(config-ipv6-acl)#
```

Configure an ACL named BLOCK_HTTP on R1 with the following statements.

A) Block HTTP and HTTPS traffic from reaching Server.

```
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
```

B) Allow all other IPv6 traffic to pass.

```
R1(config-ipv6-acl)#permit ipv6 any any
```

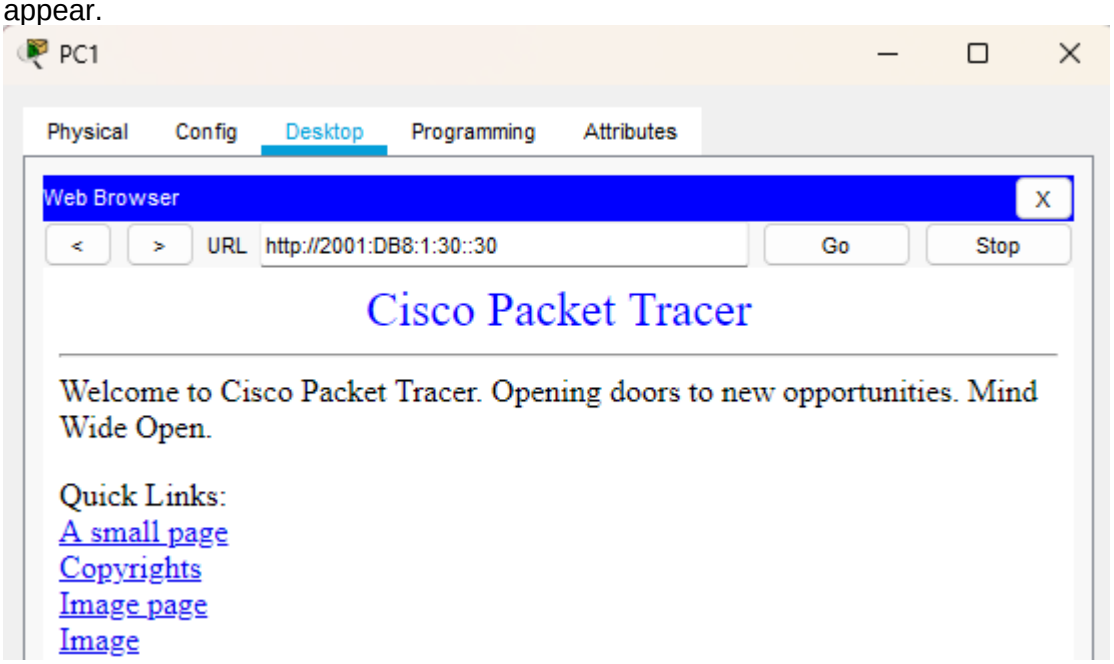
Step 2: Apply the ACL to the interface G0/1 only as PC2 is connected to this interface.
(Apply the ACL on the interface closest to the source of the traffic to be blocked)

```
R1(config)#int g0/1
R1(config-if)#ipv6 traffic-filter BLOCK_HTTP in
```

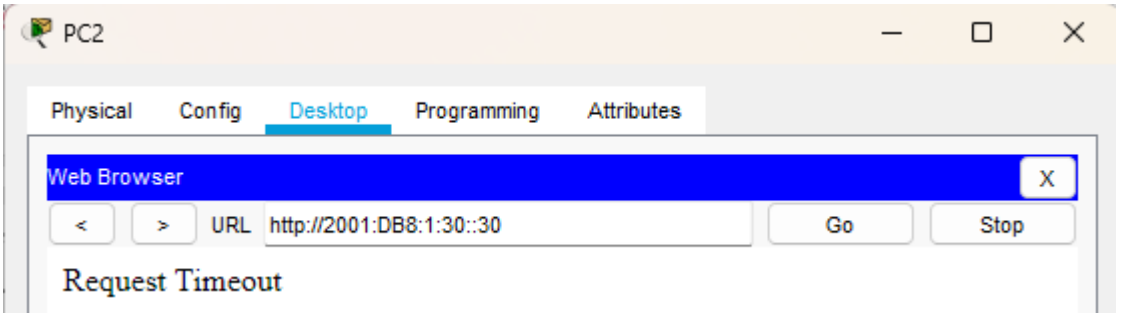
Step 3: Verify the ACL implementation.

Verify that the ACL is operating as intended by conducting the following tests:

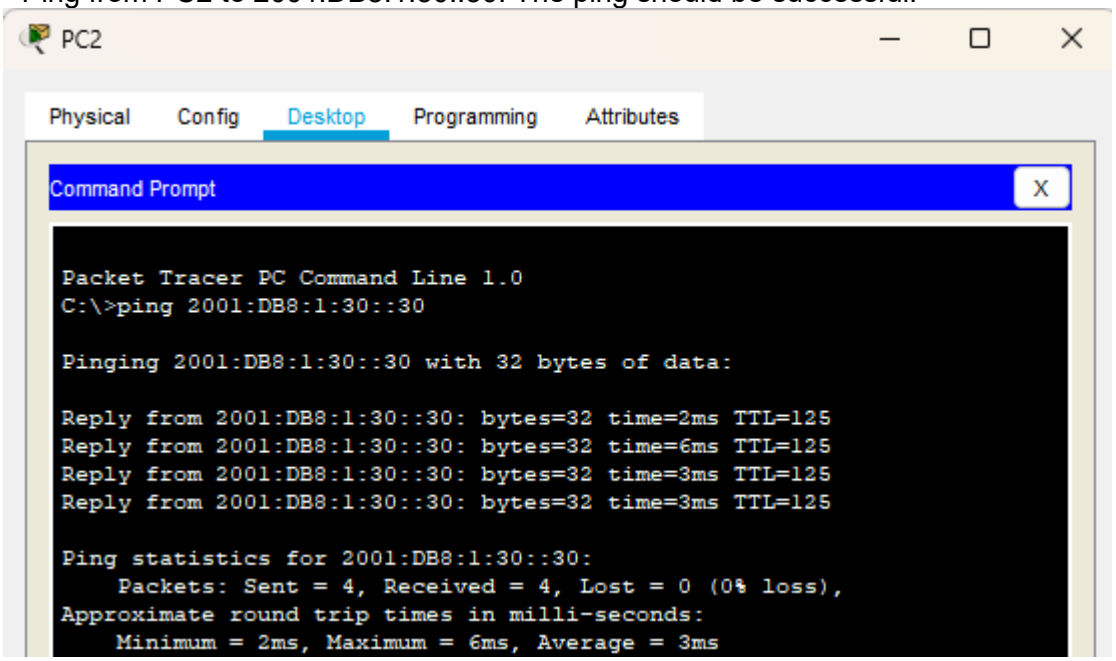
• Open the web browser of PC1 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should appear.



• Open the web browser of PC2 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should be blocked.



• Ping from PC2 to 2001:DB8:1:30::30. The ping should be successful.



PART 2: Configure an IPv6 ACL that will block ICMP access.

The logs now indicate that your server is receiving pings from many different IPv6 addresses in a Distributed Denial of Service (DDoS) attack. You must filter ICMP ping requests to your server.

Step 1: Create an access list to block ICMP.

Configure an ACL named BLOCK_ICMP on R3 with the following statements

```
R3(config)#ipv6 access-list BLOCK_ICMP
R3(config-ipv6-acl)#
```

A) Block all ICMP traffic from any hosts to any destination.

```
R3(config-ipv6-acl)#deny icmp any any
```

B) Allow all other IPv6 traffic to pass.

