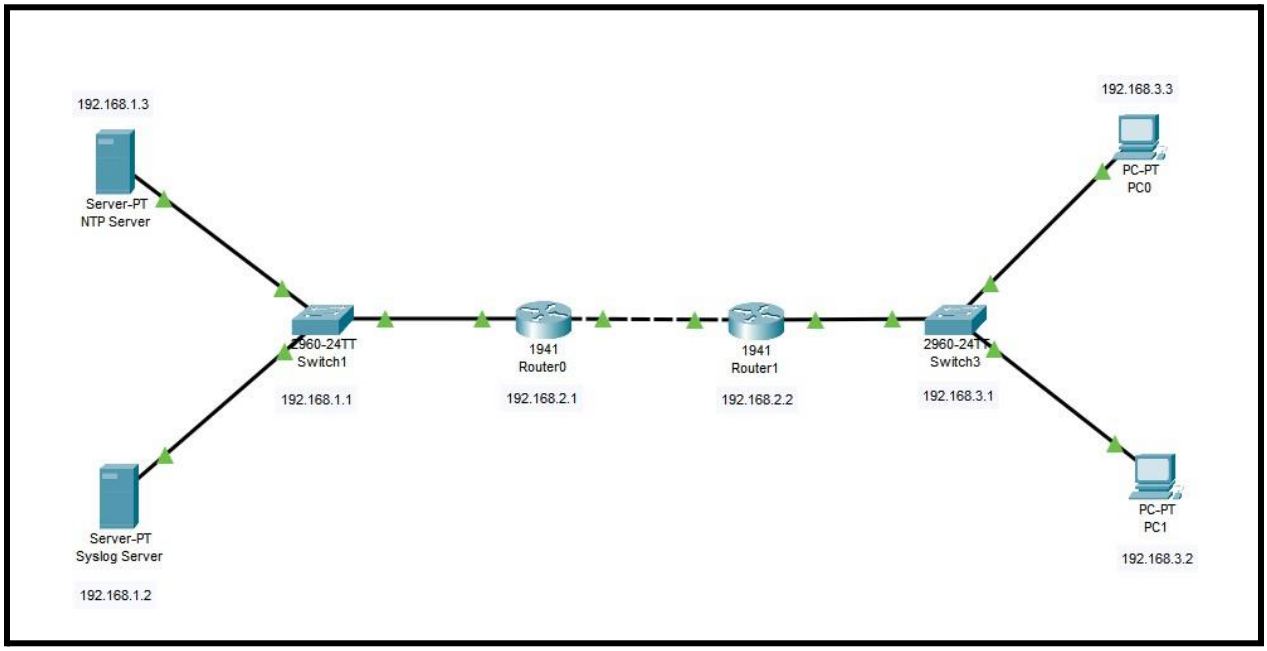
Practical 1

Configure Routers

a. OSPF MD5 authentication.
b. NTP.
c. To log messages to the syslog server.
d. To support SSH connections.

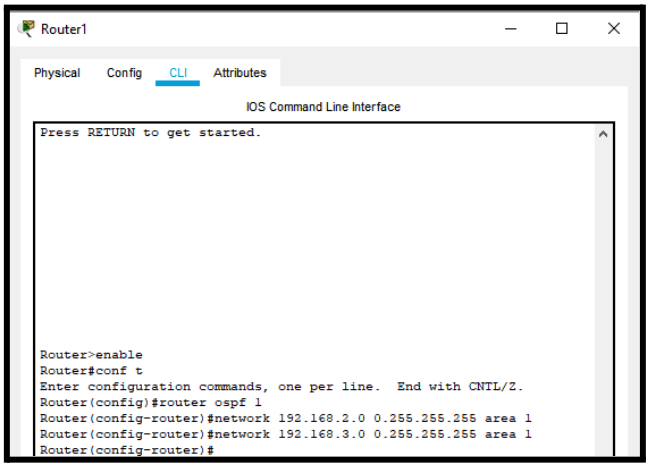


a. OSPF MD5 authentication.

- ☐ **OSPF - FINDING THE SHORTEST PATH**
- ☐ **ALGO – DIJKSTRA**
- ☐ **TOPOLOGY & DEVICE CONFIGURE**

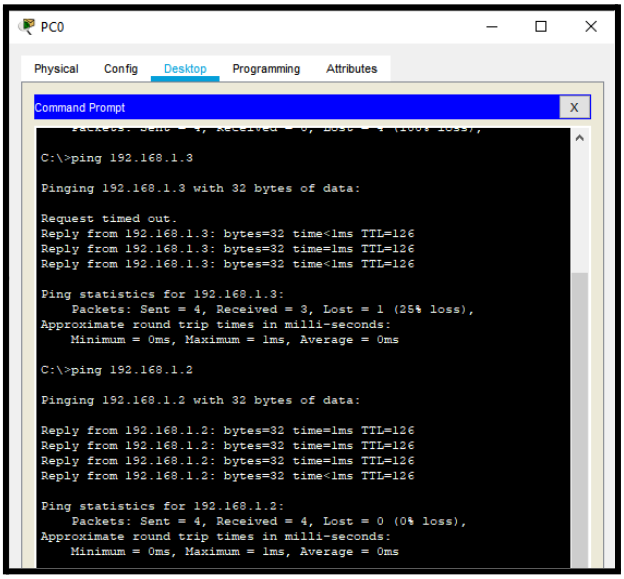
TO CONFIGURE OSPF
ON BOTH ROUTER -> CLI

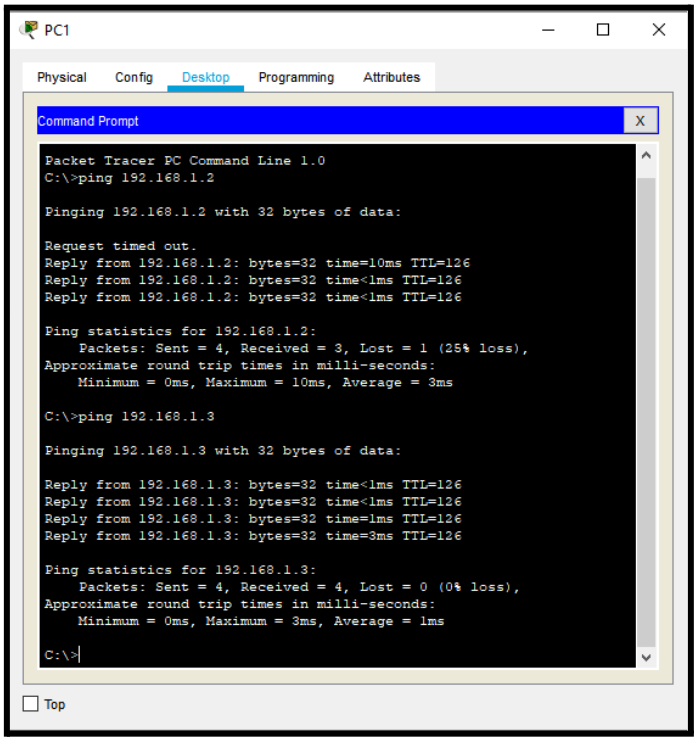
1) **exit**
2) **enable**
3) **conf t (Configure Terminal)**
4) **router ospf 1**
5) **network 192.168.1.0 0.255.255.255 area 1**
6) **network 192.168.2.0 0.255.255.255 area 1**
7) **exit**
8) **exit**



ON PC -> CMD

> ping server ip address

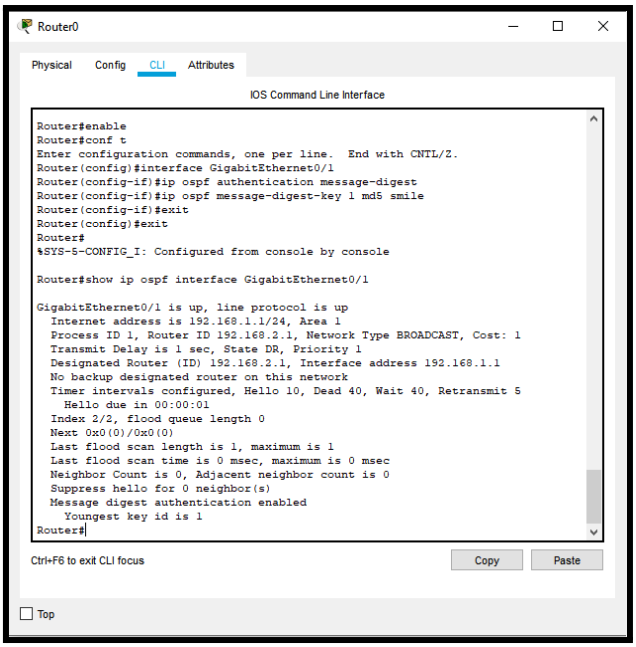


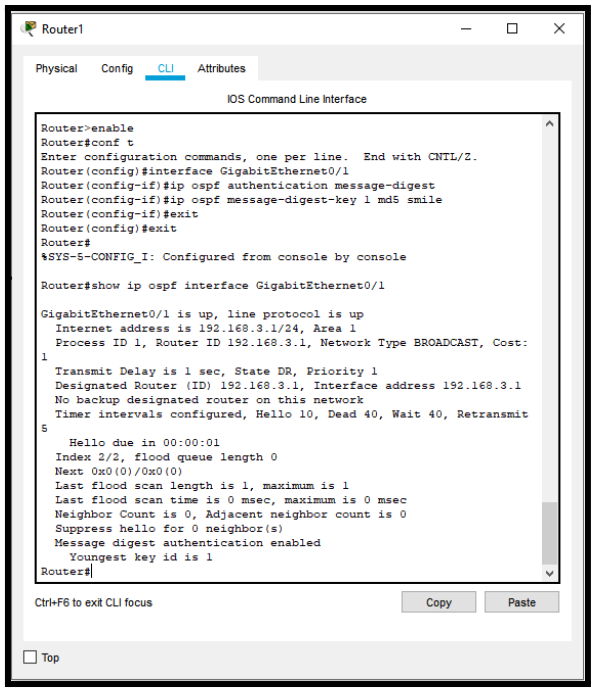


MD5 (For both the routers)

ROUTER -> CLI

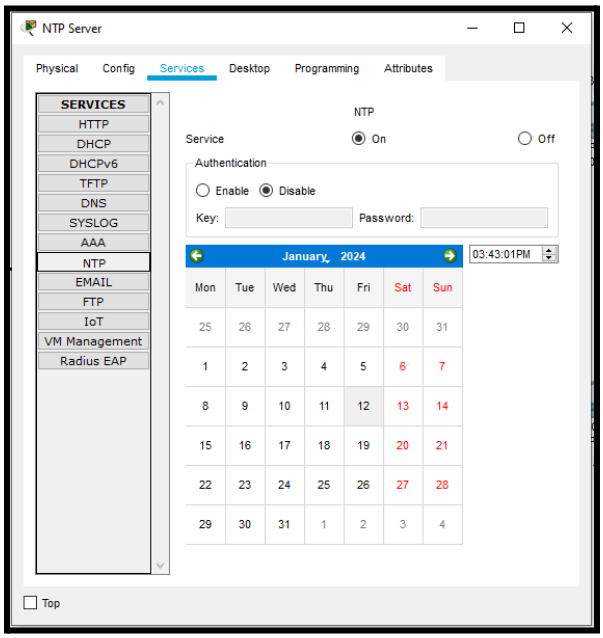
1) **enable**
2) **conf t**
3) **interface GigabitEthernet0/1**
4) **ip ospf authentication message-digest**
5) **ip ospf message-digest-key 1 md5 smile**
6) **exit**
7) **show ip ospf interface GigabitEthernet0/1**





b. NTP.

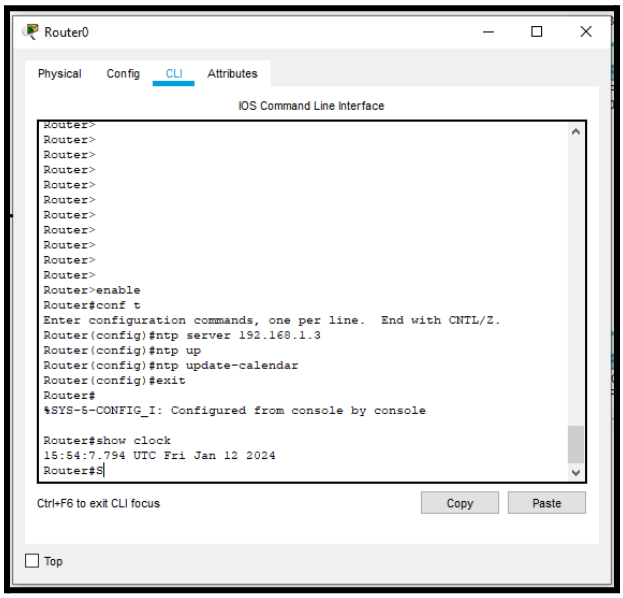
- ☐ **NTP -: Synchronization**

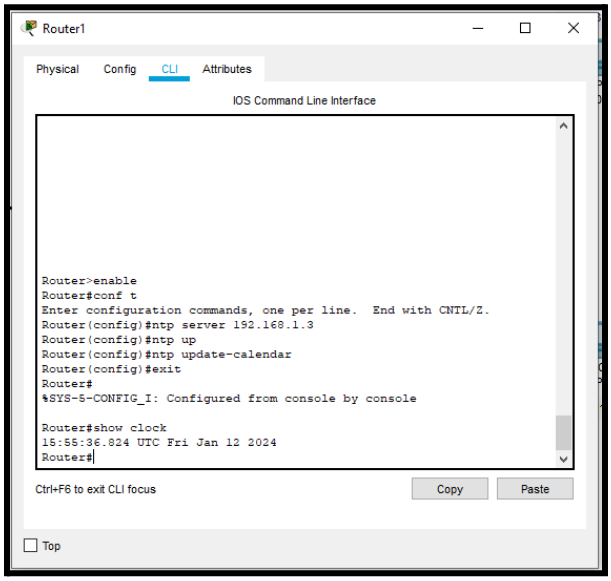


NTP (For both the routers)

1) **enable**
2) **conf t**
3) **ntp server 192.168.1.3**

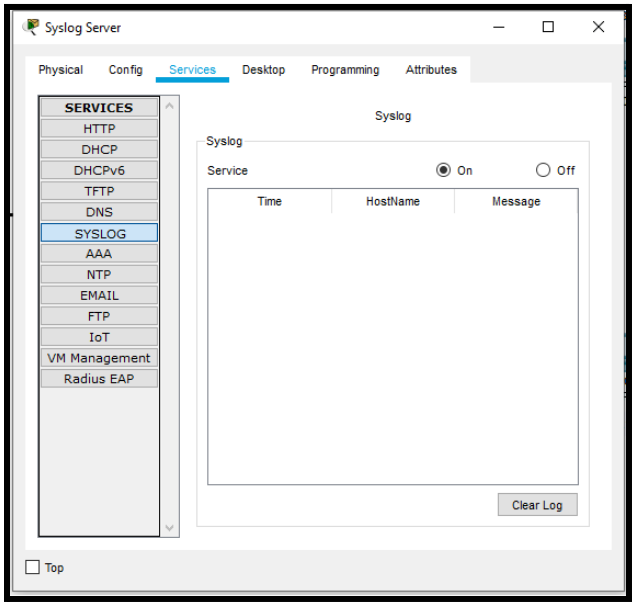
4) **ntp up (Services up)**
5) **ntp update-calendar**
6) **exit**
7) **show clock**





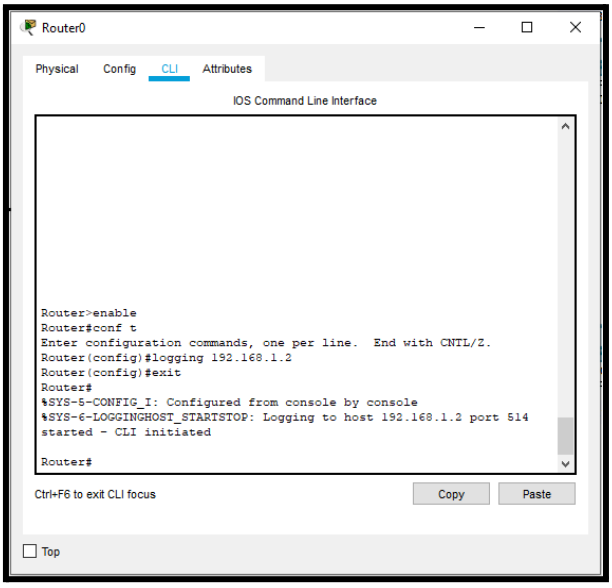
c. To log messages to the syslog server.

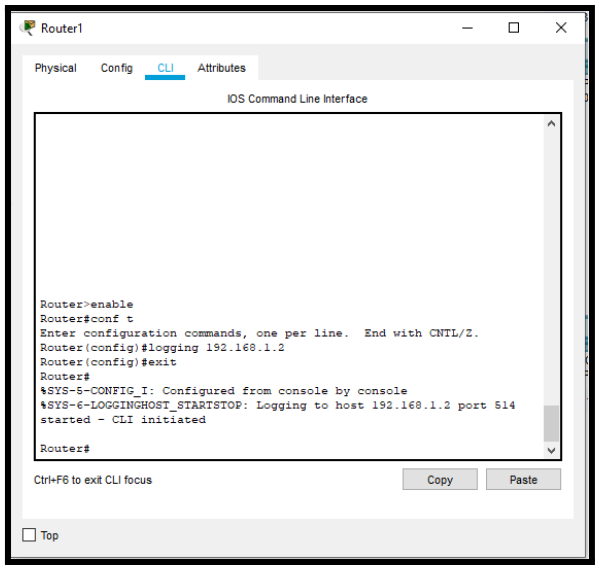
- ☐ **Syslog -: Service which provides logging server. Place the log files**
- ☐ **Maintain the log of data transfer**



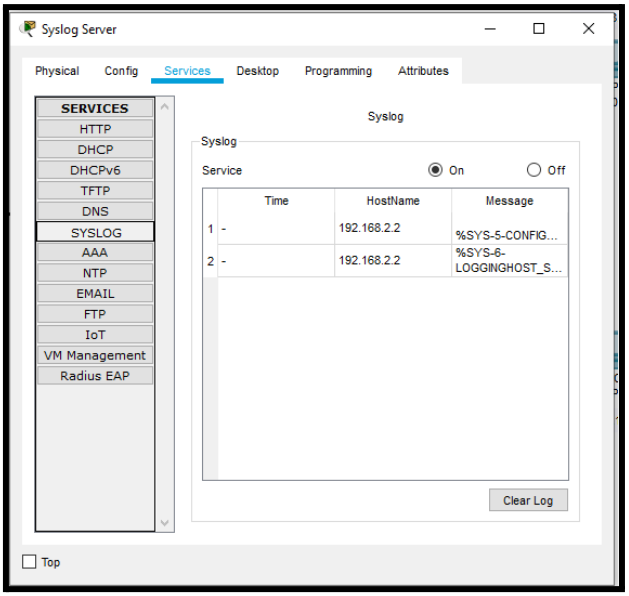
Syslog(For both the routers)

1) **enable**
2) **conf t**
3) **logging 192.168.1.2**
4) **exit**





Server -> Check



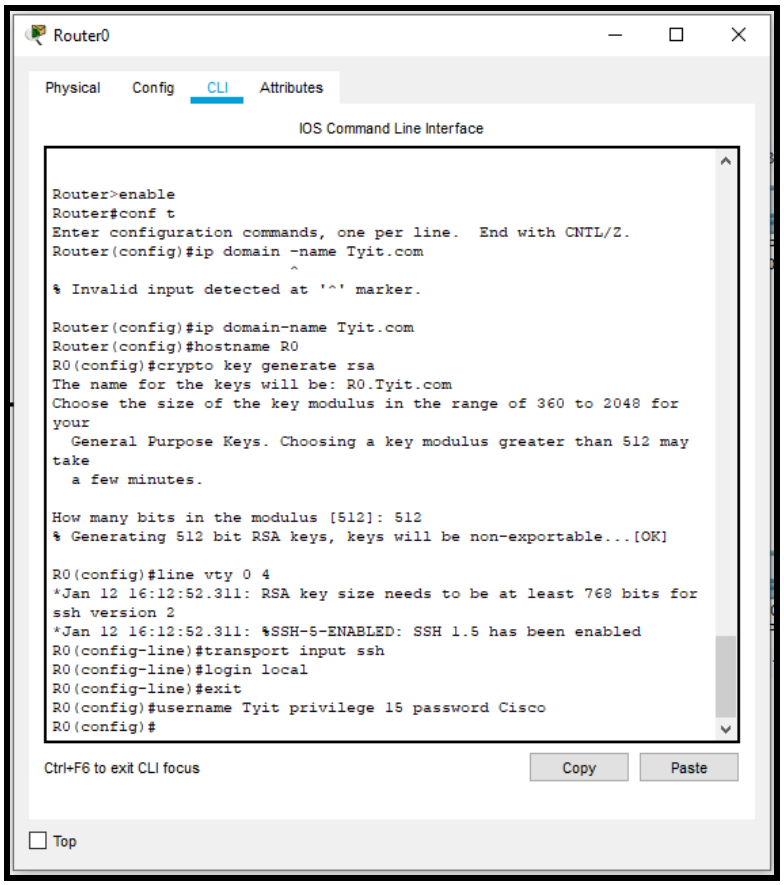
d. To support SSH connections.

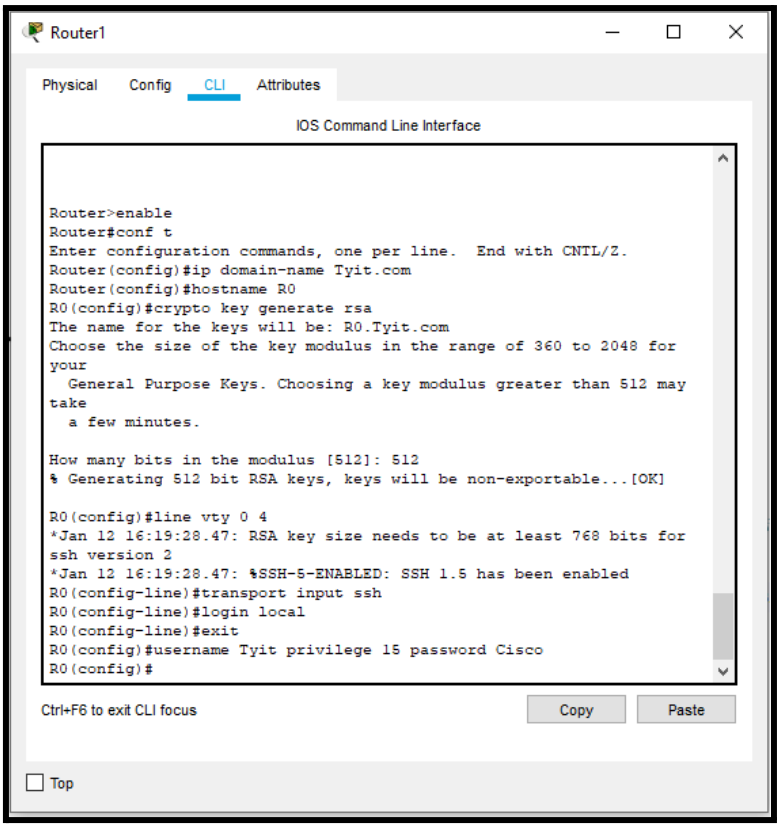
SSH -: Secure Shell

Login ID & Password

SSH(For both the routers)

1) **enable**
2) **conf t**
3) **ip domain -name Tyit.com**
4) **hostname R0**
5) **crypto key generate rsa (rsa – algo)**
   Enter key size: 512 (minimum)
6) **line vty 0 4**
7) **transport input ssh**
8) **login local**
9) **exit**
10) **username Tyit privilege 15 password Cisco**

