Practical 1

AIM: Configure Routers

a. OSPF MD5 authentication.

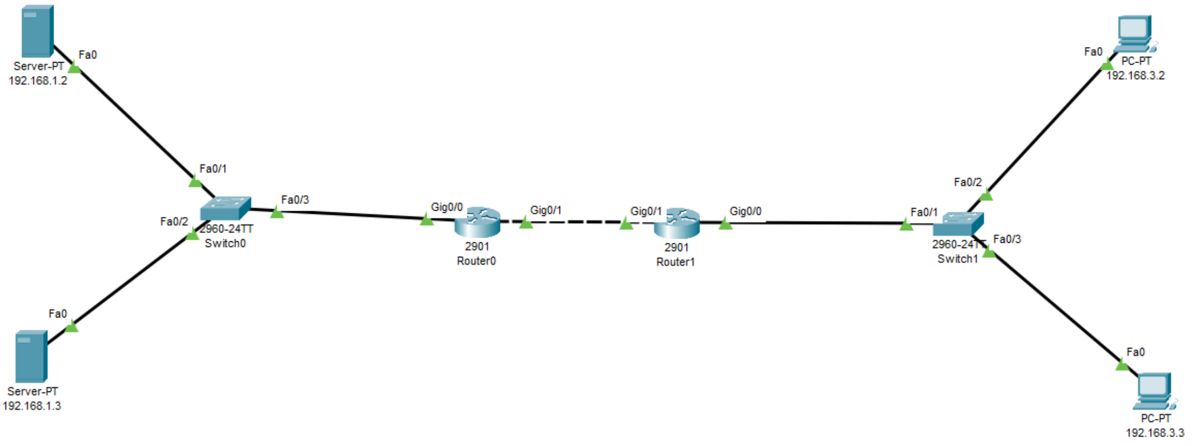
b. NTP.

c. to log messages to the syslog server.

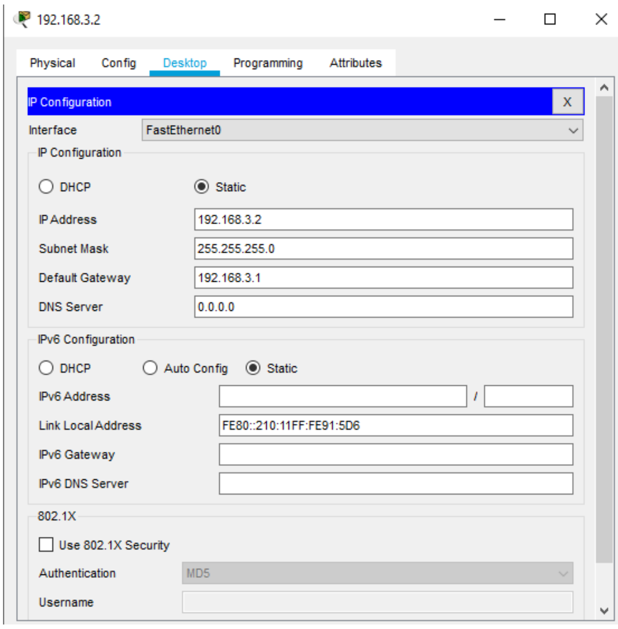
d. to support SSH connections.

Solution:

<u>Topology</u>



Pc Configuration



192.168.3.2

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.3.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::210:11FF:FE91:5D6

IPv6 Gateway:

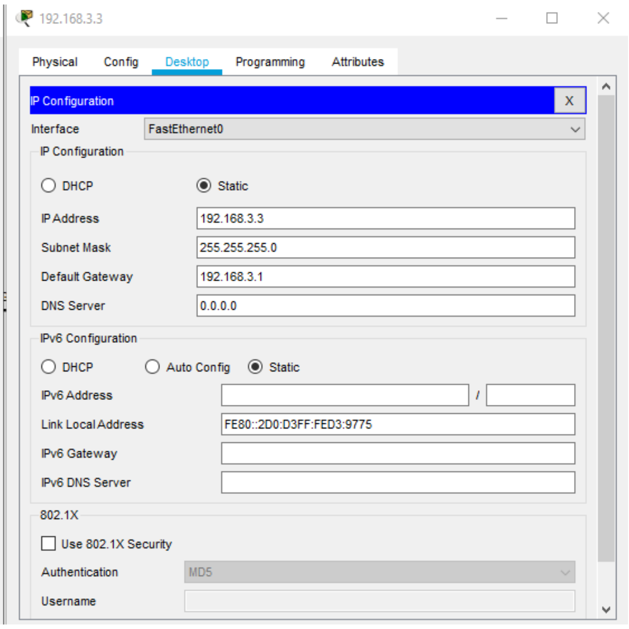
IPv6 DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:



192.168.3.3

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.3.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:D3FF:FED3:9775

IPv6 Gateway:

IPv6 DNS Server:

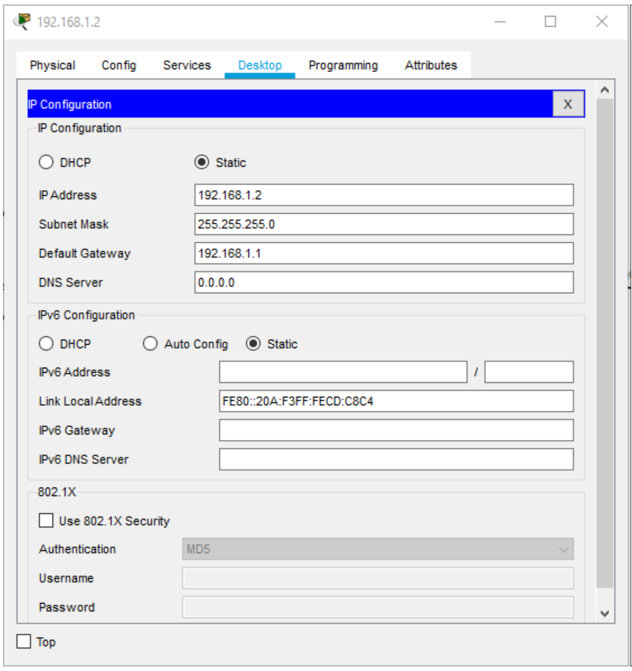
802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Server 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::20A:F3FF:FECD:C8C4

IPv6 Gateway:

IPv6 DNS Server:

802.1X

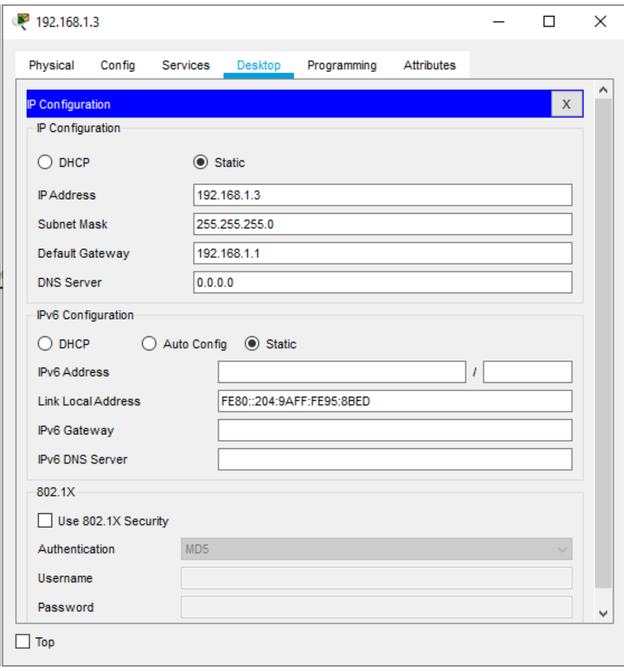
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

□ Top



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::204:9AFF:FE95:8BED

IPv6 Gateway:

IPv6 DNS Server:

802.1X

□ Use 802.1X Security

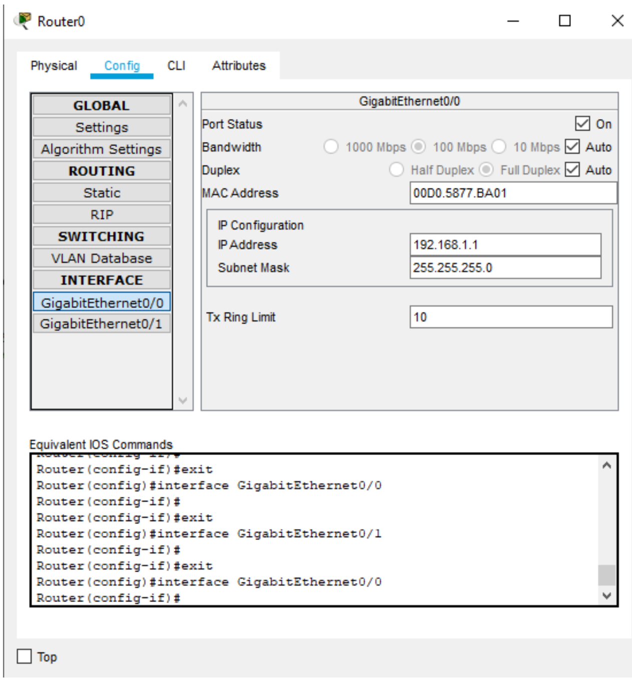
Authentication: MD5

Username:

Password:

□ Top

Router configurations



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 00D0.5877.BA01

IP Configuration

IP Address: 192.168.1.1

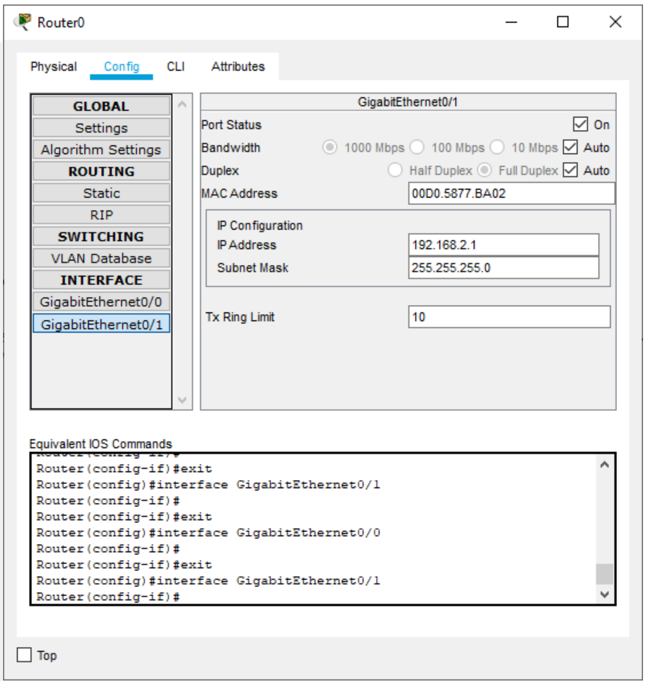
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```

□ Top



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 00D0.5877.BA02

IP Configuration

IP Address: 192.168.2.1

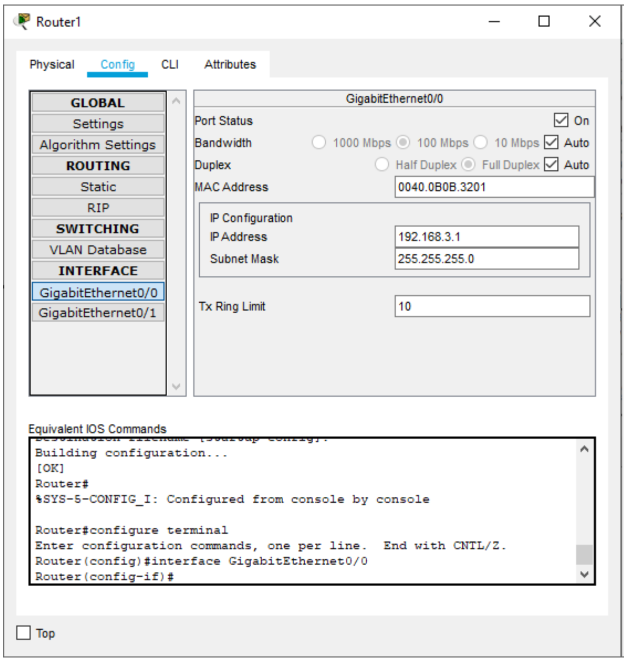
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

□ Top



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0040.0B0B.3201

IP Configuration

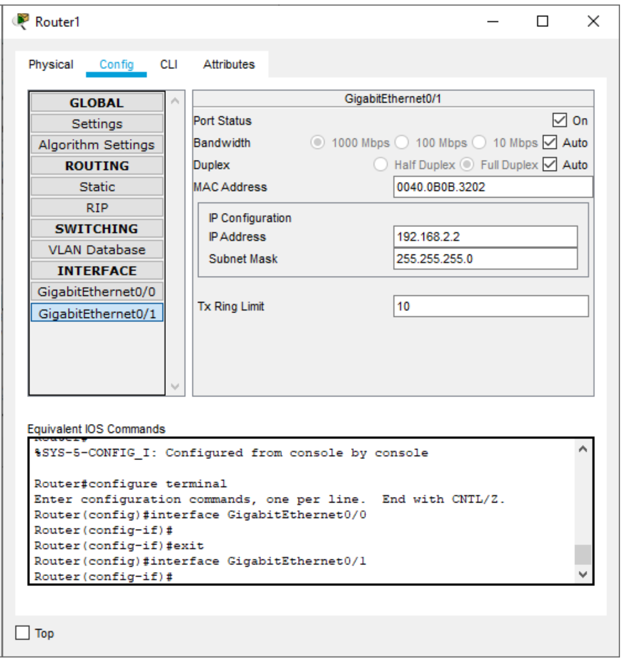
IP Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0040.0B0B.3202

IP Configuration

IP Address 192.168.2.2

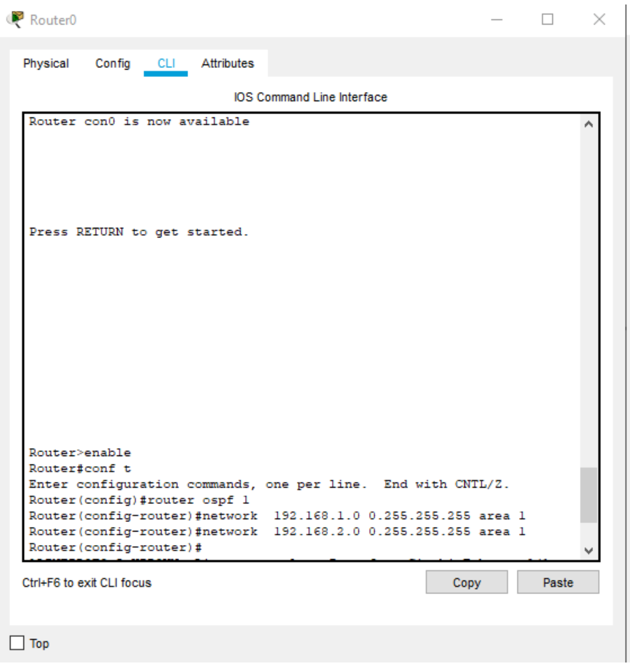
Subnet Mask 255.255.255.0

Tx Ring Limit 10

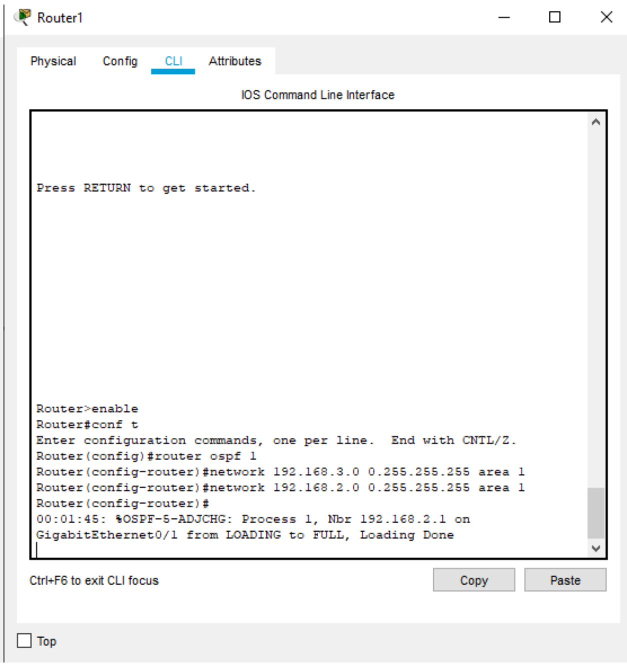
Equivalent IOS Commands

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

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)#
```

OSPF and MD5 authentication



```
Router con0 is now available



Press RETURN to get started.









Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network  192.168.1.0 0.255.255.255 area 1
Router(config-router)#network  192.168.2.0 0.255.255.255 area 1
Router(config-router)#
```



```
Press RETURN to get started.









Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#
00:01:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done
```

Commands for ospf configuration

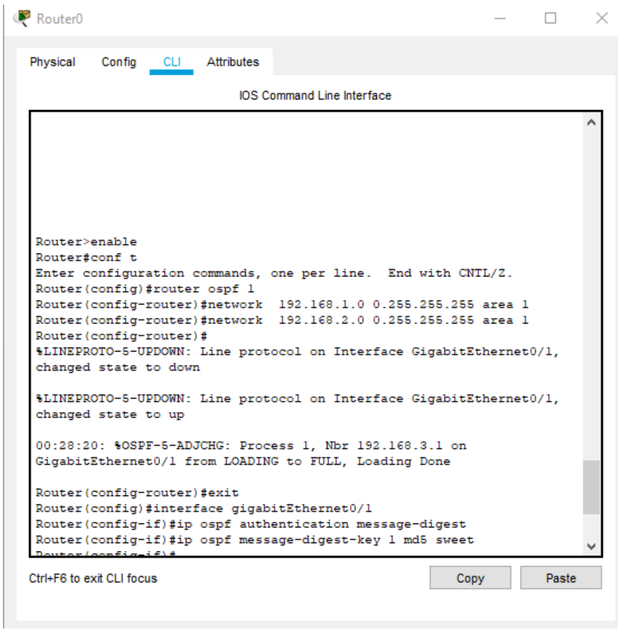
Router 0:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
```

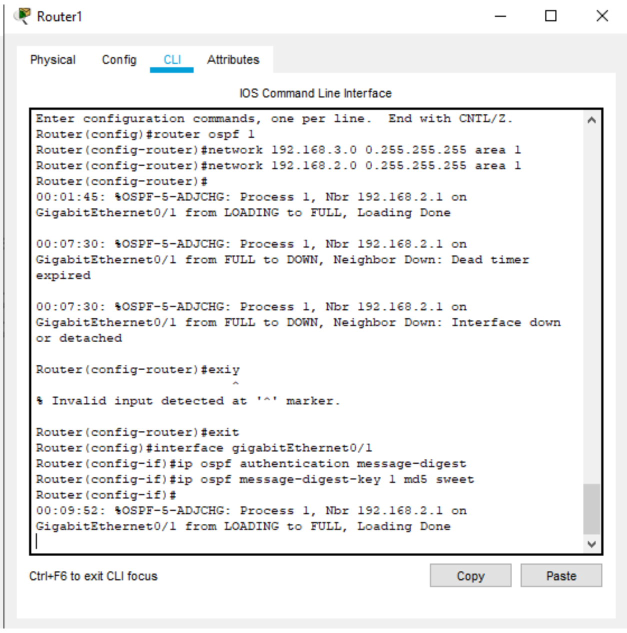
Router 1:

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
```

MD5 authentication commands



```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network  192.168.1.0 0.255.255.255 area 1
Router(config-router)#network  192.168.2.0 0.255.255.255 area 1
Router(config-router)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

00:28:20: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done

Router(config-router)#exit
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 sweet
Router(config-if)#
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#
00:01:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done

00:07:30: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired

00:07:30: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
GigabitEthernet0/1 from FULL to DOWN, Neighbor Down: Interface down
or detached

Router(config-router)#exiy
                         ^
% Invalid input detected at '^' marker.

Router(config-router)#exit
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 sweet
Router(config-if)#
00:09:52: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done
```

Commands for router 0:

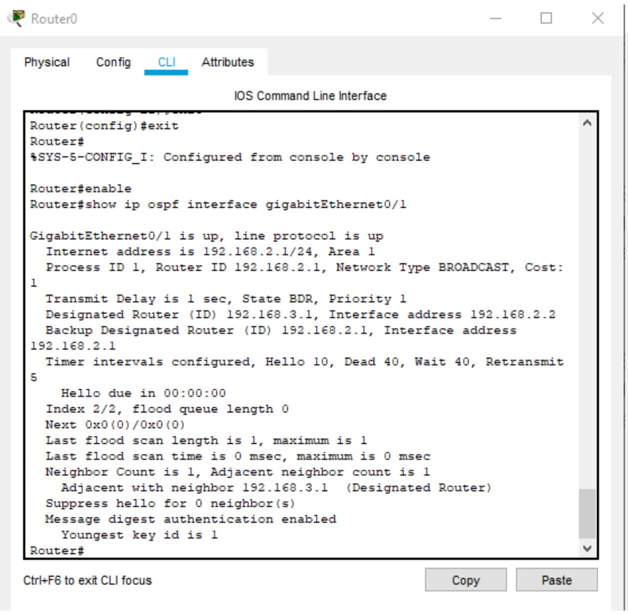
```
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 sweet
```

Commands for router 1:

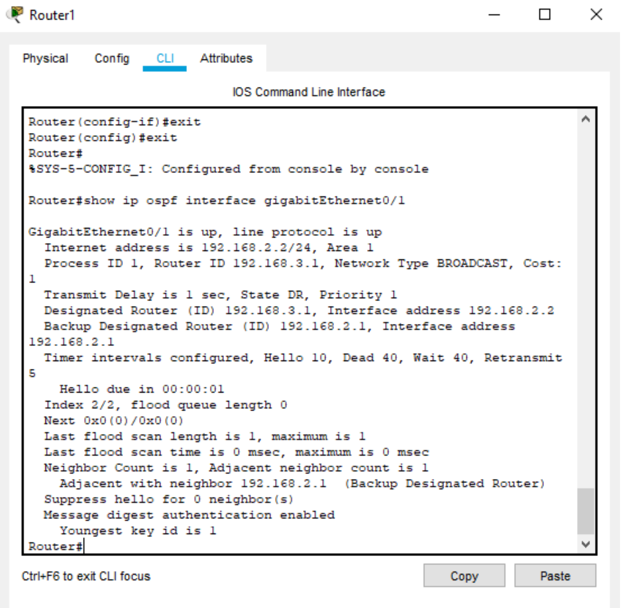
```
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 sweet
```

Verifying configuration

Command: `show ip ospf interface gigabitEthernet0/1`

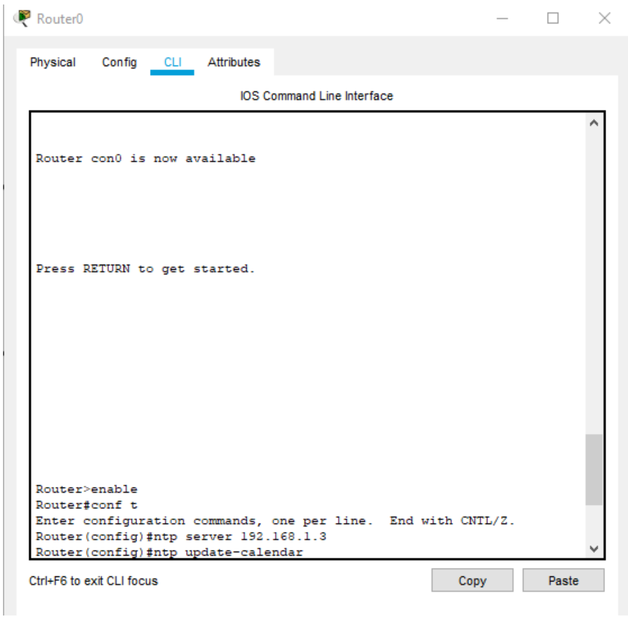


```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#enable
Router#show ip ospf interface gigabitEthernet0/1

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.2.1/24, Area 1
  Process ID 1, Router ID 192.168.2.1, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2
  Backup Designated Router (ID) 192.168.2.1, Interface address
192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.3.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Router#
```

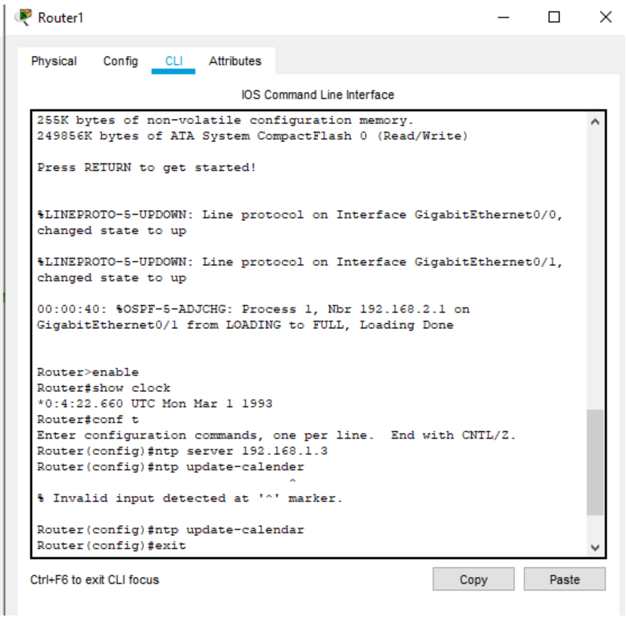


```
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip ospf interface gigabitEthernet0/1

GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.2.2/24, Area 1
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2
  Backup Designated Router (ID) 192.168.2.1, Interface address
192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Router#
```

NTP configuration



```


Router con0 is now available






Press RETURN to get started.













Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ntp server 192.168.1.3
Router(config)#ntp update-calendar
```



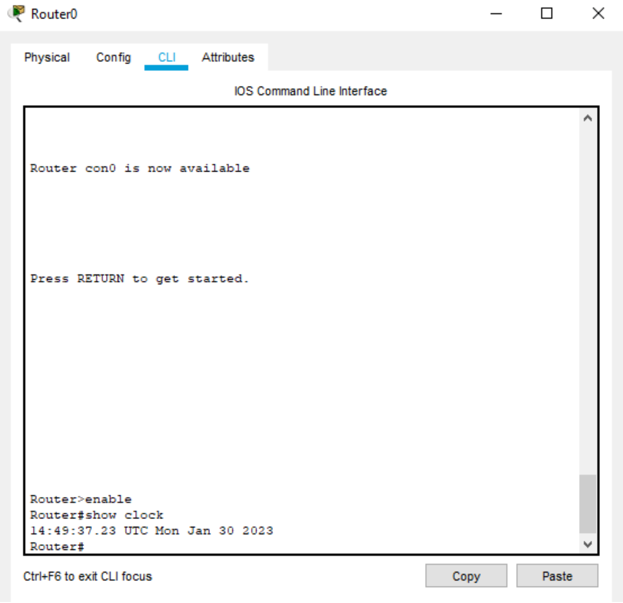
```
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


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

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

00:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
GigabitEthernet0/1 from LOADING to FULL, Loading Done


Router>enable
Router#show clock
*0:4:22.660 UTC Mon Mar 1 1993
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ntp server 192.168.1.3
Router(config)#ntp update-calender
                                   ^
% Invalid input detected at '^' marker.

Router(config)#ntp update-calendar
Router(config)#exit
```

Commands (for both routers):

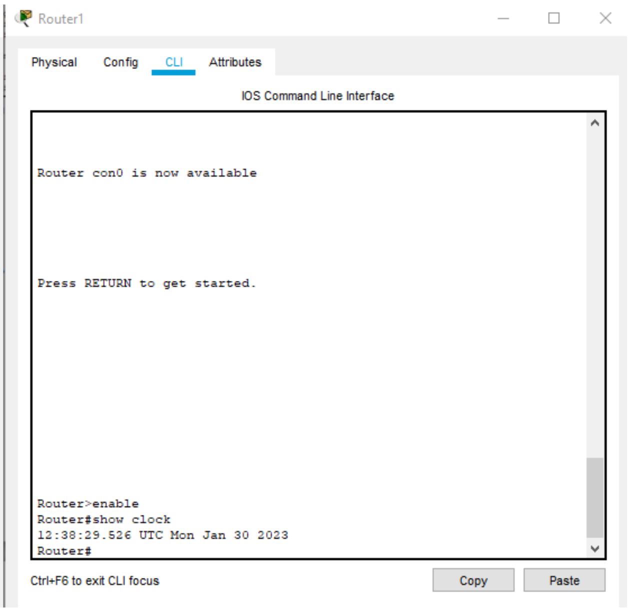
```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.1.3
Router(config)#ntp update-calendar
```

Turn off all services in server (192.168.1.3) except NTP

OUTPUT:



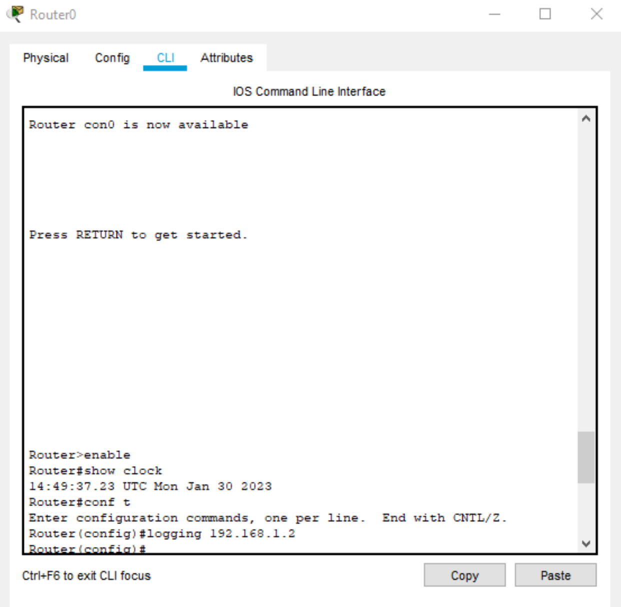
```
Router con0 is now available



Press RETURN to get started.









Router>enable
Router#show clock
14:49:37.23 UTC Mon Jan 30 2023
Router#
```



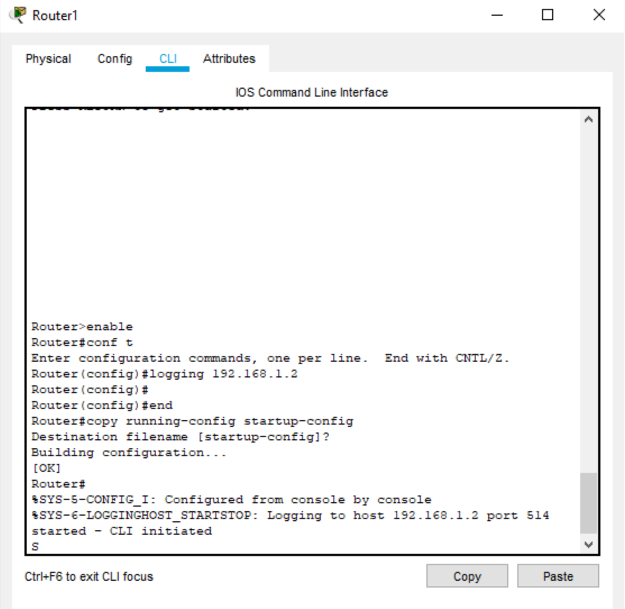
```
Router con0 is now available



Press RETURN to get started.









Router>enable
Router#show clock
12:38:29.526 UTC Mon Jan 30 2023
Router#
```

Syslog services

Turn off all services in server (192.168.1.2) except syslog



```
Router con0 is now available



Press RETURN to get started.