```
R3(config-ipv6-acl)#permit ipv6 any any
```

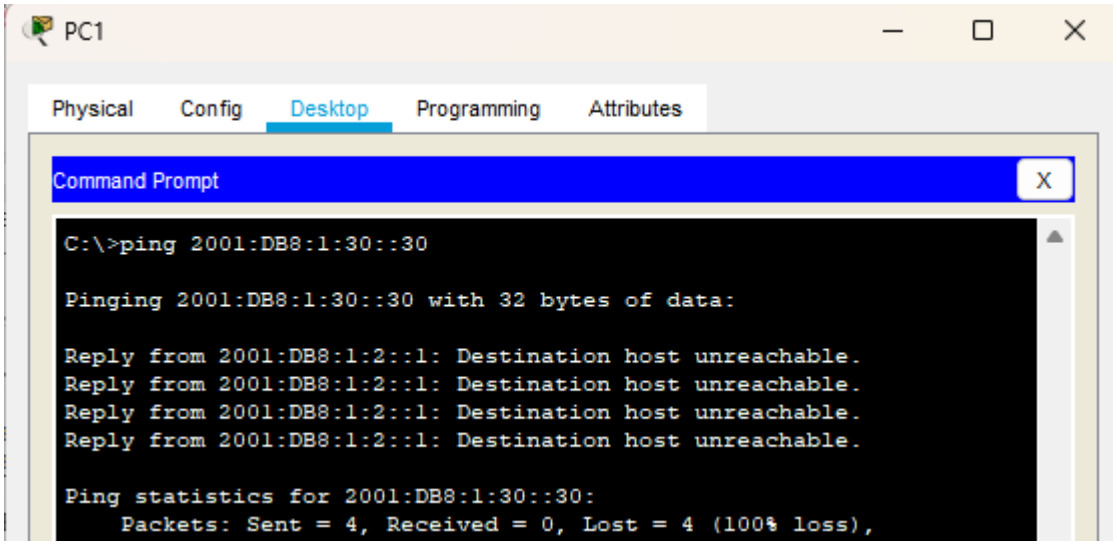
Step 2: Apply the ACL to the correct interface.

In this case, ICMP traffic can come from any source (PC1 or PC2). To ensure that ICMP traffic is blocked regardless of its source or any changes that occur to the network topology, apply the ACL closest to the destination (interface G0/0 of R3).

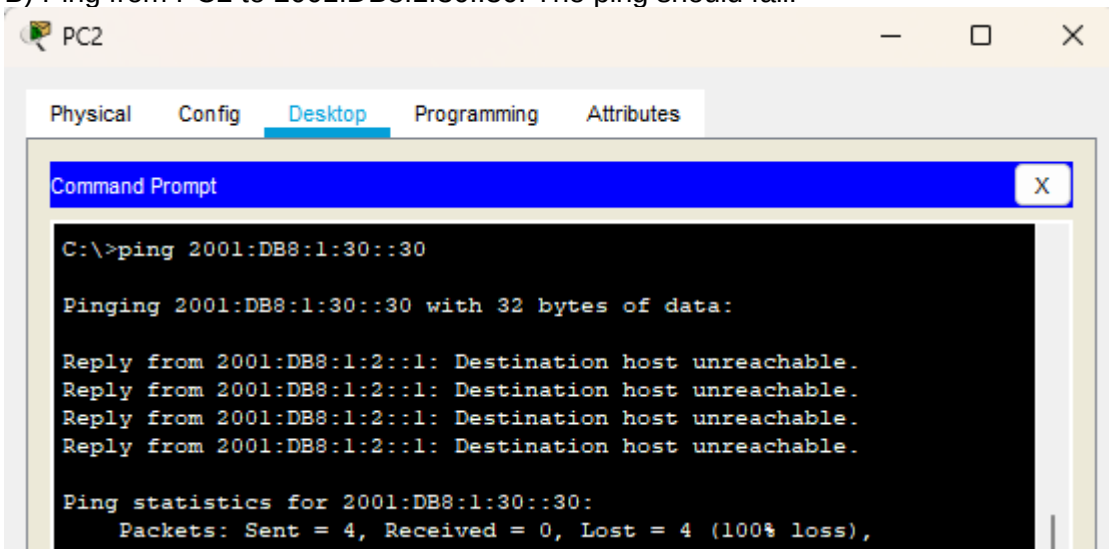
```
R3(config)#int g0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP out
```

Step 3: Verify that the proper access list functions.

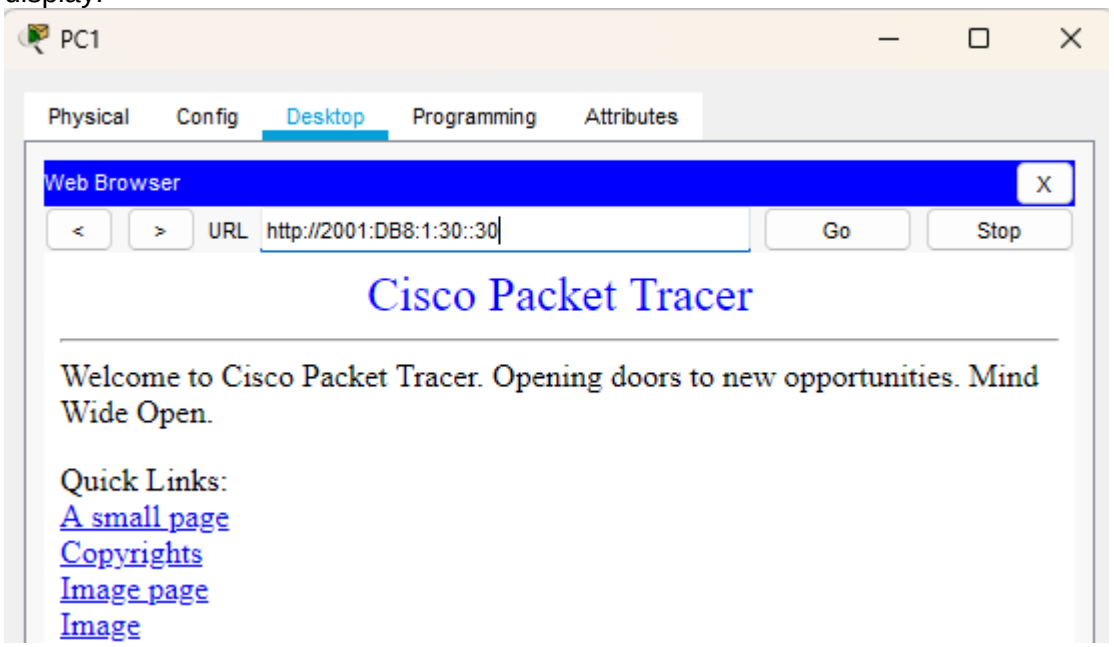
A) Ping from PC1 to 2001:DB8:1:30::30. The ping should fail.



B) Ping from PC2 to 2001:DB8:1:30::30. The ping should fail.



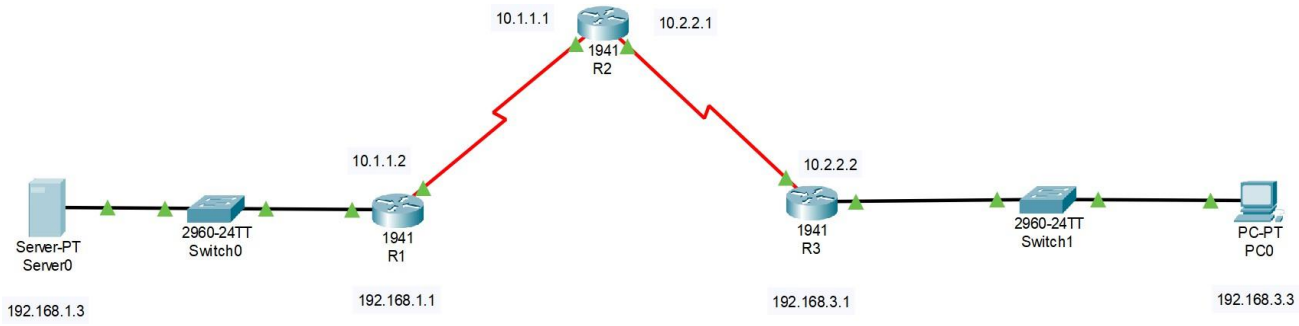
C) Open the web browser of PC1 to http://2001:DB8:1:30::30 or https://2001:DB8:1:30::30. The website should display.



Practical-5

Aim : Configuring a Zone-Based Policy Firewall (ZPF)

Topology:



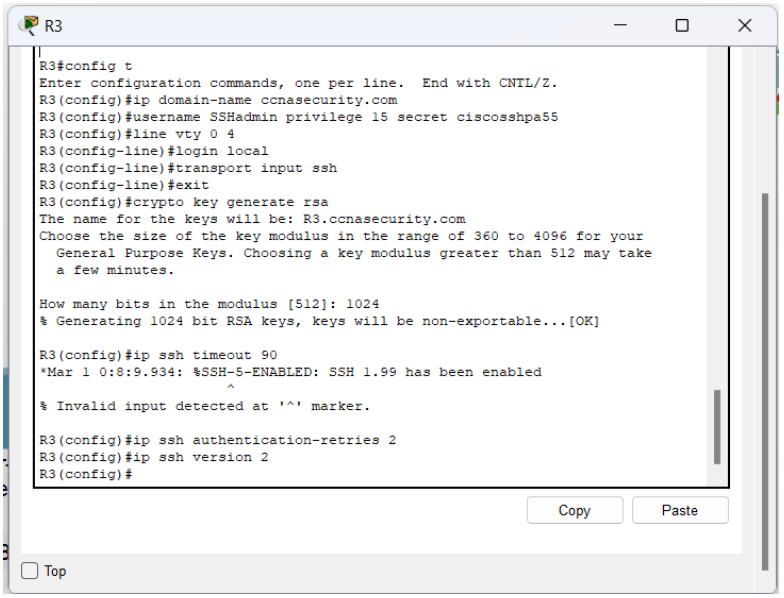
Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	-
	S0/1/0	10.1.1.1	255.255.255.252	-
R2	S0/1/0	10.1.1.2	255.255.255.252	-
	S0/1/1	10.2.2.2	255.255.255.252	-
R3	G0/0	192.168.3.1	255.255.255.0	-
	S0/1/0	10.2.2.1	255.255.255.252	-
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

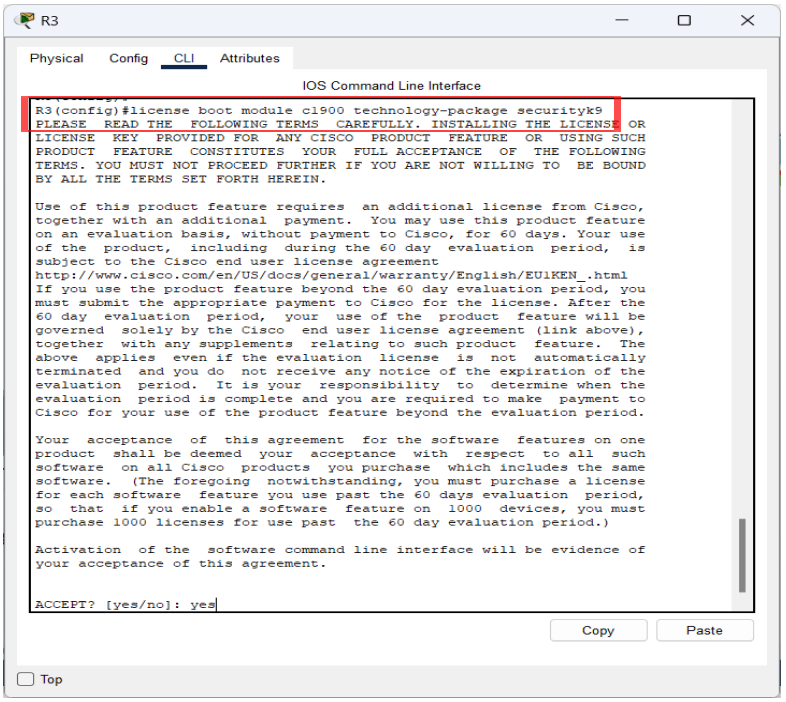
(NOTE: After applying the RIP, check with the ping command from multiple devices to verify successful connection.)

Commands:

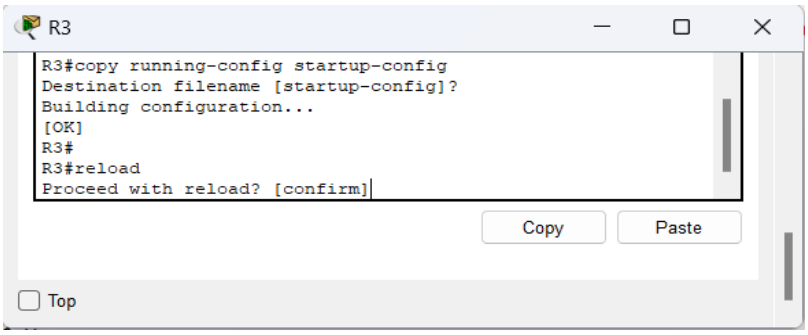
R3



R3



R3



R3

R3

Physical Config CLI Attributes

IOS Comma

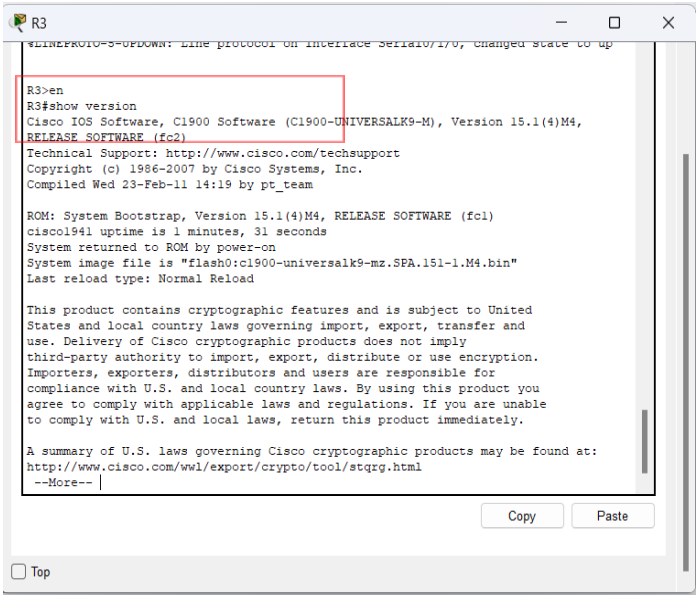
```
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                 SN
-------------------------------------------------
*0        CISCO1941/K9        FTX1524R90Z-


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


R3#
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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
% Incomplete command.
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)#int G0/0
R3(config-if)# zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#int s0/1/0
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#
```

R3

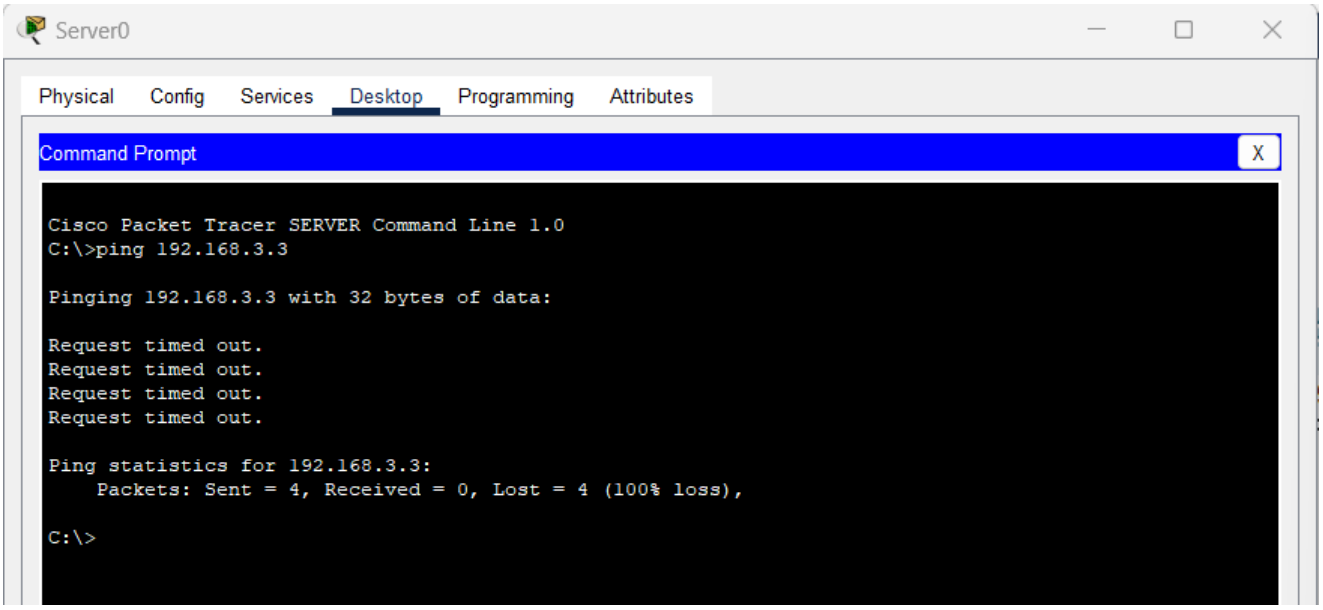
Physical Config CLI Attributes

```
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################ [OK]
Smart Init is enabled
smart init is sizing iomem
           TYPE        MEMORY_REQ
          HWIC Slot 0      0x00200000
          HWIC Slot 1      0x00200000     Onboard devices &
         buffer pools      0x01E8F000
-------------------------------------------------
           TOTAL:          0x02E8F000
Rounded IOMEM up to: 48Mb.
Using 6 percent iomem. [48Mb/512Mb]

             Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
4 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
```

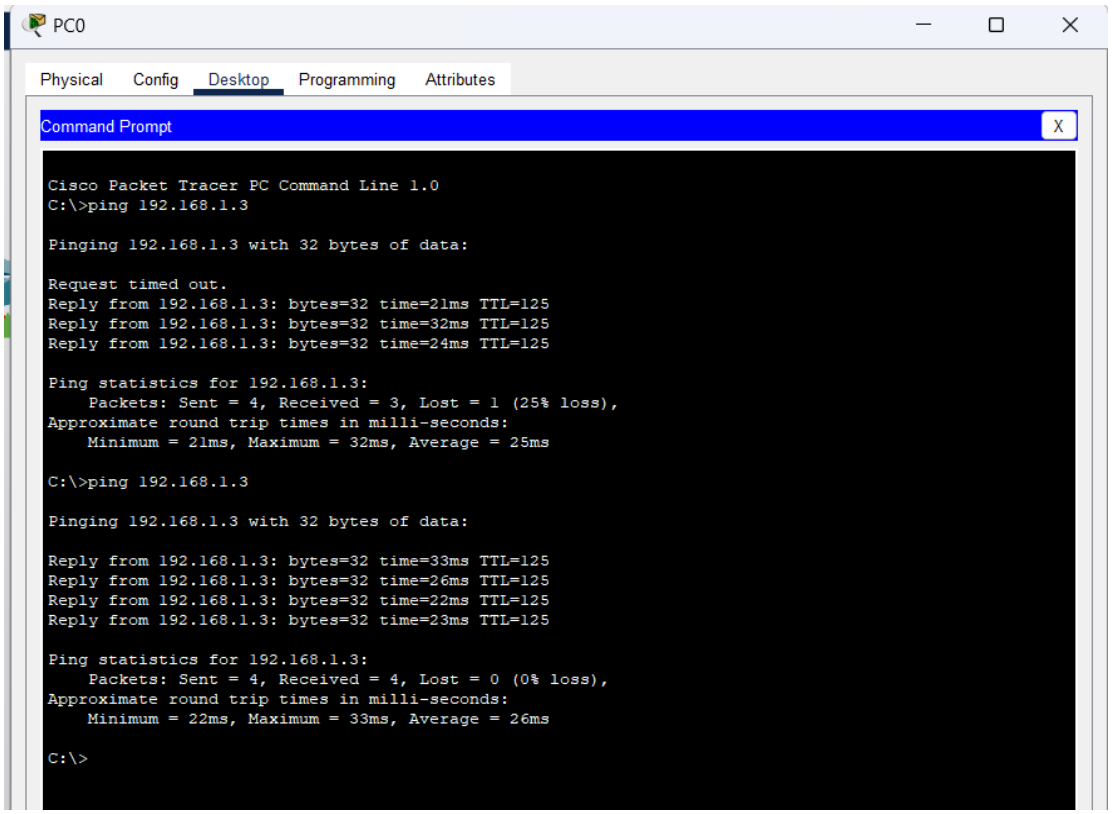
R3



Ping from PC-A -> PC-C, will not work.



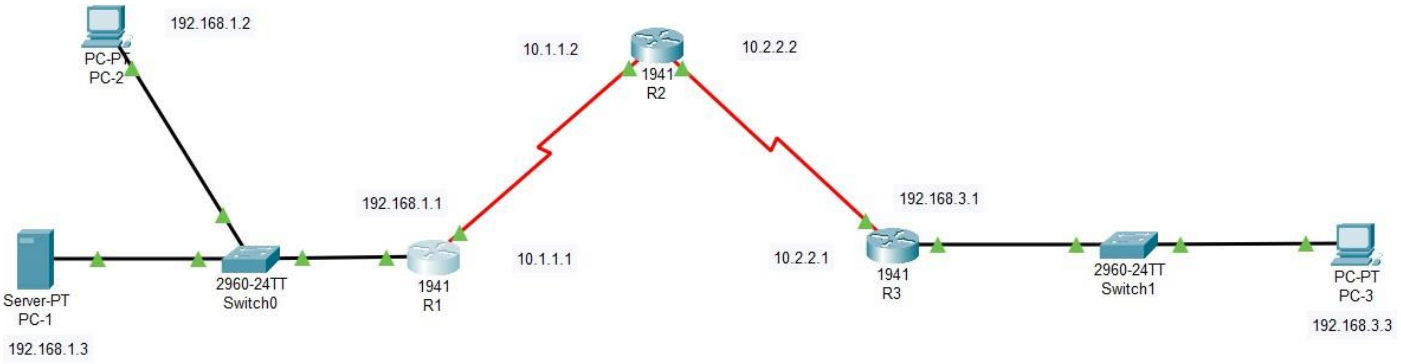
Ping from PC-C -> PC-A, will work.



Practical-6

Aim: Configure Intrusion Prevention System (IPS), using the CLI

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	-
	S0/1/0	10.1.1.1	255.255.255.252	-
R2	S0/1/0	10.1.1.2	255.255.255.252	-
	S0/1/1	10.2.2.2	255.255.255.252	-
R3	G0/0	192.168.3.1	255.255.255.0	-
	S0/1/0	10.2.2.1	255.255.255.252	-
PC-1	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-2	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-3	NIC	192.168.3.3	255.255.255.0	192.168.3.1

(NOTE: After applying the RIP, check with the ping command from multiple devices to verify successful connection.)

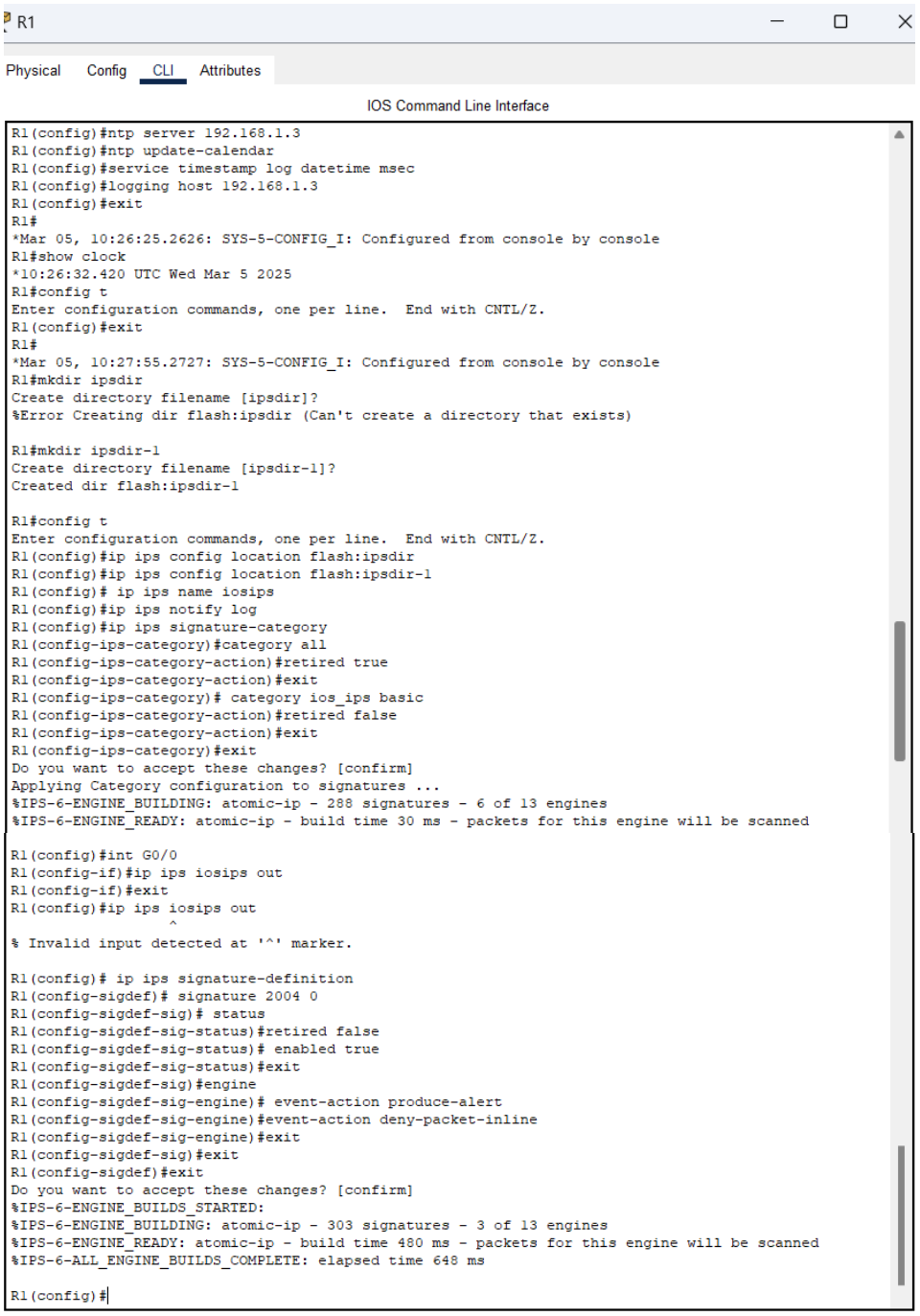
Commands:
(First the Security Technology Package enabling commands.)