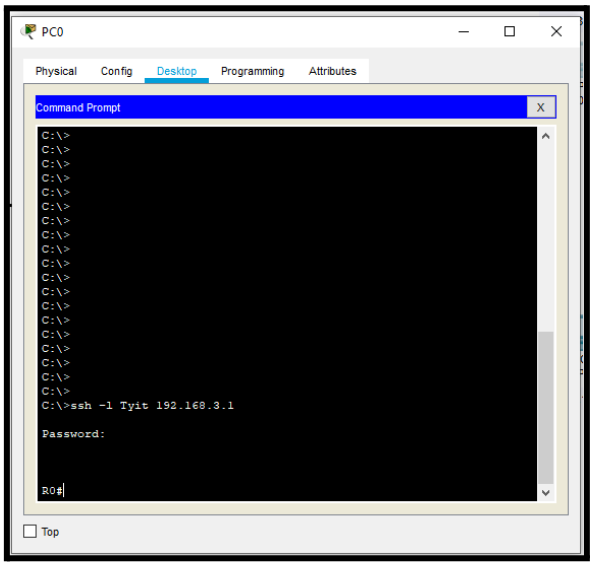


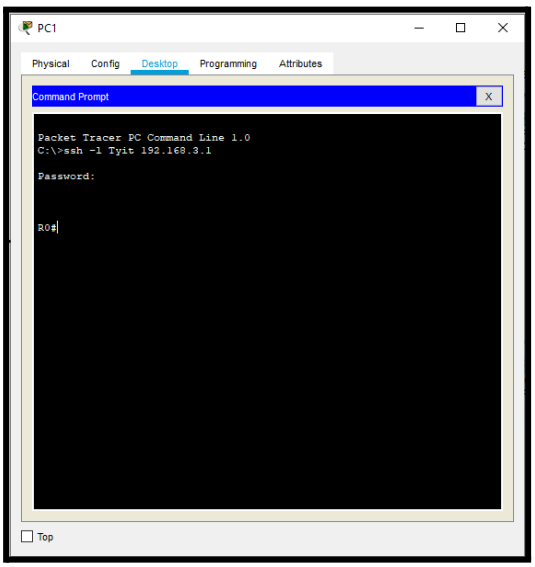


On PC -> CMD

> ssh -l Tyit 192.168.3.1

Enter password: Cisco





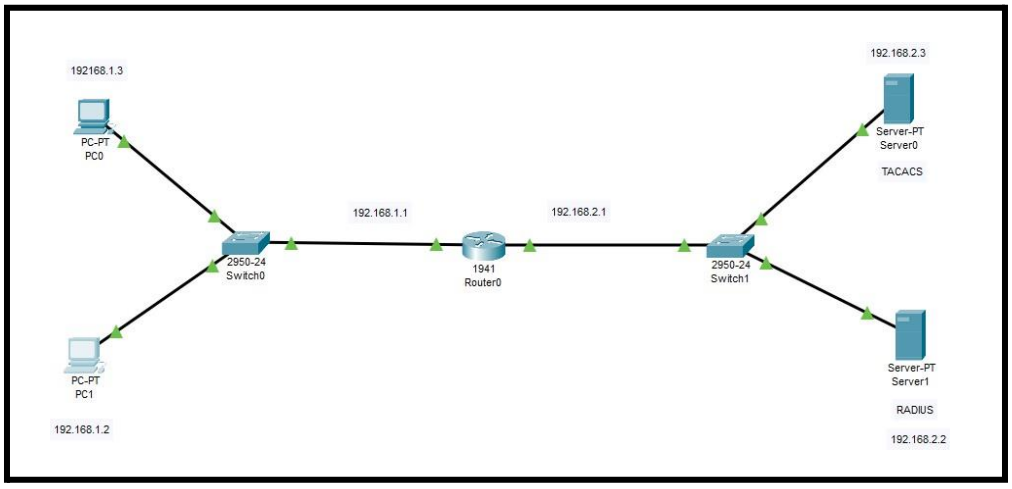
Practical 2

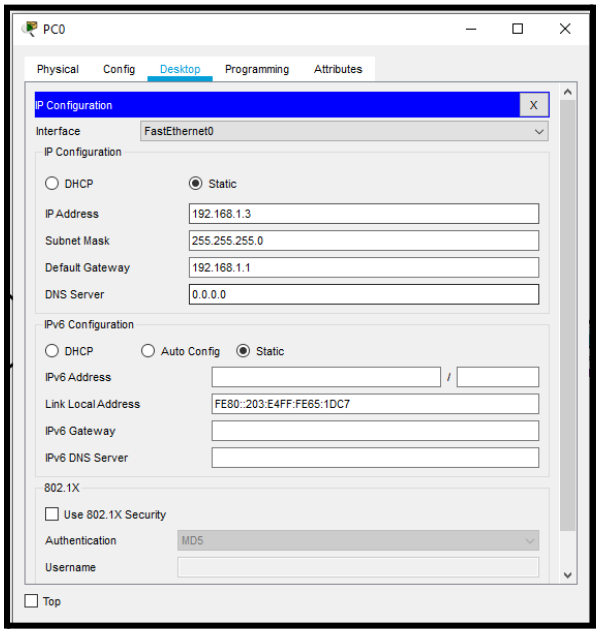
Configure AAA Authentication

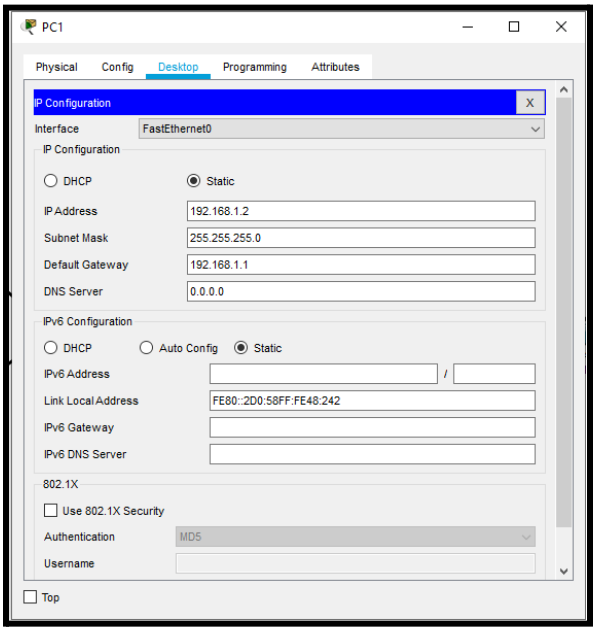
a. Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA

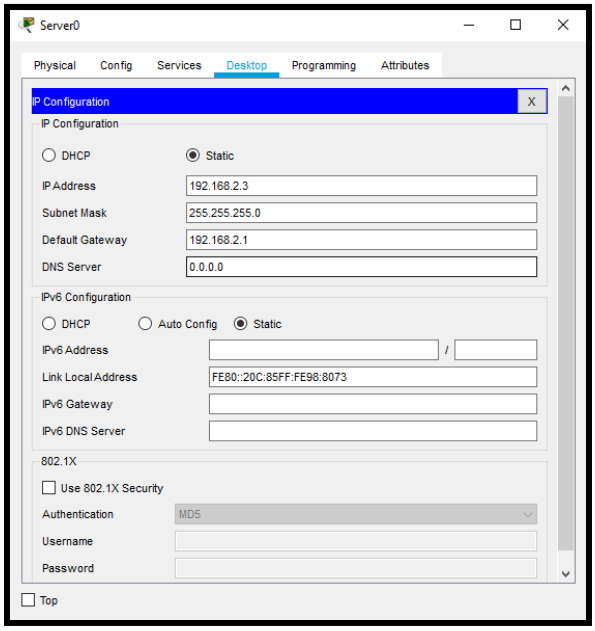
b. Verify local AAA authentication from the Router console and the PC-A client

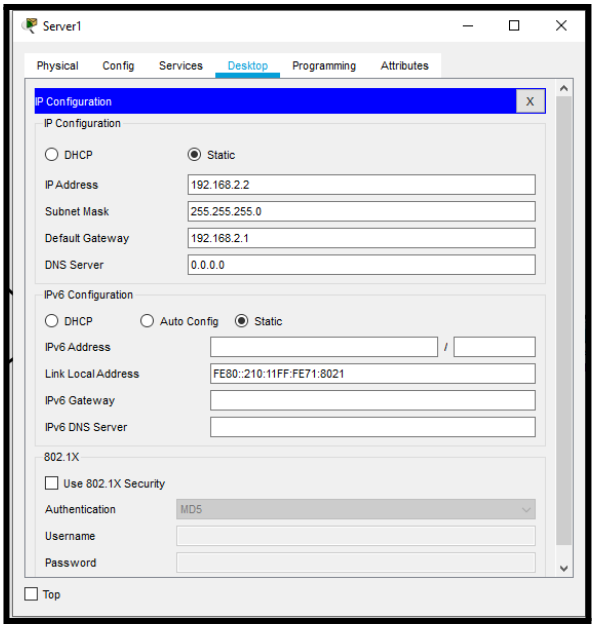
- ☐ **AAA - AUTHENTICATION, AUTHORIZATION, ACCOUNTING**
- ☐ **TERMINAL ACCESS CONTROL ACCESS CONTROL SERVICES (TACACS) – PROPRIETARY PROTOCOL, USES TCP, 49 PORT NO, AAA**
- ☐ **RADIUS - OPEN, USES UDP, AA**

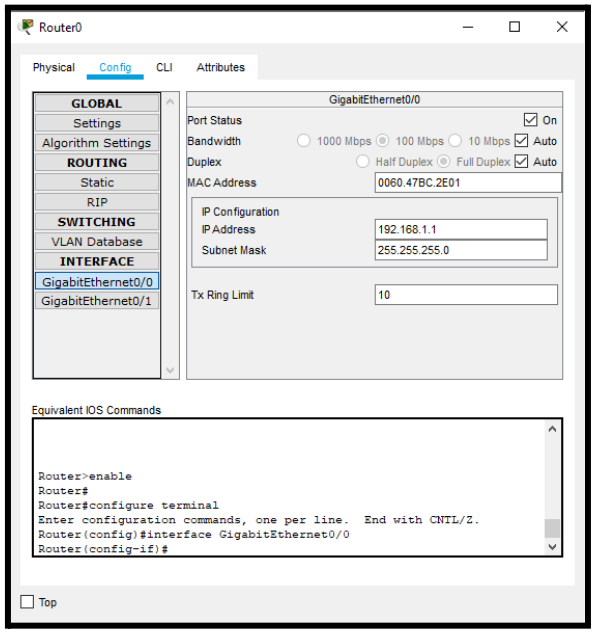


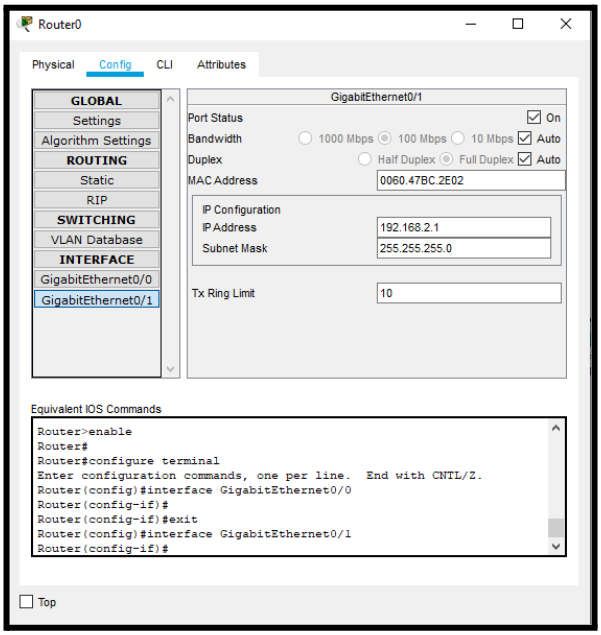


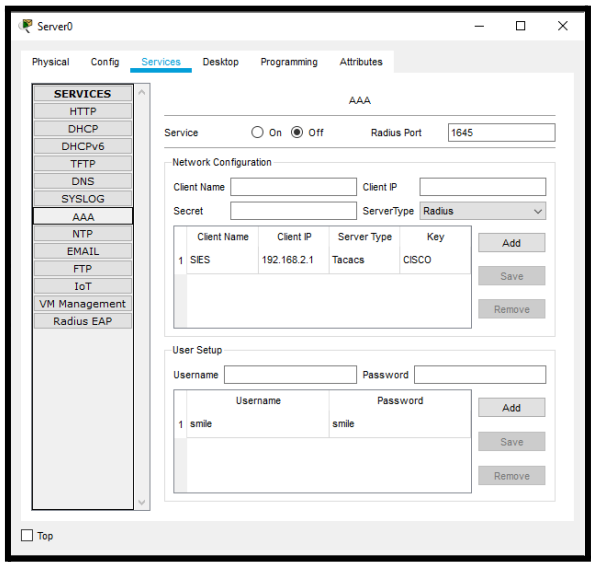


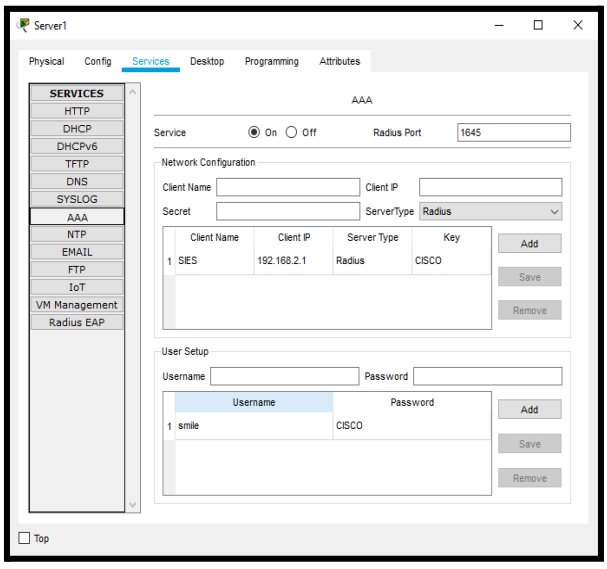

Server0
Physical Config Services Desktop Programming Attributes
IP Configuration
IP Configuration
DHCP Static
IP Address 192.168.2.3
Subnet Mask 255.255.255.0
Default Gateway 192.168.2.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::20C:85FF:FE98:8073
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top


Server1
Physical Config Services Desktop Programming Attributes
IP Configuration
IP Configuration
DHCP Static
IP Address 192.168.2.2
Subnet Mask 255.255.255.0
Default Gateway 192.168.2.1
DNS Server 0.0.0.0
IPv6 Configuration
DHCP Auto Config Static
IPv6 Address
Link Local Address FE80::210:11FF:FE71:8021
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top


Router0
Physical Config CLI Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status On
Bandwidth 1000 Mbps 100 Mbps 10 Mbps Auto
Duplex Half Duplex Full Duplex Auto
MAC Address 0060.47BC.2E01
IP Configuration
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top

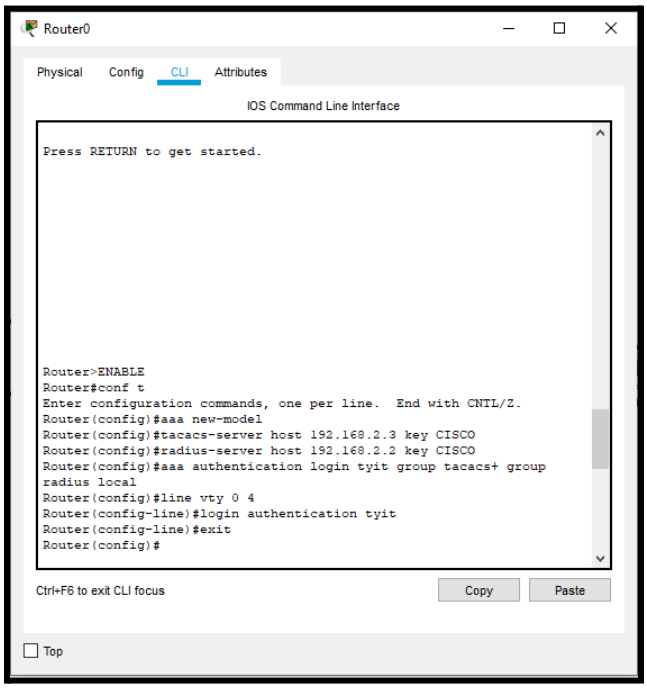

Router0
Physical Config CLI Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status On
Bandwidth 1000 Mbps 100 Mbps 10 Mbps Auto
Duplex Half Duplex Full Duplex Auto
MAC Address 0060.47BC.2E02
IP Configuration
IP Address 192.168.2.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top


Server0
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service On Off Radius Port 1645
Network Configuration
Client Name Client IP
Secret ServerType Radius
Client Name Client IP Server Type Key
1 SIES 192.168.2.1 Tacacs CISCO
Add Save Remove
User Setup
Username Password
Username Password
1 smile smile
Add Save Remove
Top


Server1
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service On Off Radius Port 1645
Network Configuration
Client Name Client IP
Secret ServerType Radius
Client Name Client IP Server Type Key
1 SIES 192.168.2.1 Radius CISCO
Add Save Remove
User Setup
Username Password
Username Password
1 smile CISCO
Add Save Remove
Top

On Router -> cmd

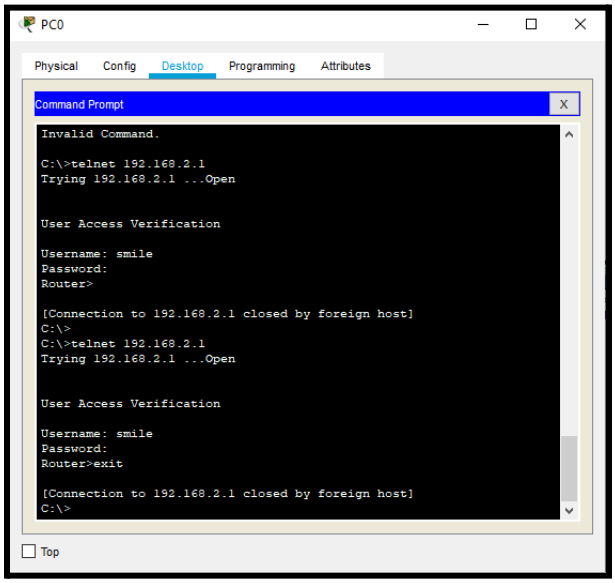
1) **enable**
2) **conf t**
3) **aaa new-model**
4) **tacacs-server host 192.168.2.3 key CISCO**
5) **radius-server host 192.168.2.2 key CISCO**
6) **aaa authentication login tyit group tacacs+ group radius local**
7) **line vty 0 4**
8) **login authentication tyit**
9) **exit**

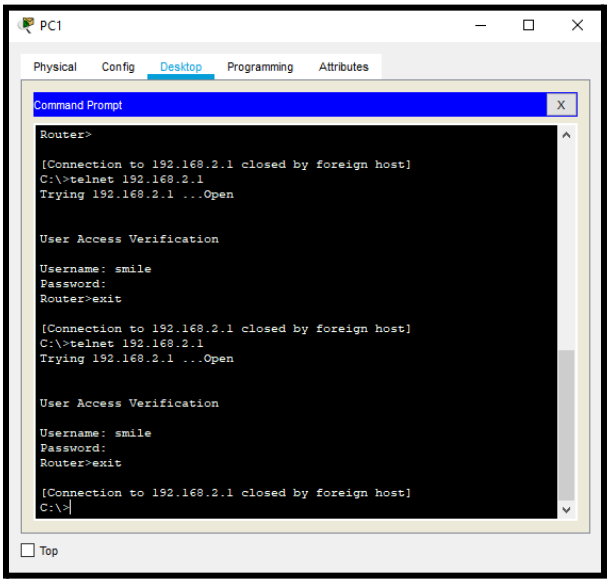


Check authentication -> PC -> cmd

> telnet 192.168.2.1 Ask for a username & password

PC0 - Tacacs (Tacacs ON, Radius OFF) PC1 - Radius (Tacacs OFF, Radius ON)



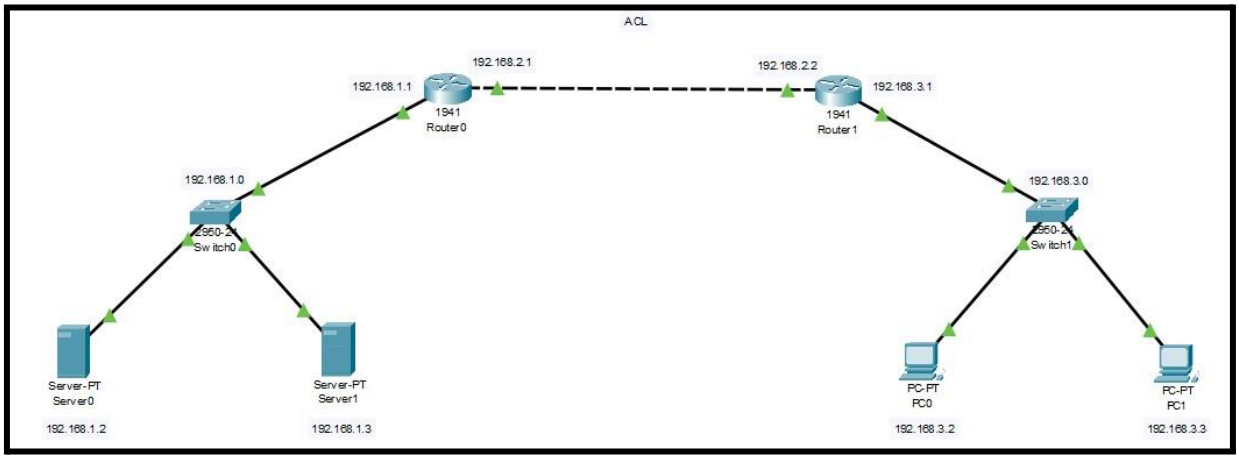


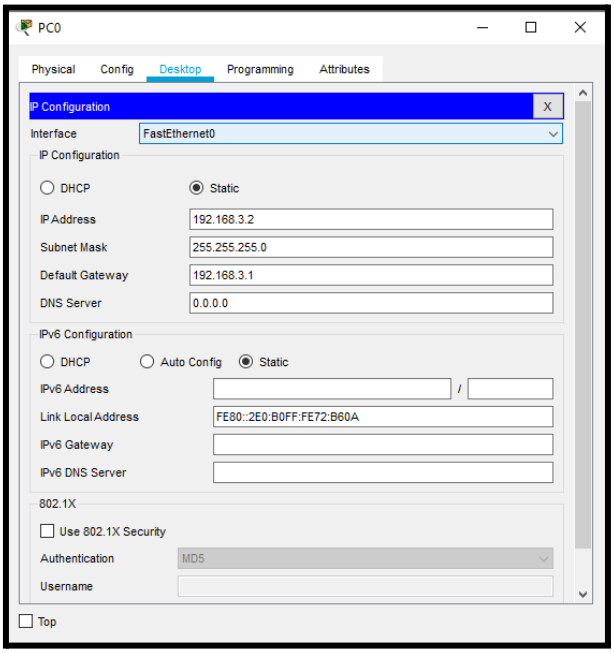
Practical 3

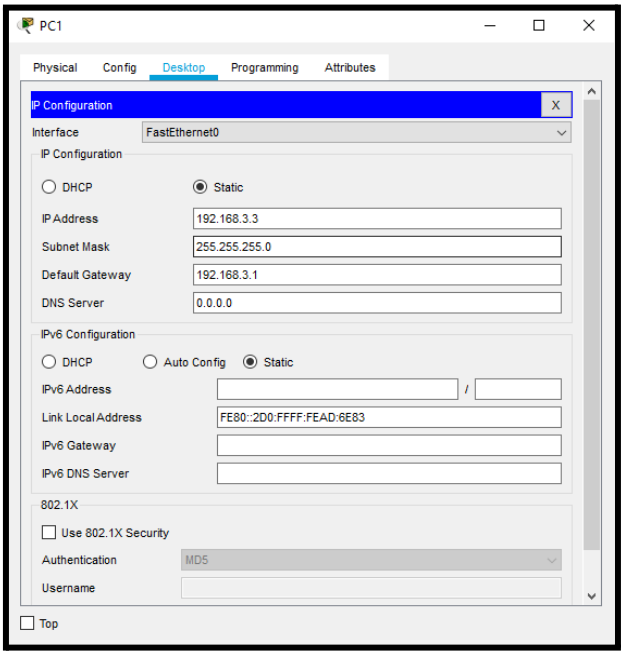
Configuring Extended ACLs

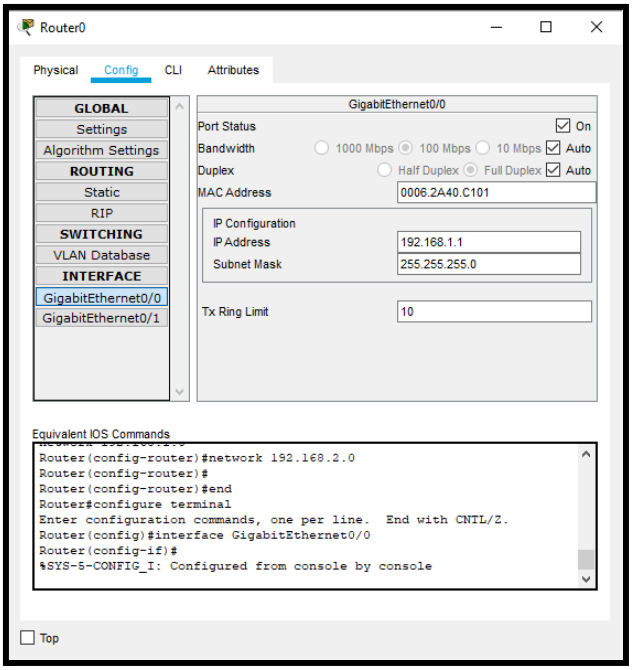
a. Configure, Apply and Verify an Extended Numbered ACL

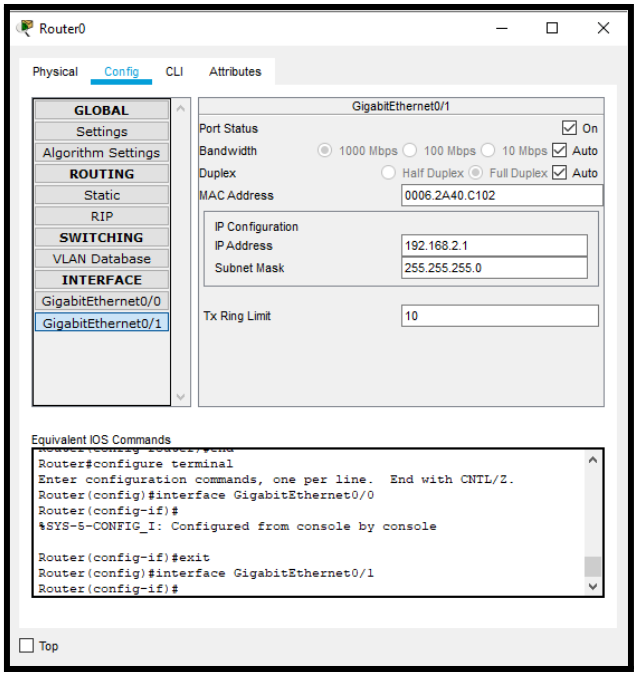
- ☐ ACL – ACCESS CONTROL LIST
- ☐ FILTRATION – FILTER THE TRAFFIC ON ROUTER / SWITCH
- ☐ STANDARD ACLS & EXTENDED ACLS
- ☐ BASIC FILTRATION (STANDARD) RANGE FROM 1-99, PERMIT OR DENY THE TRAFFIC FROM SPECIFIC ADDRESS
- ☐ EXHAUSTIVE FILTRATION (ADVANCED / EXTENDED) RANGE FROM 100 ONWARDS, FROM & TO SPECIFIC ADDRESS PERMIT & DENY

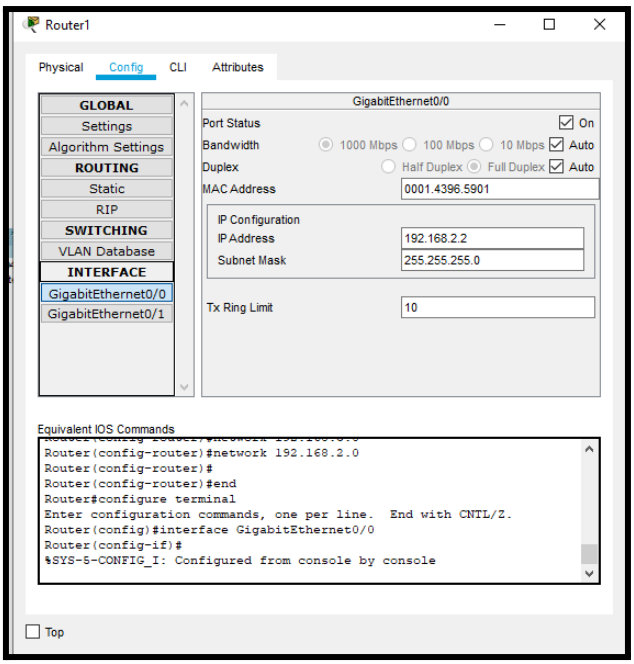


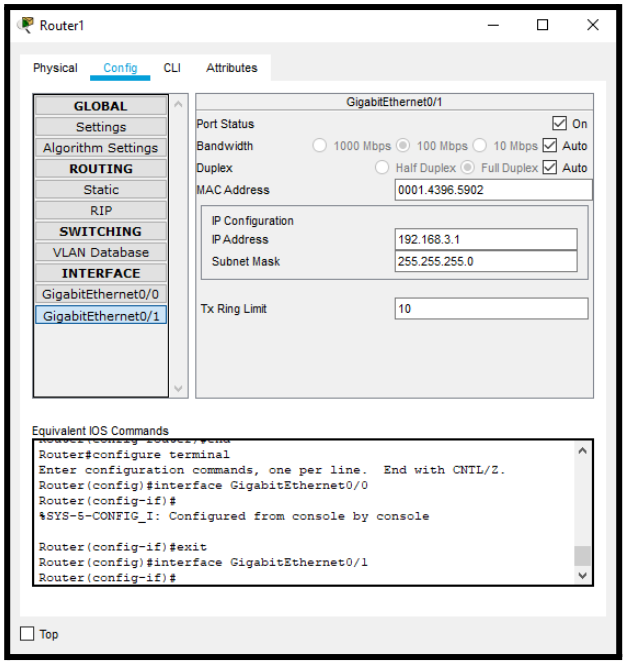


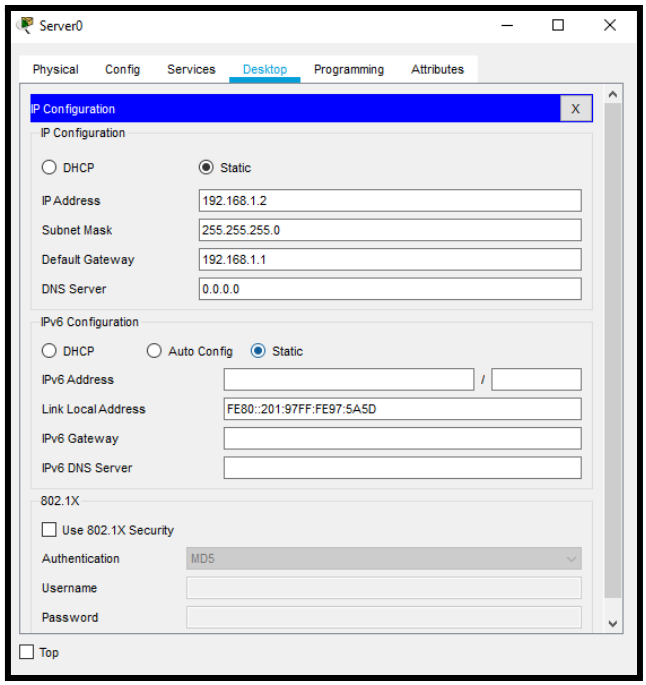


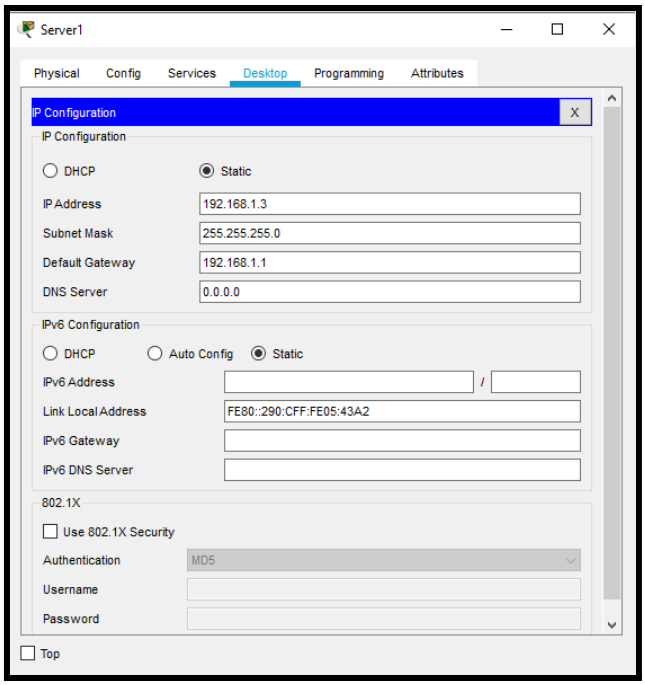

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0006.2A40.C101
IP Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-router)#network 192.168.2.0
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Top

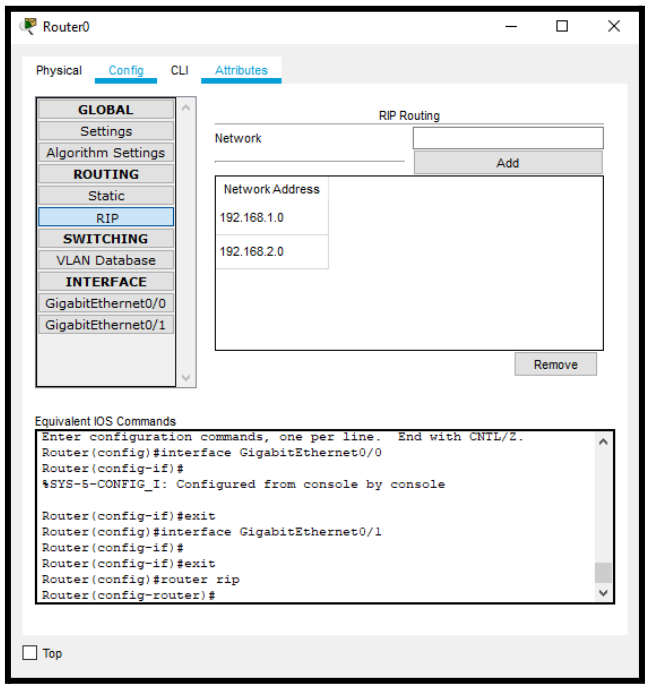

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0006.2A40.C102
IP Configuration
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top

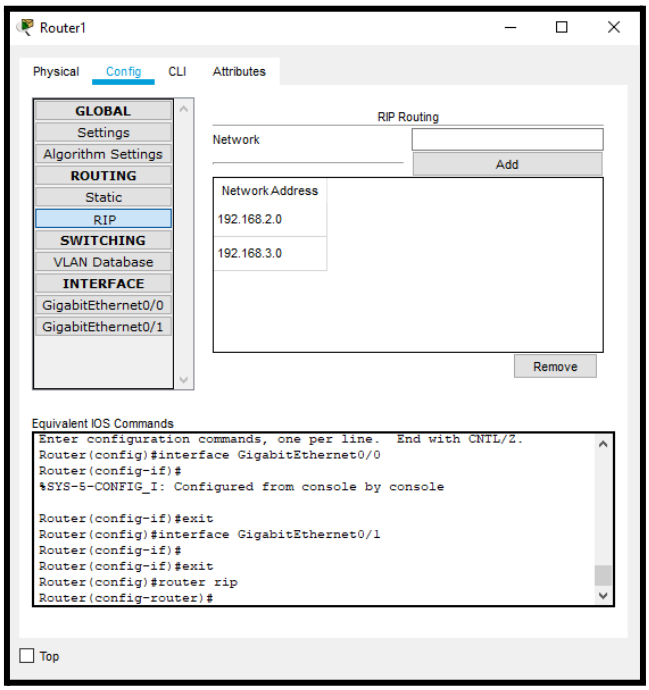

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.4396.5901
IP Configuration
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-router)#network 192.168.2.0
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Top

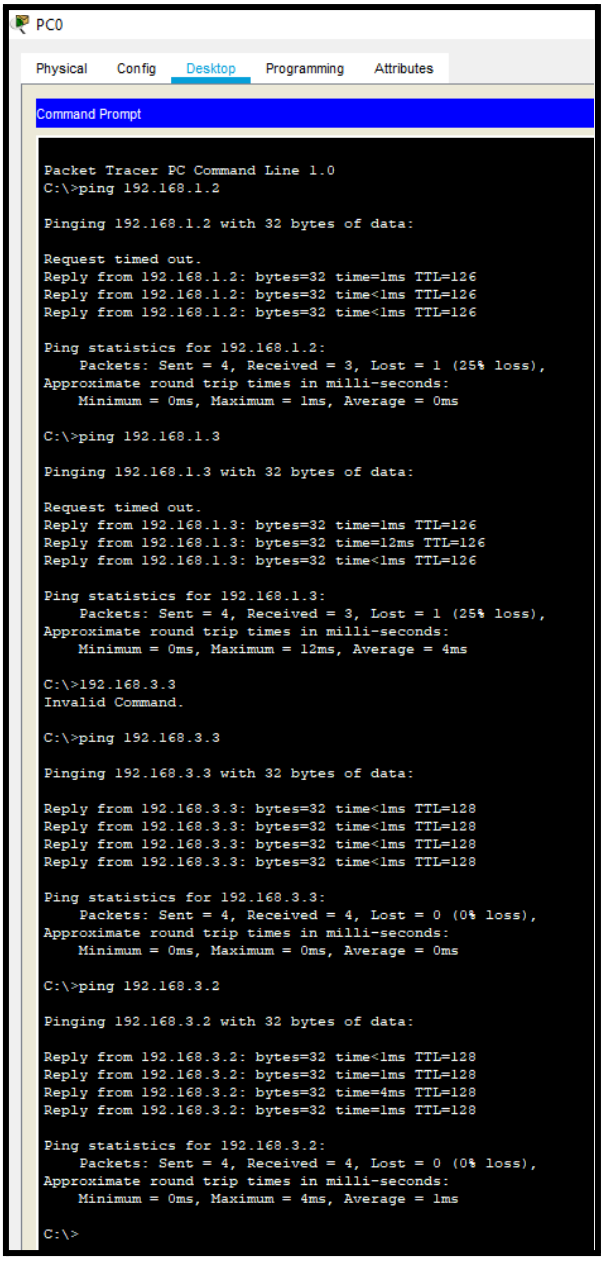

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.4396.5902
IP Configuration
IP Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top

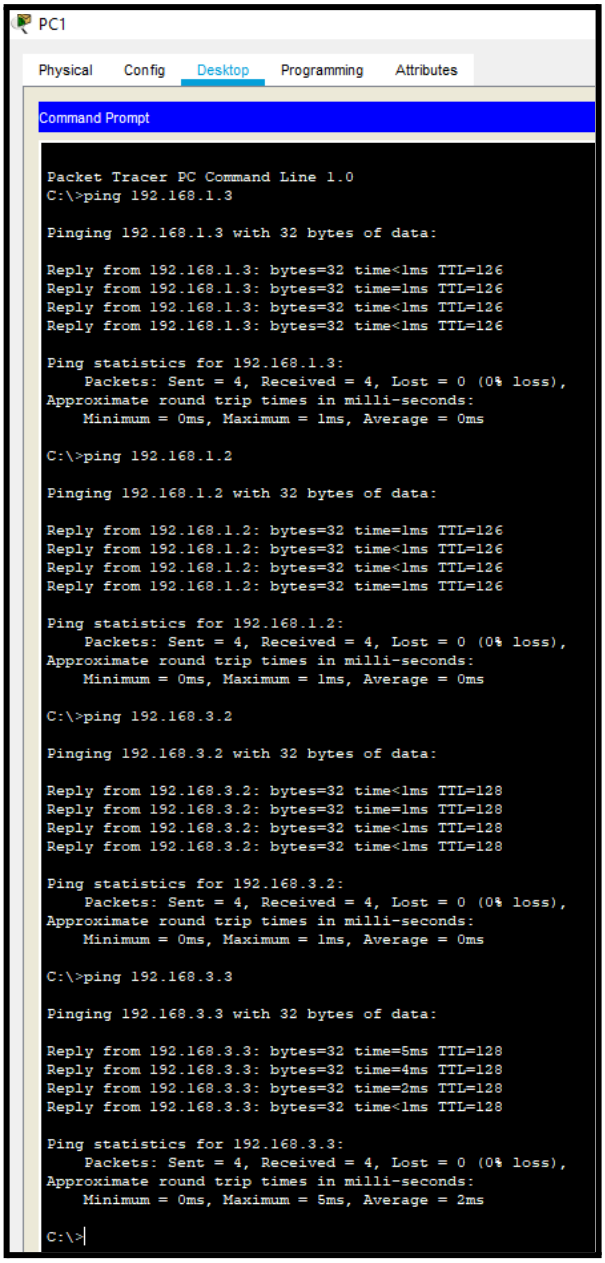

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::201:97FF:FE97:5A5D
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Server1
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::290:CFF:FE05:43A2
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
RIP Routing
Network
Add
Network Address
192.168.1.0
192.168.2.0
Remove
Equivalent IOS Commands
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
RIP Routing
Network
Add
Network Address
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#
Top





Apply and verify extended ACL

Router -> cli

1) **enable**
2) **conf t**
3) **access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq ftp**

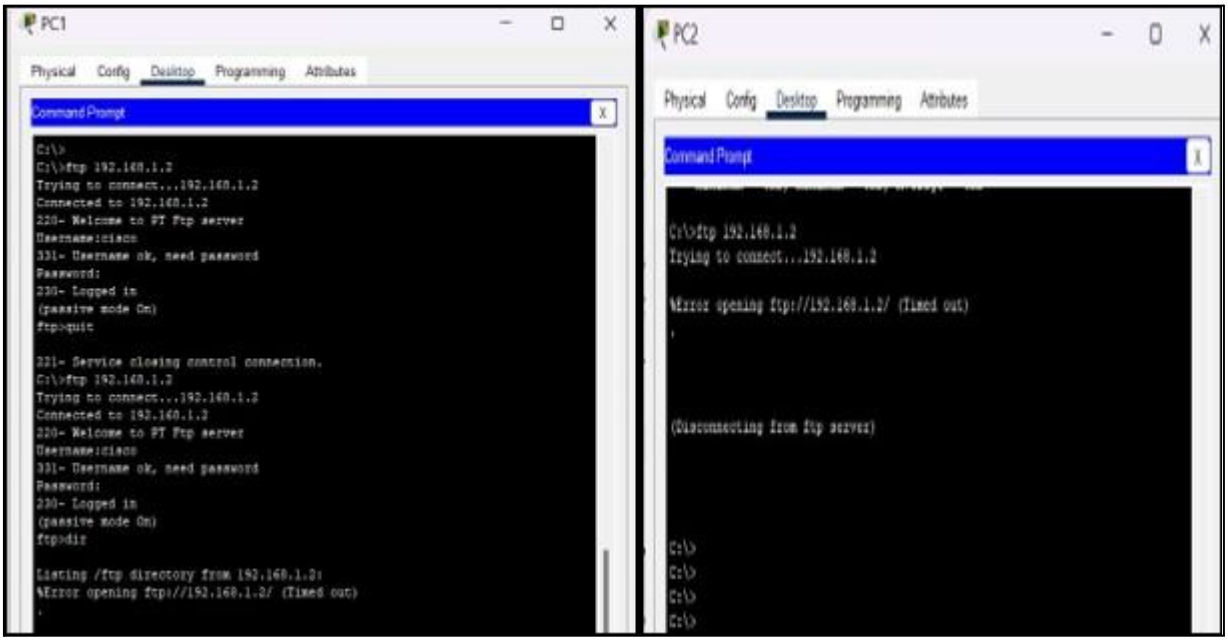
(eq - What services?)

4) **interface GigabitEthernet0/1**
5) **ip access-group 100 out**
6) **exit**

Verify

On PC0 -> cmd

1) **ftp 192.168.1.2**




PC2
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.3
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://192.168.1.3
Go
Stop

Practical 4

Configure IP ACLs to Mitigate Attacks and IPV6 ACLs

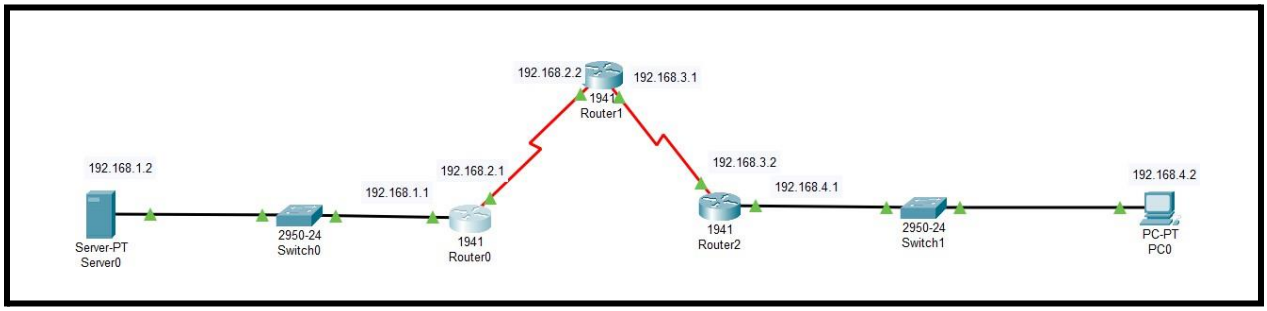
a. Verify connectivity among devices before firewall configuration.

b. Use ACLs to ensure remote access to the routers is available only from management station PC-C.

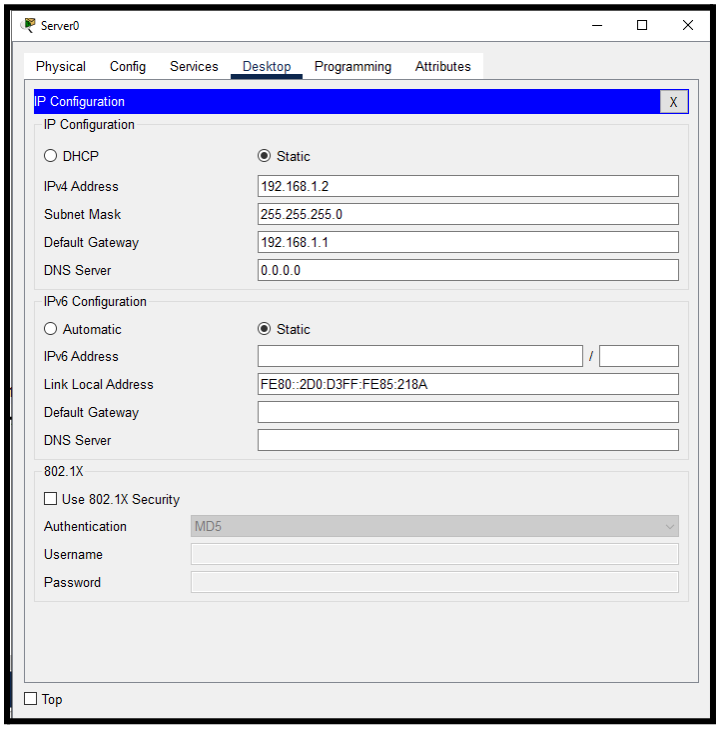
c. Configure ACLs on to mitigate attacks.

d. Configuring IPv6 ACLs

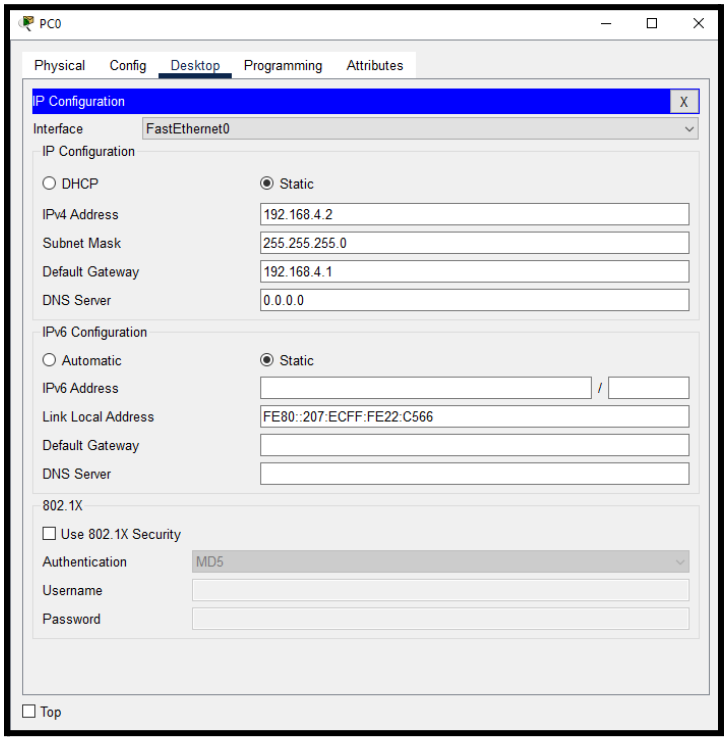
c. Configure ACLs on to mitigate attacks.



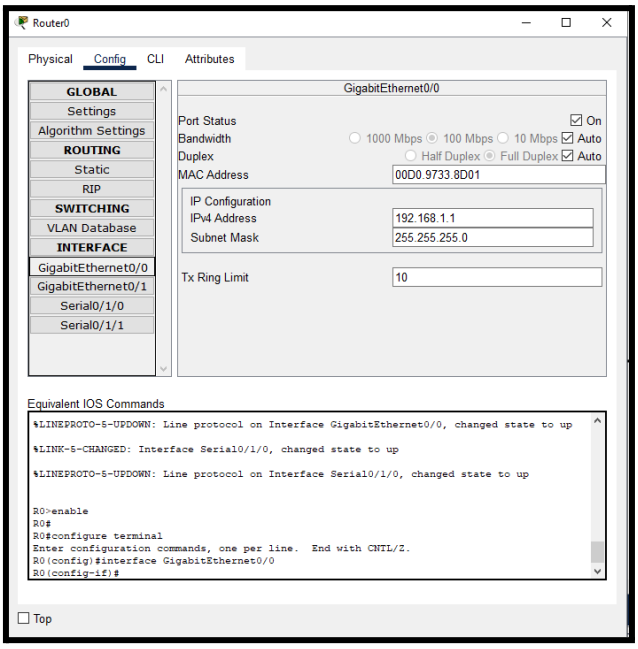
Server

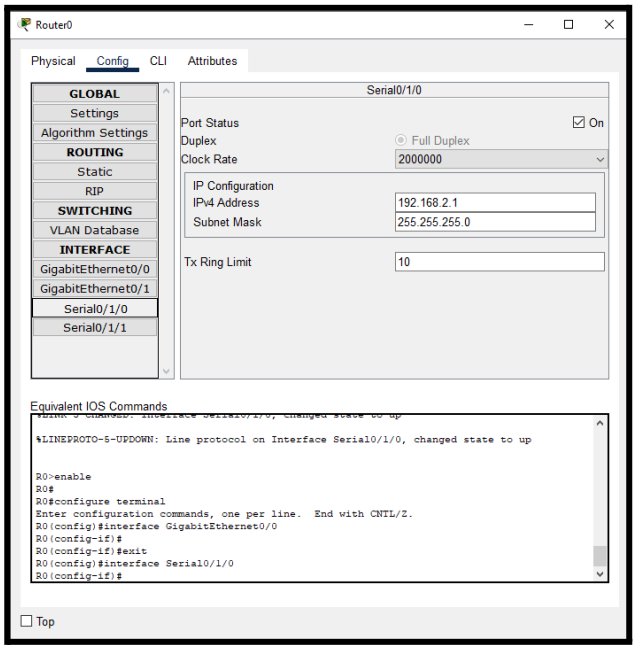


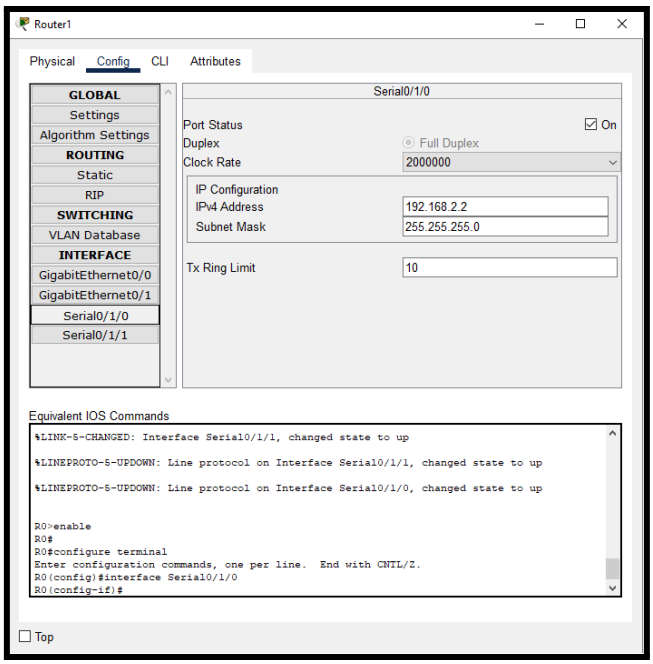
PC

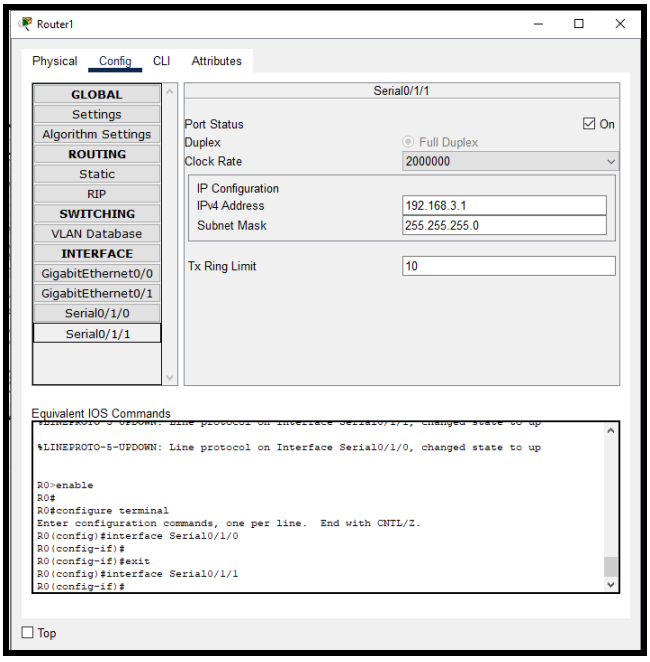


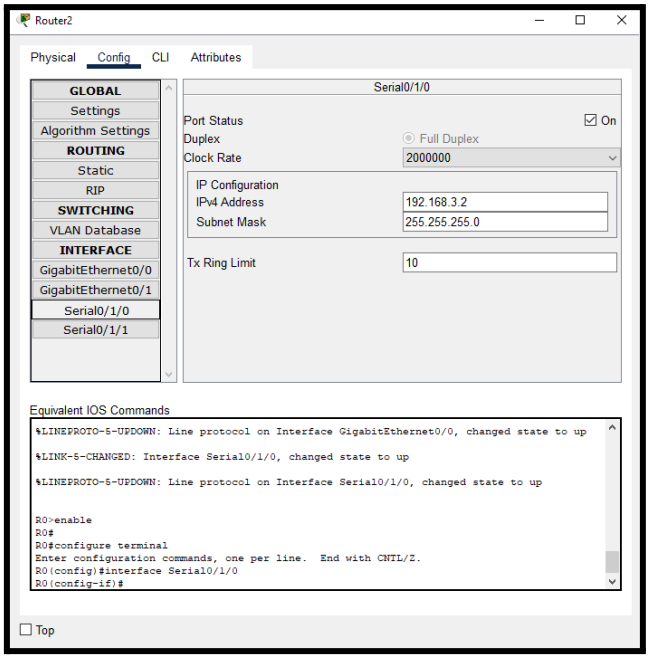
3 Routers Config

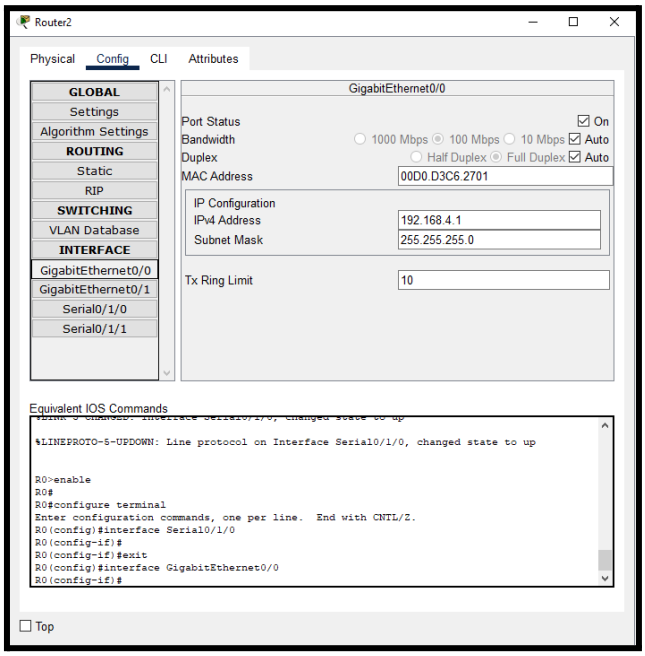




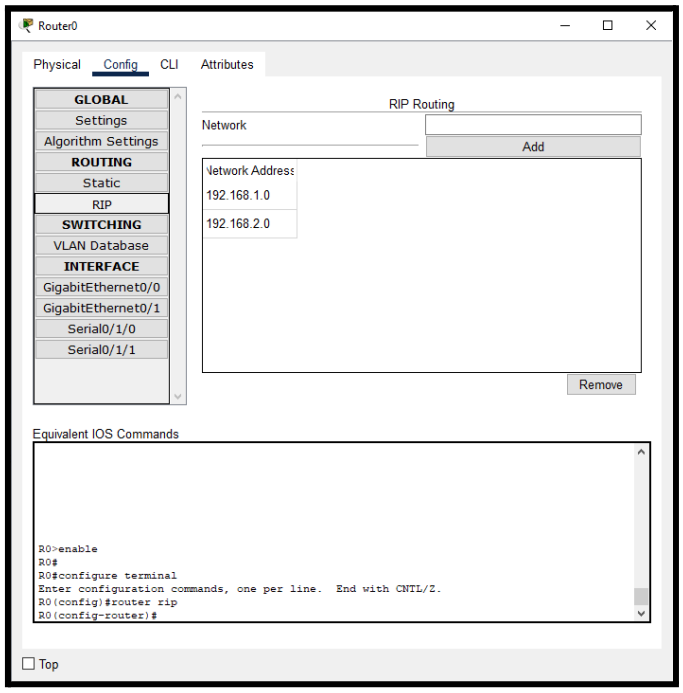

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
Top

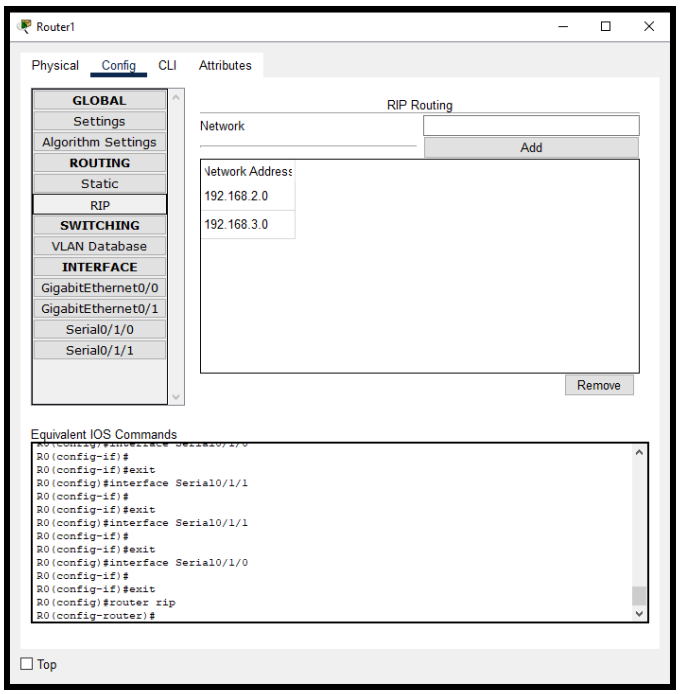

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/1
R0(config-if)#
Top

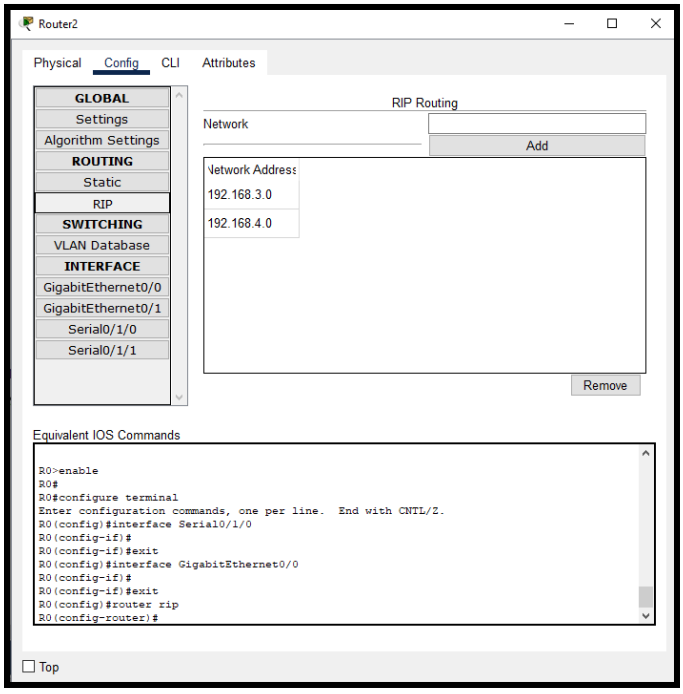

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
192.168.3.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
Top


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.D3C6.2701
IP Configuration
IPv4 Address
192.168.4.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface GigabitEthernet0/0
R0(config-if)#
Top

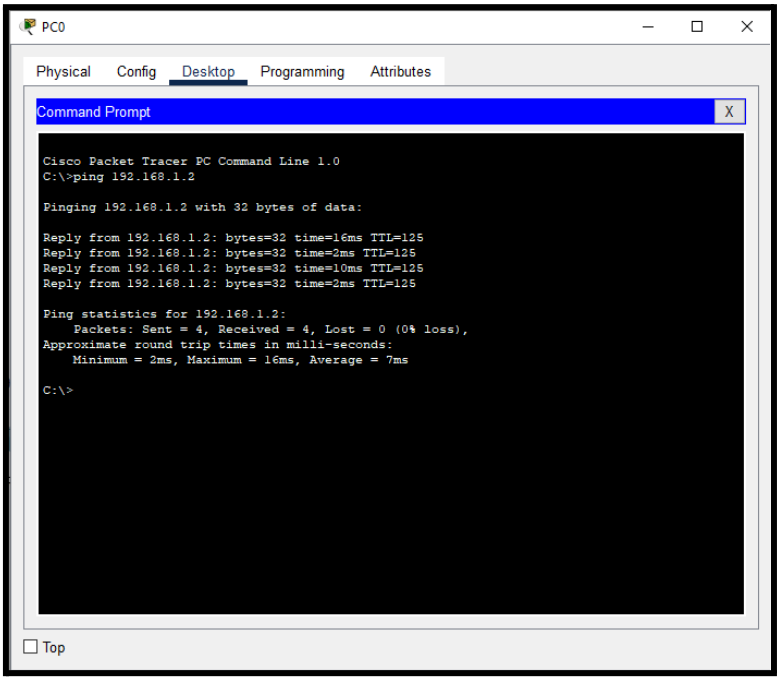
RIP


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.1.0
192.168.2.0
Remove
Equivalent IOS Commands
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#router rip
R0(config-router)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/1
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/1
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#router rip
R0(config-router)#
Top


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.3.0
192.168.4.0
Remove
Equivalent IOS Commands
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface GigabitEthernet0/0
R0(config-if)#
R0(config-if)#exit
R0(config)#router rip
R0(config-router)#
Top

On PC -> Verify the connectivity



Routers -> Cli

I. SSH Enable

1) **enable**
2) **conf t**
3) **ip domain-name tyit.com**
4) **hostname R0**
5) **crypto key generate rsa 512**
6) **line vty 0 4**
7) **transport input ssh**
8) **login local**
9) **exit**
10) **username ssh_admin privilege 15 password ty**
11) **exit**

II. Access List Define

1) **enable**
2) **conf t**
3) **access-list 10 permit host 192.168.4.2**
4) **line vty 0 4**
5) **access-class 10 in**

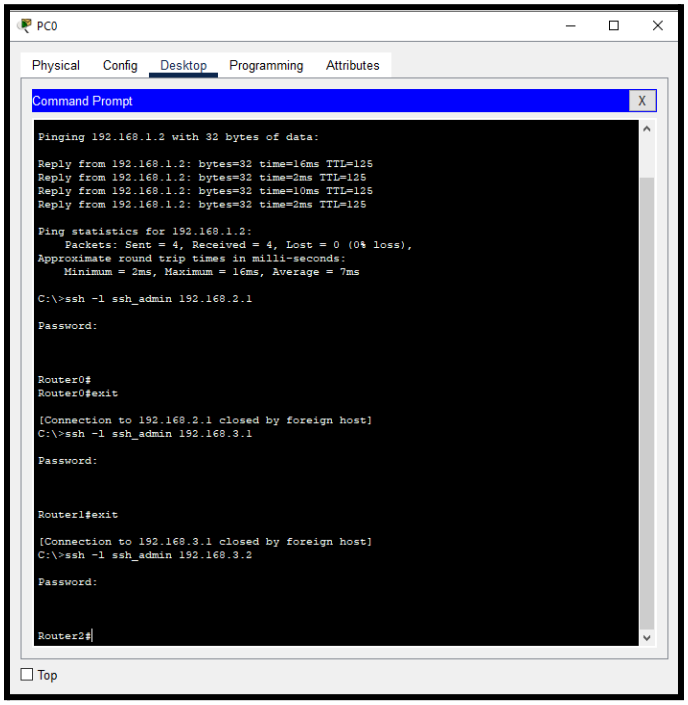
On PC -> Verify on CMD

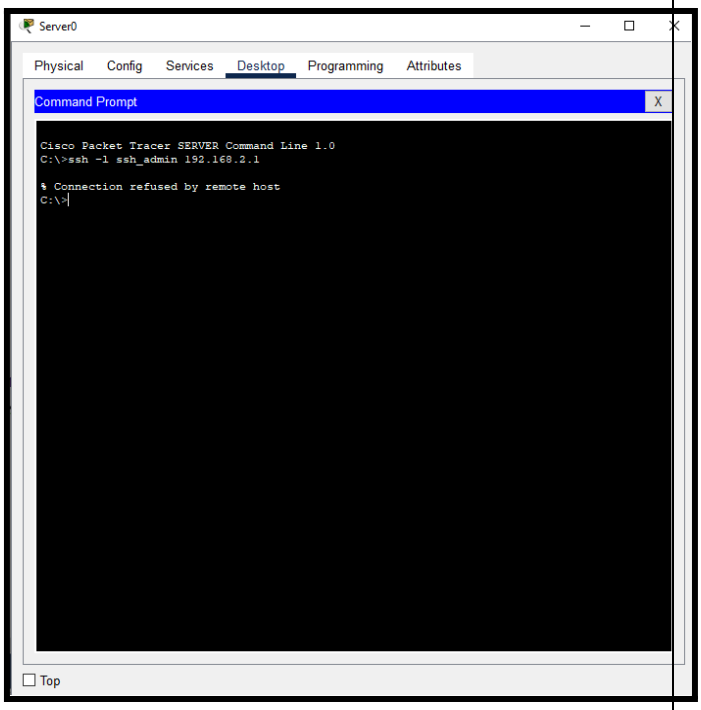
> ssh -l ssh_admin 192.168.3.2

Password: ty

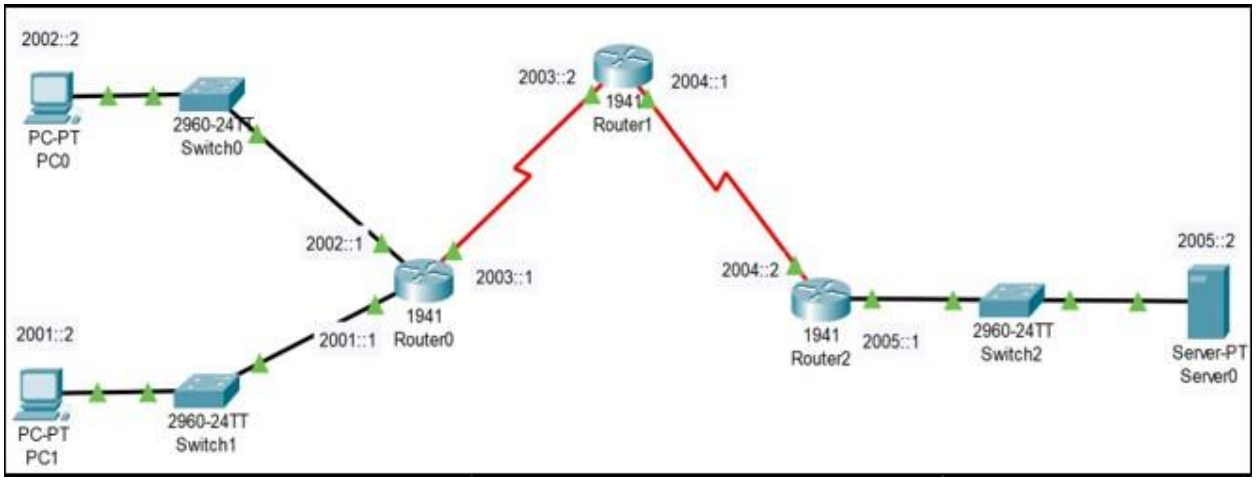
On Server -> Verify on CMD

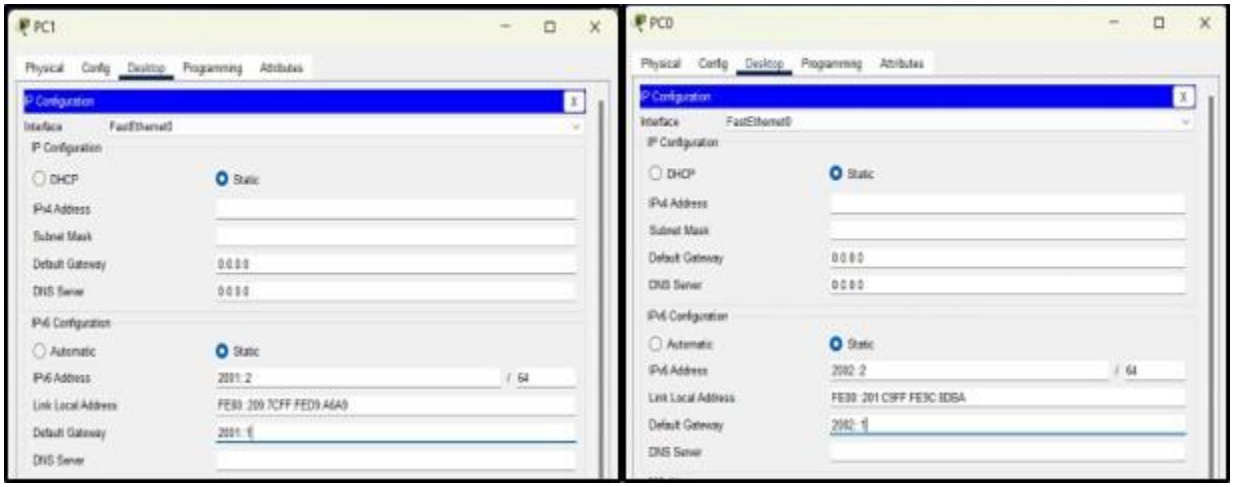
> ssh -l ssh_admin 192.168.2.1

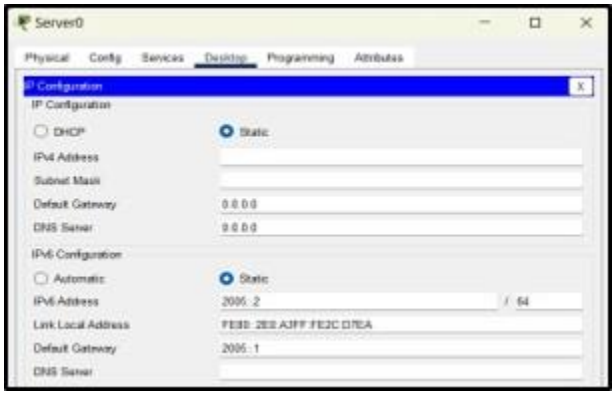




d. Configuring IPv6 ACLs







Router 0:

Router>enable

Router#

Router#configure terminal

Router(config)#ipv6 unicast-routing

Router(config)#interface GigabitEthernet0/0

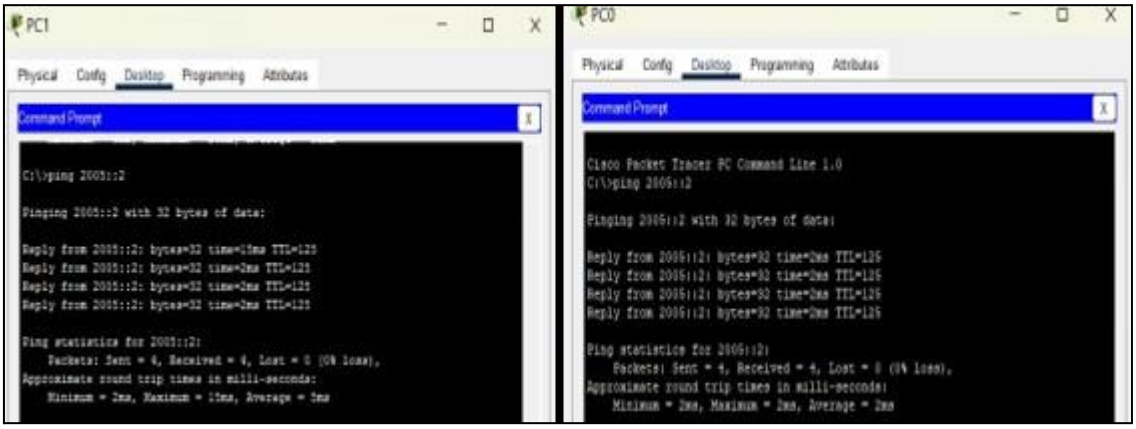
Router(config-if)#ipv6 address 2002::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ipv6 address 2001::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

Router 1:
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 address 2004::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#

Router2:
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 address 2004::2/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ipv6 address 2005::1/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

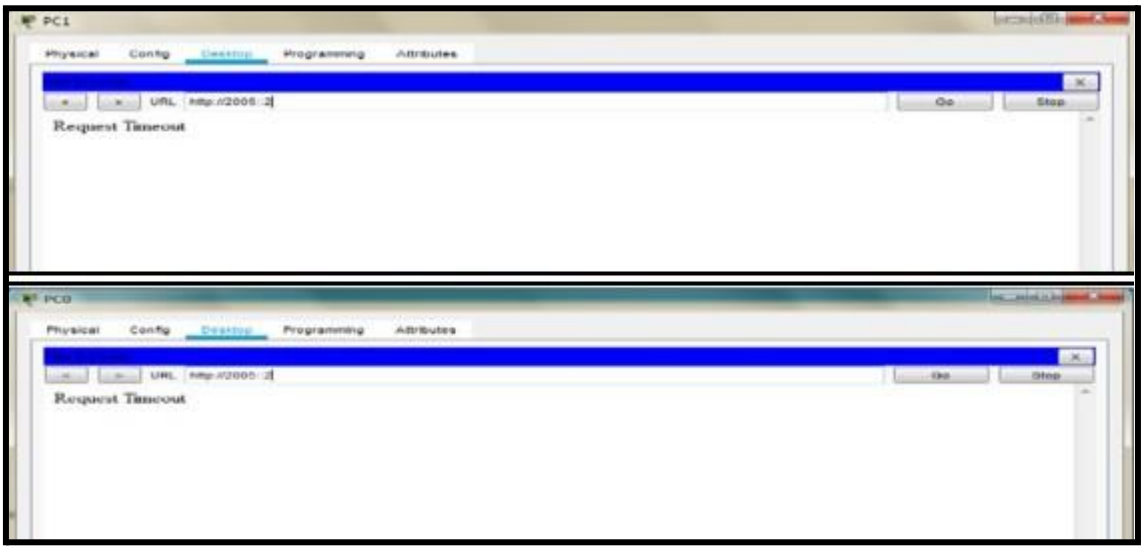
Check the connectivity by pinging from PCs to Server

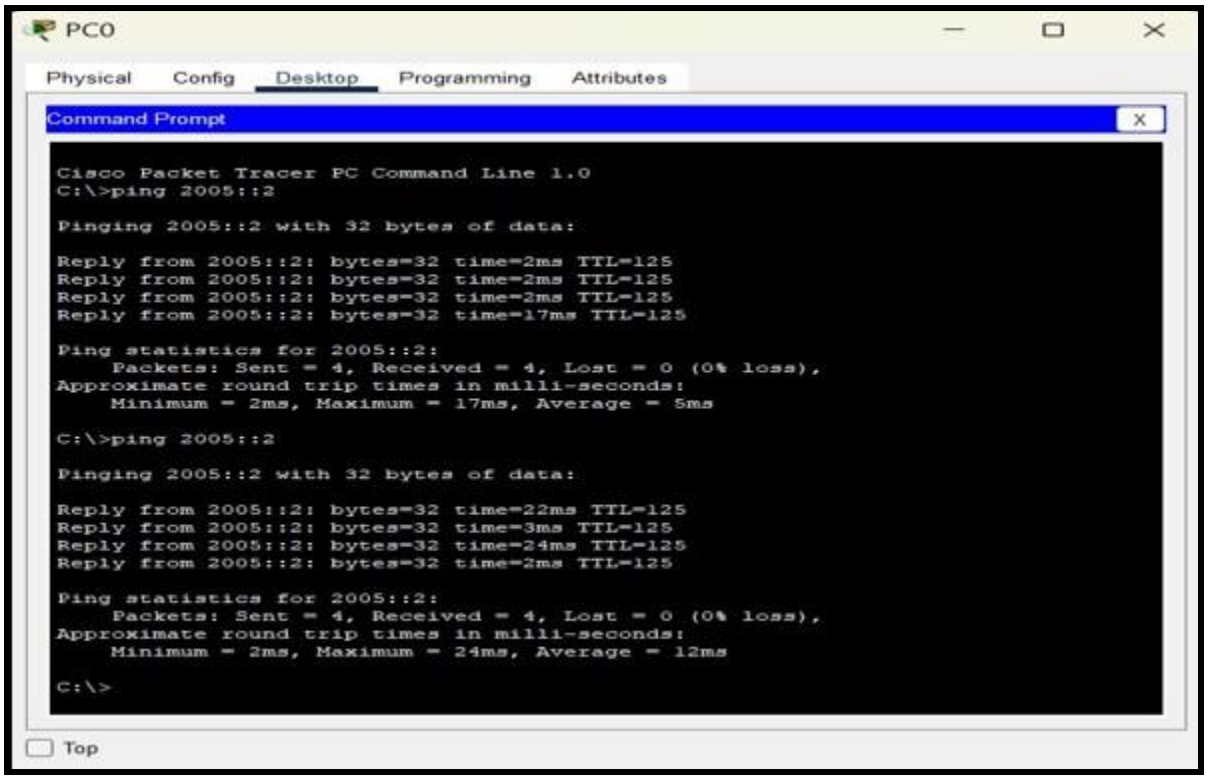


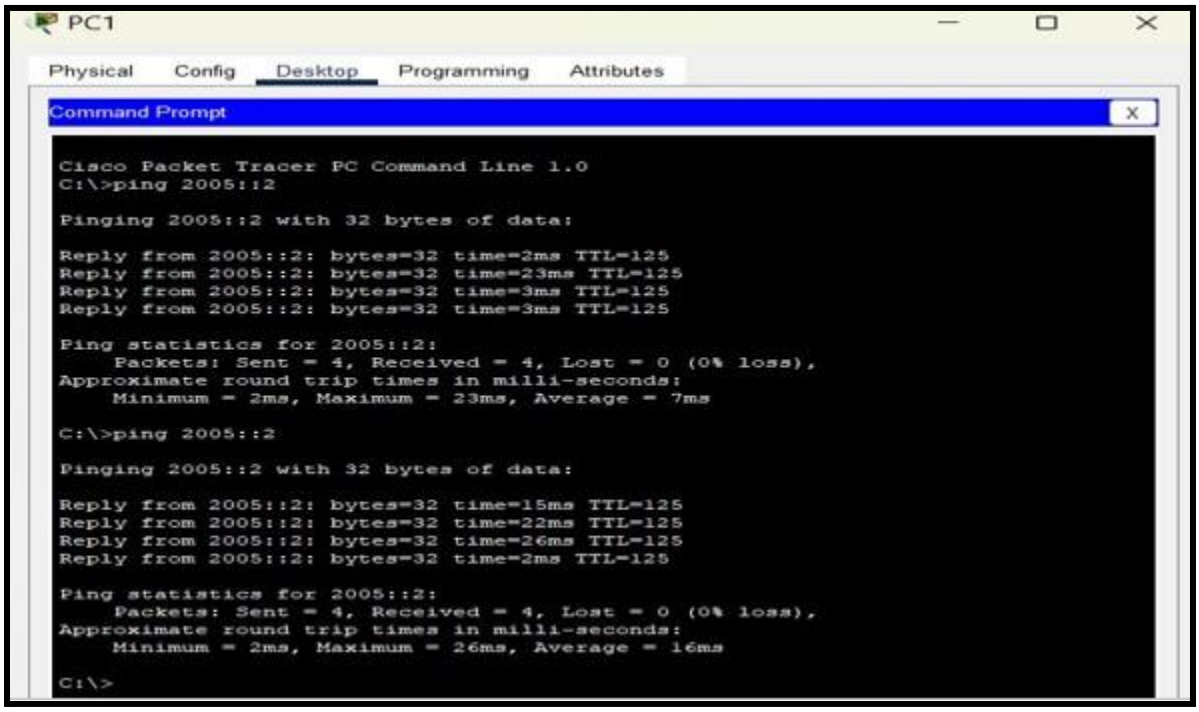
Enter the following commands in the CLI mode of the Router1 and apply it at the proper interface:-

Router>enable
Router#configure terminal
Router(config)#ipv6 access-list smile
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq www
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq 443
Router(config-ipv6-acl)#permit ipv6 any any
Router(config-ipv6-acl)#

Router(config-ipv6-acl)#exit
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#ipv6 tra c-filter smile in
Router(config-if)#exit
Router(config)#

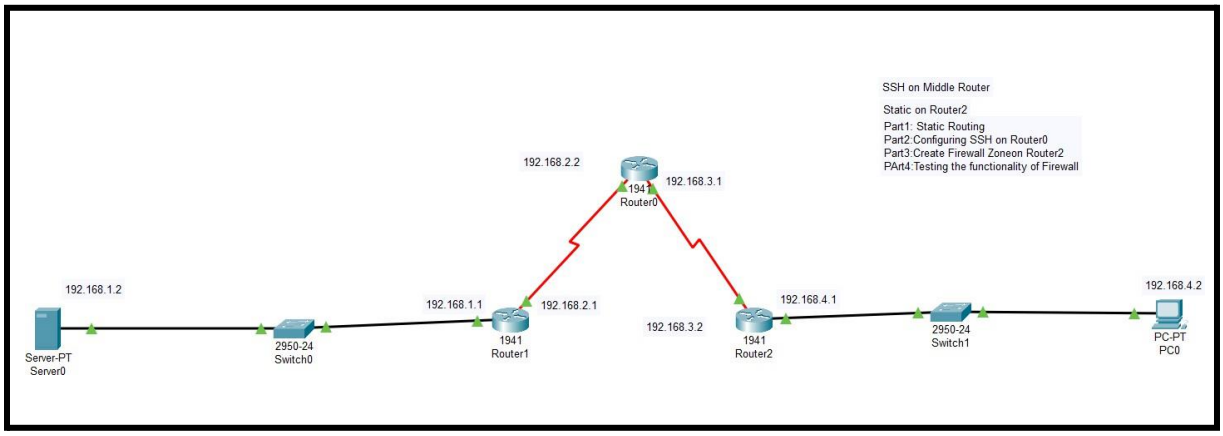




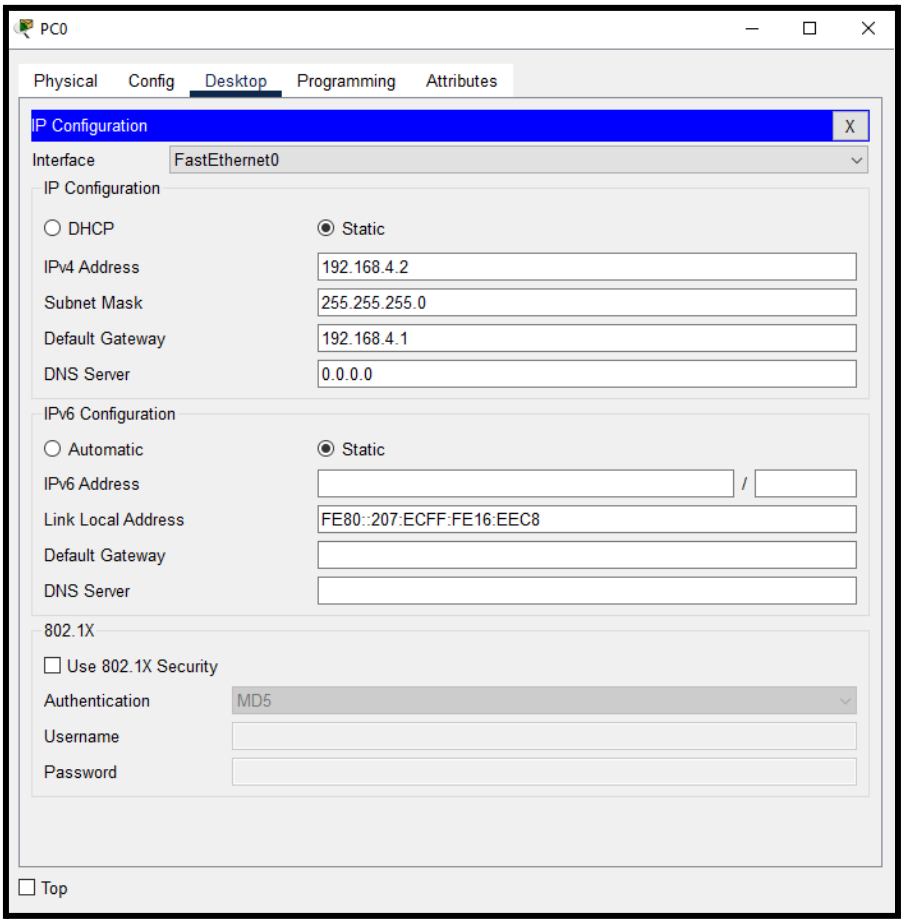

PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2005::2
Pinging 2005::2 with 32 bytes of data:
Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=23ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125
Ping statistics for 2005::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 23ms, Average = 7ms
C:\>ping 2005::2
Pinging 2005::2 with 32 bytes of data:
Reply from 2005::2: bytes=32 time=15ms TTL=125
Reply from 2005::2: bytes=32 time=22ms TTL=125
Reply from 2005::2: bytes=32 time=26ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125
Ping statistics for 2005::2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 26ms, Average = 16ms
C:\>

Practical 5

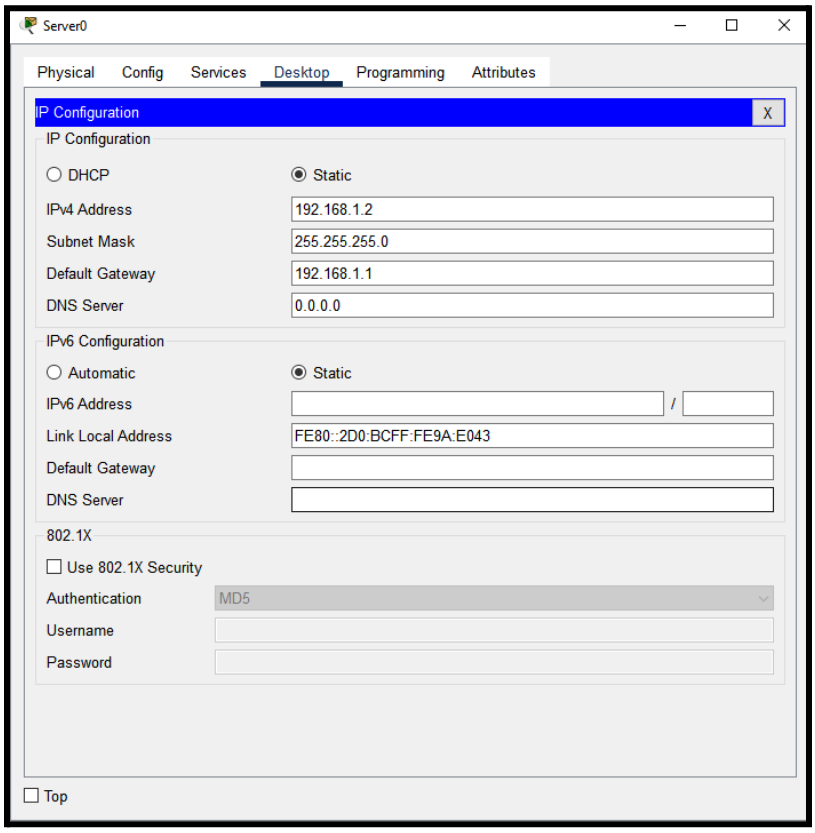
Configuring a Zone-Based Policy Firewall



Configuring PC0

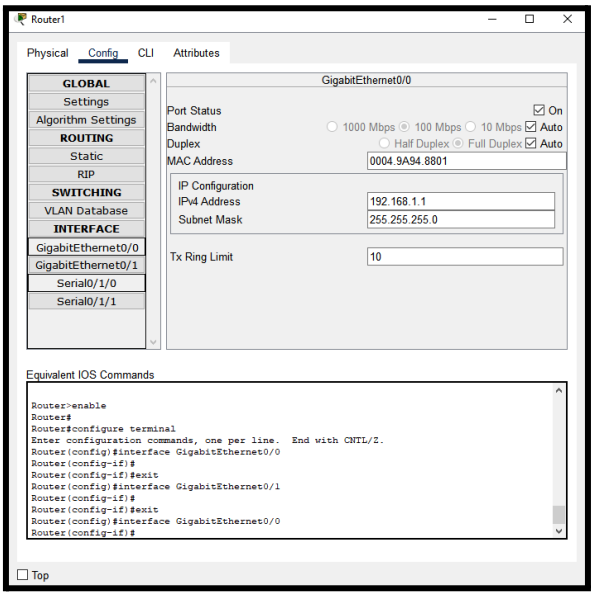


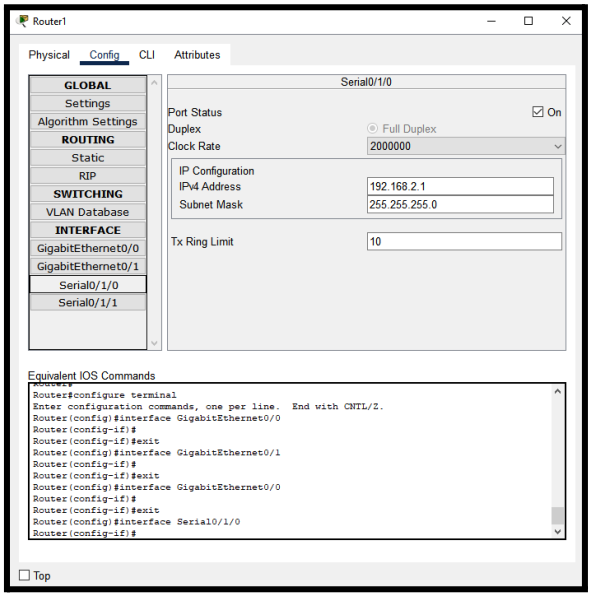
Configuring server0



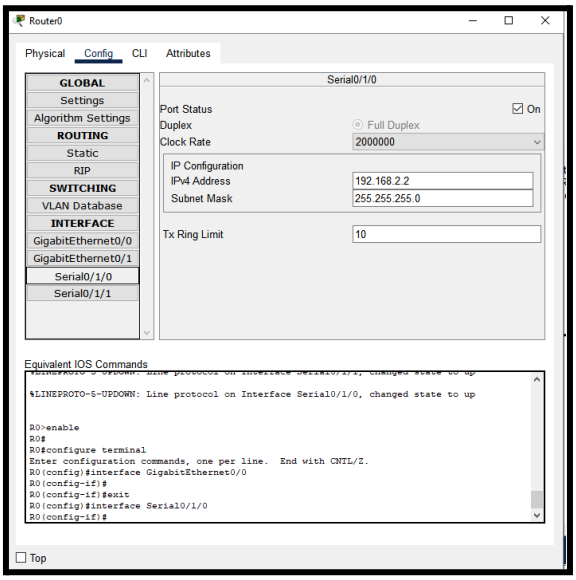
Serial interface must be added in each Router before configuring it

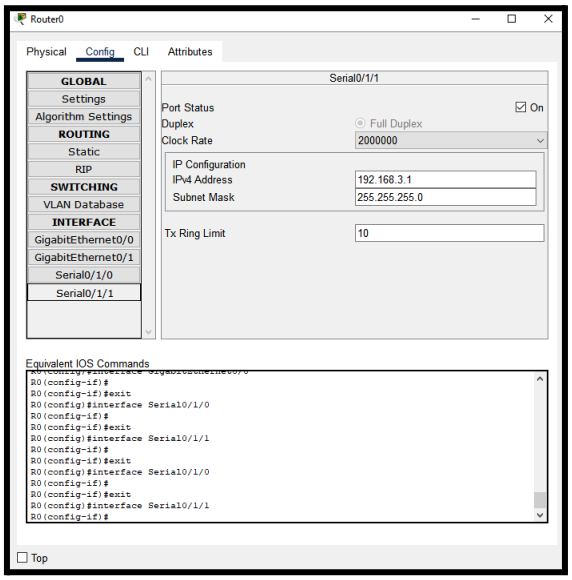
Configuring Router1



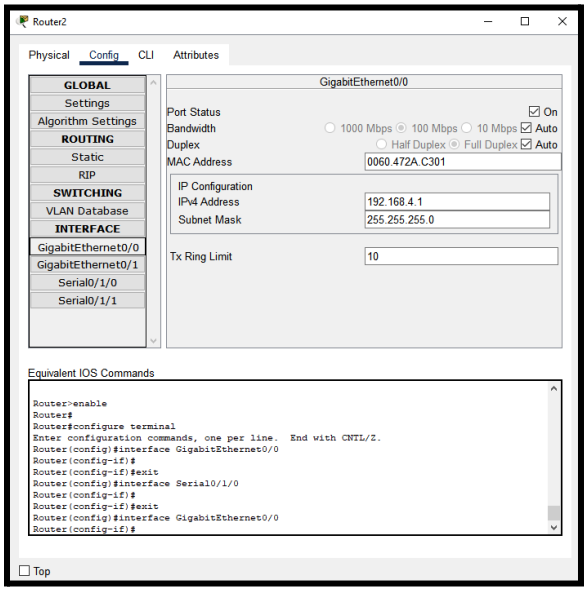


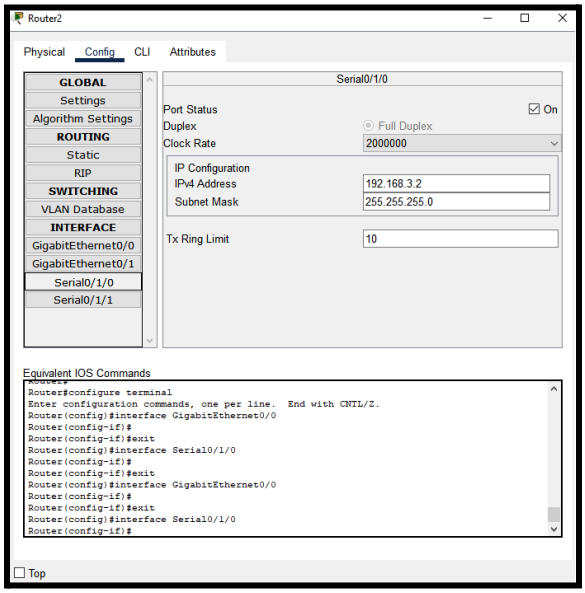
Configuring Router0





Configuring Router2

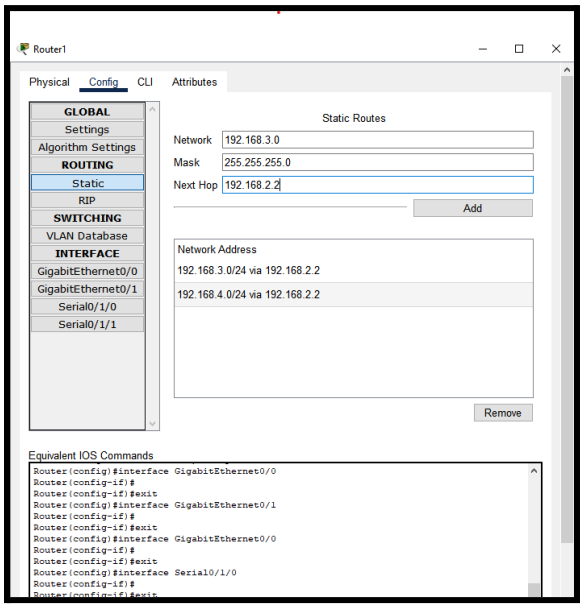


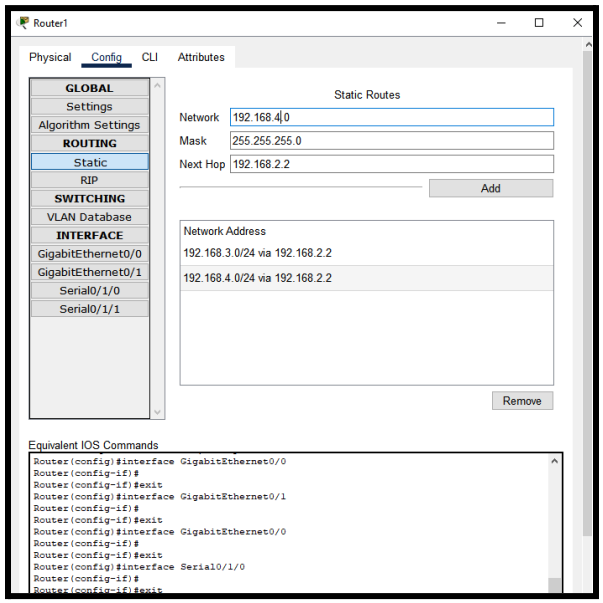


Part1: Static Routing

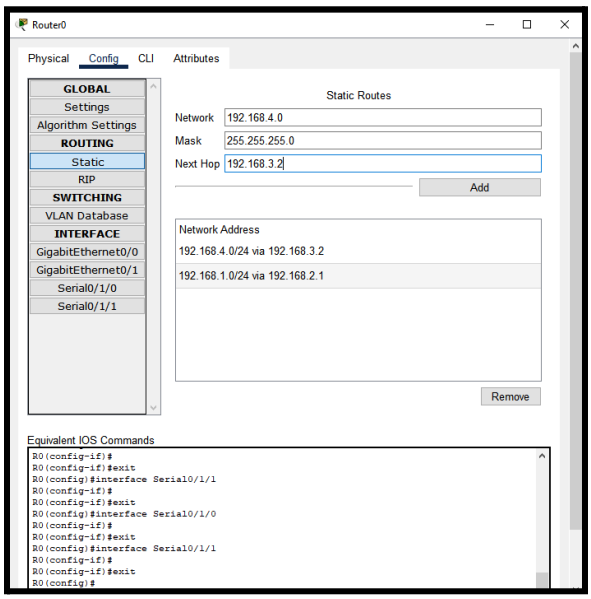
Static Routing is done using the following procedure for each Router

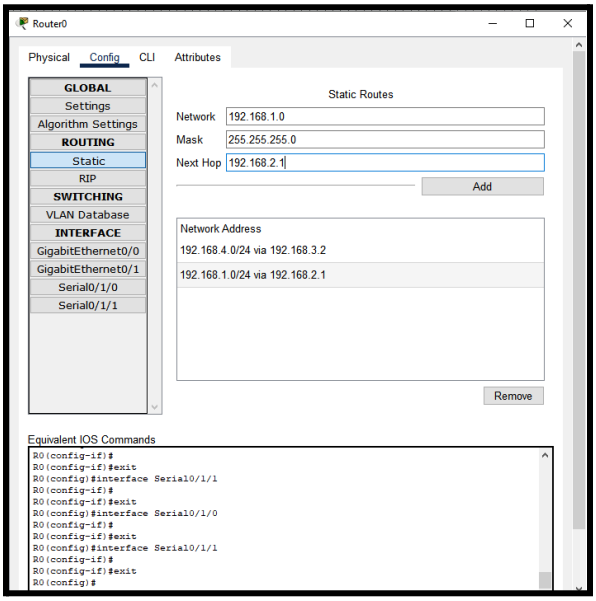
Router 1:



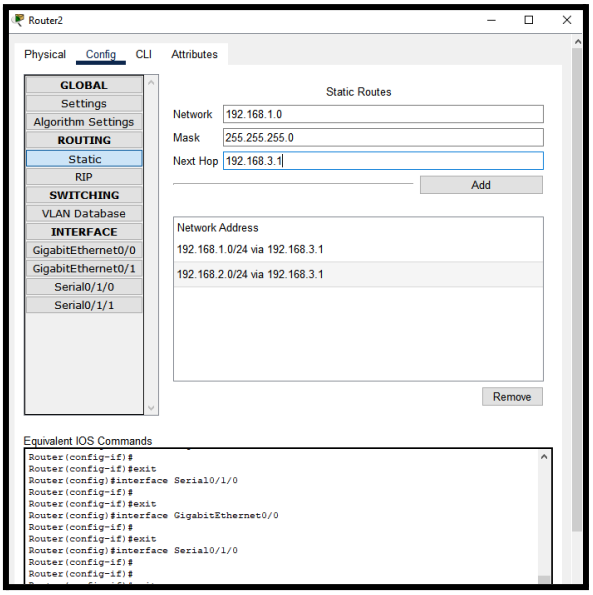


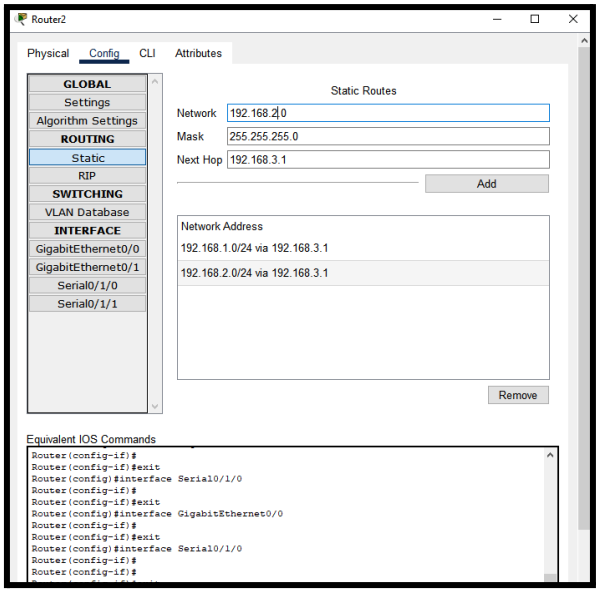
Router 0:



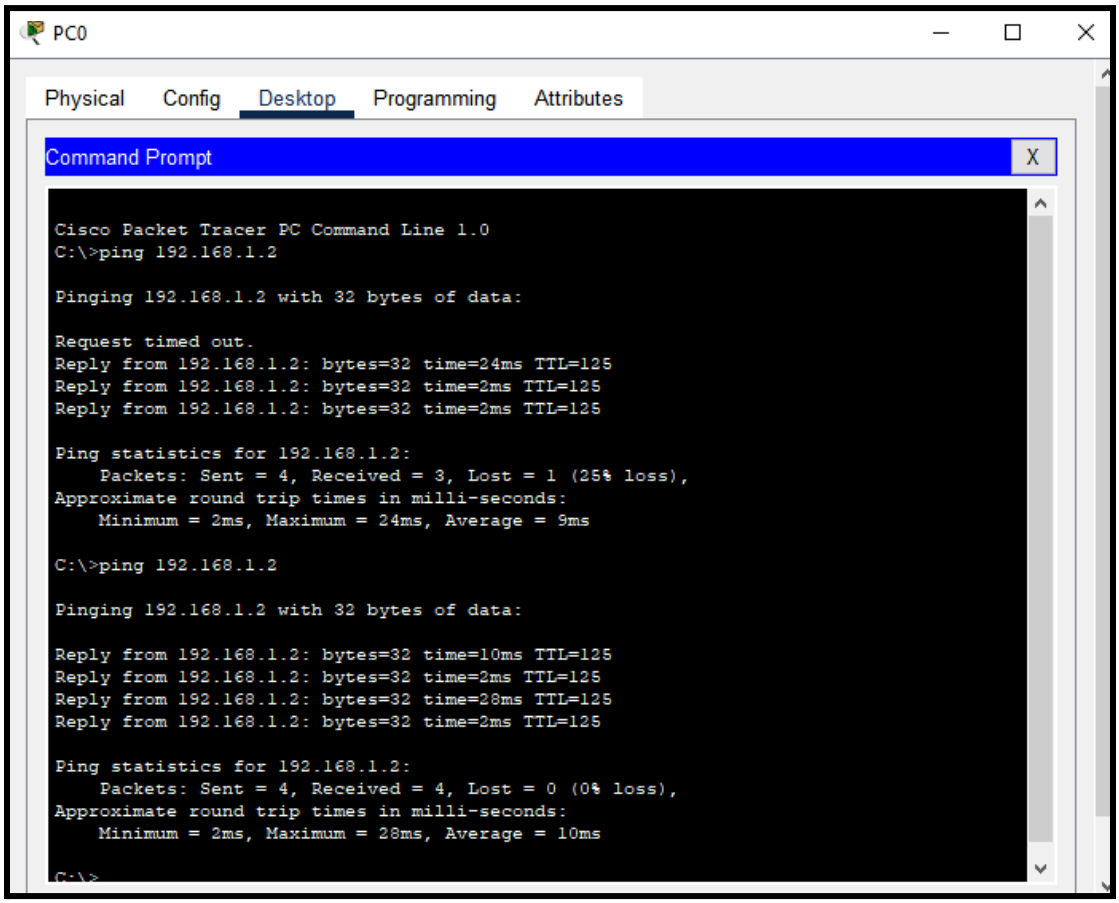


Router 2:





Check the connectivity by pinging the server from the PC

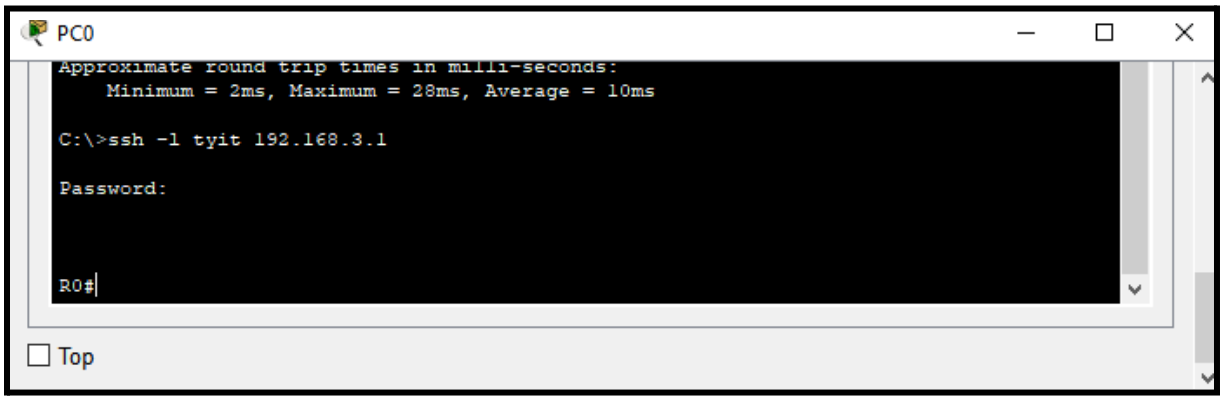


Part 2: Configuring SSH on Router 0

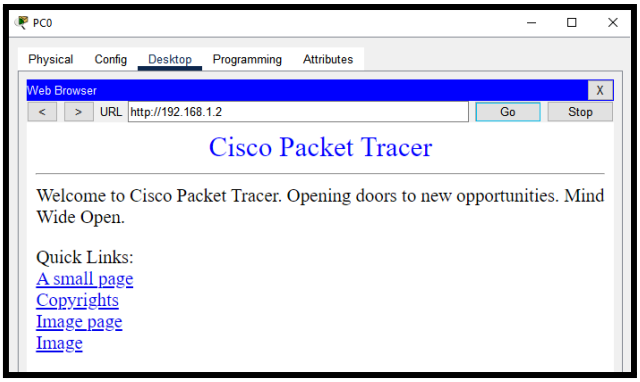
Router 0→ CLI

Router#enable
Router#conf t
Router(config)#ip domain-name tyit.com
Router(config)#hostname R0
R2(config)#crypto key generate rsa
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#exit
R2(config)#username tyit privilege 15 password pass

Now we verify the SSH using PC as follows



Next we access the web services of the Server using the web browser of PC using the following



Check whether the securityk9 package exist on Router2 or not by writing the following command on CLI→
show version

If not type the below command in CLI
enable
conf t
license boot module c1900 technology-package securityk9
Accept→ yes
Click enter
exit
copy run start
reload

Now check whether the securityk9 package has been installed or not.

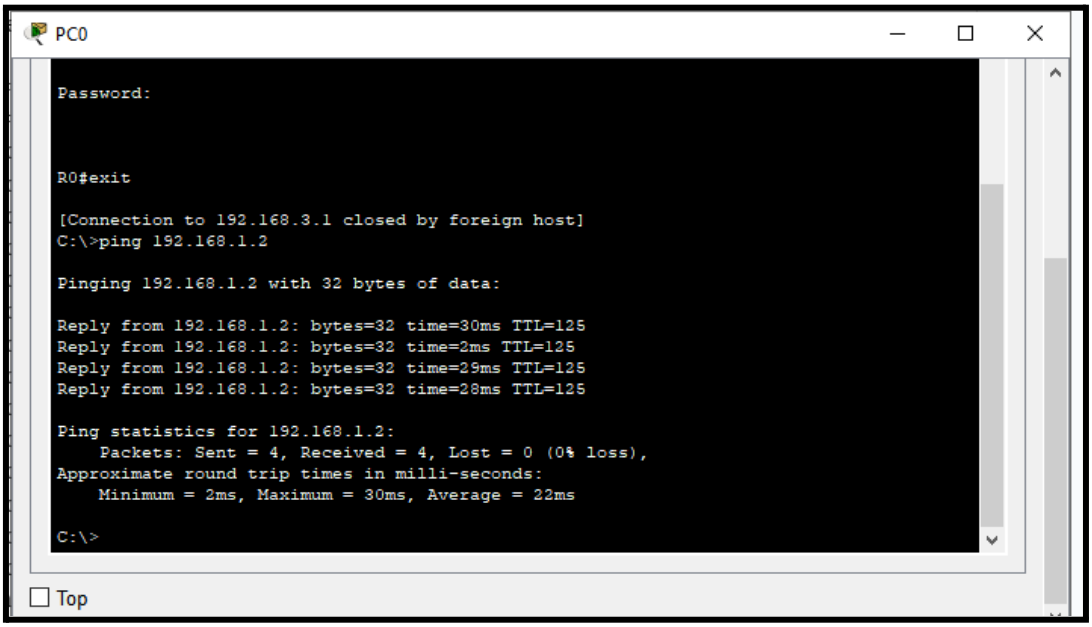
Part 3: Create the Firewall Zones on Router2
Type the following commands in the CLI mode of Router2

Router#
Router#configure terminal
Router(config)#zone security in-zone
Router(config-sec-zone)#exit
Router(config)#zone security out-zone
Router(config-sec-zone)#exit
Router(config)#access-list 101 permit ip 192.168.4.0 0.0.0.255 any
Router(config)#class-map type inspect match-all in-map
Router(config-cmap)#match access-group 101
Router(config-cmap)#exit
Router(config)#policy-map type inspect in-out
Router(config-pmap)#class type inspect in-map
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#zone-pair security in-out-zone source in-zone destination out-zone
Router(config-sec-zone-pair)#service-policy type inspect in-out

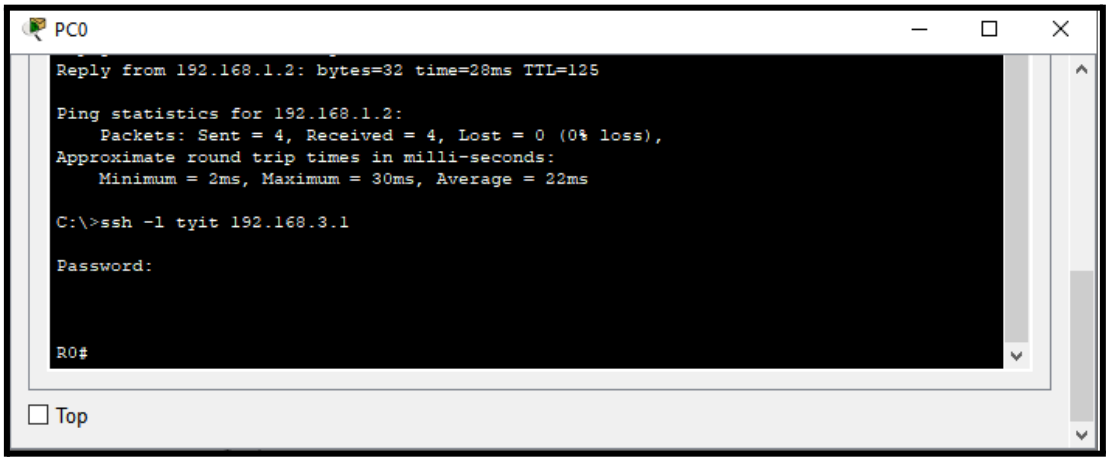
Router(config-sec-zone-pair)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0
Router(config-if)#zone-member security in-
zone Router(config-if)#exit
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#zone-member security out-zone
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config

Part 4: Testing the Firewall Functionality (from in-zone to out-zone)by the following steps

Step 1: Pinging SERVER from the PC (it will succeed)



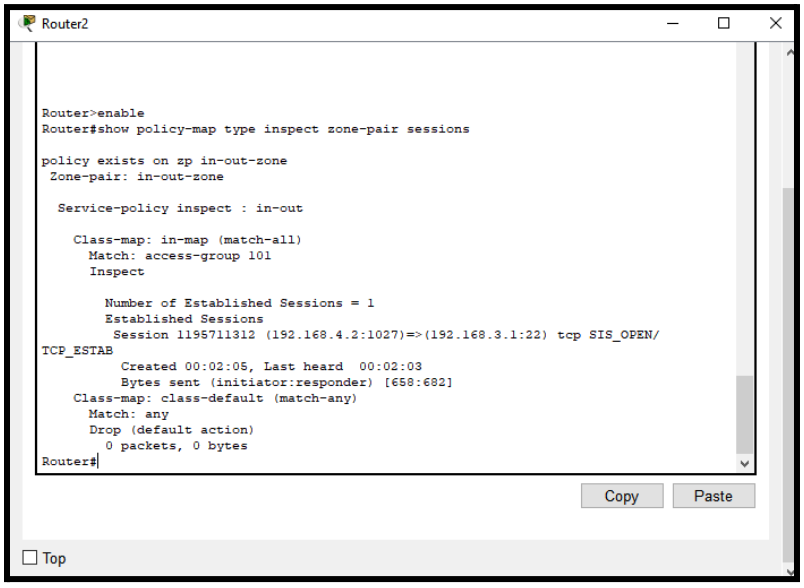
Step 2: Start an SSH session from PC to Router 0(ip 192.168.1.2)



Step 3: Type the following command in the CLI mode of Router1

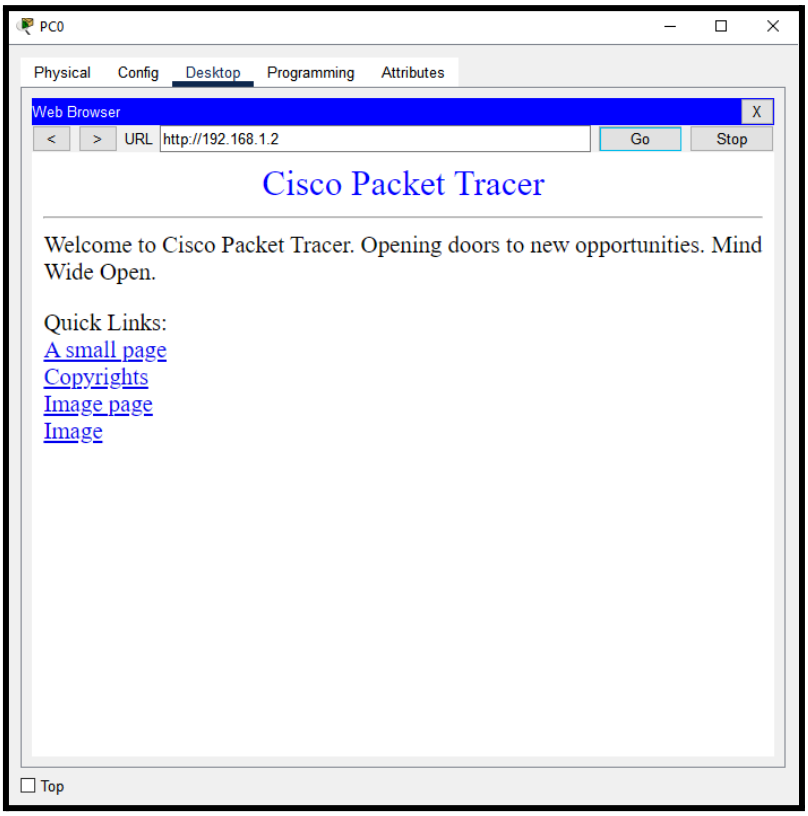
Router#show policy-map type inspect zone-pair sessions

We will get the following output



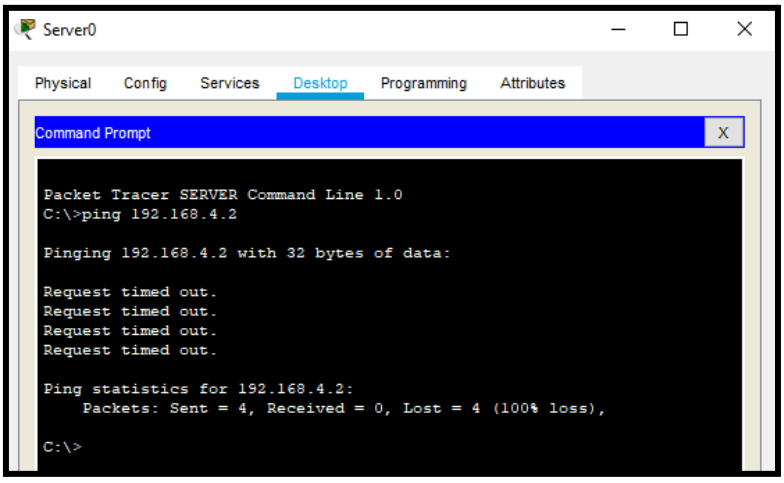
Step 4: We close the SSH connection and open the web browser and access the server

address (192.168.1.2) and get the following



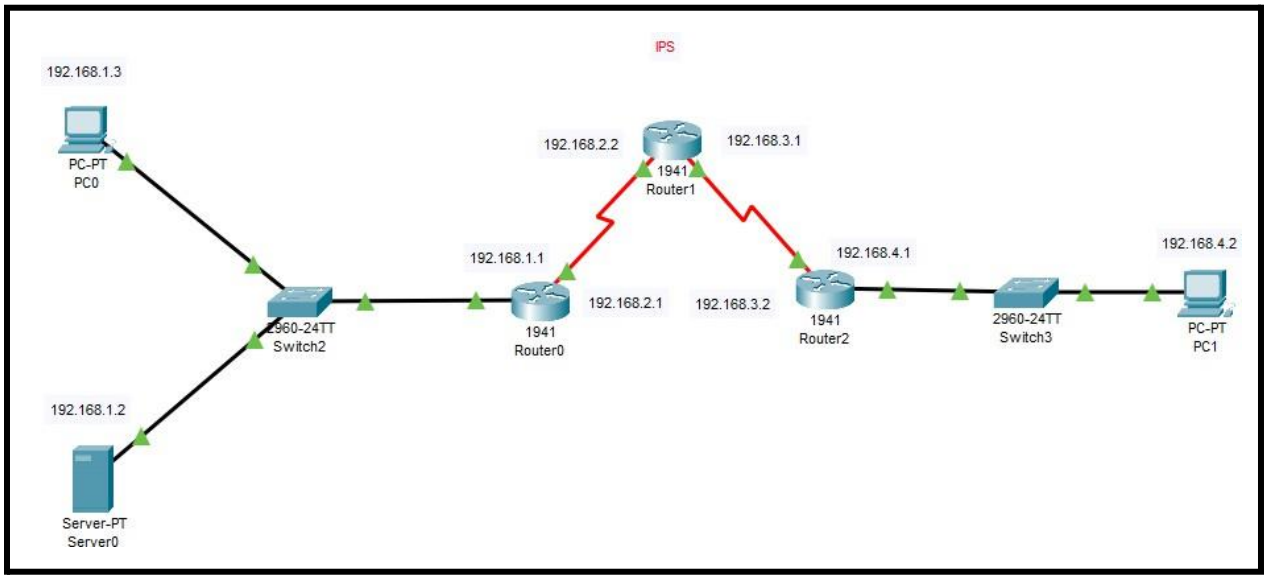
Part 5: Testing the Firewall Functionality (from out-zone to in-zone)by the following steps

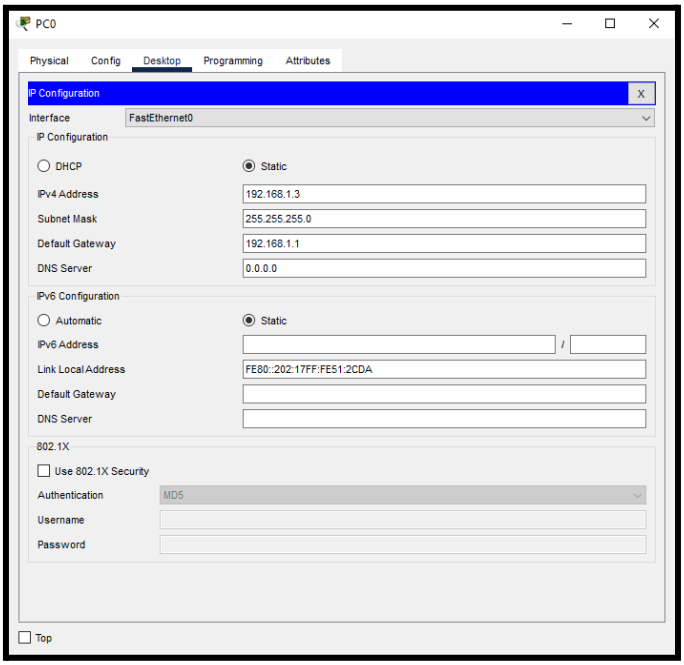
Step 1: Ping PC0 from the SERVER (it will result in Failure)

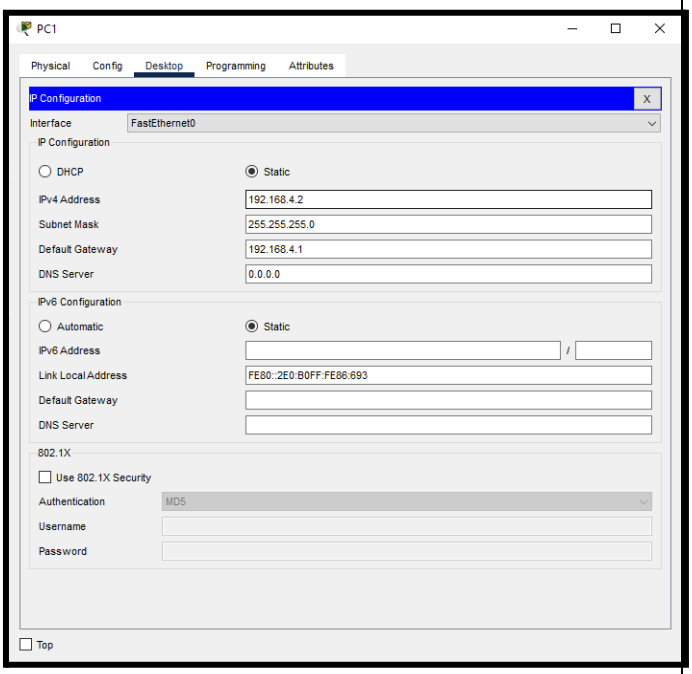


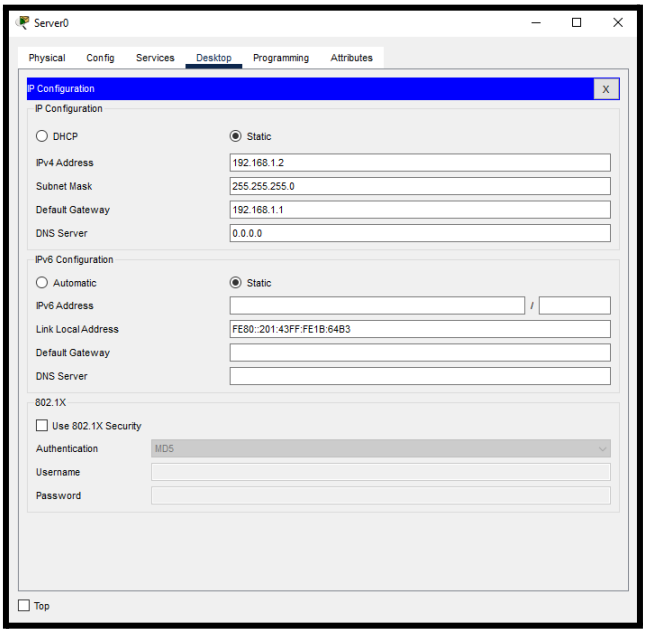
Practical 6

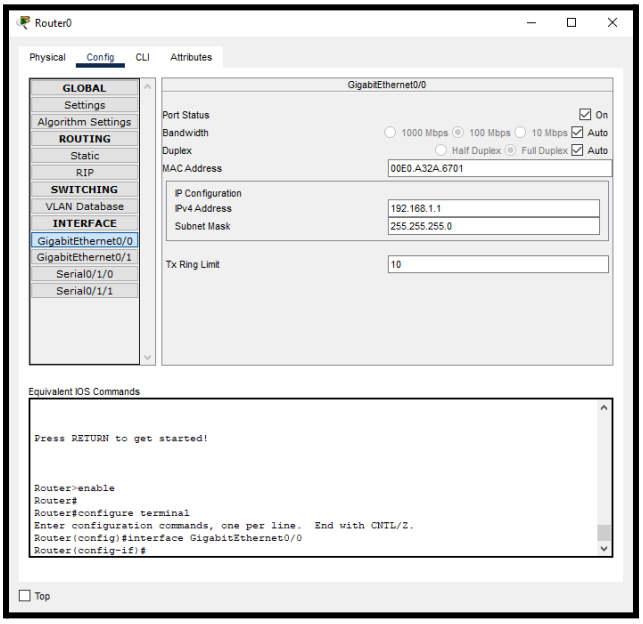
Configure IOS Intrusion Prevention System (IPS) Using the CLI

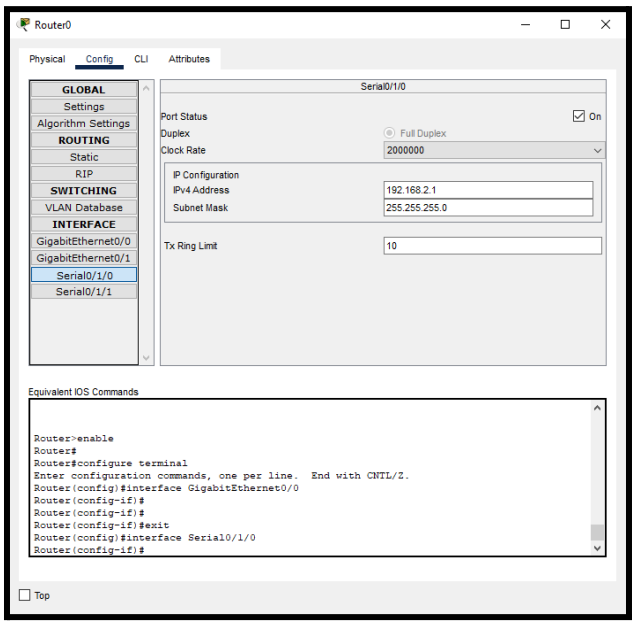


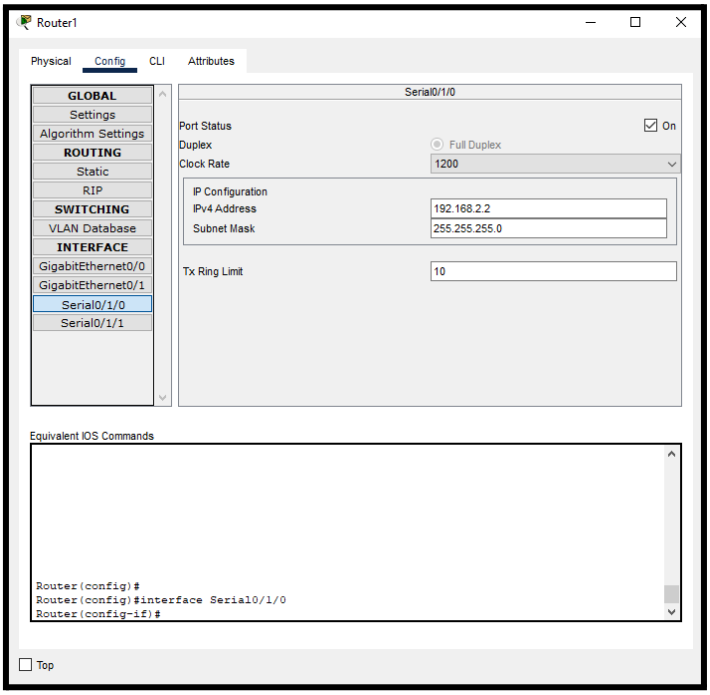


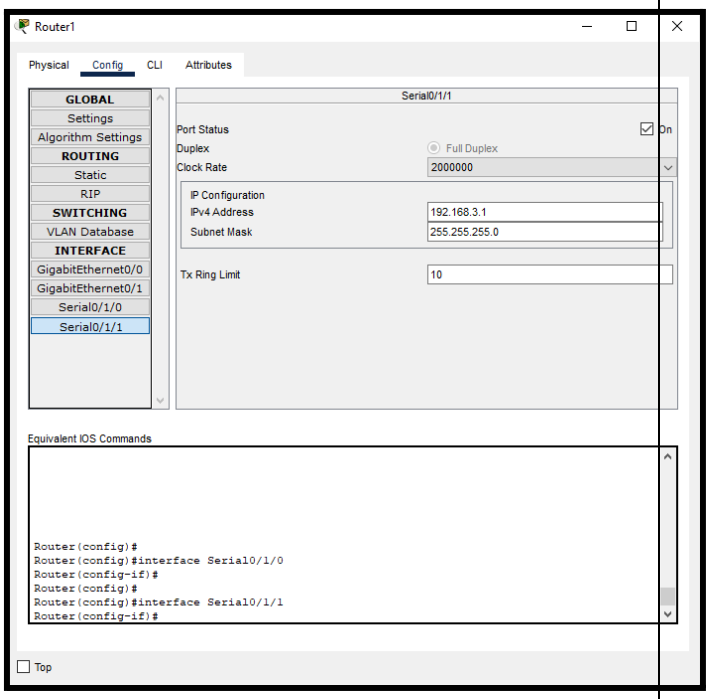


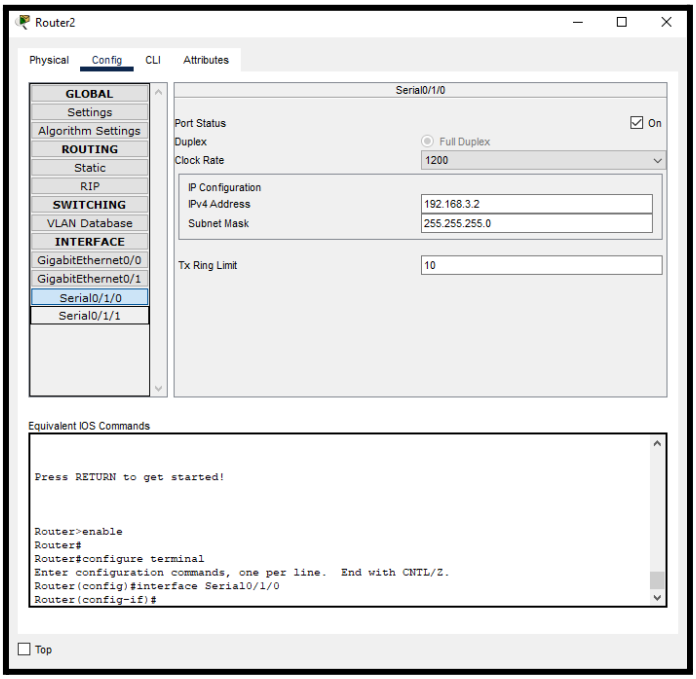

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:43FF:FE1B:64B3
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

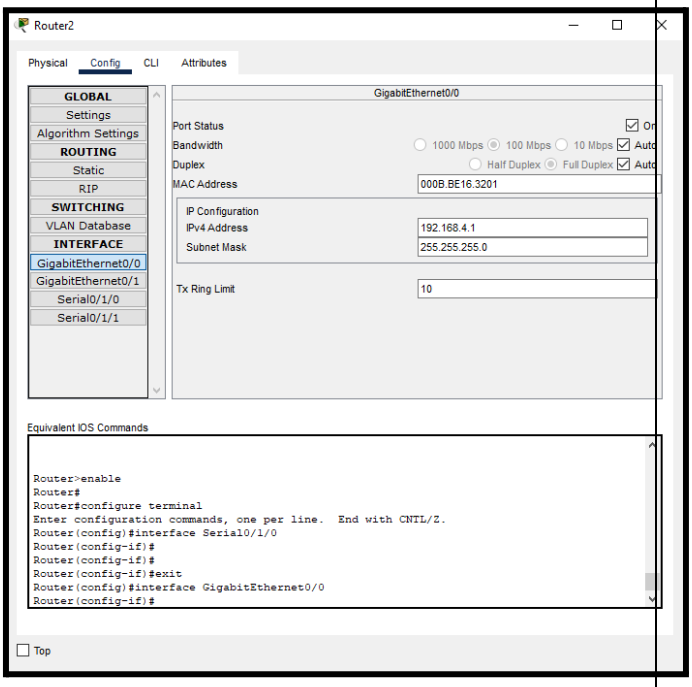

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.A32A.6701
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Press RETURN to get started!
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top

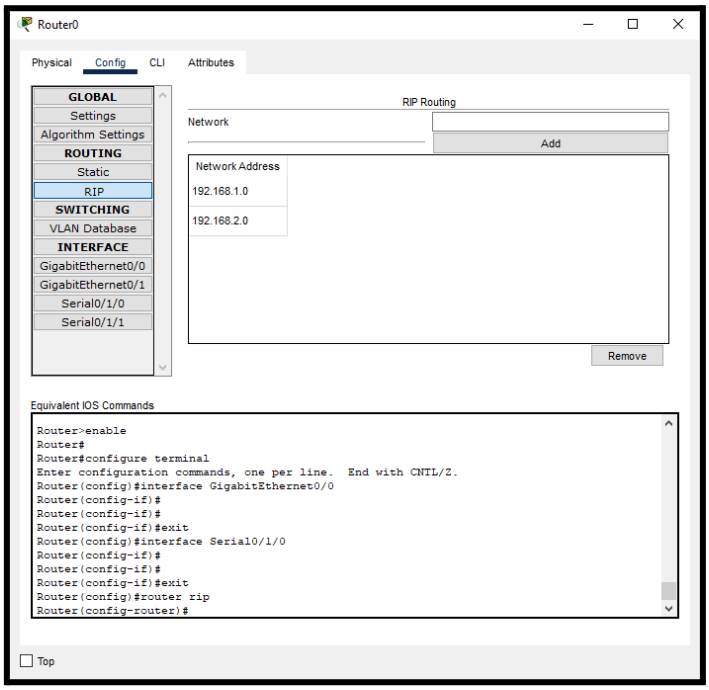

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Top

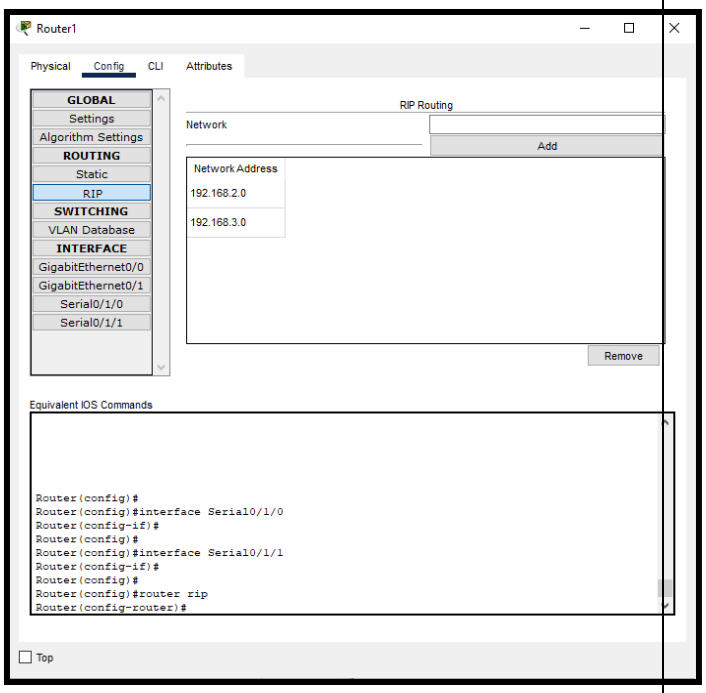

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#
Top

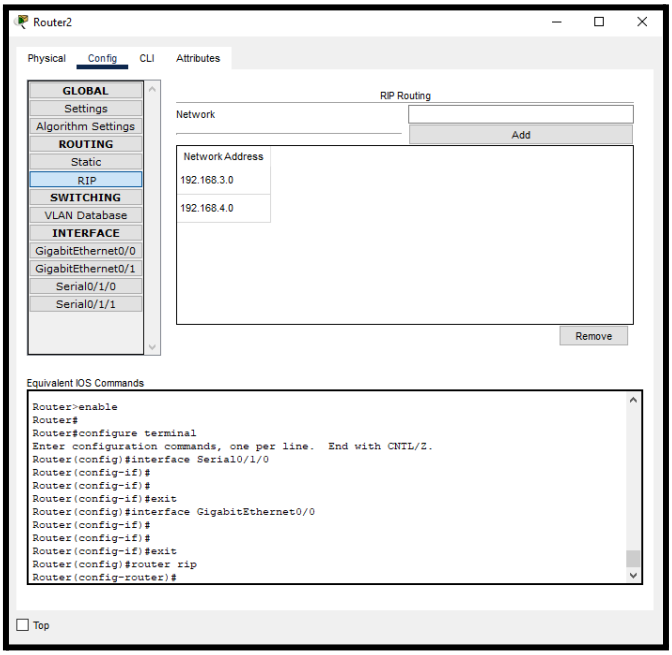

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IPv4 Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#
Top


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IPv4 Address
192.168.3.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Press RETURN to get started!
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
Top


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000B.BE16.3201
IP Configuration
IPv4 Address
192.168.4.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.1.0
192.168.2.0
Remove
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.2.0
192.168.3.0
Remove
Equivalent IOS Commands
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#
Router(config)#
Router(config)#router rip
Router(config-router)#
Top

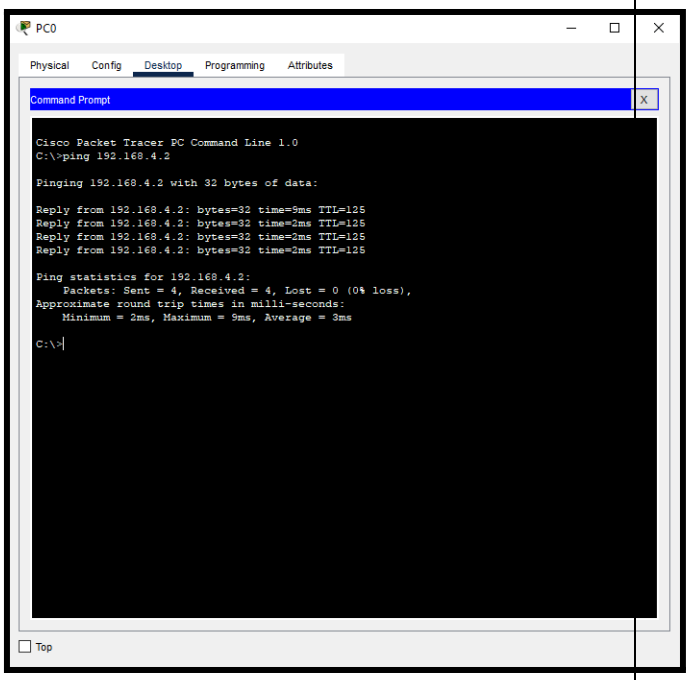

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.3.0
192.168.4.0
Remove
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#
Top

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco 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.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=18ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 7ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

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=8ms TTL=125
Reply from 192.168.1.3: bytes=32 time=13ms TTL=125
Reply from 192.168.1.3: bytes=32 time=5ms 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 = 13ms, Average = 7ms
```

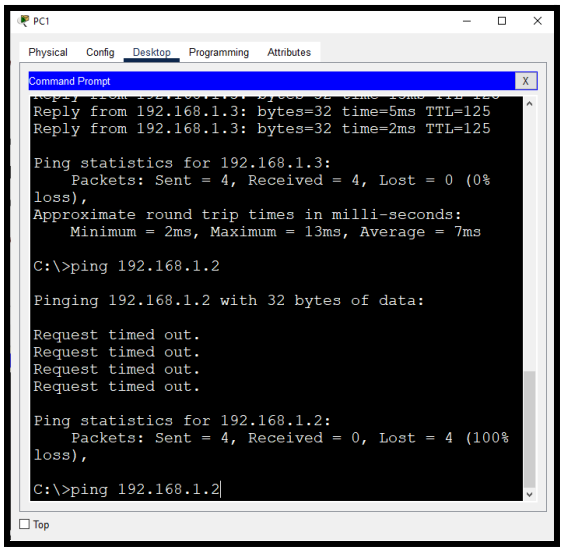


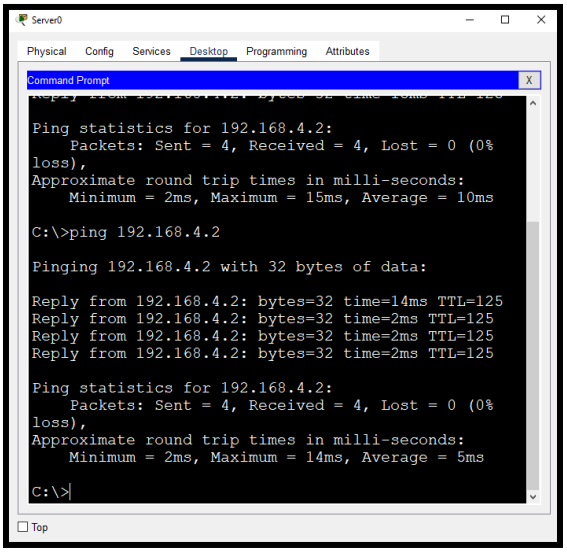
Router>enable
Router#show version
Router#conf t
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#exit
Router#reload
##
Router>enable
Router#
Router#show version
securityk9 installed successfully

Router#
Router#clock set 15:40:56 MARCH 5 2024
Router#mkdir smile
Router#configure terminal
Router(config)#ip ips config location flash:smile
Router(config)#ip ips name tyit
Router(config)#ip ips notify log
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip ips tyit out
Router(config-if)#exit
Router(config)#

Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true

Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Router(config)#exit



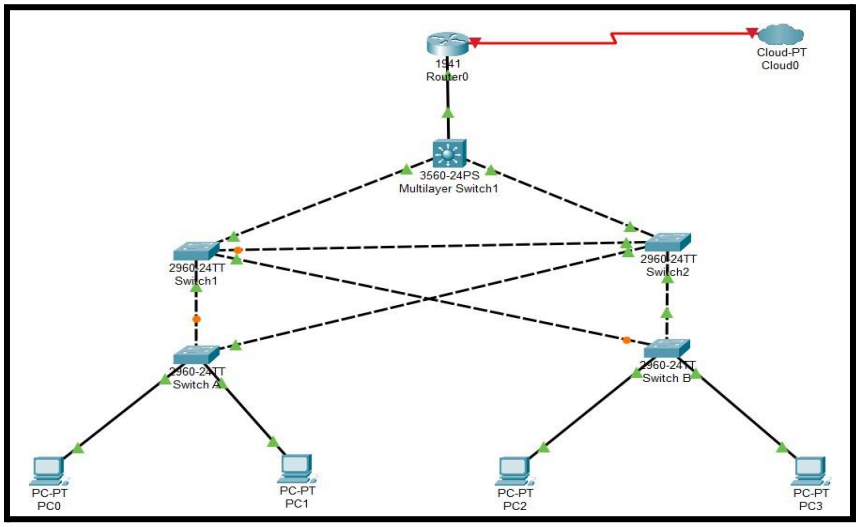


Practical 7

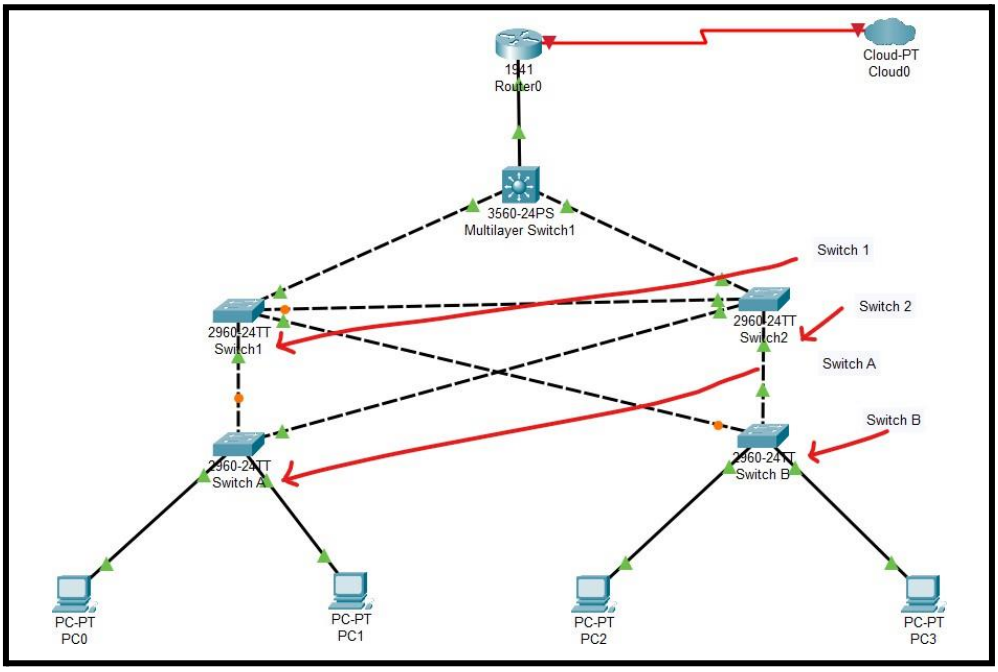
Layer 2 Security

a) Assign the Central switch as the root bridge.
b) Secure spanning-tree parameters to prevent STP manipulation attacks.
c) Enable port security to prevent CAM table overflow attacks.

a) Assign the Central switch as the root bridge.



Add serial interface to cloud and router both ports.. Once the topology is ready
Rename your first switch to switch A



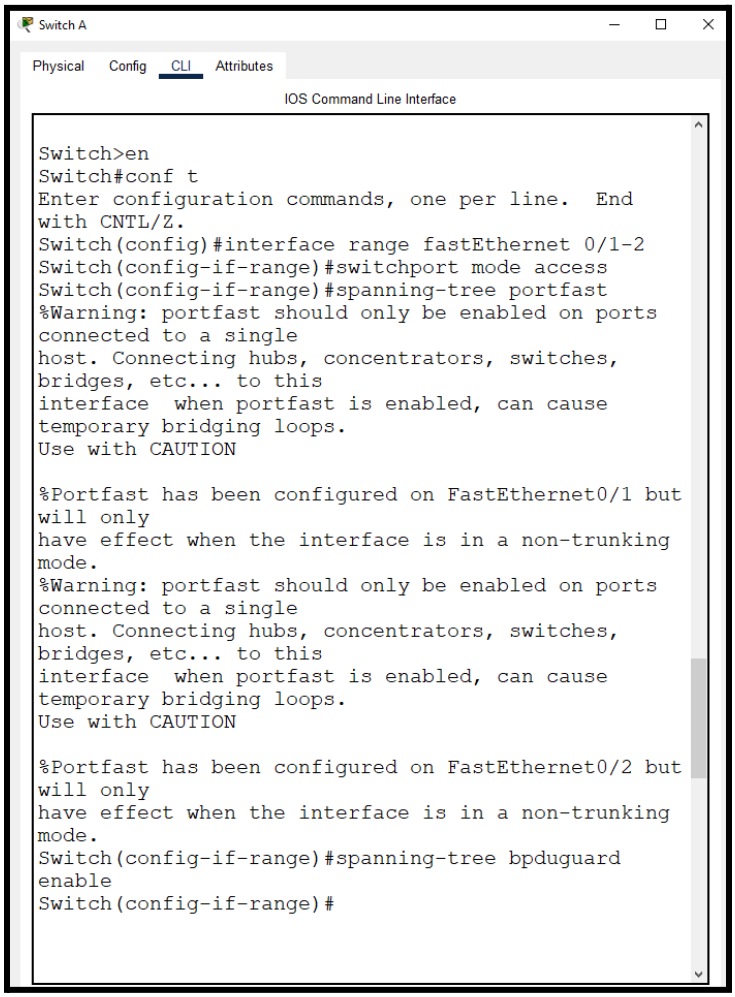
Part 1 : Root Bridge is set up

Part 2–Protect Against STP Attack

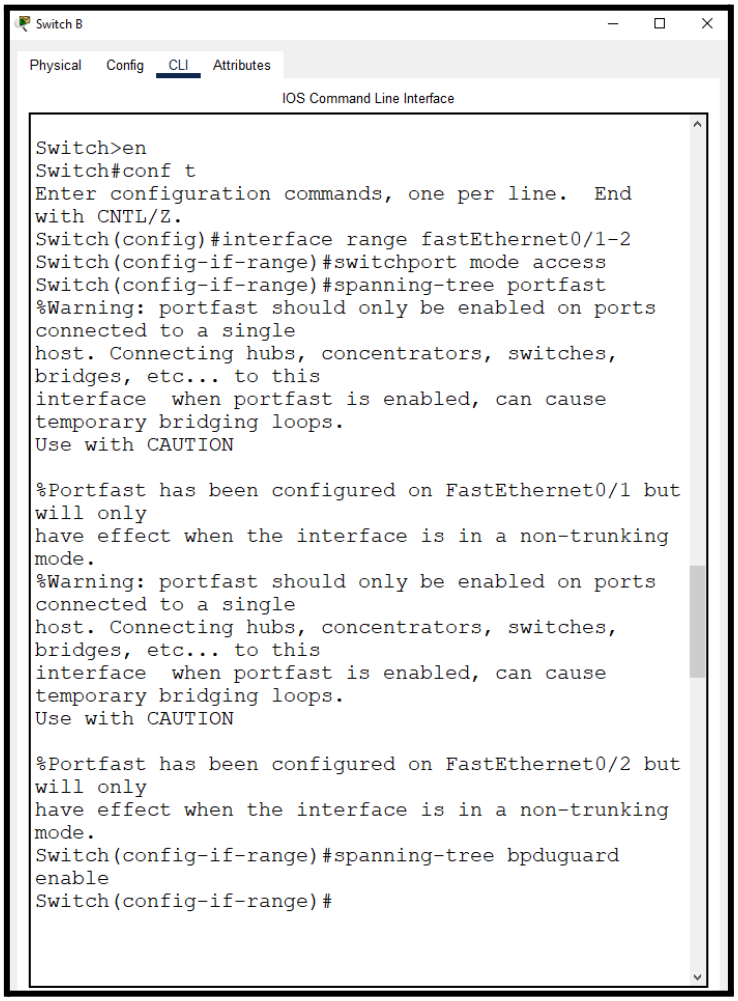
Redundant links are always welcome in switch topology as they are increasing the
network's availability and robustness.

Redundant links, if we look at them from layer 2 perspective, can cause Layer 2 loops.

Switch A Configuration

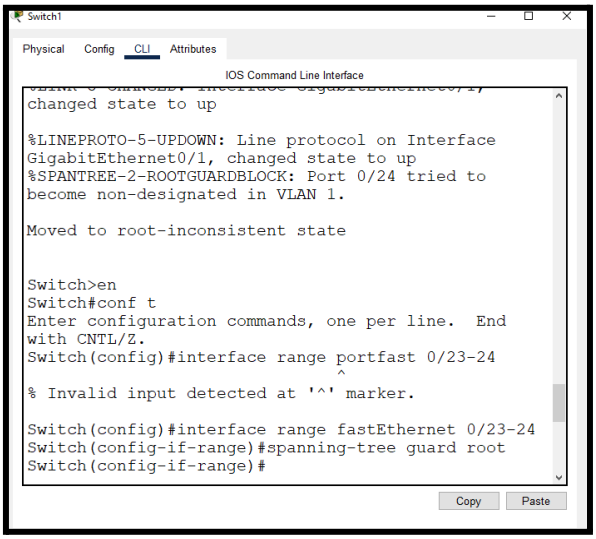


Switch B Configuration

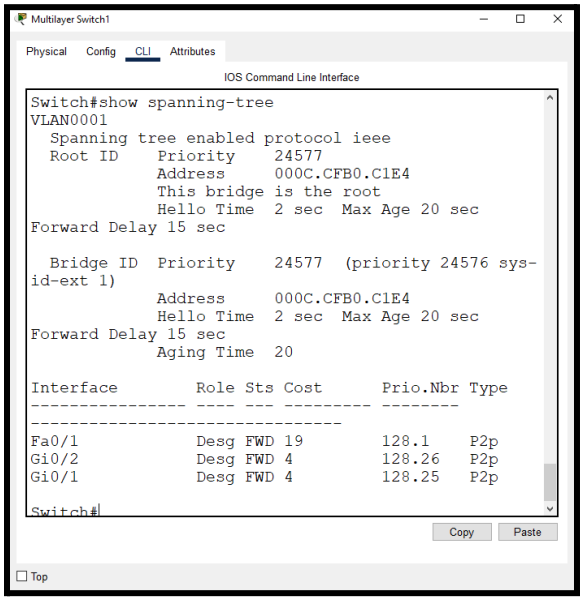


Switch 1 and Switch 2 Same command

Switch 1 and Switch 2 Configuration



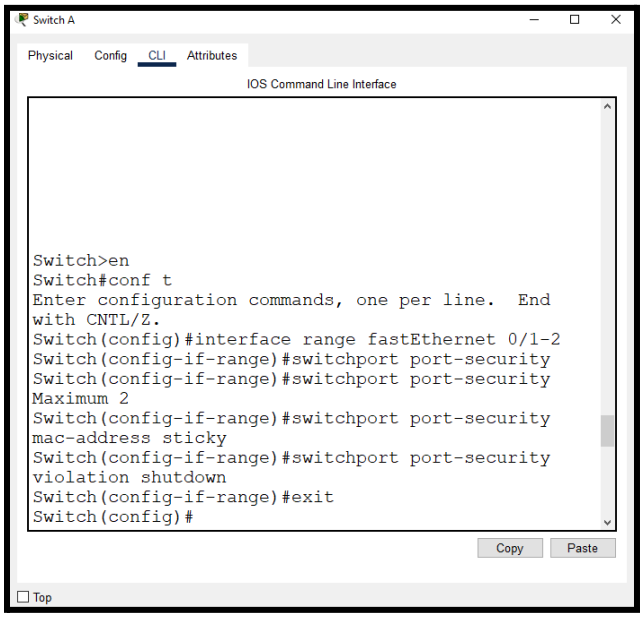
MultiLayer Switch



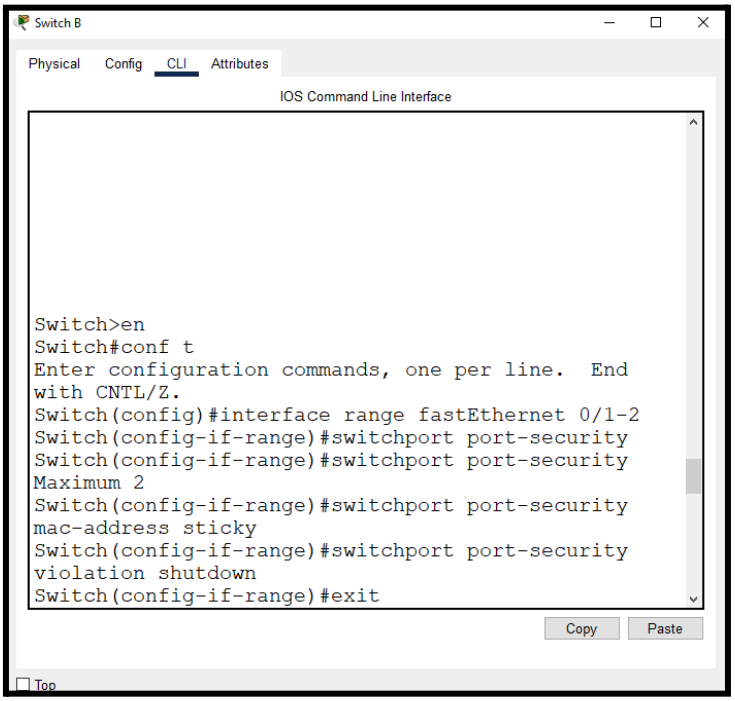
c) Enable port security to prevent CAM table overflow attacks.

Part 3 –Port Security and Disable Unused ports

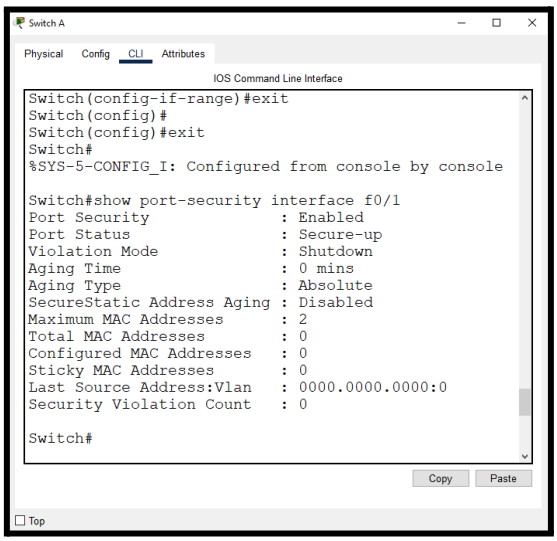
Switch A Configuration

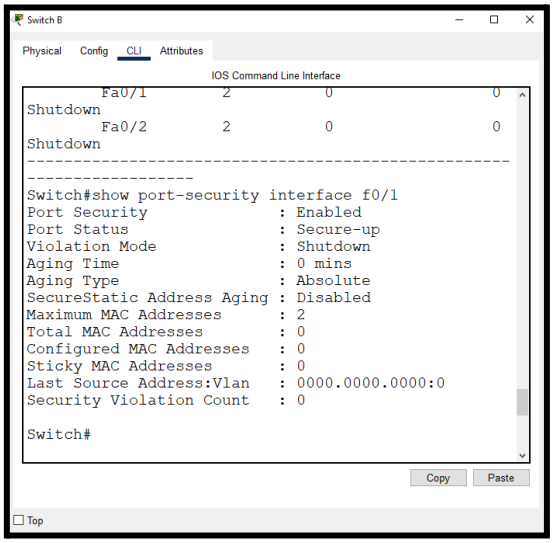


Switch B Configuration

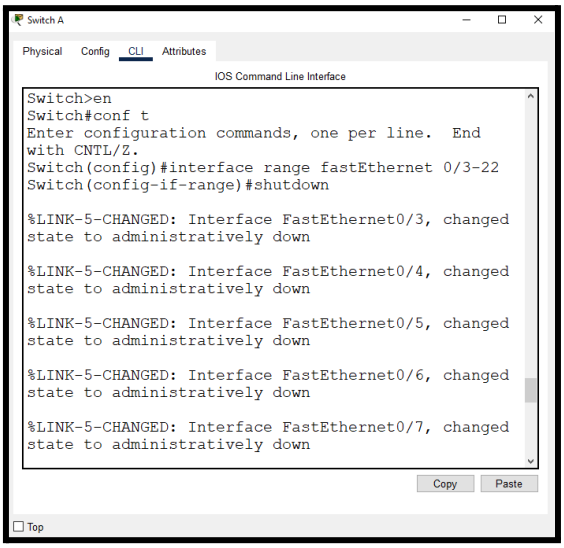


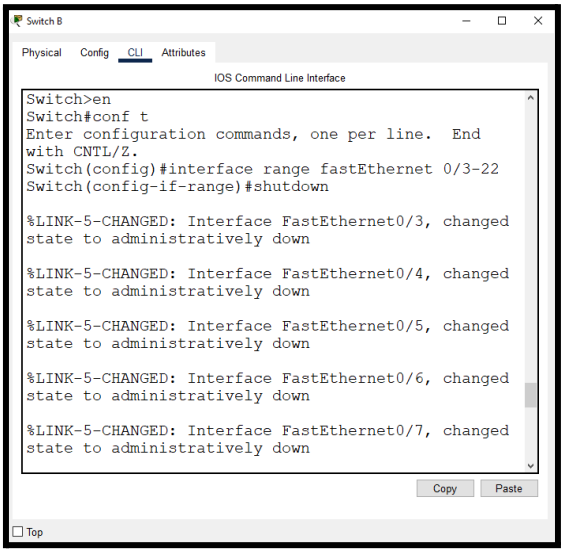
Checking whether the port security has been enabled or not on both the Switches





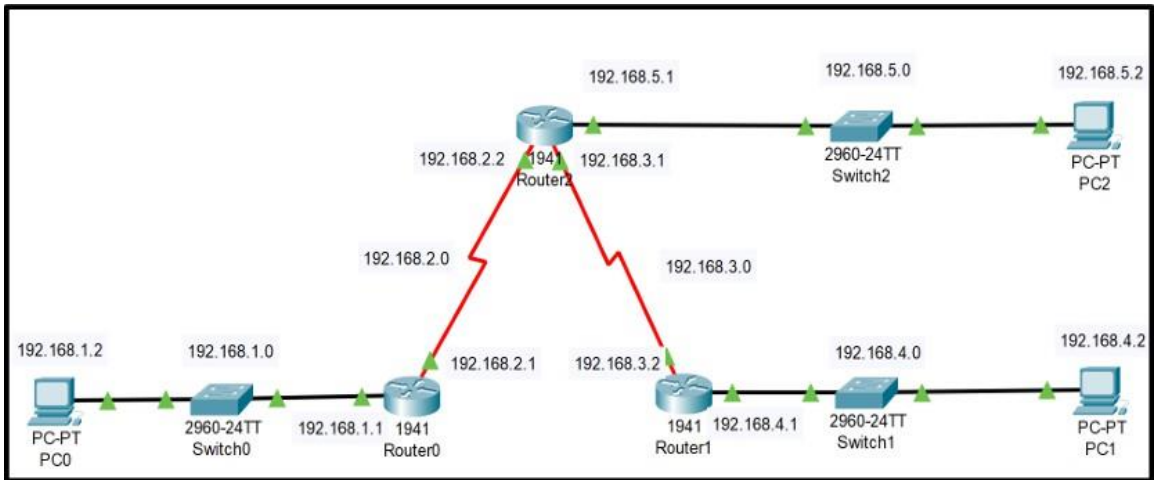
Shutting down all the unused ports



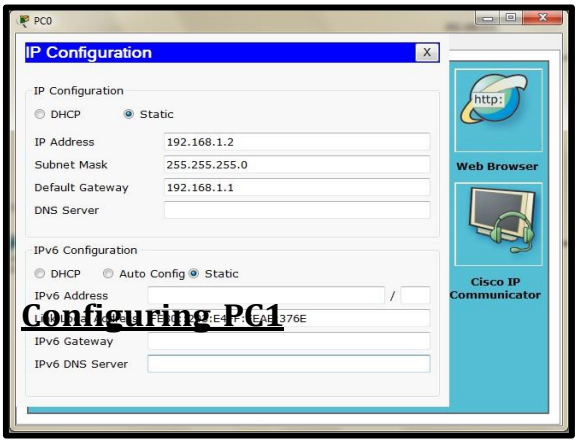


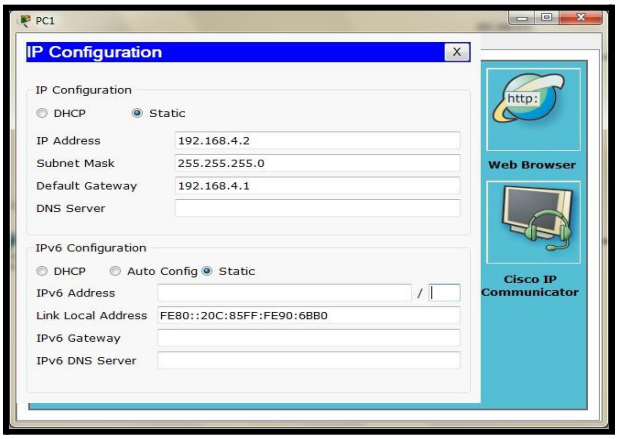
Practical

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



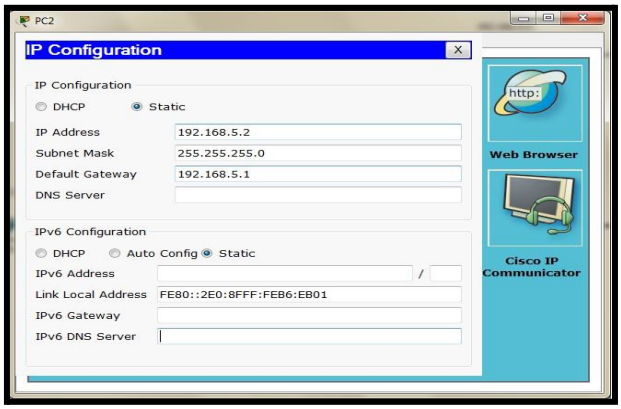
Configuring PC0 and PC1



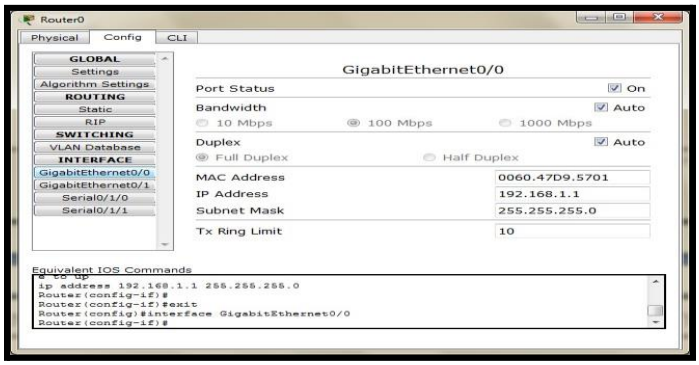


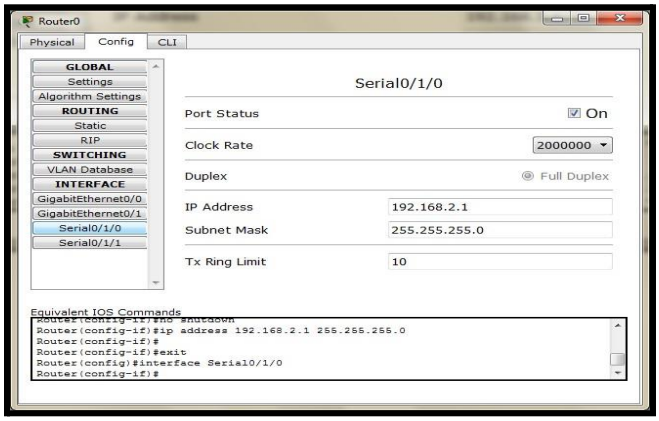
Configuring PC1

Configuring PC2

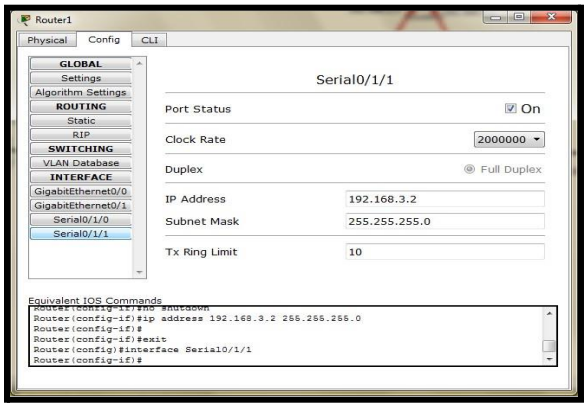


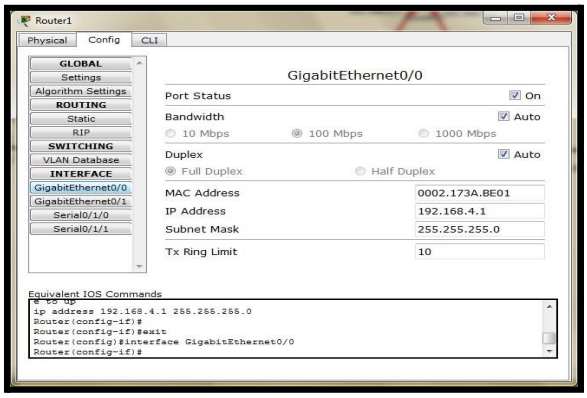
Configuring Router 0



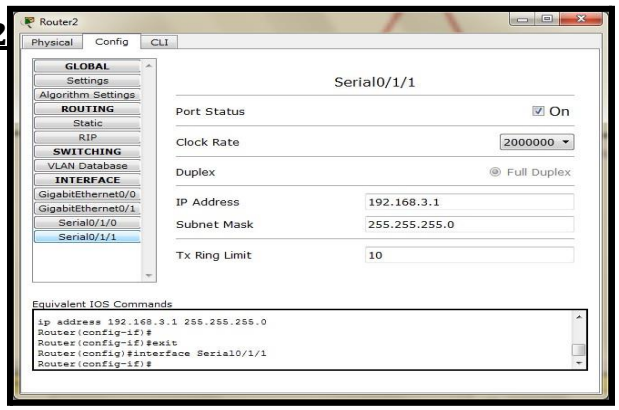


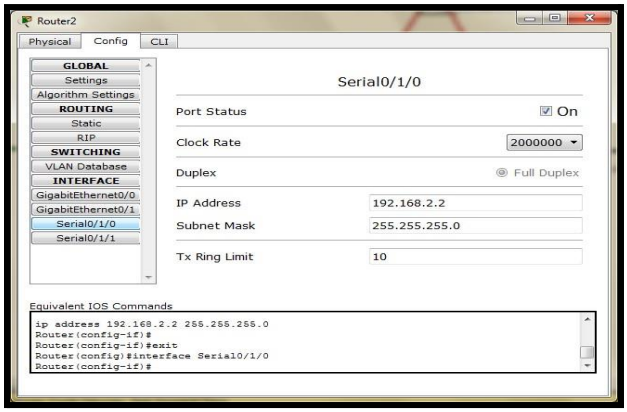
Configuring Router1

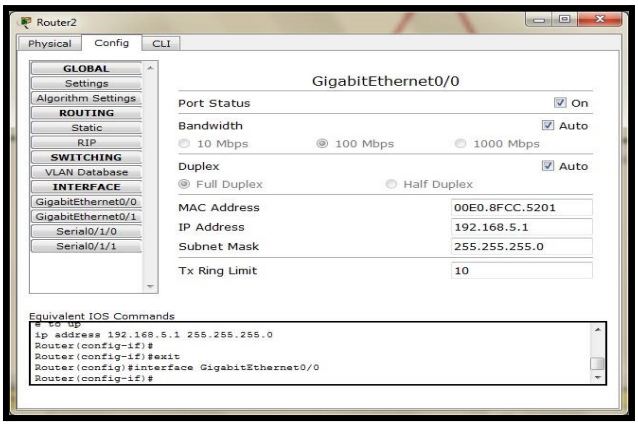




Configuring Router2

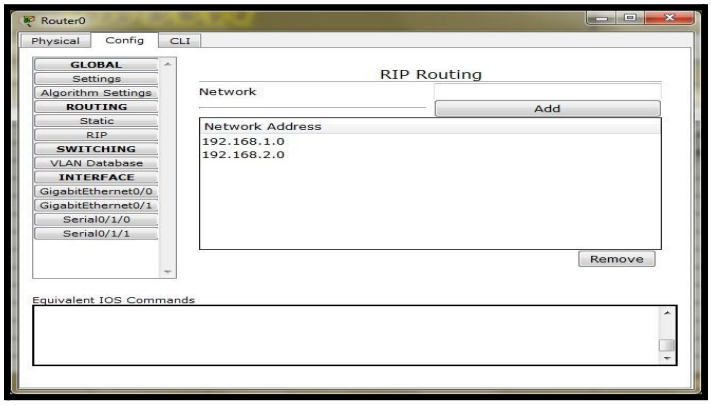




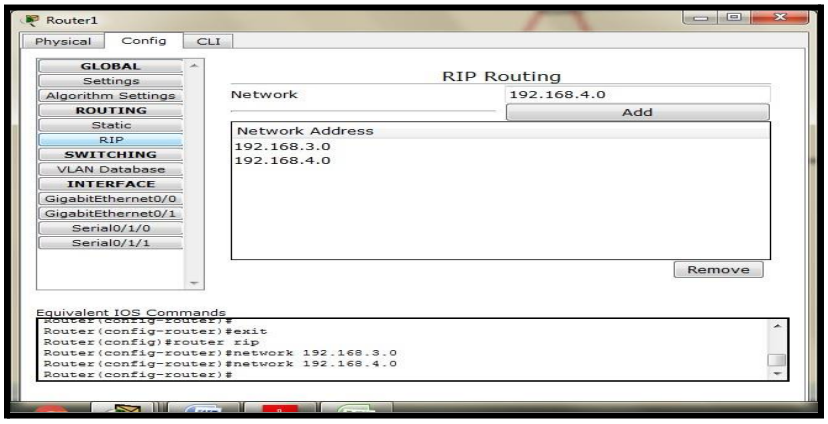


Part 1: Configuring RIP on each Router

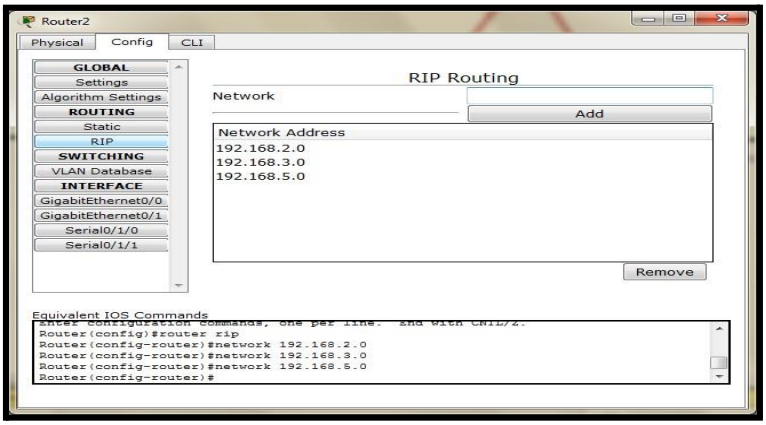
Router 0: Add the following networks



Router 1: Add the following networks

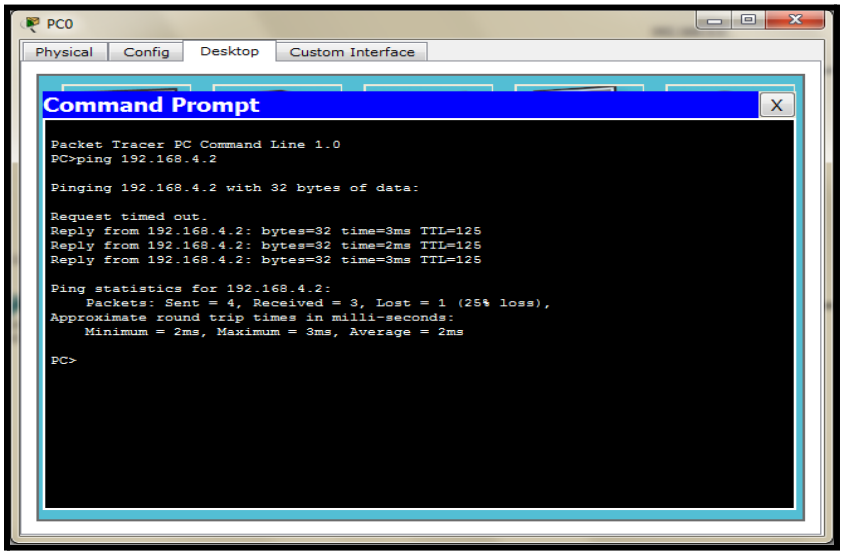


Router 2: Add the following networks

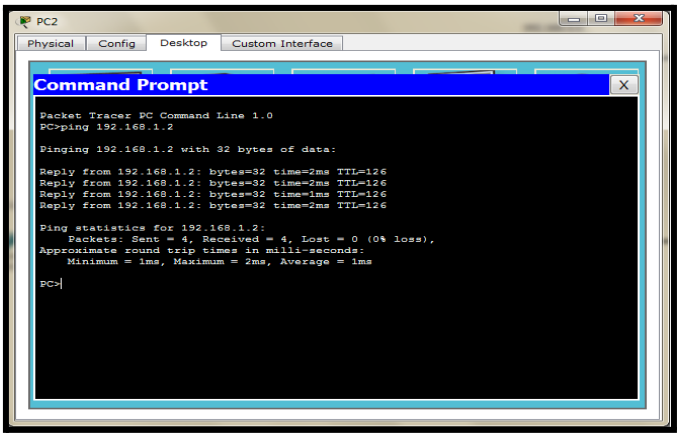


Now check the connectivity by ping command

PCO to PC1 (it should be successful)



PC2 to PC0 (it should be successful)



Part 2: Configure IPSec Parameters on Router0

In order to configure the IPSec parameters on Router0 we go by the following steps

Step 1: Enable the security package on Router0 through the following commands in CLI mode

```
Router>enable
Router#configure terminal
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#do write
Router(config)#exit
Router#reload
Router>
Router>enable
```

Now we need to check if the security package is enabled, so we type the following command

```
Router#show version
```

Step 2: Configuring IKA phase 1 ISAKMP policy on Router0

Type the following commands in the CLI mode of Router0

```
Router#configure terminal
Router(config)#access-list 110 permit ip 92.168.1.0 0.0.0.255 192.168.4.0
0.0.0.255
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key smile1234 address 192.168.3.2
Router(config)#crypto ipsec transform-set vpn-set esp-aes esp-sha-hmac
Router(config)#crypto map vpn-map 10 ipsec-isakmp
Router(config-crypto-map)#set peer 192.168.3.2
Router(config-crypto-map)#set transform-set vpn-set
Router(config-crypto-map)#match address 110
Router(config-crypto-map)#exit
Router(config)#
Router(config)#interface Serial0/1/0
```

```
Router(config-if)#crypto map vpn-map
Router(config-if)#exit
Router(config)#
```

Part 3: Configure IPSec Parameters on Router1

In order to configure the IPSec parameters on Router1 we go by the following steps

Step 1: Enable the security package on Router1 through the following commands in CLI mode

```
Router>enable
Router#configure terminal
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#do write
Router(config)#exit
Router#reload
Router>
Router>enable
```

Now we need to check if the security package is enabled, so we type the following command

```
Router#show version
```

Step 2: Configuring IKA phase 1 ISAKMP policy on Router1

In order to configure the IPSec parameters on Router1 we go by the following steps

```
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 permit ip 192.168.4.0 0.0.0.255 192.168.1.0
0.0.0.255
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
```

Router(config)#crypto isakmp key smile1234 address 192.168.2.1
Router(config)#crypto ipsec transform-set vpn-set esp-aes esp-sha-hmac
Router(config)#crypto map vpn-set 10 ipsec-isakmp
Router(config-crypto-map)#description vpn
Router(config-crypto-map)#set peer 192.168.2.1
Router(config-crypto-map)#set transform-set vpn-set
Router(config-crypto-map)#match address 110
Router(config-crypto-map)#exit
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#crypto map vpn-set
Router(config-if)#

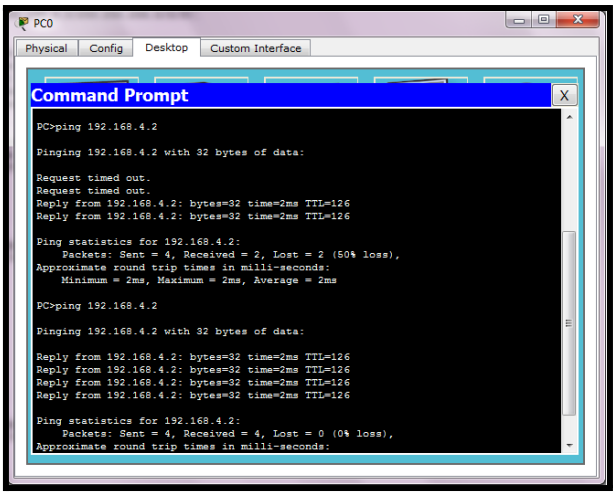
Part 4: Verify the IPSec VPN

Step 1: Type the following command in the CLI mode of Router0

Router>
Router>EN
Router>enable
Router#show crypto ipsec sa

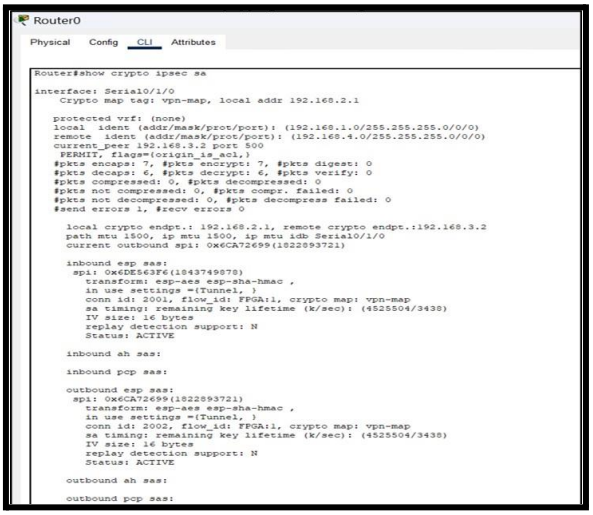
Step 2: Ping PC1 from PC0 (Creating interesting tra c)

We ping PC1 from PC0 (which is the interesting tra c)



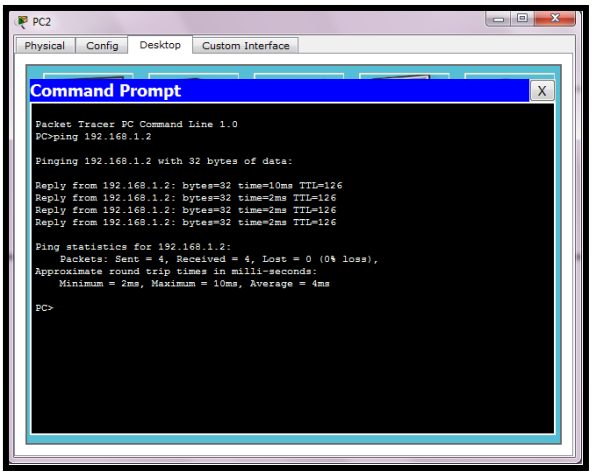
And now we check the Router0 by typing the following Command

Router#show crypto ipsec sa

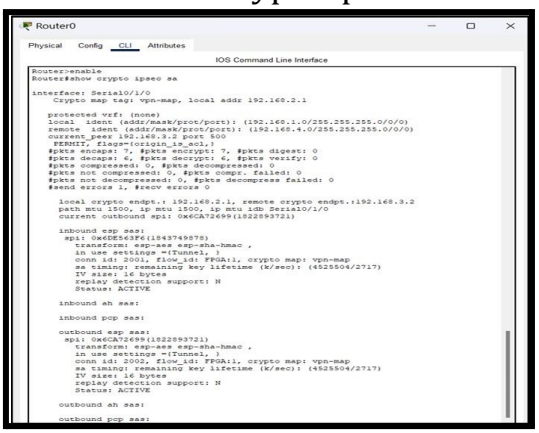


Step 3: Ping PC1 from PC0 (Creating another interesting tra c)

Now we ping PC0 from PC0 (which is interesting tra c)

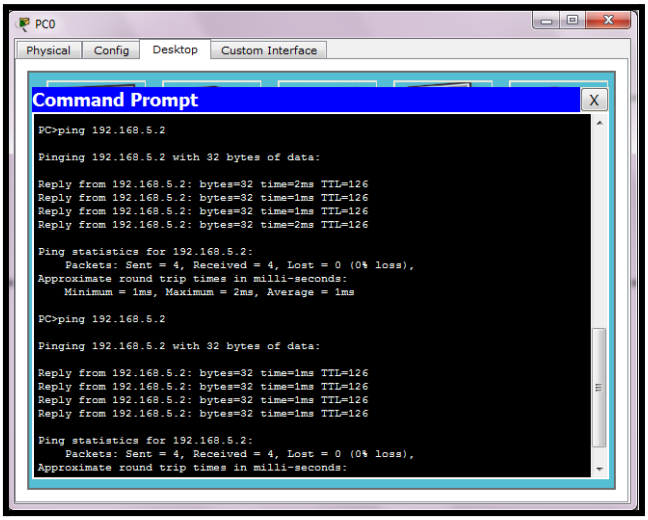


And now we check the Router0 by typing the following Command
Router#show crypto ipsec sa



Step 4: Ping PC2 from PC0 (Creating NON interesting tra c)

Now we ping PC2 from PC0 (Not interesting tra c)



And now we check the Router0 by typing the following Command

Router#show crypto ipsec sa