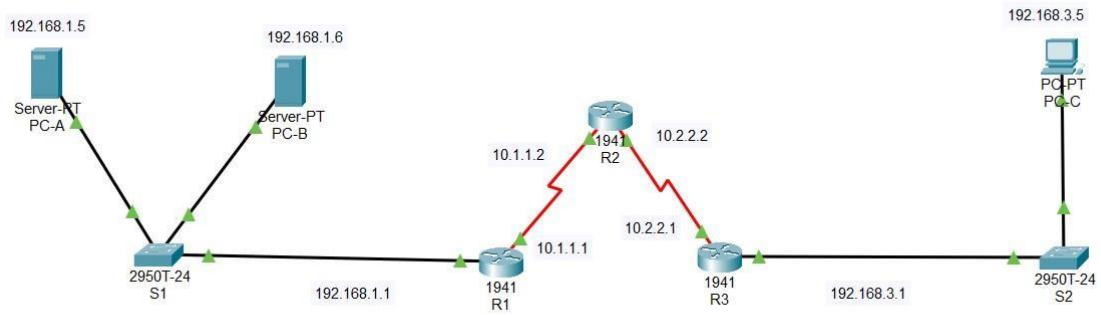
Practical – 1 Configure Cisco Routers for Syslog, NTP, and SSH Operations



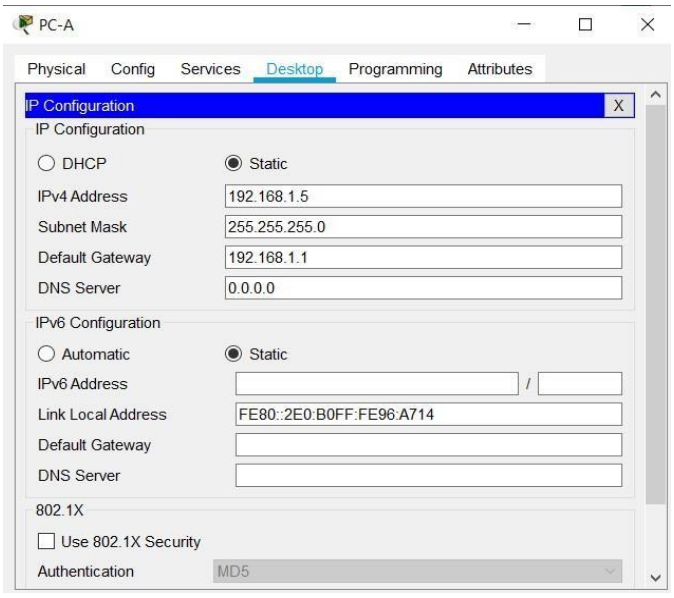
Address Table :-

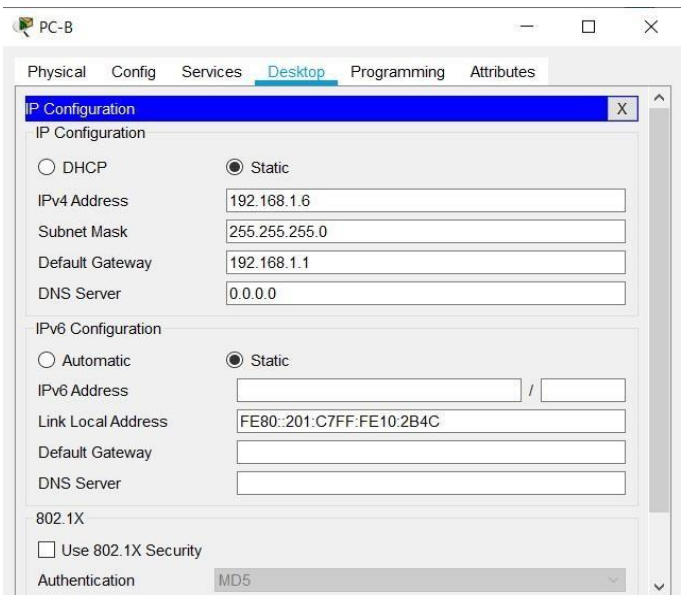
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G 0/0	192.168.1.1	255.255.255.0	N/A
	S 0/1/0	10.1.1.1	255.255.255.252	N/A
R2	S 0/1/0	10.1.1.2	255.255.255.252	N/A
	S 0/1/1	10.2.2.2	255.255.255.252	N/A
R3	G 0/0	192.168.3.1	255.255.255.0	N/A
	S 0/1/0	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.5	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

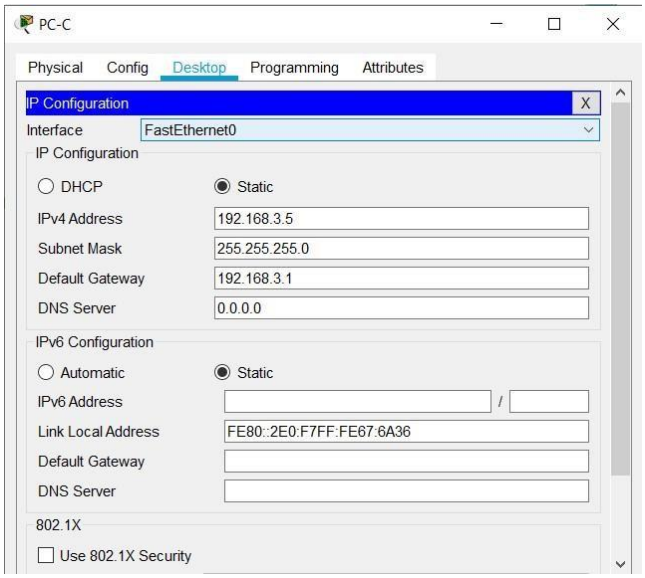
Part-1 :- Configure OSPF MD5 Authentication

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

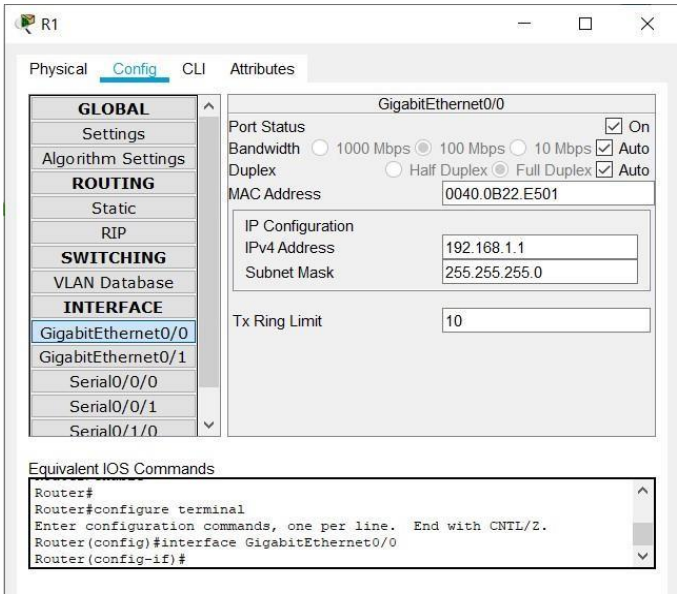
PC and Server Configuration :-

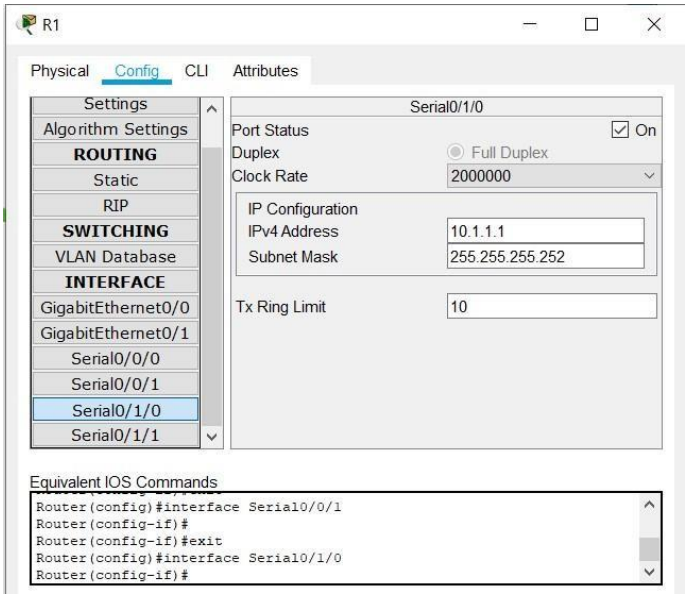


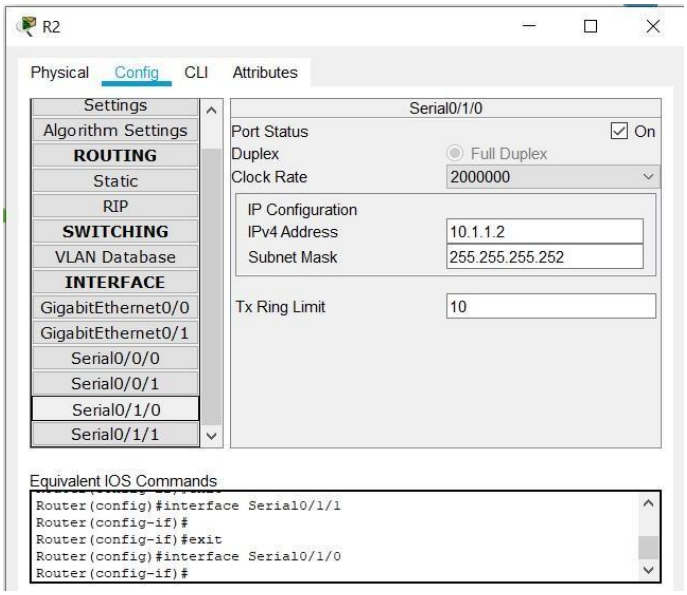


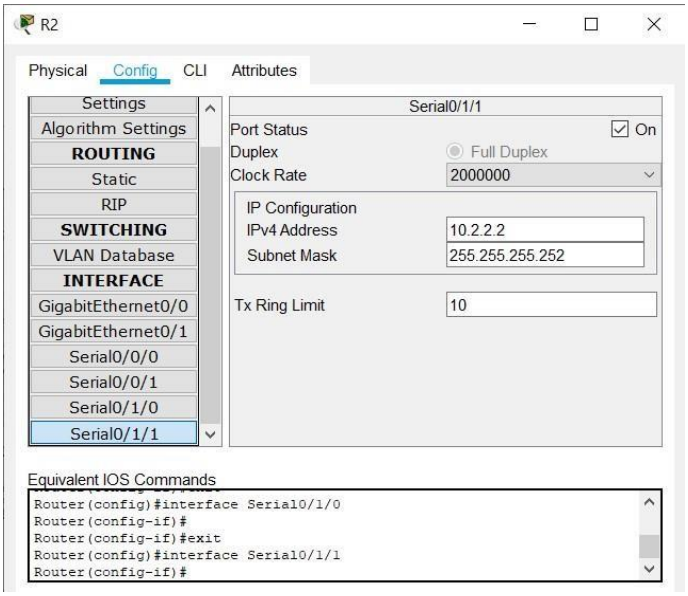


Router Configuration :-

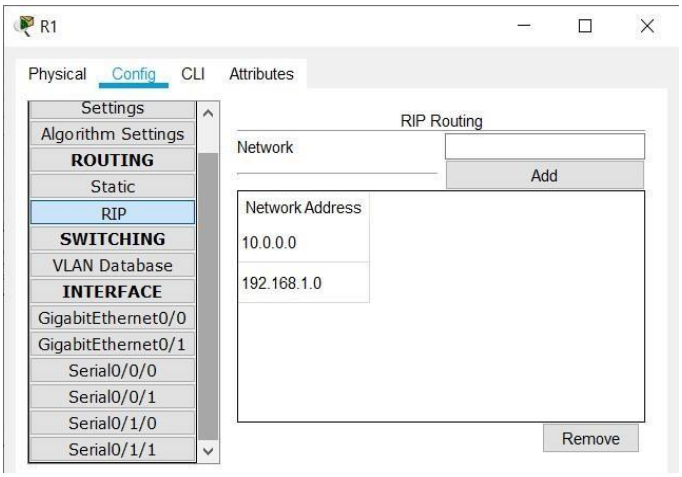


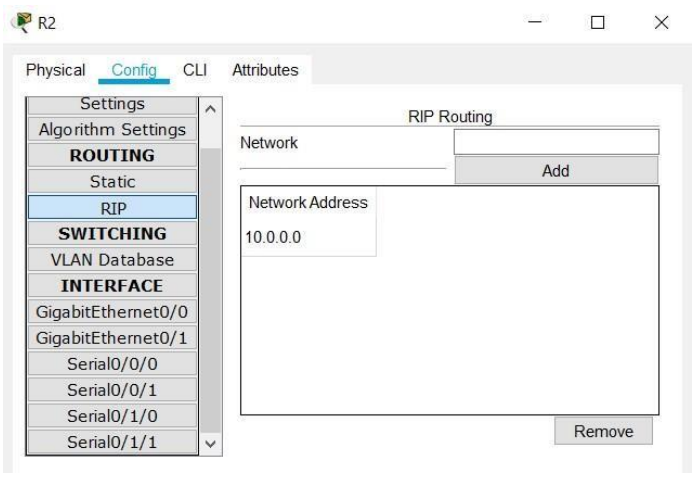


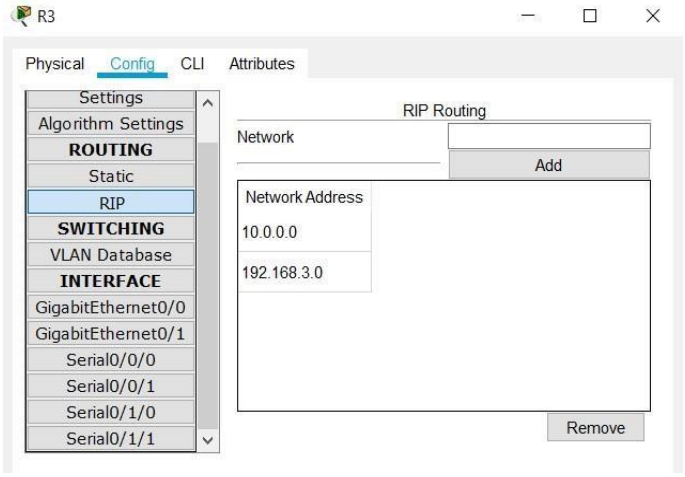




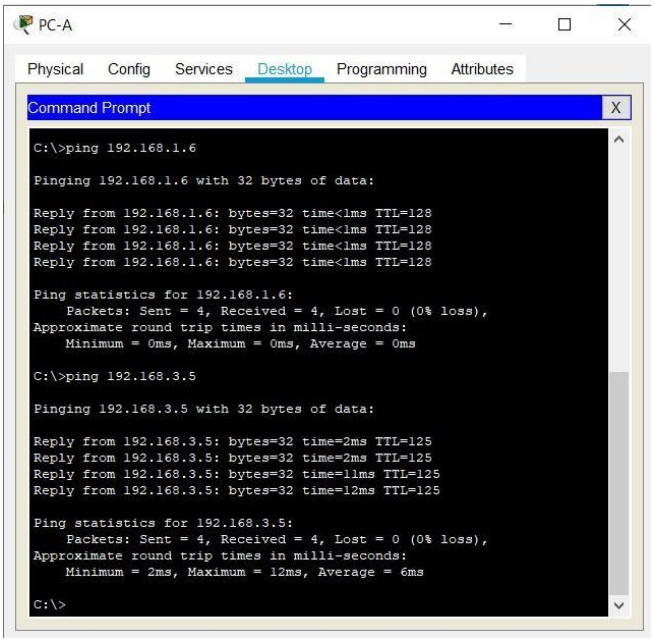
RIP Routing :-

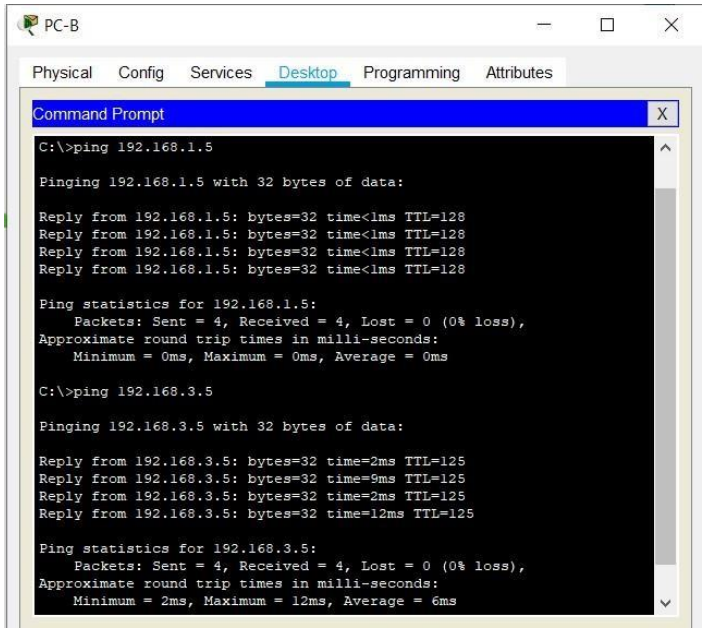


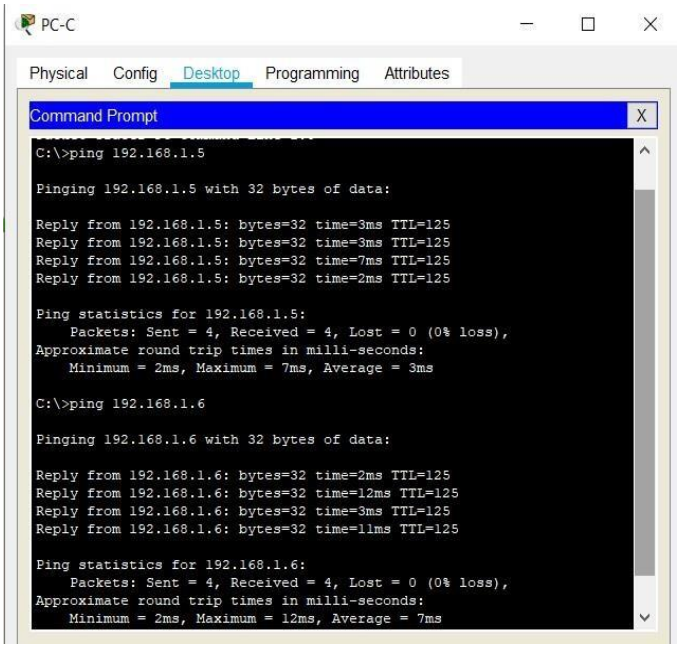




Checking ping between PC and Servers :-







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

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
R1(config-router)#exit

R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
R2(config-router)#exit
R2(config)#

R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
R3(config-router)#ex
R3(config)#
```

Step-3 :- Configure the MD5 key for all routers in area 0.

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

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

R3(config)#interface s0/1/0
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R3(config-if)#exut
             ^
% Invalid input detected at '^' marker.

R3(config-if)#ex
```

Step-4 :- Verify configurations.

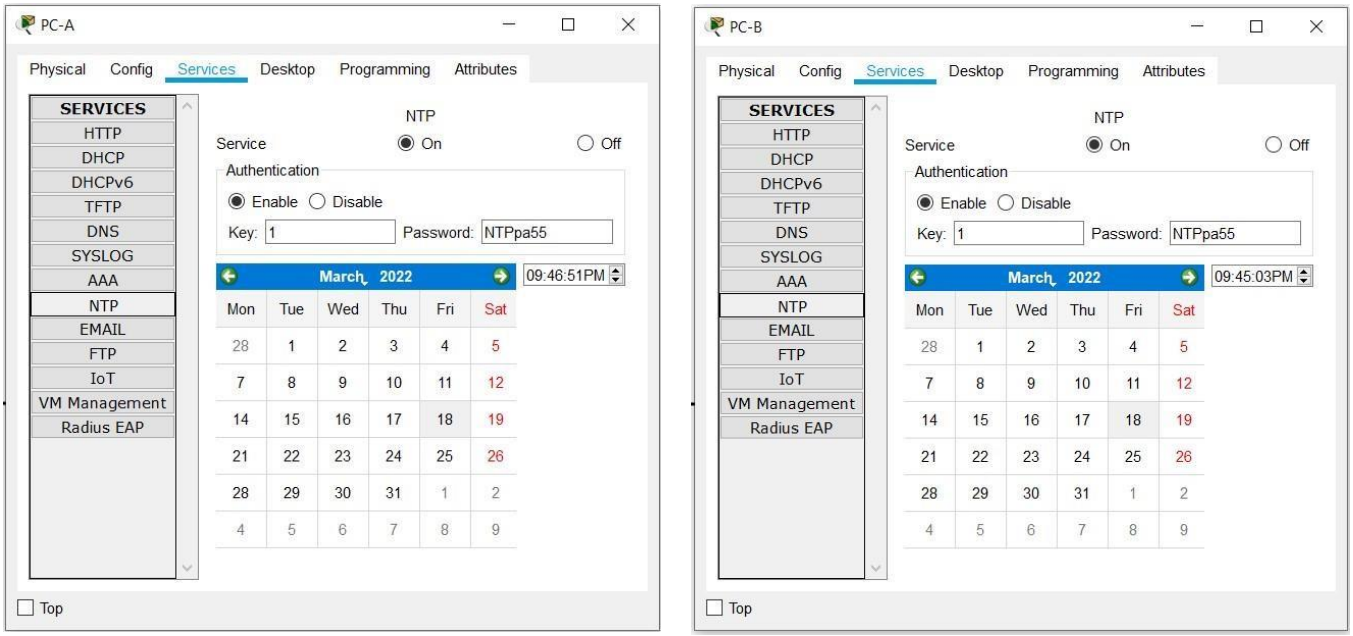
```
R1#show ip ospf 1
 Routing Process "ospf 1" with ID 192.168.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
```

```
R2>en
R2#show ip ospf 1
 Routing Process "ospf 1" with ID 10.2.2.2
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
```

```
R3#show ip ospf 1
 Routing Process "ospf 1" with ID 192.168.3.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
```

Part-2 :- Configure NTP

Step-1 :- Enable NTP authentication on Both Server.