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

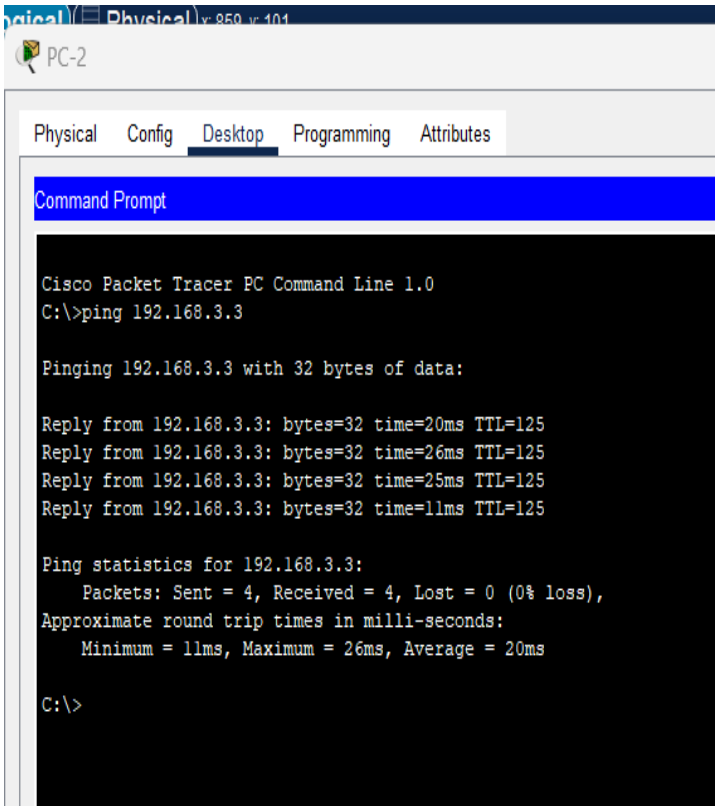
- yes

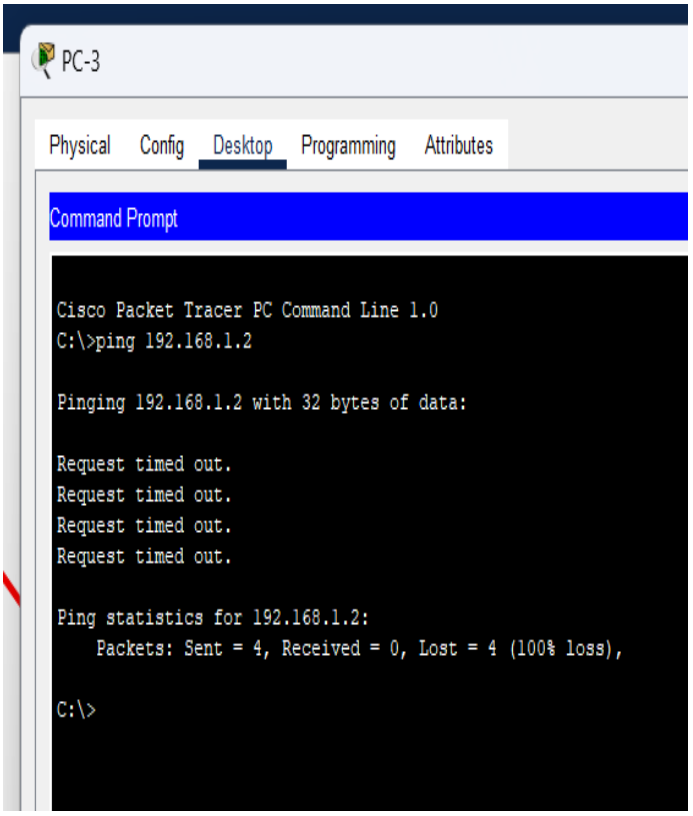
#copy running-config startup-config #reload

#show version

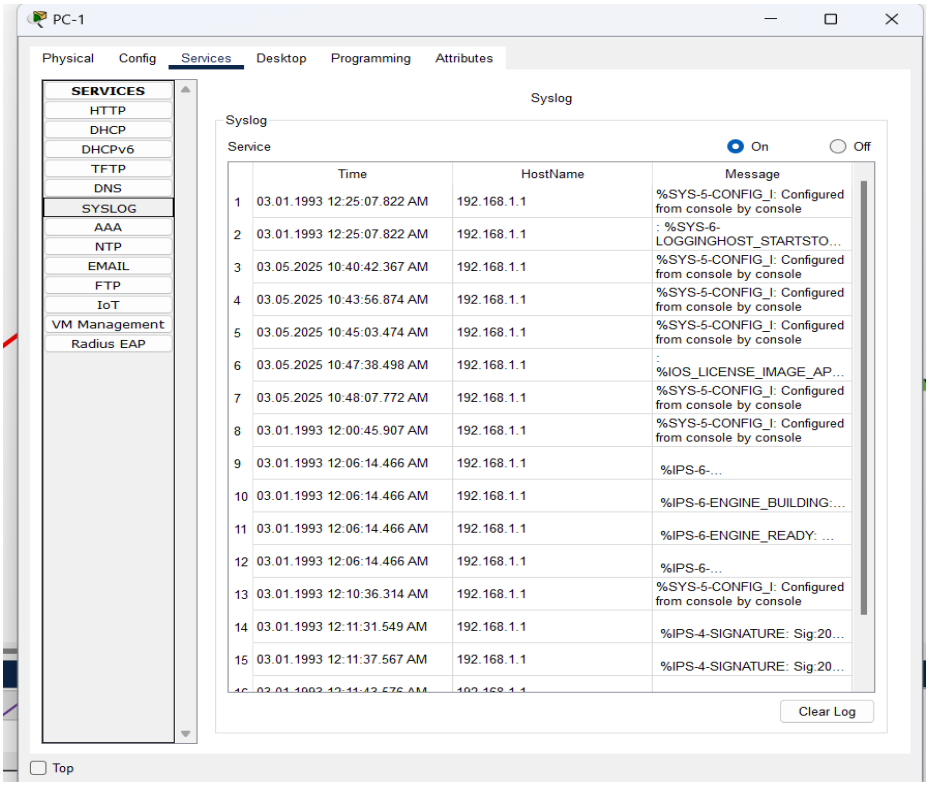


(PC-2 will ping PC-3, but PC-3 will not be able to ping PC-2)





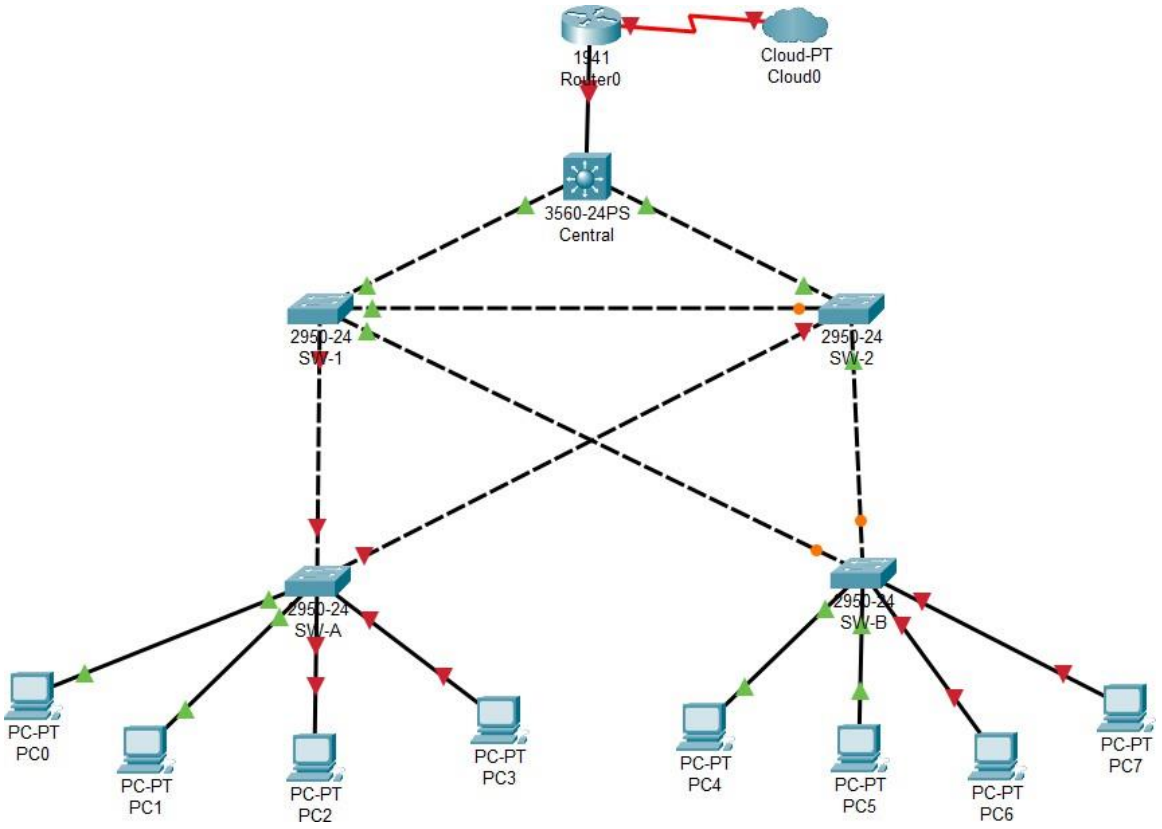
PC1 Syslog service



Practical-7

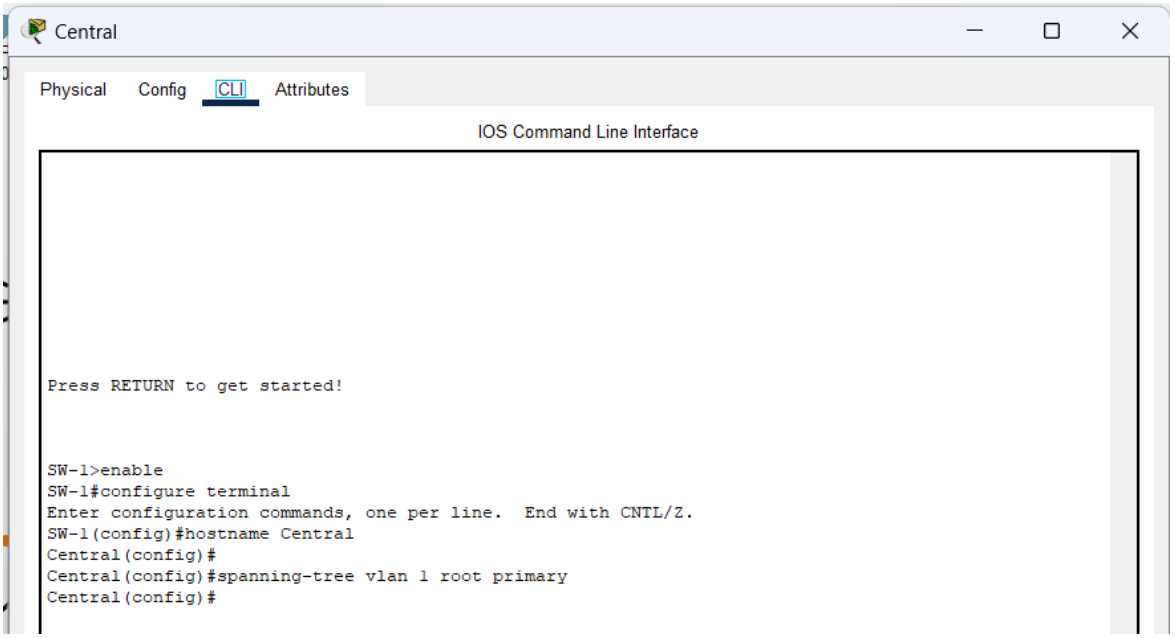
Aim : Packet Tracer - Layer 2 Security

Topology:

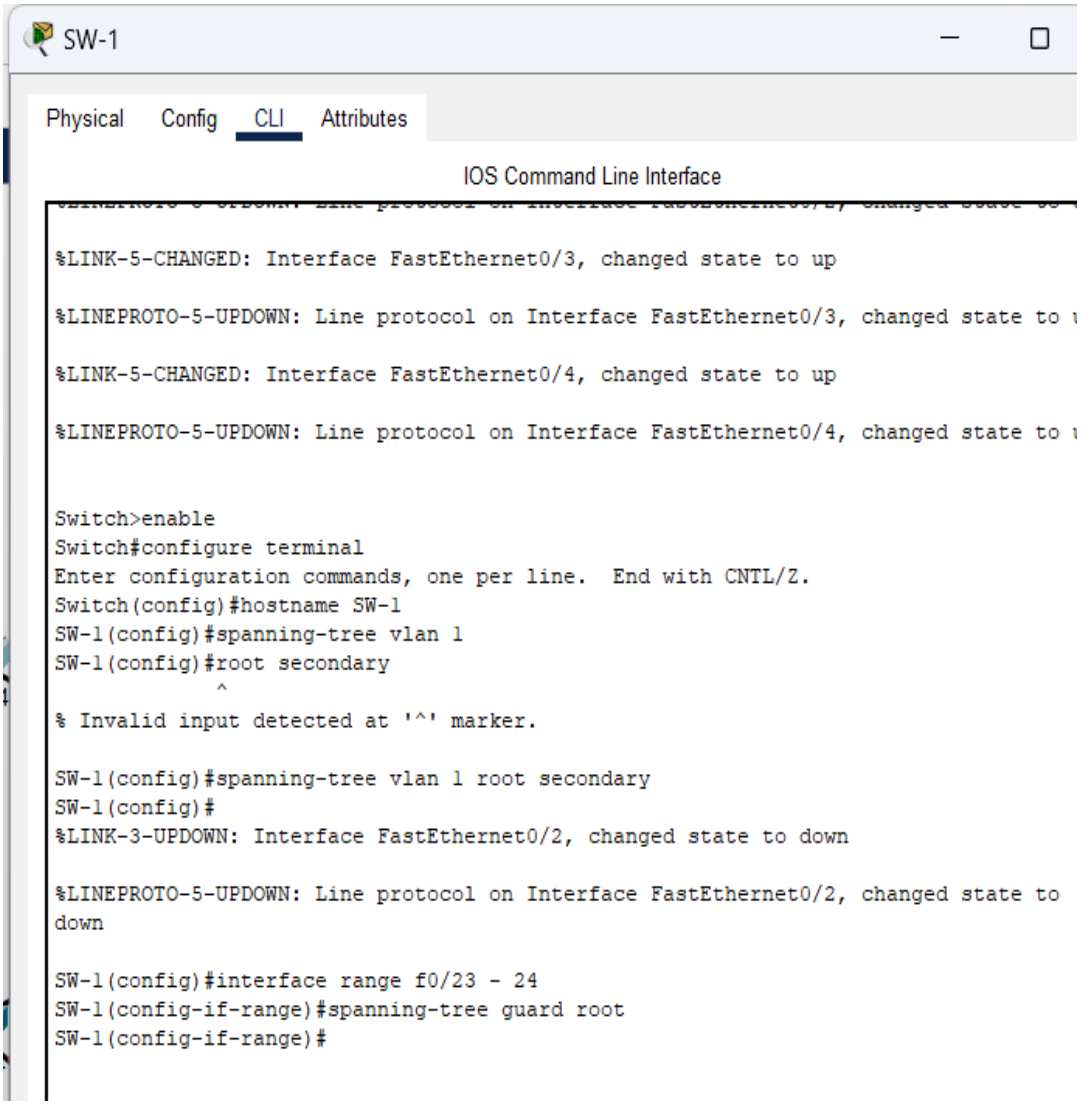


Commands:

Switch 1



Switch 1


SW-1
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-1
SW-1(config)#spanning-tree vlan 1
SW-1(config)#root secondary
^
% Invalid input detected at '^' marker.
SW-1(config)#spanning-tree vlan 1 root secondary
SW-1(config)#
%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to
down
SW-1(config)#interface range f0/23 - 24
SW-1(config-if-range)#spanning-tree guard root
SW-1(config-if-range)#

Switch A

SW-A

Physical Config CLI Attributes