Router>enable
Router#show clock
14:49:37.23 UTC Mon Jan 30 2023
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging 192.168.1.2
Router(config)#
```

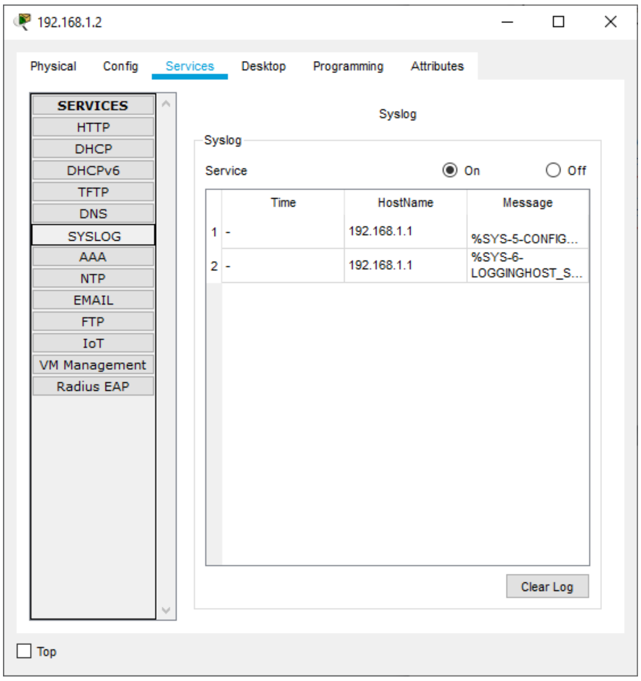


```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging 192.168.1.2
Router(config)#
Router(config)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.2 port 514
started - CLI initiated
S
```

Commands

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#logging 192.168.1.2
```

OUTPUT



Syslog

Syslog

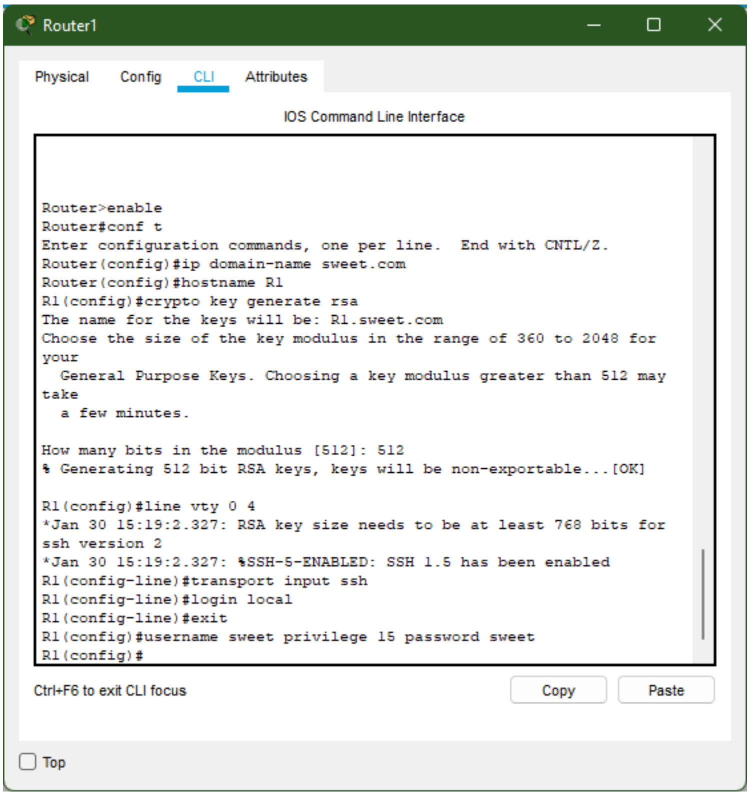
Service ● On ○ Off

	Time	HostName	Message
1	-	192.168.1.1	%SYS-5-CONFIG...
2	-	192.168.1.1	%SYS-6- LOGGINGHOST_S...

SSH

Type following commands in Router1:

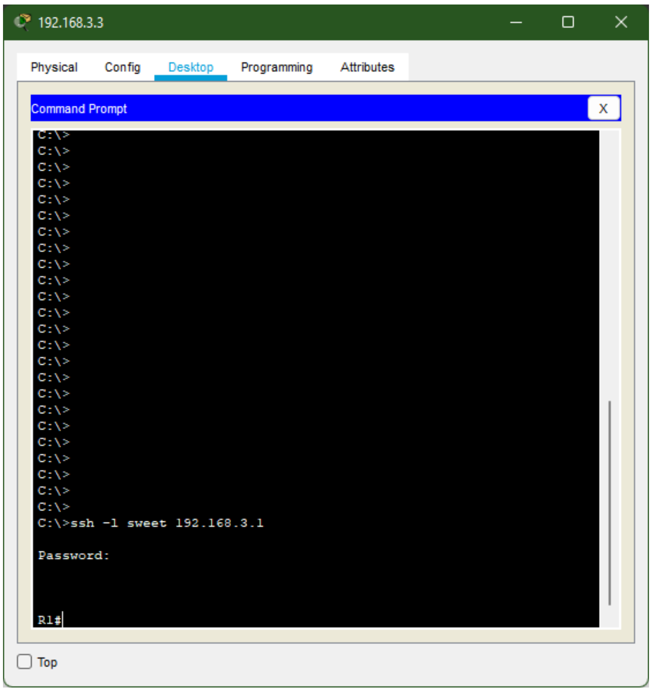
```
enable
conf t
ip domain-name sweet.com
hostname R1
line vty 0 4
transport input ssh
login local
exit
username sweet privilege 15 password sweet
```



```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip domain-name sweet.com
Router(config)#hostname R1
R1(config)#crypto key generate rsa
The name for the keys will be: R1.sweet.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]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#line vty 0 4
*Jan 30 15:19:2.327: RSA key size needs to be at least 768 bits for
ssh version 2
*Jan 30 15:19:2.327: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#username sweet privilege 15 password sweet
R1(config)#
```

Now open cmd of PC and type following command:

`Ssh -l sweet 192.168.3.1`



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

Password:



R1#
```

Hence SSH is verified.

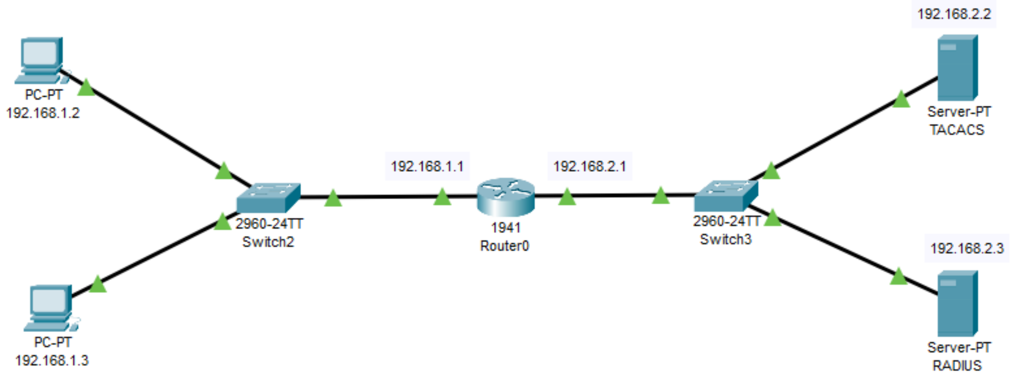
Practical 2

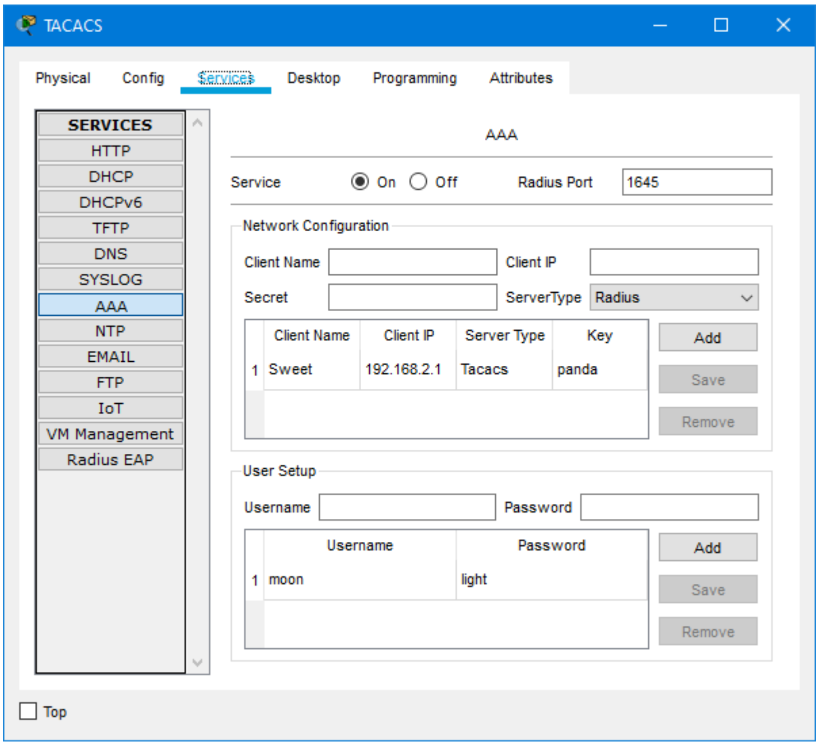
AIM: Configure AAA Authentication

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

Solution:

Topology





AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

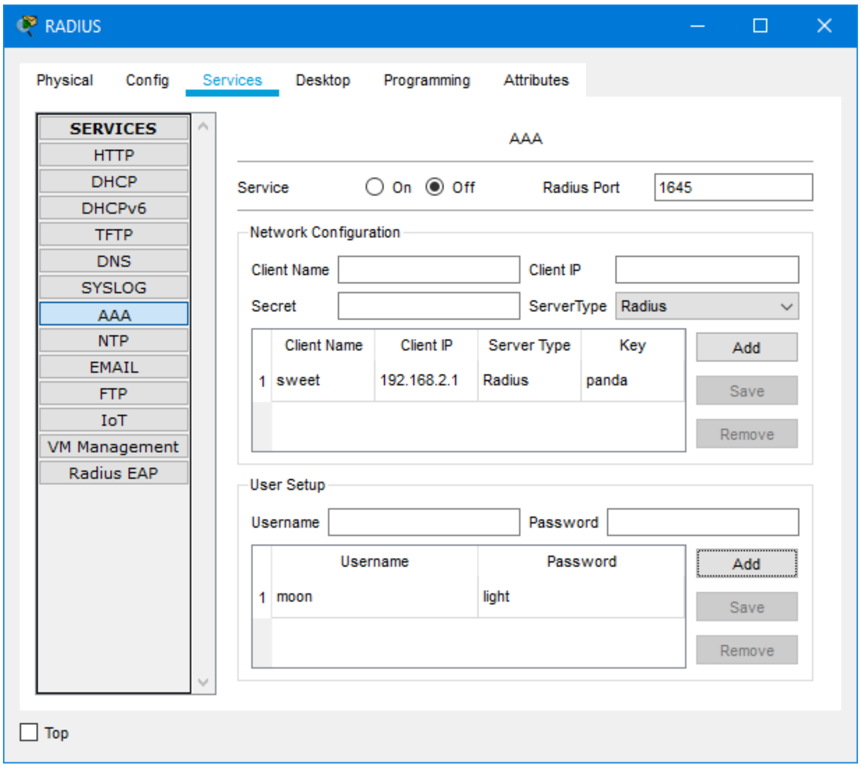
Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	Sweet	192.168.2.1	Tacacs	panda

User Setup

Username Password

	Username	Password
1	moon	light



AAA

Service ○ On ● Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

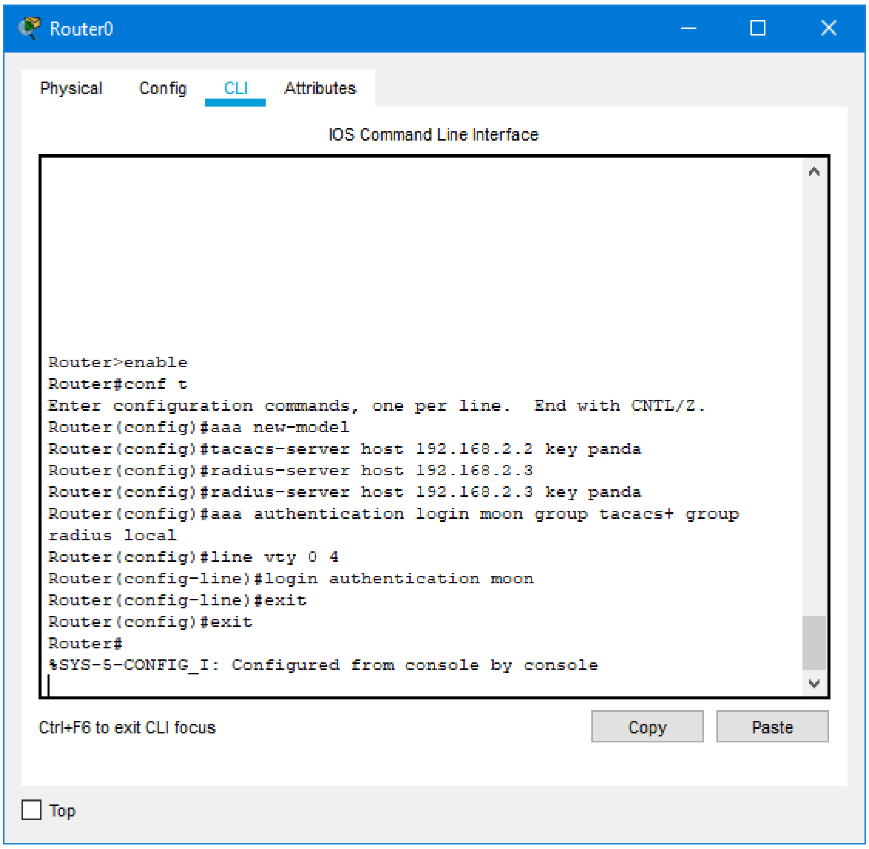
	Client Name	Client IP	Server Type	Key
1	sweet	192.168.2.1	Radius	panda

User Setup

Username Password

	Username	Password
1	moon	light

Router configuration (CLI)



IOS Command Line Interface

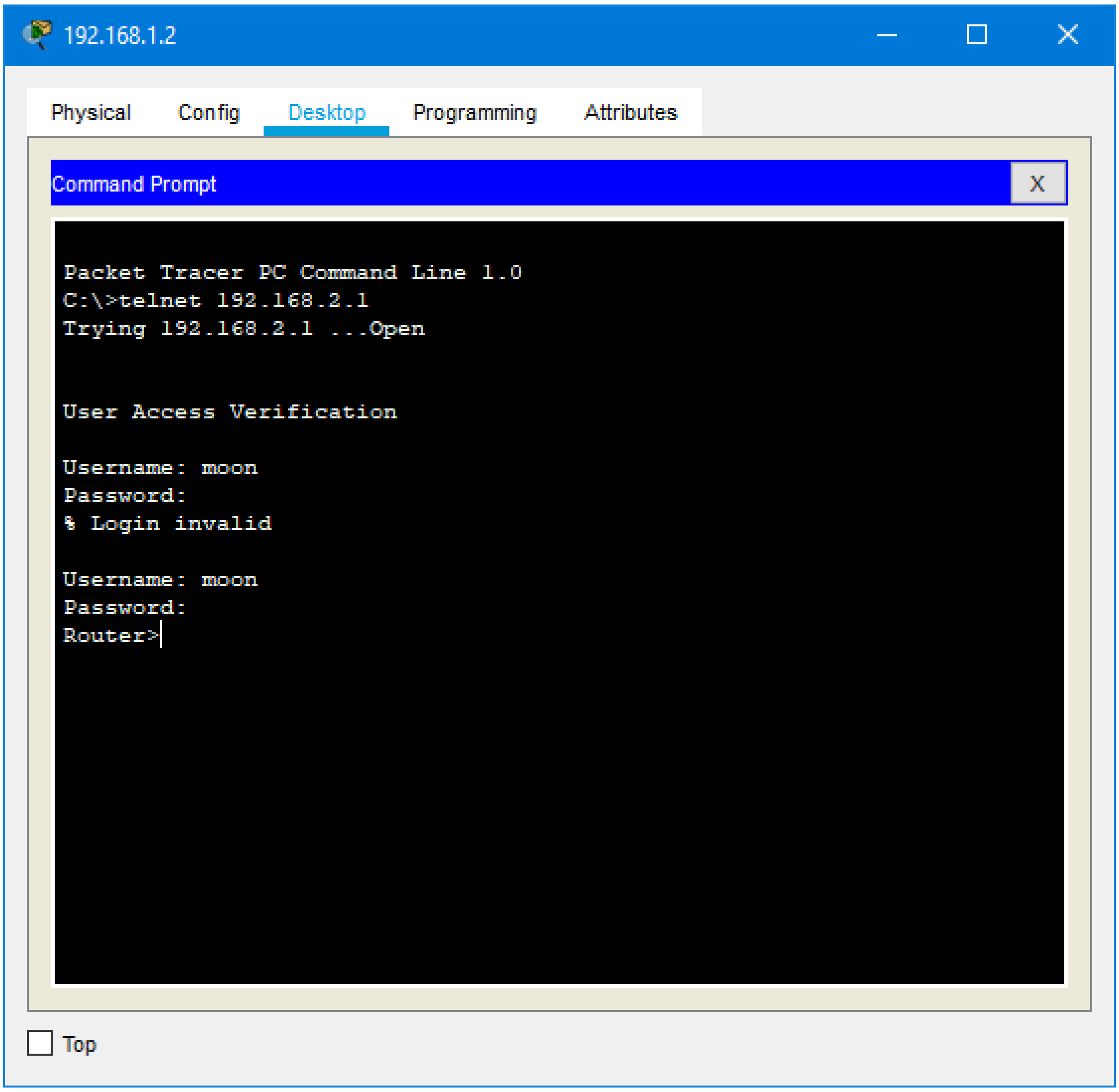
```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.2.2 key panda
Router(config)#radius-server host 192.168.2.3
Router(config)#radius-server host 192.168.2.3 key panda
Router(config)#aaa authentication login moon group tacacs+ group
radius local
Router(config)#line vty 0 4
Router(config-line)#login authentication moon
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Commands:

```
Router>enable
Router#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.2.2 key panda
Router(config)#radius-server host 192.168.2.3 key panda
Router(config)#aaa authentication login moon group tacacs+ group radius
local
Router(config)#line vty 0 4
Router(config-line)#login authentication moon
Router(config-line)#exit
Router(config)#exit
```

Verifying using pc:

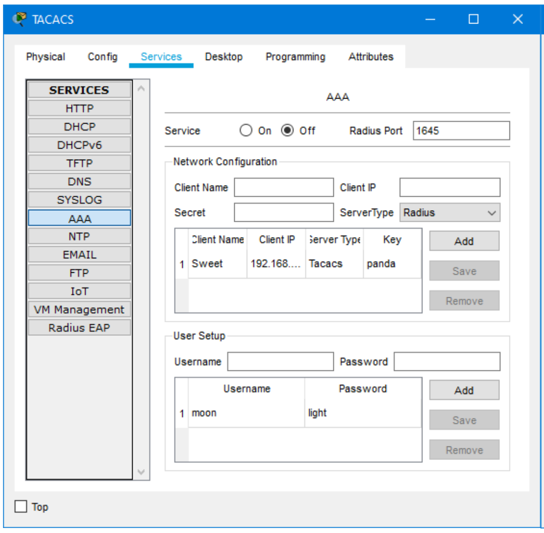


```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open


User Access Verification

Username: moon
Password:
% Login invalid

Username: moon
Password:
Router>
```

Commands

`telnet 192.168.2.1`

To verify RADIUS, go to tacacs server and turn off the AAA service and turn on AAA service from RADIUS server



TACACS

Services — AAA

Service ○ On ● Off Radius Port 1645

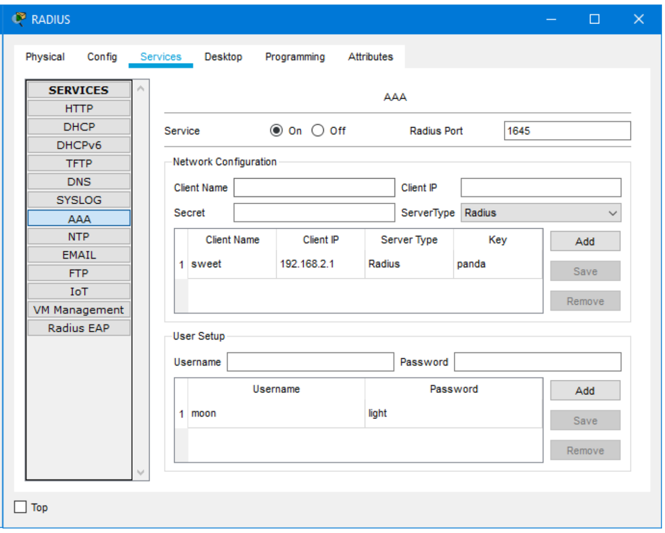
Network Configuration

ServerType Radius

	Client Name	Client IP	Server Type	Key
1	Sweet	192.168....	Tacacs	panda

User Setup

	Username	Password
1	moon	light



RADIUS

Services — AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

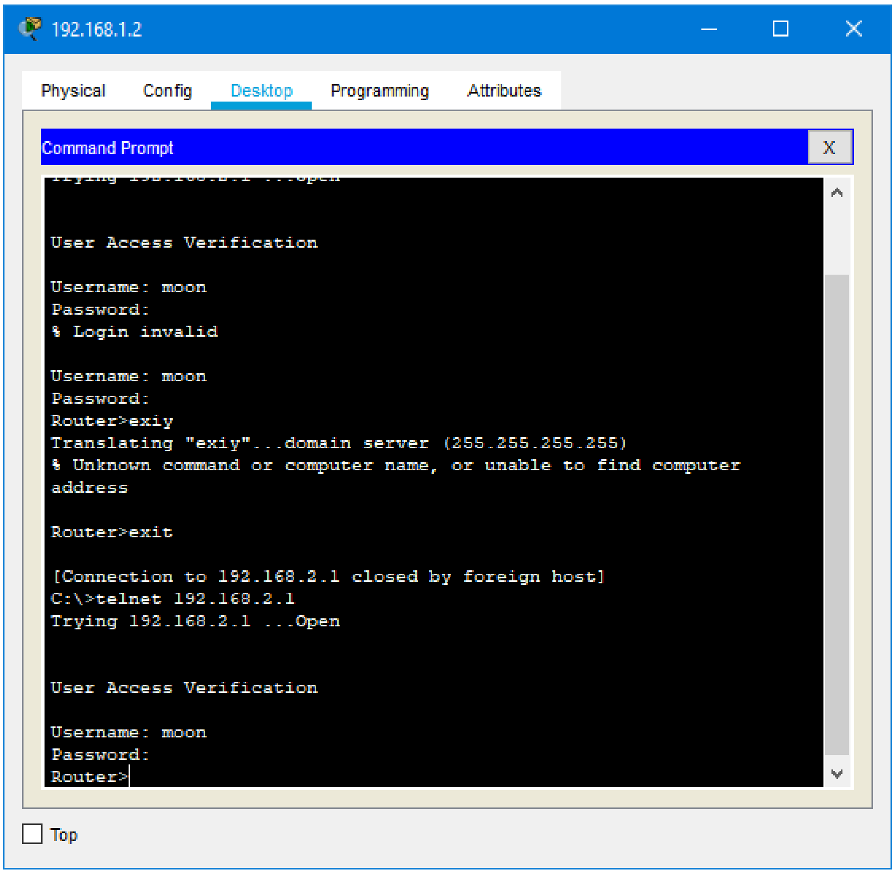
ServerType Radius

	Client Name	Client IP	Server Type	Key
1	sweet	192.168.2.1	Radius	panda

User Setup

	Username	Password
1	moon	light

Verification using pc



```
Trying 192.168.2.1 ...Open


User Access Verification

Username: moon
Password:
% Login invalid

Username: moon
Password:
Router>exiy
Translating "exiy"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address

Router>exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open


User Access Verification

Username: moon
Password:
Router>
```

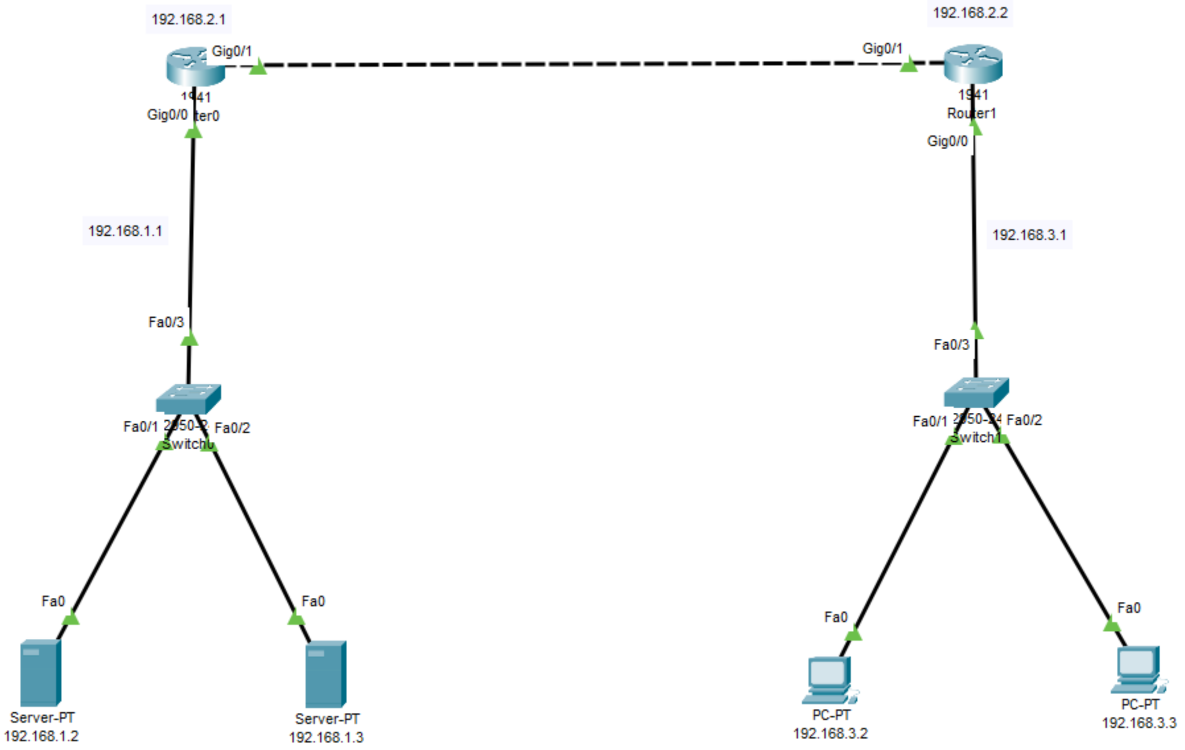
Practical 3

AIM: Configuring Extended ACLs

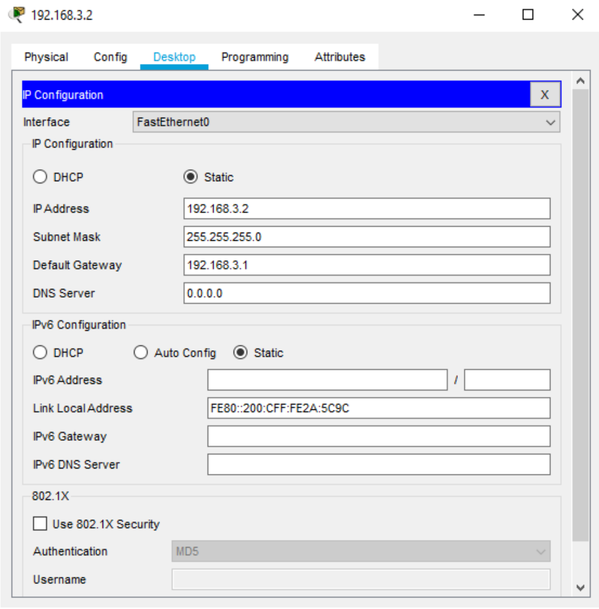
a. Configure, Apply and Verify an Extended Numbered ACL

Solution:

Topology



PC Configurations



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.3.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::200:CFF:FE2A:5C9C

IPv6 Gateway:

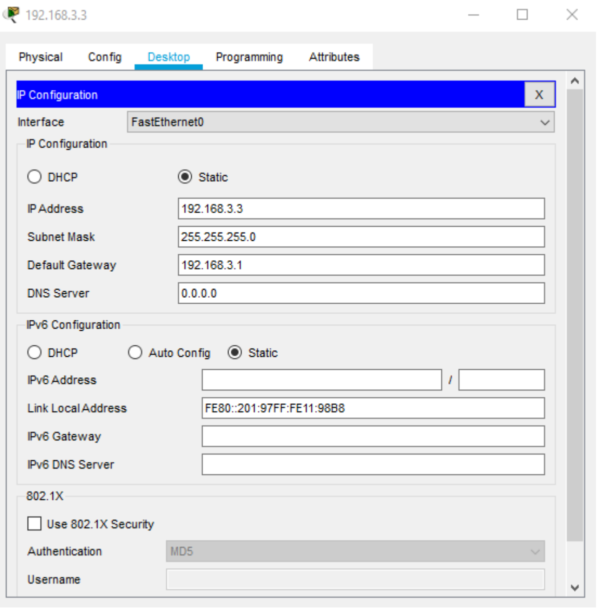
IPv6 DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 192.168.3.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::201:97FF:FE11:98B8

IPv6 Gateway:

IPv6 DNS Server:

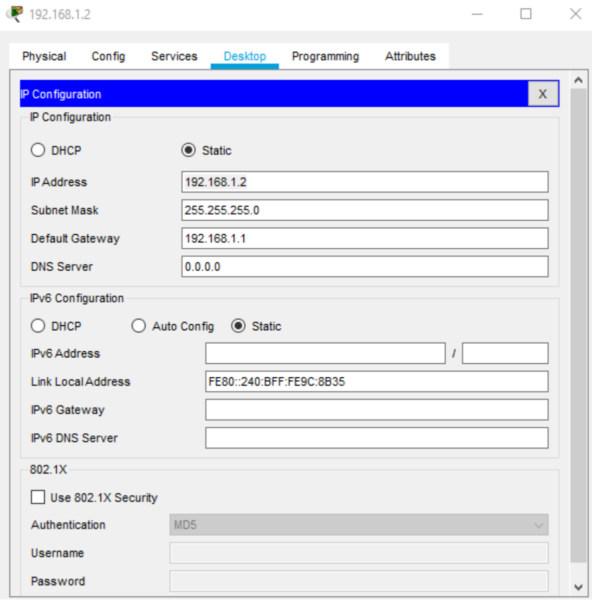
802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Server configurations



192.168.1.2

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::240:BFF:FE9C:8B35

IPv6 Gateway:

IPv6 DNS Server:

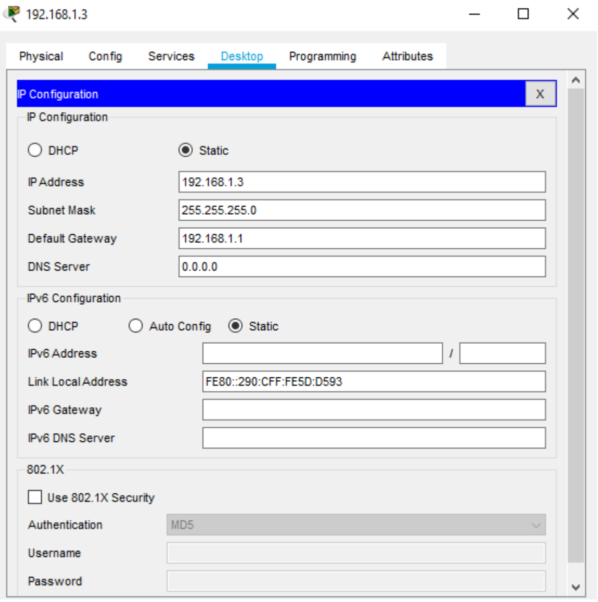
802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:



192.168.1.3

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:FE5D:D593

IPv6 Gateway:

IPv6 DNS Server:

802.1X

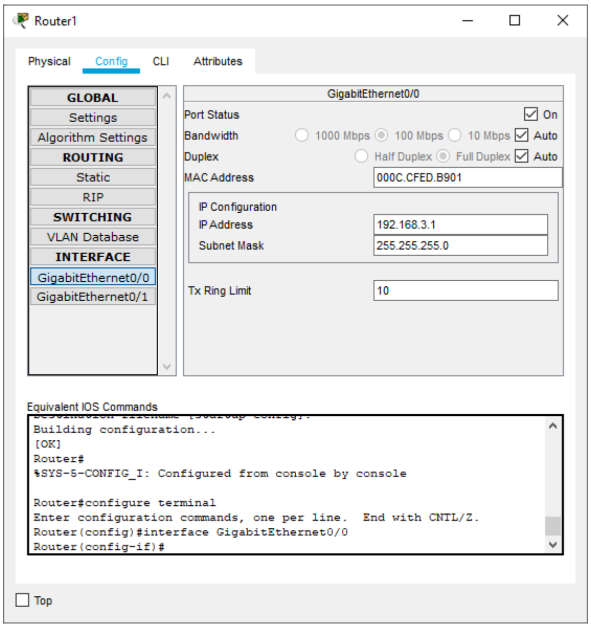
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Router configurations



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: 000C.CFED.B901

IP Configuration

IP Address: 192.168.3.1

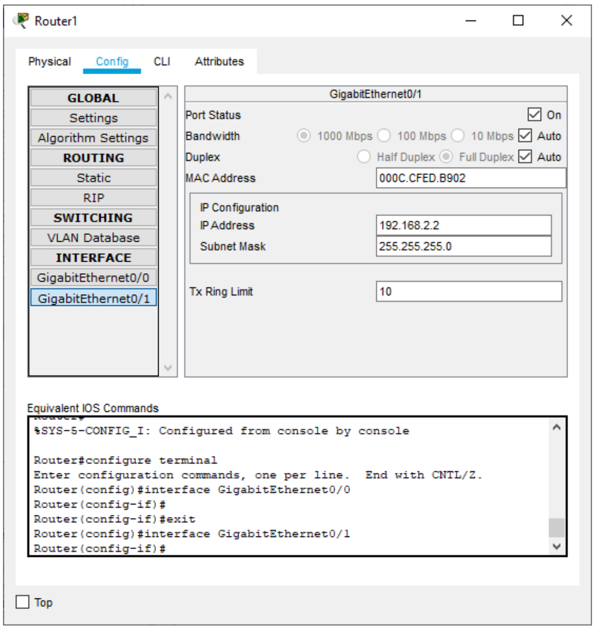
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```