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

```
R1(config)#ntp server 192.168.1.5
R1(config)#
```

```
R2(config)#ntp server 192.168.1.5
R2(config)#
```

```
R3(config)#ntp server 192.168.1.5
R3(config)#
```

Step-3 :- Configure routers to update hardware clock.

```
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
```

```
R2(config)#ntp update-calendar
R2(config)#
```

```
R3(config)#ntp update-calendar
R3(config)#
```

Step-4 :- Configure NTP authentication on the routers.

```
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp authenticate-key 1 md5 NTPpa55
                                  ^
% Invalid input detected at '^' marker.

R1(config)#ntp authentication-key 1 md5 NTPpa55
R1(config)#

R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authentication-key 1 md5 NTPpa55
R2(config)#

R3(config)#ntp authenticate
R3(config)#ntp trusted-key 1
R3(config)#ntp authentication-key 1 md5 NTPpa55
R3(config)#
```

Step-5 :- Configure routers to timestamp log messages.

```
R1(config)#service timestamps log datetime msec
R1(config)#

R2(config)#service timestamps log datetime msec
R2(config)#

R3(config)#service timestamps log datetime msec
R3(config)#
```

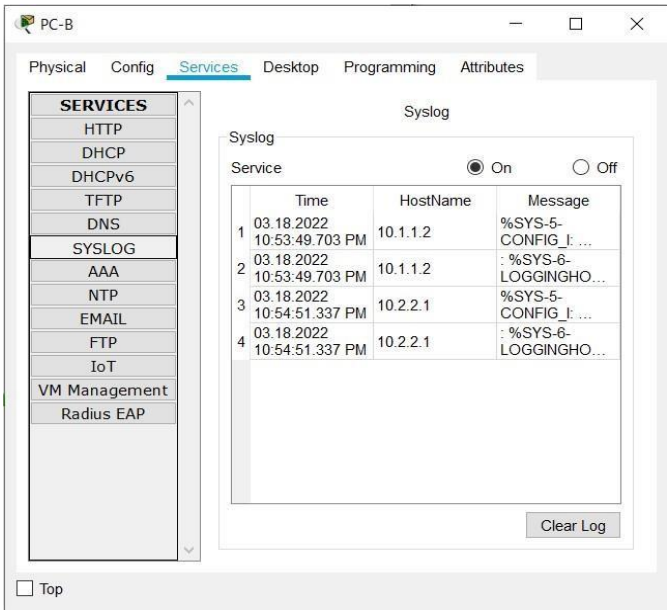
Part-3 :- Configure Routers to Log Messages to Syslog Server

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

```
R1(config)#logging host 192.168.1.6
R1(config)#exit
R1#
*Mar 18, 22:52:08.5252: SYS-5-CONFIG_I: Configured from console by
console
*Mar 18, 22:52:08.5252:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

R2(config)#logging host 192.168.1.6
R2(config)#exit
R2#
*Mar 18, 22:53:49.5353: SYS-5-CONFIG_I: Configured from console by
console
*Mar 18, 22:53:49.5353:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 7 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 7 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled
```

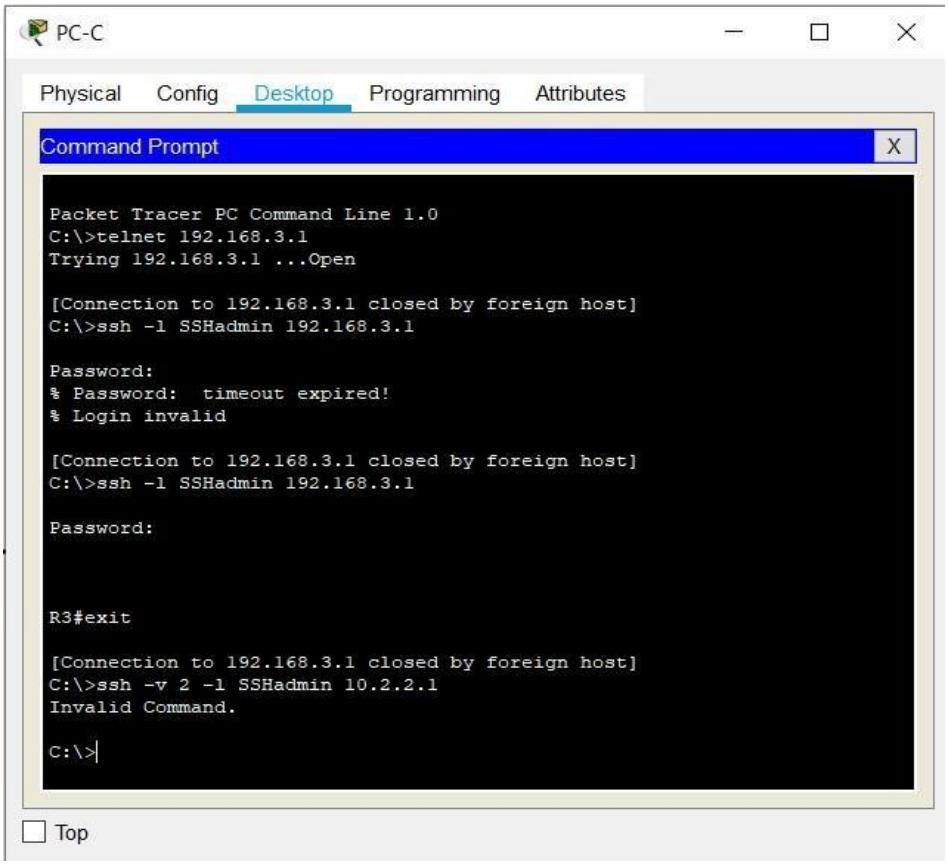
```
R3(config)#logging host 192.168.1.6
R3(config)#ex
R3#
*Mar 18, 22:54:51.5454: SYS-5-CONFIG_I: Configured from console by
console
*Mar 18, 22:54:51.5454:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
R3#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 9 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 9 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled
```

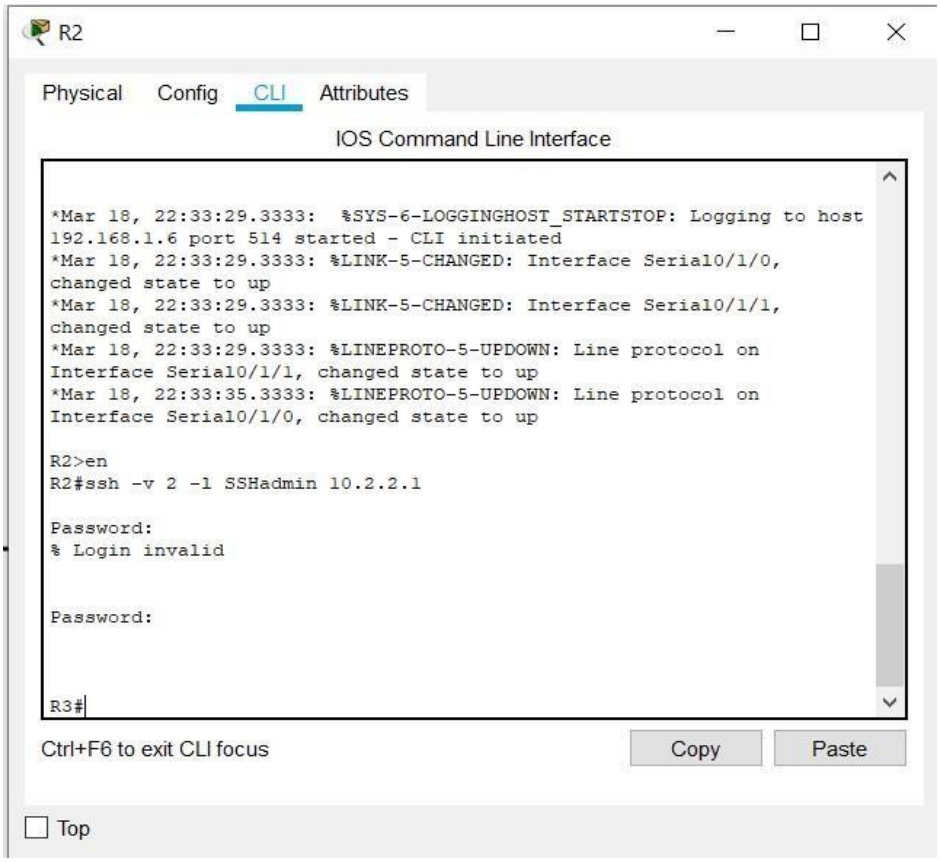
Step-2 :- Show Syslog.



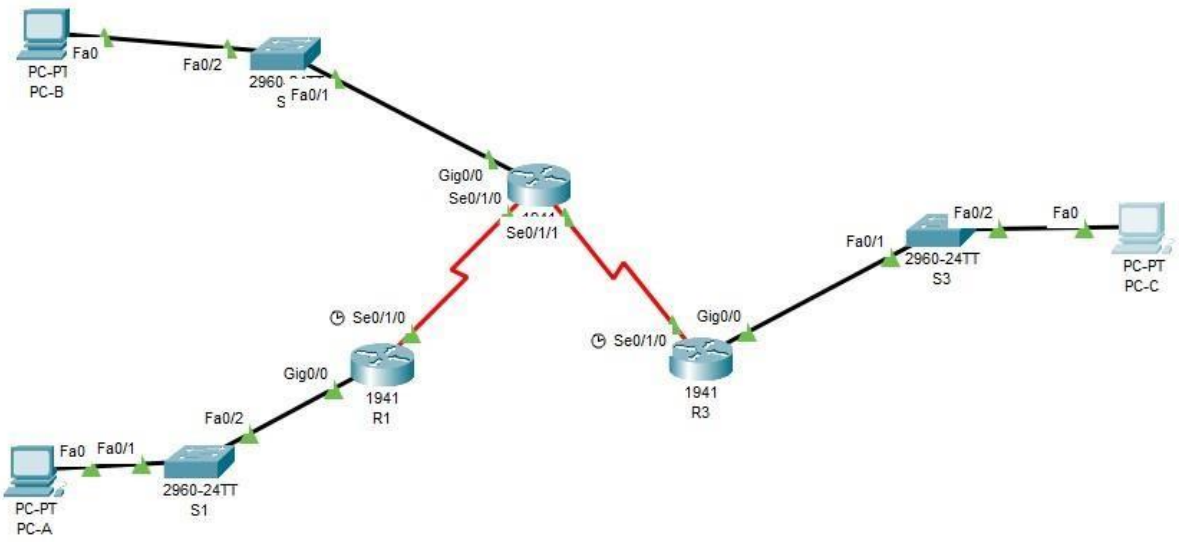
Part-4 :- Configure R3 to Support SSH Connections

```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip domain-name ccnasecurity.com
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#exit
R3(config)#username SSHadmin privilege 15 sercet ciscosshpa55
                                          ^
% Invalid input detected at '^' marker.

R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
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 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

R3(config)#ex
*Mar 18 21:53:14.40: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3#
*Mar 18, 21:53:59.5353: SYS-5-CONFIG_I: Configured from console by console
R3#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip ssh time-out 90
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh version 2
R3(config)#exit
R3#
*Mar 18, 22:00:16.000: SYS-5-CONFIG_I: Configured from console by console
R3#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
R3#
```


PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1
Password:
% Password: timeout expired!
% Login invalid
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1
Password:
R3#exit
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -v 2 -l SSHadmin 10.2.2.1
Invalid Command.
C:\>
Top


R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
*Mar 18, 22:33:29.3333: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
*Mar 18, 22:33:29.3333: %LINK-5-CHANGED: Interface Serial0/1/0,
changed state to up
*Mar 18, 22:33:29.3333: %LINK-5-CHANGED: Interface Serial0/1/1,
changed state to up
*Mar 18, 22:33:29.3333: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/1/1, changed state to up
*Mar 18, 22:33:35.3333: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/1/0, changed state to up
R2>en
R2#ssh -v 2 -l SSHadmin 10.2.2.1
Password:
% Login invalid
Password:
R3#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

Practical – 2 Packet Tracer – Configure AAA Authentication on Cisco Routers



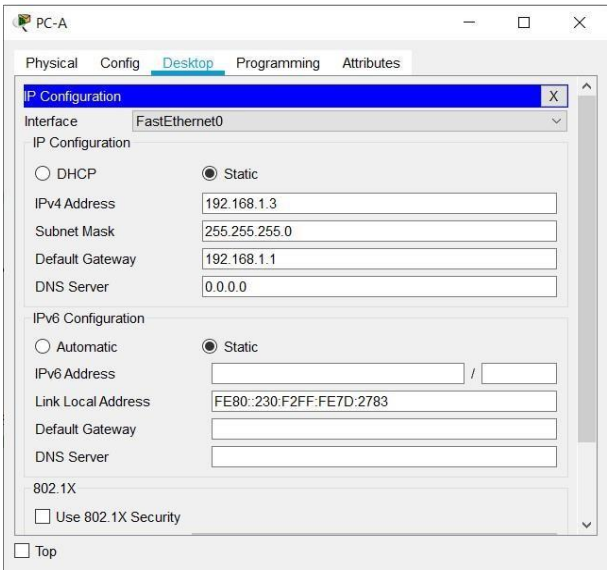
Address Table :-

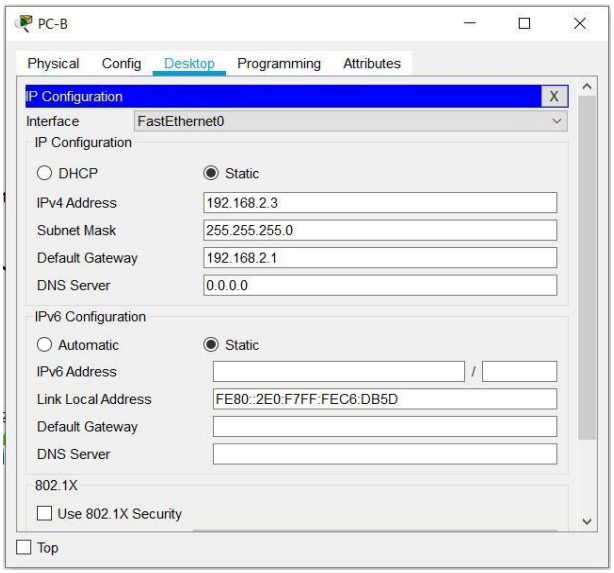
Device	Interface	IP Address	Subnet Mask
R1	G0/1	192.168.1.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
R2	G0/0	192.168.2.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
R3	G0/1	192.168.3.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC-A	NIC	192.168.1.3	255.255.255.0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

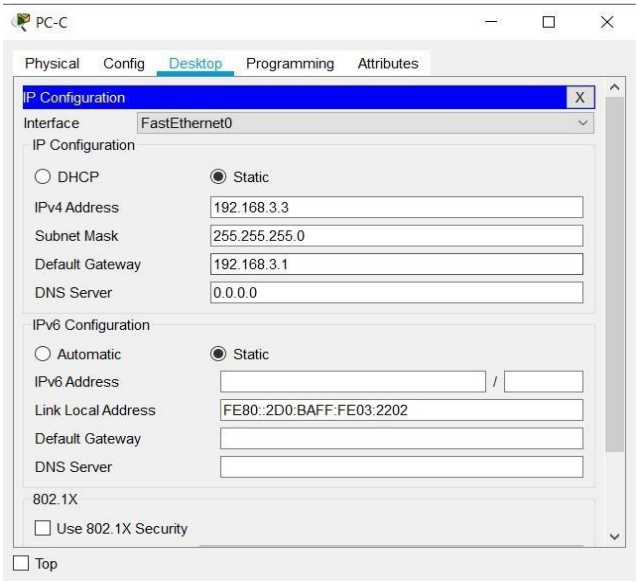
Part-1 :- Configure Local AAA Authentication for Console Access on R1.

Step-1 :- Test Connectivity.

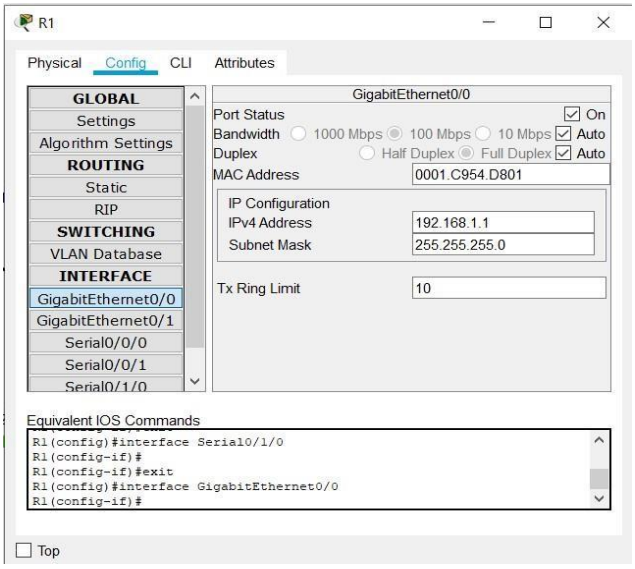
PC Configuration :-

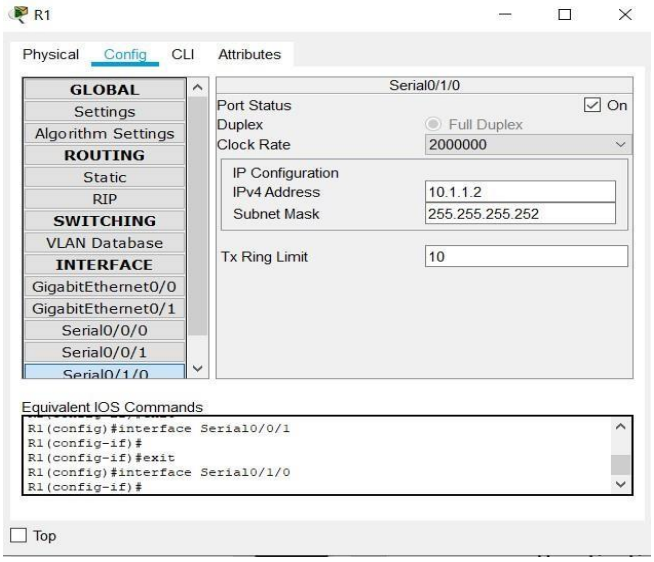


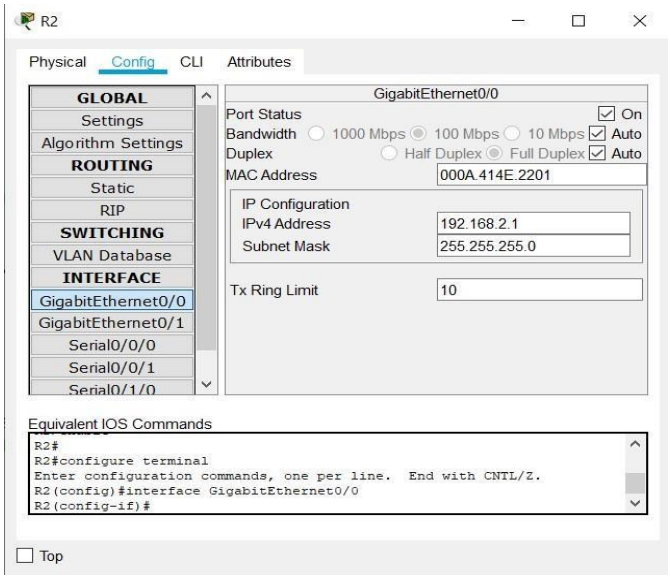


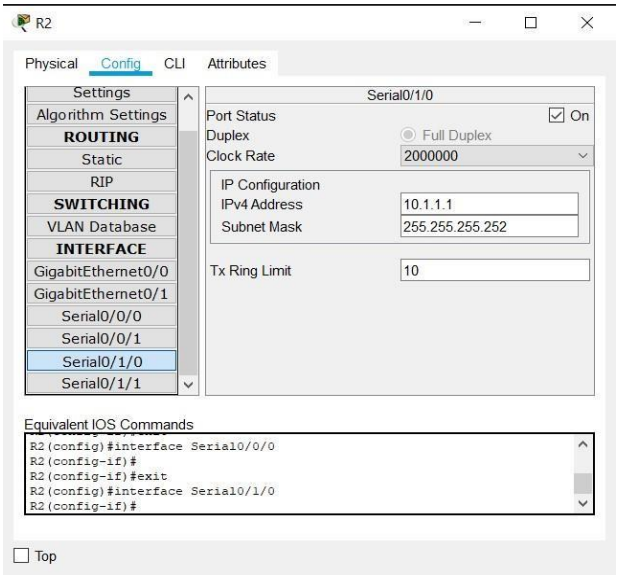


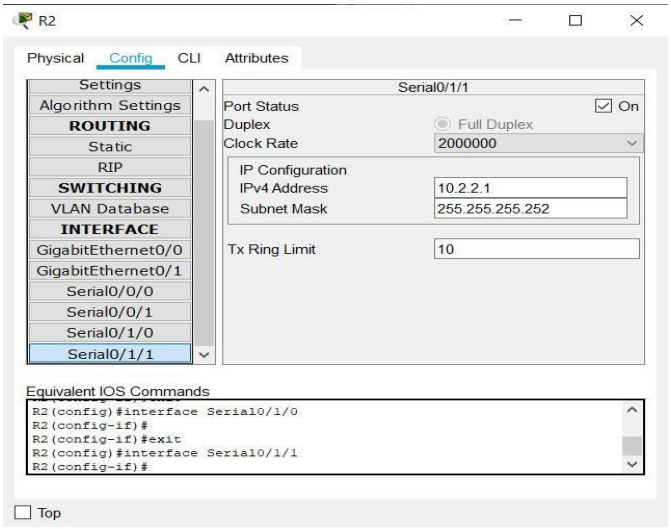
Router Configuration :-

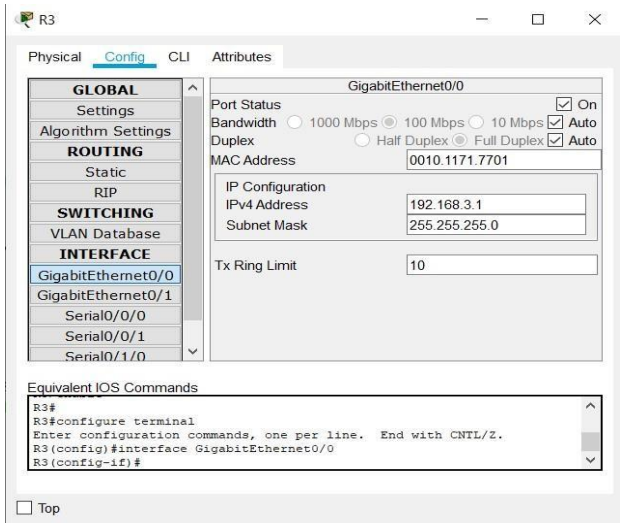


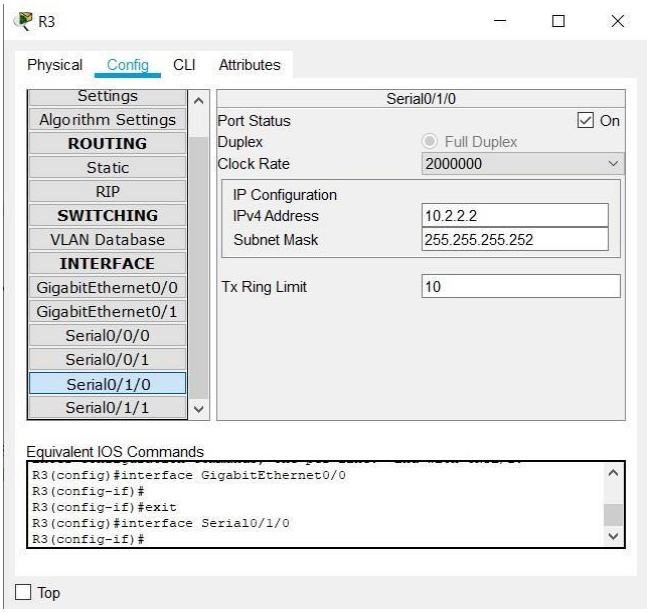


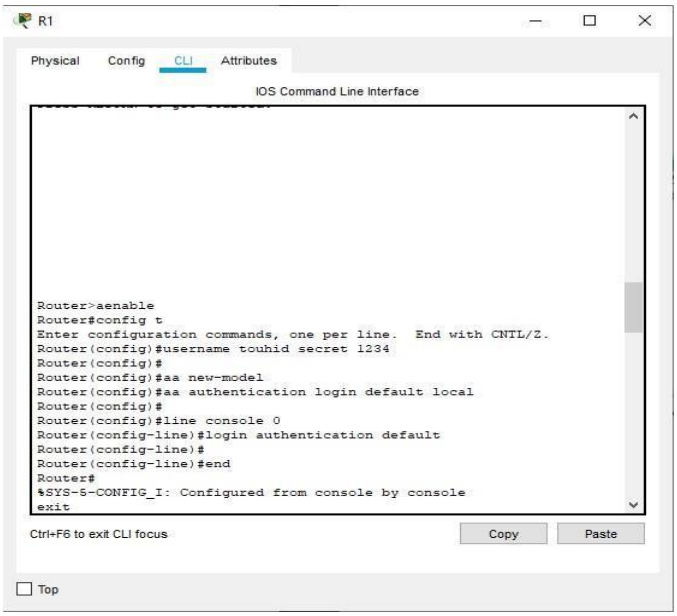




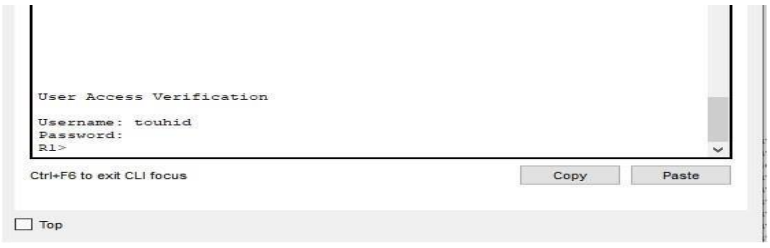




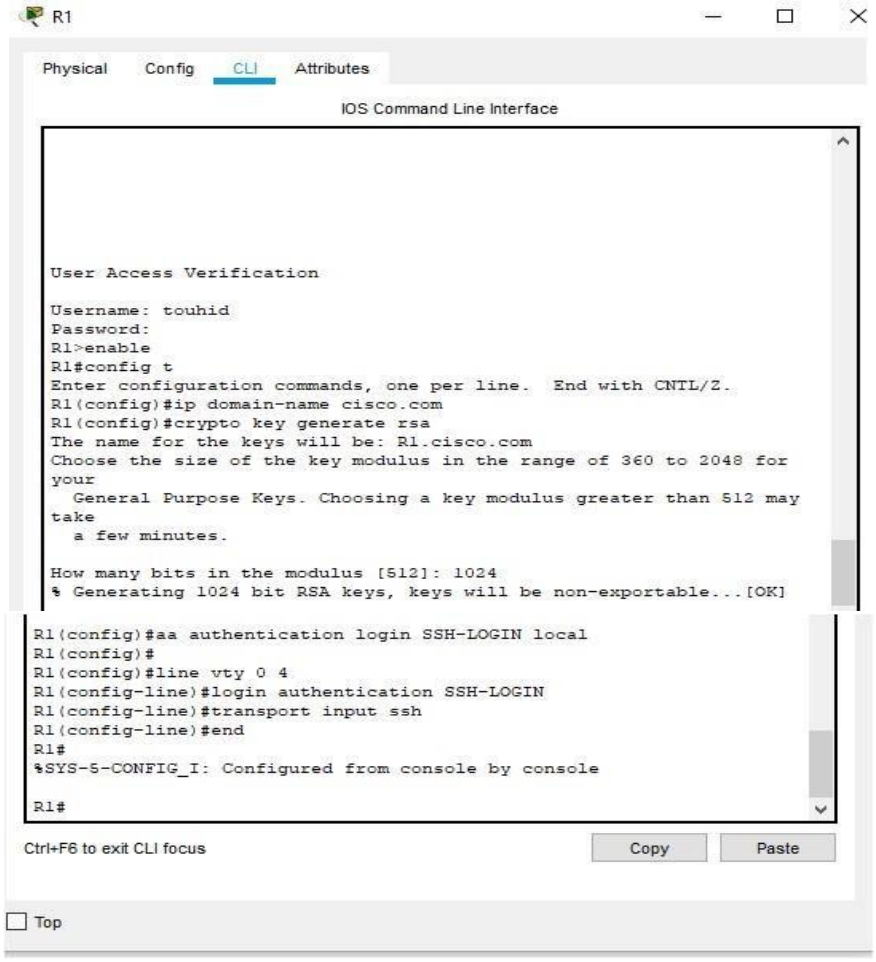


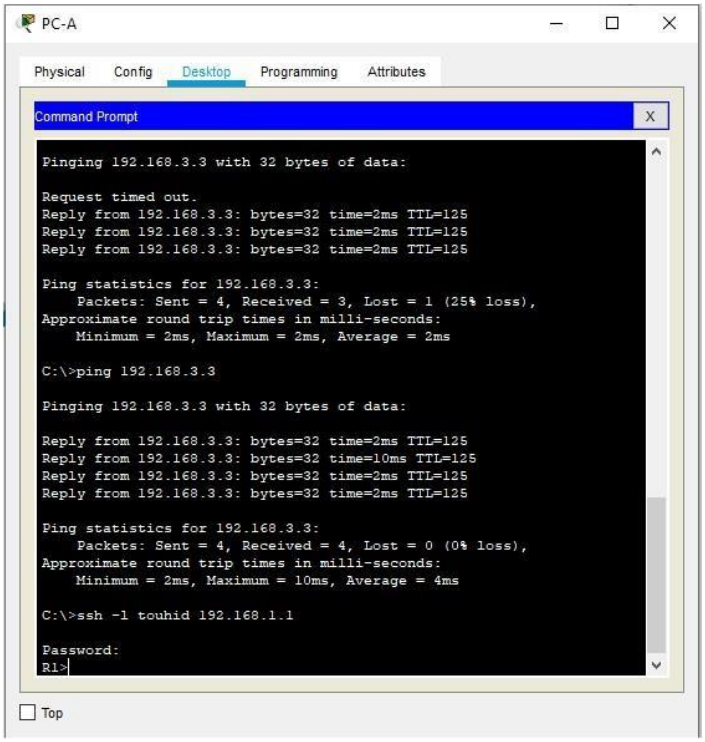


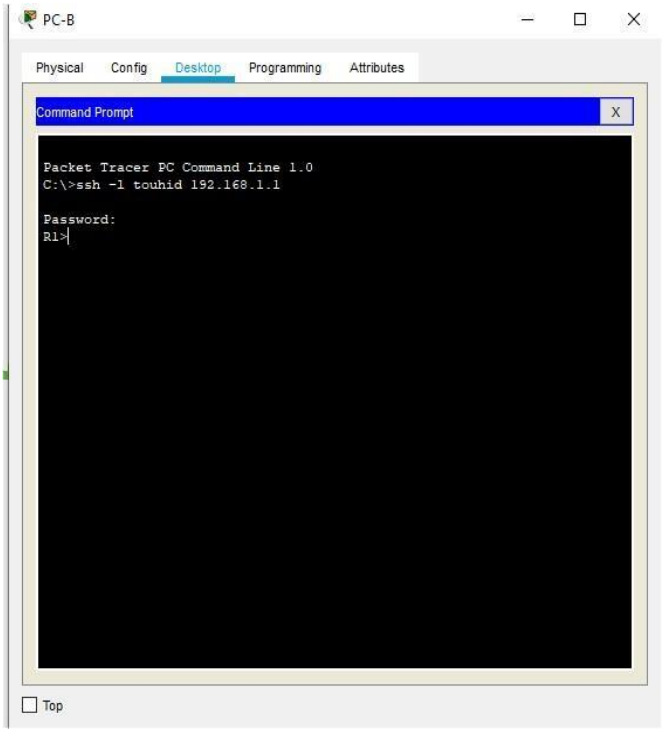
Username: touhid Password: 1234



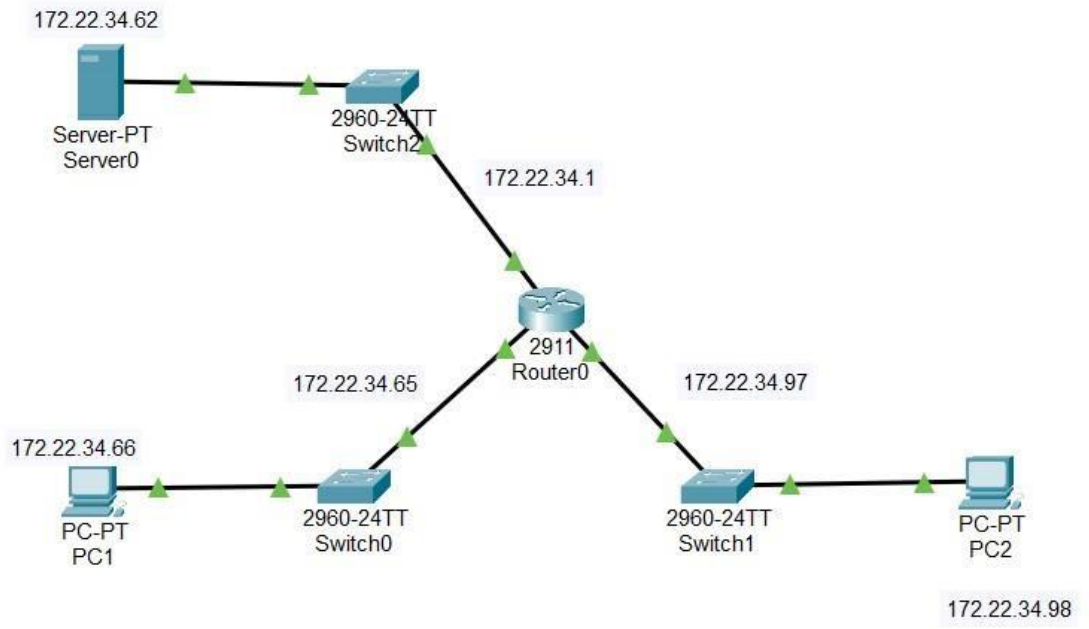
Part-2 :- Configure Local AAA Authentication for vty Lines on R1







Practical – 3 Configure Extended ACLs – Scenario 1



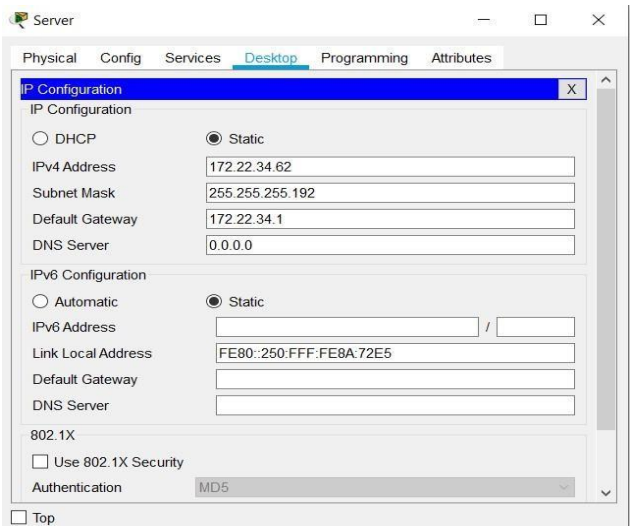
Address Table :-

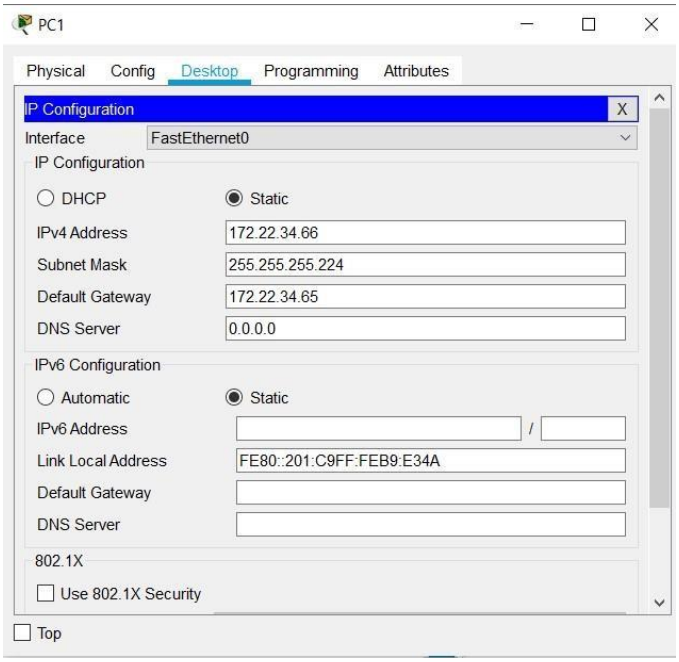
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G 0/0	172.22.34.1	255.255.255.252	N/A
	S 0/1	172.22.34.65	255.255.255.252	N/A
	S 0/2	172.22.34.97	255.255.255.252	N/A
Server	NIC	172.22.34.62	255.255.255.0	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.0	172.22.34.68
PC1	NIC	172.22.34.98	255.255.255.0	172.22.34.97

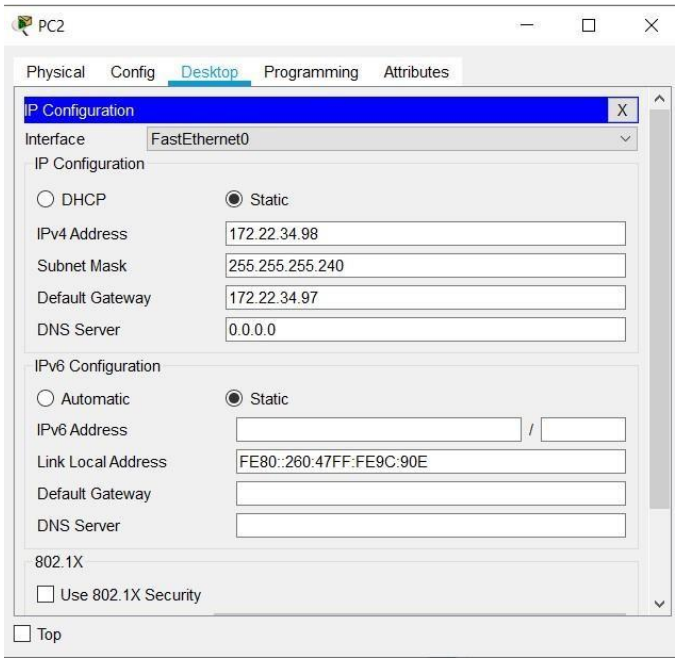
Necessary Step :-

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

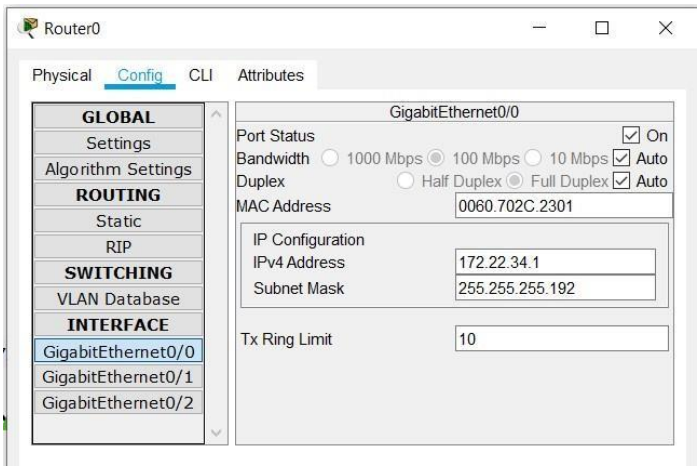
PC and Server Configuration :-

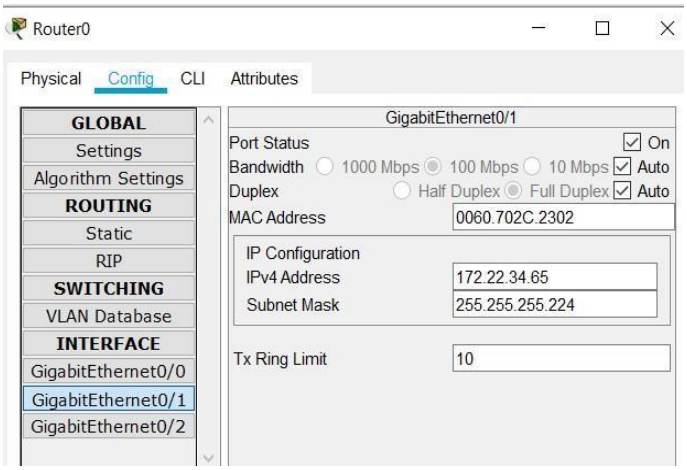


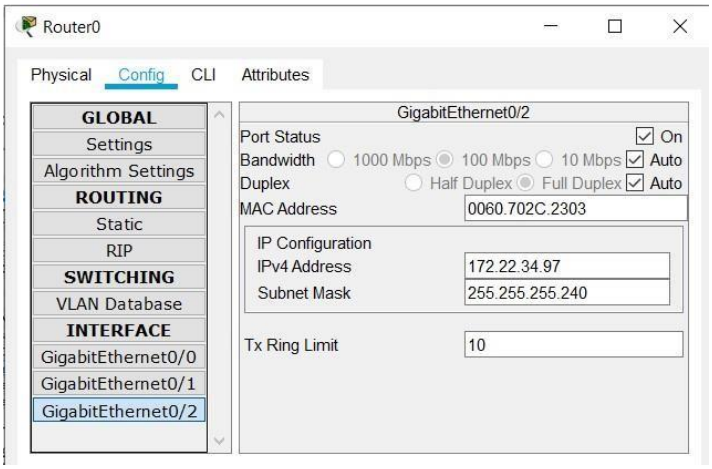




Router Configuration :-







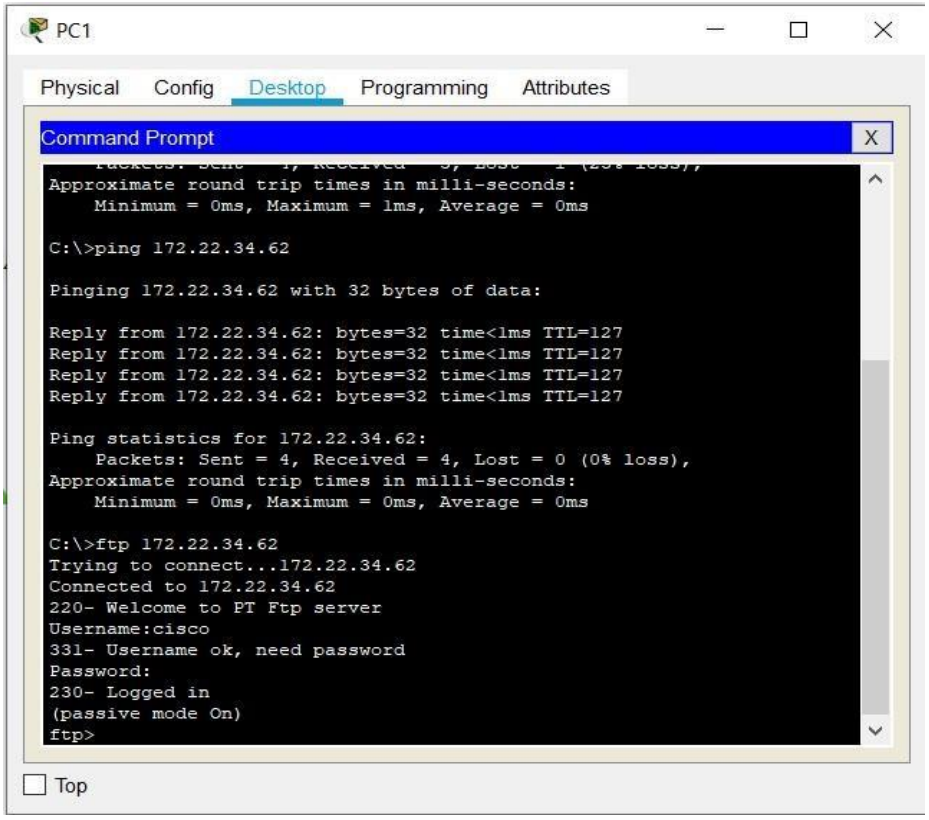
Note :- Check ping command from PC's to Server and it should work.

Part-1 :- Configure, Apply and Verify and Extended Numbered ACL.

Step-1 :- Configure an ACL to permit FTP and ICMP.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
Router(config)#access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Router(config)#
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
```

Step-2 :- Verify the ACL implementation in PC1.

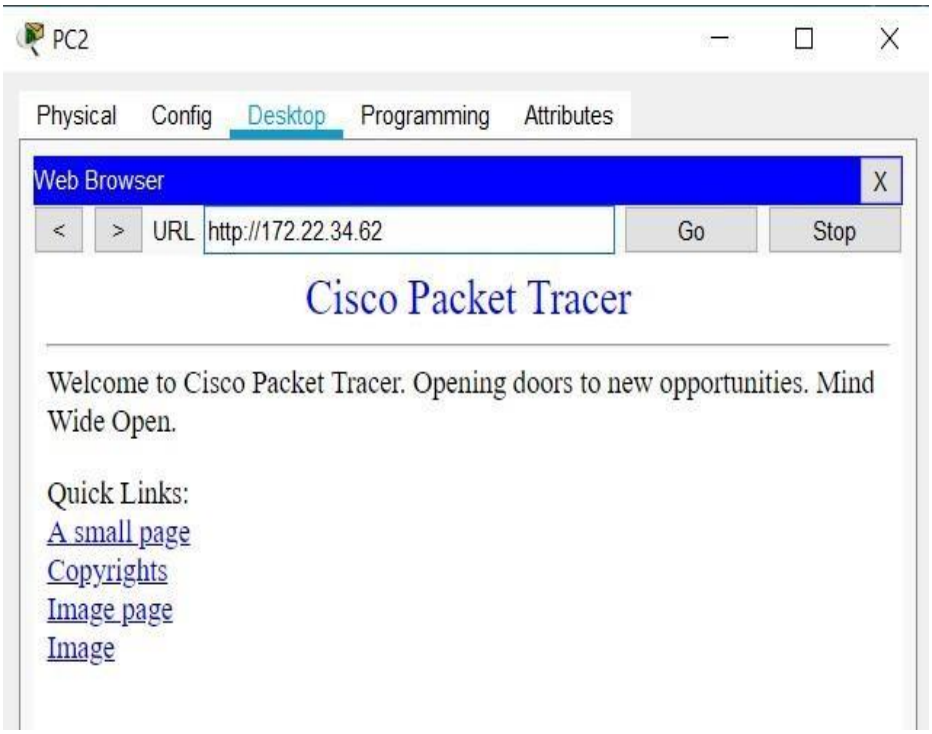


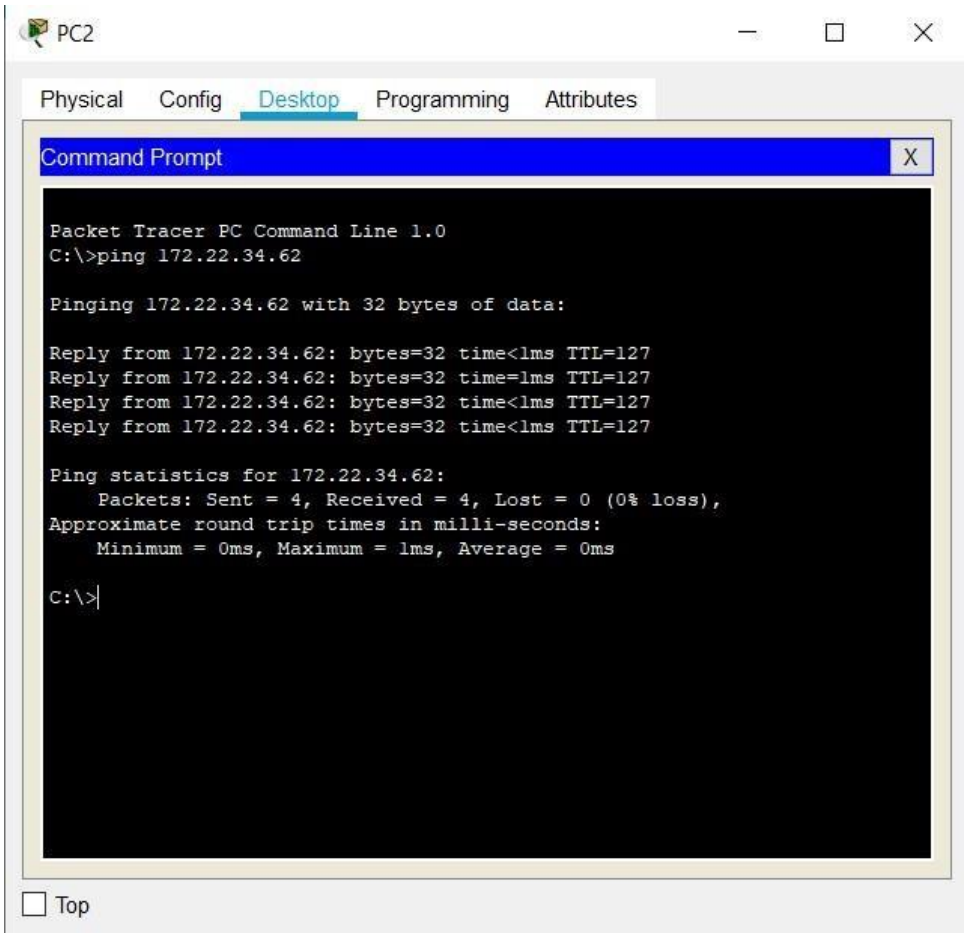
Note :- username = cisco, Password = cisco.

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

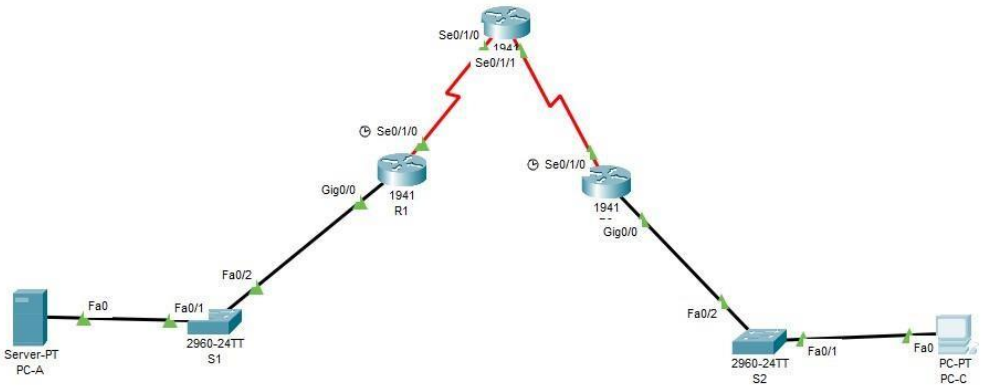
Step-1 :- Configure and ACL to permit HTTP access and ICMP.

```
Router(config)#ip access-list extended HTTP_ONLY
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
Router(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/2
Router(config-if)#ip access-group HTTP_ONLY in
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/2
Router(config-if)#
```


PC2
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://172.22.34.62
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


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.62
Pinging 172.22.34.62 with 32 bytes of data:
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time=1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Ping statistics for 172.22.34.62:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
Top

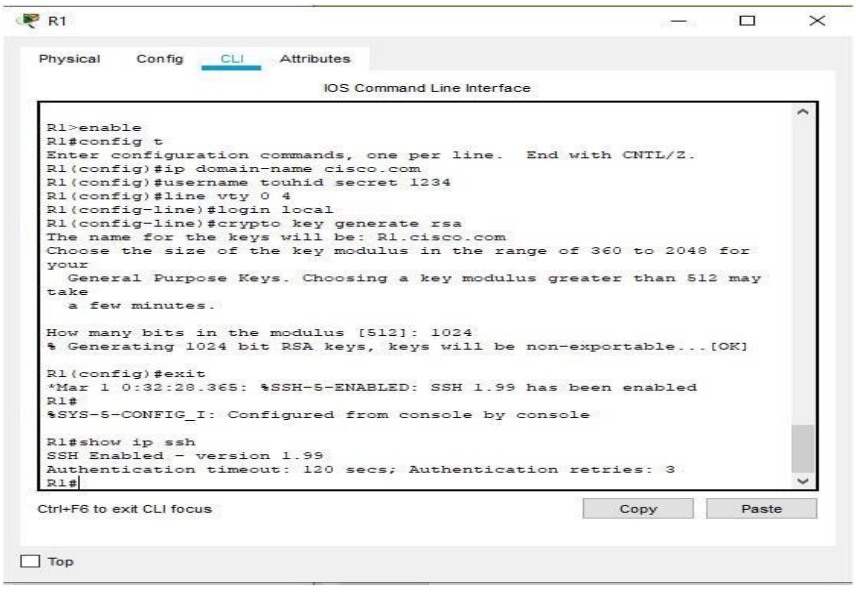
Practical – 4 Configure IP ACLs to Mitigate Attacks



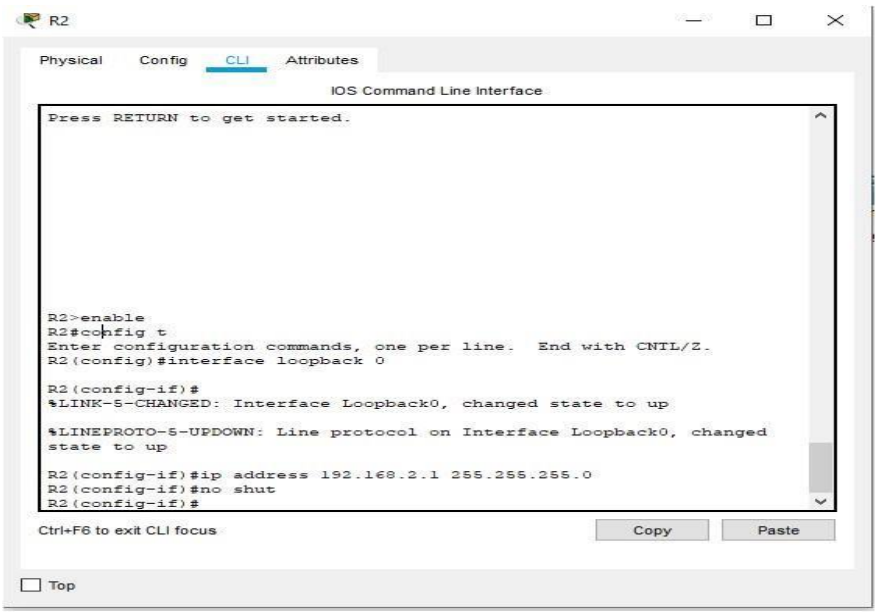
Address Table :-

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/0	192.168.1.1	255.255.255.0	
	Se0/1/0	10.1.1.1	255.255.255.252	
R2	Se0/1/0	10.1.1.2	255.255.255.252	
	Se0/1/1	10.2.2.2	255.255.255.252	
	Lo0	192.168.2.1	255.255.255.0	
R3	Gig0/0	192.168.3.1	255.255.255.0	
	Se0/1/0	10.2.2.1	255.255.255.252	
PC-A	Fa0	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	Fa0	192.168.3.3	255.255.255.0	192.168.3.1

Step-1 :- Configure SSH login on all 3 routers (Repeat same steps for all 3 Routers)

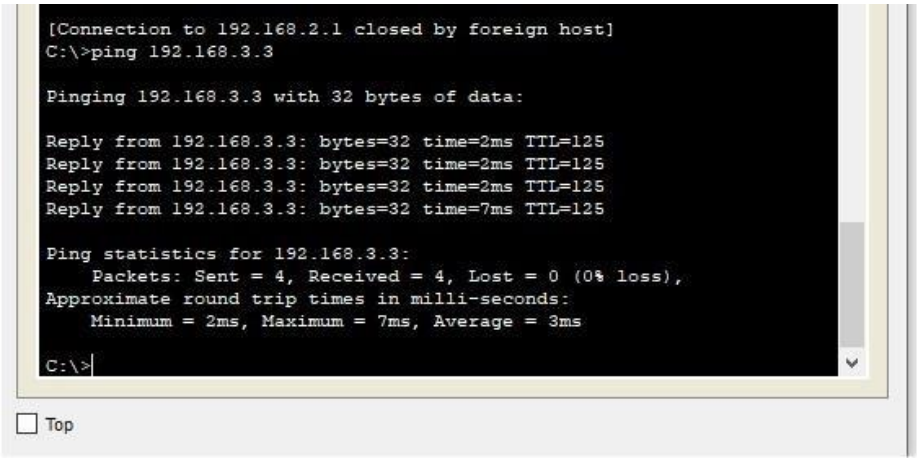


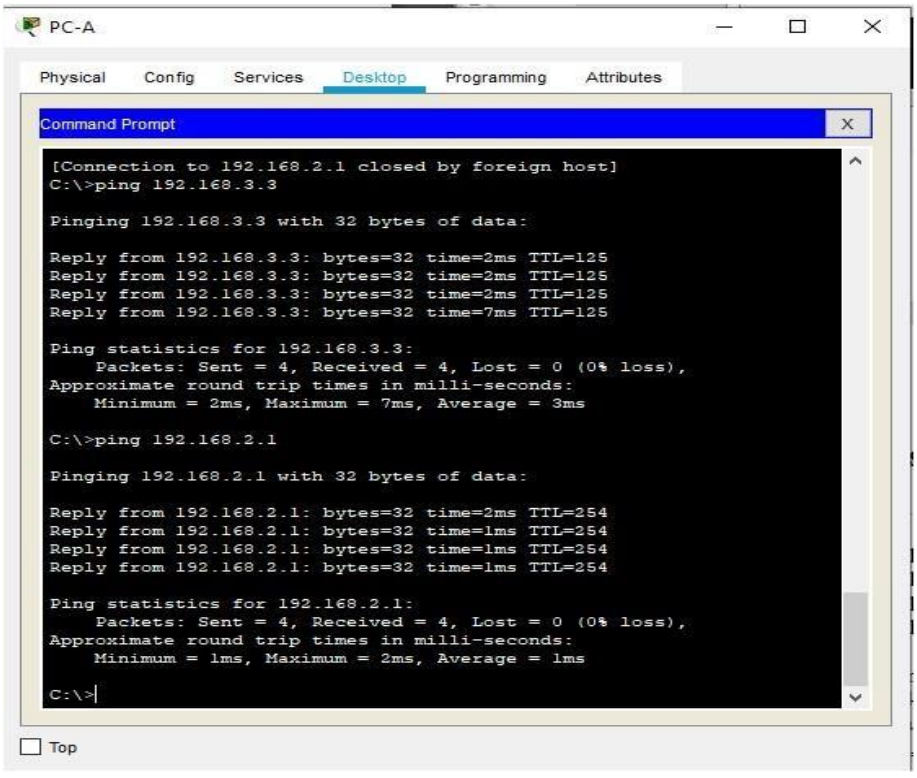
Step-2 :- Configure loop back address on Router 2.



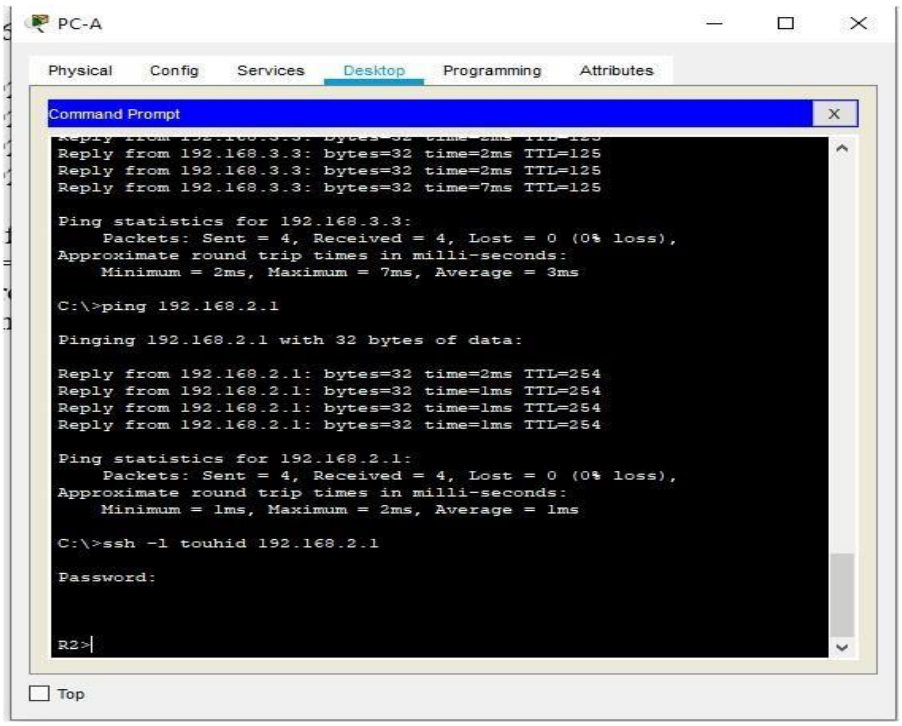
Part-1 :- Verify Basic Network Connectivity.

Step-1 :- From PC-A, Verify connectivity to PC-C and R2.

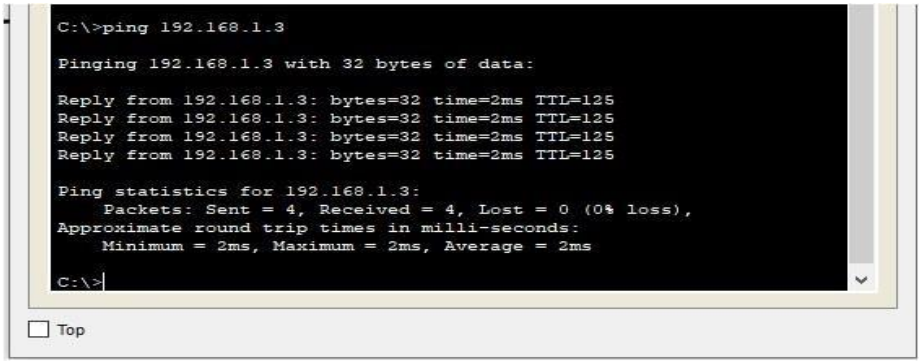


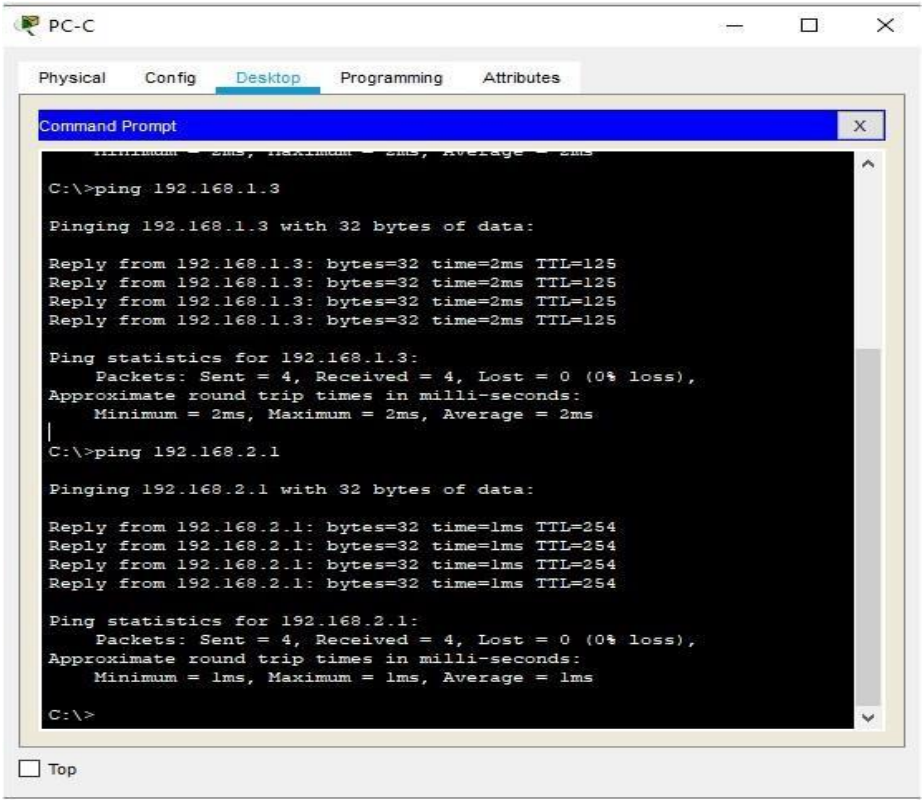


Checking SSH from PC :-

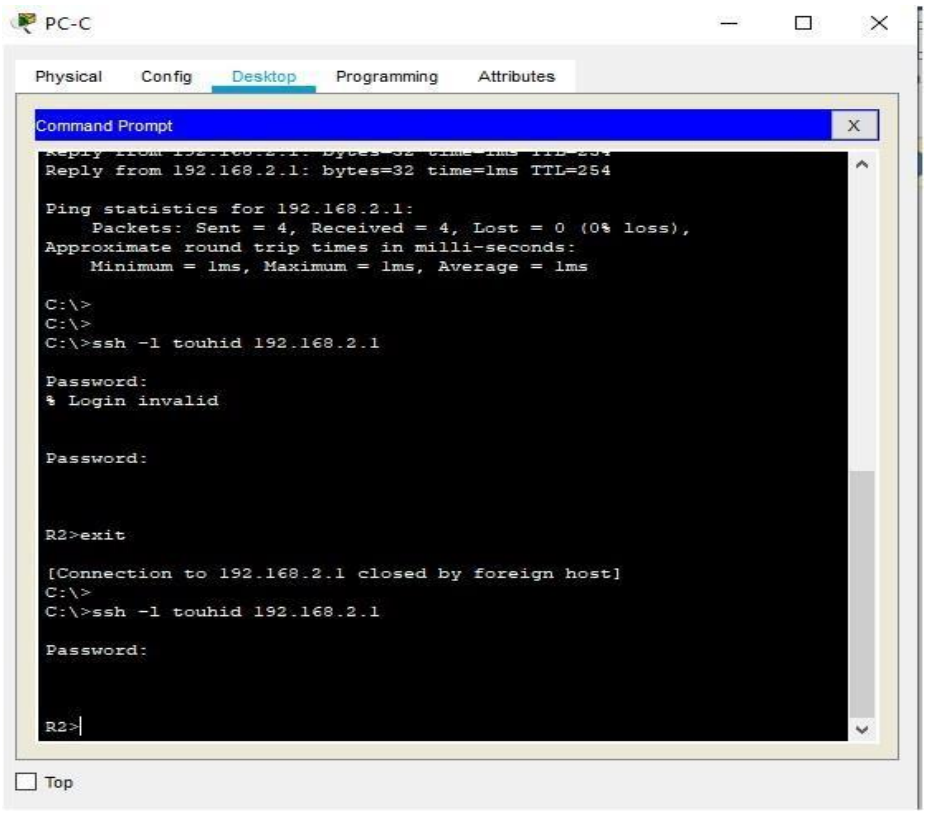


Step-2 :- From PC-C, Verify connectivity to PC-A and R2.



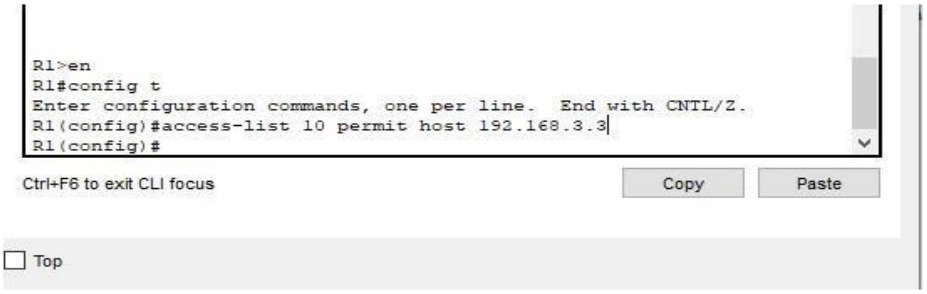


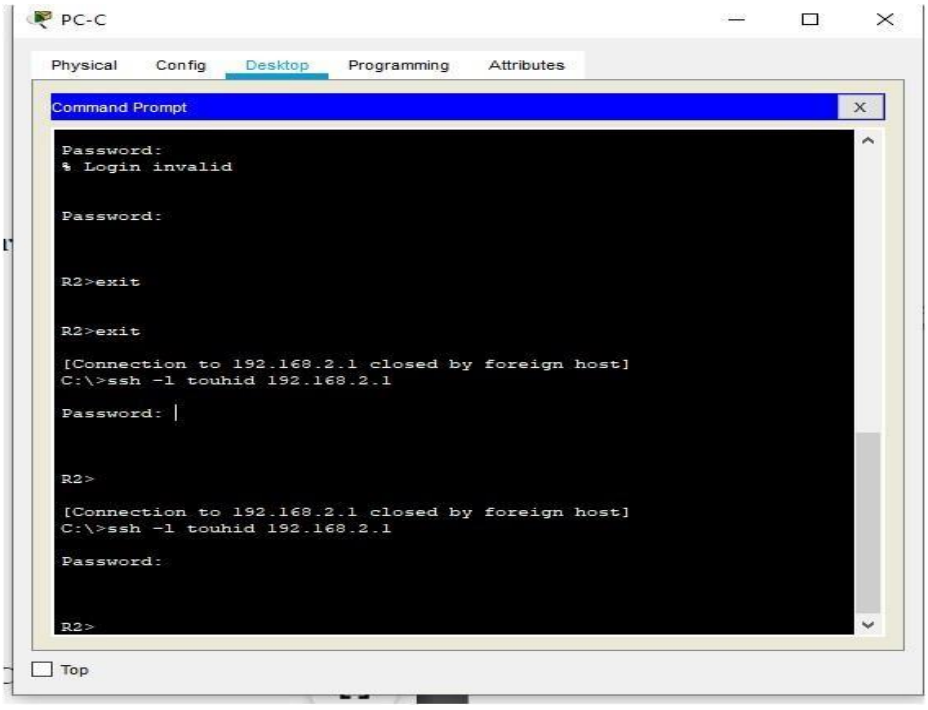
Checking SSH via loopback address :-

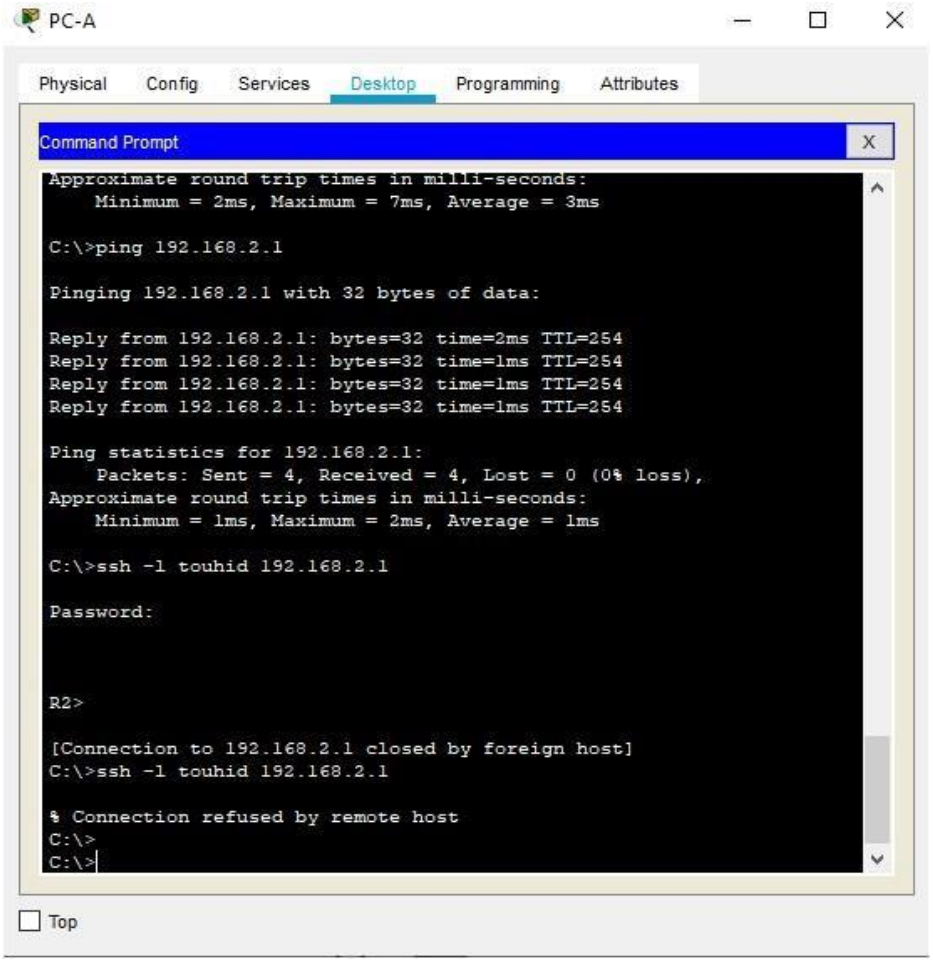


Part-2 :- Secure Access to Routers.

Step-1 :- Configure ACL 10 to block all remote access to the routers except from PC-C.
Execute command on all Routers (R1, R2, R3)

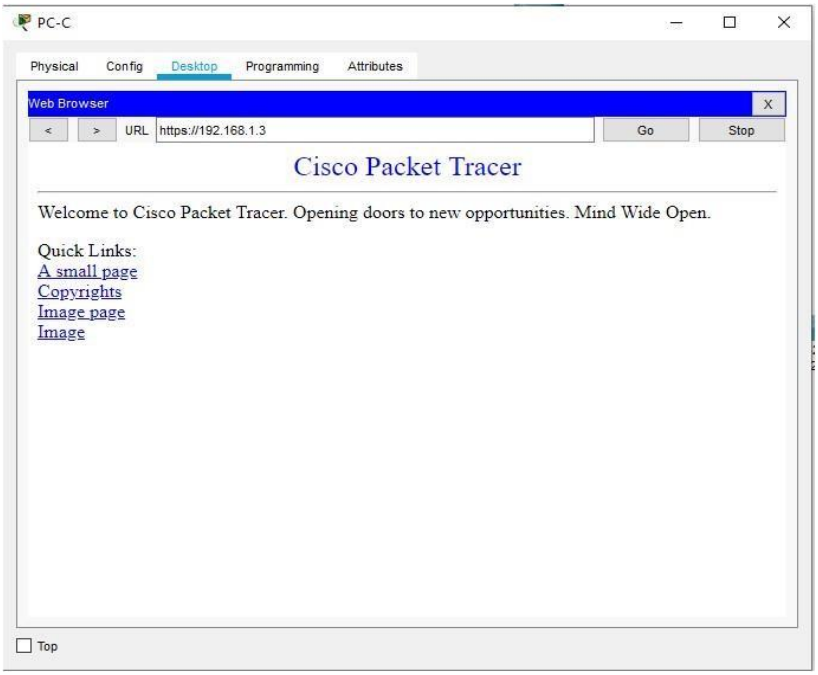




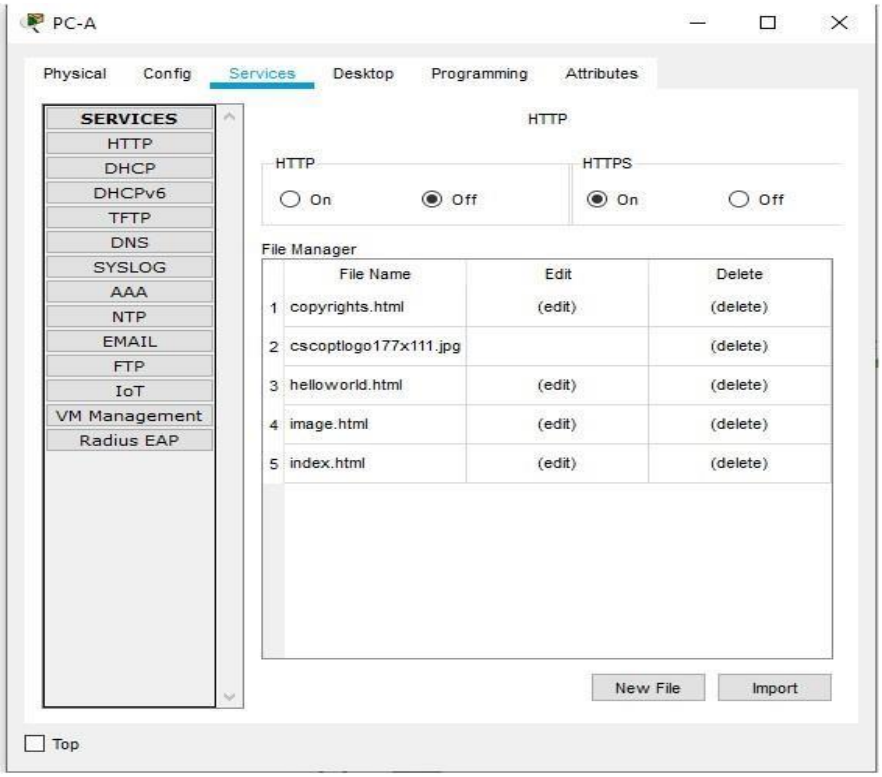


Part-3 :- Create a Numbered IP ACL 120 on R1.

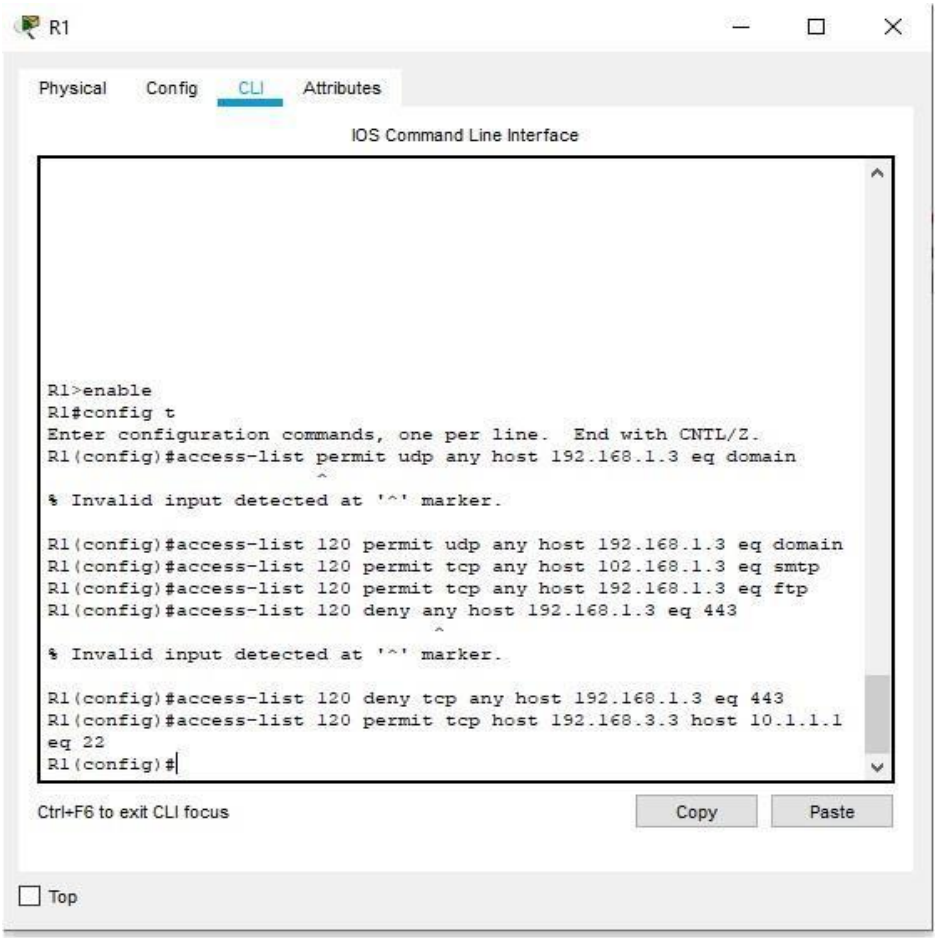
Step-1 :- Verify that PC-C can access the PC-A via HTTP using the web browser.



Be sure to disable HTTP and enable HTTP on server PC-A in Services tab.

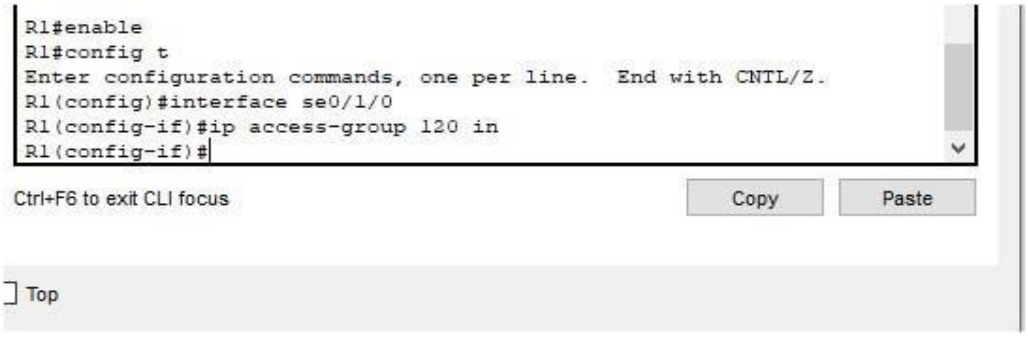


Step-2 :- Configure ACL 120 to specifically permit and deny the specified traffic.

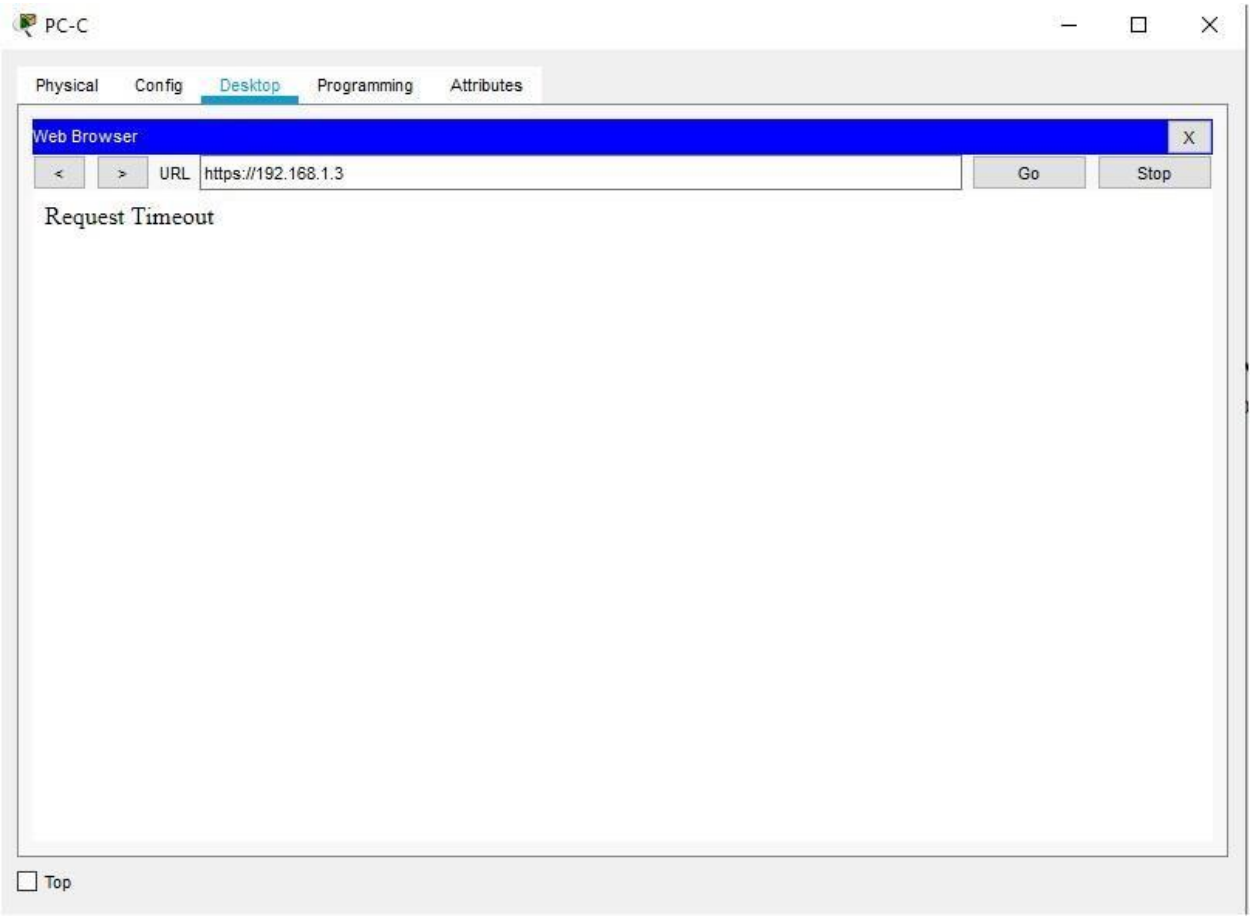


192.168.1.3 (PC-A IP address)

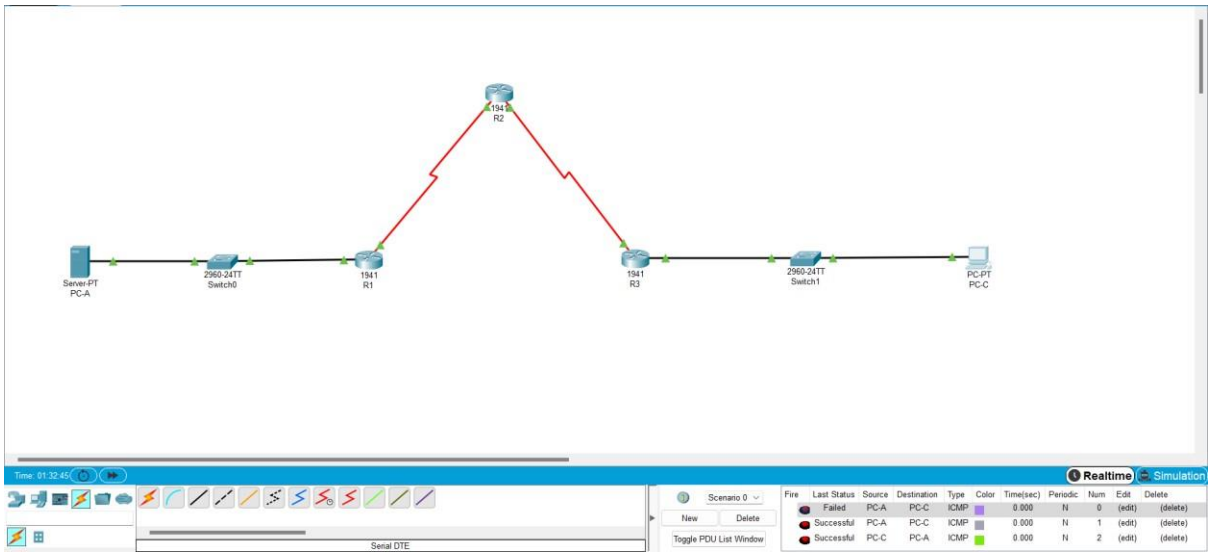
Step-3 :- Apply the ACL to interface (on Router 1)



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



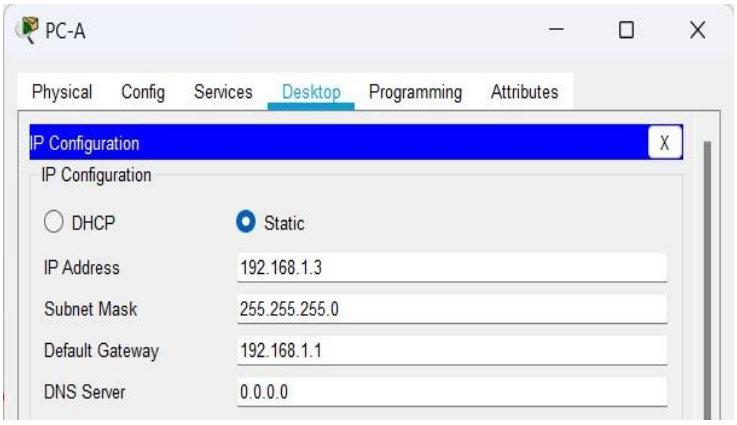
Practical – 5 Configuring a Zone-Based Policy Firewall (ZPF)

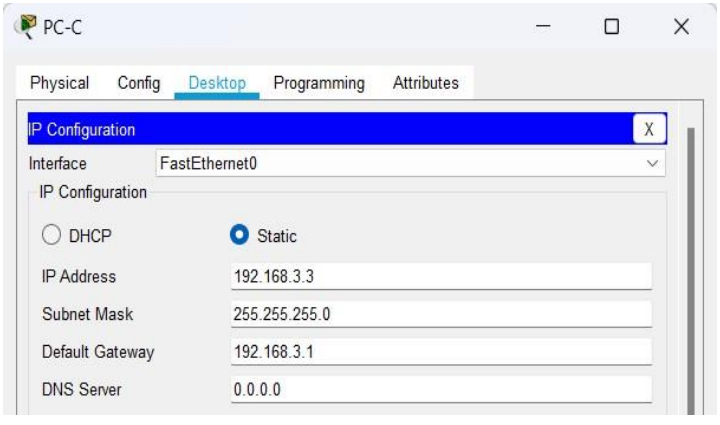


Addressing Table :-

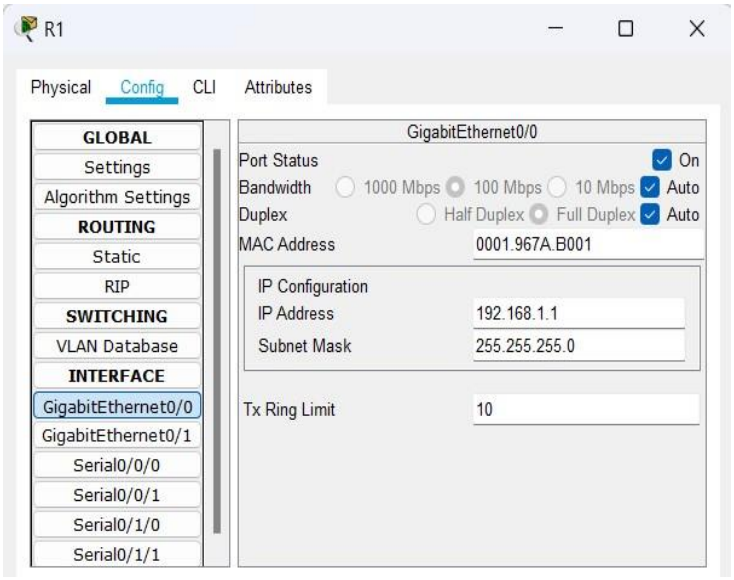
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	
	S0/1/0	10.1.1.1	255.255.255.252	
R2	S0/1/0	10.1.1.2	255.255.255.252	
	S0/1/1	10.2.2.2	255.255.255.252	
	Lo0	192.168.2.1	255.255.255.0	
R3	Gig0/0	192.168.3.1	255.255.255.0	
	Se0/1/0	10.2.2.1	255.255.255.252	
PC-A	Fa0	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	Fa0	192.168.3.3	255.255.255.0	192.168.3.1

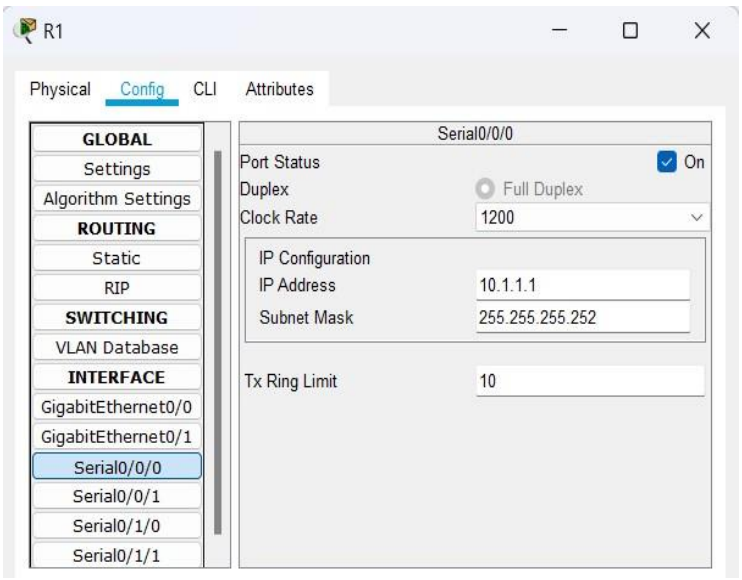
IP Configuration :-

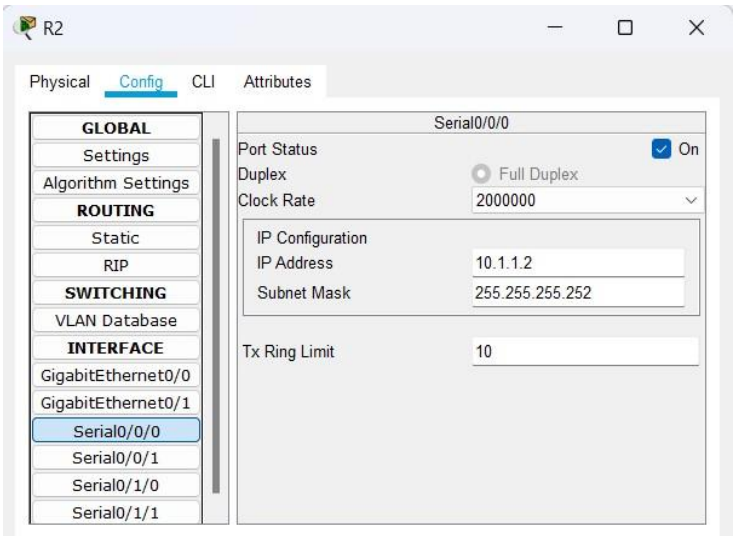


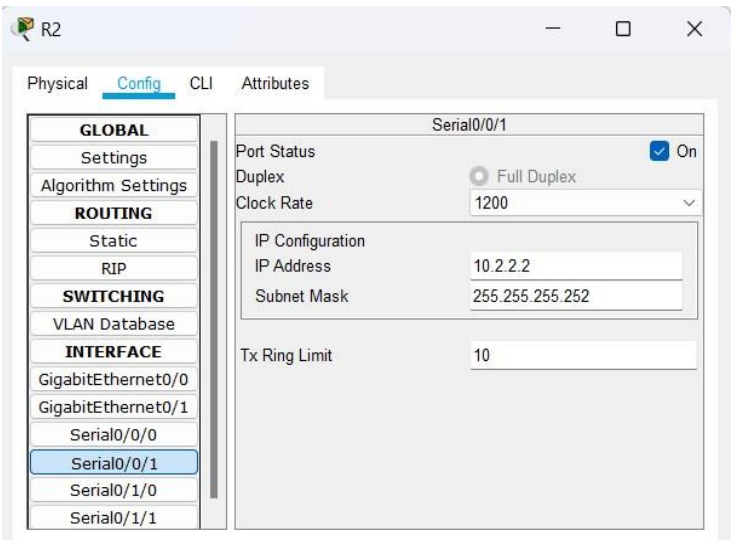


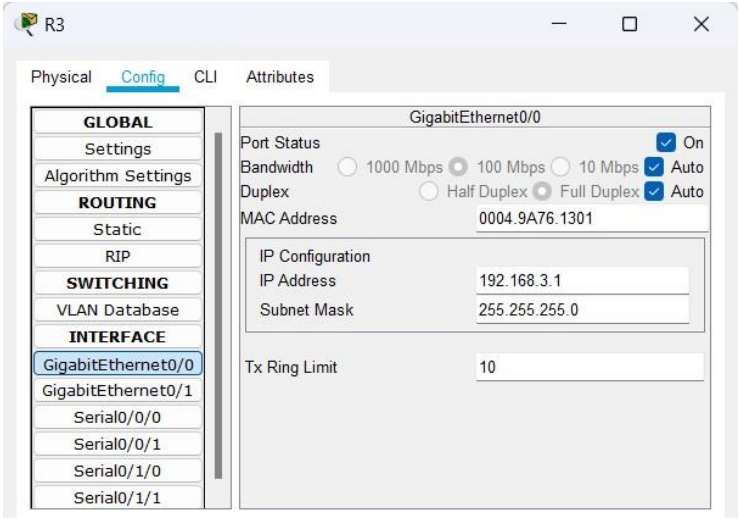
Router Configuration :-

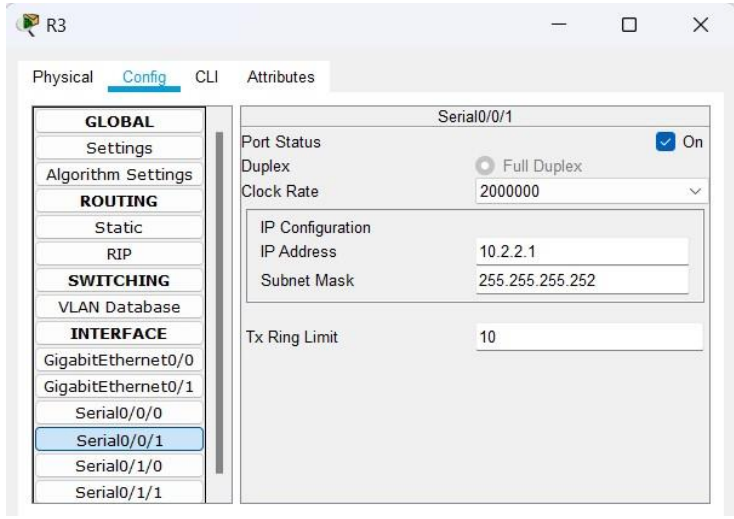




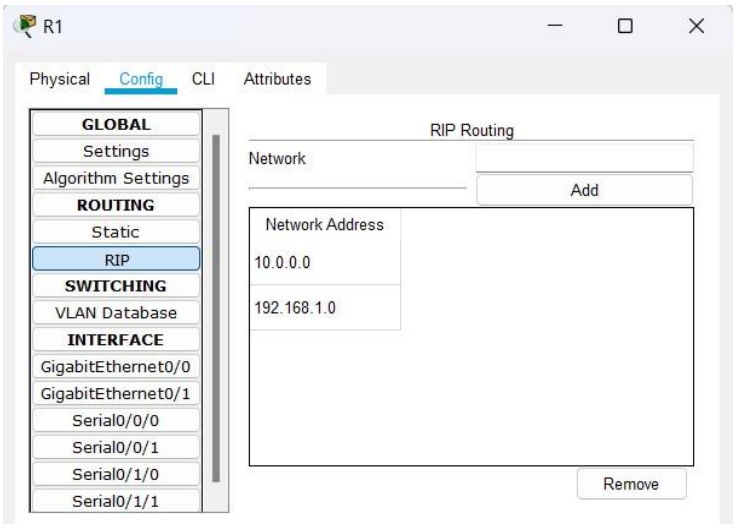


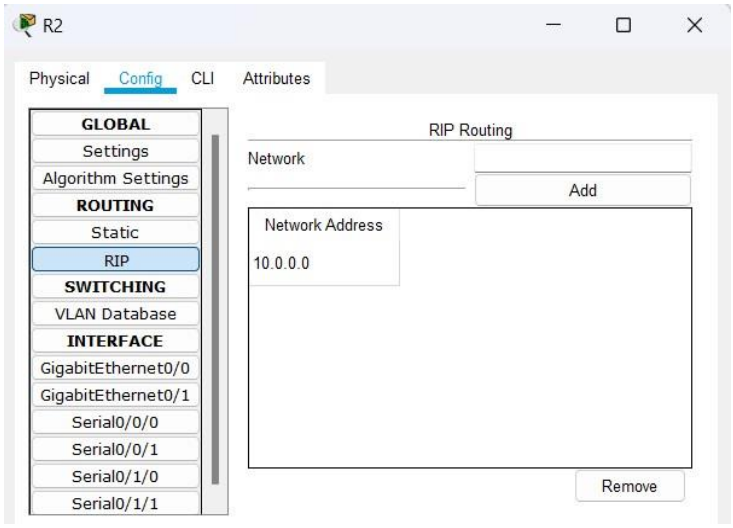


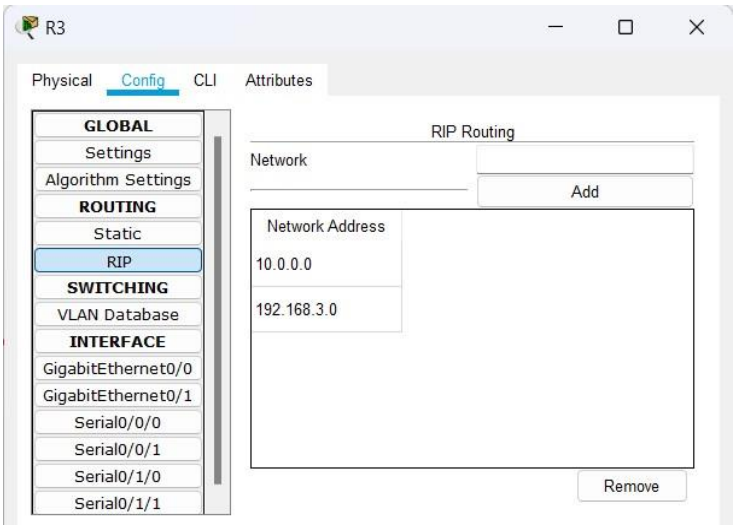




RIP Configuration :-







Verify Basic Network Connectivity.

```
R3(config)#ip domain-name security.com
R3(config)#username admin privilege 15 secret admin123
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#crypto key generate rsa
The name for the keys will be: R3.security.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

R3(config)#ip ssh time-out 90
*Mar 1 0:7:3.815: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh version 2
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
```

Part-1 :- Create Firewall Zones on R3

```
R3(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
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: y
% 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
exit
```

```
exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
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.
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)
```

```
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


R3>
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

R3>en
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)
ciscol941 uptime is 45 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.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#    PID                      SN
-------------------------------------------------
```

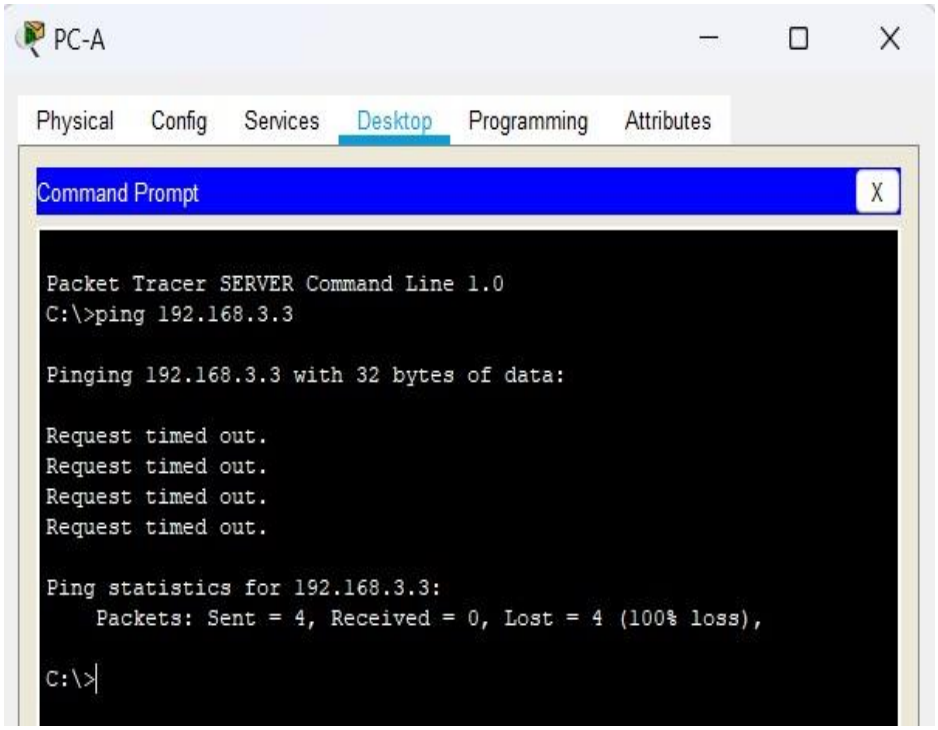
Part-2 :- Create an internal zone.

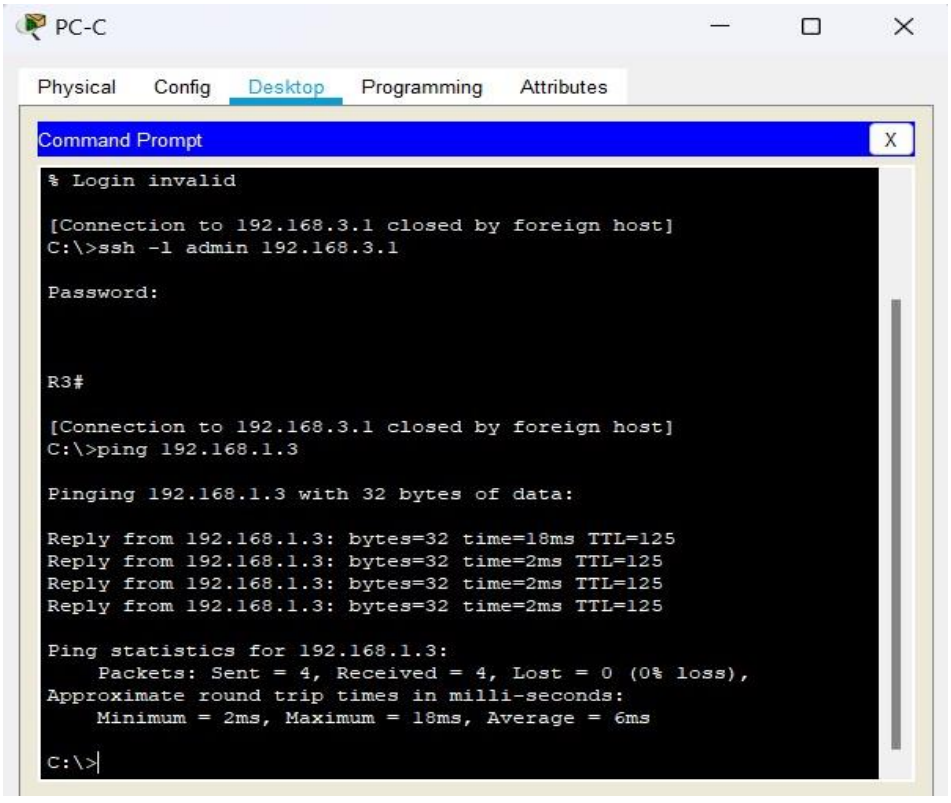
Part-3 :- Create an ACL for internal traffic.

Part-4 :- Firewall Policies.

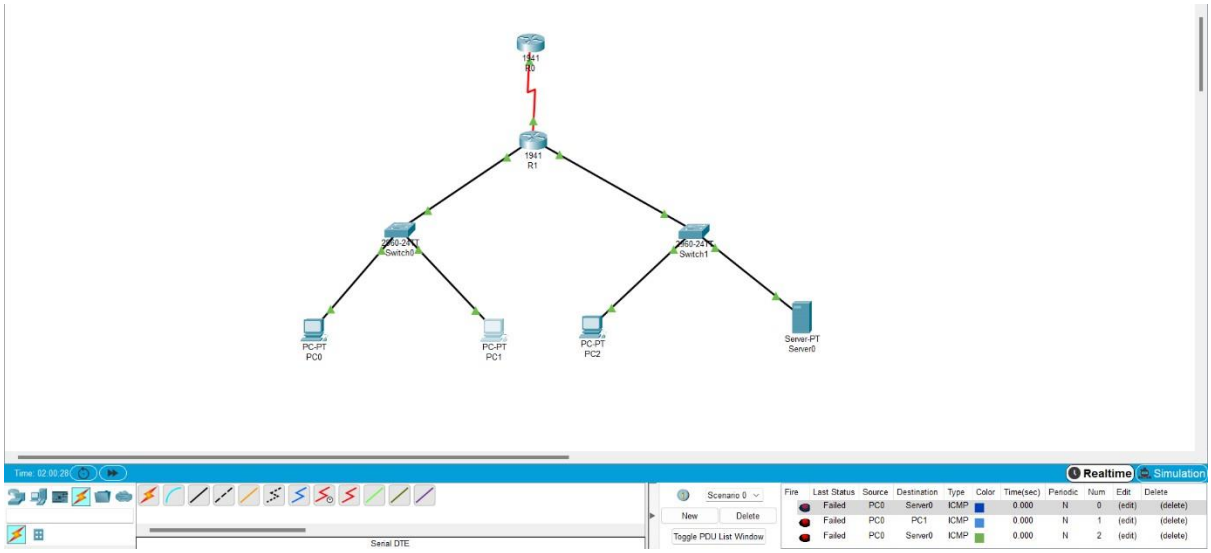
Part-5 :- Apply Policies.

```
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#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#zone security IN-ZONE
R3(config-sec-zzone security IN-ZONEzone 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)#MAMmatch 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)#eexit
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)#
R3(config)#interface GigabitEthernet0/0
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#
R3(config)#interface GigabitEthernet0/0
R3(config-if)#
R3(config-if)#exit
R3(config)#interfaczone-member security IN-ZONEzone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

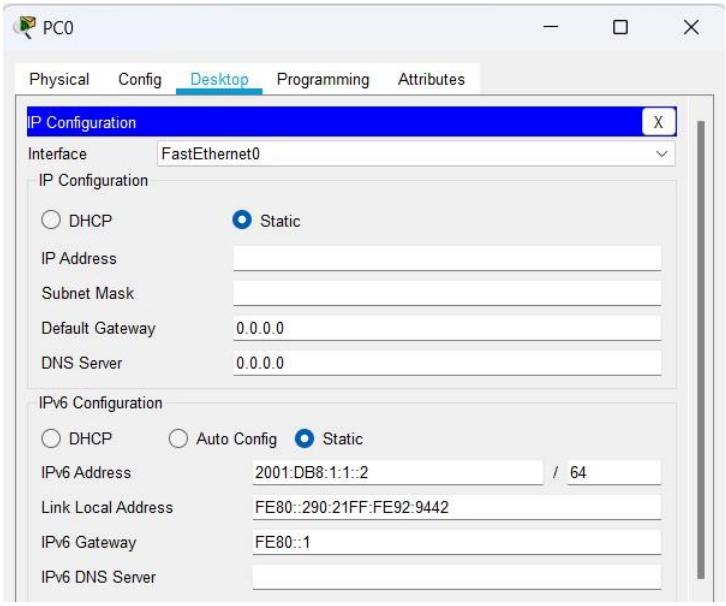

PC-A
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

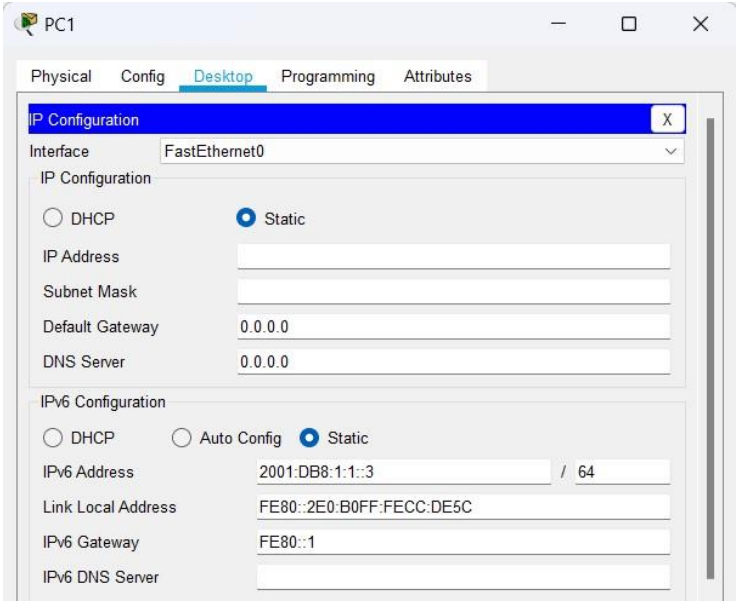

PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
% Login invalid
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l admin 192.168.3.1
Password:
R3#
[Connection to 192.168.3.1 closed by foreign host]
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=18ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 18ms, Average = 6ms
C:\>

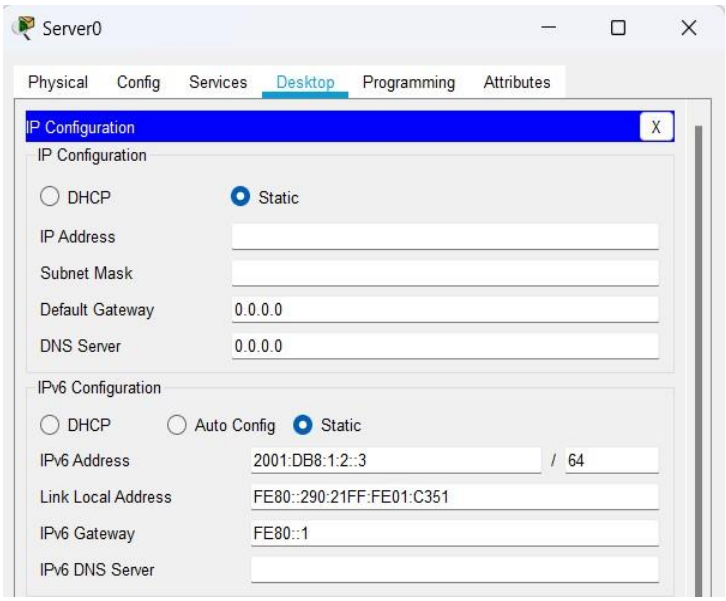
Practical – 6 Configuration IPV6 ACLs

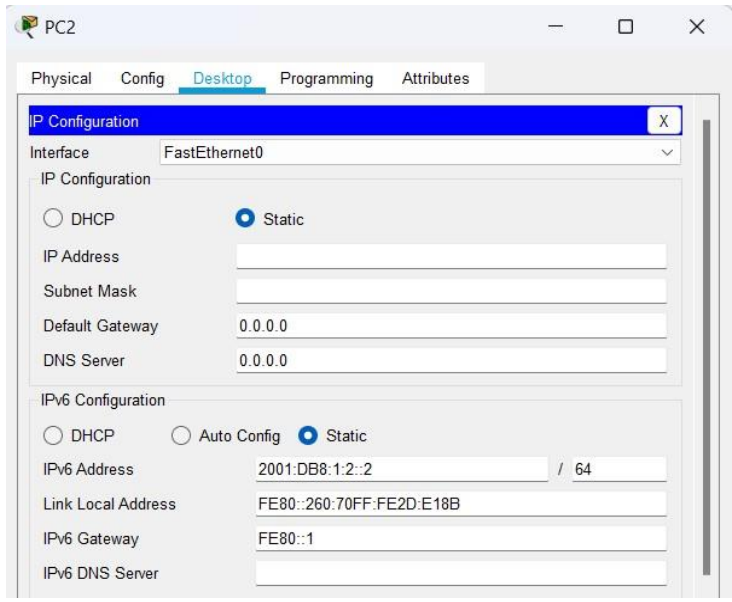


IP Configuration :-









Router Configuration :-

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R0
R0(config)#ipv6 unicast-routing
R0(config)#int serial 0/0/0
R0(config-if)#ipv6 address 2001:DB8:1:A001::1/64
R0(config-if)#ipv6 address FE80::1 link local
                                           ^
% Invalid input detected at '^' marker.

R0(config-if)#ipv6 address FE80::1 link-local
R0(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R0(config-if)#exit
R0(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#exit
R1(config)#ipv6 unicast-routing
R1(config)#int serial 0/0/0
R1(config-if)#ipv6 address 2001:DB8:1:A001::2/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
exi
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
exit
                 ^
% Invalid input detected at '^' marker.

R1(config-if)#exit
R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 address 2001:DB8:1:1::1/64
R1(config-if)#ipv6 address 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
exit
R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ipv6 address 2001:DB8:1:2::1/64
R1(config-if)#ipv6 address FE80::1 link-local
R1(config-if)#no shut

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

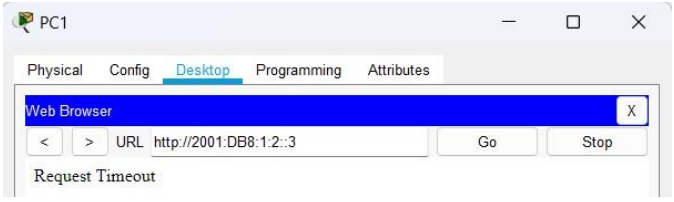
Part :- Block HTTP and HTTPS to reach server. Allow all other traffic.

```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK-HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:2::3 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:2::3 eq 443
R1(config-ipv6-acl)#exit
R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 access-list BLOCK-HTTP
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#
R1(config)#interface GigabitEthernet0/0

R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ipv6 traffic-filter BLOCK-HTTP in
R1(config-if)#exit
R1(config)#
```

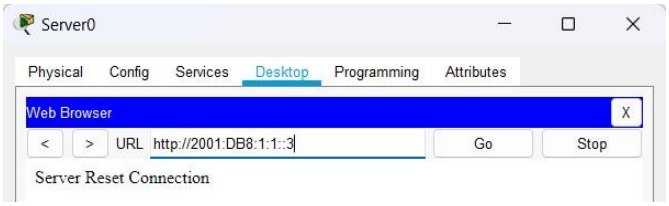
```
R1>EN
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK-HTTP
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:2::3 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:2::3 eq 443
R1(config-ipv6-acl)#exit
R1(config)#int gigabitethernet0/0
R1(config-if)#ipv6 access-list BLOCK-HTTP
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#int gigabitethernet0/0
R1(config-if)#ipv6 traffic-filter BLOCK-HTTP in
R1(config-if)#exit
R1(config)#ipv6 access-list BLOCK-ICMP
R1(config-ipv6-acl)#deny icmp any any
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#int gigabitethernet0/1
       ^
% Invalid input detected at '^' marker.

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int gigabitethernet0/1
R1(config-if)#ipv6 traffic-filter BLOCK-ICMP out
R1(config-if)#exit
R1(config)#
```

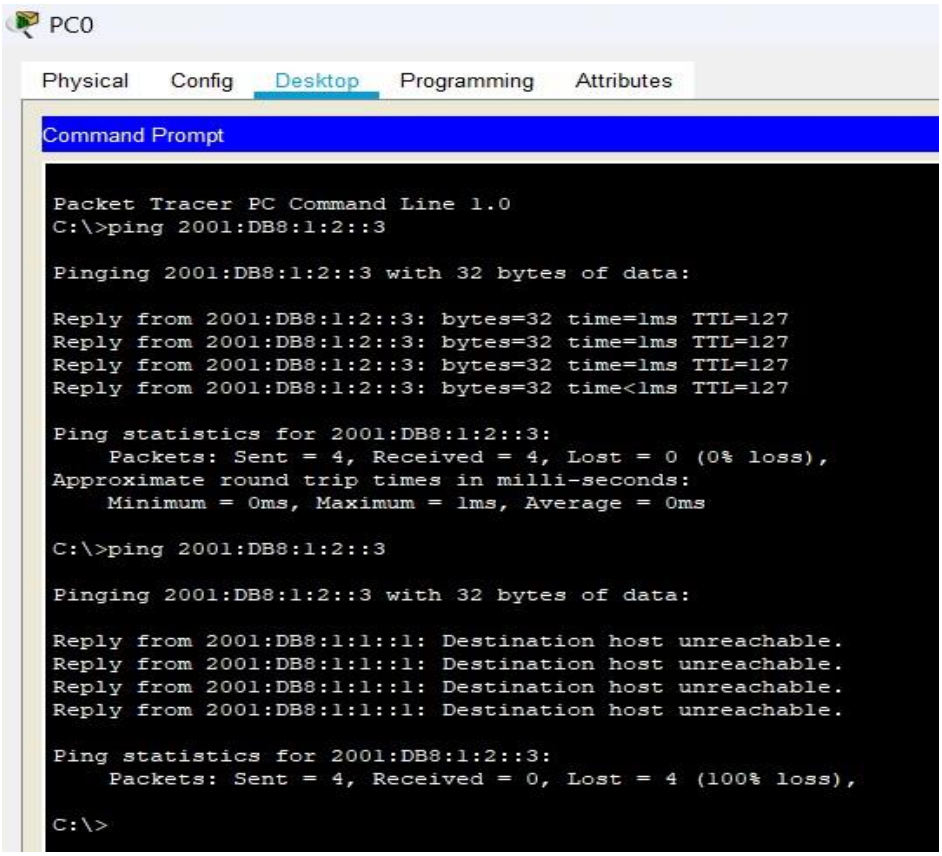
Web Browser :-

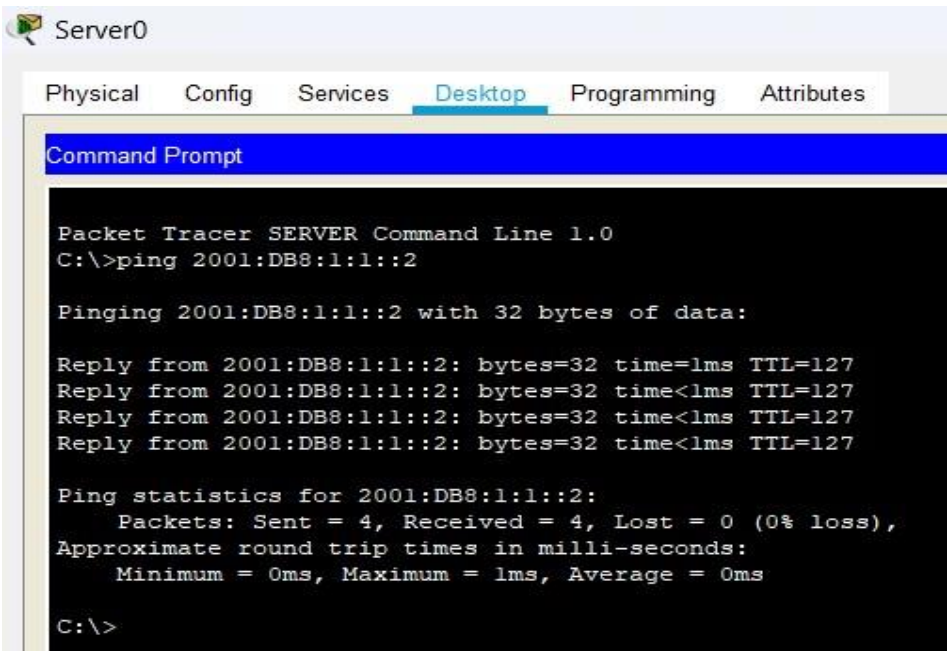

PC0
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://2001:DB8:1:2::3
Go
Stop
Request Timeout


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://2001:DB8:1:2::3
Go
Stop
Request Timeout

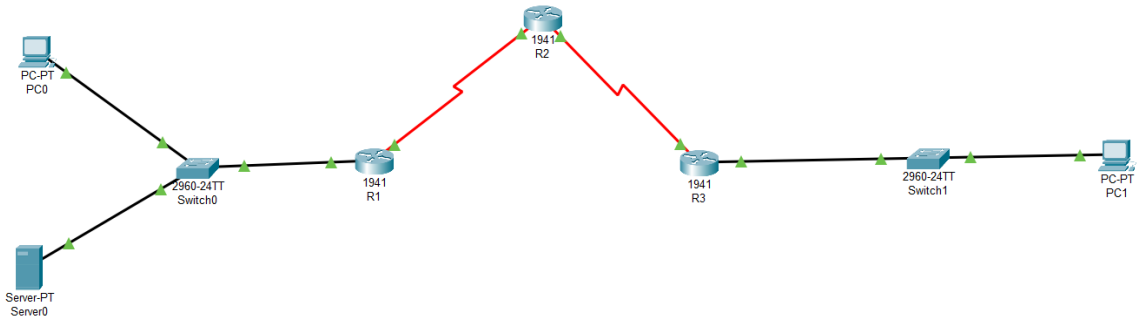

Server0
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL
http://2001:DB8:1:1::2
Go
Stop
Server Reset Connection


Server0
Physical
Config
Services
Desktop
Programming
Attributes
Web Browser
URL
http://2001:DB8:1:1::3
Go
Stop
Server Reset Connection

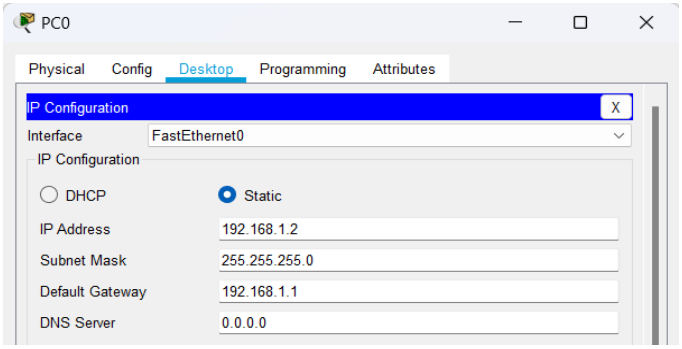

PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:DB8:1:2::3
Pinging 2001:DB8:1:2::3 with 32 bytes of data:
Reply from 2001:DB8:1:2::3: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:2::3: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:2::3: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:2::3: bytes=32 time<1ms TTL=127
Ping statistics for 2001:DB8:1:2::3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 2001:DB8:1:2::3
Pinging 2001:DB8:1:2::3 with 32 bytes of data:
Reply from 2001:DB8:1:1::1: Destination host unreachable.
Reply from 2001:DB8:1:1::1: Destination host unreachable.
Reply from 2001:DB8:1:1::1: Destination host unreachable.
Reply from 2001:DB8:1:1::1: Destination host unreachable.
Ping statistics for 2001:DB8:1:2::3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

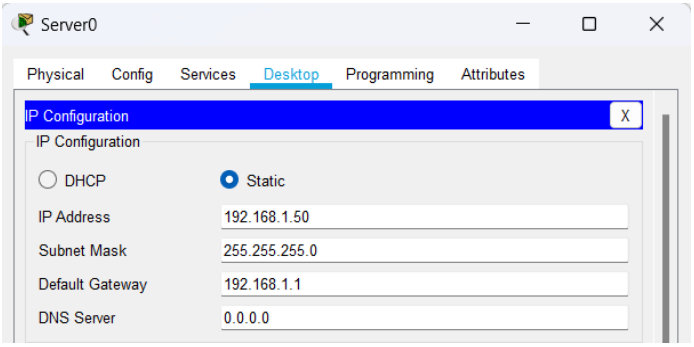

Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 2001:DB8:1:1::2
Pinging 2001:DB8:1:1::2 with 32 bytes of data:
Reply from 2001:DB8:1:1::2: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:1::2: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:1:1::2: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:1:1::2: bytes=32 time<1ms TTL=127
Ping statistics for 2001:DB8:1:1::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>

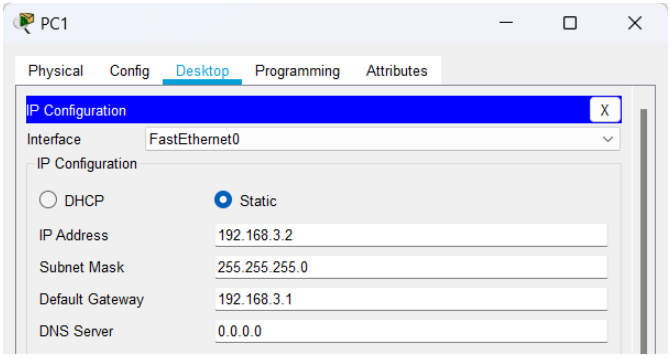
Practical – 7 Configuration IOS Intrusion Prevention System (IPS) Using the CLI



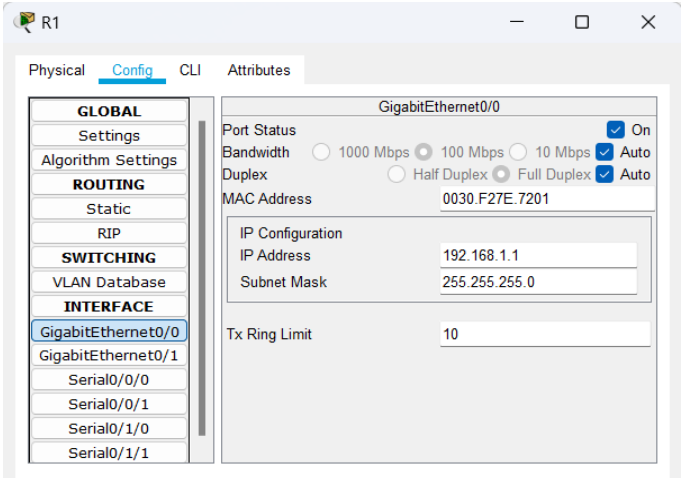
IP Configuration :-

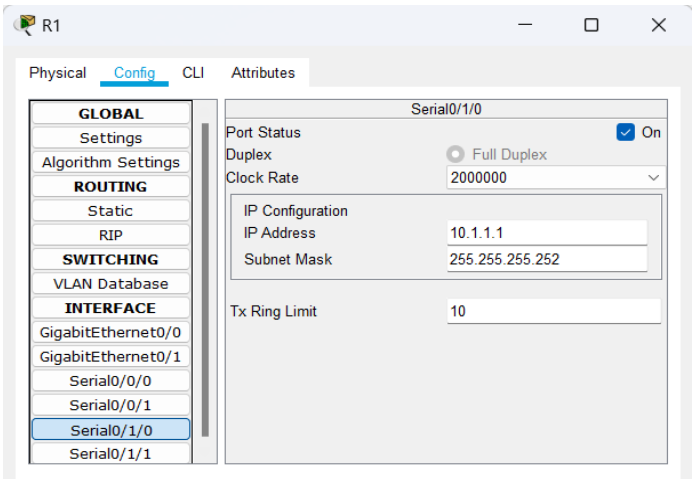


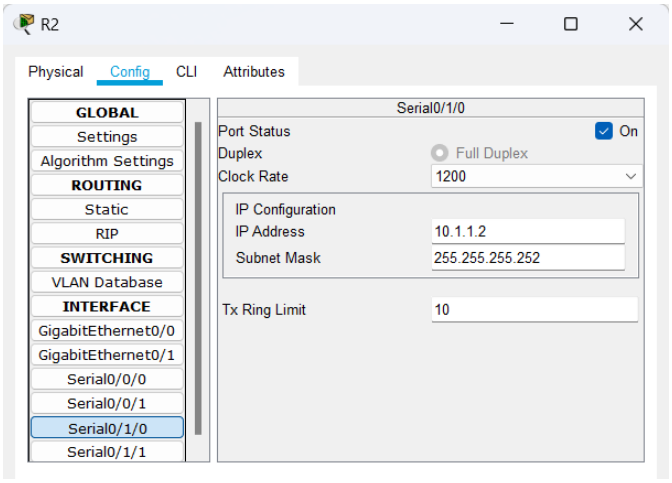


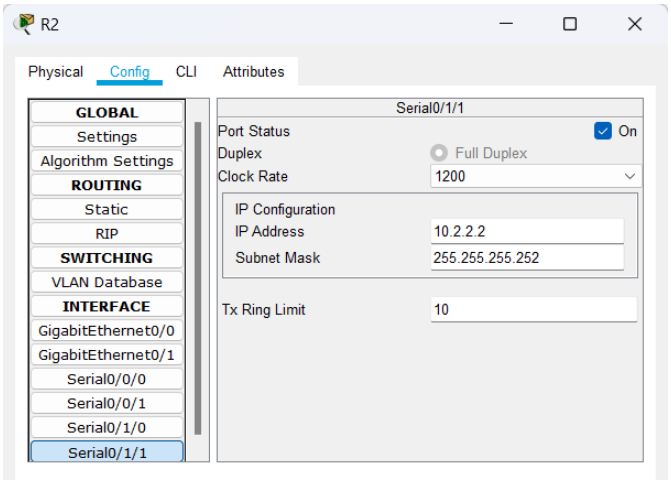


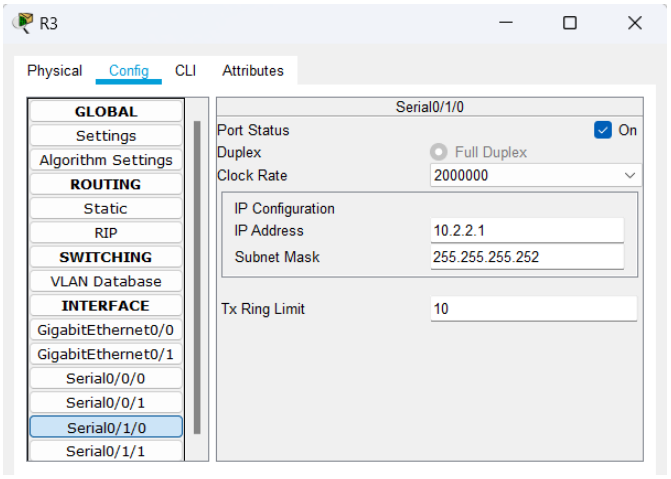
Router Configuration :-

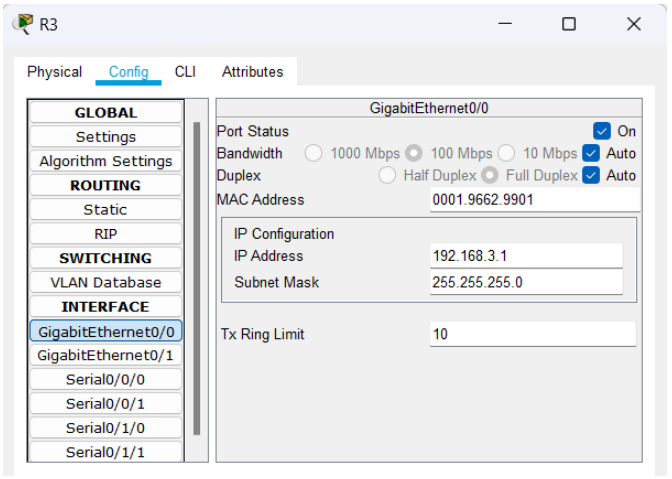




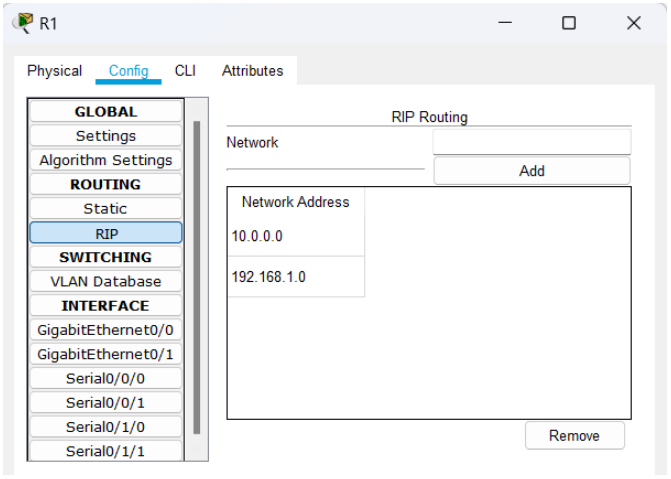


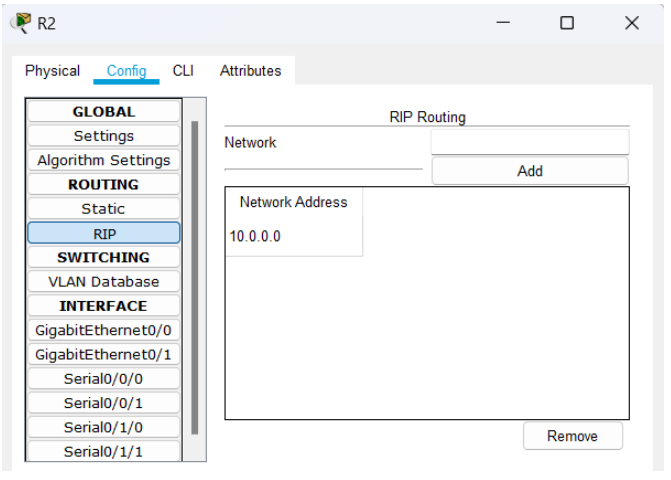


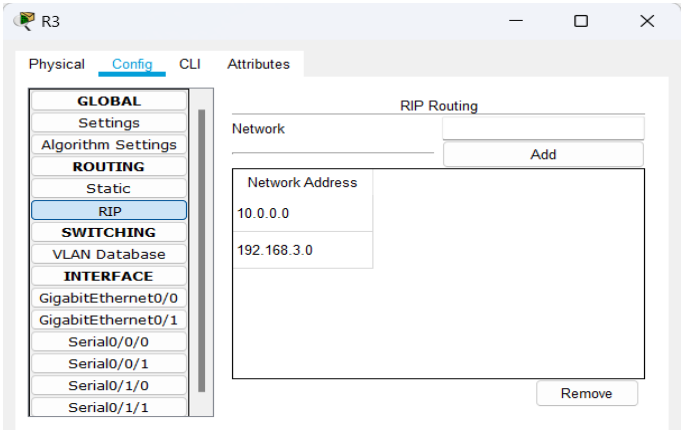




RIP Configuration :-







```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 192.168.1.50
R1(config)#ntp update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show clock
*0:4:26.775 UTC Mon Mar 1 1993
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp update-calendar
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show clock
13:31:0.711 UTC Wed Mar 8 2023
R1#service timestamp log datetime msec
          ^
% Invalid input detected at '^' marker.

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.50
R1(config)#exit
R1#
*Mar 08, 13:41:17.4141: SYS-5-CONFIG_I: Configured from console by console
*Mar 08, 13:41:17.4141:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port 514 started - CLI initiated
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...


R1(config)#
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip ips iosips out
R1(config-if)#
*Mar 08, 13:49:41.4949:  %IPS-6-ENGINE_BUILDS_STARTED:  13:49:41 UTC Mar 08 2023
*Mar 08, 13:49:41.4949:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Mar 08, 13:49:41.4949:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Mar 08, 13:49:41.4949:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
R1(config-if)#ip ips signature-definition
R1(config-sigdef)#signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#exit
R1(config-sigdef-sig)#engine
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(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 ms

R1(config)#
*Mar 08, 13:57:50.5757:  %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [192.168.3.2 -> 192.168.1.2:0] RiskRating:25
*Mar 08, 13:58:33.5858:  %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [192.168.3.2 -> 192.168.1.2:0] RiskRating:25
*Mar 08, 13:59:15.5959:  %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [192.168.3.2 -> 192.168.1.2:0] RiskRating:25
*Mar 08, 13:59:22.5959:  %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [192.168.3.2 -> 192.168.1.2:0] RiskRating:25
*Mar 08, 13:59:28.5959:  %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [192.168.3.2 -> 192.168.1.2:0] RiskRating:25
*Mar 08, 13:59:34.5959:  %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [192.168.3.2 -> 192.168.1.2:0] RiskRating:25
```

PC0

Physical Config Desktop Programming Attributes

Command Prompt

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

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

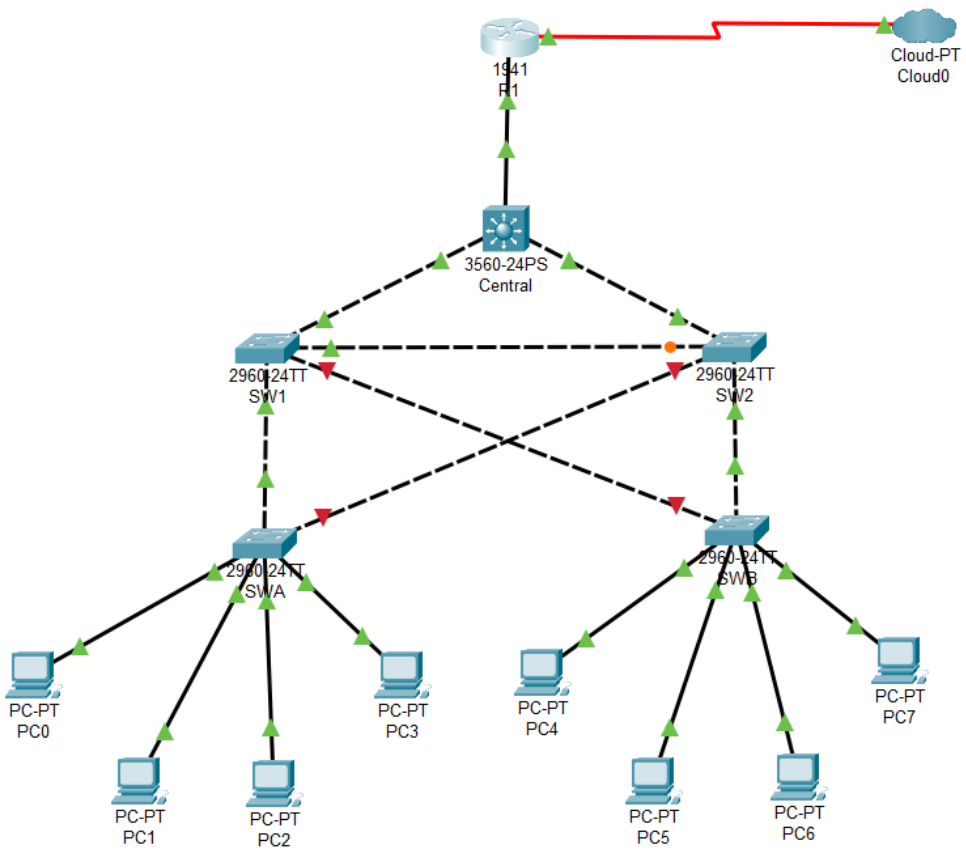
PC1

Physical Config Desktop Programming Attributes

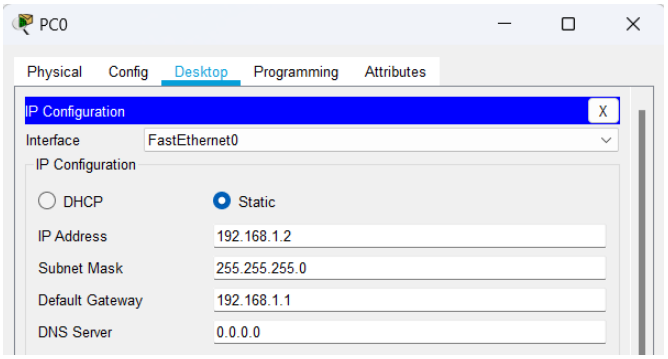
Command Prompt

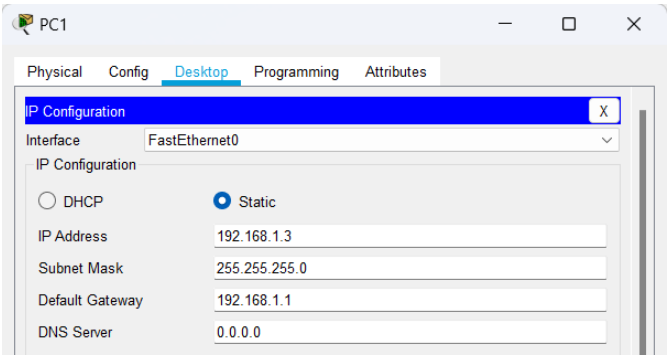
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

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

C:\>
```

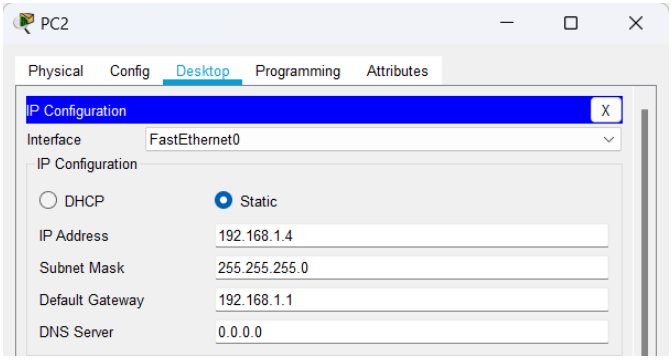
Practical – 8 Packet Tracer – Layer 2 Security

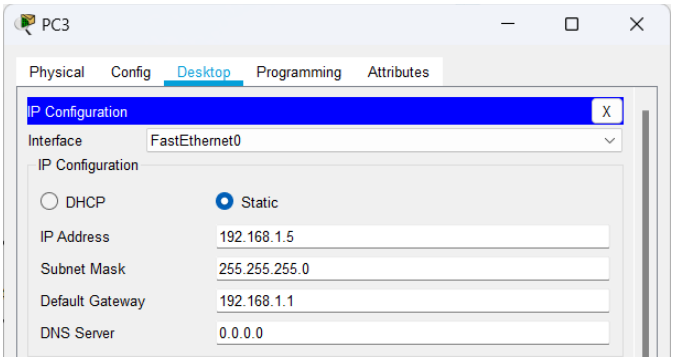


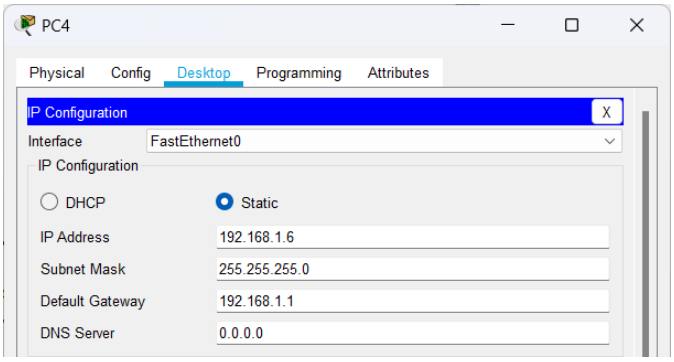
IP Configuration :-

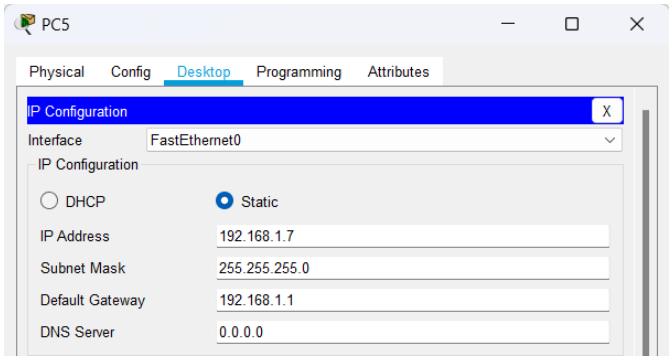


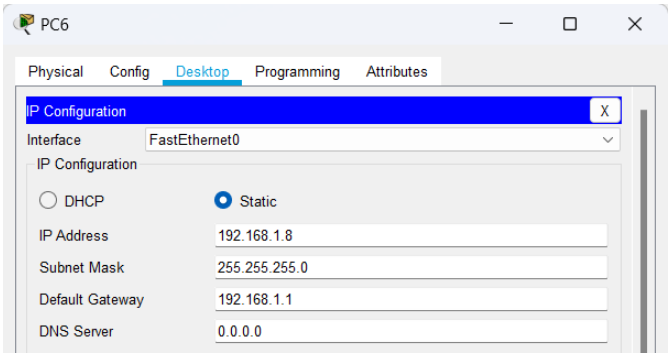


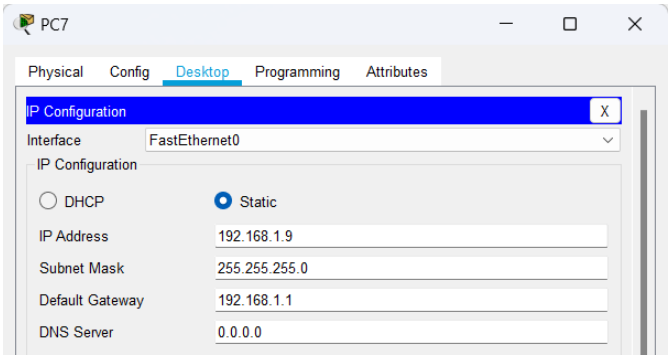




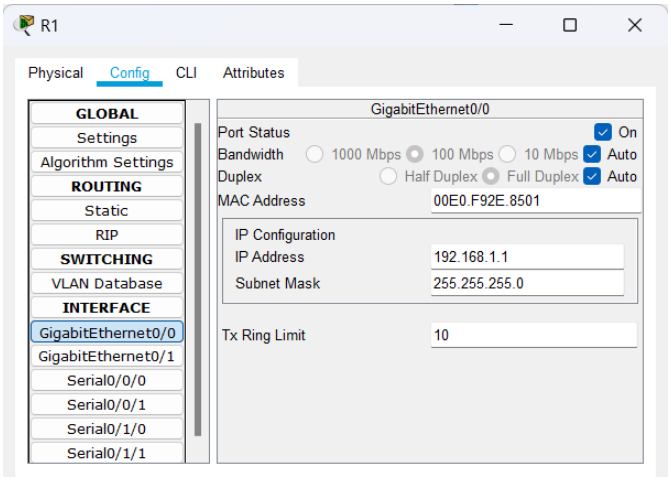


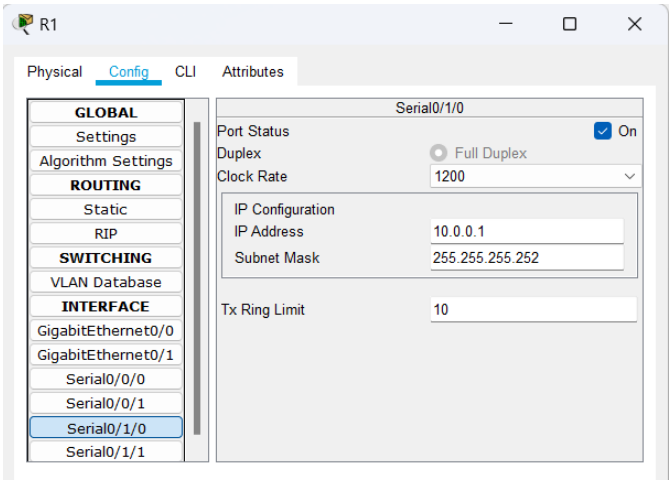




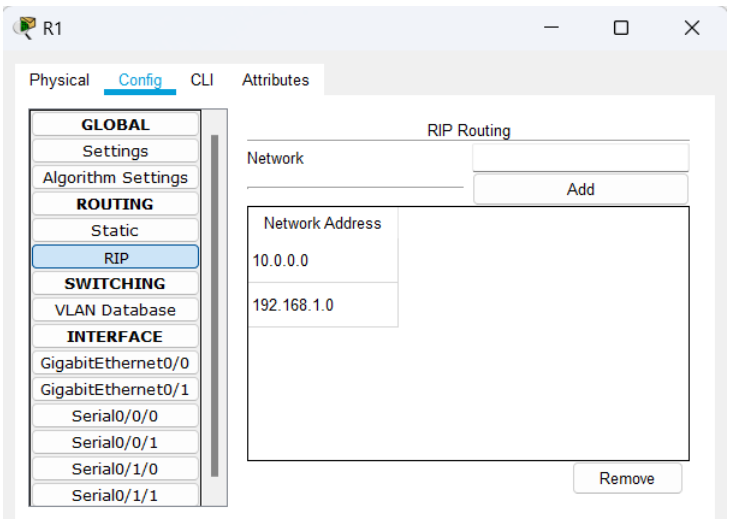


Router Configuration :-





RIP Configuration :-



Step-1 :- Configure Root Bridge.

```
Central#
%SYS-5-CONFIG_I: Configured from console by console

Central#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0001.9708.1015
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0001.9708.1015
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/2            Desg FWD 19        128.2    P2p

Central#


SW1>en
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#spanning-tree vlan 1 root secondary
SW1(config)#interface range f0/23-24
SW1(config-if-range)#spanning-tree guard root
SW1(config-if-range)#exit
SW1(config)#
%LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down

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

Step-2 :- Protect Against STP Attacks.

```
SWA>en
SWA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA(config)#interface range f0/2-5
SWA(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 FastEthernet0/2 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.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 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 FastEthernet0/4 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 FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
SWA(config-if-range)#exit
SWA(config)#interface range f0/2-5
SWA(config-if-range)#spanning-tree bpduguard enable
SWA(config-if-range)#exit
SWA(config)#interface range f0/1-22
SWA(config-if-range)#switchport mode access
SWA(config-if-range)#switchport port-security
SWA(config-if-range)#switchport port-security maximum 2
SWA(config-if-range)#switchport port-security violation shutdown
SWA(config-if-range)#switchport port-security mac-address sticky
SWA(config-if-range)#exit
SWA(config)#exit
SWA#
%SYS-5-CONFIG_I: Configured from console by console

SWA#show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
```

Step-3 :- Configure port security and disable unused ports.

- Verify port security.
- Disable unused port.

```
SWA#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        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0001.4355.D202:1
Security Violation Count   : 0

SWA#interface range f0/6-22
             ^
% Invalid input detected at '^' marker.

SWA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA(config)#interface range f0/6-22
SWA(config-if-range)#shutdown


%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down


%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
SWA(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

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

```
SWB>en
SWB#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWB(config)#interface range f0/2-5
SWB(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 FastEthernet0/2 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.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 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 FastEthernet0/4 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 FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
SWB(config-if-range)#exit
SWB(config)#interface range f0/2-5
SWB(config-if-range)#spanning-tree bpduguard enable
SWB(config-if-range)#exit
SWB(config)#interface range f0/1-22
SWB(config-if-range)#switchport mode access
SWB(config-if-range)#switchport port-security
SWB(config-if-range)#switchport port-security maximum 2
SWB(config-if-range)#switchport port-security violation shutdown
SWB(config-if-range)#switchport port-security mac-address sticky
SWB(config-if-range)#exit
SWB(config)#exit
SWB#
```