```
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-A
SW-A(config)# interface range f0/1 - 4
SW-A(config-if-range)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
```

SW-A

Physical Config CLI Attributes

IOS Command Line Interface

```
SW-A(config-if-range)#exit
SW-A(config)# interface range f0/1 - 22
SW-A(config-if-range)# switchport mode access
SW-A(config-if-range)#switchport port-security
SW-A(config-if-range)#switchport port-security maximum 2
SW-A(config-if-range)#switchport port-security violation shutdown
SW-A(config-if-range)#switchport port-security mac-address stick
SW-A(config-if-range)#exit
SW-A(config)#interface range f0/5 - 22
SW-A(config-if-range)# shutdown
```

Top

Switch B

SW-B

Physical Config CLI Attributes

```
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up


Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-B
SW-B(config)#interface range f0/1 - 4
SW-B(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
```

Top

SW-B

Physical Config CLI Attributes

IOS Comm

```
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
SW-B(config-if-range)#exit
SW-B(config)# interface range f0/1 - 22
SW-B(config-if-range)# switchport mode access
SW-B(config-if-range)#%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.

%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/2 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/2 on VLAN0001. Inconsistent port type.


SW-B(config-if-range)#switchport port-security
SW-B(config-if-range)#
SW-B(config-if-range)# switchport port-security maximum 2
SW-B(config-if-range)# switchport port-security violation shutdown
SW-B(config-if-range)# switchport port-security mac-address sticky
SW-B(config-if-range)#exit
SW-B(config)# interface range f0/5 - 22
SW-B(config-if-range)#shutdown
```

SW-A

Physical Config CLI Attributes

```
SW-A(config-if-range)#exit
SW-A(config)#exit
SW-A#
%SYS-5-CONFIG_I: Configured from console by console

SW-A#show port-security int f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW-A#
```

SW-B

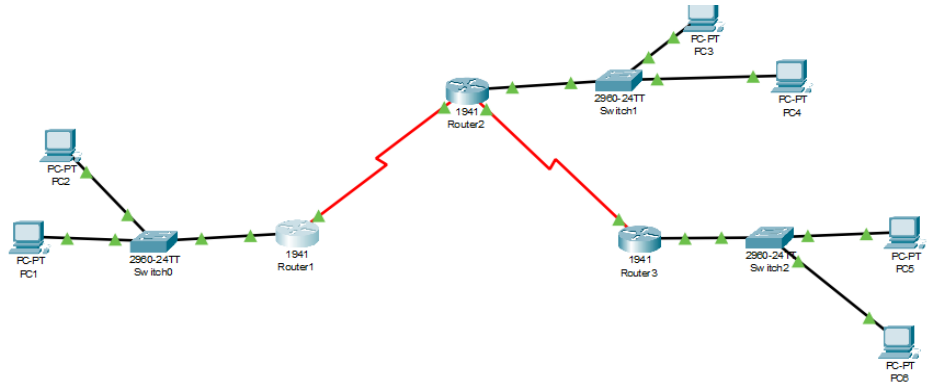
Physical Config CLI Attributes

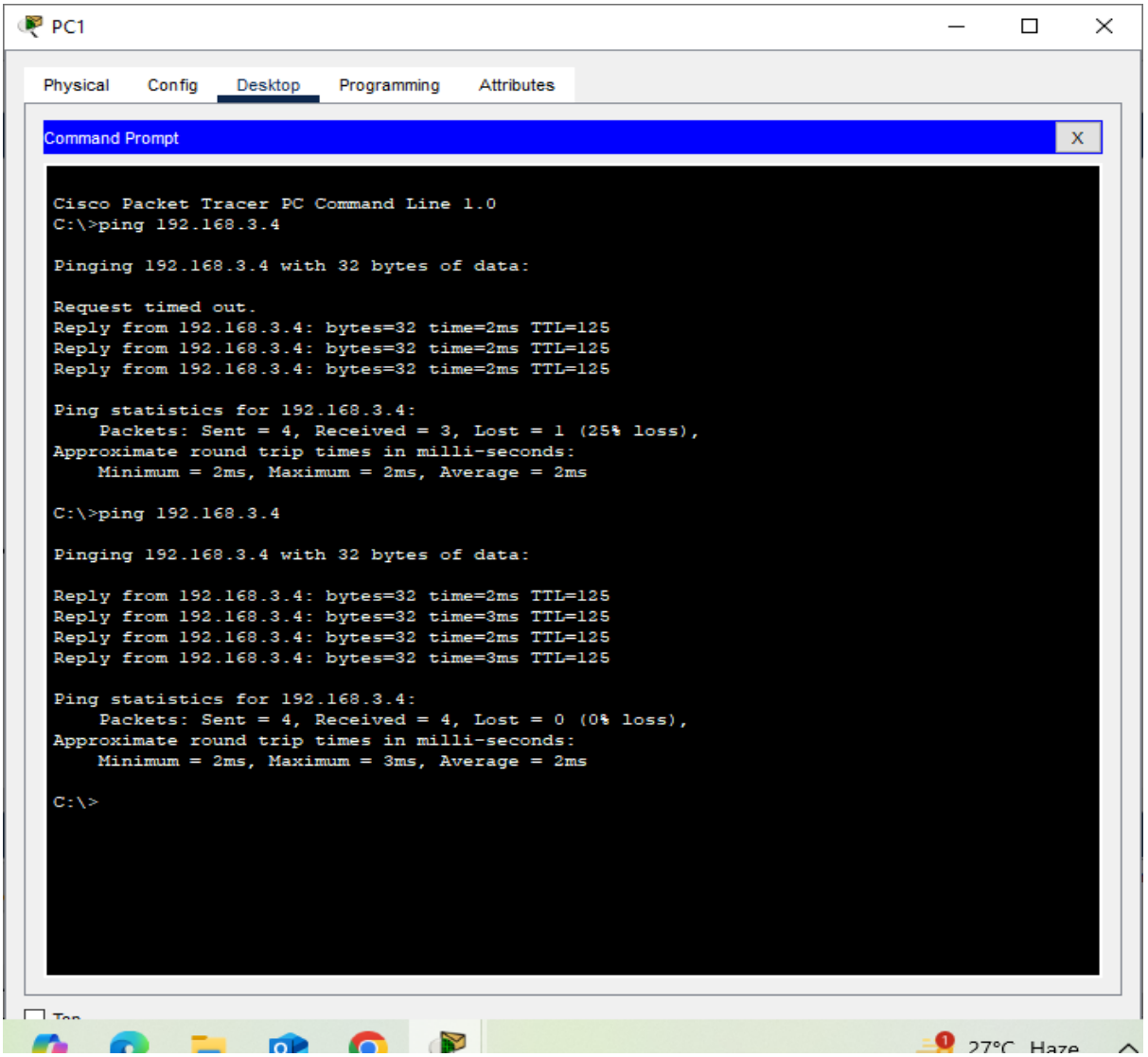
```
SW-B(config-if-range)#exit
SW-B(config)#exit
SW-B#
%SYS-5-CONFIG_I: Configured from console by console