□ Top



Router1

Physical | Config | CLI | Attributes

GLOBAL: Settings, Algorithm Settings
ROUTING: Static, RIP
SWITCHING: VLAN Database
INTERFACE: GigabitEthernet0/0, GigabitEthernet0/1

GigabitEthernet0/1

Port Status: ☑ On

Bandwidth: ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex: ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 000C.CFED.B902

IP Configuration

IP Address: 192.168.2.2

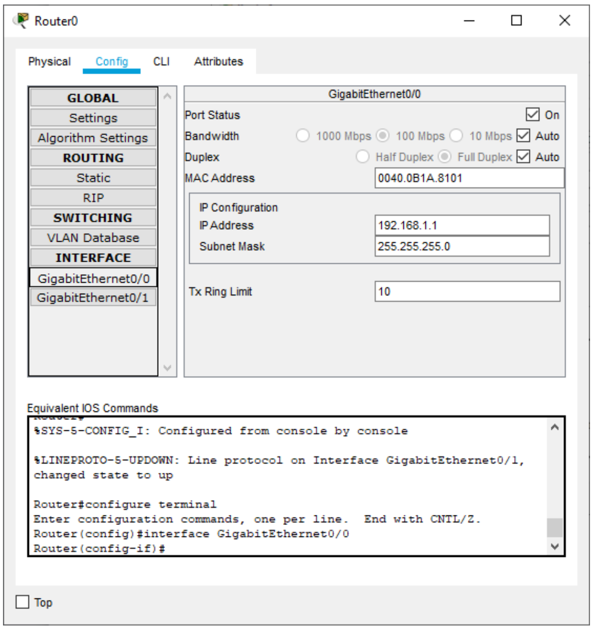
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

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

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



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0040.0B1A.8101

IP Configuration

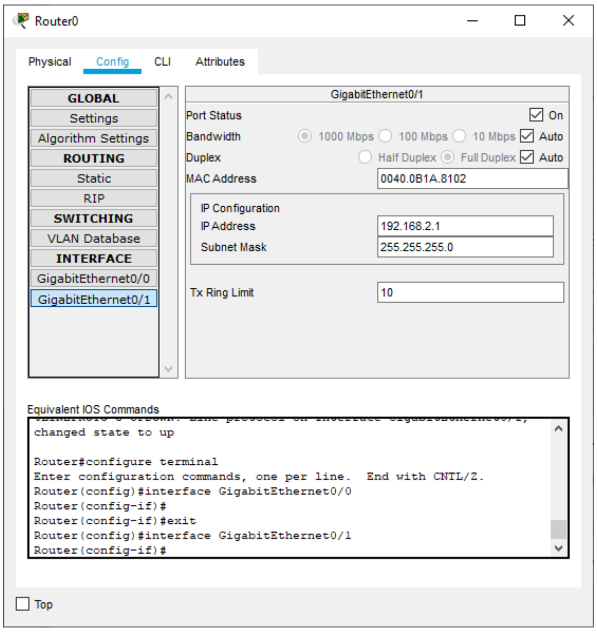
IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```



GigabitEthernet0/1

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0040.0B1A.8102

IP Configuration

IP Address 192.168.2.1

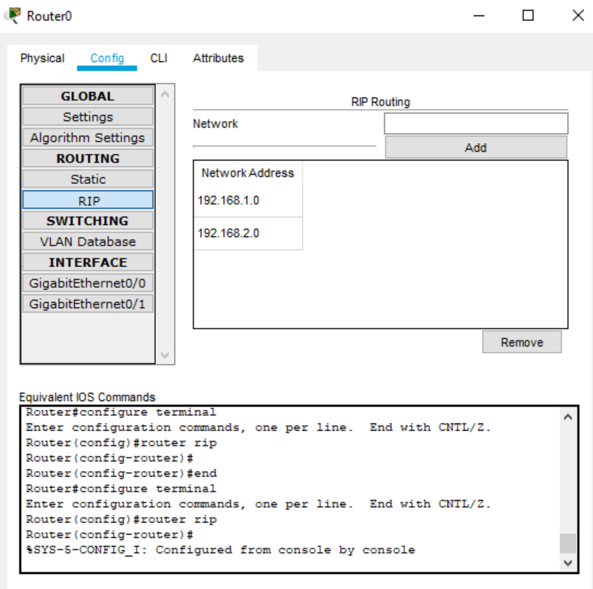
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

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)#
```

RIP routing



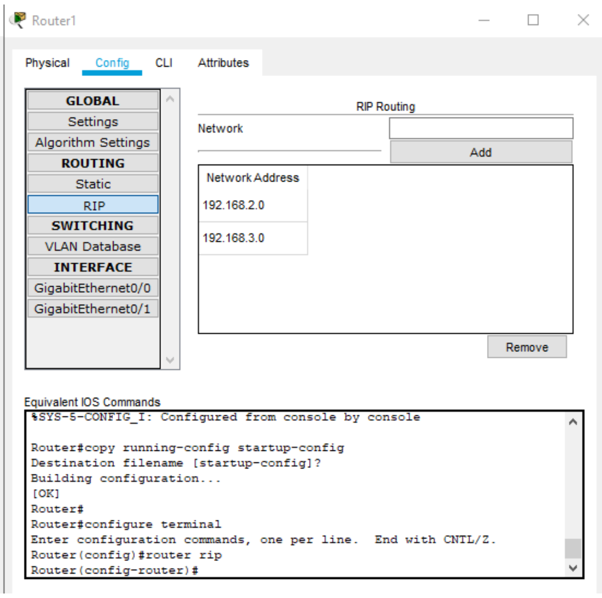
RIP Routing

Network

Network Address
192.168.1.0
192.168.2.0

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
%SYS-5-CONFIG_I: Configured from console by console
```



RIP Routing

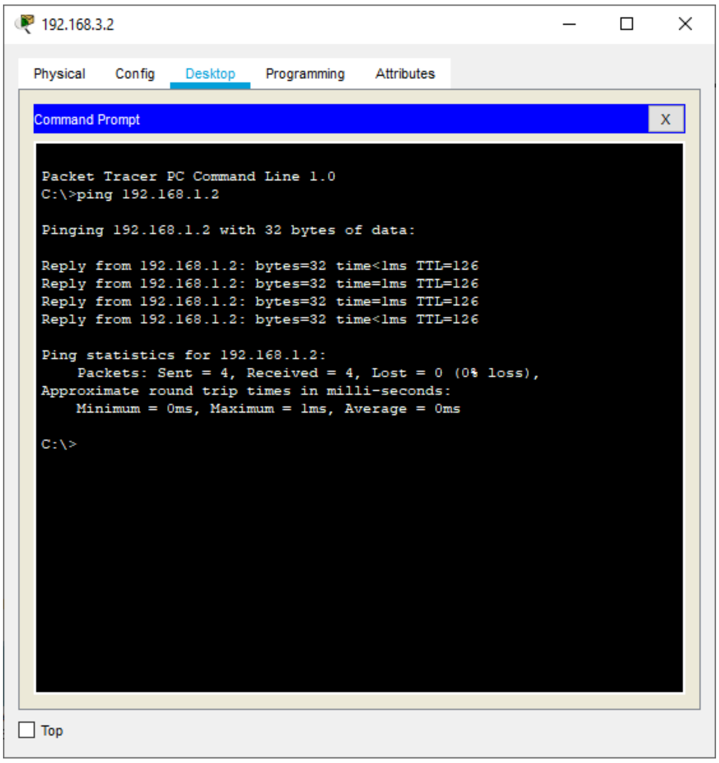
Network

Network Address
192.168.2.0
192.168.3.0

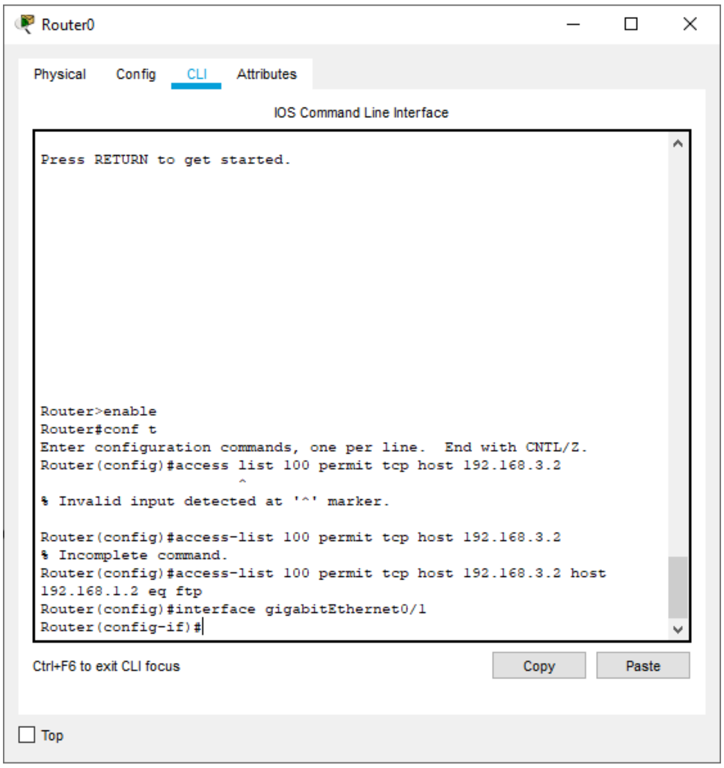
Equivalent IOS Commands

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

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

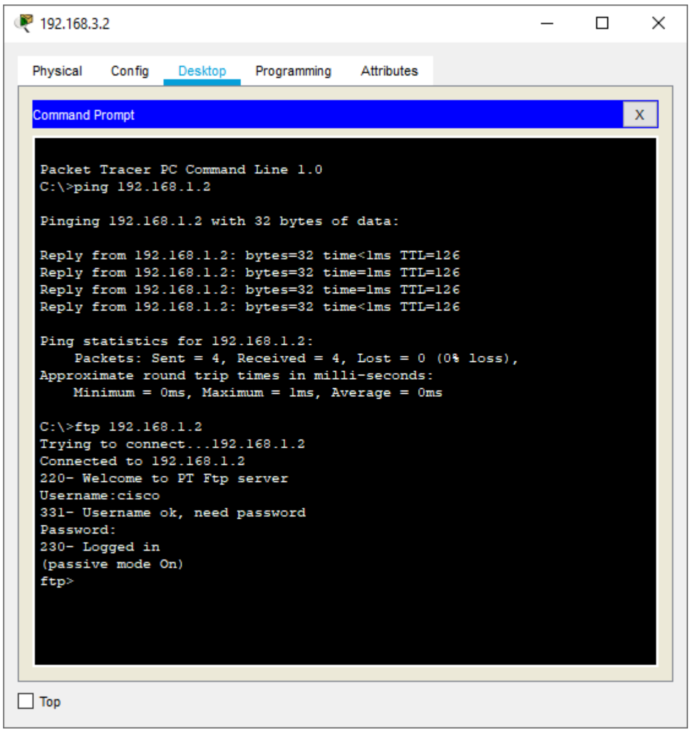
Check the connection using ping command



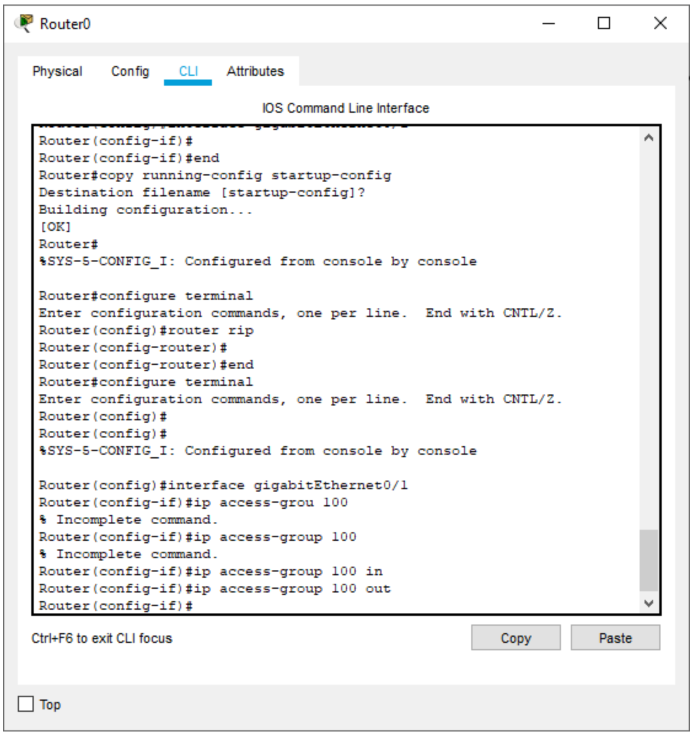
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```



```
Press RETURN to get started.






Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access list 100 permit tcp host 192.168.3.2
                      ^
% Invalid input detected at '^' marker.

Router(config)#access-list 100 permit tcp host 192.168.3.2
% Incomplete command.
Router(config)#access-list 100 permit tcp host 192.168.3.2 host
192.168.1.2 eq ftp
Router(config)#interface gigabitEthernet0/1
Router(config-if)#
```



```
Packet Tracer PC Command Line 1.0
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<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ftp 192.168.1.2
Trying to connect...192.168.1.2
Connected to 192.168.1.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



```
Router(config-if)#
Router(config-if)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
%SYS-5-CONFIG_I: Configured from console by console

Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip access-grou 100
% Incomplete command.
Router(config-if)#ip access-group 100
% Incomplete command.
Router(config-if)#ip access-group 100 in
Router(config-if)#ip access-group 100 out
Router(config-if)#
```

```
enable
conf t
Router(config)#access-list 100 permit tcp host 192.168.3.2
Router(config)#access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq
ftp
Router(config)#access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq
ftp
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#ip access-group 100 out
```

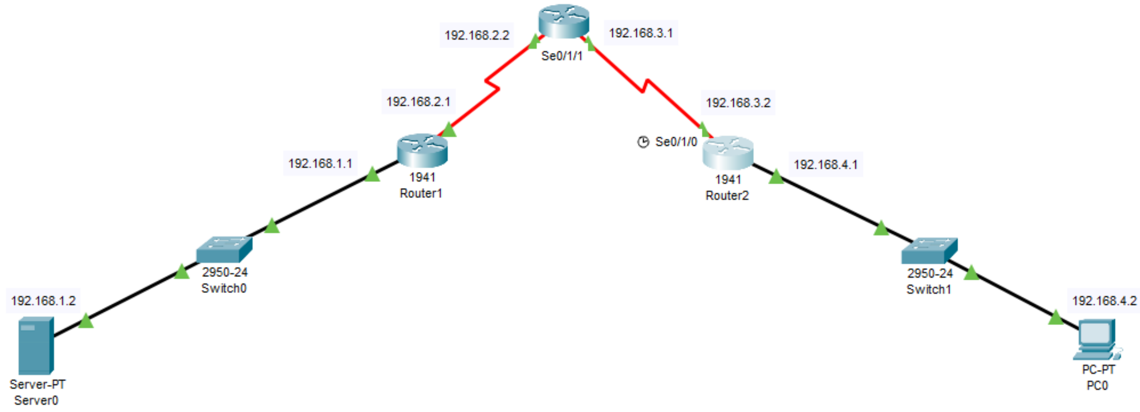
Practical 4

AIM: Configure IP ACLs to Mitigate Attacks and IPV6 ACLs

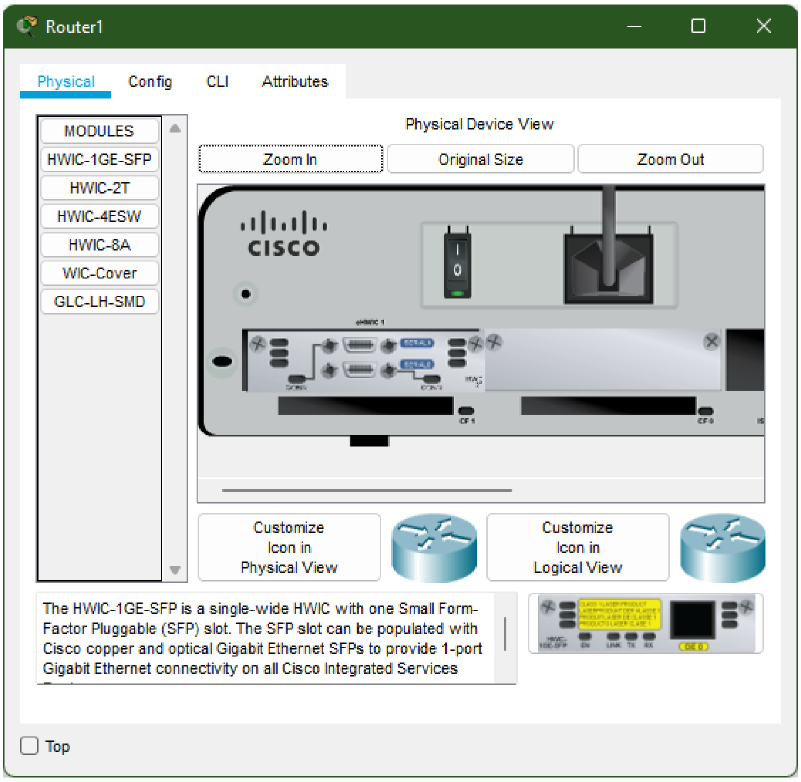
a. Verify connectivity among devices before firewall configuration.
b. Use ACLs to ensure remote access to the routers is available only from management station PC-C.
c. Configure ACLs on to mitigate attacks.
d. Configuring IPv6 ACLs

Solution:

Topology

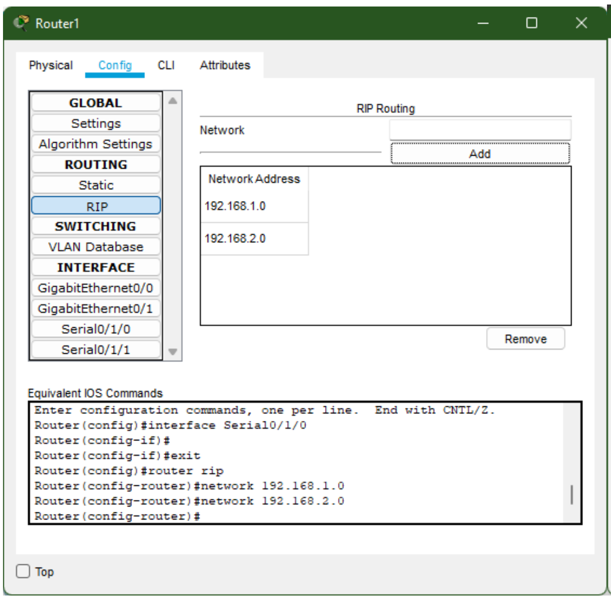


Turn off router and add HWIC-2T module to all 3 routers:



The HWIC-1GE-SFP is a single-wide HWIC with one Small Form-Factor Pluggable (SFP) slot. The SFP slot can be populated with Cisco copper and optical Gigabit Ethernet SFPs to provide 1-port Gigabit Ethernet connectivity on all Cisco Integrated Services

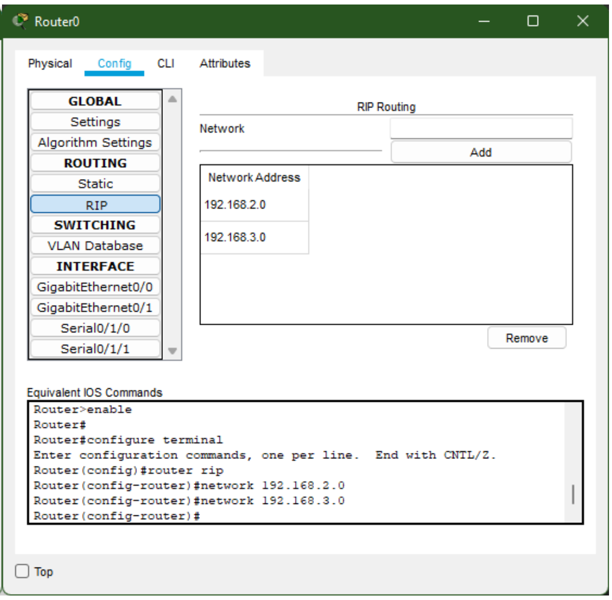
Configure RIP routing:



Network Address
192.168.1.0
192.168.2.0

Equivalent IOS Commands

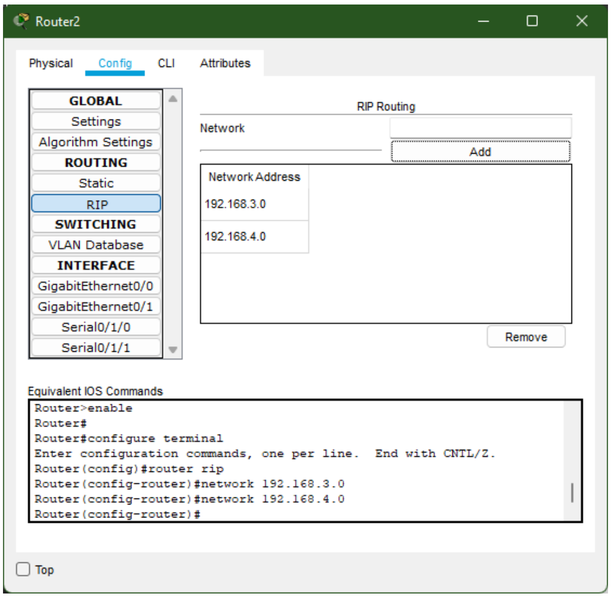
```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#
```



Network Address
192.168.2.0
192.168.3.0

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#
```

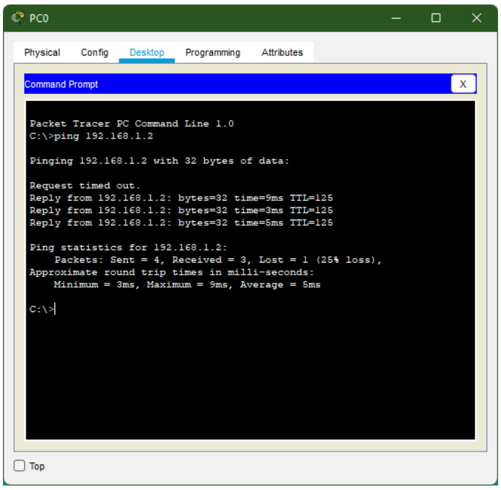


Network Address
192.168.3.0
192.168.4.0

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.4.0
Router(config-router)#
```

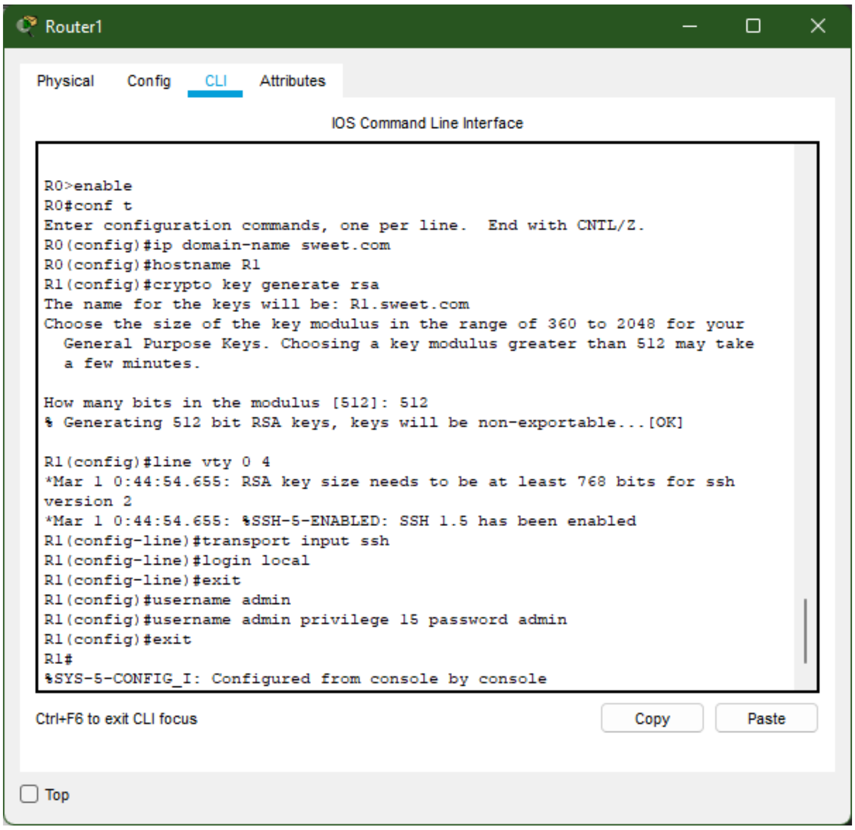
Verifying:



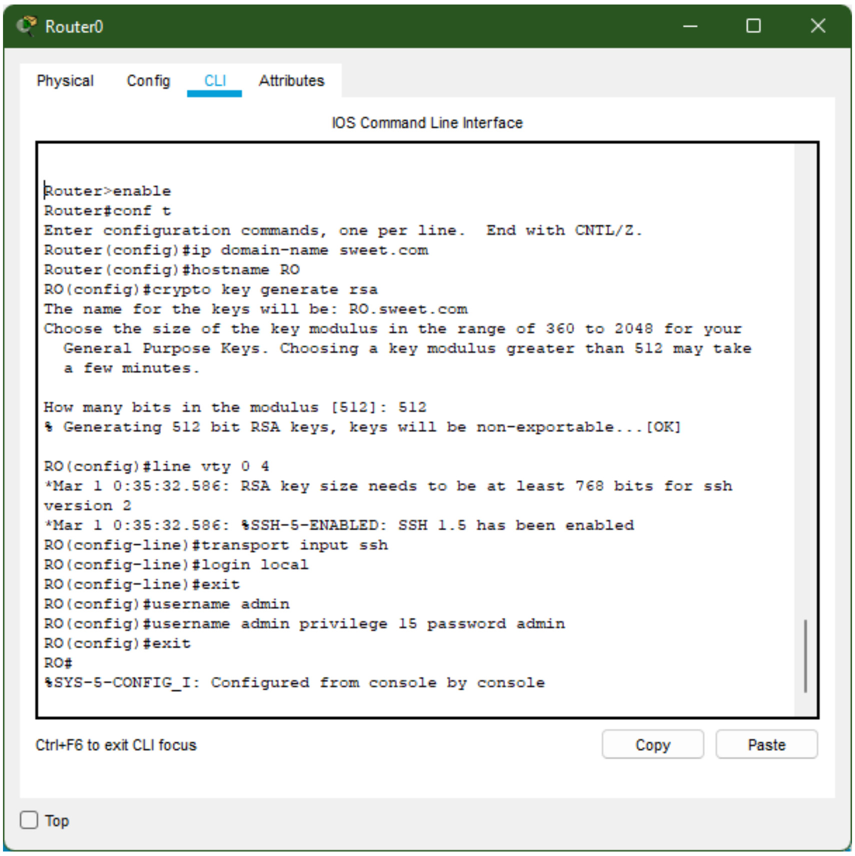
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=9ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=5ms 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 = 3ms, Maximum = 9ms, Average = 5ms

C:\>
```

Commands:

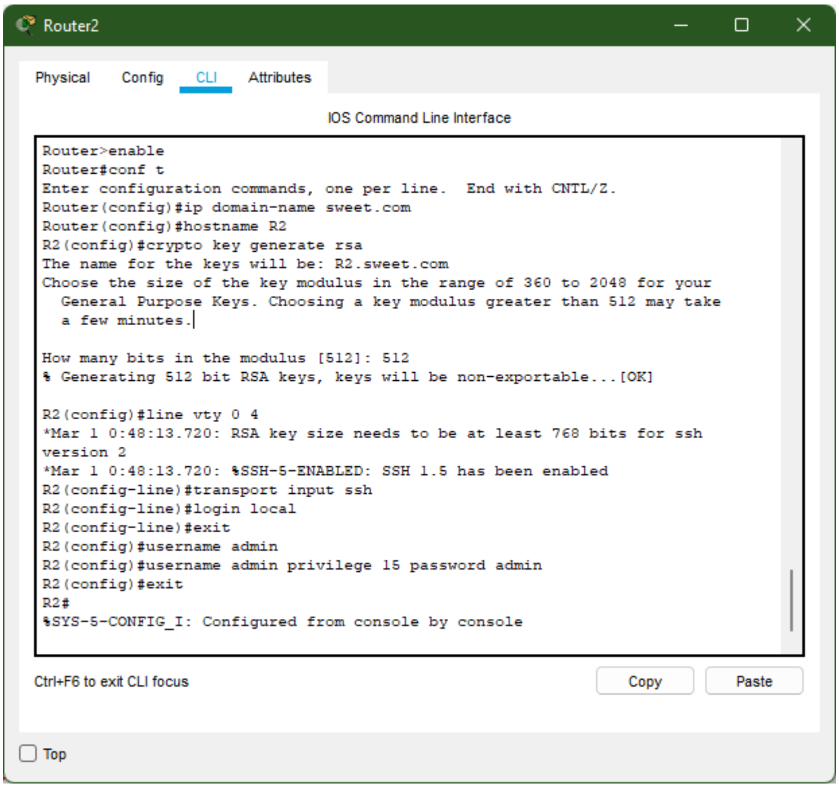
```
enable
conf t
ip domain-name sweet.com
hostname r0
crypto key generate rsa
512
line vty 0 4
transport input ssh
login local
exit
username admin
username admin privilege 15 password <password>
exit
exit
```



```
R0>enable
R0#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#ip domain-name sweet.com
R0(config)#hostname R1
R1(config)#crypto key generate rsa
The name for the keys will be: R1.sweet.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]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#line vty 0 4
*Mar 1 0:44:54.655: RSA key size needs to be at least 768 bits for ssh
version 2
*Mar 1 0:44:54.655: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#username admin
R1(config)#username admin privilege 15 password admin
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```



```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip domain-name sweet.com
Router(config)#hostname RO
RO(config)#crypto key generate rsa
The name for the keys will be: RO.sweet.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]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

RO(config)#line vty 0 4
*Mar 1 0:35:32.586: RSA key size needs to be at least 768 bits for ssh
version 2
*Mar 1 0:35:32.586: %SSH-5-ENABLED: SSH 1.5 has been enabled
RO(config-line)#transport input ssh
RO(config-line)#login local
RO(config-line)#exit
RO(config)#username admin
RO(config)#username admin privilege 15 password admin
RO(config)#exit
RO#
%SYS-5-CONFIG_I: Configured from console by console
```

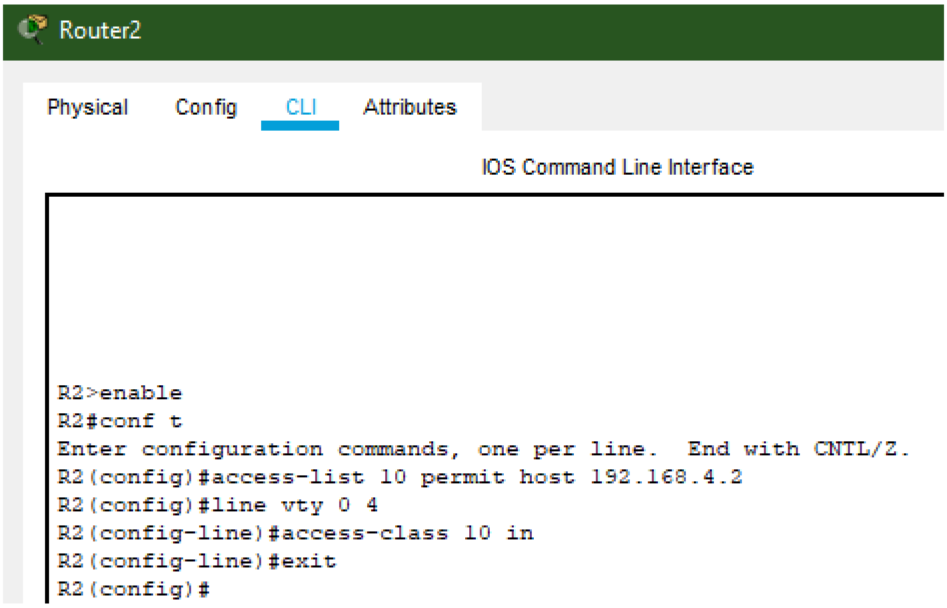


```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip domain-name sweet.com
Router(config)#hostname R2
R2(config)#crypto key generate rsa
The name for the keys will be: R2.sweet.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

R2(config)#line vty 0 4
*Mar 1 0:48:13.720: RSA key size needs to be at least 768 bits for ssh
version 2
*Mar 1 0:48:13.720: %SSH-5-ENABLED: SSH 1.5 has been enabled
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#exit
R2(config)#username admin
R2(config)#username admin privilege 15 password admin
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

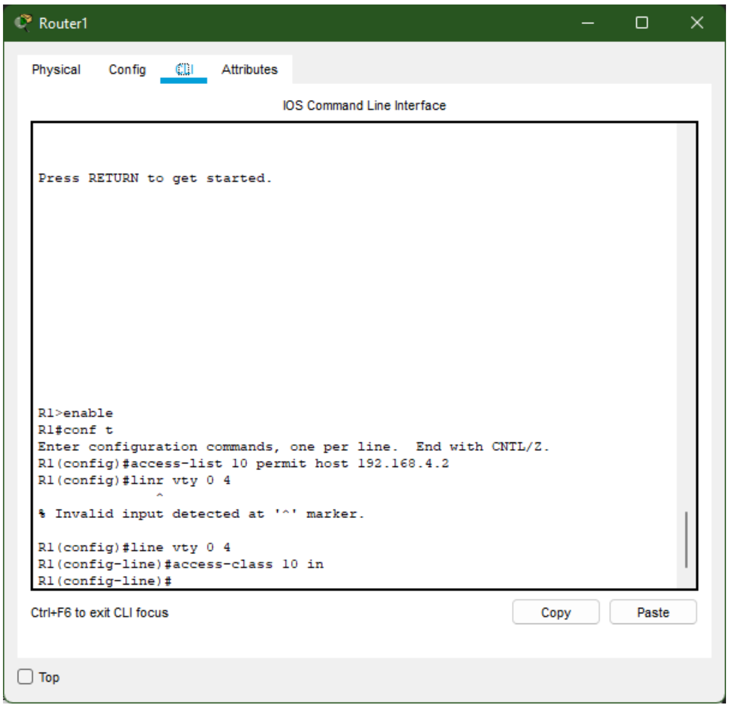
Then, type these commands in all three routers:

```
enable
conf t
access-list 10 permit host 192.168.4.2
```

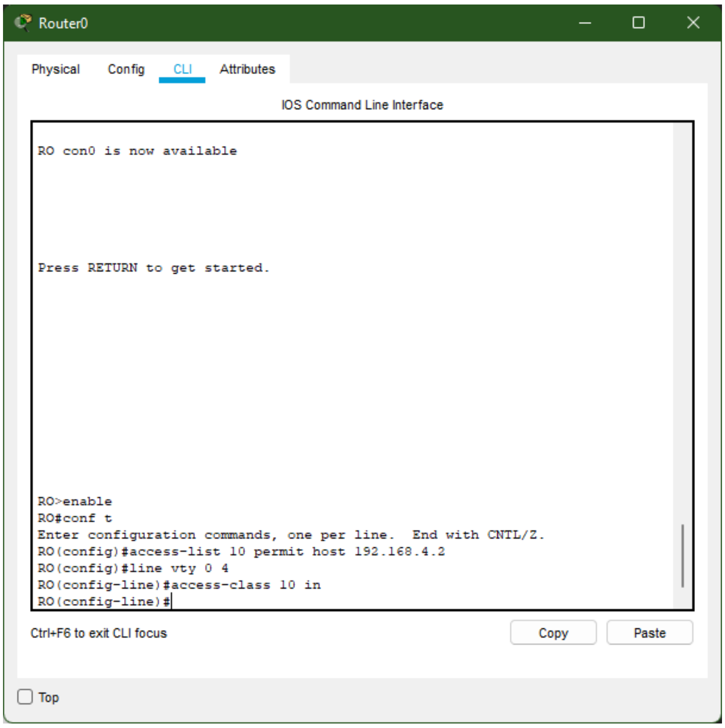
```
line vty 0 4
access-class 10 in
```



```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 10 permit host 192.168.4.2
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#exit
R2(config)#
```

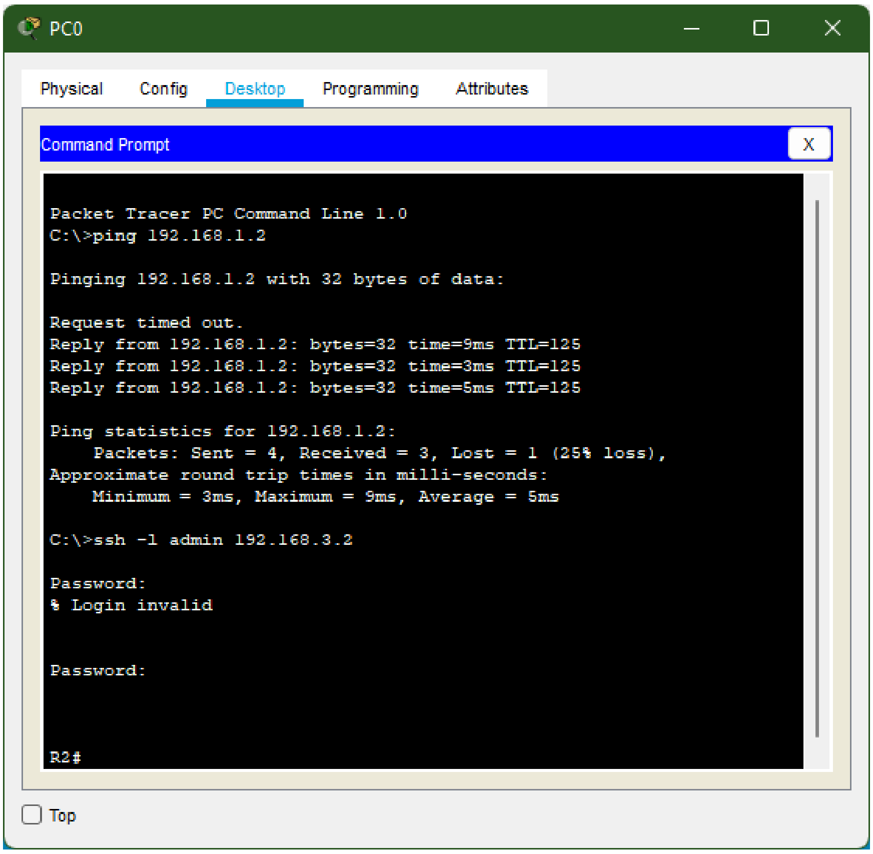


```
Press RETURN to get started.









R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit host 192.168.4.2
R1(config)#linr vty 0 4
            ^
% Invalid input detected at '^' marker.

R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#
```



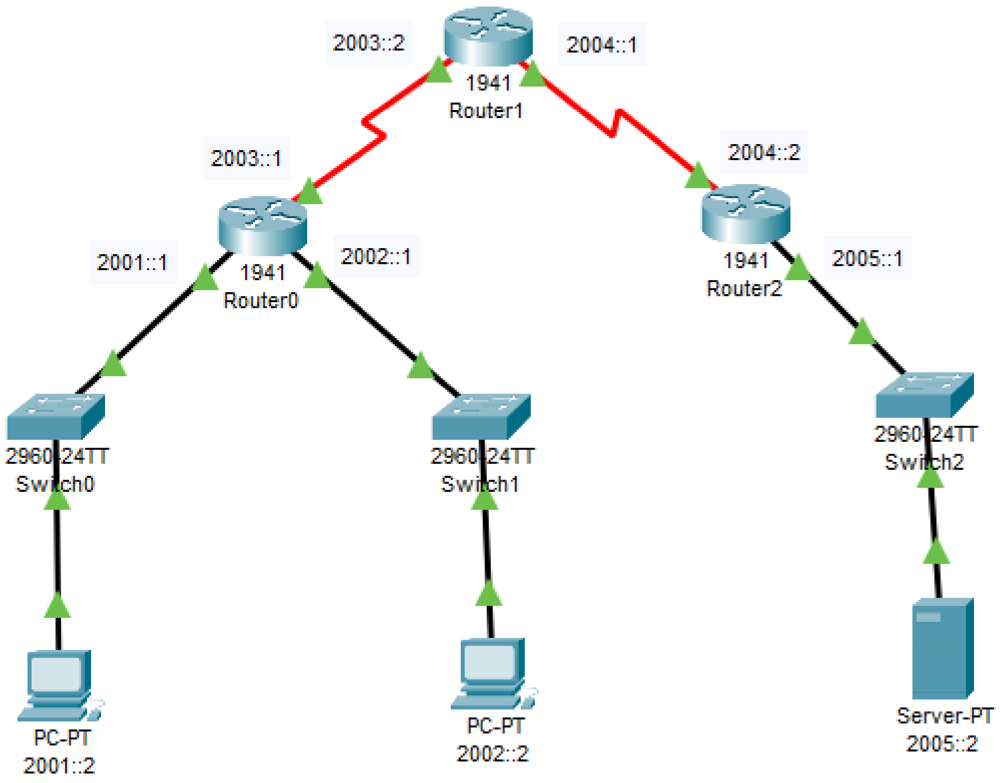
```
RO con0 is now available



Press RETURN to get started.











RO>enable
RO#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RO(config)#access-list 10 permit host 192.168.4.2
RO(config)#line vty 0 4
RO(config-line)#access-class 10 in
RO(config-line)#
```

```
Ssh enable commands for pc terminal
Ssh -l admin <router-ip>
Ssh -l admin 192.168.3.2
```

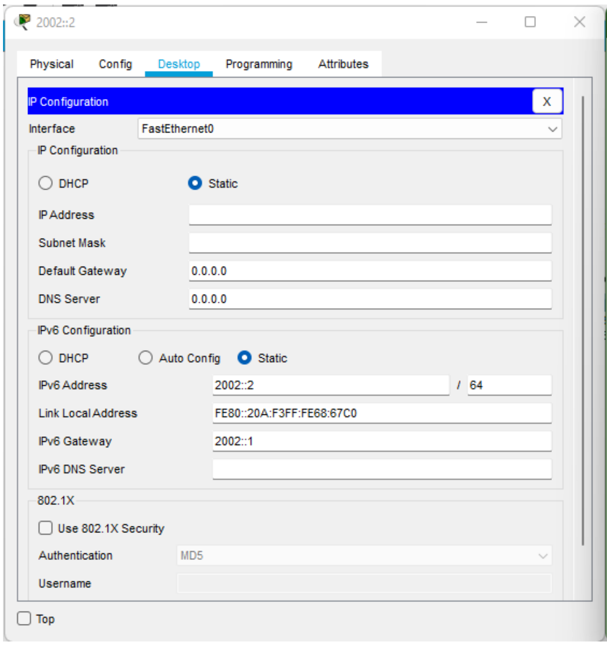


```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=9ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=5ms 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 = 3ms, Maximum = 9ms, Average = 5ms

C:\>ssh -l admin 192.168.3.2

Password:
% Login invalid


Password:



R2#
```

IPv6



PC Configurations



Interface: FastEthernet0

IP Configuration

● Static ○ DHCP

IP Address:

Subnet Mask:

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: 2002::2 / 64

Link Local Address: FE80::20A:F3FF:FE68:67C0

IPv6 Gateway: 2002::1

IPv6 DNS Server:

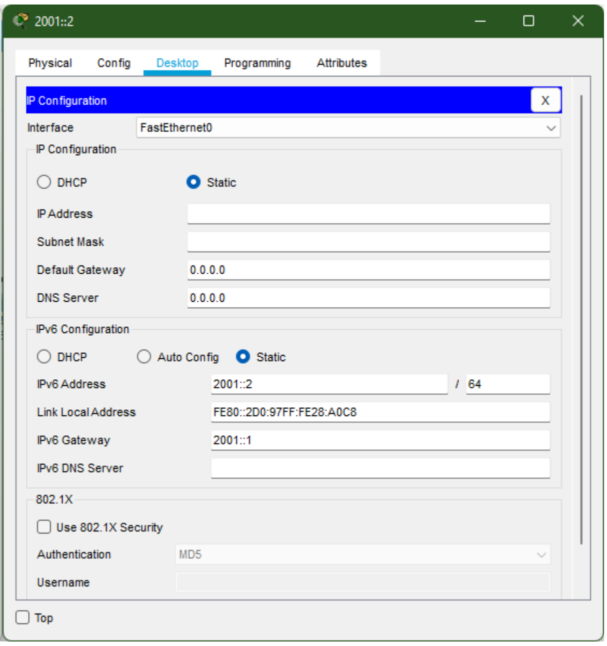
802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

□ Top



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address:

Subnet Mask:

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: 2001::2 / 64

Link Local Address: FE80::2D0:97FF:FE28:A0C8

IPv6 Gateway: 2001::1

IPv6 DNS Server:

802.1X

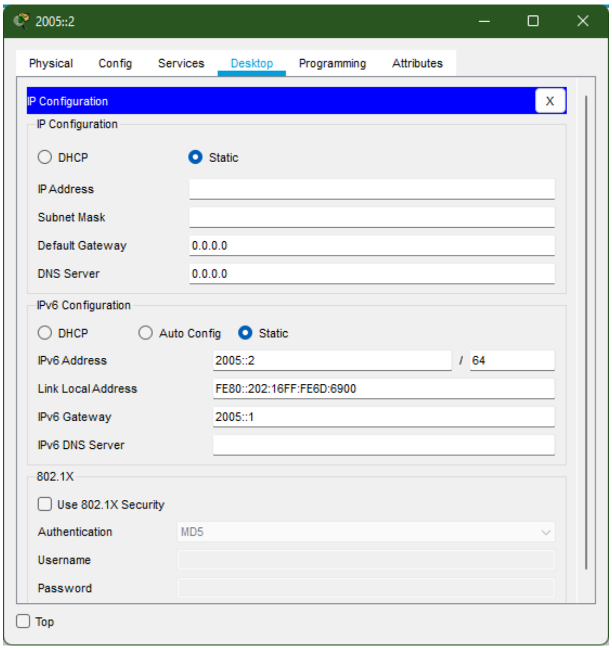
□ Use 802.1X Security

Authentication: MD5

Username:

□ Top

Server Configuration



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address	
Subnet Mask	
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address	2005::2 / 64
Link Local Address	FE80::202:16FF:FE6D:6900
IPv6 Gateway	2005::1
IPv6 DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

Router commands for ipv6 addressing and routing

Router1:

```
Router>enable
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#interface gigabitEthernet0/0
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)#ipv6 unicast-routing
Router(config)#interface gigabitEthernet0/1
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)#ipv6 unicast-routing
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 0 commands:

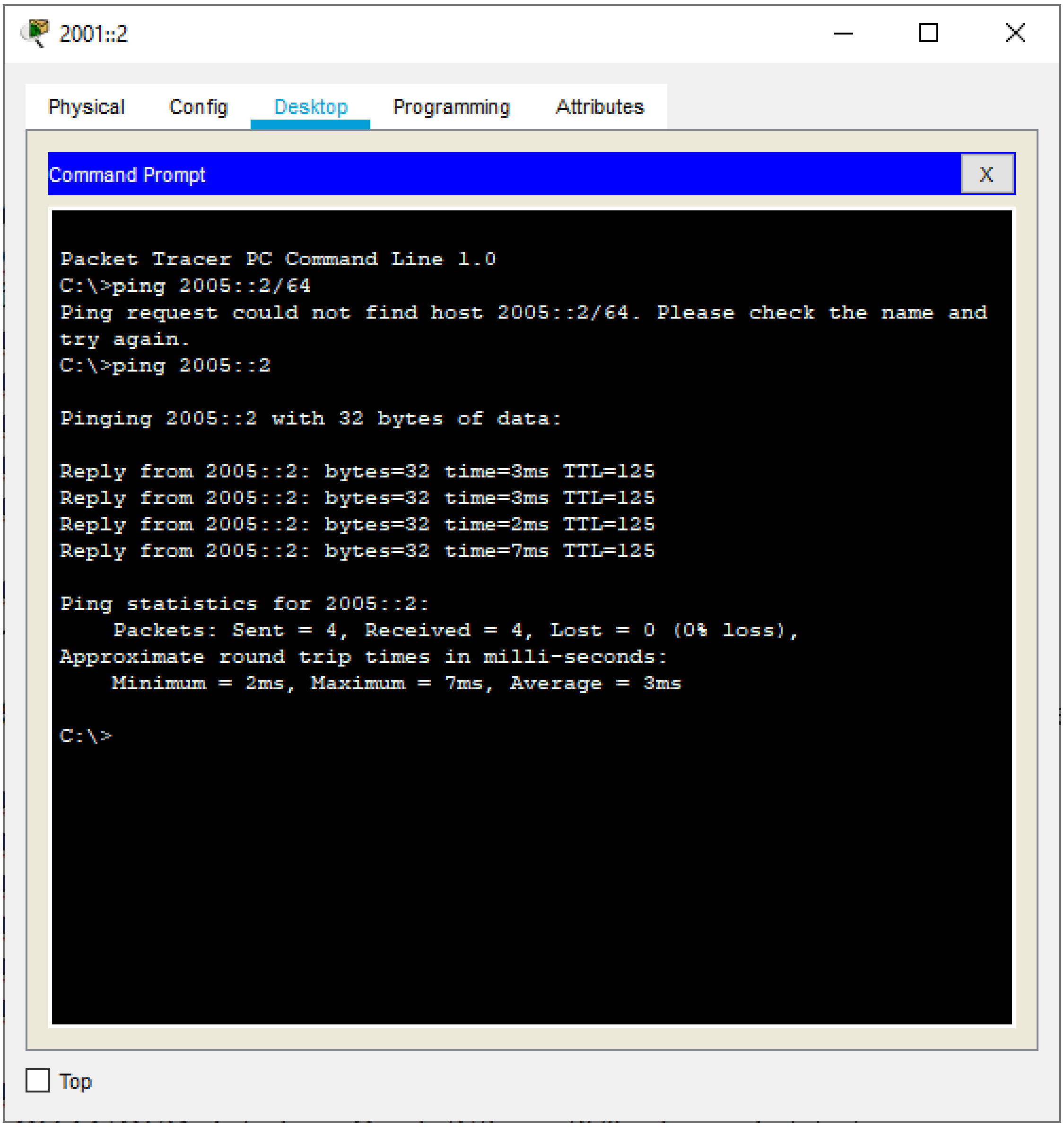
```
Router>
Router>enable
Router#conf t
Router(config)#ipv6 unicast-routing
Router(config)#interface Serial0/1/0
Router(config-if)#ipv6 address 2003::2/64
Router(config-if)#ipv6 rip a enable
Router(config-if)#no shutdown
Router(config-if)#
Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#interface 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)#
```

ROUTER 2 commands

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)#interface Serial0/1/0
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)#ipv6 unicast-routing
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)#
```

Verifying using ping command on PC

```
Ping 2005::2
```

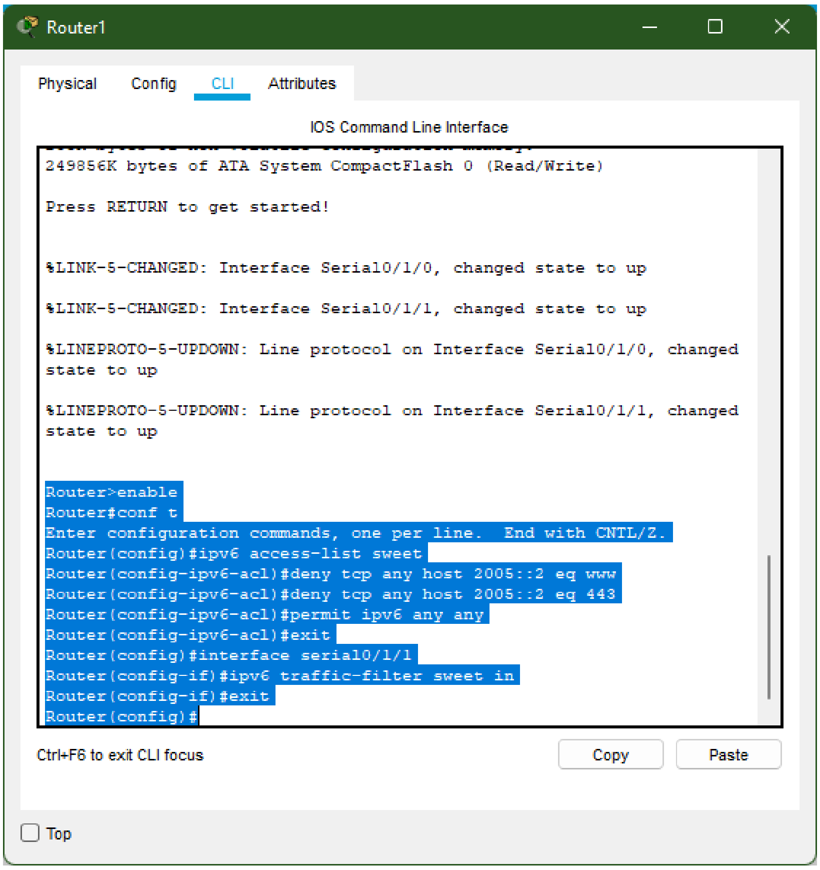


```
Packet Tracer PC Command Line 1.0
C:\>ping 2005::2/64
Ping request could not find host 2005::2/64. Please check the name and
try again.
C:\>ping 2005::2

Pinging 2005::2 with 32 bytes of data:

Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=7ms 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 = 7ms, Average = 3ms

C:\>
```

Connection is established.

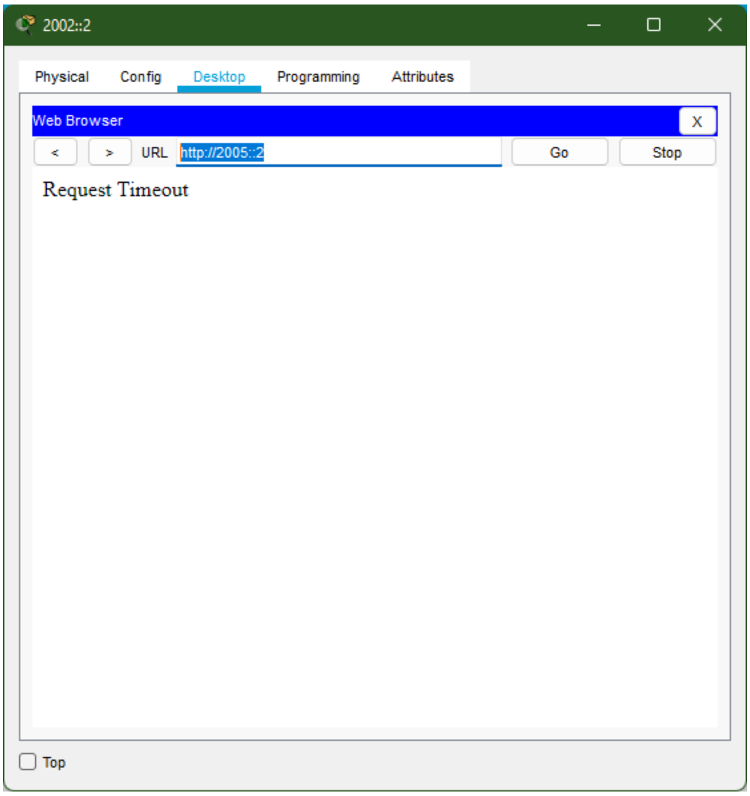
Configuring ACL

```
enable
conf t
ipv6 access-list sweet
deny tcp any host 2005::2 eq www
deny tcp any host 2005::2 eq 443
permit ipv6 any any
exit
interface serial0/1/1
ipv6 traffic-filter sweet in
exit
```



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

Press RETURN to get started!


%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up

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

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


Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ipv6 access-list sweet
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)#exit
Router(config)#interface serial0/1/1
Router(config-if)#ipv6 traffic-filter sweet in
Router(config-if)#exit
Router(config)#
```

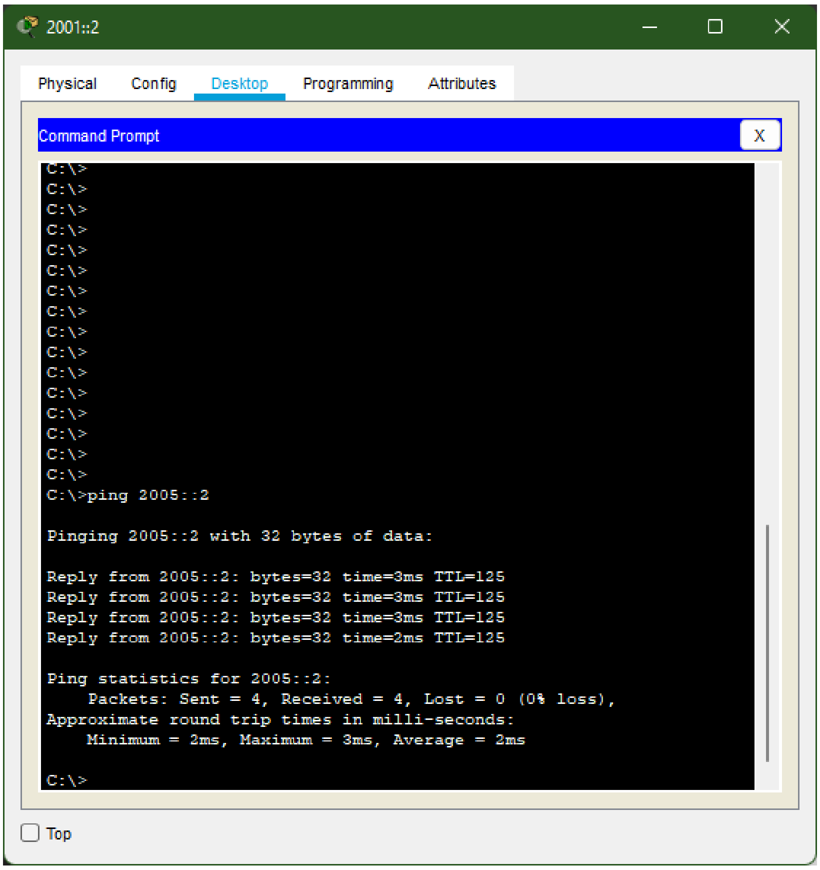
Verifying the configuration by accessing www service from the browser of both pc (expects failure)



URL: http://2005::2

Request Timeout

Now if we ping it should be successful.



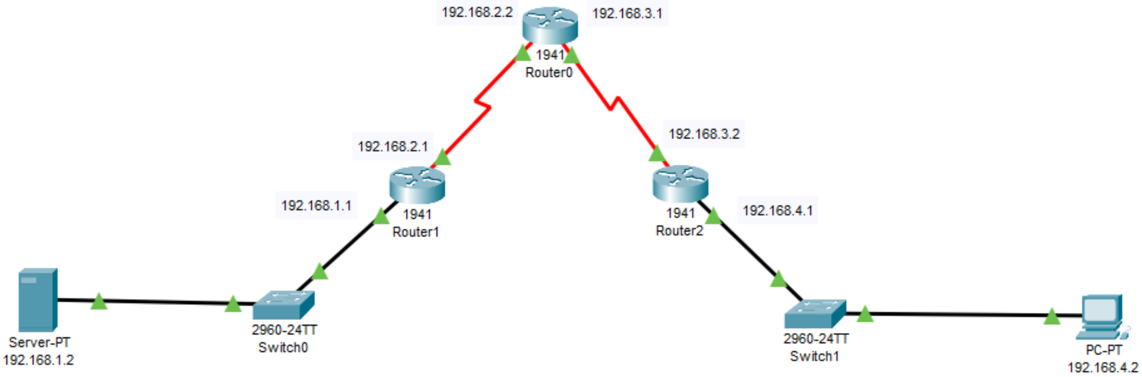
```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 2005::2

Pinging 2005::2 with 32 bytes of data:

Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=3ms 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 = 3ms, Average = 2ms

C:\>
```

Practical 5

AIM: Configuring a Zone-Based Policy Firewall

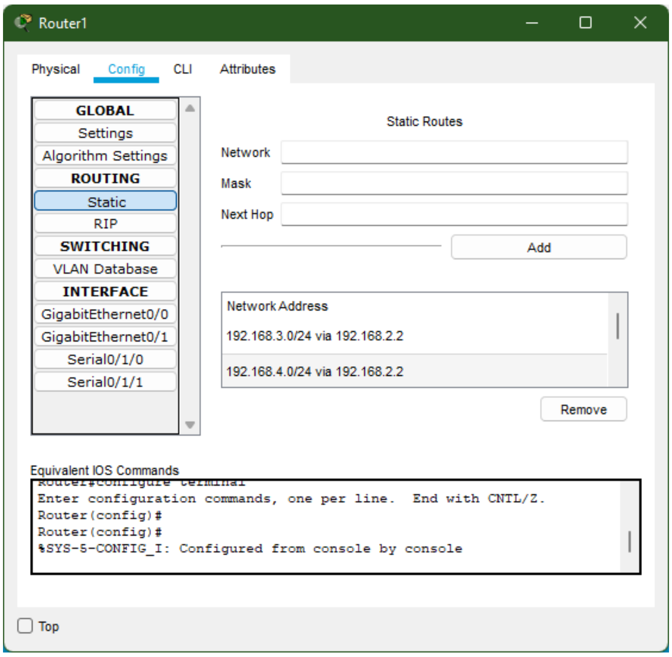
Solution:

Topology



Static routing

Router 1 (Left one)



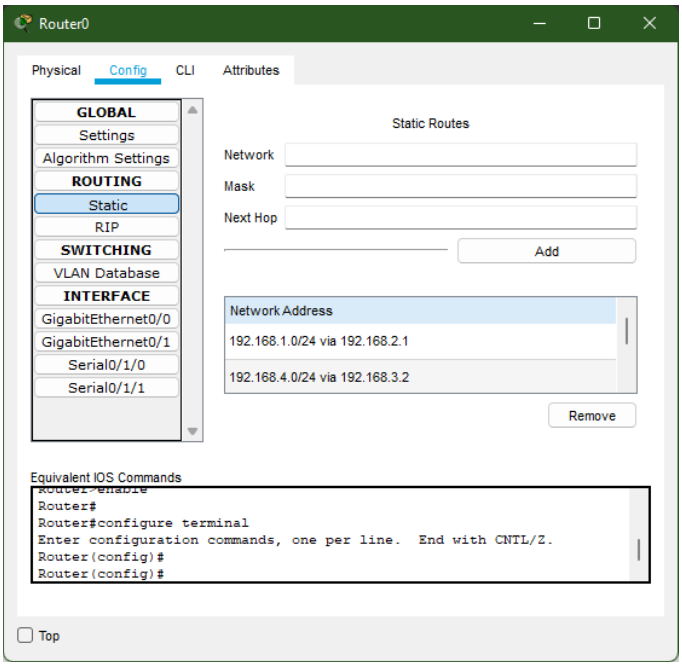
Network Address

192.168.3.0/24 via 192.168.2.2

192.168.4.0/24 via 192.168.2.2

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
%SYS-5-CONFIG_I: Configured from console by console
```

Router 0 (Centre)



Static Routes

Network

Mask

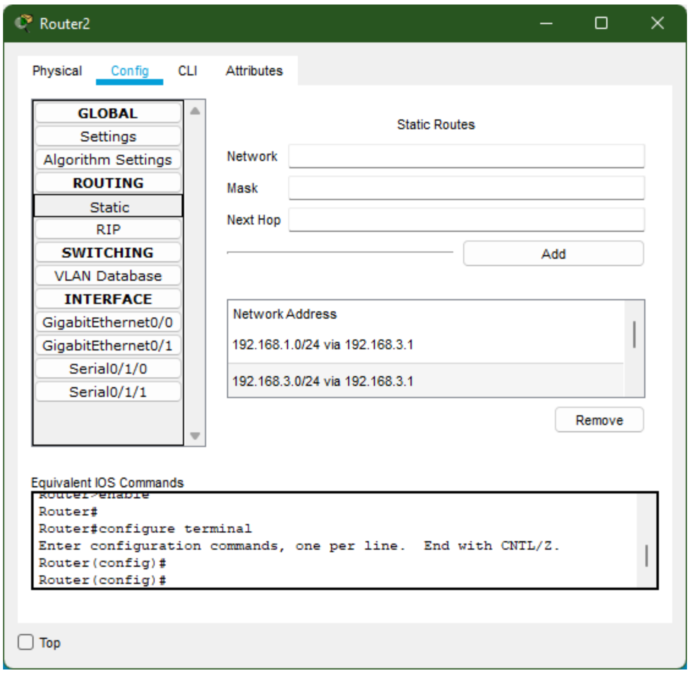
Next Hop

Network Address
192.168.1.0/24 via 192.168.2.1
192.168.4.0/24 via 192.168.3.2

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
```

Router 2 (Right one)



Static Routes

Network

Mask

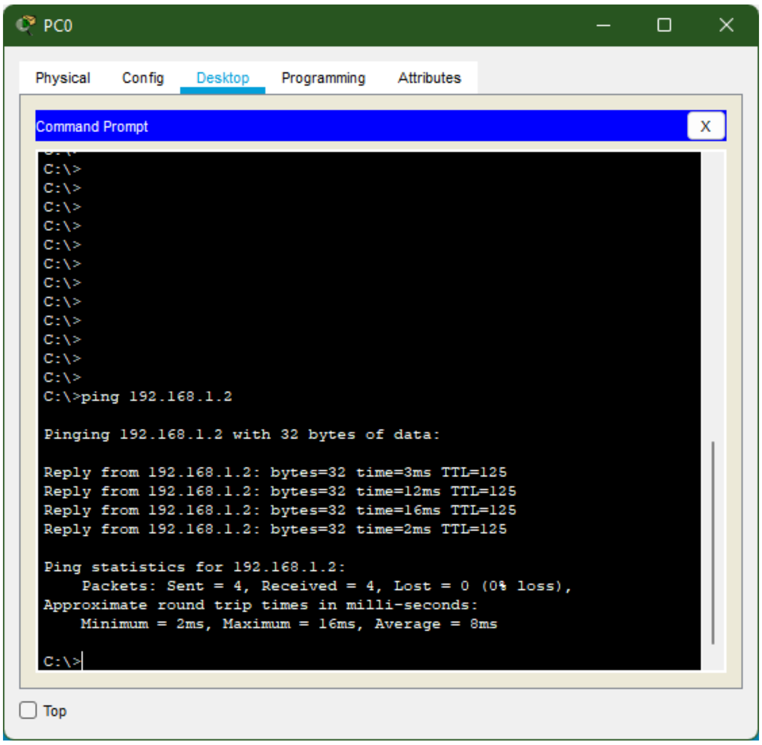
Next Hop

Network Address
192.168.1.0/24 via 192.168.3.1
192.168.3.0/24 via 192.168.3.1

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
```

Verifying routes using ping command from pc to server



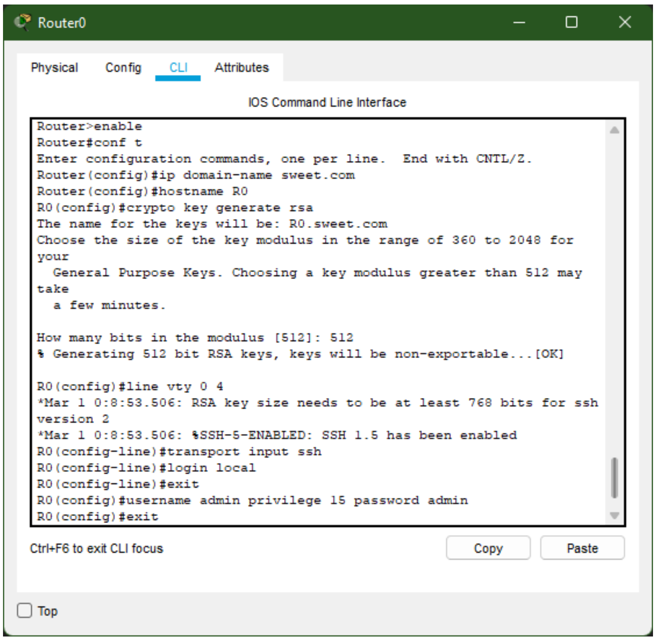
```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=16ms 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 = 16ms, Average = 8ms

C:\>
```

Part 2

Configuring ssh on router 0 (center one)

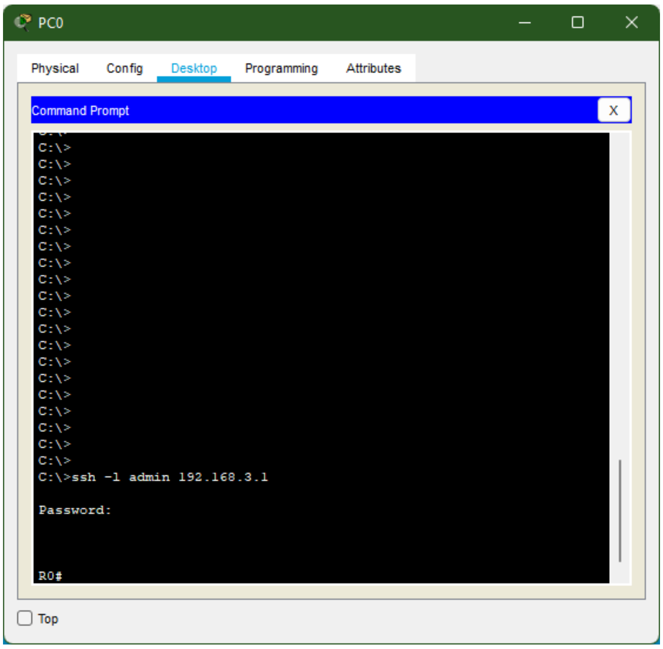
Commands for router 0:

```
> enable
> conf t
> ip domain-name sweet.com
> hostname R2
> crypto key generate rsa
> line vty 0 4
> transport input ssh
> login local
> exit
> username admin privilege 15 password admin
```

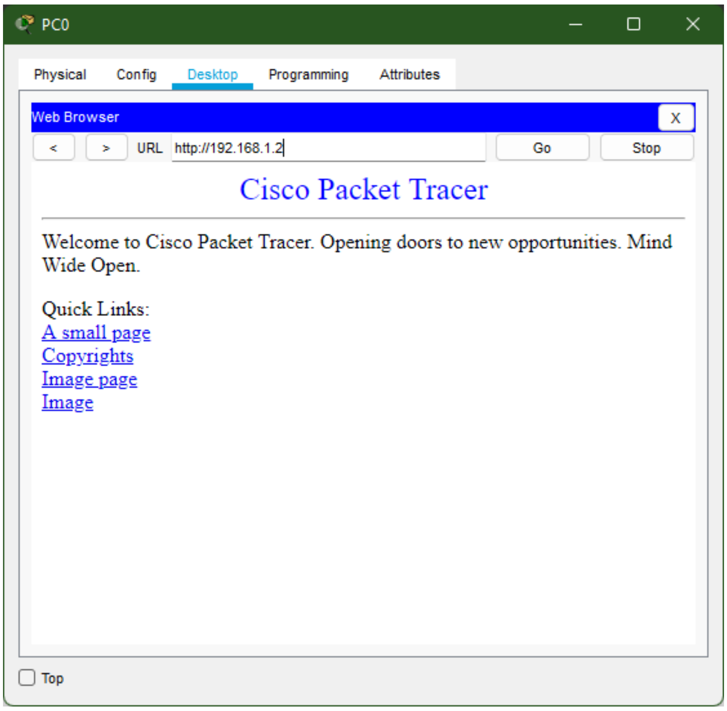


```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip domain-name sweet.com
Router(config)#hostname R0
R0(config)#crypto key generate rsa
The name for the keys will be: R0.sweet.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

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

R0(config)#line vty 0 4
*Mar 1 0:8:53.506: RSA key size needs to be at least 768 bits for ssh
version 2
*Mar 1 0:8:53.506: %SSH-5-ENABLED: SSH 1.5 has been enabled
R0(config-line)#transport input ssh
R0(config-line)#login local
R0(config-line)#exit
R0(config)#username admin privilege 15 password admin
R0(config)#exit
```

Verifying SSH using pc



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

Password:


R0#
```



http://192.168.1.2

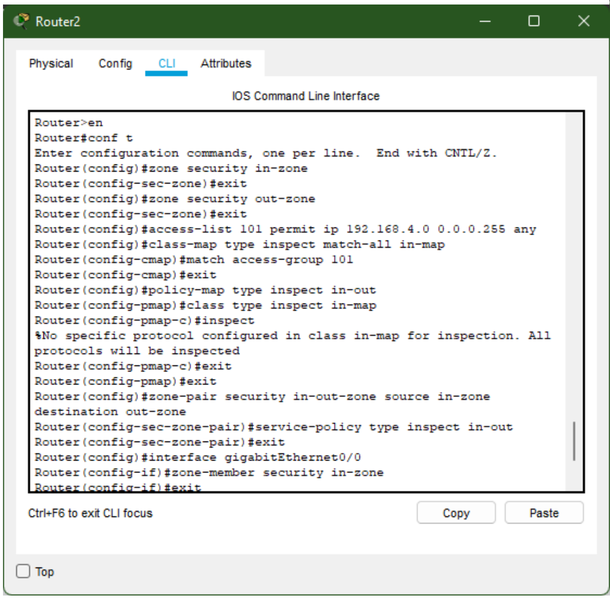
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

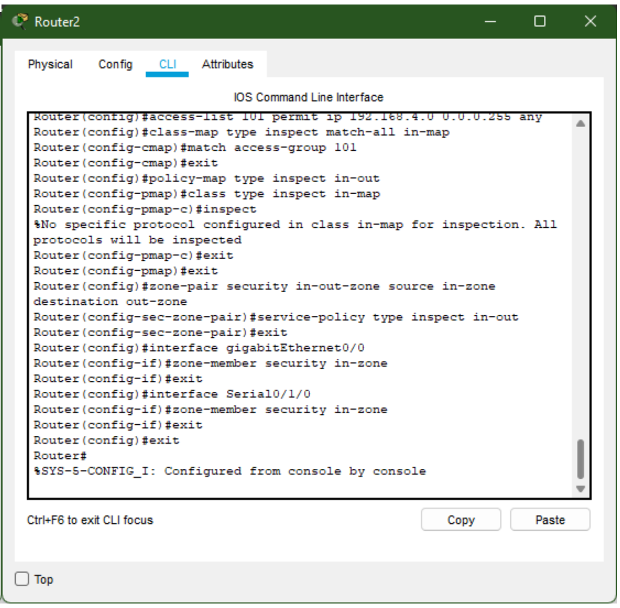
Quick Links:
A small page
Copyrights
Image page
Image

PART 3: Create firewall zones on Router2 (Right one)

```
>en
#conf t
#zone security in-zone
#exit
#zone security out-zone
#exit
#access-list 101 permit ip 192.168.4.0 0.0.0.255 any
#class-map type inspect match-all in-map
#match access-group 101
#exit
#policy-map type inspect in-out
#class type inspect in-map
#exit
#exit
#zone-pair security in-out-zone source in-zone destination out-zone
#service-policy type inspect in-out
#exit
#interface gigabitEthernet0/0
#zone-member security in-zone
#exit
#interface Serial0/1/0
#zone-member security in-zone
#exit
#exit
```



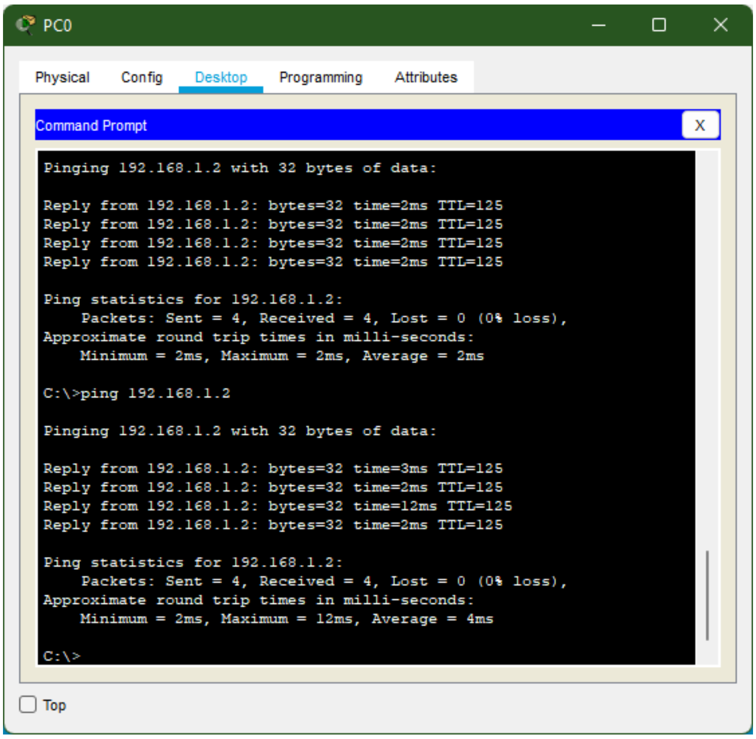
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#zone security in-zone
Router(config-sec-zone)#exit
Router(config)#zone security out-zone
Router(config-sec-zone)#exit
Router(config)#access-list 101 permit ip 192.168.4.0 0.0.0.255 any
Router(config)#class-map 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
%No specific protocol configured in class in-map for inspection. All
protocols will be inspected
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)#interface gigabitEthernet0/0
Router(config-if)#zone-member security in-zone
Router(config-if)#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
%No specific protocol configured in class in-map for inspection. All
protocols will be inspected
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)#interface gigabitEthernet0/0
Router(config-if)#zone-member security in-zone
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#zone-member security in-zone
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

PART 4: Testing firewall functionality (From in-zone to out-zone)

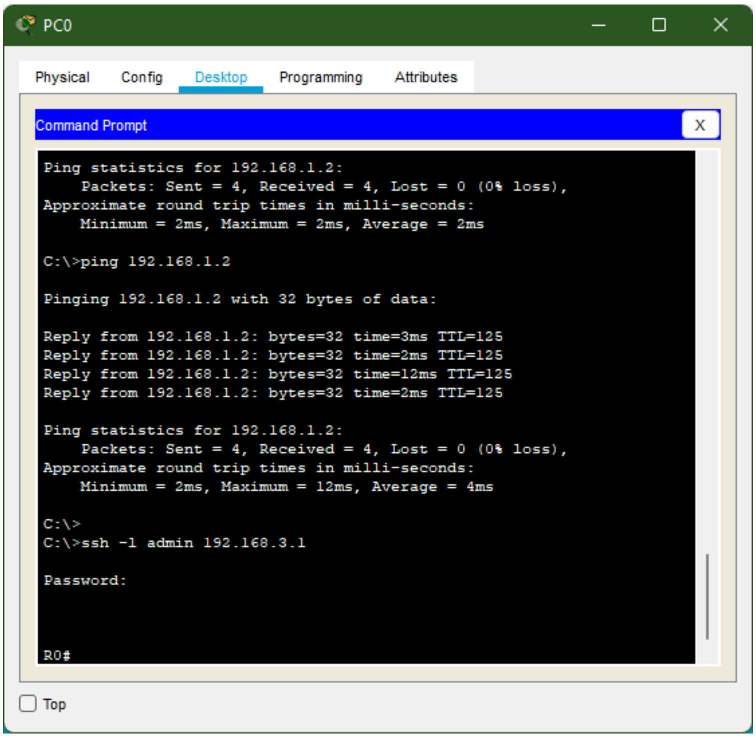
Step 1: Pinging SERVER from PC (Success)



```
Pinging 192.168.1.2 with 32 bytes of data:

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
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 = 2ms, Average = 2ms

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=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms 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 = 12ms, Average = 4ms

C:\>
```

,

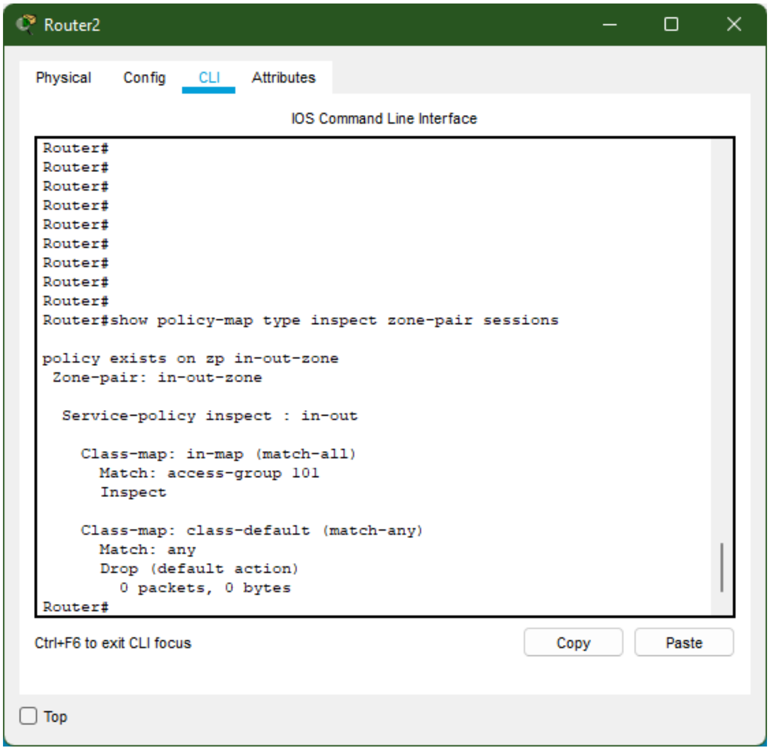
Step 2: Start an SSH session from PC to router 1



```
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 = 2ms, Average = 2ms

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=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms 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 = 12ms, Average = 4ms

C:\>
C:\>ssh -l admin 192.168.3.1

Password:



R0#
```

Step 3: Type following command in Router 2

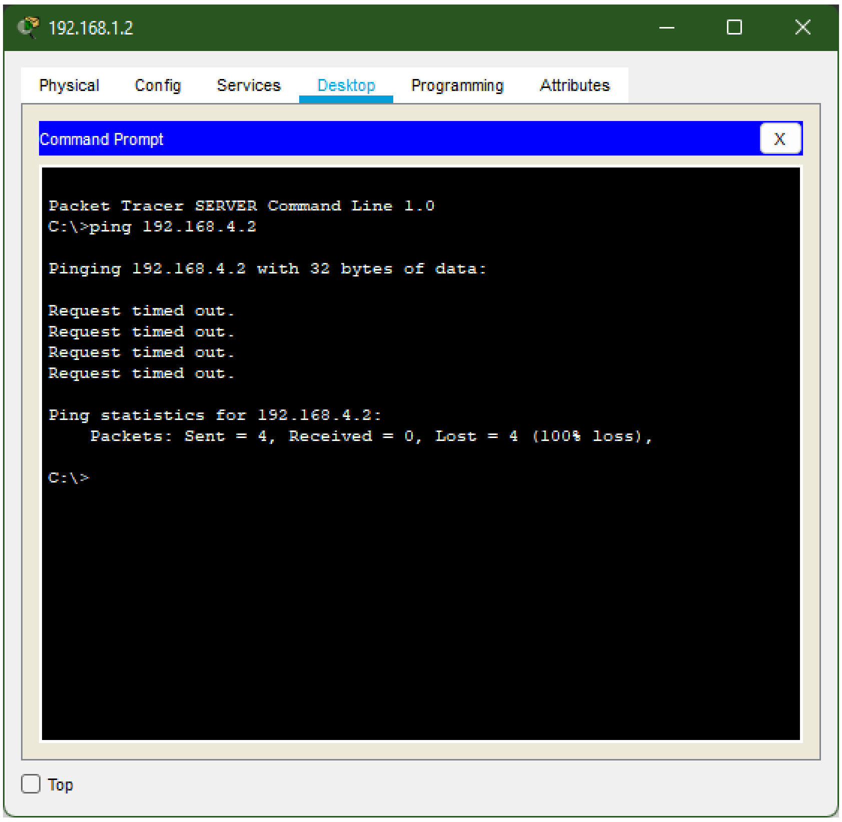
```
#show policy-map type inspect zone-pair sessions
```



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

policy exists on zp in-out-zone
 Zone-pair: in-out-zone

  Service-policy inspect : in-out

    Class-map: in-map (match-all)
      Match: access-group 101
      Inspect

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
Router#
```

PART 5: Testing the firewall functionality (From out-zone to in-zone)

Pinging pc from server (Failure)



```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

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

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Hence the firewall functionality is verified.

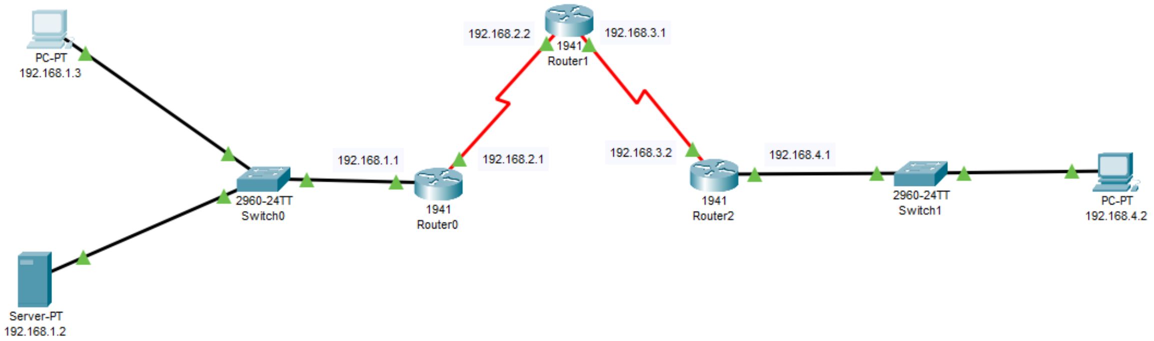
Practical 6

AIM: Configure IOS Intrusion Prevention System (IPS) Using the CLI

a. Enable IOS IPS.
b. Modify an IPS signature.

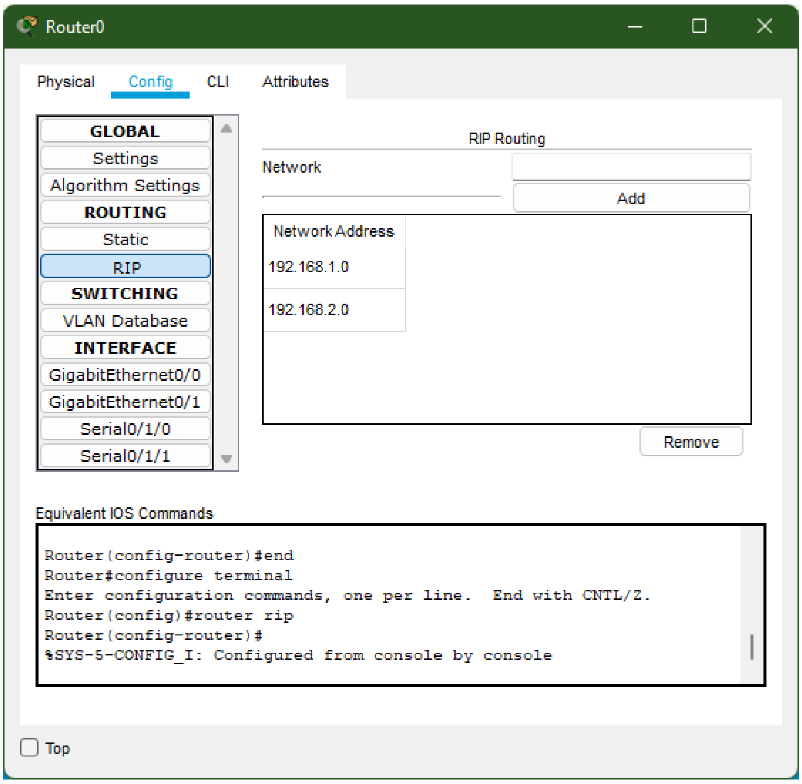
Solution:

<u>Topology</u>



Now, configure RIP Routing on All routers:

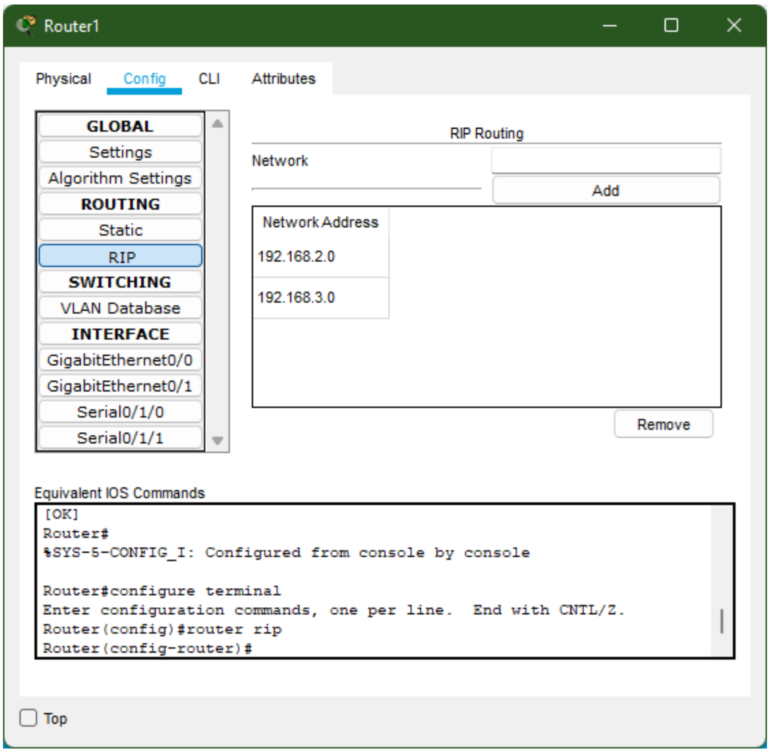
Router 0:



192.168.1.0
192.168.2.0

```
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
%SYS-5-CONFIG_I: Configured from console by console
```

Router 1:



RIP Routing

Network

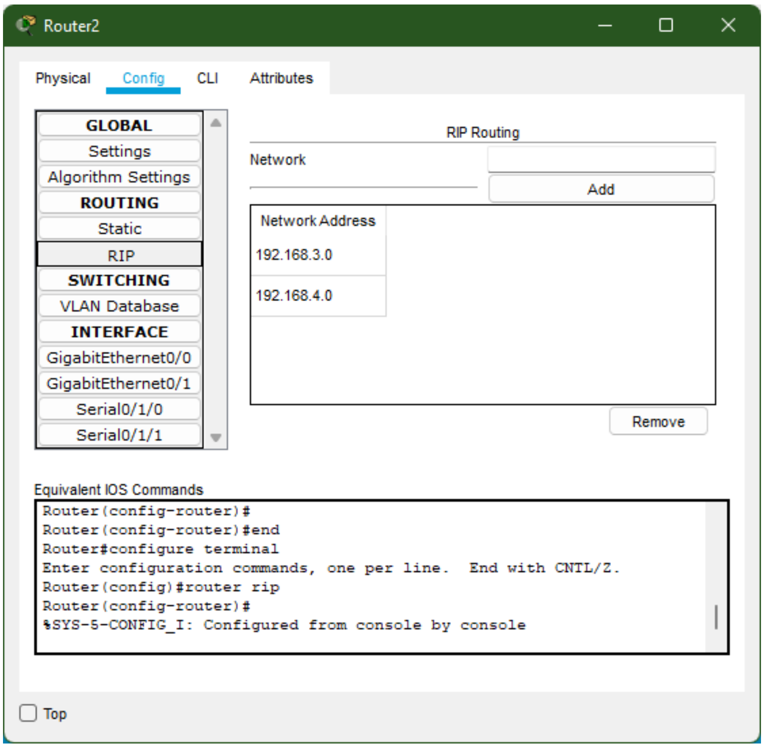
Network Address
192.168.2.0
192.168.3.0

Equivalent IOS Commands

```
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

☐ Top

Router 2:



RIP Routing

Network

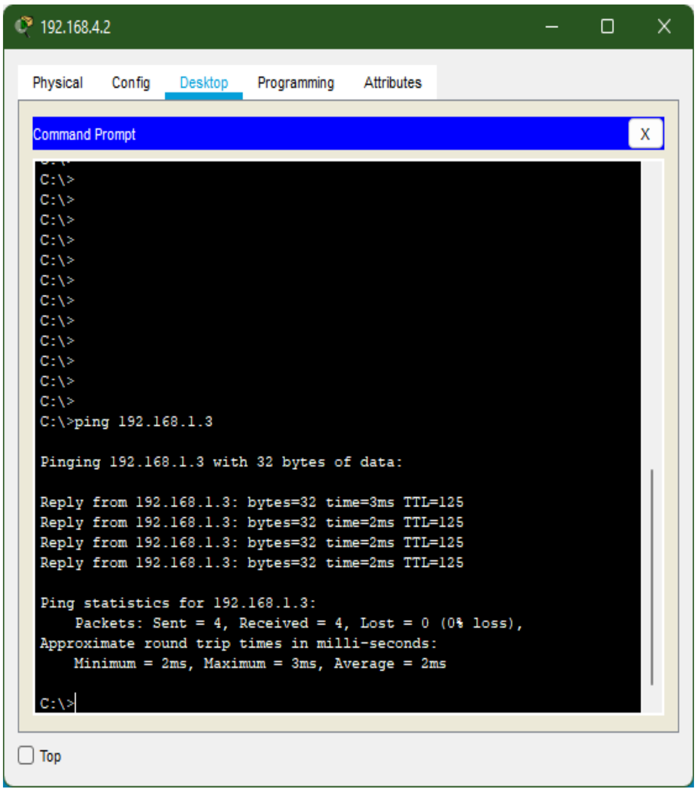
Network Address
192.168.3.0
192.168.4.0

Equivalent IOS Commands

```
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
%SYS-5-CONFIG_I: Configured from console by console
```

☐ Top

Now, verifying the routing using ping command from pc



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

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=3ms TTL=125
Reply from 192.168.1.3: bytes=32 time=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 = 3ms, Average = 2ms

C:\>
```

PART 1: Enable IOS IPS (Router 1)

Type following commands

```
Router>enable
Router#conf t
Router(config)#license boot module c1900 technology-package securityk9
Router#reload

Router#clock set 11:47:56 MARCH 3 2020
Router#mkdir sweet
Create directory filename [sweet]?
Created dir flash:sweet
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip ips config location flash:sweet
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired false
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
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
```

```
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will
be scanned
Router(config)#interface Serial0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#exit
```

PART 2: Modify the Signature

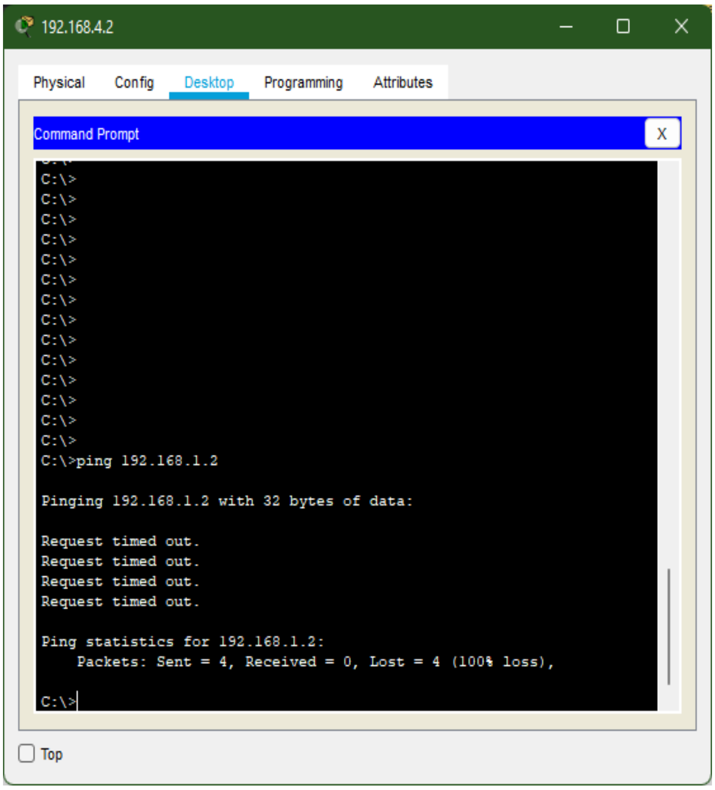
Type following commands in Router 1 again,

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
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
Router(config)#
```

Verifying IPS configuration:

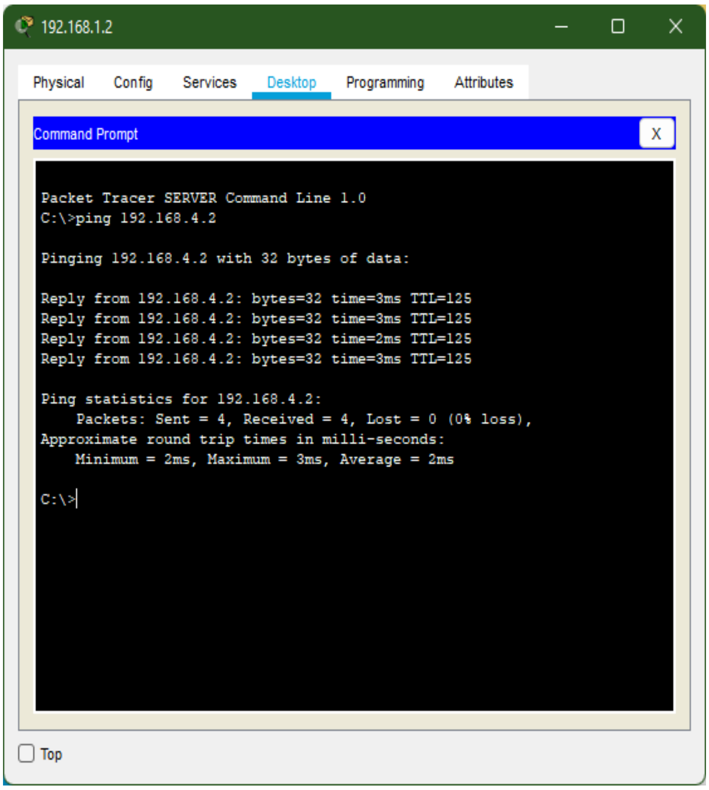
First pinging Server(192.168) from PC1(192.168.4.2)

(The ping will fail)

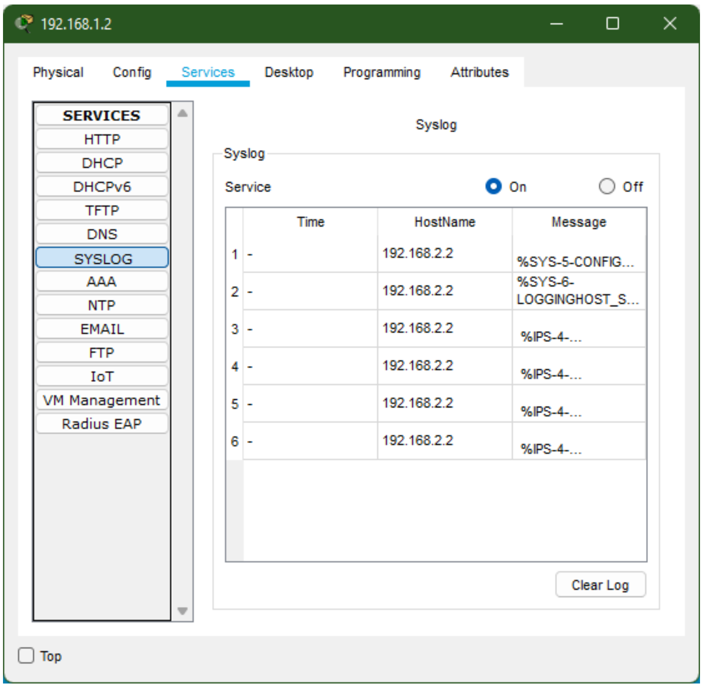


```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.2

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:\>
```

Pinging PC1(192.168.4.2) from Server(192.168.1.2)



```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=3ms TTL=125
Reply from 192.168.4.2: bytes=32 time=3ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```



Syslog

Syslog

Service ● On ○ Off

	Time	HostName	Message
1	-	192.168.2.2	%SYS-5-CONFIG...
2	-	192.168.2.2	%SYS-6-LOGGINGHOST_S...
3	-	192.168.2.2	%IPS-4-...
4	-	192.168.2.2	%IPS-4-...
5	-	192.168.2.2	%IPS-4-...
6	-	192.168.2.2	%IPS-4-...

Practical 7

AIM: Layer 2 Security

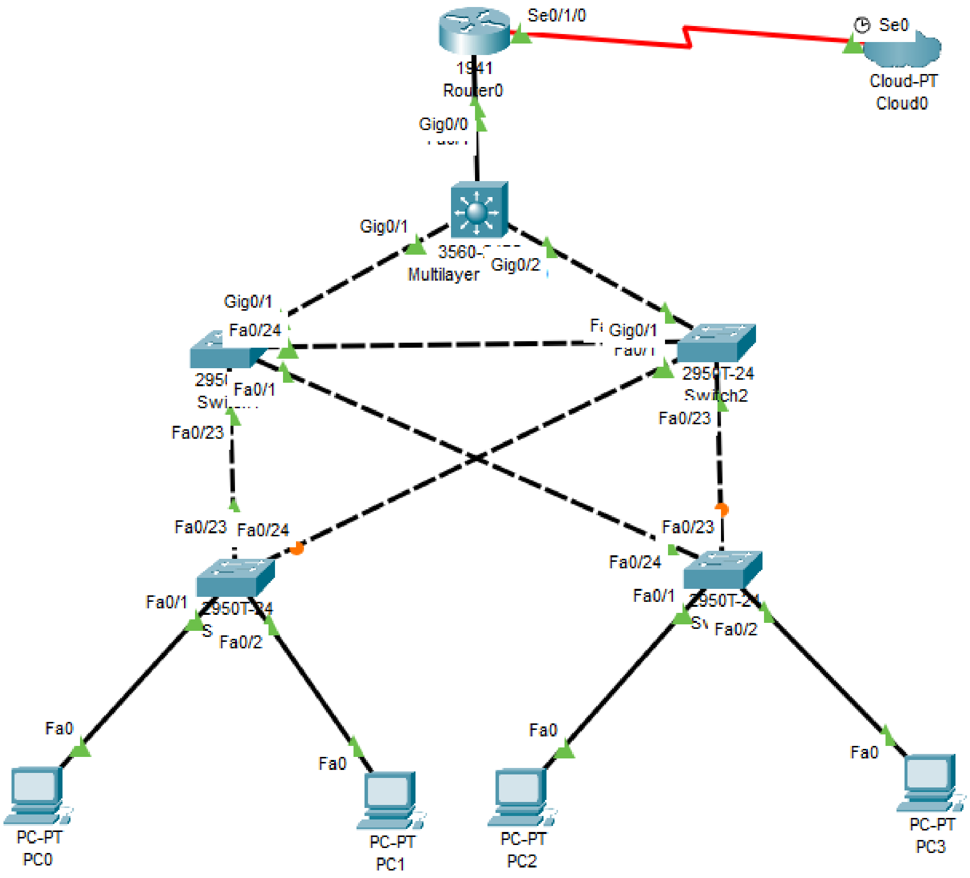
a. Assign the Central switch as the root bridge.

b. Secure spanning-tree parameters to prevent STP manipulation attacks.

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

Solution:

Topology

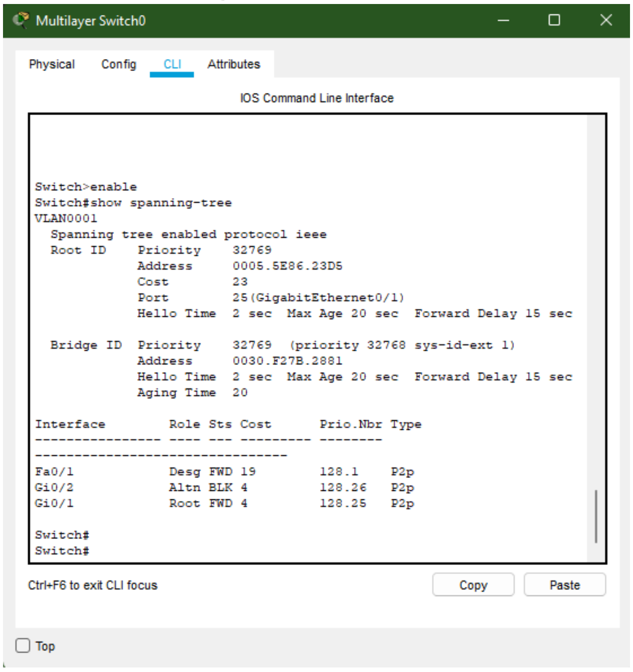


We'll use this topology with given port numbers.

PART 1: Root Bridge is set up

Go to MultilayerSwitch's CLI and type following commands:

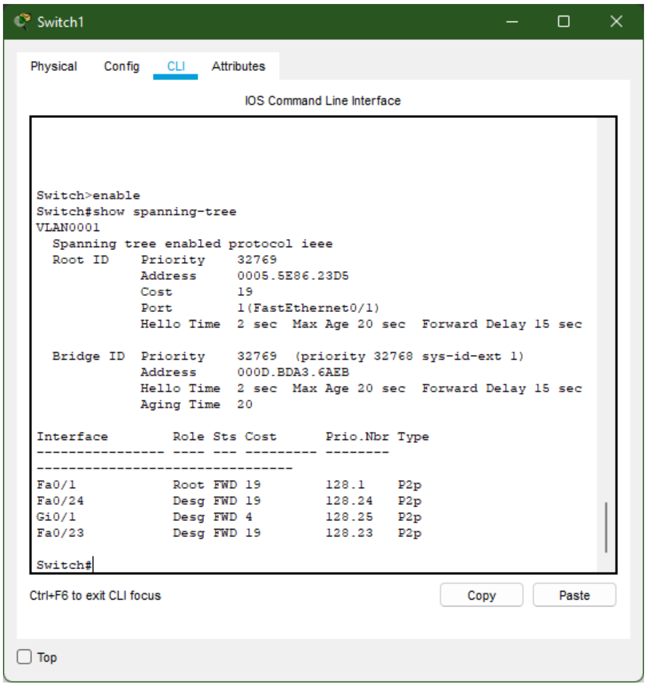
```
enable
show spanning-tree
```



```
Switch>enable
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E86.23D5
             Cost        23
             Port        25(GigabitEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0030.F27B.2881
             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
Gi0/2            Altn BLK 4         128.26   P2p
Gi0/1            Root FWD 4         128.25   P2p

Switch#
Switch#
```

Switch connected on GI0/1 is root, Go to, switch connected to the port GI0/1 and type these commands

```
enable
show spanning-tree
```

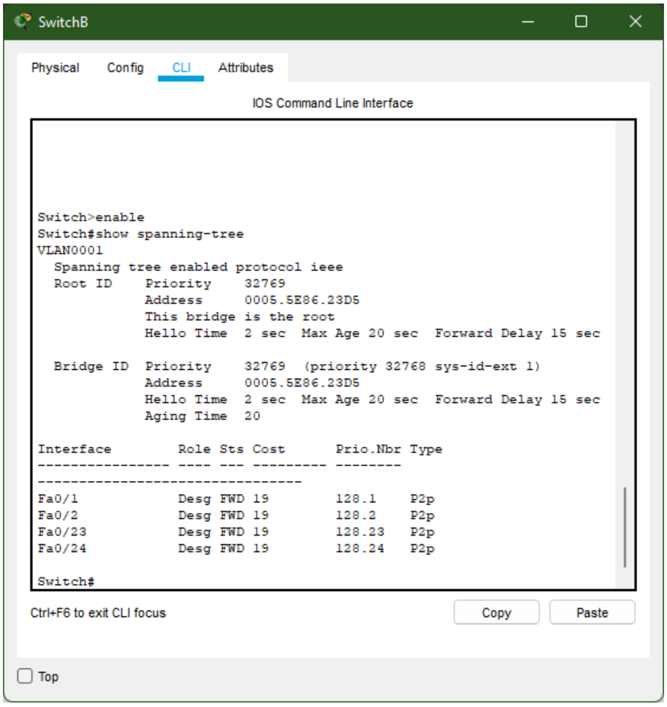


```
Switch>enable
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E86.23D5
             Cost        19
             Port        1(FastEthernet0/1)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     000D.BDA3.6AEB
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/24           Desg FWD 19        128.24   P2p
Gi0/1            Desg FWD 4         128.25   P2p
Fa0/23           Desg FWD 19        128.23   P2p

Switch#
```

Here we can see that another switch connected to Switch1's port Fa0/1 is root. Open that switch and type command:

```
enable
```

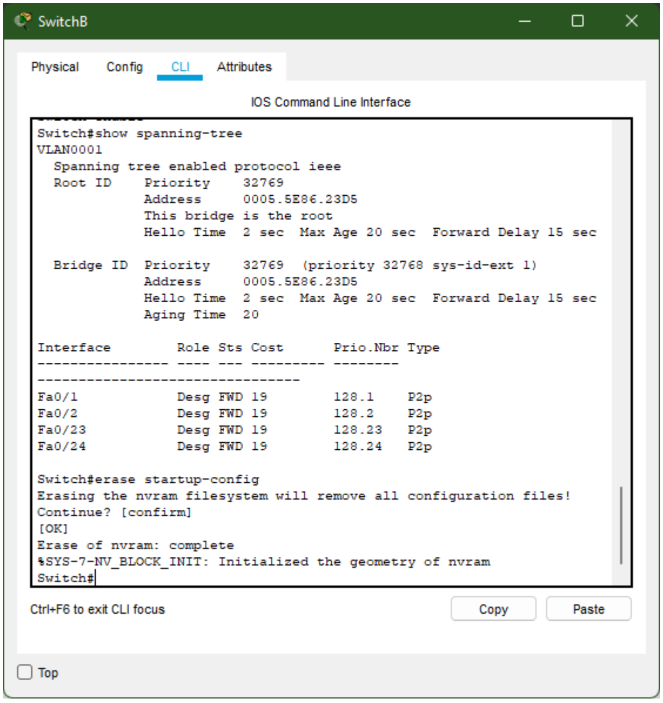
```
show spanning-tree
```



```
Switch>enable
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E86.23D5
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0005.5E86.23D5
             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
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p

Switch#
```

This is the root, we have to change the root to MultilayerSwitch for that type this command:

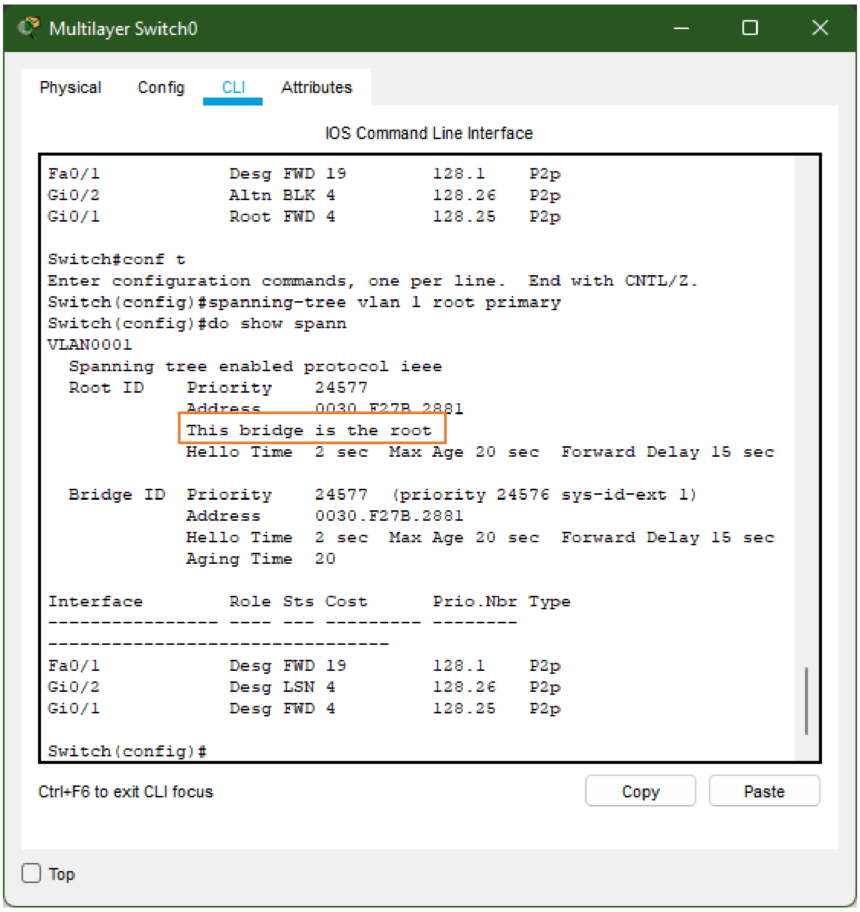
```
erase startup-config
```



```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.5E86.23D5
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0005.5E86.23D5
             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
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/23           Desg FWD 19        128.23   P2p
Fa0/24           Desg FWD 19        128.24   P2p

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#
```

Now, go-to multilayerSwitch and type following commands:

```
conf t
spanning-tree vlan 1 root primary
do show spann
```



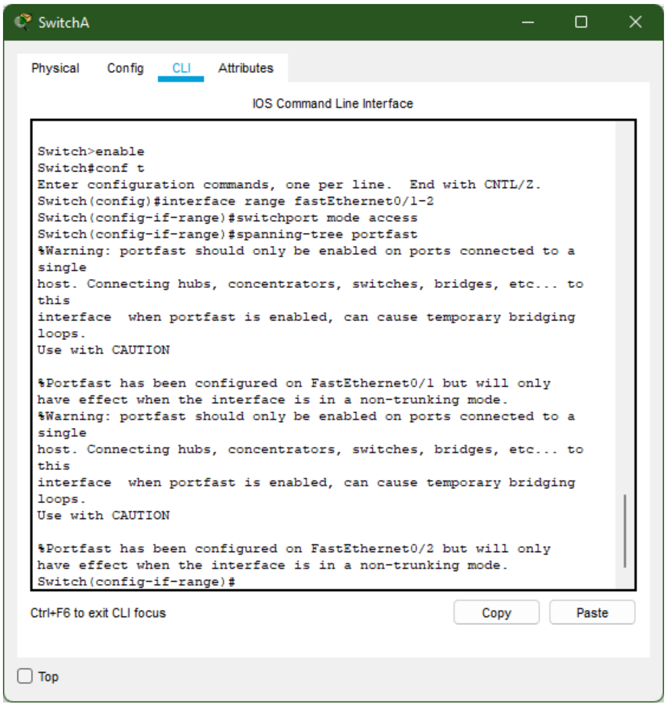
```
Fa0/1            Desg FWD 19        128.1    P2p
Gi0/2            Altn BLK 4         128.26   P2p
Gi0/1            Root FWD 4         128.25   P2p

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#spanning-tree vlan 1 root primary
Switch(config)#do show spann
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0030.F27B.2881
             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     0030.F27B.2881
             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
Gi0/2            Desg LSN 4         128.26   P2p
Gi0/1            Desg FWD 4         128.25   P2p

Switch(config)#
```

MultilayerSwitch is primary now.

PART 2: Protect Against STP Attack

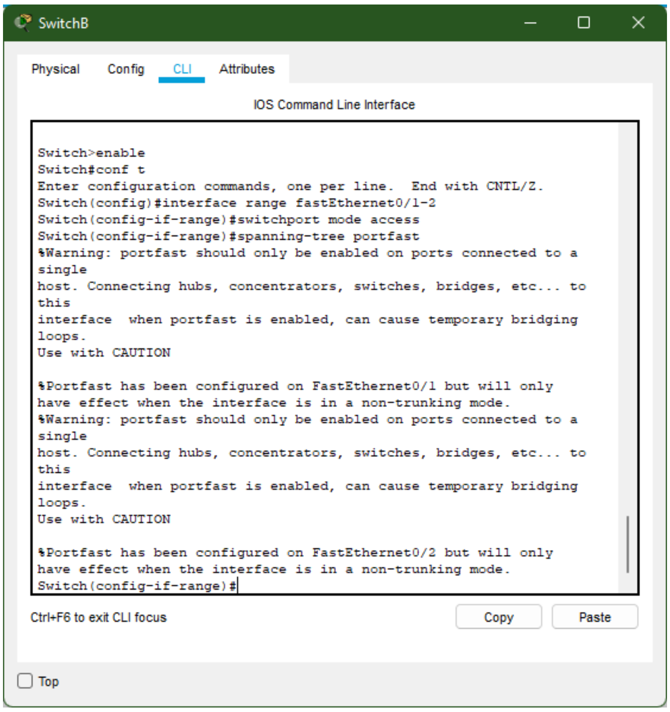
Open CLI of SwitchA and type following commands

```
enable
conf t
interface range fastEthernet0/1-2
switchport mode access
spanning-tree portfast
```



```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

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

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if-range)#
```

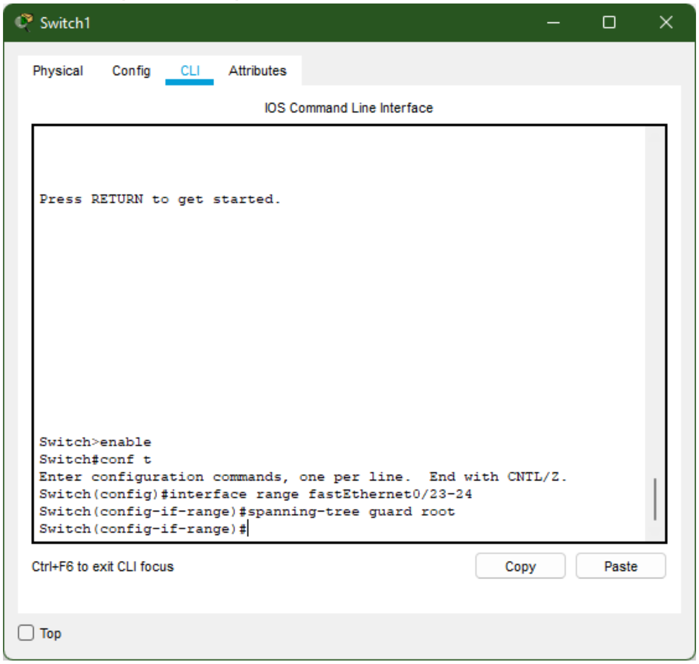
For SwitchB also type same commands



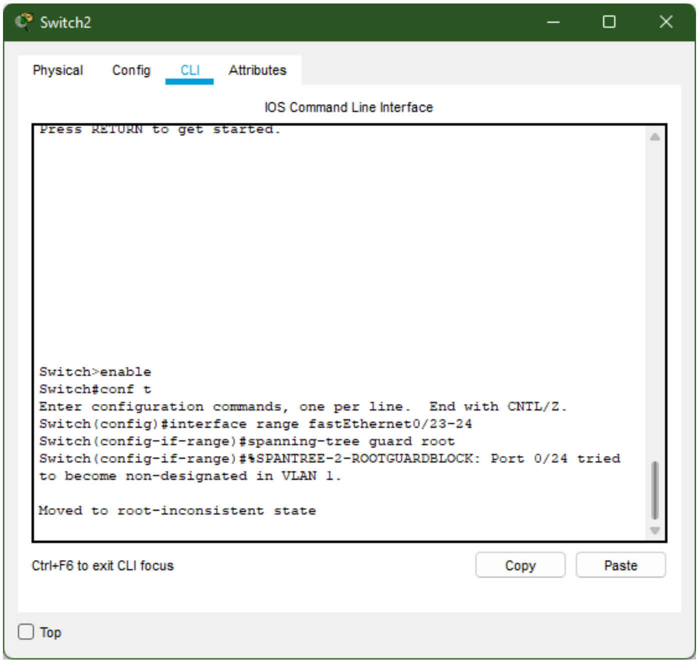
```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

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

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if-range)#
```

Commands for Switch1 and Switch 2:

```
enable
conf t
interface range fastEthernet0/23-24
spanning-tree guard root
```



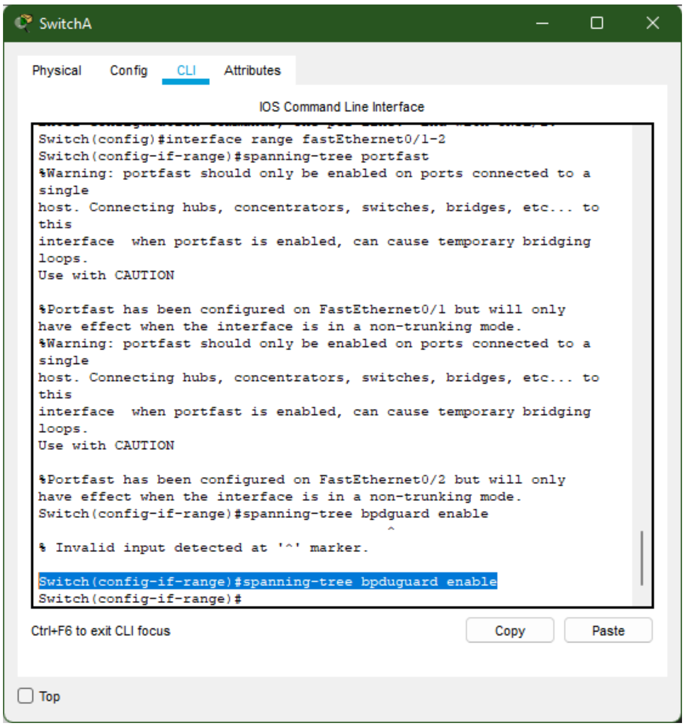
```
Press RETURN to get started.






Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet0/23-24
Switch(config-if-range)#spanning-tree guard root
Switch(config-if-range)#
```



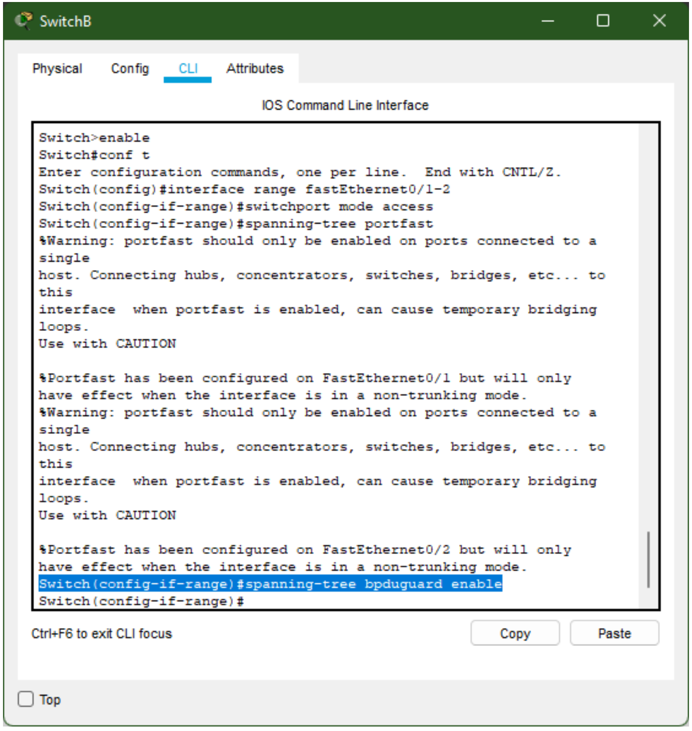
```
Press RETURN to get started.






Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet0/23-24
Switch(config-if-range)#spanning-tree guard root
Switch(config-if-range)#%SPANTREE-2-ROOTGUARDBLOCK: Port 0/24 tried
to become non-designated in VLAN 1.

Moved to root-inconsistent state
```

Now open cli of SwitchA and SwitchB and type following command:

```
spanning-tree bpdguard enable
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet0/1-2
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

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

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpdguard enable
                                         ^
% Invalid input detected at '^' marker.

Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#
```

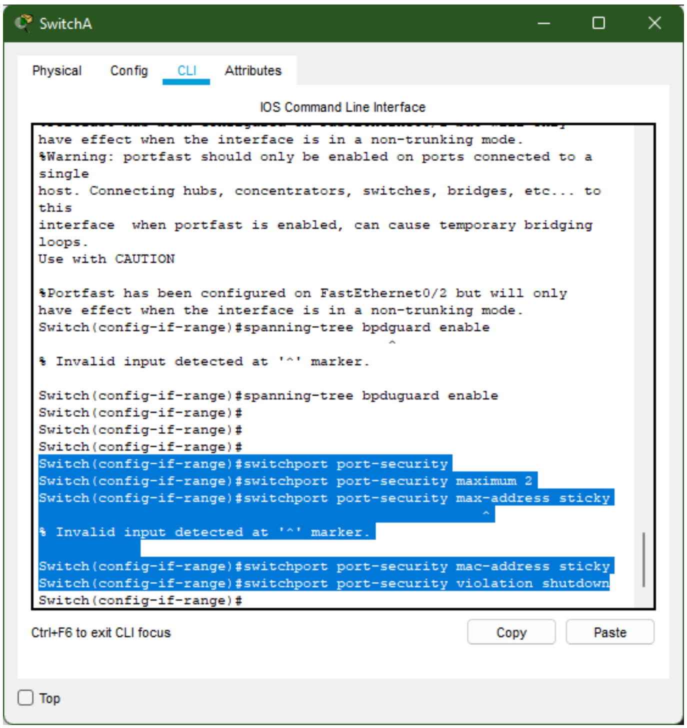


```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fastEthernet0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

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

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#
```

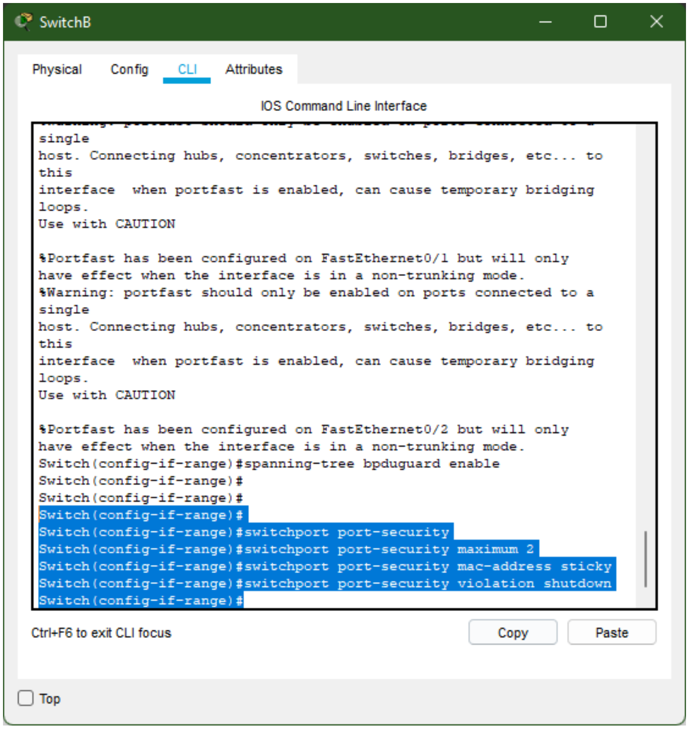
PART 3: Enable port security

Type these commands in SwitchA and SwitchB's cli.

```
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation shutdown
```



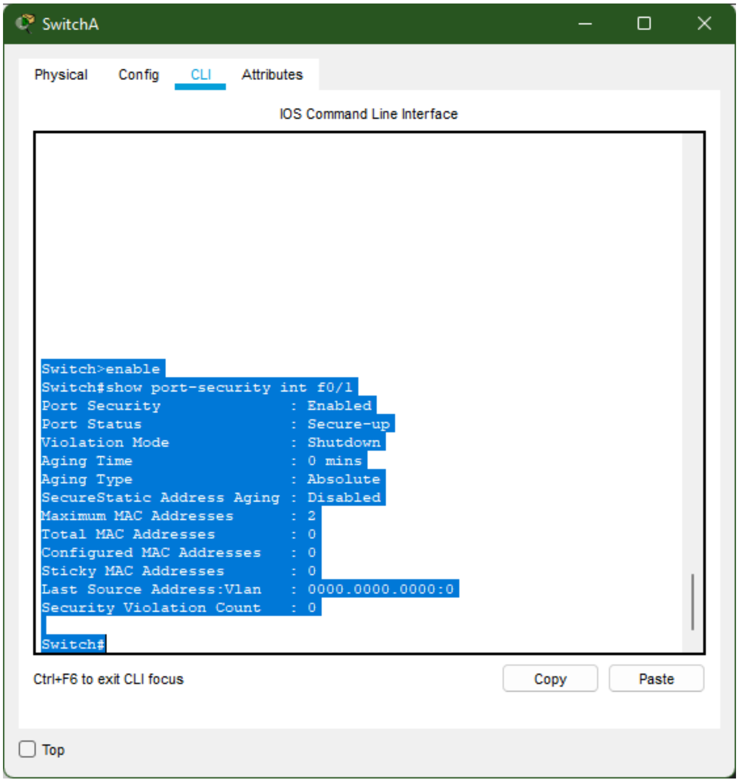
```
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Switch(config-if-range)#spanning-tree bpdguard enable
                                         ^
% Invalid input detected at '^' marker.

Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#switchport port-security max-address sticky
                                                    ^
% Invalid input detected at '^' marker.

Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#
```



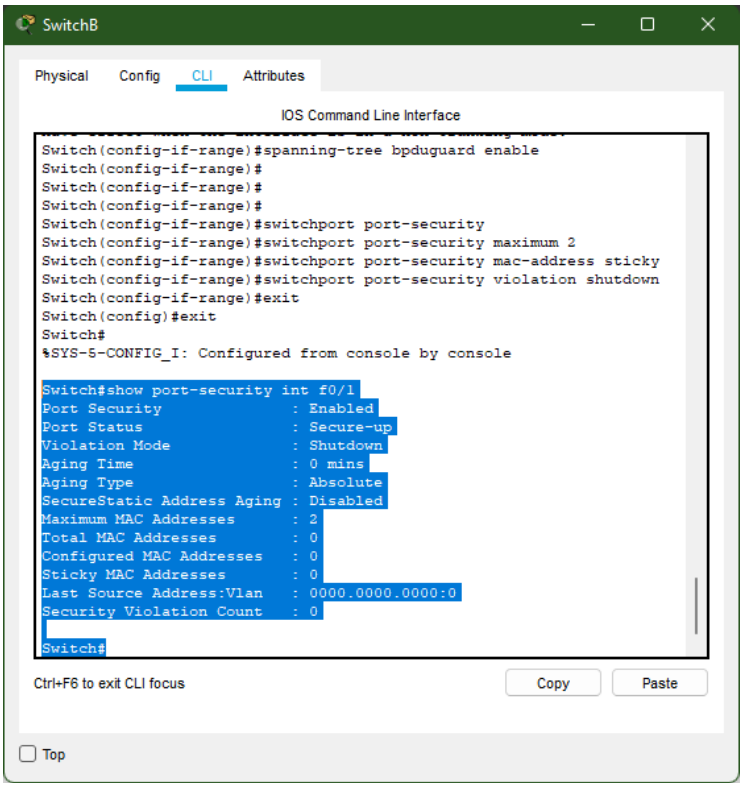
```
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

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

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

Verifying using command:

`show port-security int f0/1`



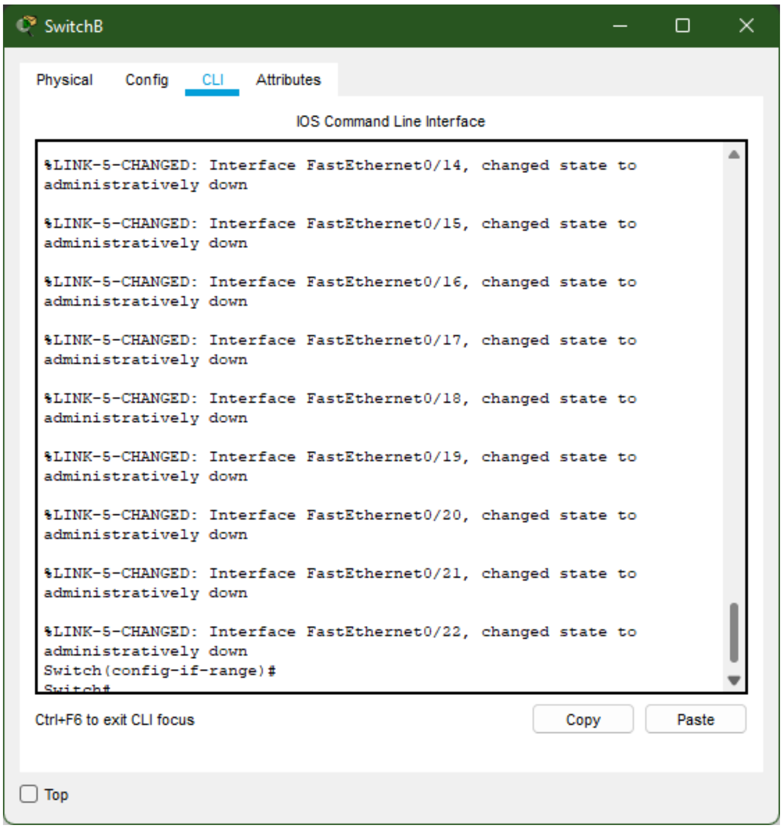
```
Switch>enable
Switch#show port-security int f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses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

Switch#
```



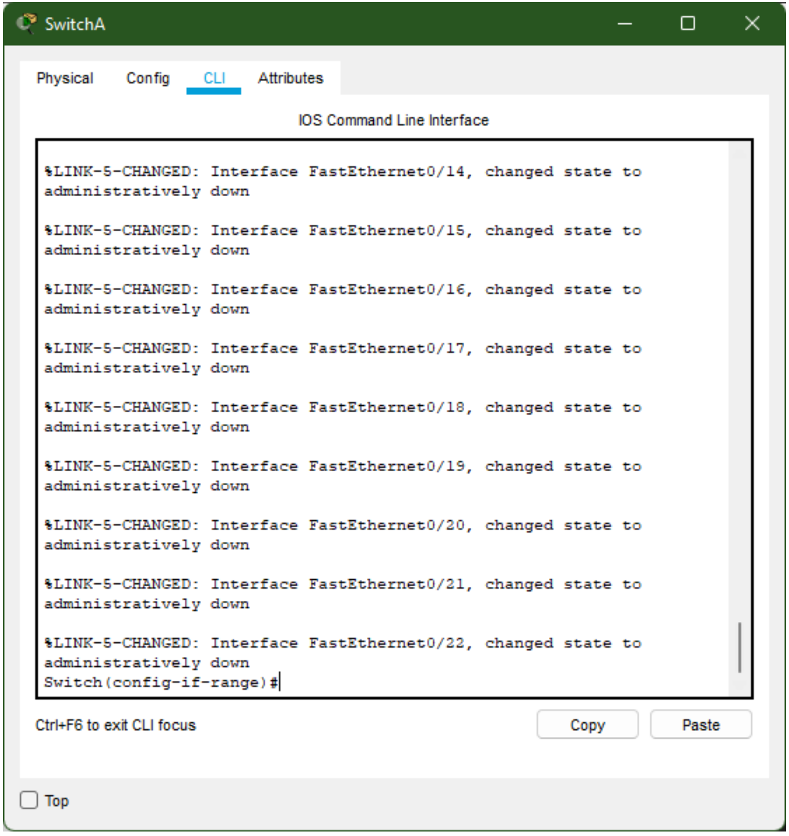
```
Switch(config-if-range)#spanning-tree bpduguard enable
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Switch#
```

Shutting down the remaining ports

```
conf t
interface range f0/3-22
shutdown
```



```
%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
Switch(config-if-range)#
Switch#
```



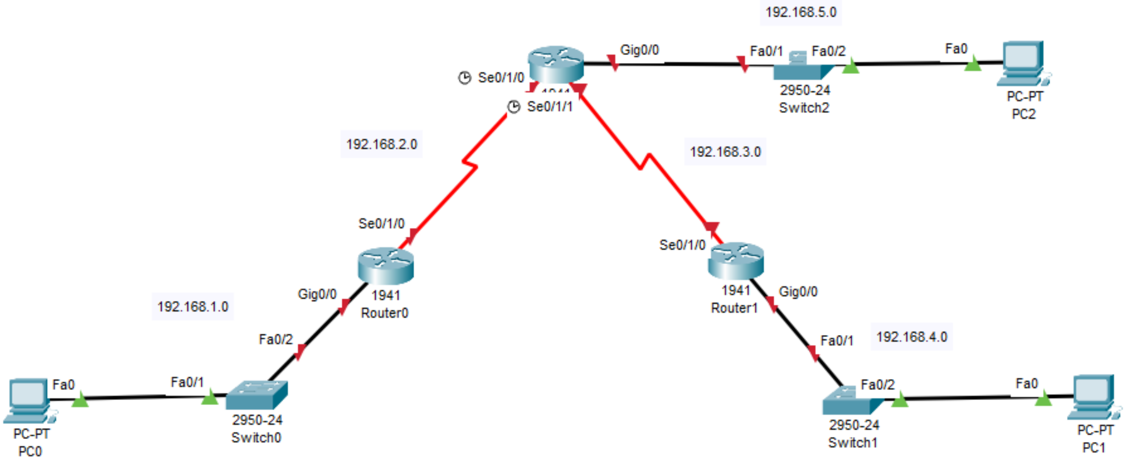
```
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to
administratively down

%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
Switch(config-if-range)#
```

Practical 8

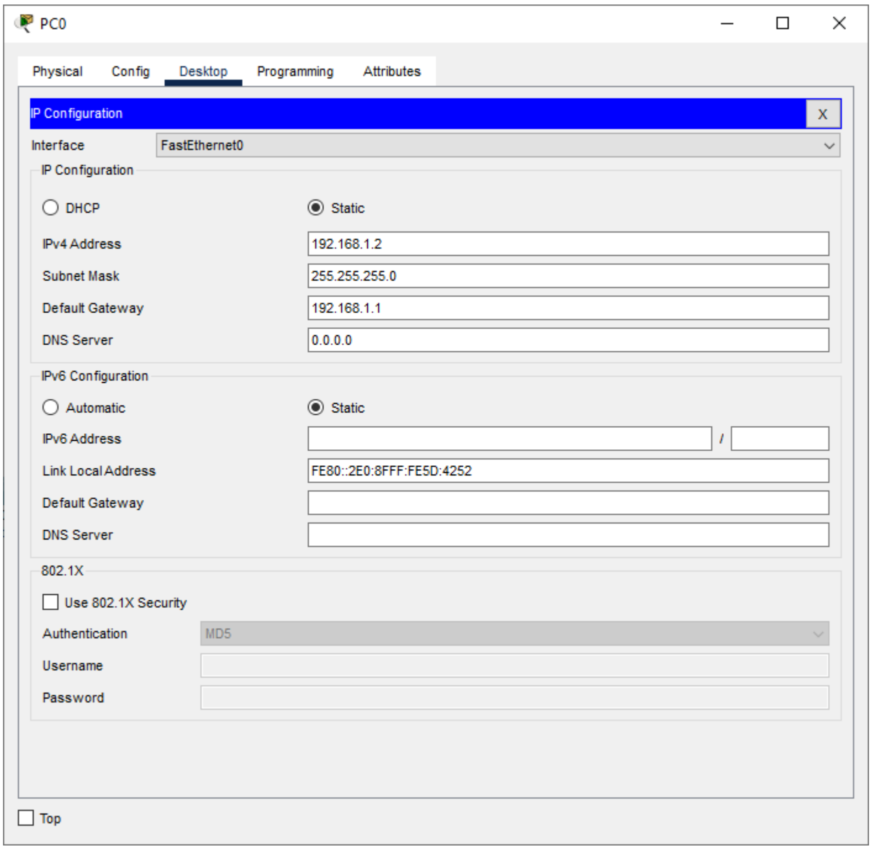
AIM: Configure and Verify a Site-to-Site IPsec VPN Using CLI

Solution:

Topology



Pc0 configuration



PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface	FastEthernet0

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::2E0:8FFF:FE5D:4252
Default Gateway	
DNS Server	

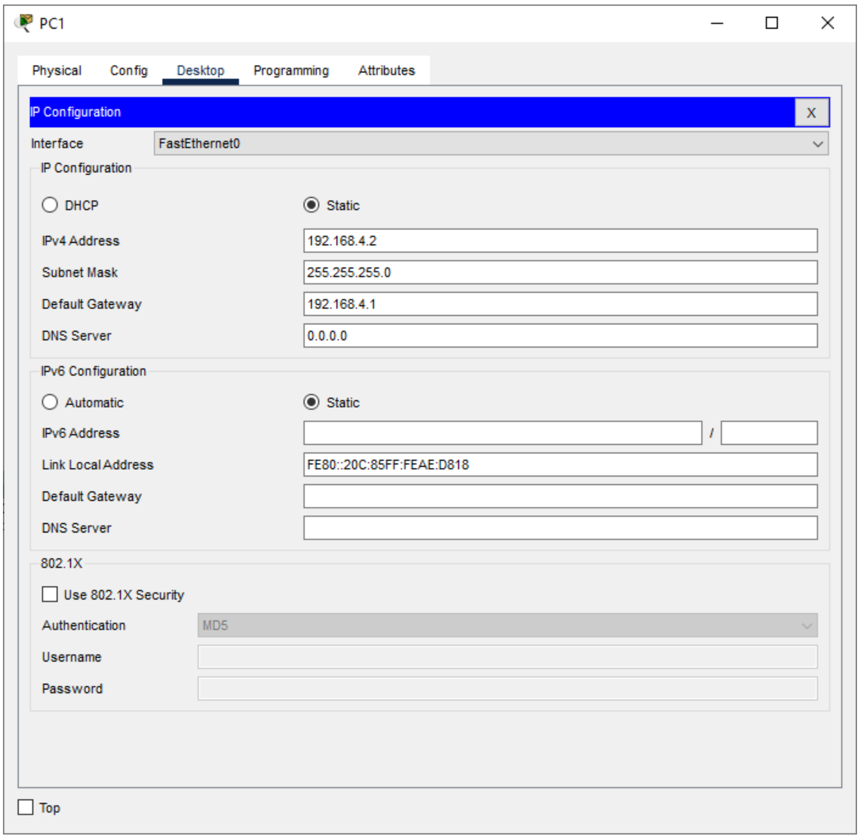
802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

Pc1 Configuration



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.4.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.4.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20C:85FF:FEAE:D818

Default Gateway:

DNS Server:

802.1X

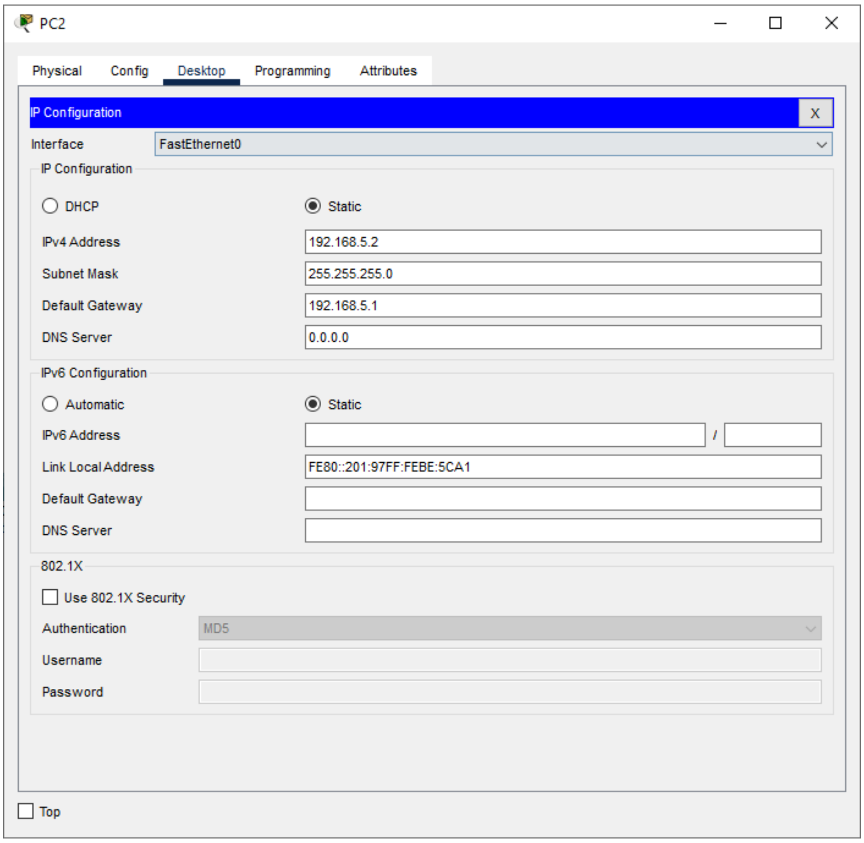
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Pc2 Configuration



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.5.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.5.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:97FF:FEBE:5CA1

Default Gateway:

DNS Server:

802.1X

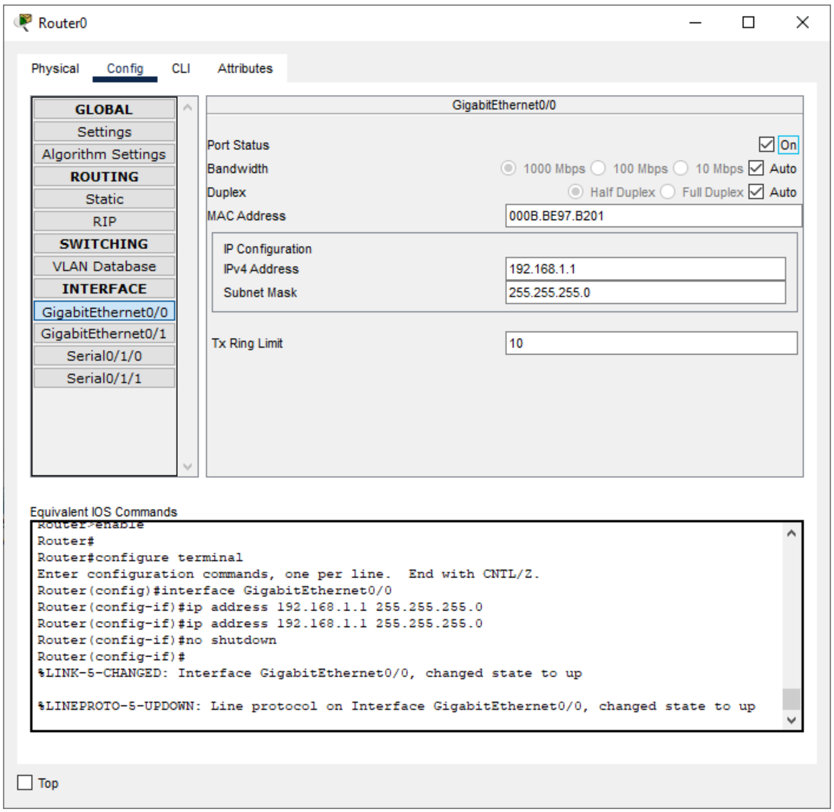
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Router0 configuration



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 000B.BE97.B201

IP Configuration

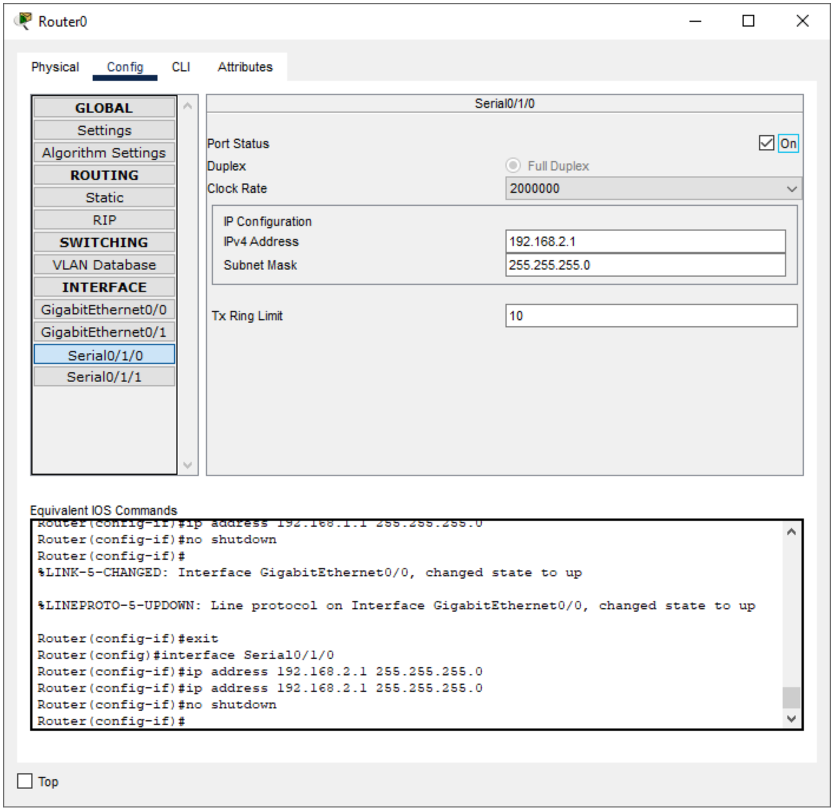
IPv4 Address 192.168.1.1

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)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(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
```



Serial0/1/0

Port Status ☑ On

Duplex ● Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.2.1

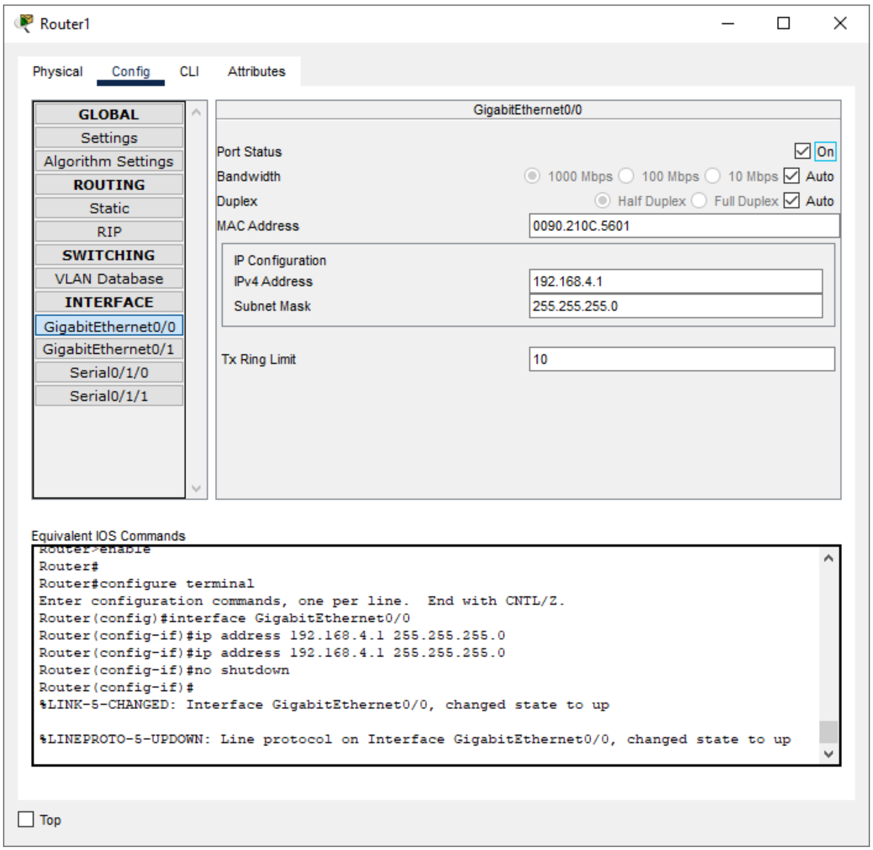
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(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

Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
```

Router1 configuration



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0090.210C.5601

IP Configuration

IPv4 Address 192.168.4.1

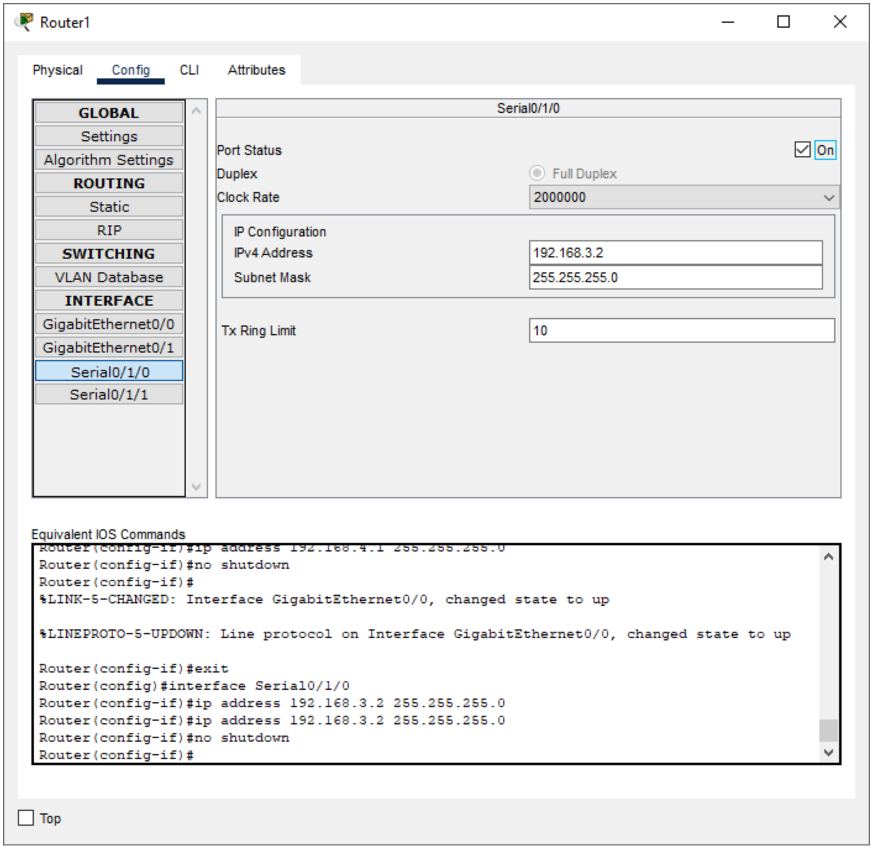
Subnet Mask 255.255.255.0

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 GigabitEthernet0/0
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shutdown
Router(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
```

□ Top



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

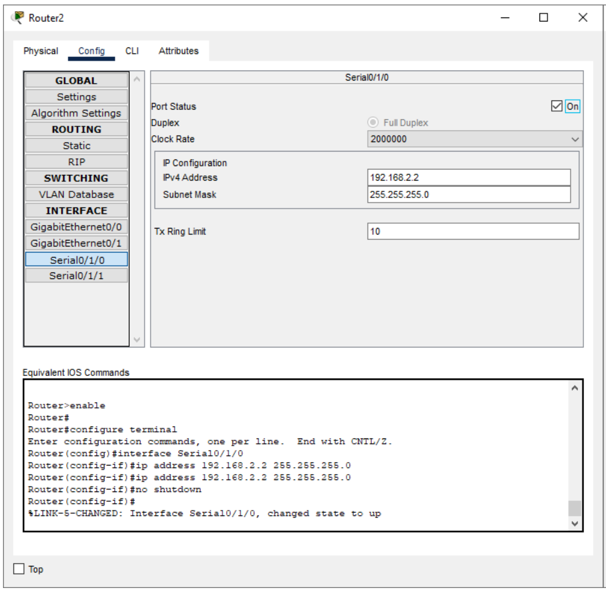
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shutdown
Router(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

Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
```

□ Top

Router2 configuration



Serial0/1/0

Port Status ☑ On

Duplex ● Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.2.2

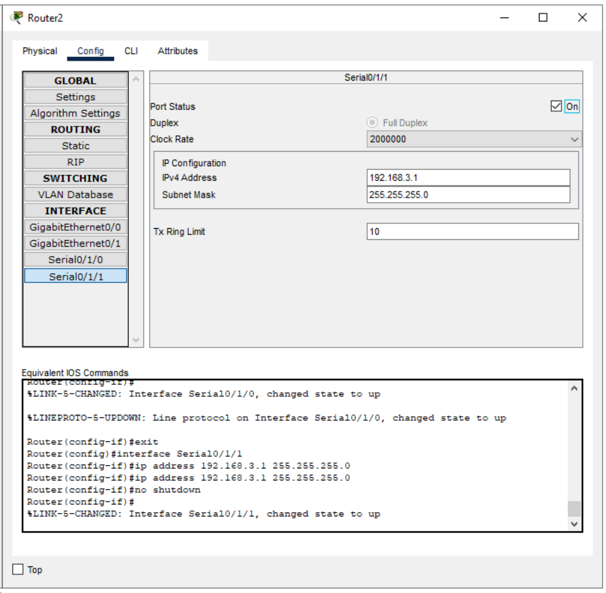
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
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)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#ip address 192.168.2.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
```

☐ Top



Serial0/1/1

Port Status ☑ On

Duplex ● Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.3.1

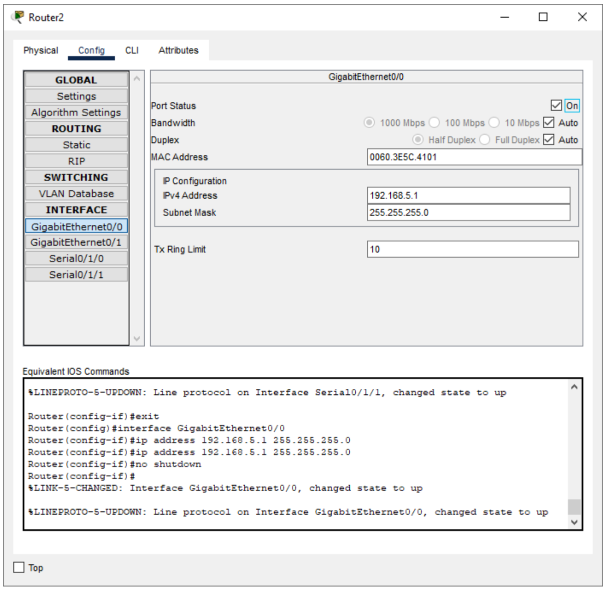
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#
%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

Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
```

☐ Top



GigabitEthernet0/0

Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ● Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0060.3E5C.4101

IP Configuration

IPv4 Address 192.168.5.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

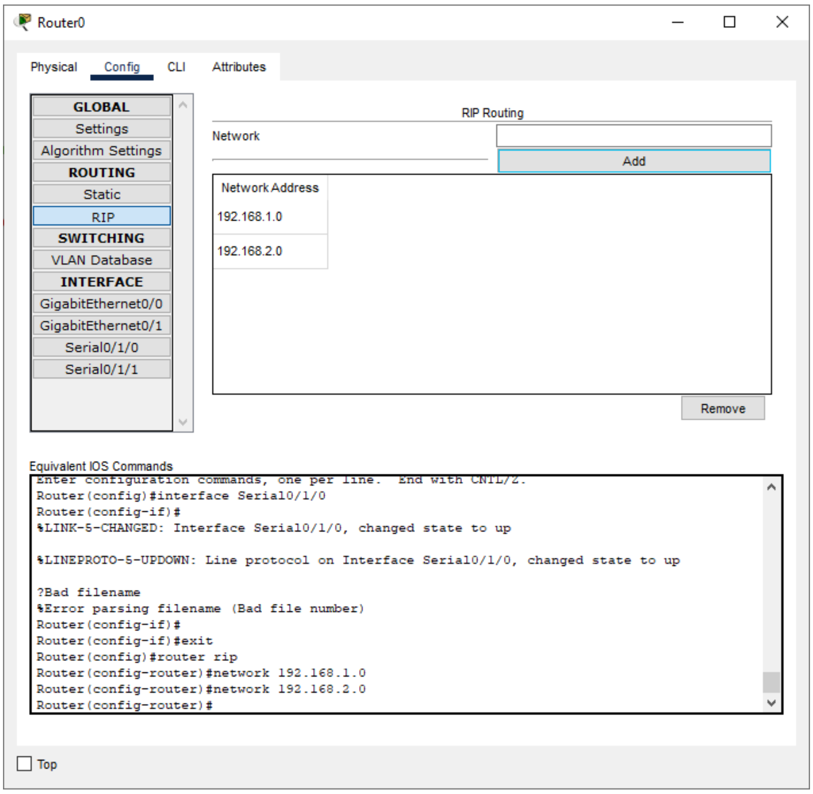
Equivalent IOS Commands

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

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shutdown
Router(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
```

☐ Top

Part 1: Configuring RIP on each router

Router 0



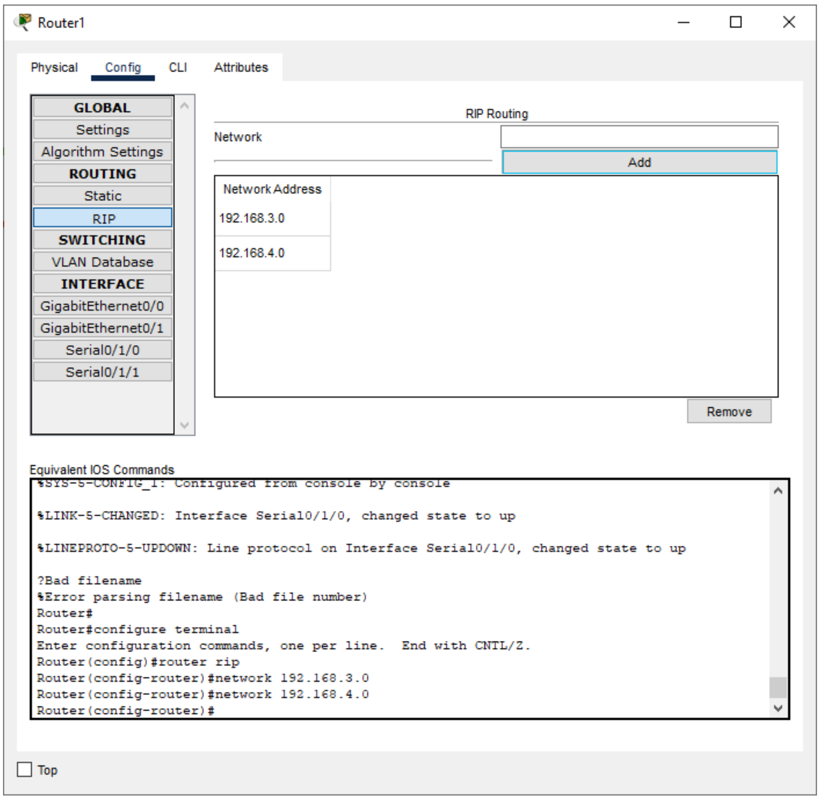
Network Address

192.168.1.0

192.168.2.0

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
%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

?Bad filename
%Error parsing filename (Bad file number)
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#
```

Router 1



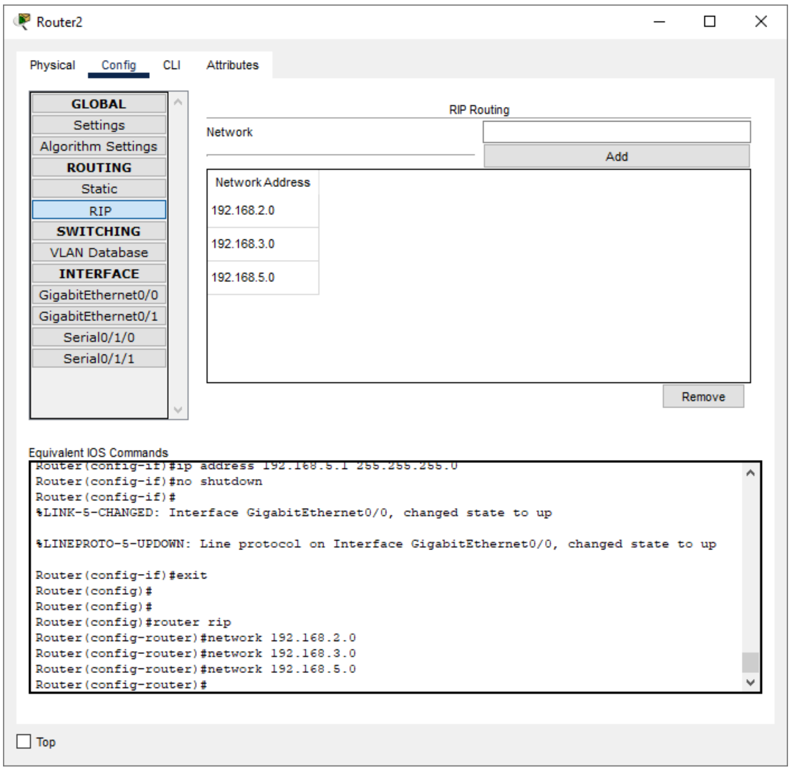
Network Address

192.168.3.0

192.168.4.0

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

%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

?Bad filename
%Error parsing filename (Bad file number)
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.4.0
Router(config-router)#
```

Router 2



RIP Routing

Network

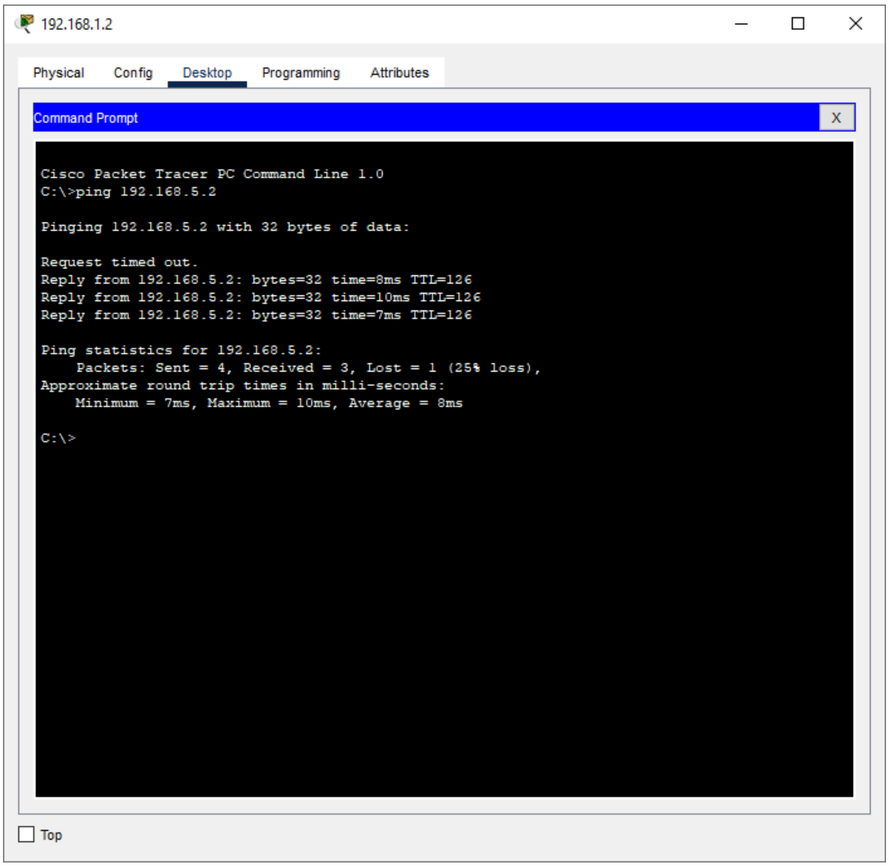
Network Address
192.168.2.0
192.168.3.0
192.168.5.0

Equivalent IOS Commands

```
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shutdown
Router(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

Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.5.0
Router(config-router)#
```

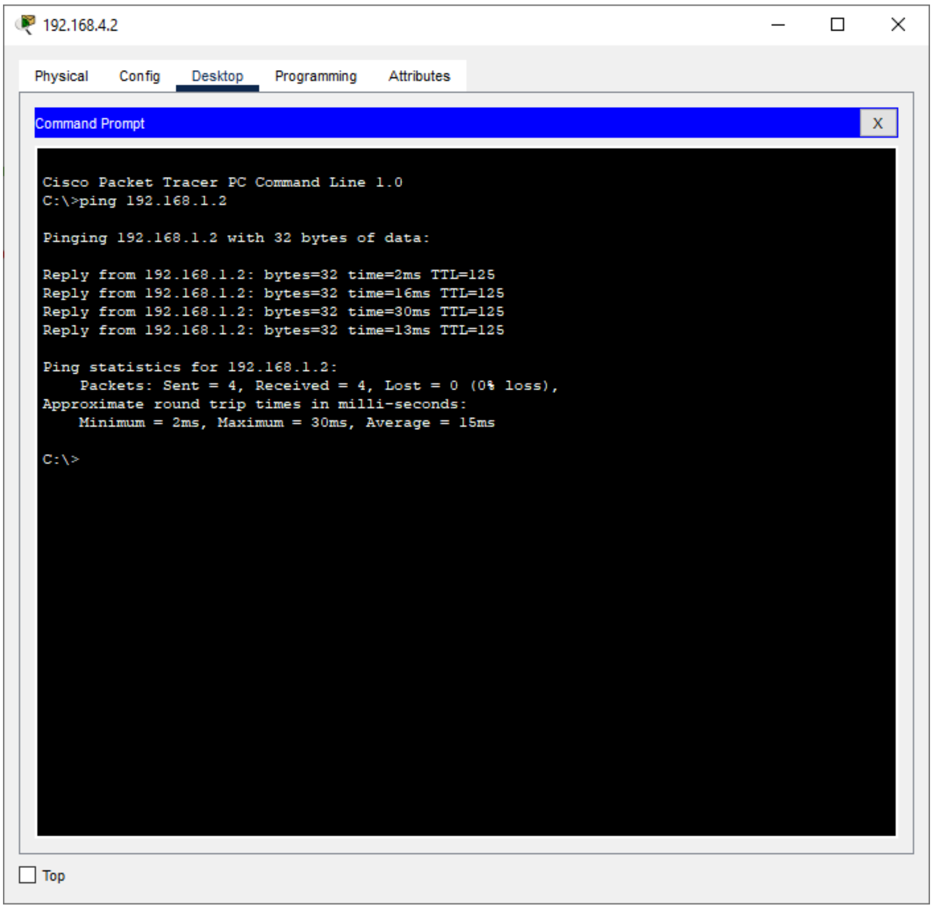
Now check the connectivity by ping command

PC0 (192.168.1.2) to PC2 (192.168.5.2)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.2: bytes=32 time=8ms TTL=126
Reply from 192.168.5.2: bytes=32 time=10ms TTL=126
Reply from 192.168.5.2: bytes=32 time=7ms TTL=126

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 10ms, Average = 8ms

C:\>
```

PC1 (192.168.4.2) to PC0 (192.168.1.2)



```
Cisco Packet Tracer PC Command Line 1.0
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=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=16ms TTL=125
Reply from 192.168.1.2: bytes=32 time=30ms TTL=125
Reply from 192.168.1.2: bytes=32 time=13ms 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 = 30ms, Average = 15ms

C:\>
```

Part 2: Configure IPSec parameters on router0

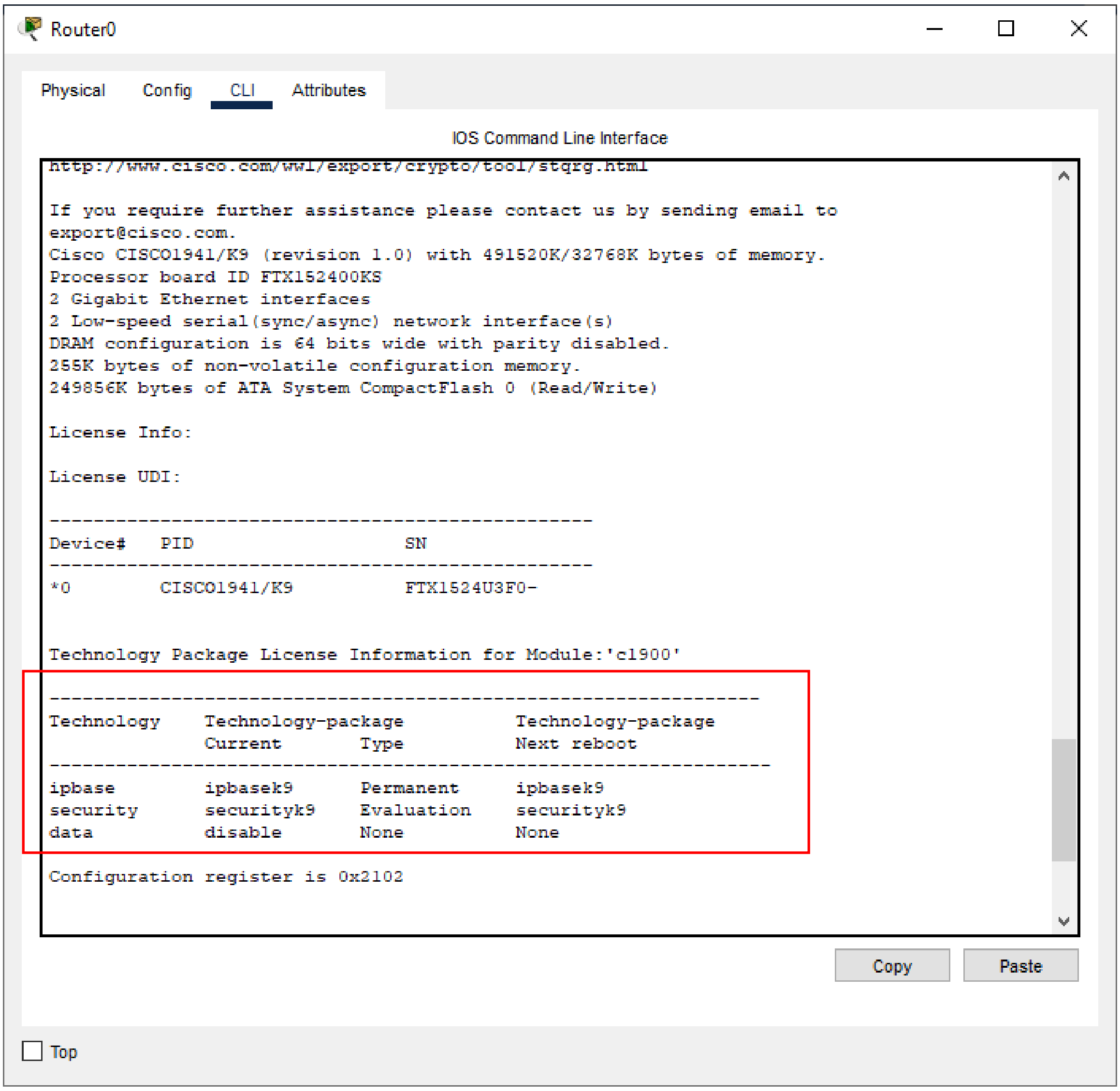
In order to configure the IPSec parameters on router0 we go by the following steps

Step 1: Enable the security package on router0 through the following commands in CLI mode

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#do write
Building configuration...
[OK]
Router(config)#exit
Router#reload
```

Now we need to check if the security package is enabled

```
Router>enable
Router#show version
```



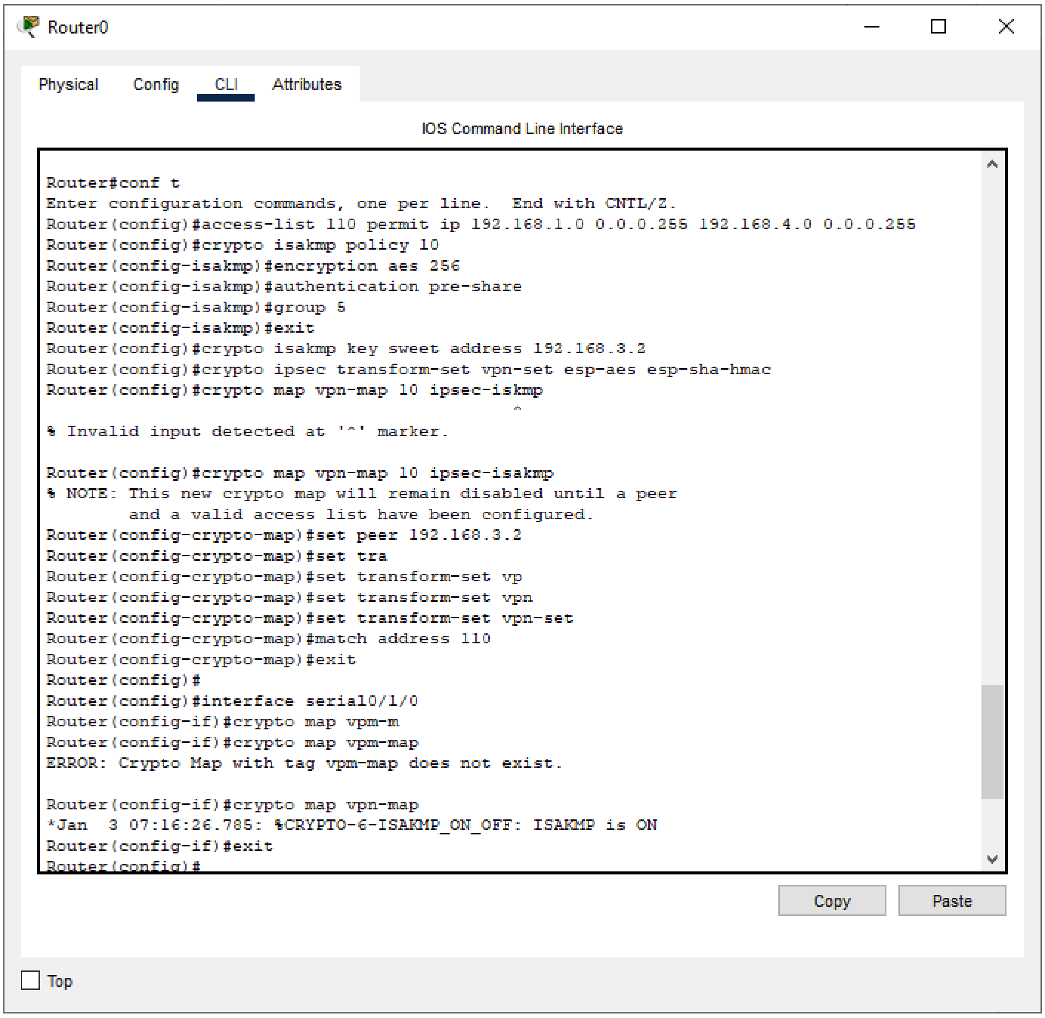
```
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

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
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524U3F0-


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
```

The above shows that the security package has been enabled

Step 2: Configuring IKA phase 1 ISAKMP policy on router0

Type the following command in CLI mode of router 0

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 110 permit ip 192.168.1.0 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 sweet 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
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
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
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
```



```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 permit ip 192.168.1.0 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 sweet 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-iskmp
                                                ^
% Invalid input detected at '^' marker.

Router(config)#crypto map vpn-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.168.3.2
Router(config-crypto-map)#set tra
Router(config-crypto-map)#set transform-set vp
Router(config-crypto-map)#set transform-set vpn
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 vpm-m
Router(config-if)#crypto map vpm-map
ERROR: Crypto Map with tag vpm-map does not exist.

Router(config-if)#crypto map vpn-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#exit
Router(config)#
```

Part 3: Configure IPSec parameters on router1

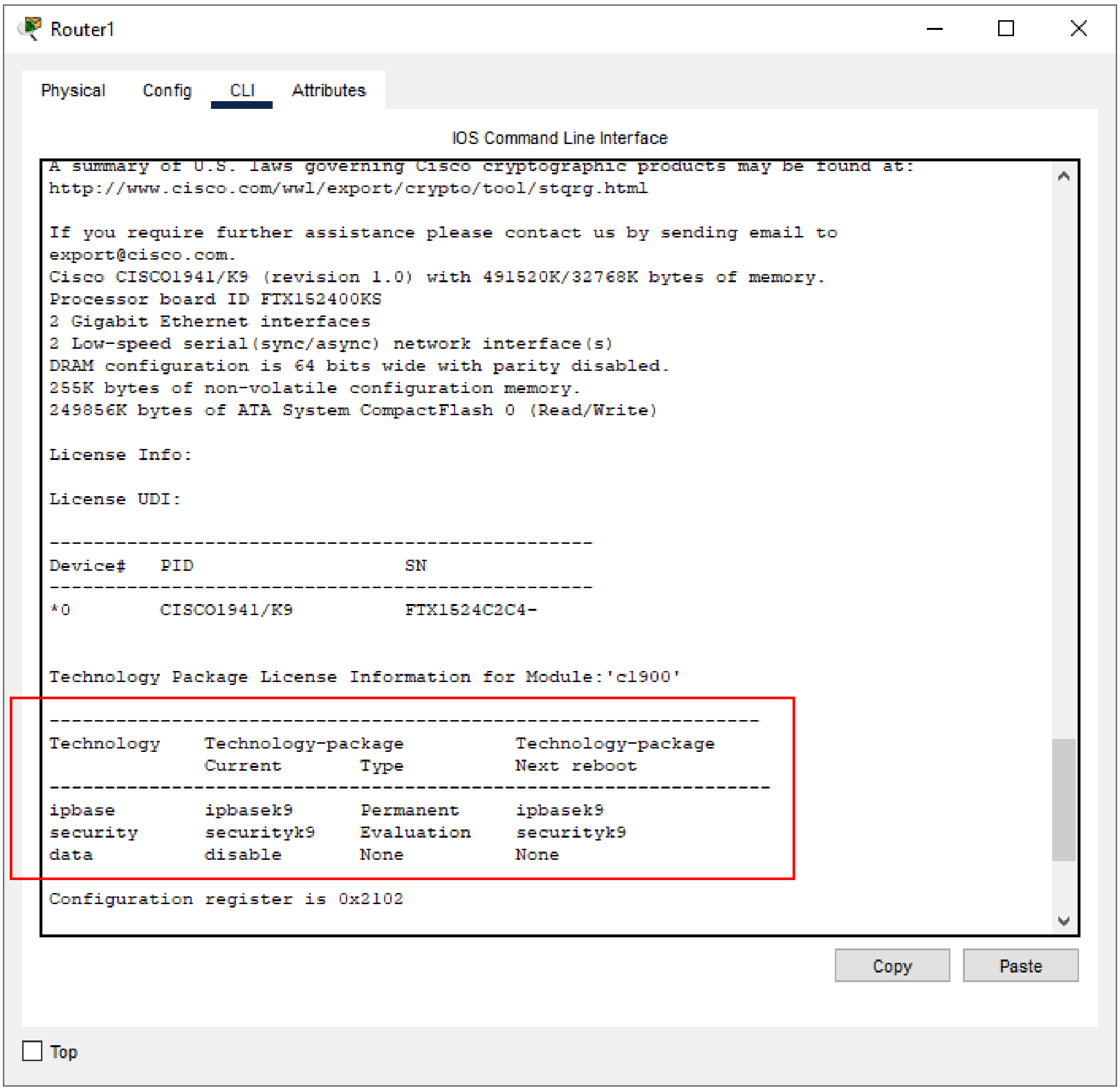
Step 1: Enable the security package on router1 through the following command.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#do write
Building configuration...
[OK]
Router(config)#exit
Router#reload
```

Now we need to check if the security package is enabled

```
Router>enable
```

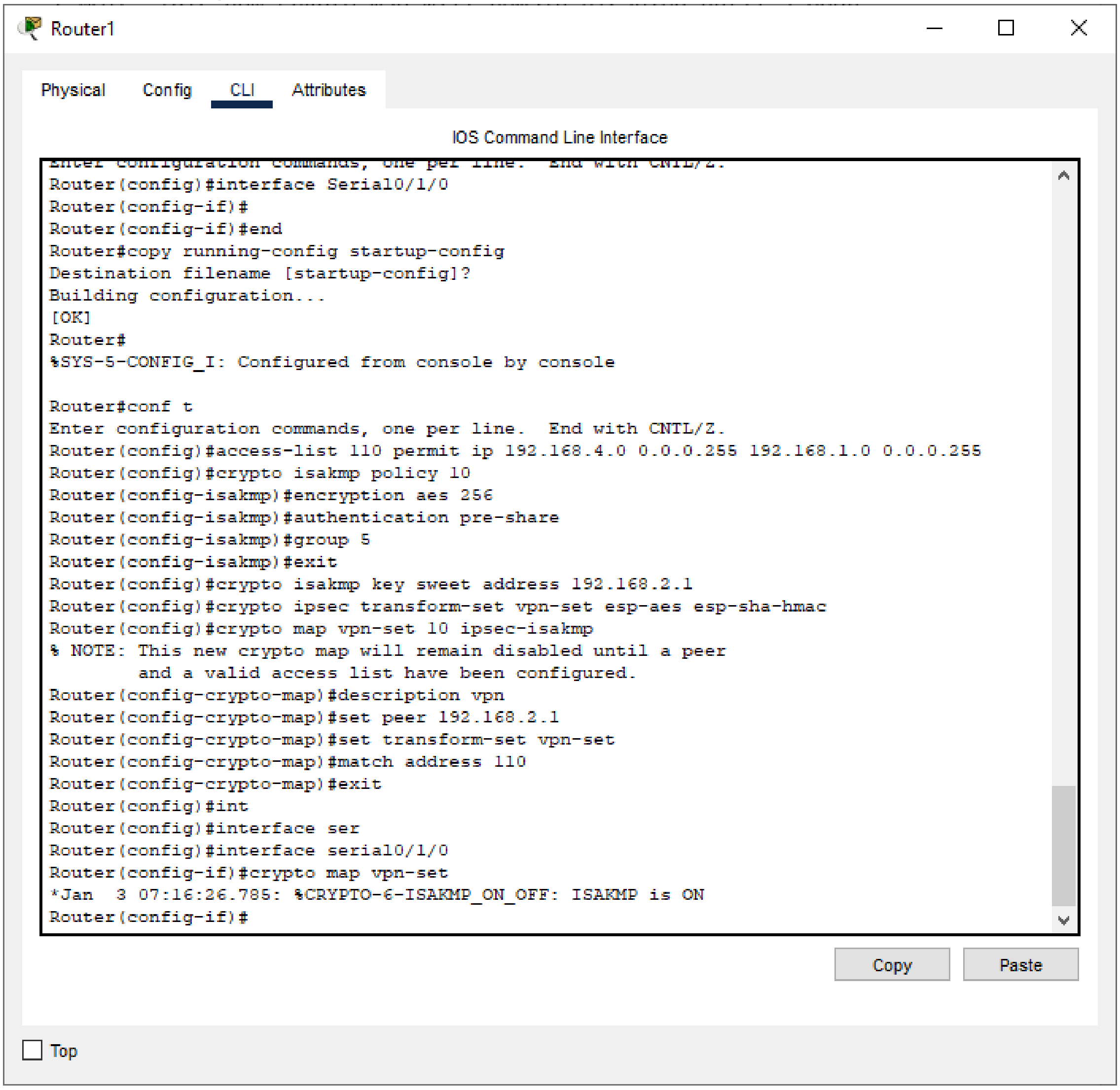
```
Router#show version
```



```
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
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524C2C4-


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
```

Step 2: Configuring IKA phase 1 ISAKMP policy on router1

```
Router#conf t
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 sweet 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
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
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 serial0/1/0
Router(config-if)#crypto map vpn-set
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
```



```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
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 sweet 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
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
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)#int
Router(config)#interface ser
Router(config)#interface serial0/1/0
Router(config-if)#crypto map vpn-set
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
```

Part 4: Verify the IPSec VPN

Step 1: Type the following command in the CLI mode of router 0

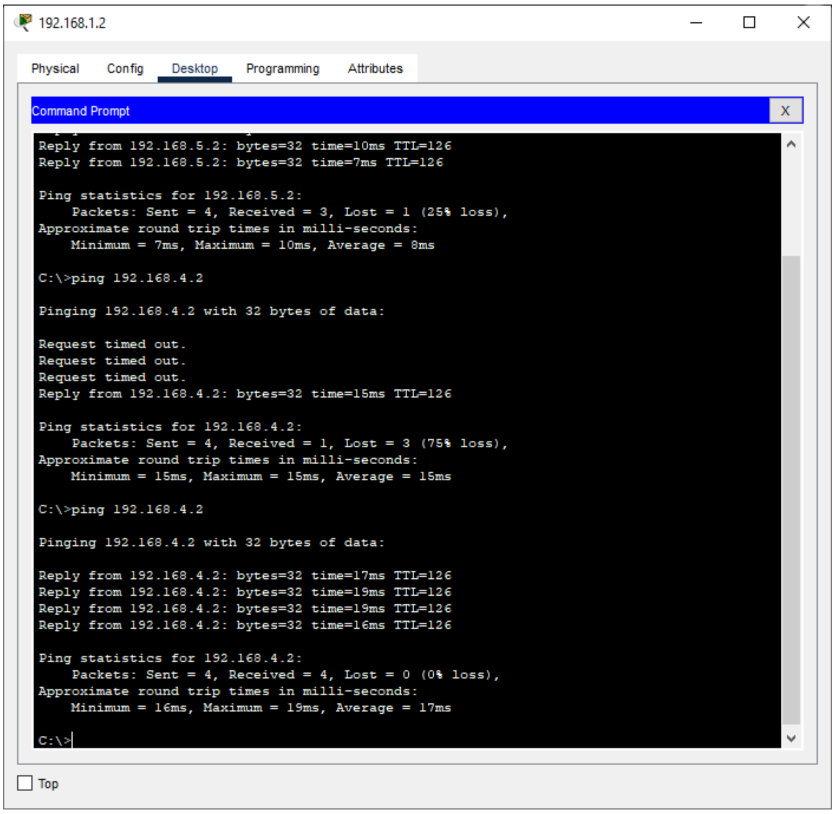
```
Router>enable
Router#show crypto ipsec sa
```

OUTPUT:

```
interface: Serial0/1/0
Crypto map tag: vpn-map, local addr 192.168.2.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
```

```
current_peer 192.168.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.:192.168.3.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

outbound esp sas:

outbound ah sas:

outbound pcp sas:

Router#
```

Step 2: Ping PC1 from PC0



```
Reply from 192.168.5.2: bytes=32 time=10ms TTL=126
Reply from 192.168.5.2: bytes=32 time=7ms TTL=126

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 10ms, Average = 8ms

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.4.2: bytes=32 time=15ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 15ms, Average = 15ms

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=17ms TTL=126
Reply from 192.168.4.2: bytes=32 time=19ms TTL=126
Reply from 192.168.4.2: bytes=32 time=19ms TTL=126
Reply from 192.168.4.2: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 19ms, Average = 17ms

C:\>
```

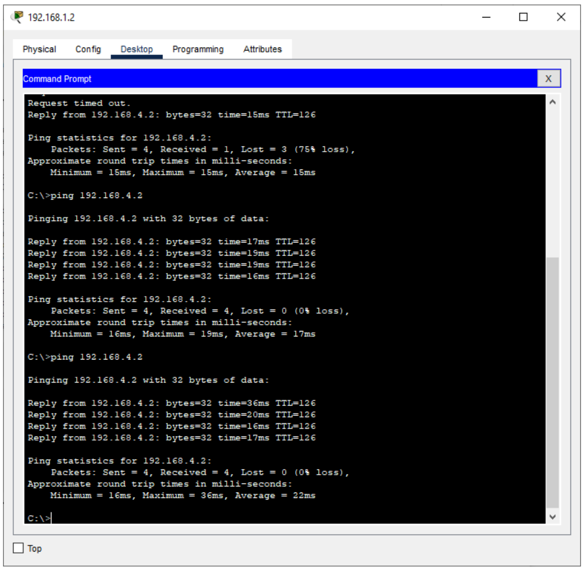
And now we check the router 0 by typing the following command

```
Router#show crypto ipsec sa
```

```
interface: Serial0/1/0
Crypto map tag: vpn-map, local addr 192.168.2.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer 192.168.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.:192.168.3.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x0322E684(52618884)

inbound esp sas:
spi: 0xC1647660(3244586592)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: FPGA:1, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/3487)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x0322E684(52618884)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/3487)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

```
Router#
```

Ping again PC1 from PC0



```
Request timed out.
Reply from 192.168.4.2: bytes=32 time=15ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 15ms, Average = 15ms

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=17ms TTL=126
Reply from 192.168.4.2: bytes=32 time=19ms TTL=126
Reply from 192.168.4.2: bytes=32 time=19ms TTL=126
Reply from 192.168.4.2: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 19ms, Average = 17ms

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=36ms TTL=126
Reply from 192.168.4.2: bytes=32 time=20ms TTL=126
Reply from 192.168.4.2: bytes=32 time=16ms TTL=126
Reply from 192.168.4.2: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 36ms, Average = 22ms

C:\>
```

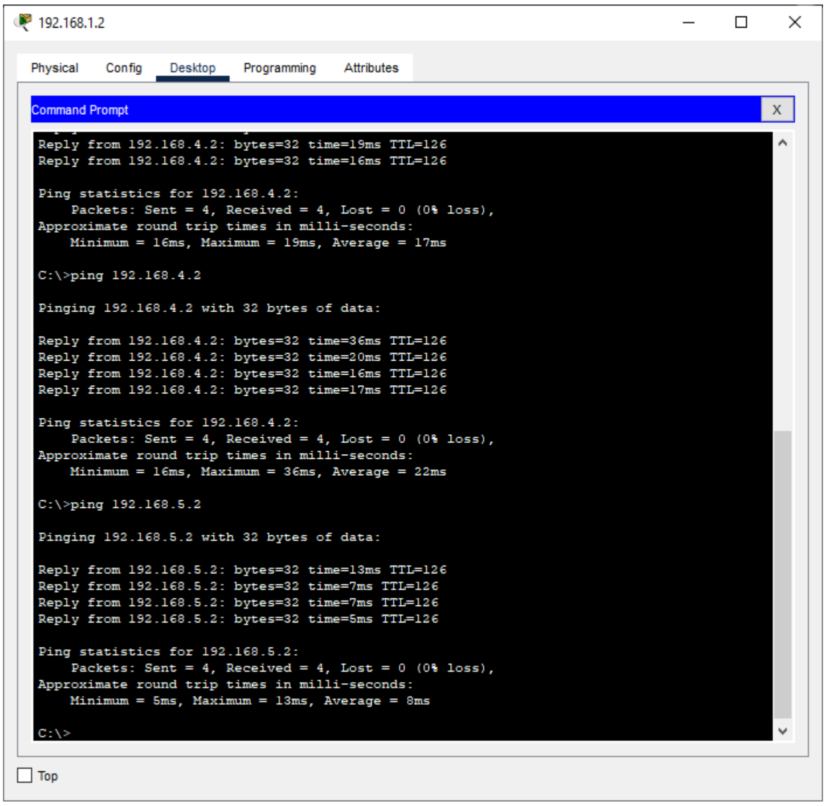
Now check again the following command on router 0

```
Router#show crypto ipsec sa
```

```
interface: Serial0/1/0
Crypto map tag: vpn-map, local addr 192.168.2.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer 192.168.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.:192.168.3.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x0322E684(52618884)

inbound esp sas:
spi: 0xC1647660(3244586592)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: FPGA:1, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/3314)
IV size: 16 bytes
replay detection support: N
```

```
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x0322E684(52618884)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/3314)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

Router#
```

Ping PC2 from PC0



```
Reply from 192.168.4.2: bytes=32 time=19ms TTL=126
Reply from 192.168.4.2: bytes=32 time=16ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 19ms, Average = 17ms

C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=36ms TTL=126
Reply from 192.168.4.2: bytes=32 time=20ms TTL=126
Reply from 192.168.4.2: bytes=32 time=16ms TTL=126
Reply from 192.168.4.2: bytes=32 time=17ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 36ms, Average = 22ms

C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=13ms TTL=126
Reply from 192.168.5.2: bytes=32 time=7ms TTL=126
Reply from 192.168.5.2: bytes=32 time=7ms TTL=126
Reply from 192.168.5.2: bytes=32 time=5ms TTL=126

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 13ms, Average = 8ms

C:\>
```

Now check the following command on **Router 0**

```
Router#show crypto ipsec sa
```

```
interface: Serial0/1/0
Crypto map tag: vpn-map, local addr 192.168.2.1
```

```
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer 192.168.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 192.168.2.1, remote crypto endpt.:192.168.3.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
current outbound spi: 0x0322E684(52618884)

inbound esp sas:
spi: 0xC1647660(3244586592)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: FPGA:1, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/2170)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x0322E684(52618884)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2005, flow_id: FPGA:1, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/2170)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

Router#
```