SW-B# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0002.177A.B902:1
Security Violation Count   : 0

SW-B#
```

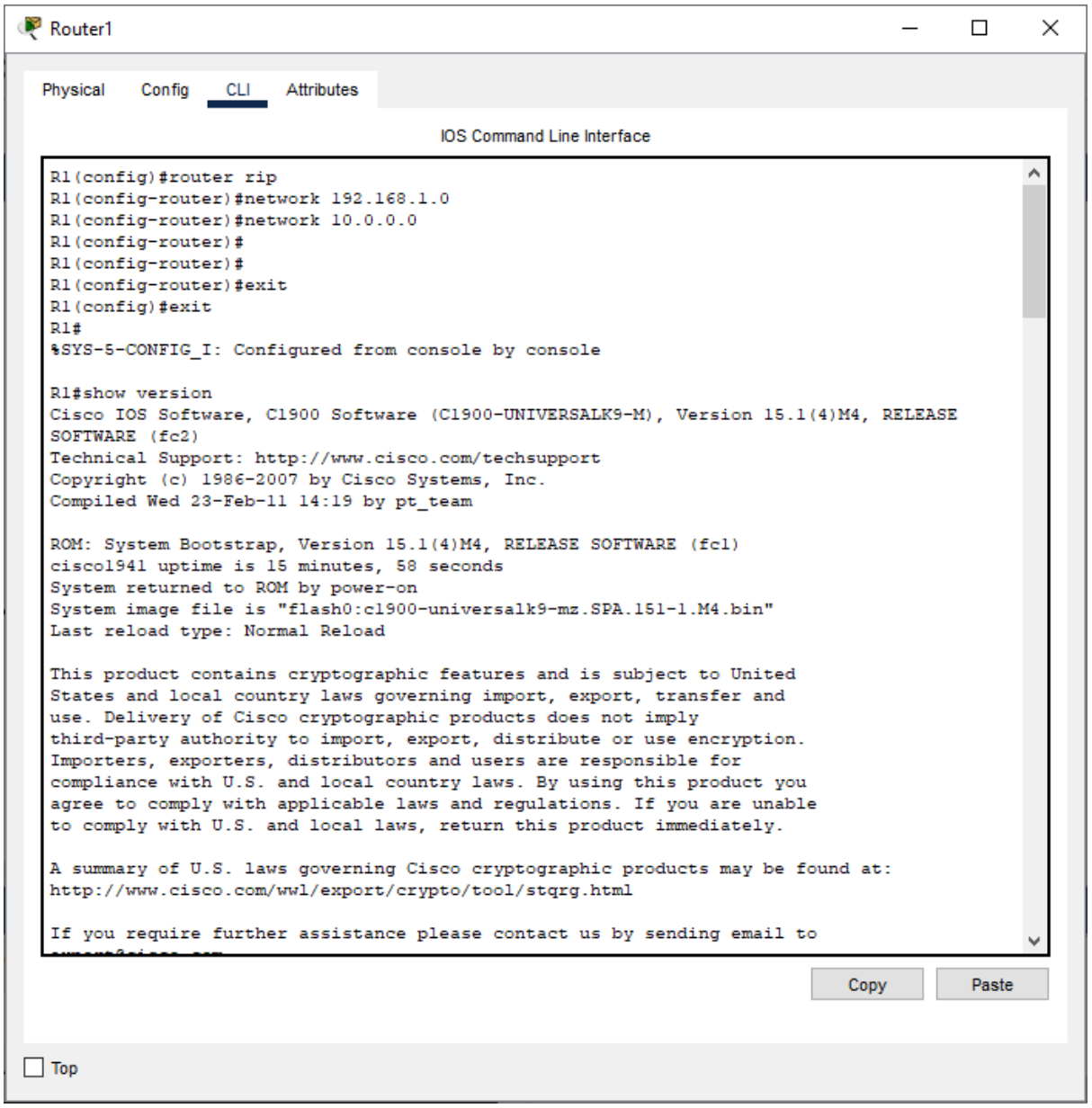
Practical-8

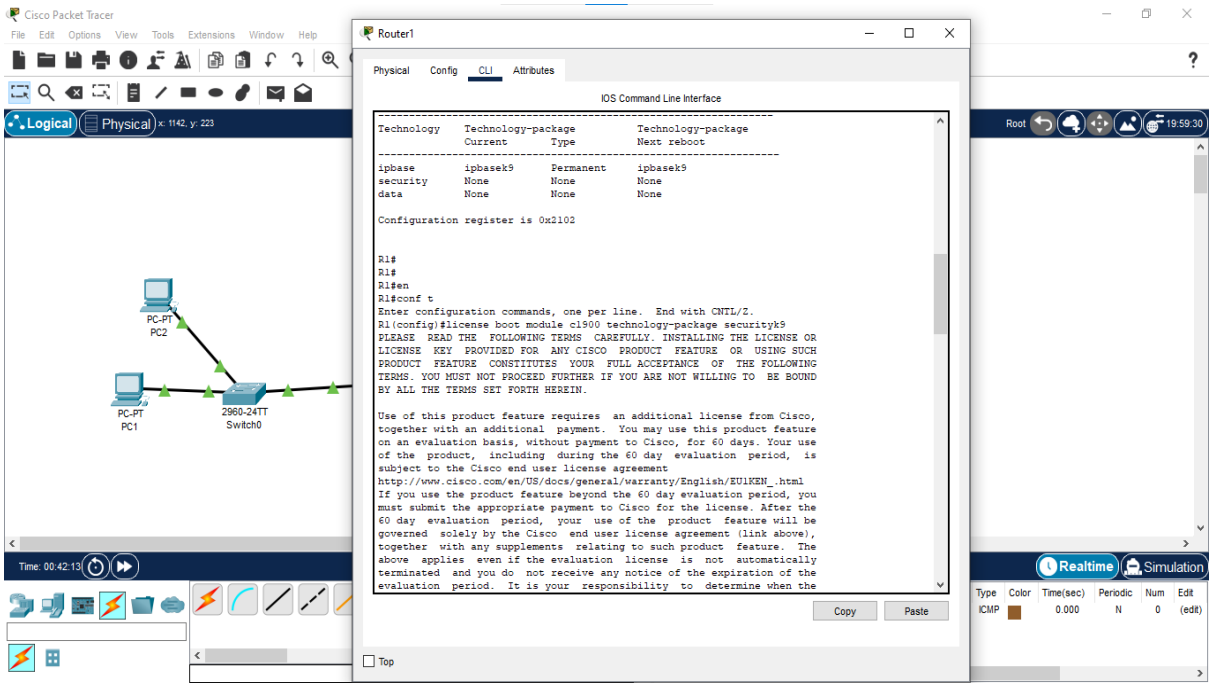
Configure and Verify a Site-to-Site IPsec VPN Using CLI

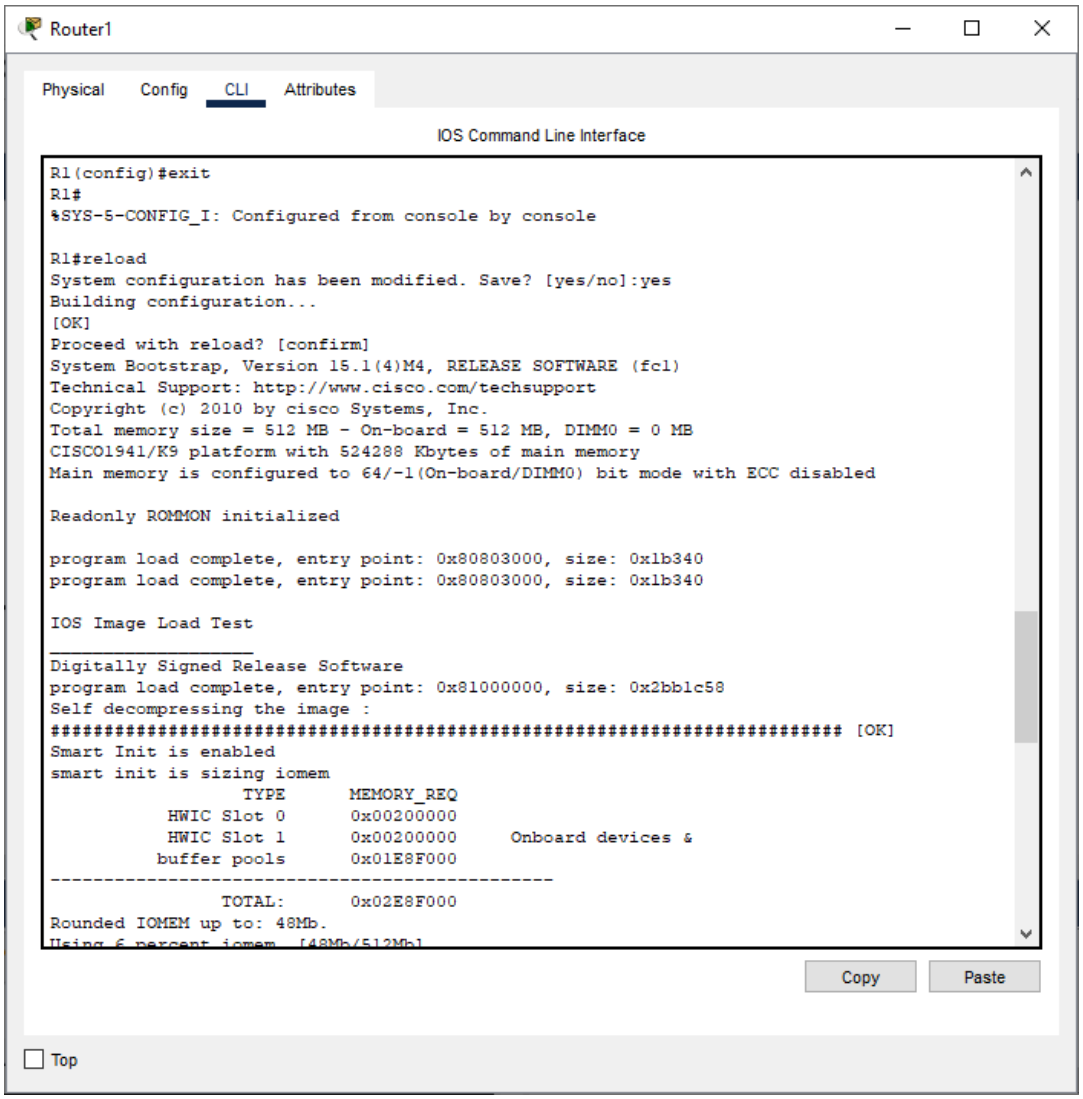
Topology



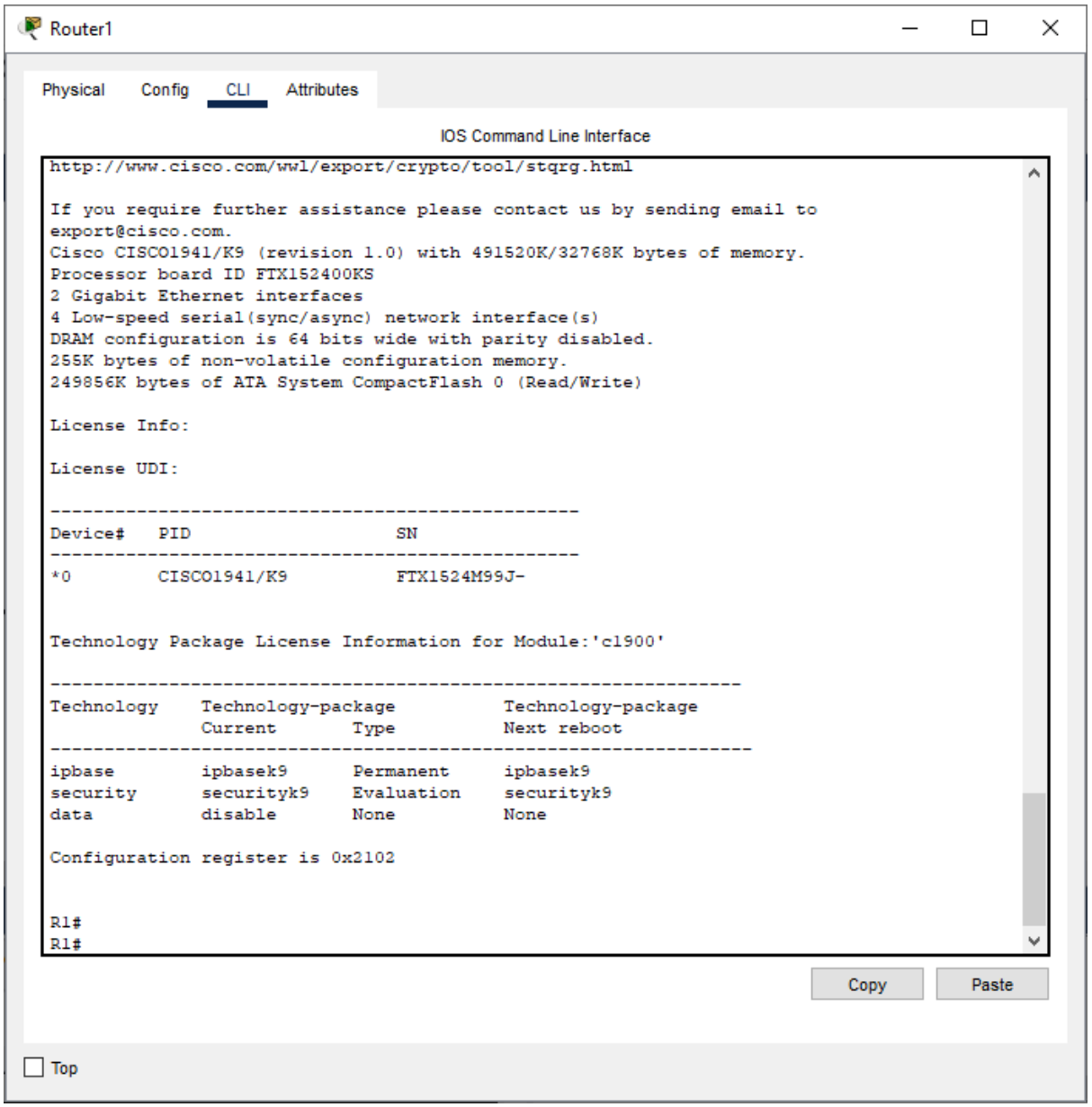



Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.0.0.0
R1(config-router)#
R1(config-router)#
R1(config-router)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team
ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 15 minutes, 58 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
Copy
Paste
Top

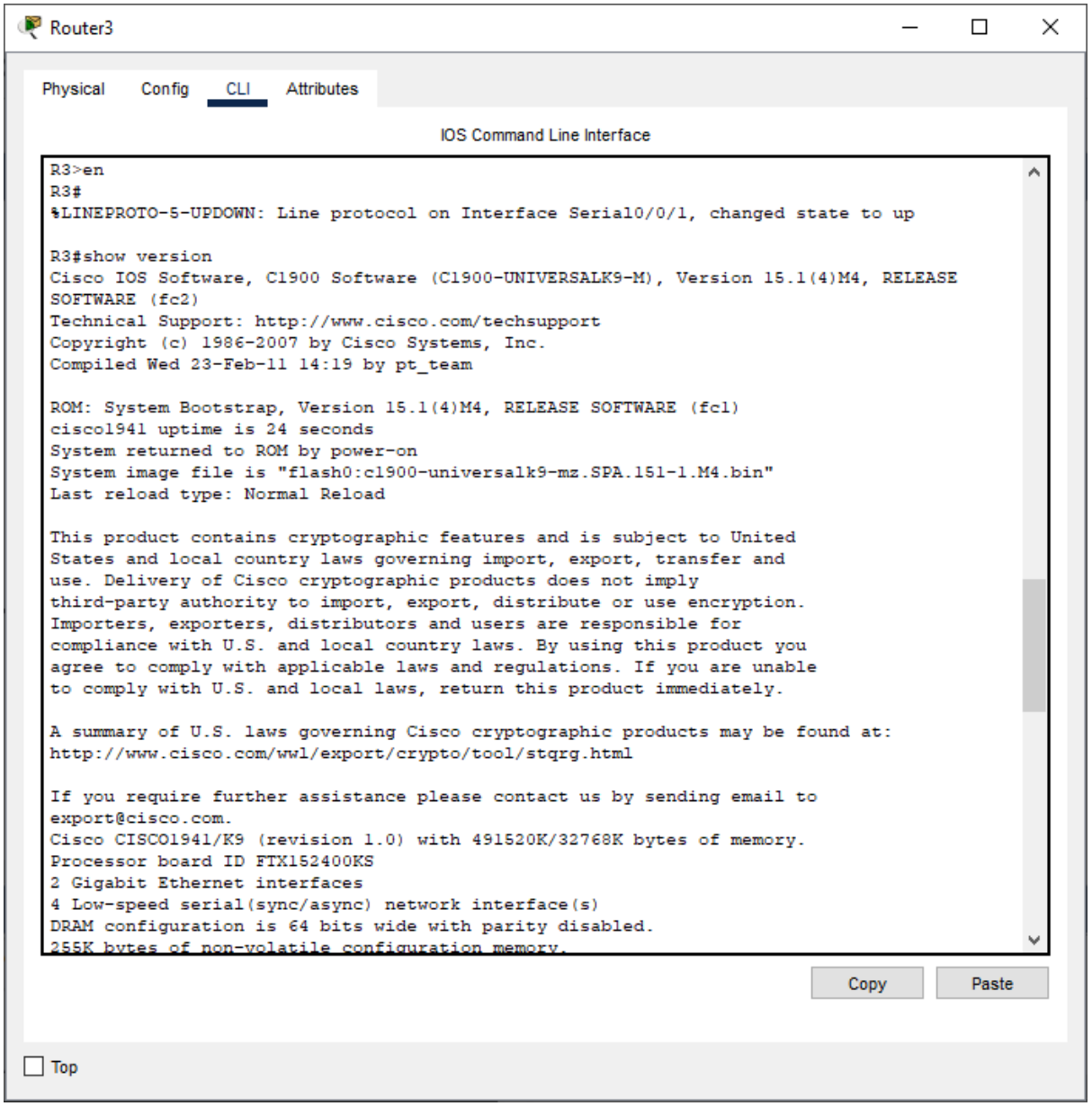

Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Technology Technology-package Technology-package
Current Type Next reboot
ipbase ipbasek9 Permanent ipbasek9
security None None None
data None None None
Configuration register is 0x2102
R1#
R1#
R1#en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.
Use of this product feature requires an additional license from Cisco,
together with an additional payment. You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the product, including during the 60 day evaluation period, is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day evaluation period, your use of the product feature will be
governed solely by the Cisco end user license agreement (link above),
together with any supplements relating to such product feature. The
above applies even if the evaluation license is not automatically
terminated and you do not receive any notice of the expiration of the
evaluation period. It is your responsibility to determine when the
Copy Paste
Top
PC-PT PC2
PC-PT PC1
2960-24TT Switch0
Realtime Simulation

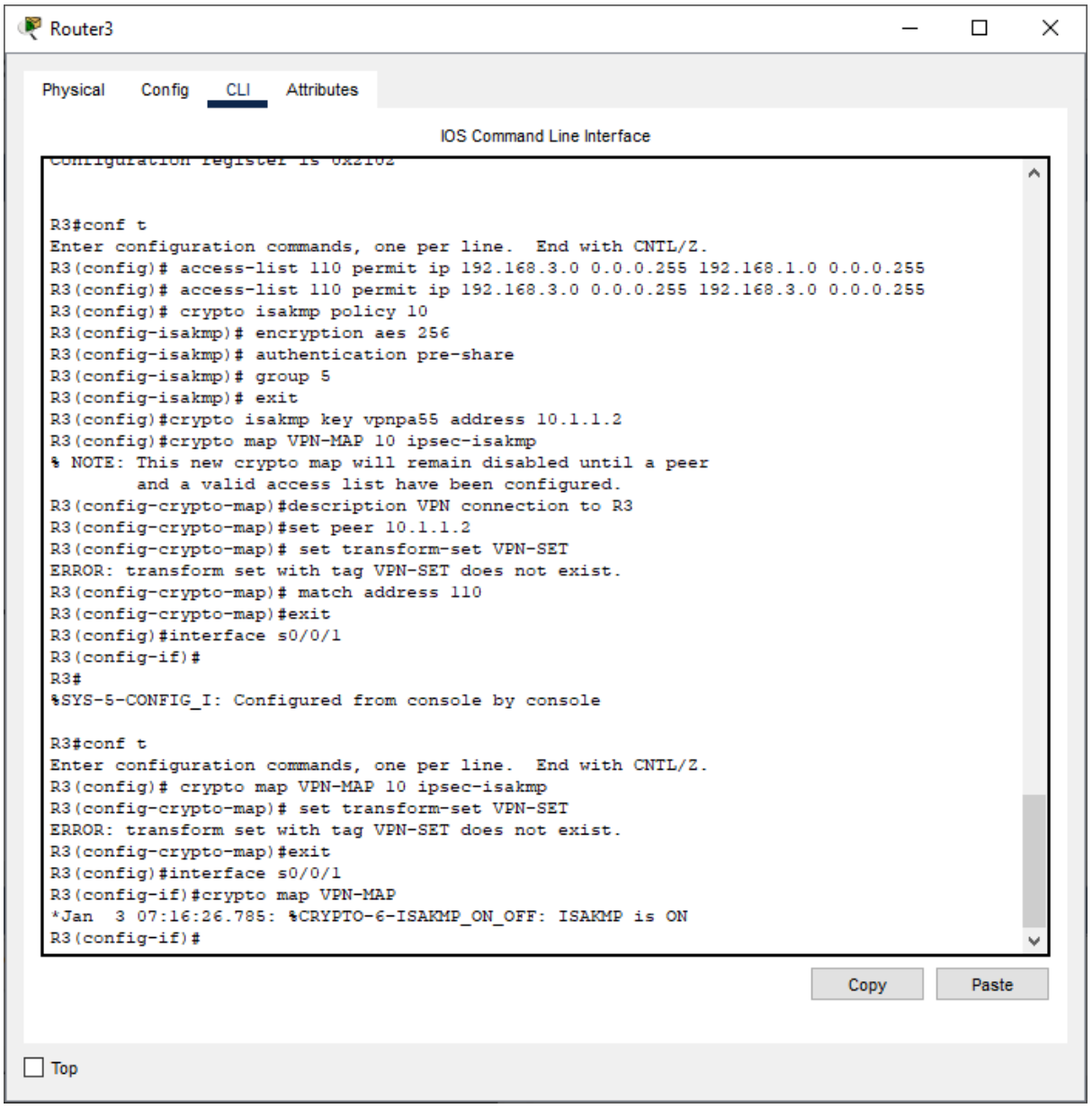

Router1
Physical Config CLI Attributes
IOS Command Line Interface
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized
program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340
IOS Image Load Test
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
[OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 0 0x00200000
HWIC Slot 1 0x00200000 Onboard devices &
buffer pools 0x01E8F000
TOTAL: 0x02E8F000
Rounded IOMEM up to: 48Mb.
Copy Paste
Top

R1

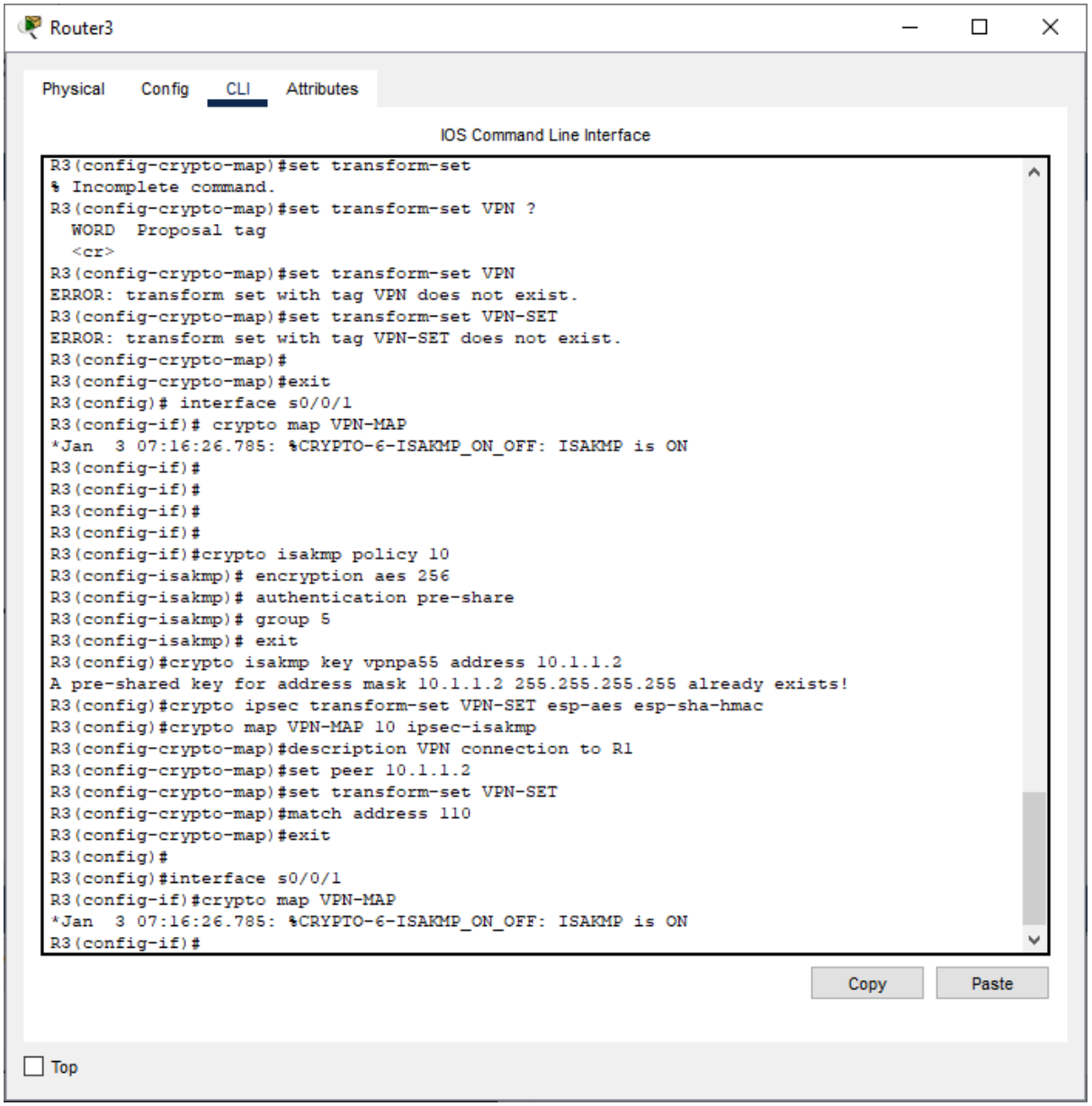

Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
4 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
Device# PID SN
*0 CISCO1941/K9 FTX1524M99J-
Technology Package License Information for Module:'c1900'
Technology Technology-package Current Type Technology-package Next reboot
ipbase ipbasek9 Permanent ipbasek9
security securityk9 Evaluation securityk9
data disable None None
Configuration register is 0x2102
R1#
R1#
Copy
Paste
Top

R3

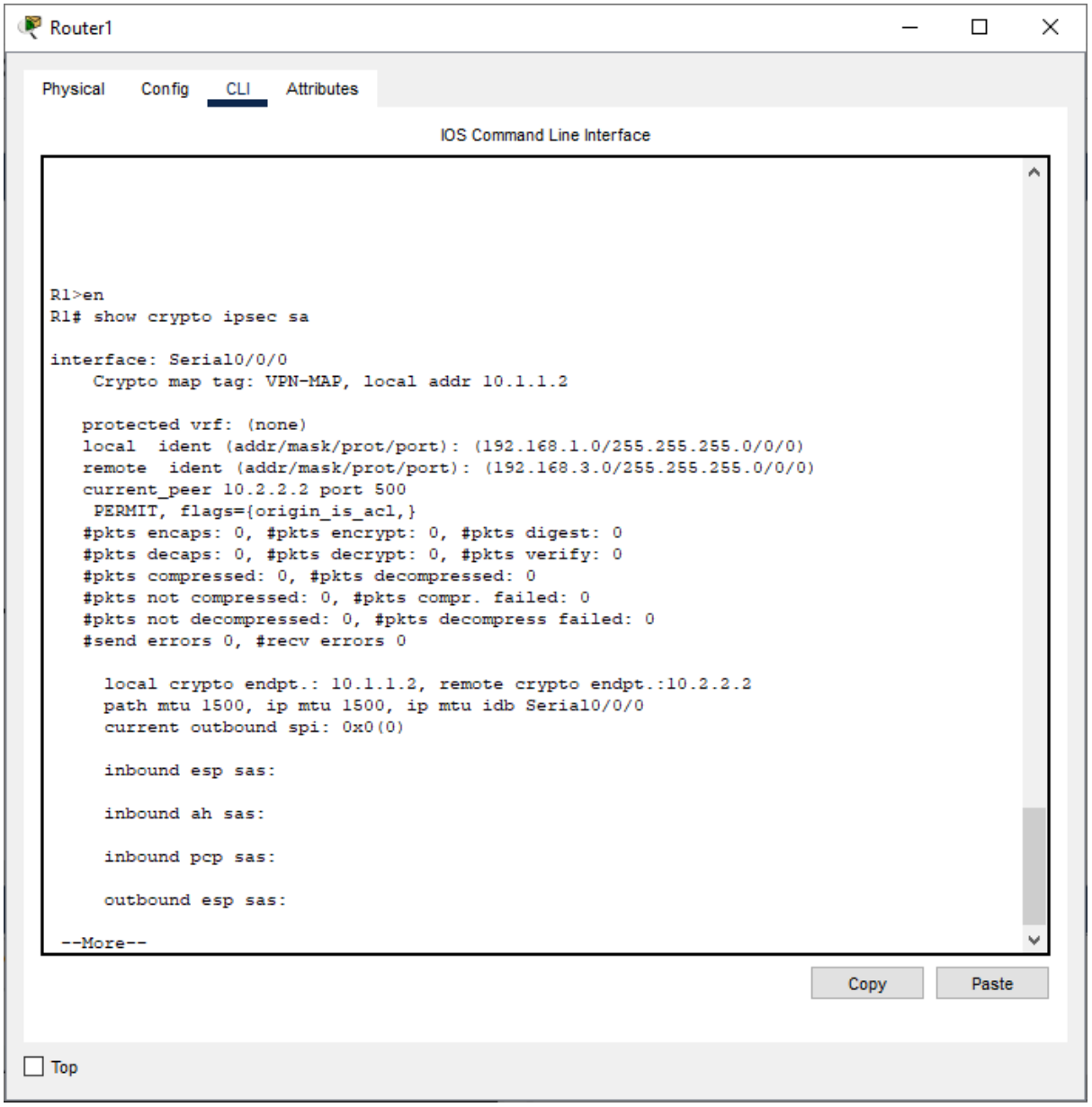

Router3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3>en
R3#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
R3#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team
ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 24 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
4 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
Copy
Paste
Top


Router3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Configuration register is 0x2102
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2
R3(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.
R3(config-crypto-map)#description VPN connection to R3
R3(config-crypto-map)#set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
ERROR: transform set with tag VPN-SET does not exist.
R3(config-crypto-map)# match address 110
R3(config-crypto-map)#exit
R3(config)#interface s0/0/1
R3(config-if)#
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# set transform-set VPN-SET
ERROR: transform set with tag VPN-SET does not exist.
R3(config-crypto-map)#exit
R3(config)#interface s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#
Copy
Paste
Top

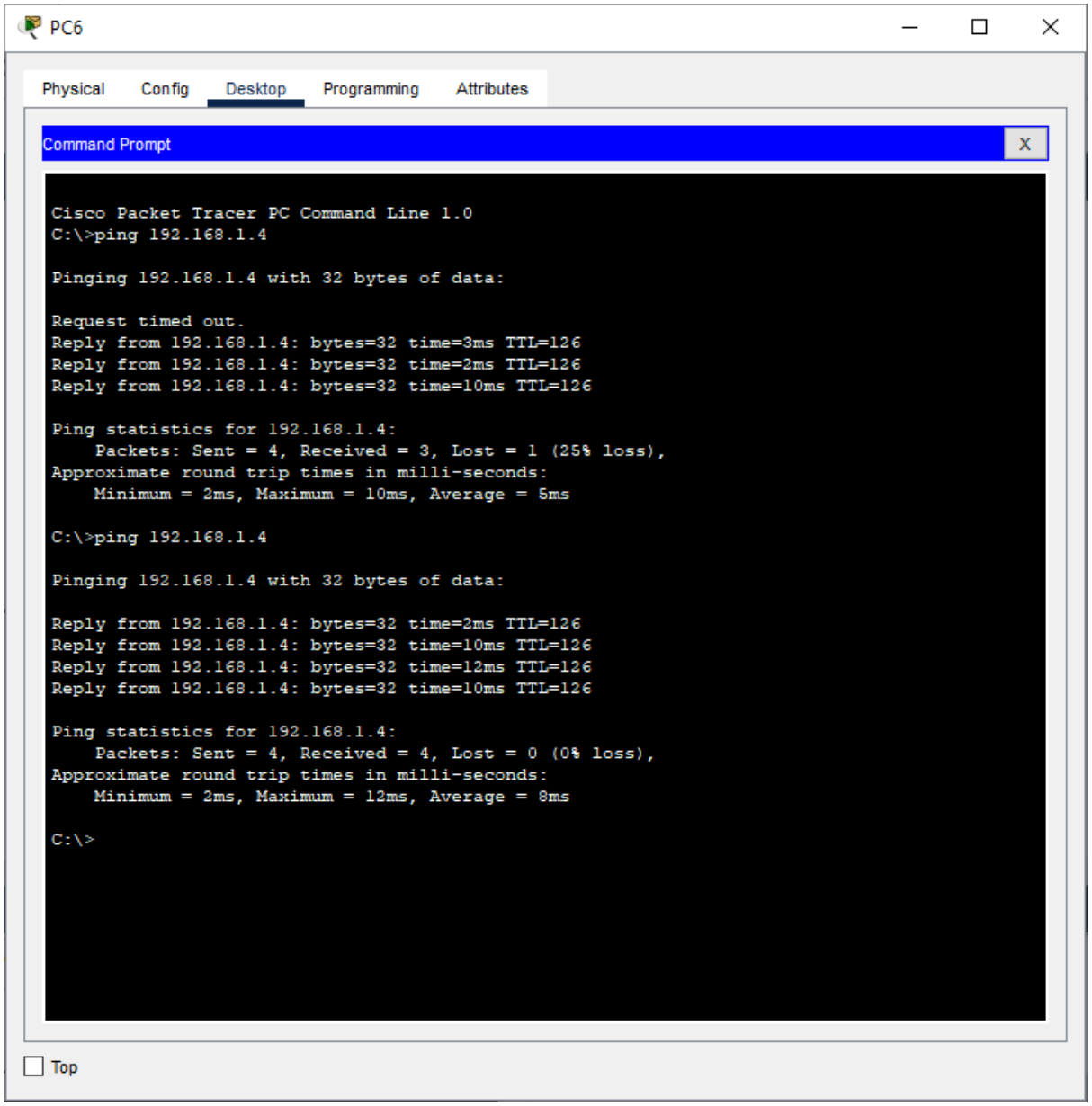
Changes(updated)



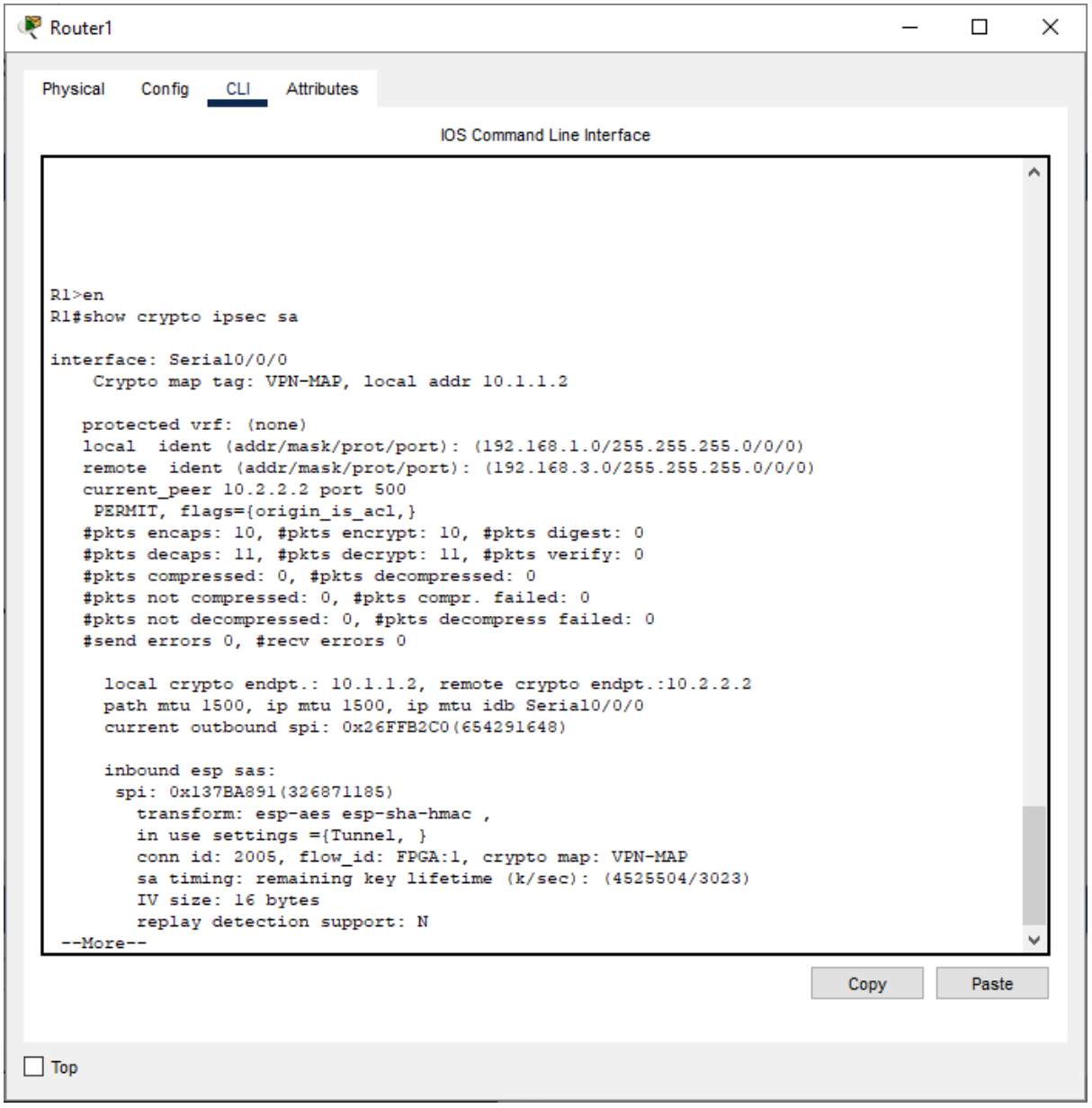
Check on R1

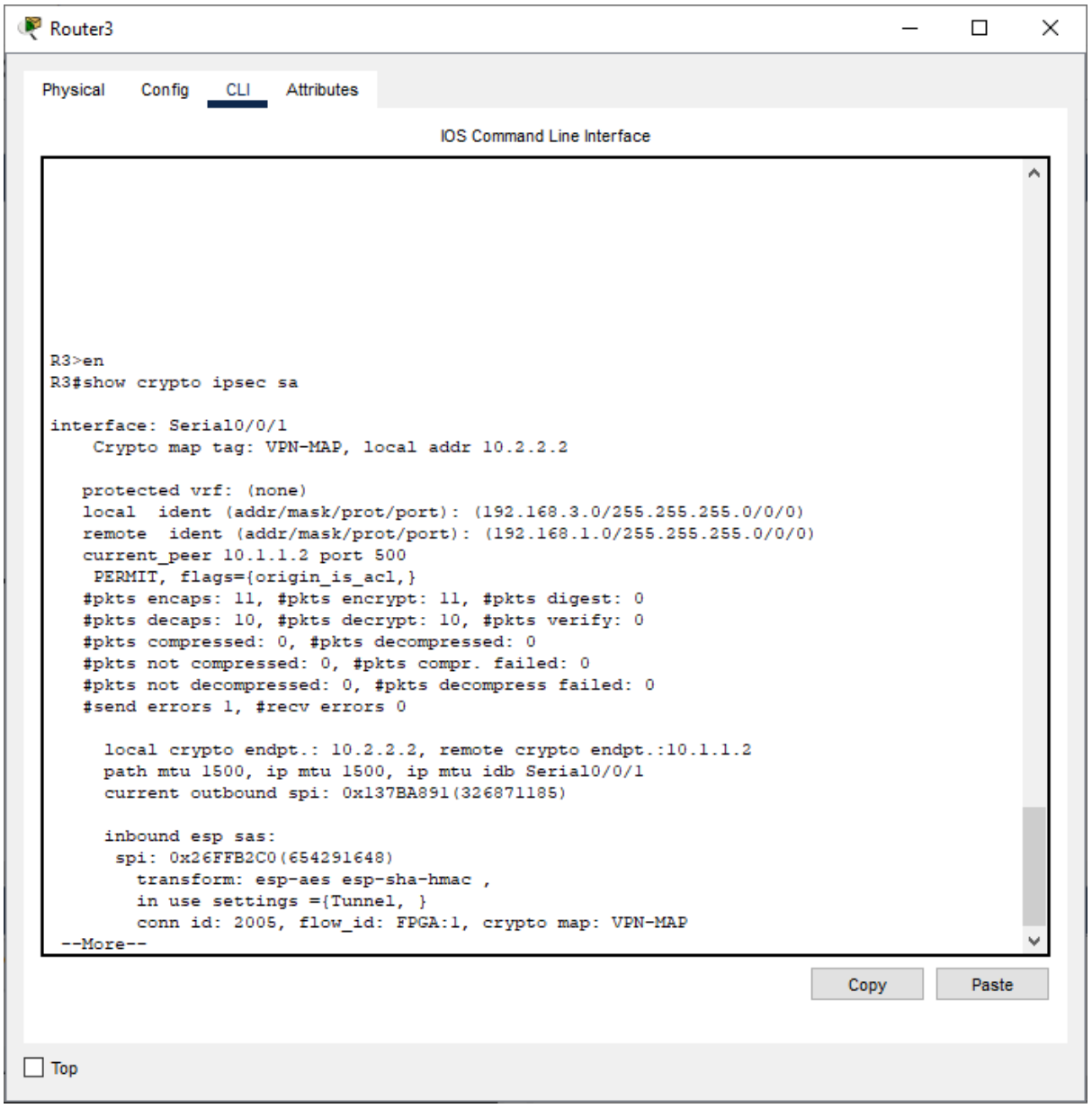

Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1>en
R1# show crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 10.2.2.2 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
local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x0(0)
inbound esp sas:
inbound ah sas:
inbound pcp sas:
outbound esp sas:
--More--
Copy
Paste
Top

Pinging from R3 side to r1

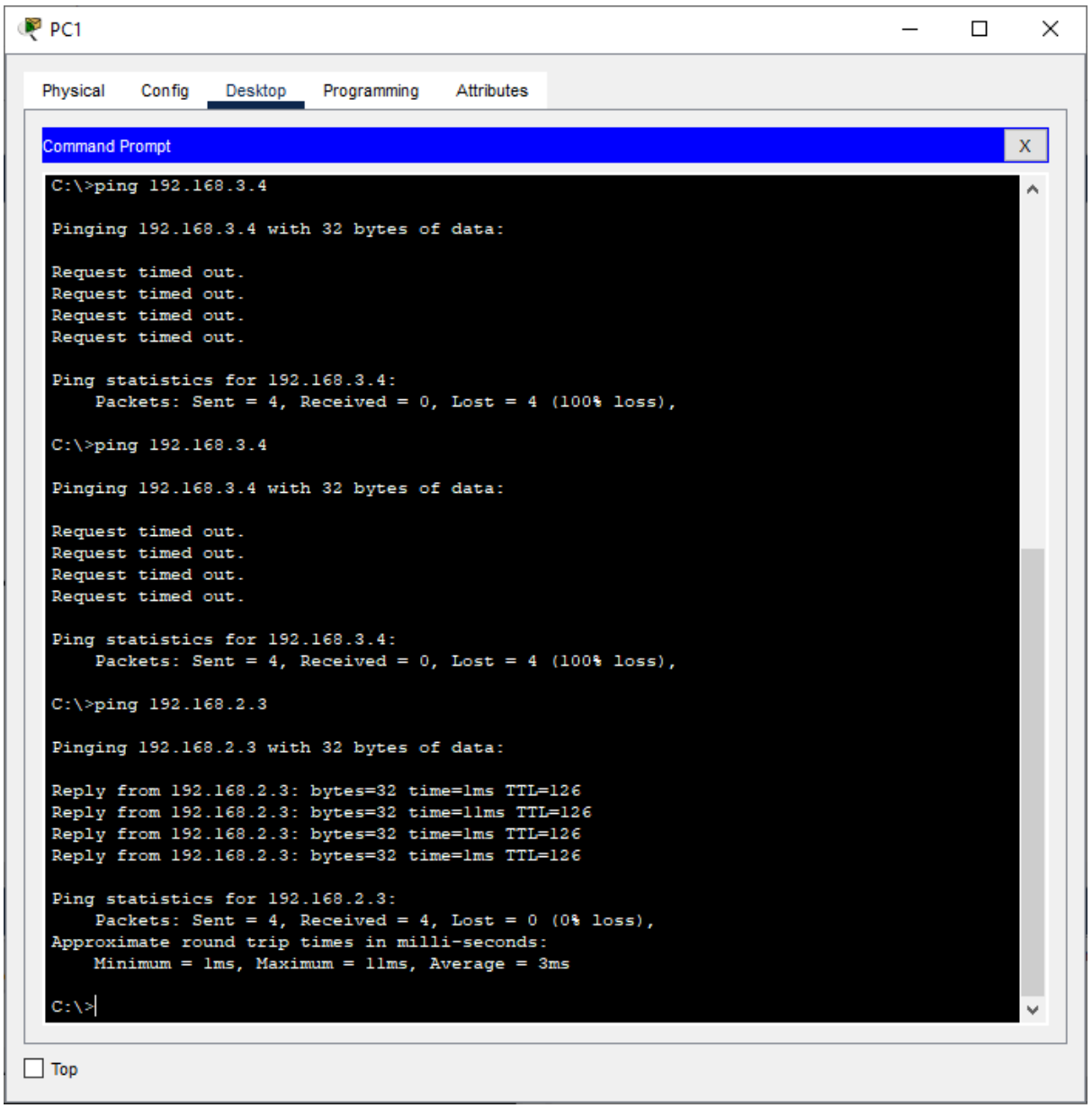


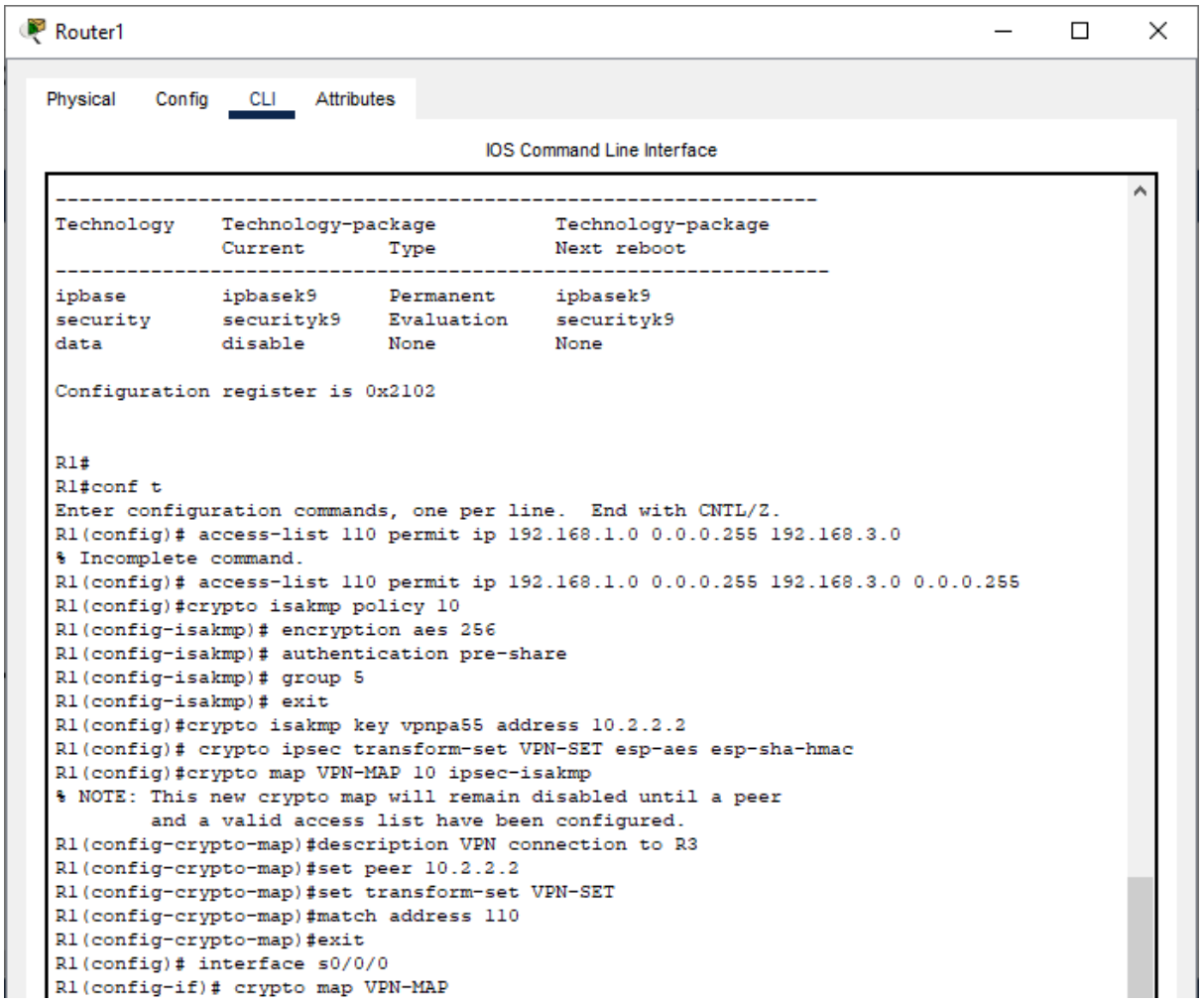
Output:


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1>en
R1#show crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: VPN-MAP, local addr 10.1.1.2
protected vrf: (none)
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 10.2.2.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 0
#pkts decaps: 11, #pkts decrypt: 11, #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
local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x26FFB2C0(654291648)
inbound esp sas:
spi: 0x137BA891(326871185)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3023)
IV size: 16 bytes
replay detection support: N
--More--
Copy
Paste
Top


Router3
Physical
Config
CLI
Attributes
IOS Command Line Interface
R3>en
R3#show crypto ipsec sa
interface: Serial0/0/1
Crypto map tag: VPN-MAP, local addr 10.2.2.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 10.1.1.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
#pkts decaps: 10, #pkts decrypt: 10, #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
local crypto endpt.: 10.2.2.2, remote crypto endpt.:10.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
current outbound spi: 0x137BA891(326871185)
inbound esp sas:
spi: 0x26FFB2C0(654291648)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: VPN-MAP
--More--
Copy
Paste
Top

Pinging uninterested traffic




Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface

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
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
% Incomplete command.
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2
R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(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.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP