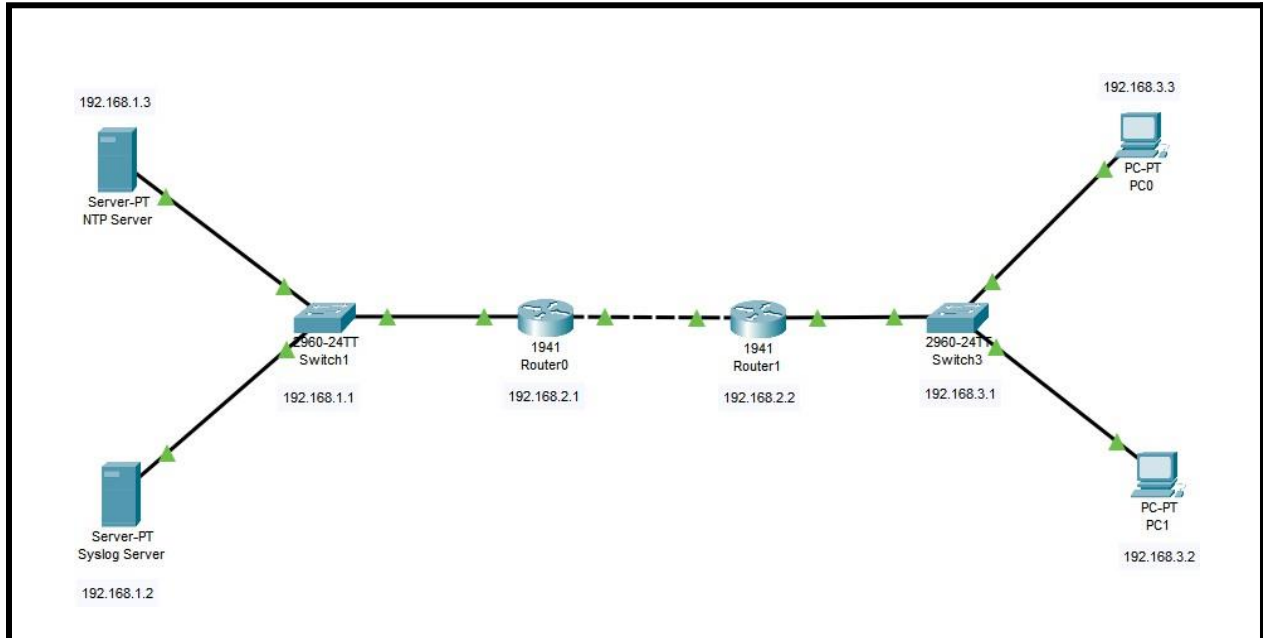


Practical 1

Configure Routers

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



- a. OSPF MD5 authentication.
 - ☐ OSPF - FINDING THE SHORTEST PATH
 - ☐ ALGO - DIJKSTRA
 - ☐ TOPOLOGY & DEVICE CONFIGURE

TO CONFIGURE OSPF

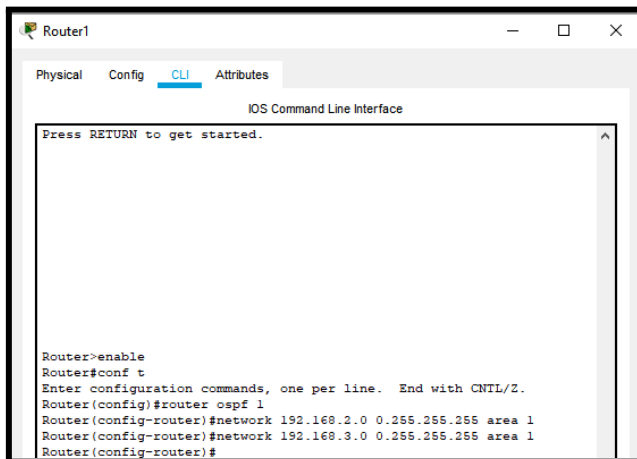
ON BOTH ROUTER -> CLI

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



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#network 192.168.1.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```



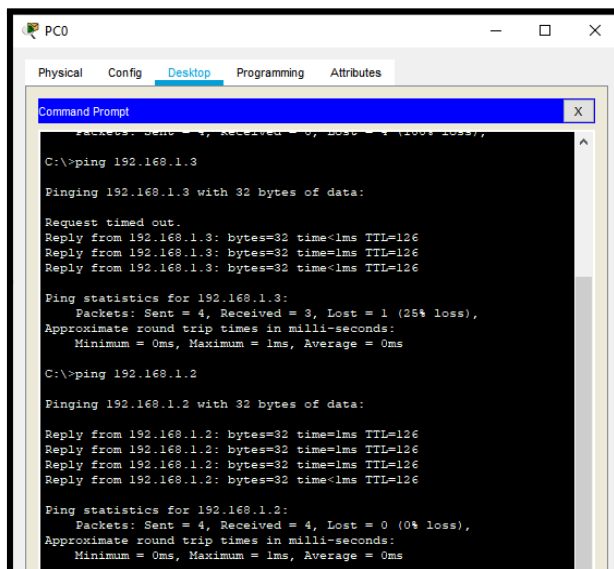
```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

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 192.168.2.0 0.255.255.255 area 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#
```

ON PC -> CMD

> ping server ip address



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

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
```

The screenshot shows a Packet Tracer PC window titled 'PC1' with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the following output:

```
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=10ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

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<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=3ms TTL=126

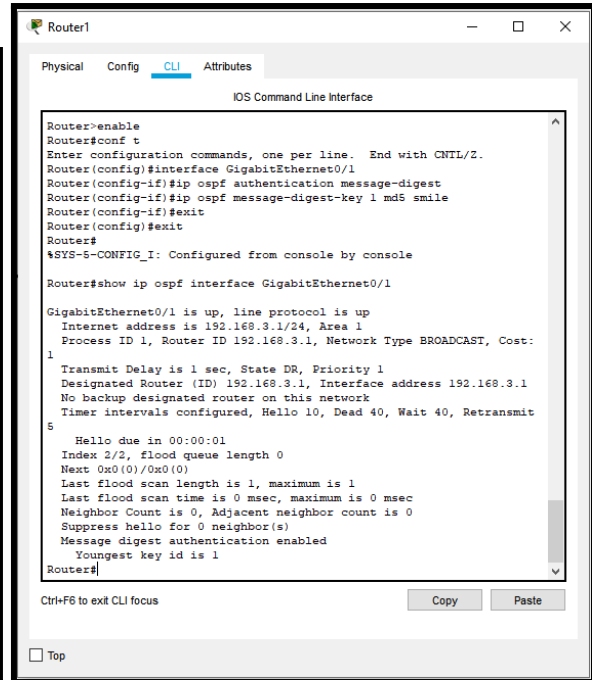
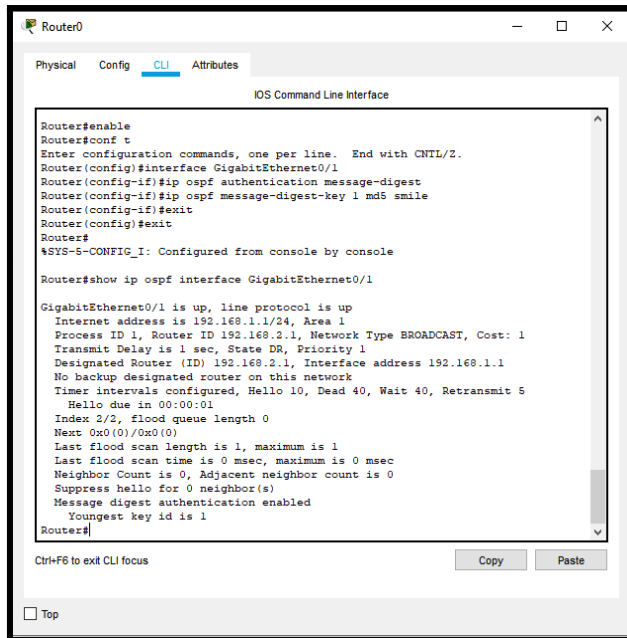
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>|
```

MD5 (For both the routers)

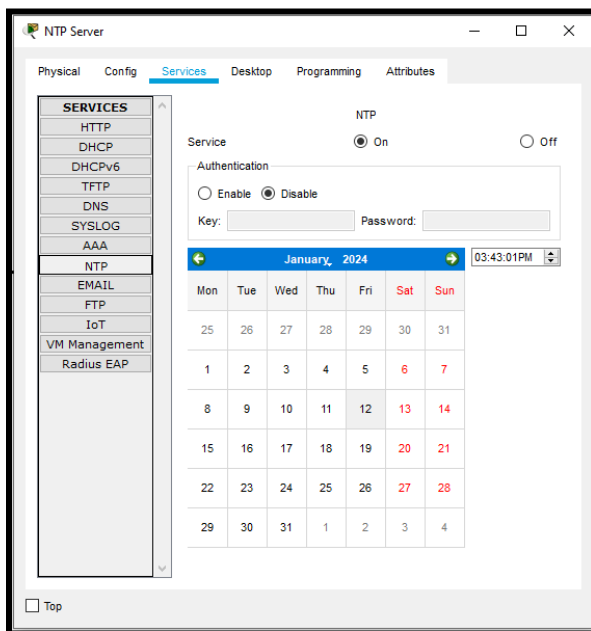
ROUTER -> CLI

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



b. NTP.

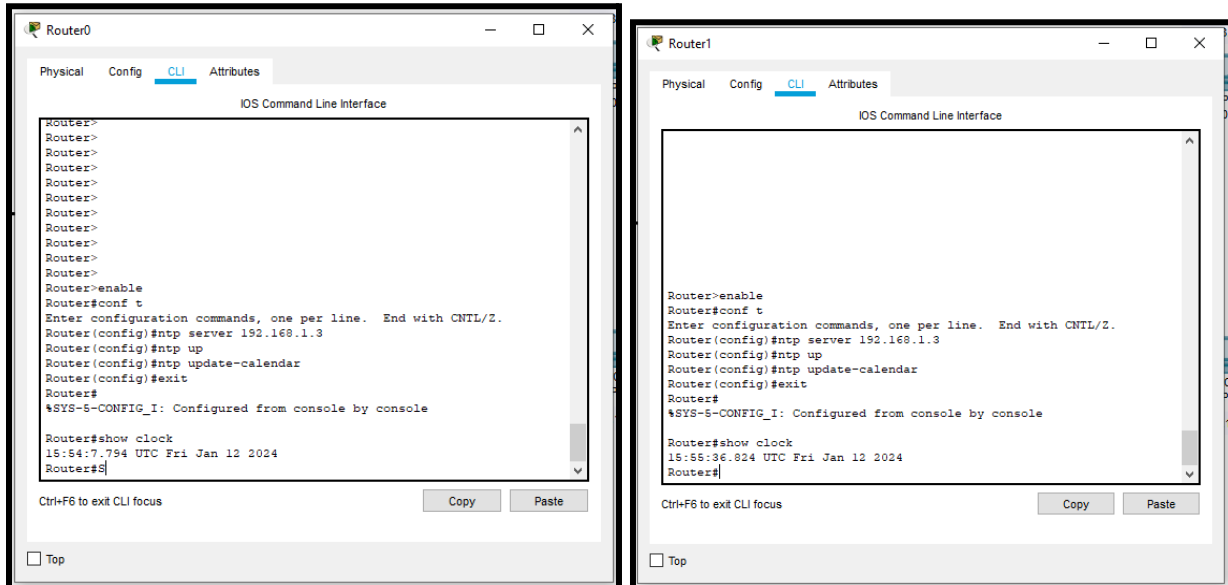
☐ NTP -: Synchronization



NTP (For both the routers)

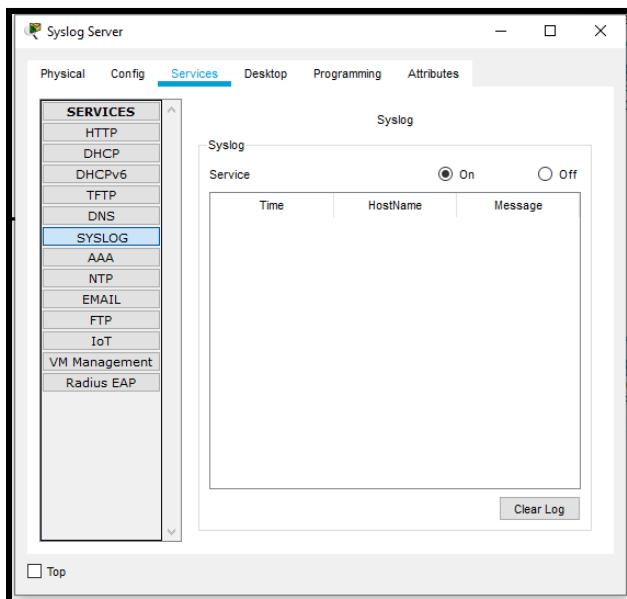
- 1) enable
- 2) conf t
- 3) ntp server 192.168.1.3

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



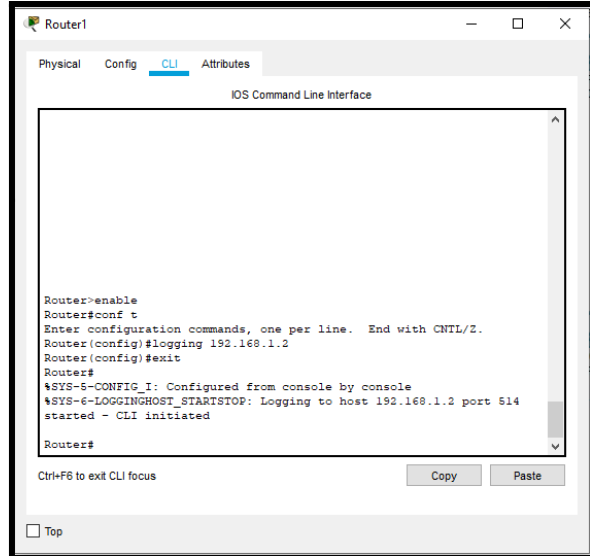
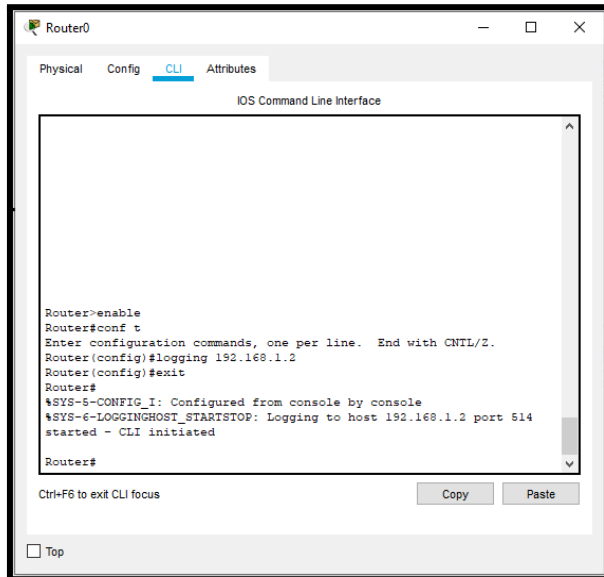
c. To log messages to the syslog server.

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

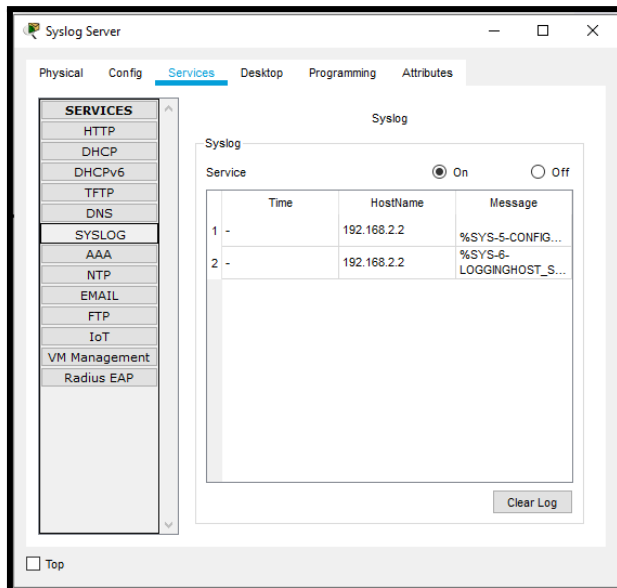


Syslog(For both the routers)

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



Server -> Check



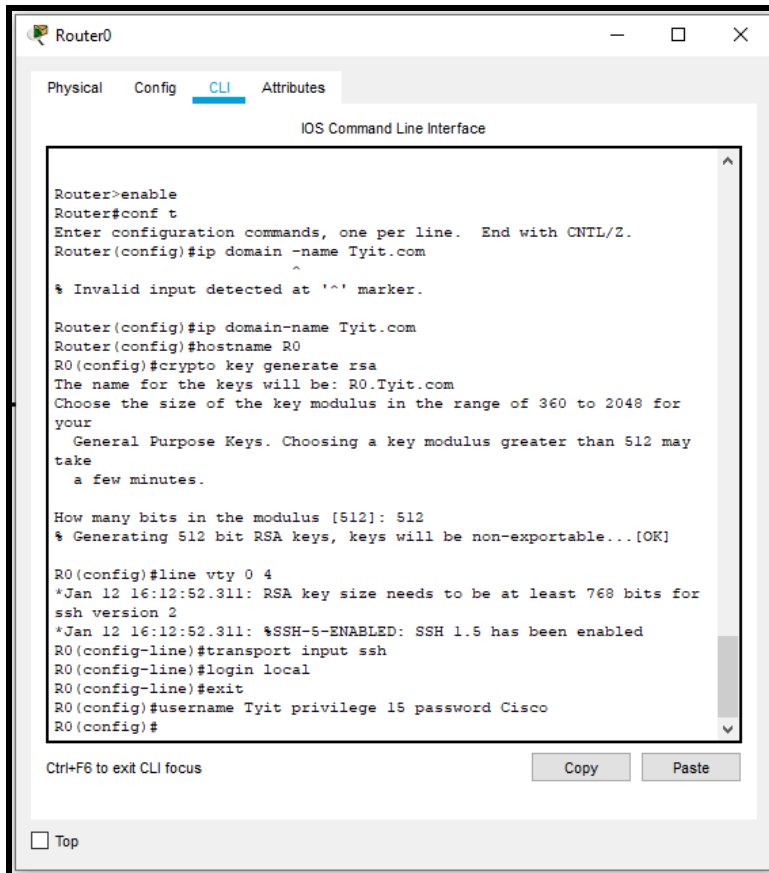
d. To support SSH connections.

SSH -: Secure Shell

Login ID & Password

SSH(For both the routers)

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



```
Router0
Physical Config CLI Attributes
IOS Command Line Interface

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip domain -name Tyit.com
^
% Invalid input detected at '^' marker.

Router(config)#ip domain-name Tyit.com
Router(config)#hostname R0
R0(config)#crypto key generate rsa
The name for the keys will be: R0.Tyit.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
*Jan 12 16:12:52.311: RSA key size needs to be at least 768 bits for
ssh version 2
*Jan 12 16:12:52.311: %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 Tyit privilege 15 password Cisco
R0(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

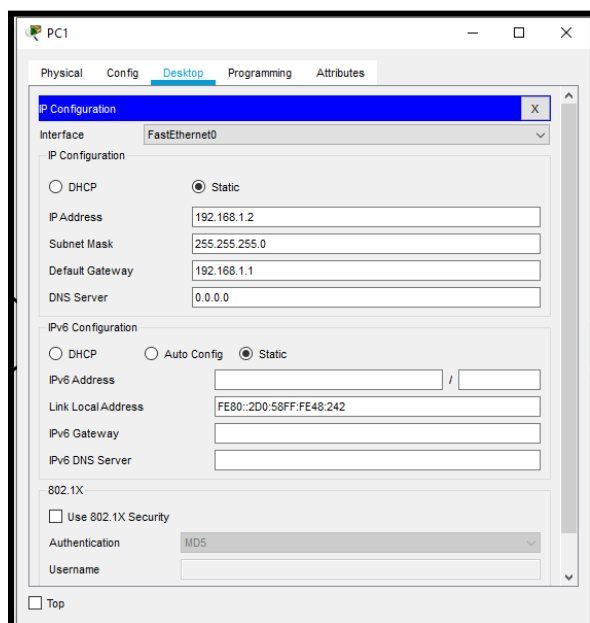
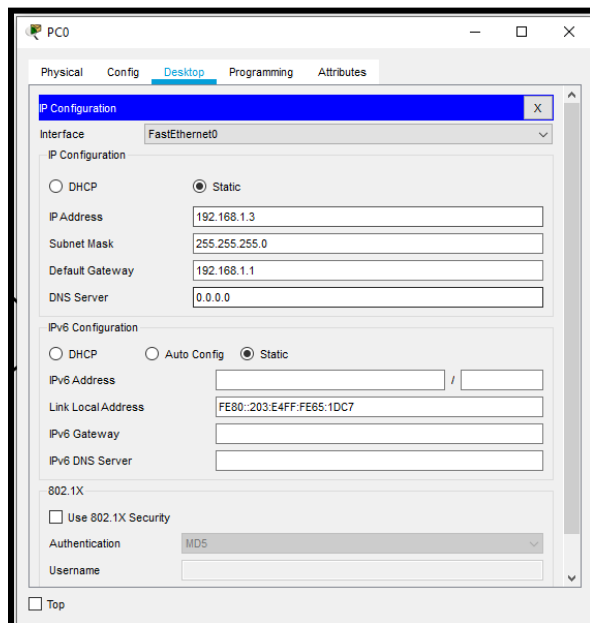
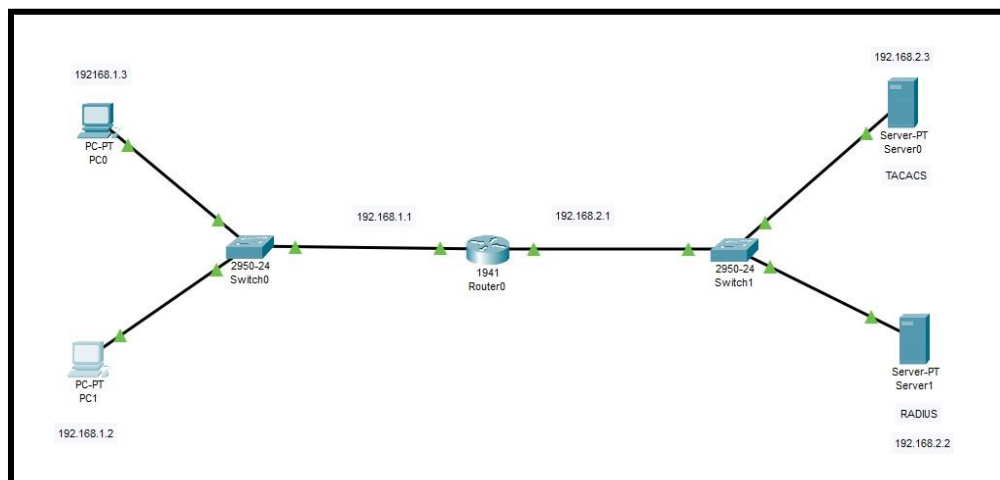
☐ Top

Practical 2

Configure AAA Authentication

- Configure a local user account on Router and configure authentication on the console and vty lines using local AAA
- Verify local AAA authentication from the Router console and the PC-A client

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



Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::20C:85FF:FE98:8073

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MDS

Username:

Password:

☐ Top

Server1

Physical Config Services **Desktop** Programming Attributes

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.2.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::210:11FF:FE71:8021

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MDS

Username:

Password:

☐ Top

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/0

Port Status: ☒ On

Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address: 0060.47BC.2E01

IP Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

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

☐ Top

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/1

Port Status: ☒ On

Bandwidth: ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address: 0060.47BC.2E02

IP Configuration

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

☐ Top

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

Service: ☐ On ☒ Off Radius Port: 1645

Network Configuration

Client Name: Client IP:

Secret: ServerType: Radius

	Client Name	Client IP	Server Type	Key
1	SIES	192.168.2.1	Tacacs	CISCO

User Setup

Username: Password:

	Username	Password
1	smile	smile

☐ Top

Server1

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

Service: ☒ On ☐ Off Radius Port: 1645

Network Configuration

Client Name: Client IP:

Secret: ServerType: Radius

	Client Name	Client IP	Server Type	Key
1	SIES	192.168.2.1	Radius	CISCO

User Setup

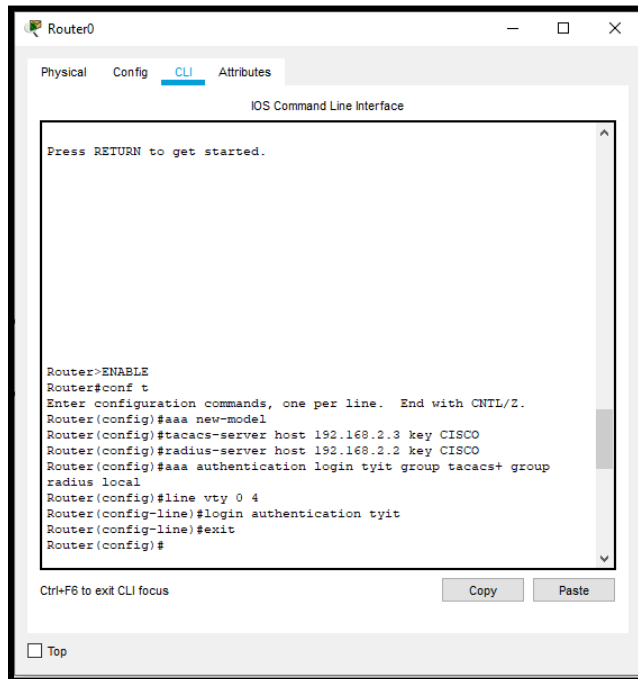
Username: Password:

	Username	Password
1	smile	CISCO

☐ Top

On Router -> cmd

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



The screenshot shows the Cisco Packet Tracer interface for Router0. The 'CLI' tab is selected, displaying the 'IOS Command Line Interface'. The text 'Press RETURN to get started.' is at the top. Below it, the following commands have been entered:

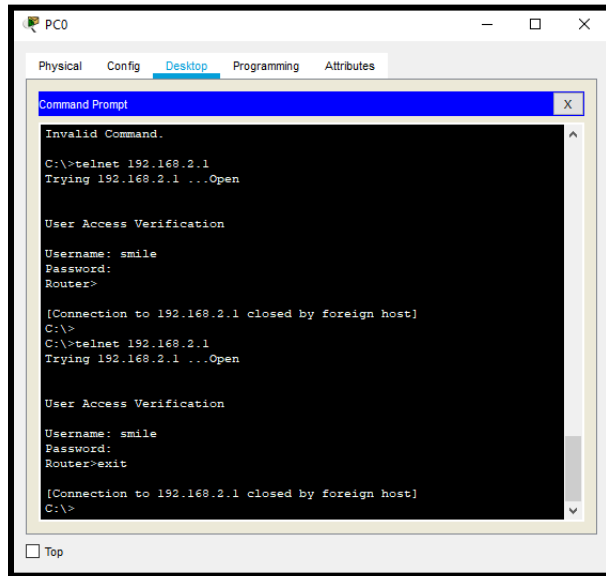
```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#tacacs-server host 192.168.2.3 key CISCO
Router(config)#radius-server host 192.168.2.2 key CISCO
Router(config)#aaa authentication login tyit group tacacs+ group
radius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

At the bottom of the CLI window, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons. A 'Top' button is also visible at the very bottom left.

Check authentication -> PC -> cmd

> telnet 192.168.2.1 Ask for a username & password

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



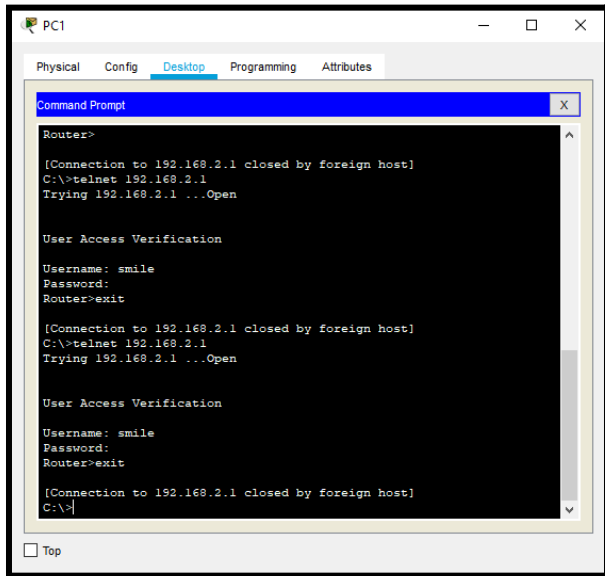
```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Invalid Command.
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

User Access Verification
Username: smile
Password:
Router>

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

User Access Verification
Username: smile
Password:
Router>exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>
```



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Router>

[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: smile
Password:
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: smile
Password:
Router>exit

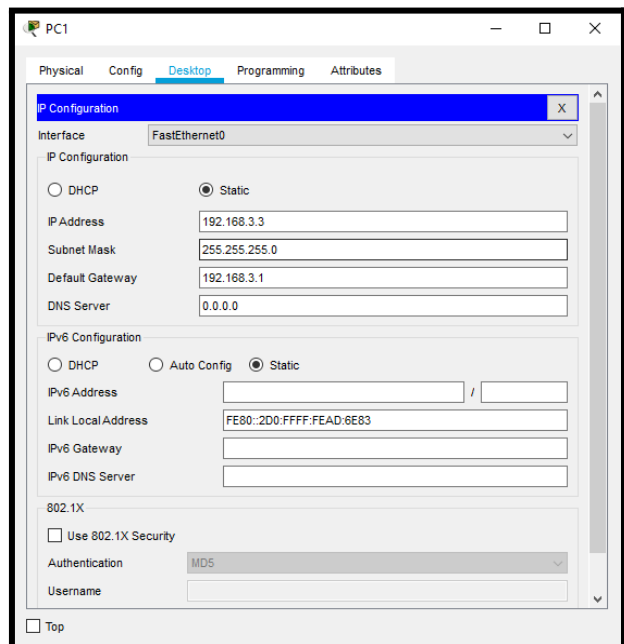
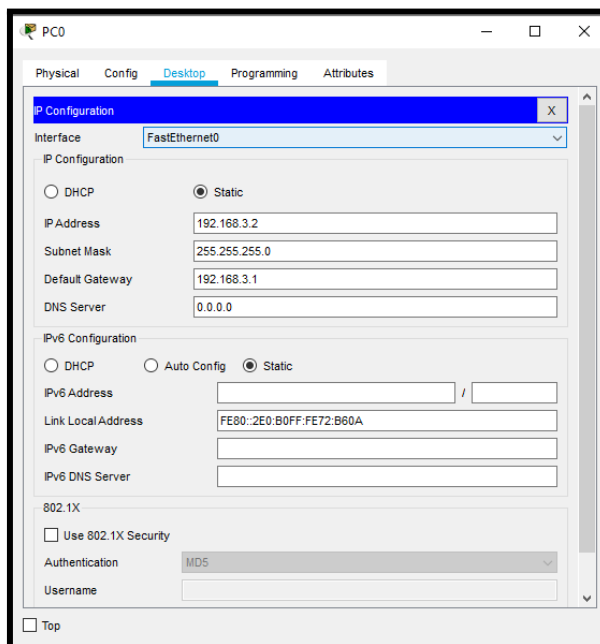
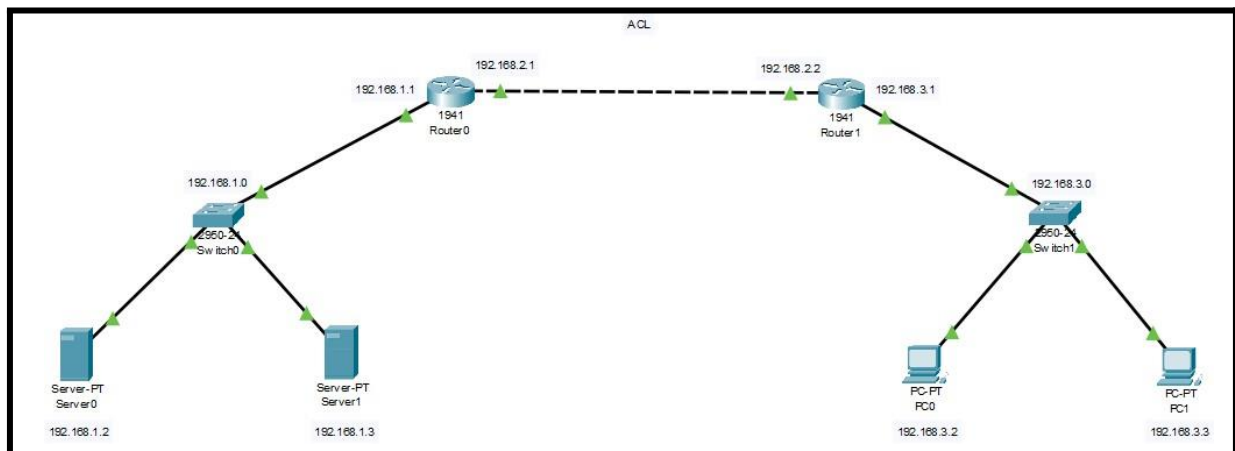
[Connection to 192.168.2.1 closed by foreign host]
C:\>
```

Practical 3

Configuring Extended ACLs

a. Configure, Apply and Verify an Extended Numbered ACL

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



Router0

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0006.2A40.C101

IP Configuration

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-router)#network 192.168.2.0
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

☐ Top

Router0

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/1

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0006.2A40.C102

IP Configuration

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

☐ Top

Router1

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.4396.5901

IP Configuration

IP Address 192.168.2.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-router)#network 192.168.2.0
Router(config-router)#
Router(config-router)#end
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

☐ Top

Router1

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/1

Port Status ☒ On

Bandwidth ☐ 1000 Mbps ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.4396.5902

IP Configuration

IP Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
```

☐ Top

Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:97FF:FE97:5A5D

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Server1

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::290:CFF:FE05:43A2

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

RIP Routing

Network

Add

Network Address

192.168.1.0

192.168.2.0

Remove

Equivalent IOS Commands

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console

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

☐ Top

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

RIP Routing

Network

Add

Network Address

192.168.2.0

192.168.3.0

Remove

Equivalent IOS Commands

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console

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

☐ Top

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

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

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 4ms

C:\>192.168.3.3
Invalid Command.

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=4ms TTL=128
Reply from 192.168.3.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
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<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 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:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time=1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=5ms TTL=128
Reply from 192.168.3.3: bytes=32 time=4ms TTL=128
Reply from 192.168.3.3: bytes=32 time=2ms TTL=128
Reply from 192.168.3.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 2ms

C:\>
```

Apply and verify extended ACL

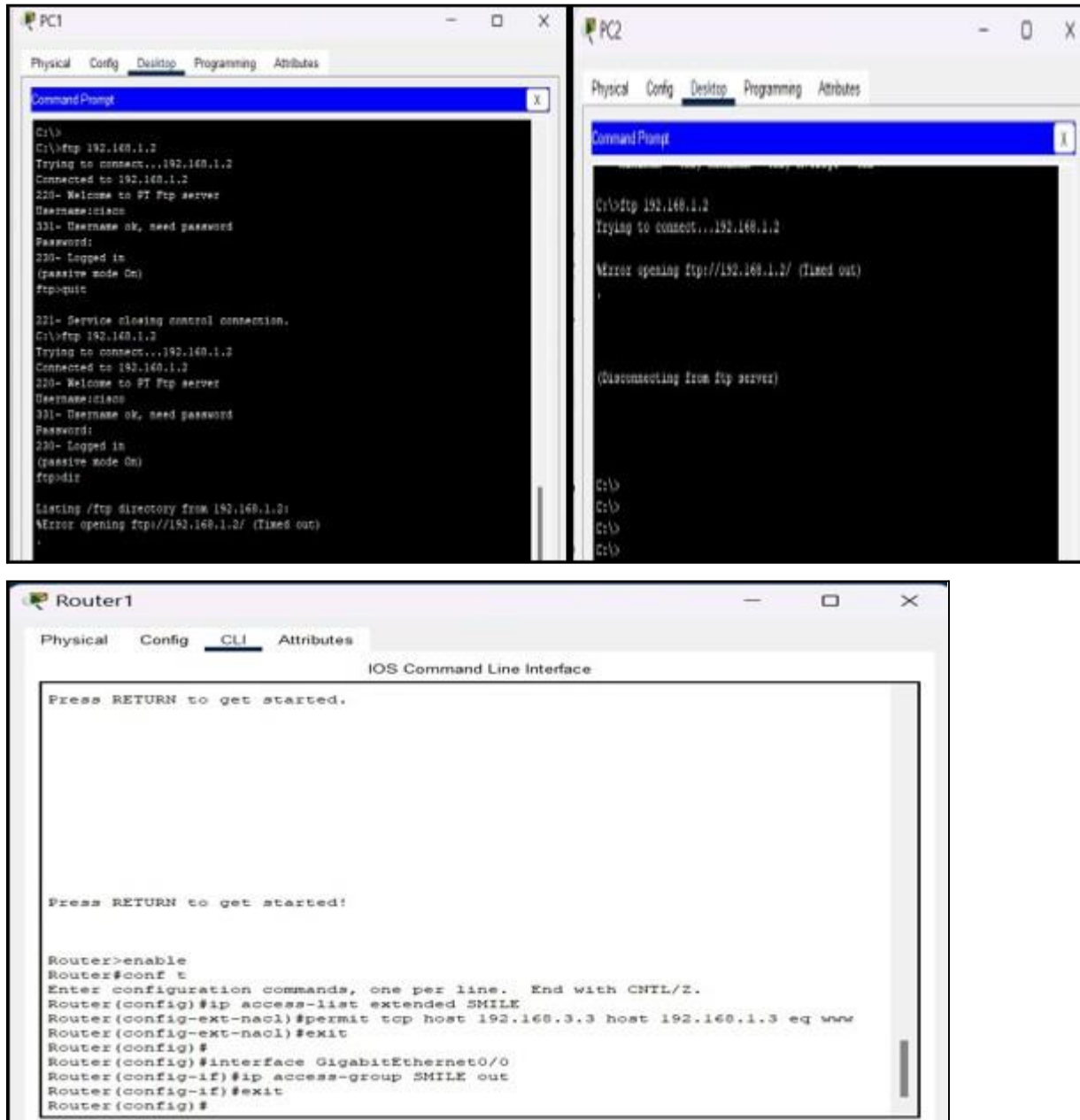
Router -> cli

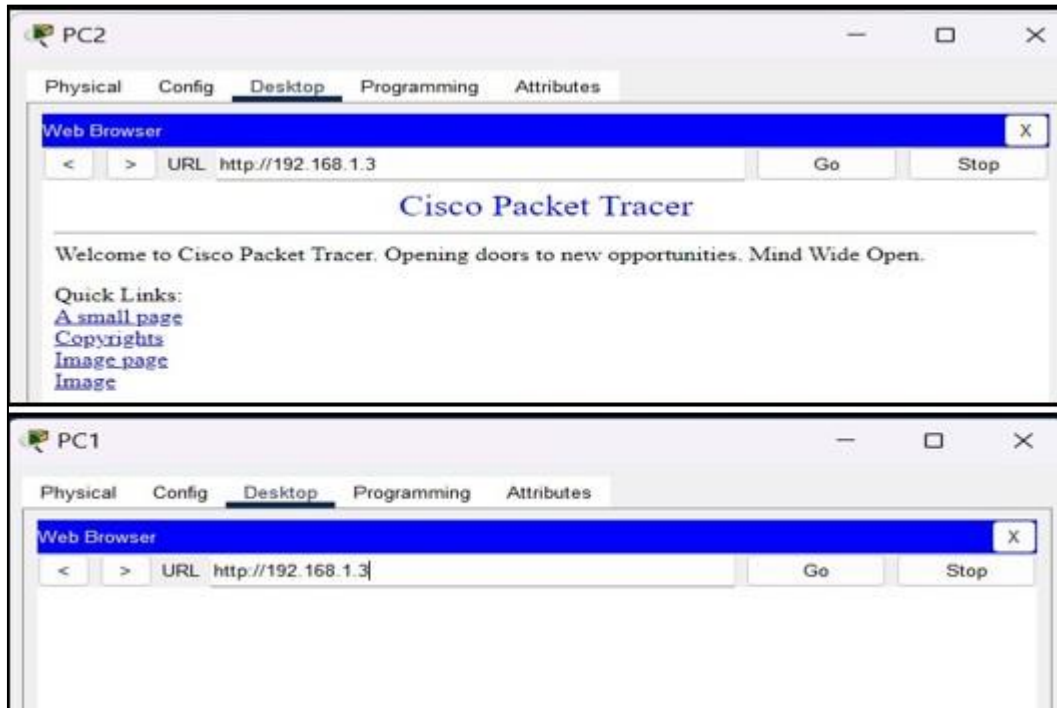
- 1) enable**
- 2) conf t**
- 3) access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq ftp**
(eq - What services?)
- 4) interface GigabitEthernet0/1**
- 5) ip access-group 100 out**
- 6) exit**

Verify

On PC0 -> cmd

1) ftp 192.168.1.2



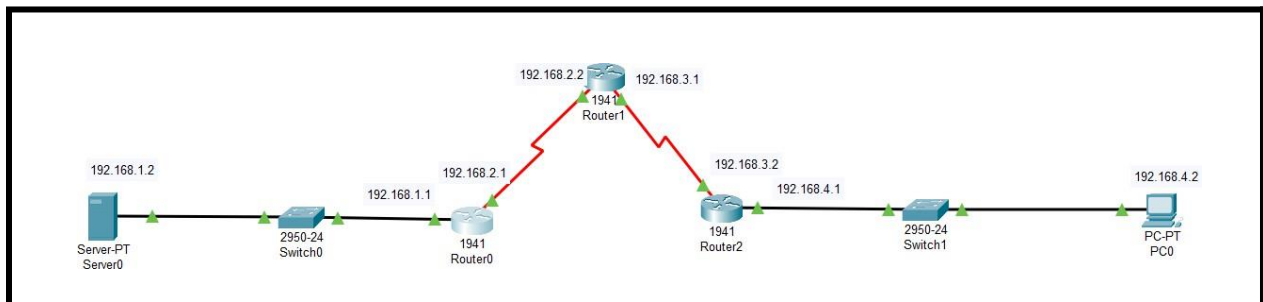


Practical 4

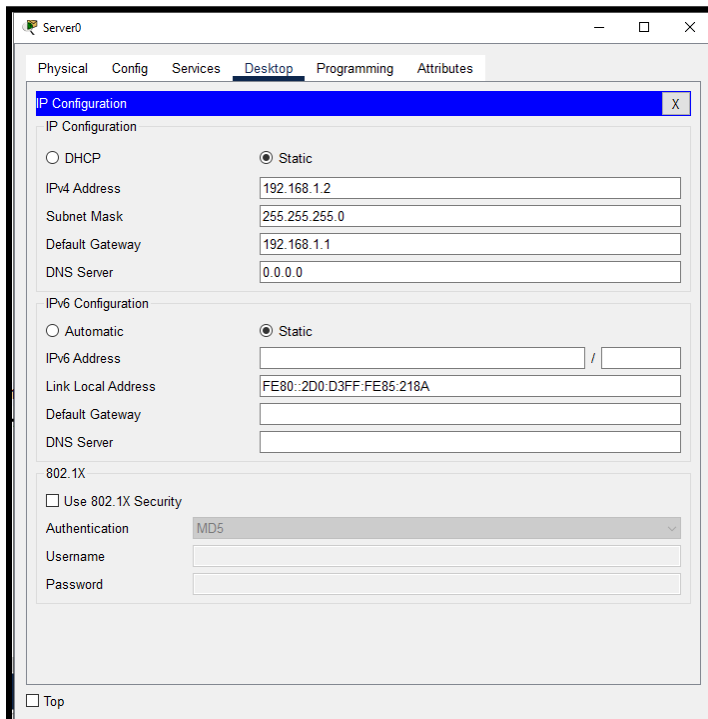
Configure IP ACLs to Mitigate Attacks and IPV6 ACLs

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

c. Configure ACLs on to mitigate attacks.



Server



PC

The screenshot shows the configuration window for PC0. The 'Config' tab is active, and the 'IP Configuration' section is expanded. The 'Interface' dropdown is set to 'FastEthernet0'. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with: IPv4 Address: 192.168.4.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.4.1, and DNS Server: 0.0.0.0. Under 'IPv6 Configuration', the 'Static' radio button is also selected. The fields are filled with: IPv6 Address: (empty), Link Local Address: FE80::207:ECFF:FE22:C566, Default Gateway: (empty), and DNS Server: (empty). At the bottom, there is a section for '802.1X' with a checkbox for 'Use 802.1X Security' (unchecked), an 'Authentication' dropdown set to 'MD5', and fields for 'Username' and 'Password'.

PC0

Physical Config Desktop Programming Attributes

IP Configuration X

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::207:ECFF:FE22:C566

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

3 Routers Config

The screenshot shows the configuration window for Router0. The 'Config' tab is active, and the 'GigabitEthernet0/0' interface is selected. The 'Port Status' is 'On'. The 'Bandwidth' is set to '1000 Mbps'. The 'Duplex' is set to 'Full Duplex'. The 'MAC Address' is 00D0.9733.8D01. The 'IP Configuration' section is expanded, showing: IPv4 Address: 192.168.1.1, Subnet Mask: 255.255.255.0, and Tx Ring Limit: 10. The 'Equivalent IOS Commands' section at the bottom contains the following commands: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up; %LINK-5-CHANGED: Interface Serial0/1/0, changed state to up; %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up; R0>enable; R0#; R0#configure terminal; Enter configuration commands, one per line. End with CNTL/Z.; R0(config)#interface GigabitEthernet0/0; R0(config-if)#.

Router0

Physical Config CLI Attributes

GLOBAL Settings Algorithm Settings ROUTING Static RIP SWITCHING VLAN Database INTERFACE GigabitEthernet0/0 GigabitEthernet0/1 Serial0/1/0 Serial0/1/1

GigabitEthernet0/0

Port Status On

Bandwidth 1000 Mbps 100 Mbps 10 Mbps Auto

Duplex Half Duplex Full Duplex Auto

MAC Address 00D0.9733.8D01

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface GigabitEthernet0/0
R0(config-if)#
```

☐ Top

The screenshot shows the configuration window for Router0. The 'Config' tab is active, and the 'Serial0/1/0' interface is selected. The 'Port Status' is 'On'. The 'Duplex' is set to 'Full Duplex'. The 'Clock Rate' is 2000000. The 'IP Configuration' section is expanded, showing: IPv4 Address: 192.168.2.1, Subnet Mask: 255.255.255.0, and Tx Ring Limit: 10. The 'Equivalent IOS Commands' section at the bottom contains the following commands: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up; R0>enable; R0#; R0#configure terminal; Enter configuration commands, one per line. End with CNTL/Z.; R0(config)#interface GigabitEthernet0/0; R0(config-if)#; R0(config-if)#exit; R0(config)#interface Serial0/1/0; R0(config-if)#.

Router0

Physical Config CLI Attributes

GLOBAL Settings Algorithm Settings ROUTING Static RIP SWITCHING VLAN Database INTERFACE GigabitEthernet0/0 GigabitEthernet0/1 Serial0/1/0 Serial0/1/1

Serial0/1/0

Port Status On

Duplex Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.2.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

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

R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface GigabitEthernet0/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/0
R0(config-if)#
```

☐ Top

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/0

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINK-S-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
```

☐ Top

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/1

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINK-S-CHANGED: Interface Serial0/1/1, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/1
R0(config-if)#
```

☐ Top

Router2

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/0

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.3.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-S-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
```

☐ Top

Router2

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

GigabitEthernet0/0

Port Status ☒ On

Bandwidth ☒ 100 Mbps

Duplex ☒ Full Duplex

MAC Address 00D0.D3C6.2701

IP Configuration

IPv4 Address 192.168.4.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
%LINK-S-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#exit
R0(config)#interface GigabitEthernet0/0
R0(config-if)#
```

☐ Top

RIP

Router0

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

RIP Routing

Network

Add

Network Address:

192.168.1.0

192.168.2.0

Remove

Equivalent IOS Commands

```
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#router rip
R0(config-router)#
```

☐ Top

Router1

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

RIP Routing

Network

Add

Network Address:

192.168.2.0

192.168.3.0

Remove

Equivalent IOS Commands

```
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/1
R0(config-if)#
R0(config-if)#exit
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#router rip
R0(config-router)#
```

☐ Top

Router2

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

RIP Routing

Network

Add

Network Address:

192.168.3.0

192.168.4.0

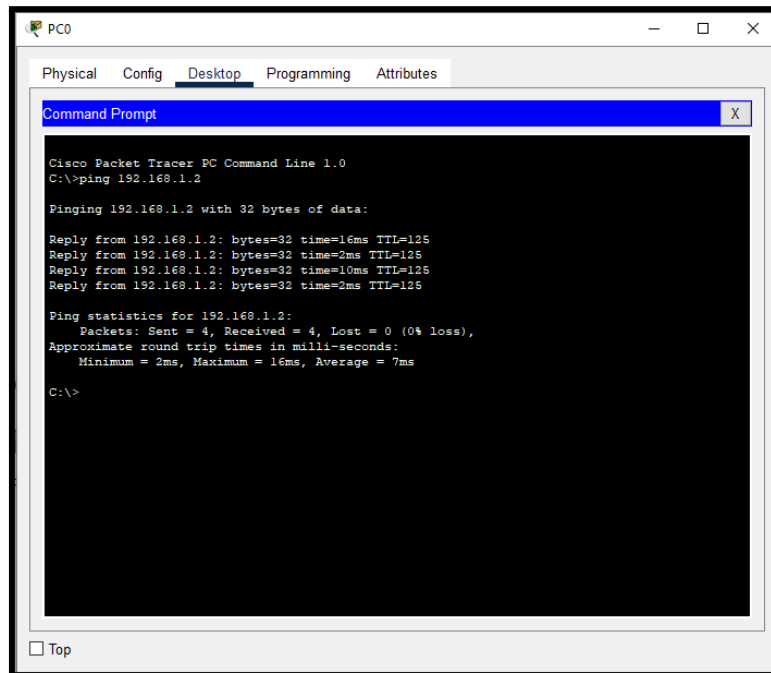
Remove

Equivalent IOS Commands

```
R0>enable
R0#
R0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/1/0
R0(config-if)#
R0(config-if)#exit
R0(config)#interface GigabitEthernet0/0
R0(config-if)#
R0(config-if)#exit
R0(config)#router rip
R0(config-router)#
```

☐ Top

On PC -> Verify the connectivity



Routers -> Cli

I. SSH Enable

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

II. Access List Define

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

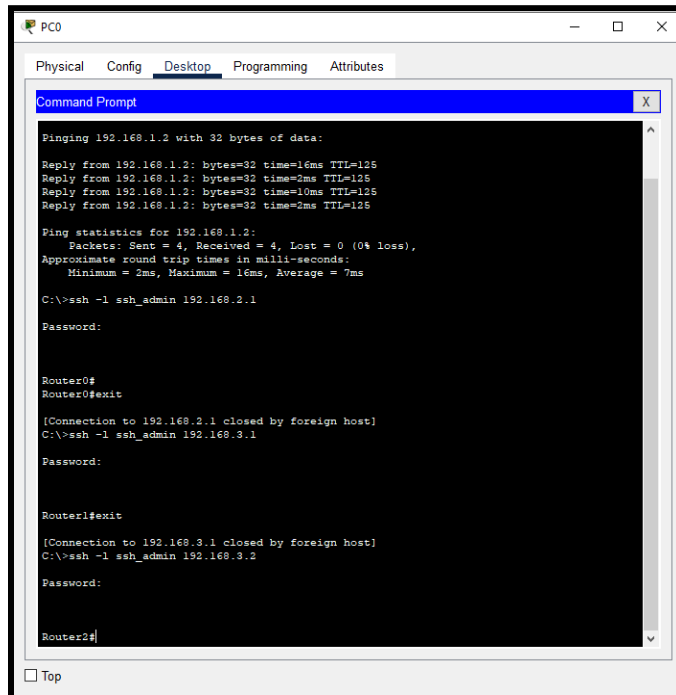
On PC -> Verify on CMD

> ssh -l ssh_admin 192.168.3.2

Password: ty

On Server -> Verify on CMD

> ssh -l ssh_admin 192.168.2.1



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=16ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=10ms 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 = 7ms

C:\>ssh -l ssh_admin 192.168.2.1
Password:

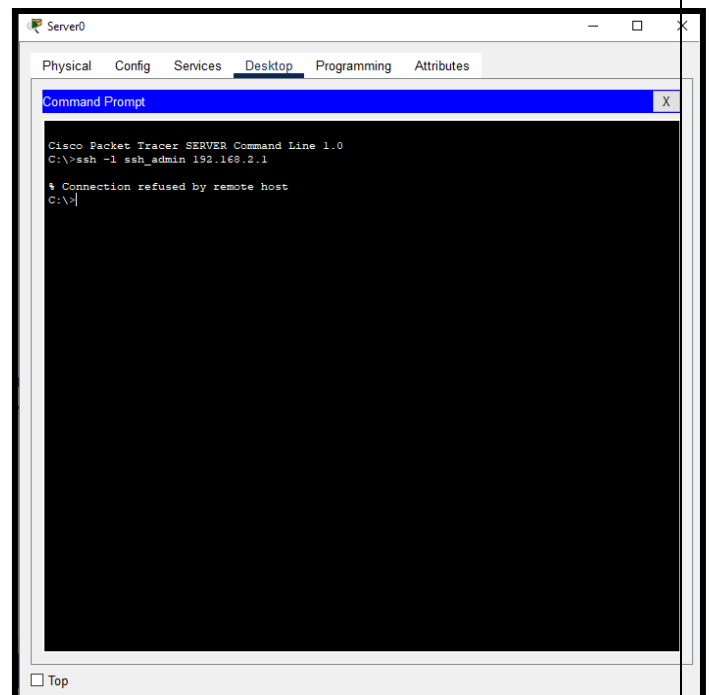
Router0#
Router0#exit

[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l ssh_admin 192.168.3.1
Password:

Router1#exit

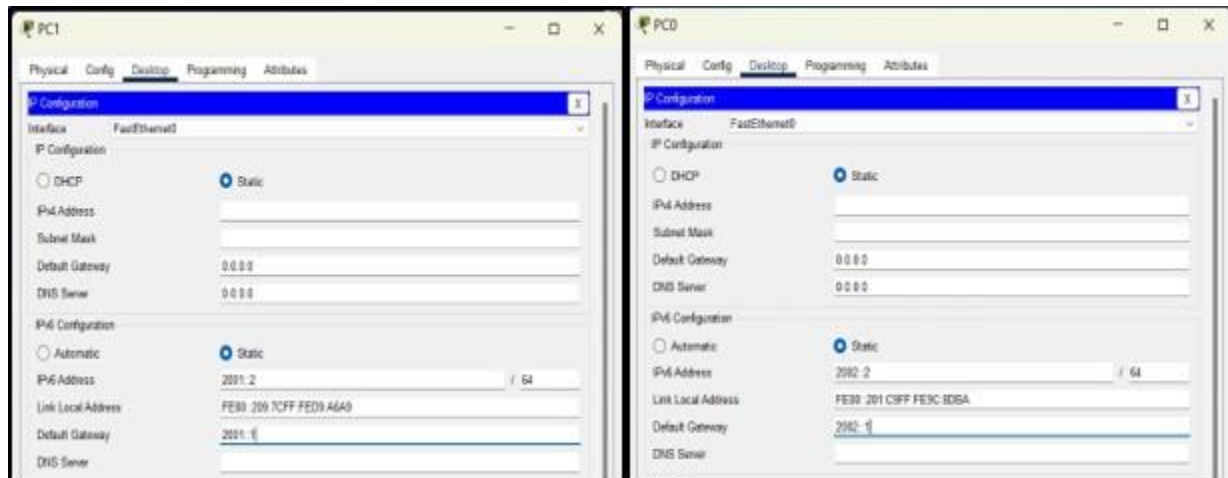
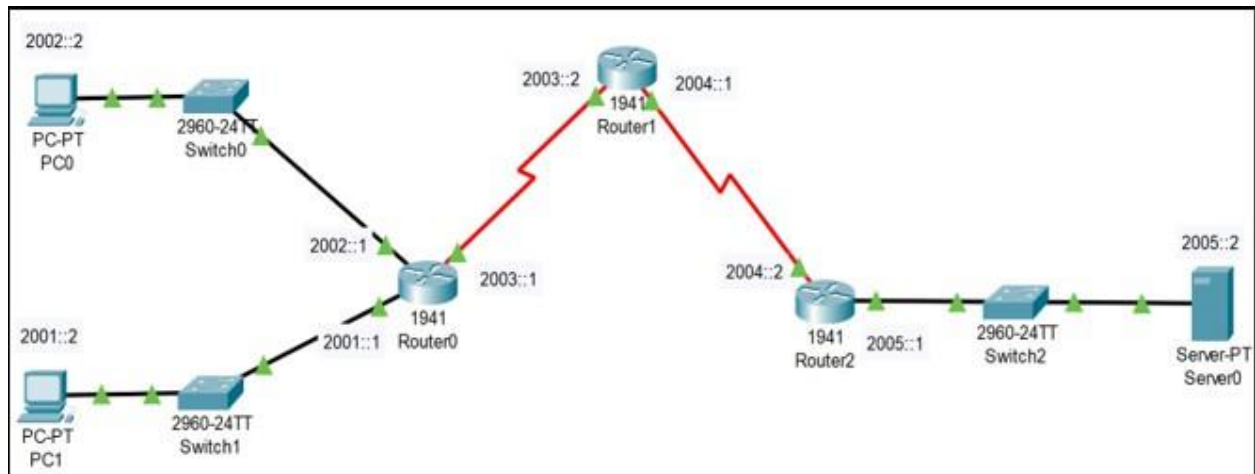
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l ssh_admin 192.168.3.2
Password:

Router2#
```



```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ssh -l ssh_admin 192.168.2.1
* Connection refused by remote host
C:\>
```


d. Configuring IPv6 ACLs



Router 0:

Router>enable

Router#

Router#configure terminal

Router(config)#ipv6 unicast-routing

Router(config)#interface GigabitEthernet0/0

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

Router 1:

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

Router(config)#
```

Router2:

Router>enable

Router#configure terminal

Router(config)#ipv6 unicast-routing

Router(config)#

Router(config)#interface Serial0/1/1

Router(config-if)#ipv6 address 2004::2/64

Router(config-if)#ipv6 rip a enable

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ipv6 address 2005::1/64

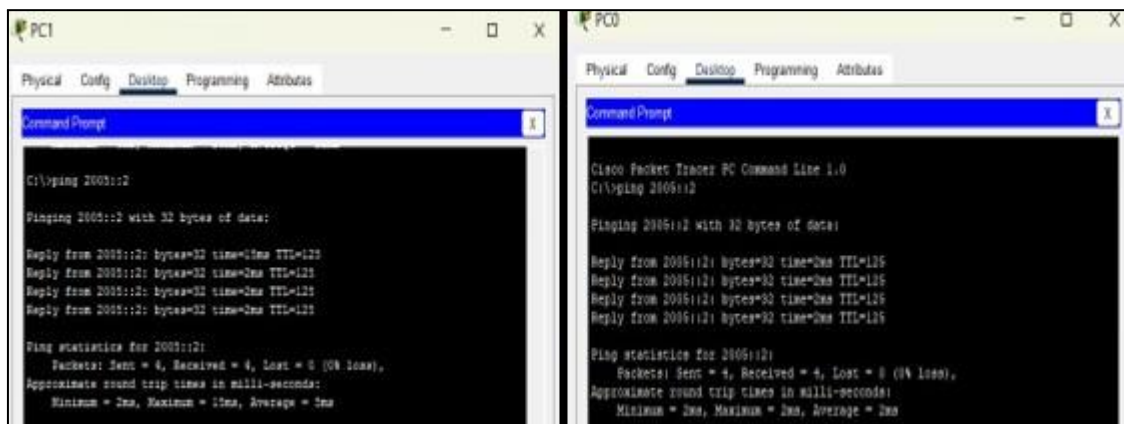
Router(config-if)#ipv6 rip a enable

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#

Check the connectivity by pinging from PCs to Server



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

Router>enable

Router#configure terminal

Router(config)#ipv6 access-list smile

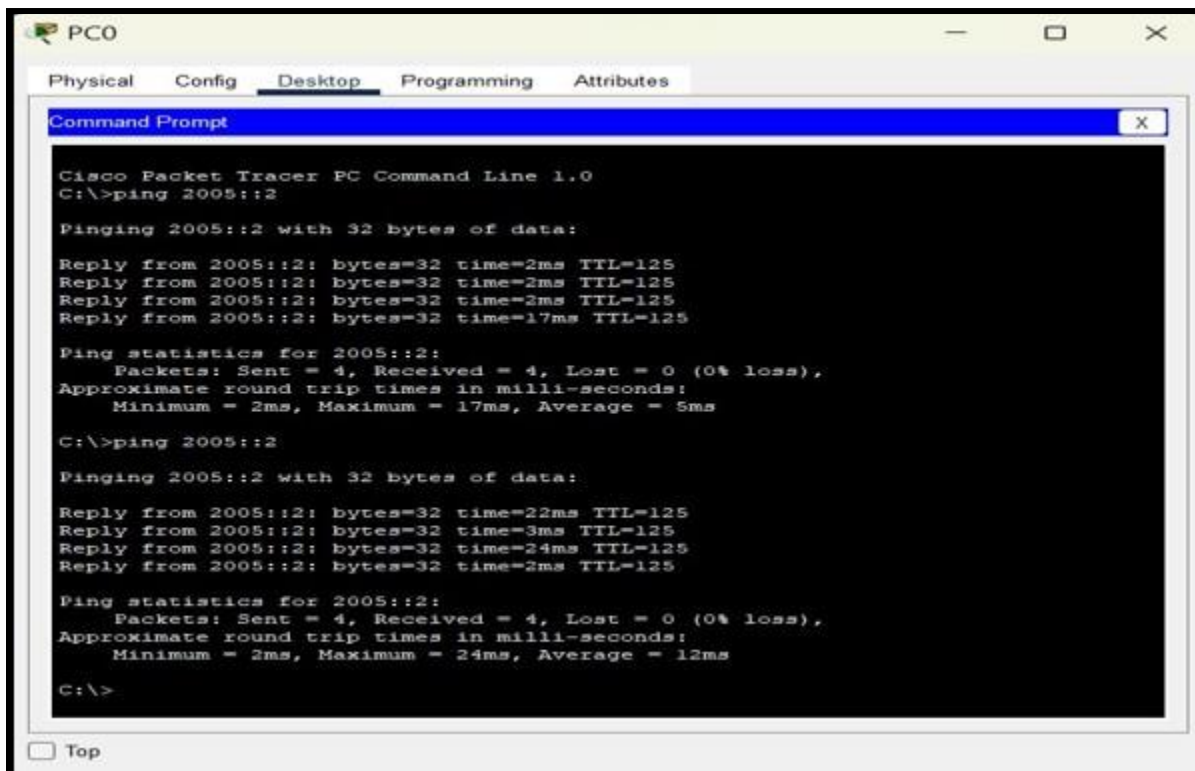
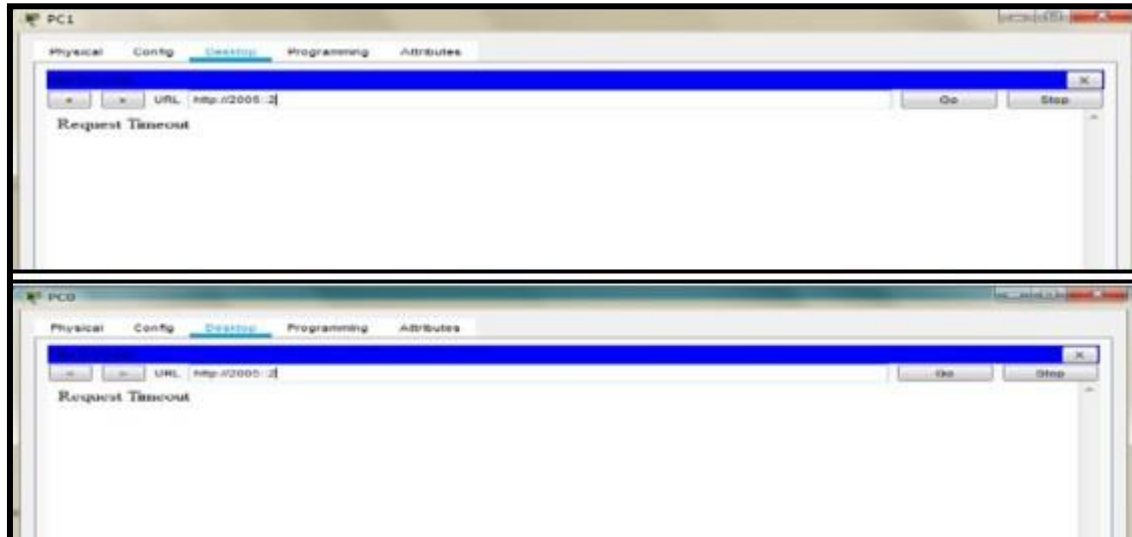
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq www

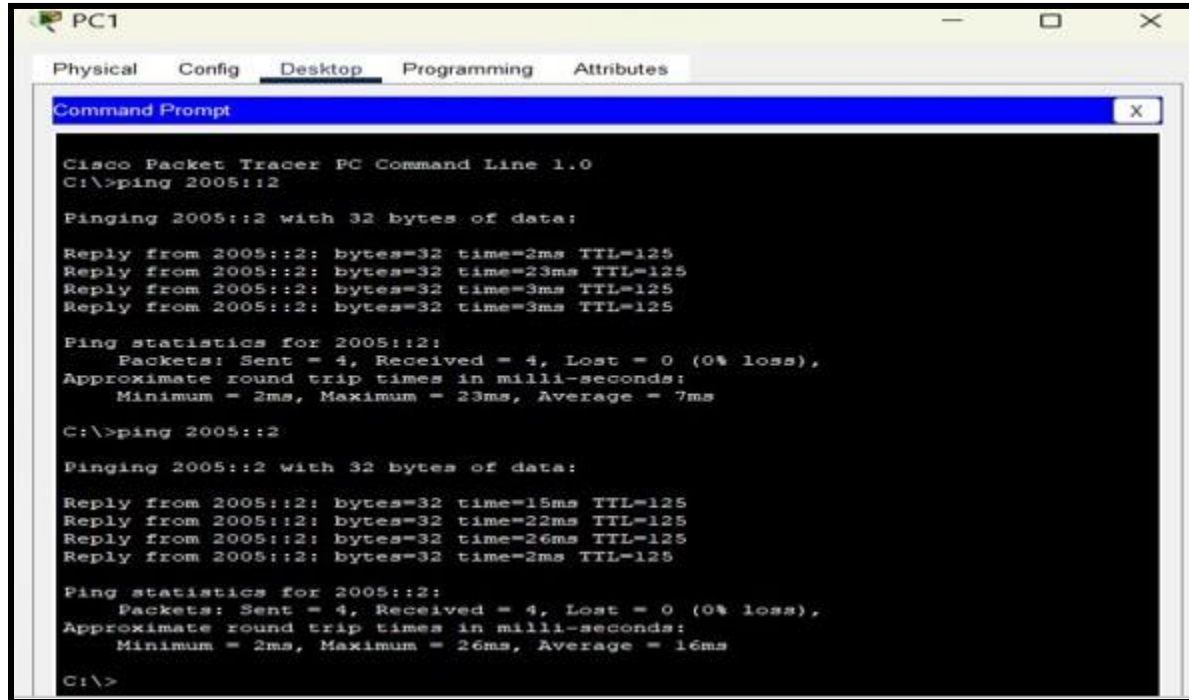
Router(config-ipv6-acl)#deny tcp any host 2005::2 eq 443

Router(config-ipv6-acl)#permit ipv6 any any

Router(config-ipv6-acl)#

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





The image shows a screenshot of a Cisco Packet Tracer PC Command Prompt window. The window has a title bar with 'PC1' and standard minimize, maximize, and close buttons. Below the title bar are tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' currently selected. The Command Prompt window itself has a blue title bar with 'Command Prompt' and a close button. The text inside the Command Prompt is as follows:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2005::2

Pinging 2005::2 with 32 bytes of data:

Reply from 2005::2: bytes=32 time=2ms TTL=125
Reply from 2005::2: bytes=32 time=23ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125
Reply from 2005::2: bytes=32 time=3ms TTL=125

Ping statistics for 2005::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 23ms, Average = 7ms

C:\>ping 2005::2

Pinging 2005::2 with 32 bytes of data:

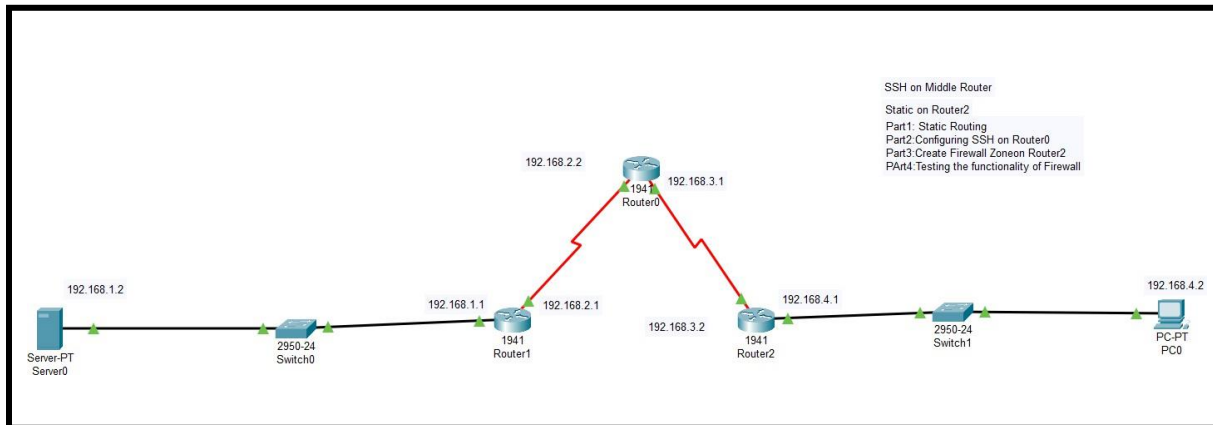
Reply from 2005::2: bytes=32 time=15ms TTL=125
Reply from 2005::2: bytes=32 time=22ms TTL=125
Reply from 2005::2: bytes=32 time=26ms TTL=125
Reply from 2005::2: bytes=32 time=2ms TTL=125

Ping statistics for 2005::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 26ms, Average = 16ms

C:\>
```

Practical 5

Configuring a Zone-Based Policy Firewall



Configuring PC0

PC0

Physical Config Desktop Programming Attributes

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::207:ECFF:FE16:EEC8

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Configuring server0

The screenshot shows the 'Server0' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the following settings:

- 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: (empty)
 - Link Local Address: FE80::2D0:BCFF:FE9A:E043
 - Default Gateway: (empty)
 - DNS Server: (empty)
- 802.1X:**
 - ☐ Use 802.1X Security
 - Authentication: MD5
 - Username: (empty)
 - Password: (empty)

At the bottom left, there is a 'Top' button.

Serial interface must be added in each Router before configuring it

Configuring Router1

The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The 'GigabitEthernet0/0' interface is selected in the left sidebar. The configuration for this interface is shown on the right:

- Port Status:** On
- Bandwidth:** 1000 Mbps
- Duplex:** Full Duplex
- MAC Address:** 0004.9A94.8801
- IP Configuration:**
 - IPv4 Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
- Tx Ring Limit:** 10

At the bottom left, there is a 'Top' button.

The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The 'Serial0/1/0' interface is selected in the left sidebar. The configuration for this interface is shown on the right:

- 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

At the bottom left, there is a 'Top' button.

Configuring Router0

Configuring Router2

The image displays two side-by-side screenshots of the Cisco Packet Tracer interface, showing the configuration of two different routers (Router2 and Router5).

Router2 Configuration (Left Screenshot):

- Physical Tab:** Shows the router's hardware components.
- Config Tab:** The configuration page for Router2.
- Attributes:** Lists the configured interfaces: GigabitEthernet0/0, GigabitEthernet0/1, Serial0/1/0, and Serial0/1/1.
- GigabitEthernet0/0 Configuration:**
 - Port Status:** On (checked).
 - Bandwidth:** 1000 Mbps (selected).
 - Duplex:** Full Duplex (selected).
 - MAC Address:** 0060.472A.C301.
 - IP Configuration:** IP 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)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```

Router5 Configuration (Right Screenshot):

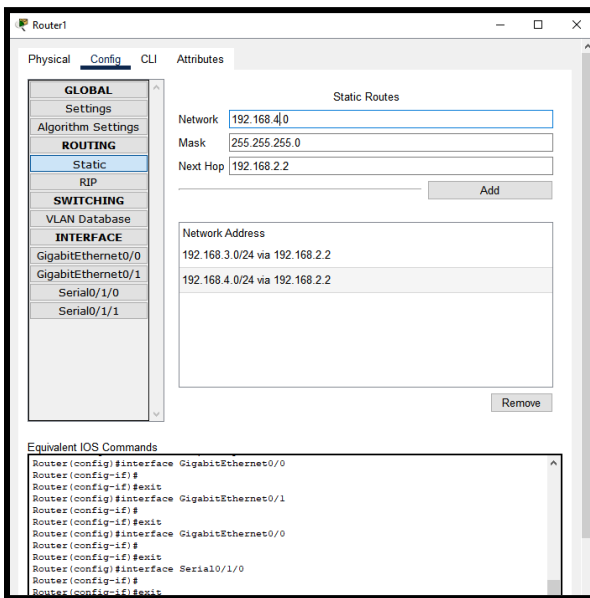
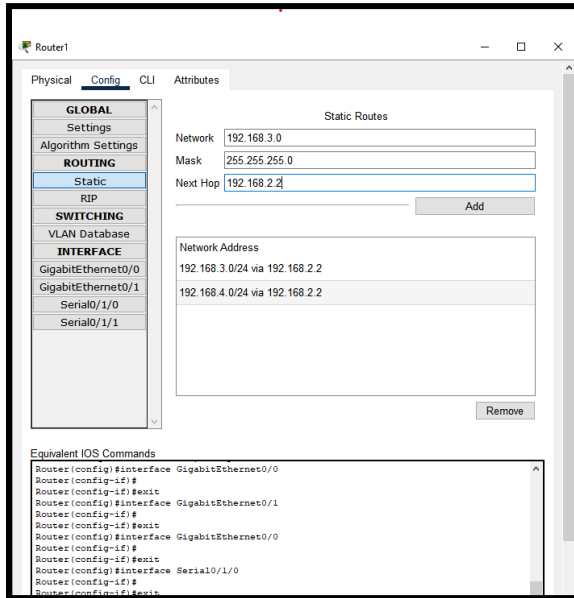
- Physical Tab:** Shows the router's hardware components.
- Config Tab:** The configuration page for Router5.
- Attributes:** Lists the configured interfaces: Serial0/1/0.
- Serial0/1/0 Configuration:**
 - Port Status:** On (checked).
 - Duplex:** Full Duplex (selected).
 - Clock Rate:** 2000000.
 - IP Configuration:** IP Address: 192.168.3.2, Subnet Mask: 255.255.255.0.
 - Tx Ring Limit:** 10.
- Equivalent IOS Commands:**

```
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
```

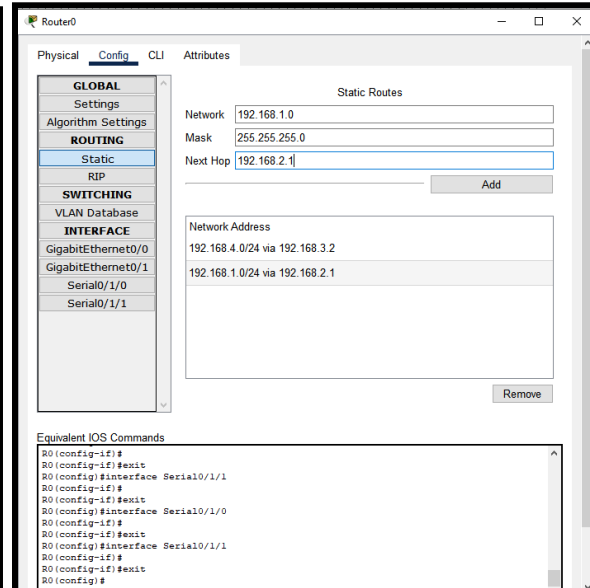
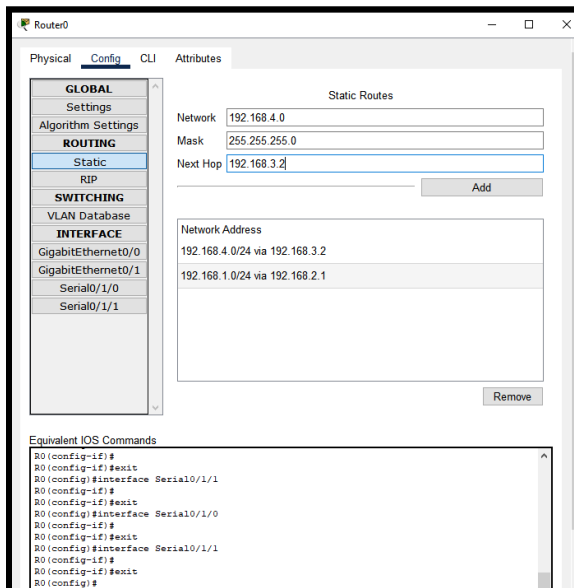
Part1: Static Routing

Static Routing is done using the following procedure for each Router

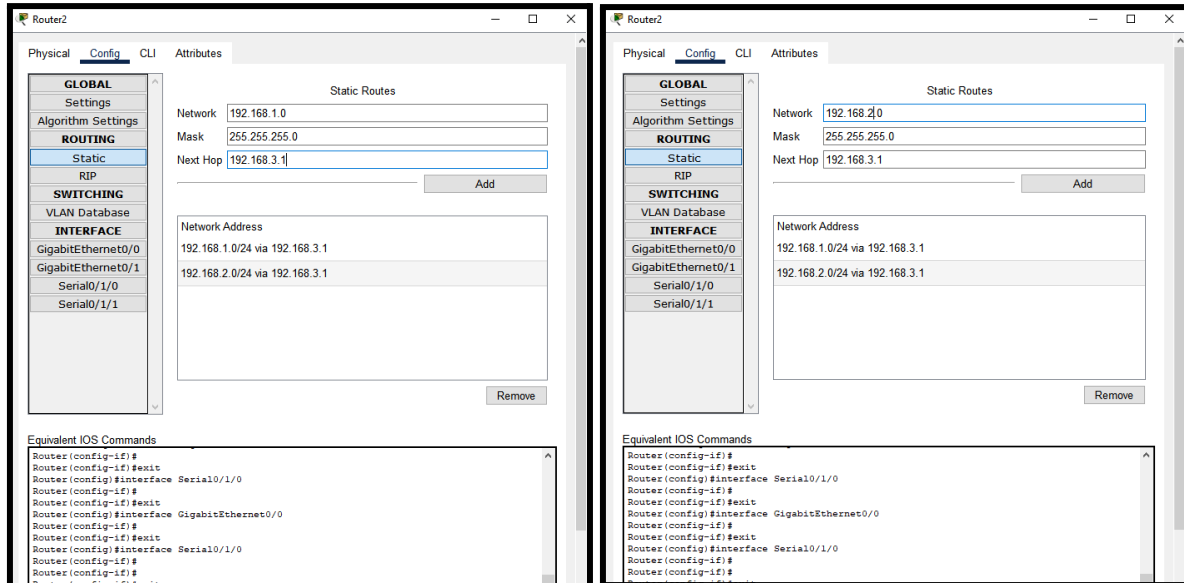
Router 1:



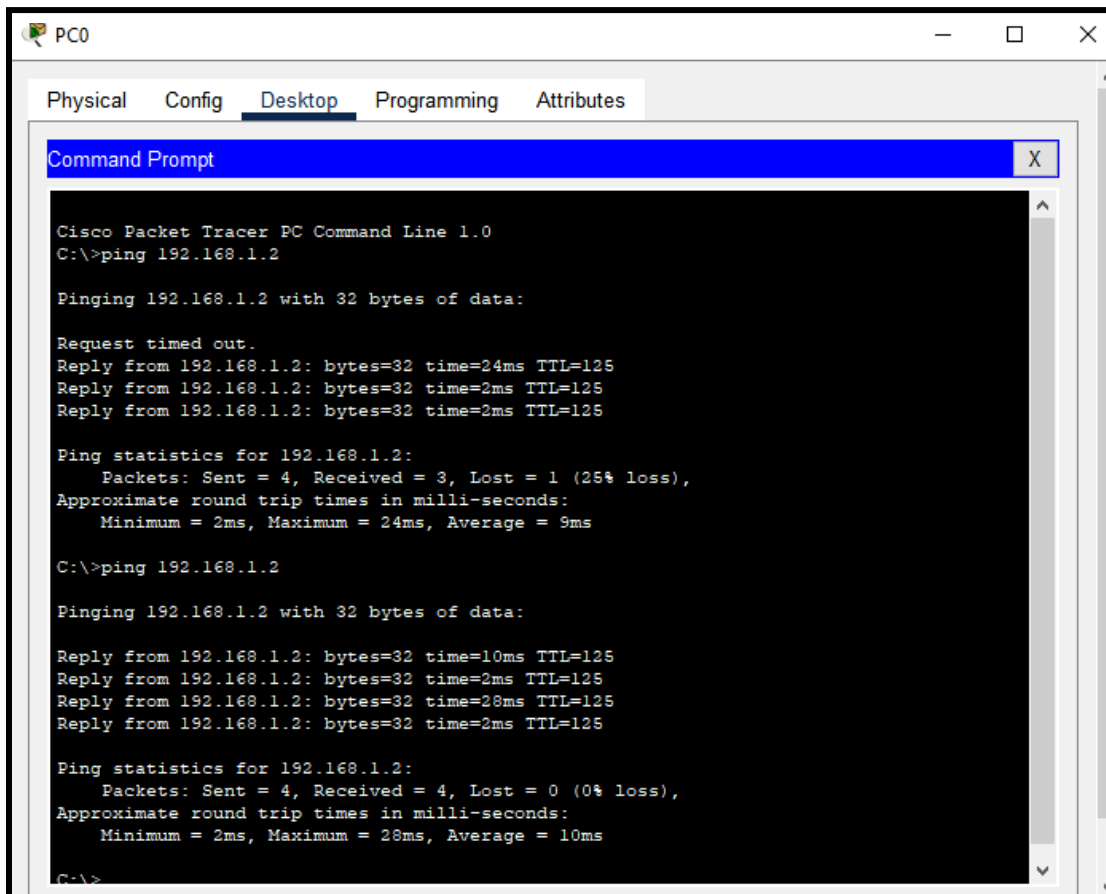
Router 0:



Router 2:



Check the connectivity by pinging the server from the PC

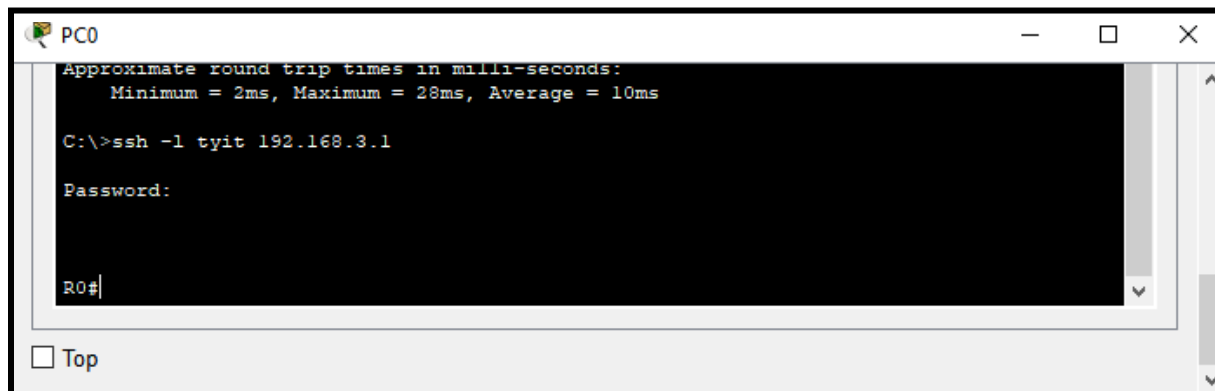


Part 2: Configuring SSH on Router 0

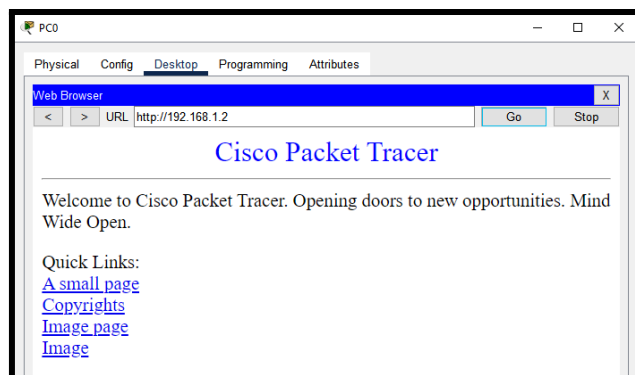
Router 0 → CLI

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

Now we verify the SSH using PC as follows



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



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

show version

If not type the below command in CLI

enable

conf t

license boot module c1900 technology-package securityk9

Accept→ yes

Click enter

exit

copy run start

reload

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

Part 3: Create the Firewall Zones on Router2

Type the following commands in the CLI mode of Router2

Router#

Router#configure terminal

Router(config)#zone security in-zone

Router(config-sec-zone)#exit

Router(config)#zone security out-zone

Router(config-sec-zone)#exit

Router(config)#access-list 101 permit ip 192.168.4.0 0.0.0.255 any

Router(config)#class-map type inspect match-all in-map

Router(config-cmap)#match access-group 101

Router(config-cmap)#exit

Router(config)#policy-map type inspect in-out

Router(config-pmap)#class type inspect in-map

Router(config-pmap-c)#inspect

Router(config-pmap-c)#exit

Router(config-pmap)#exit

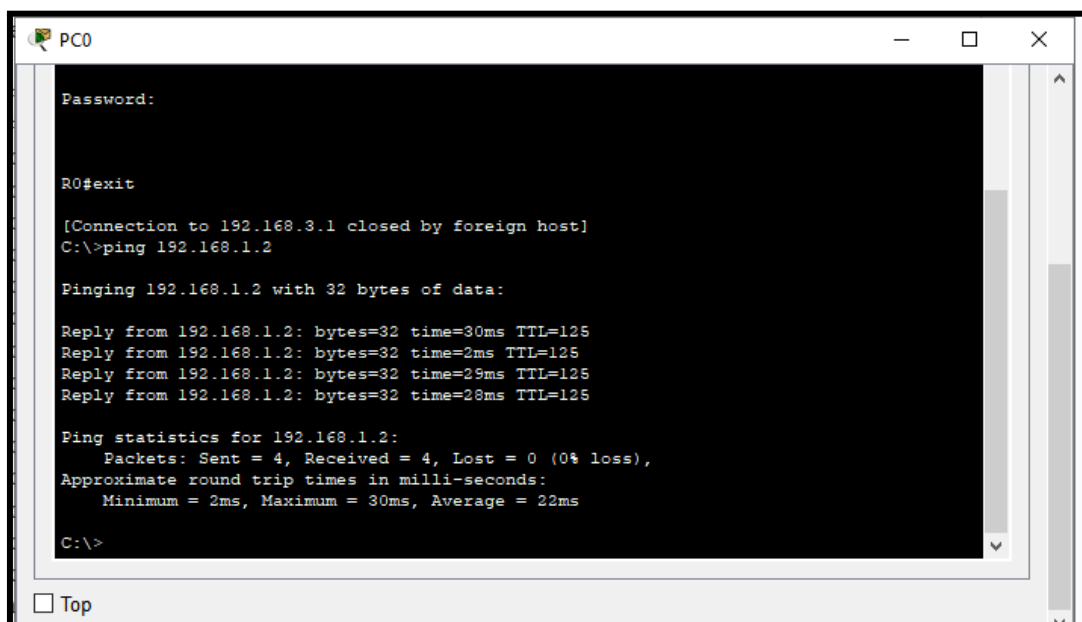
Router(config)#zone-pair security in-out-zone source in-zone destination out-zone

Router(config-sec-zone-pair)#service-policy type inspect in-out

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

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

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



```
PC0
Password:

R0#exit

[Connection to 192.168.3.1 closed by foreign host]
C:\>ping 192.168.1.2

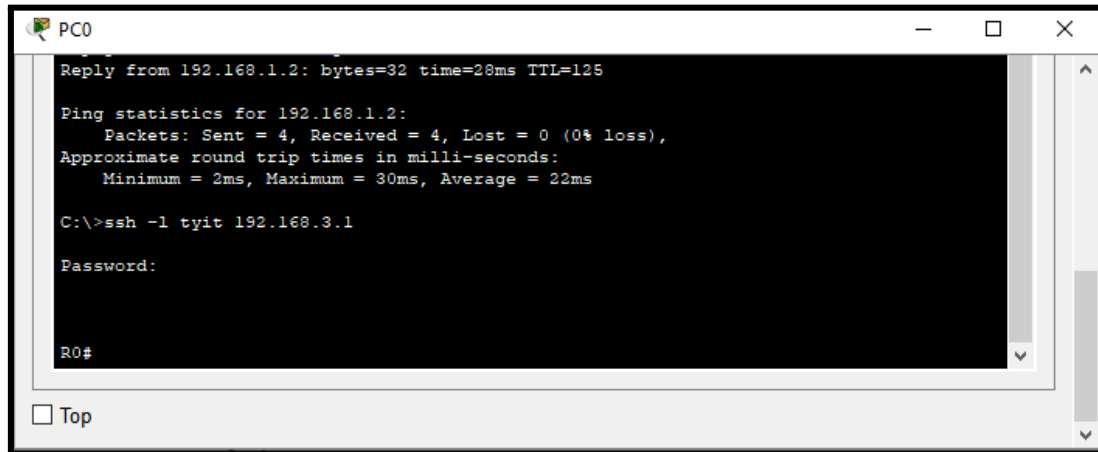
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=30ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=29ms TTL=125
Reply from 192.168.1.2: bytes=32 time=28ms 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 = 22ms

C:\>
```

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



```
Reply from 192.168.1.2: bytes=32 time=28ms 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 = 22ms

C:\>ssh -l tyit 192.168.3.1

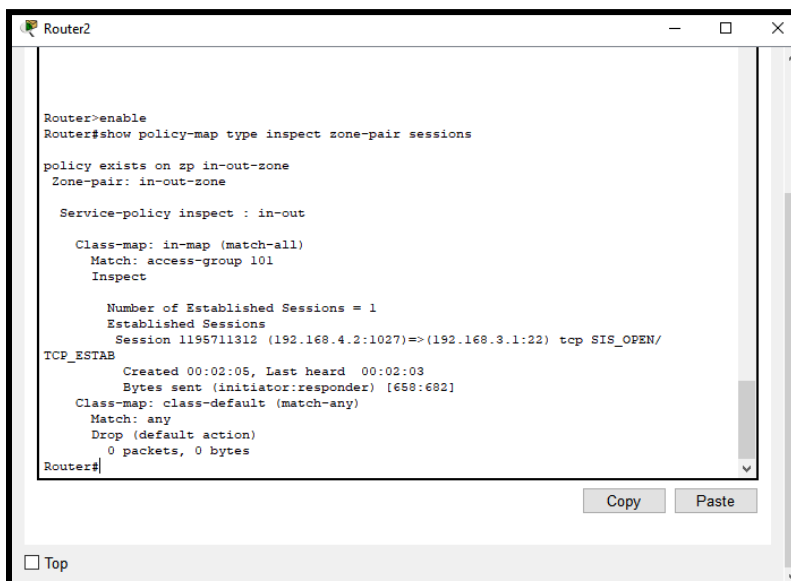
Password:

R0#
```

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

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

We will get the following output



```
Router2
Router>enable
Router#show policy-map type inspect zone-pair sessions

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

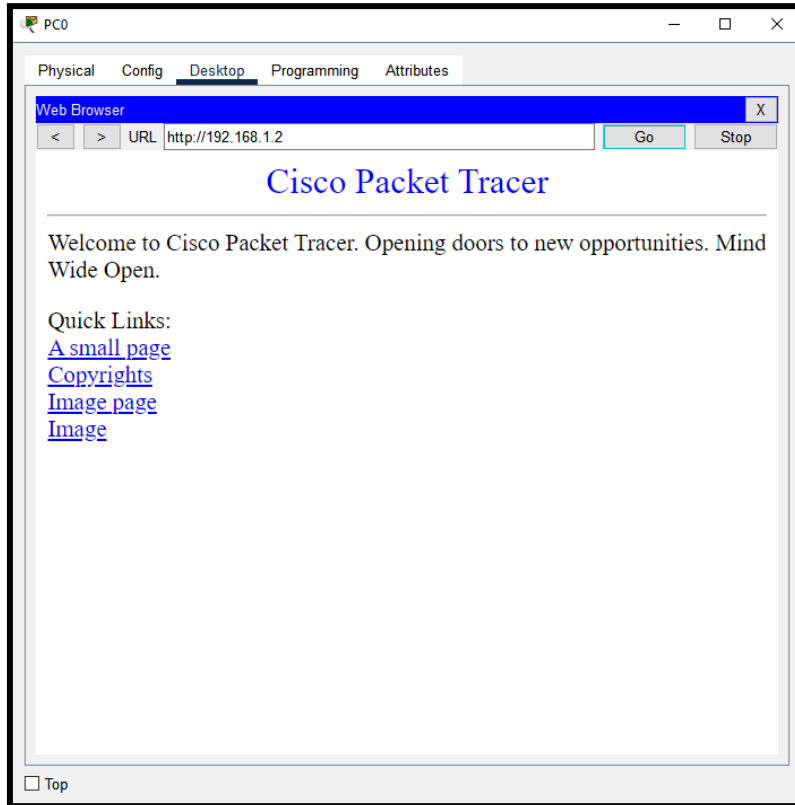
Service-policy inspect : in-out

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

    Number of Established Sessions = 1
    Established Sessions
      Session 1195711312 (192.168.4.2:1027)=>(192.168.3.1:22) tcp SIS_OPEN/
TCP_ESTAB
  Created 00:02:05, Last heard 00:02:03
  Bytes sent (initiator:responder) [658:682]
  Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    0 packets, 0 bytes
Router#
```

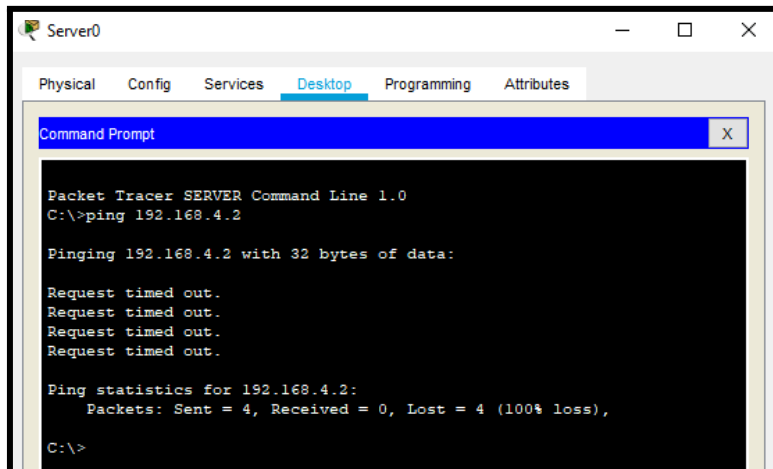
Step 4: We close the SSH connection and open the web browser and access the server

address (192.168.1.2) and get the following



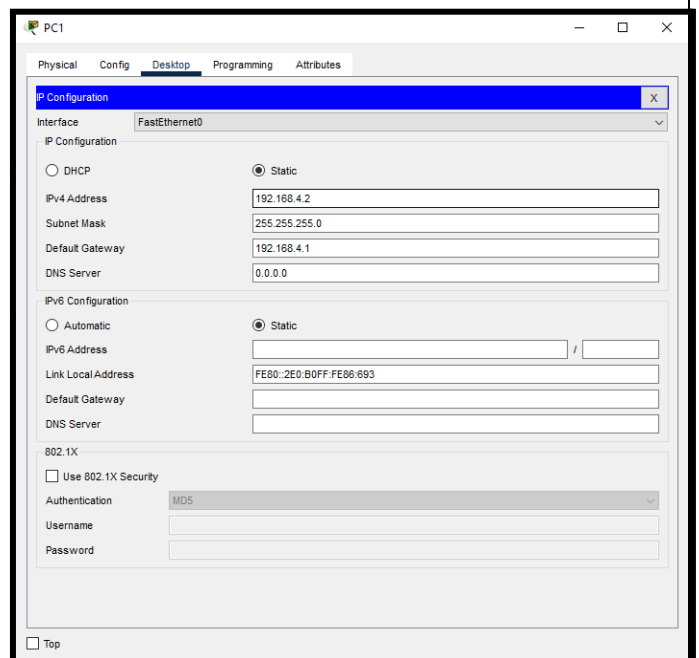
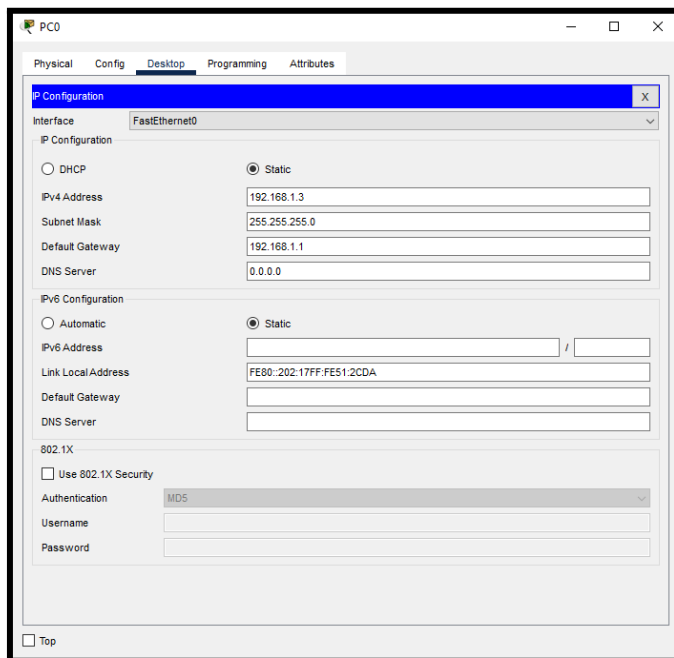
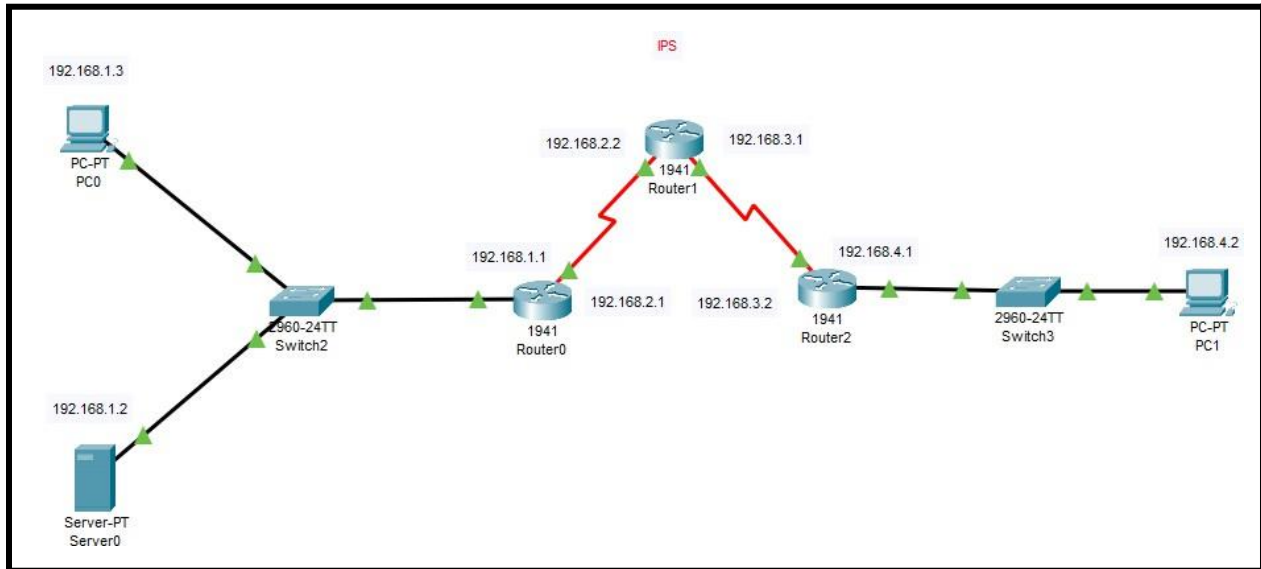
Part 5: Testing the Firewall Functionality (from out-zone to in-zone) by the following steps

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



Practical 6

Configure IOS Intrusion Prevention System (IPS) Using the CLI



Server0

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:43FF:FE15:64B3

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Router0

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

GigabitEthernet0/0

Port Status: ☒ On

Bandwidth: 1000 Mbps 100 Mbps 10 Mbps ☒ Auto

Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address: 00E0.A32A.6701

IP Configuration

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

Press RETURN to get started!

```

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

☐ Top

Router0

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Serial0/1/0

Port Status: ☒ On

Duplex: ☒ Full Duplex

Clock Rate: 2000000

IP Configuration

IPv4 Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#
  
```

☐ Top

Router1

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Port Status

Duplex ☒ Full Duplex

Clock Rate 1200

IP Configuration

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#
```

☐ Top

Router1

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Port Status

Duplex ☒ Full Duplex

Clock Rate 2000000

IP Configuration

IPv4 Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config)#
Router(config)#interface Serial0/1/1
Router(config-if)#
```

☐ Top

Router2

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Port Status

Duplex ☒ Full Duplex

Clock Rate 1200

IP Configuration

IPv4 Address 192.168.3.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Press RETURN to get started!

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

☐ Top

Router2

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

Port Status

Bandwidth ☐ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 000B.BE16.3201

IP Configuration

IPv4 Address 192.168.4.1

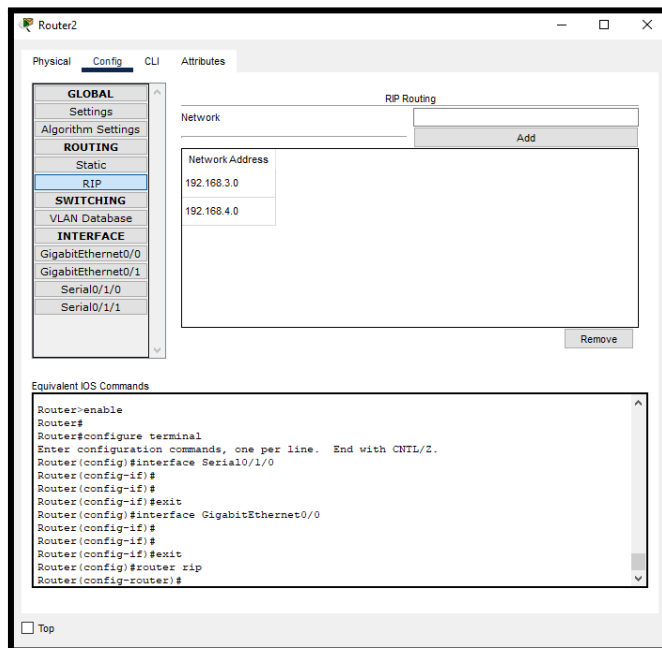
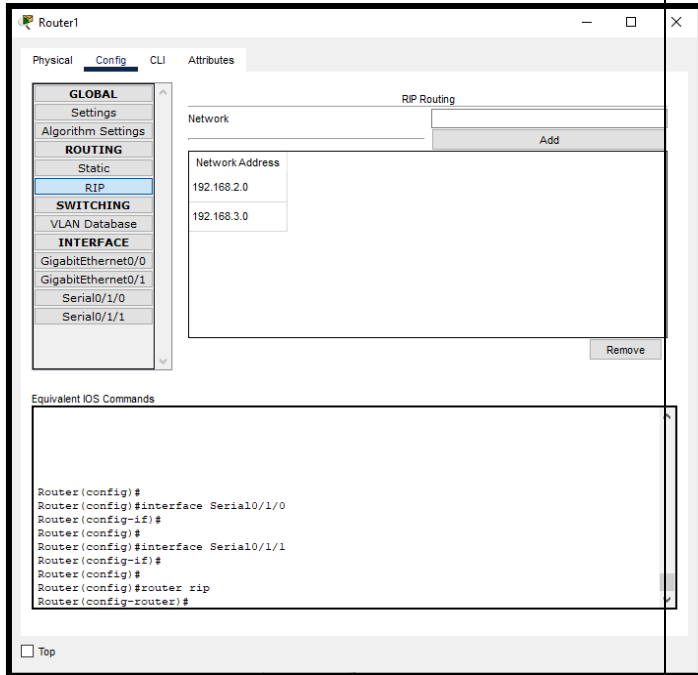
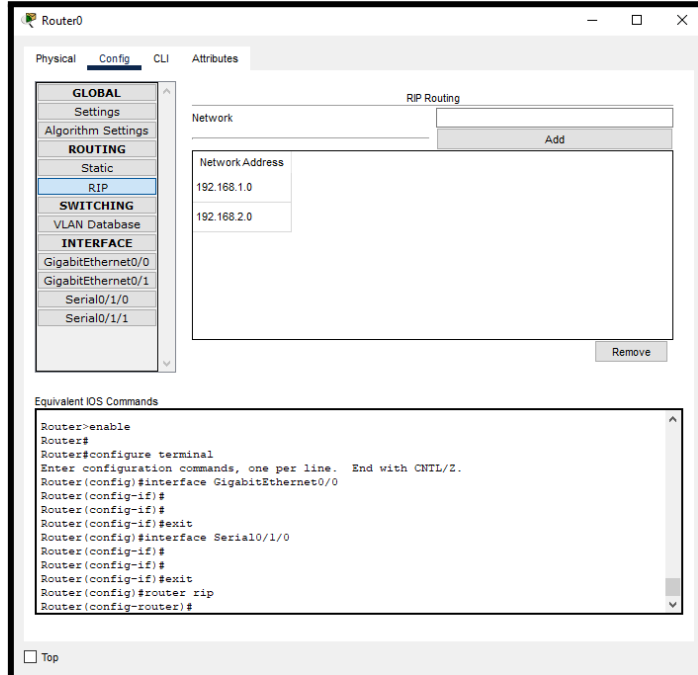
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
```

☐ Top



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt

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

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=18ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125

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

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

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

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

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

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

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=8ms TTL=125
Reply from 192.168.1.3: bytes=32 time=13ms TTL=125
Reply from 192.168.1.3: bytes=32 time=5ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 7ms
```

```
PC0
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC 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=9ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms 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 = 9ms, Average = 3ms

C:\>
```

```

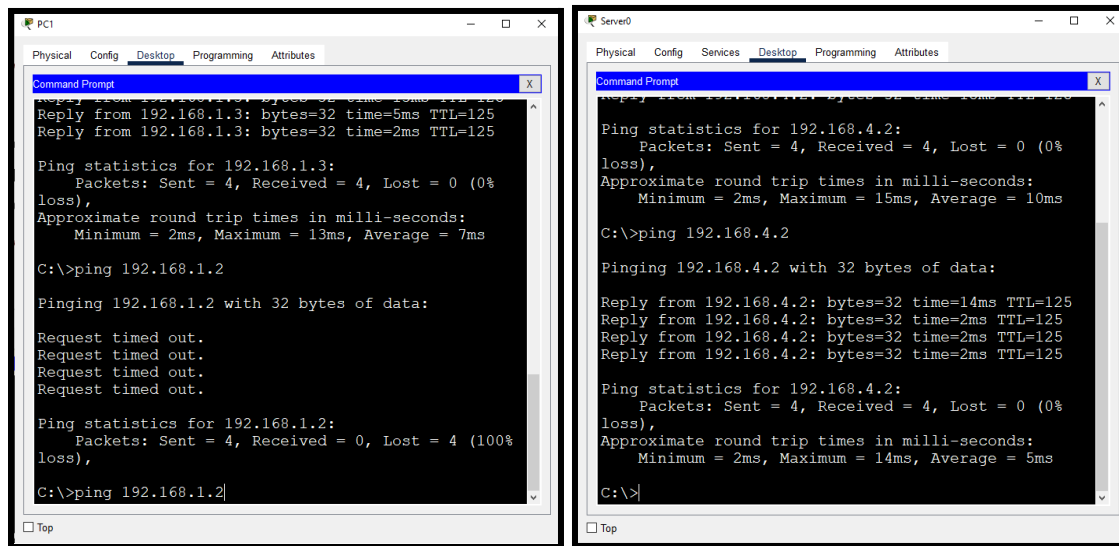
Router>enable
Router#show version
Router#conf t
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#exit
Router#reload
#####
Router>enable
Router#
Router#show version
securityk9 installed successfully

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

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

```

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



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.3: bytes=32 time=5ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 13ms, Average = 7ms

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:\>ping 192.168.1.2

Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
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 = 15ms, Average = 10ms

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=14ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms 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 = 14ms, Average = 5ms

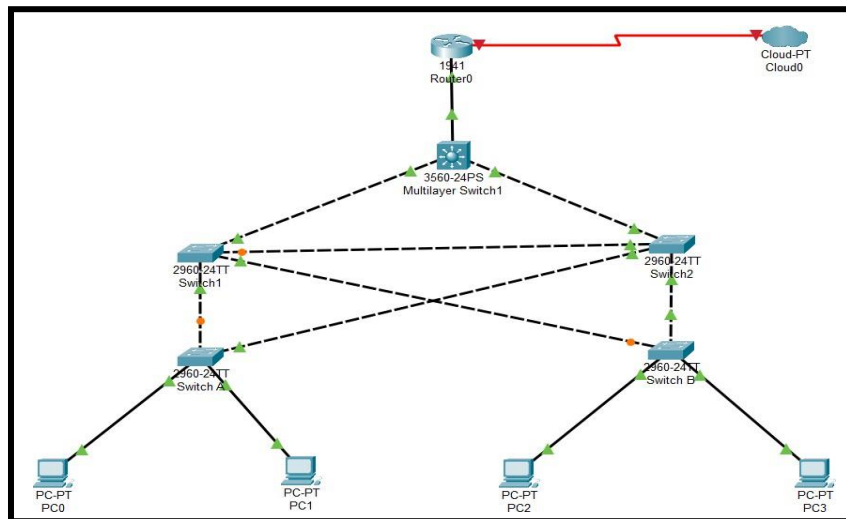
C:\>
```

Practical 7

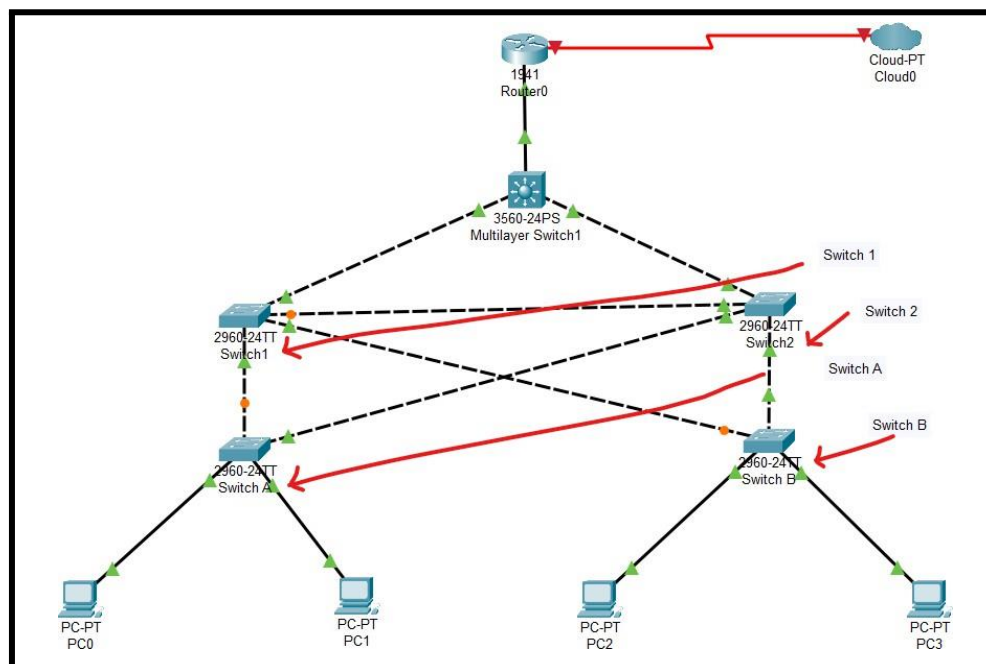
Layer 2 Security

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

- a) Assign the Central switch as the root bridge.



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



Part 1 : Root Bridge is set up

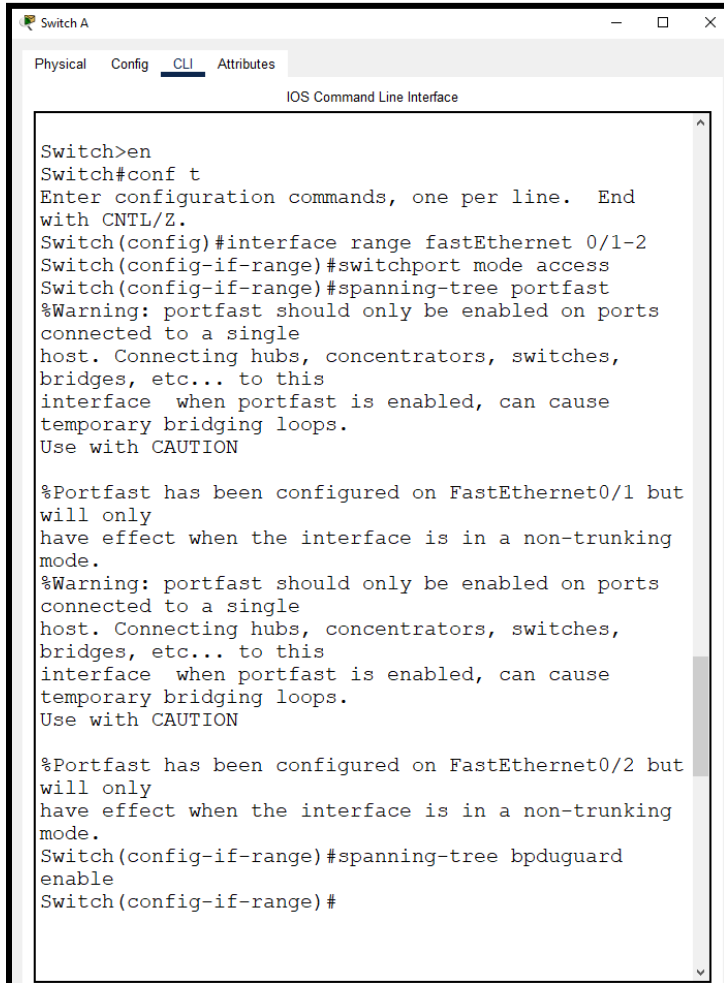
Part 2-Protect Against STP Attack

Redundant links are always welcome in switch topology as they are increasing the

network's availability and robustness.

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

Switch A Configuration



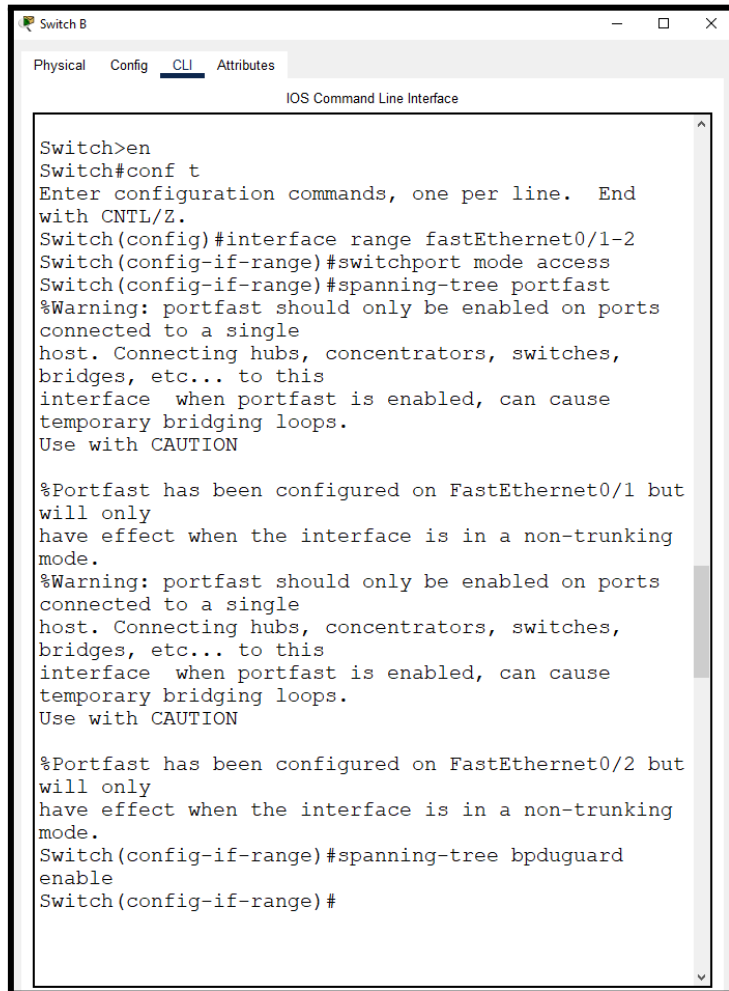
```
Switch A
Physical Config CLI Attributes
IOS Command Line Interface

Switch>en
Switch#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-2
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)#
```

Switch B Configuration

A screenshot of a network switch's CLI interface, titled 'Switch B'. The window has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The main area is labeled 'IOS Command Line Interface'. The text shows the user entering 'en' to enter enable mode, then 'conf t' to enter configuration mode. They then configure interfaces fastEthernet0/1 and fastEthernet0/2, setting them to access mode and enabling portfast. Warnings are displayed for each interface. Finally, they enable bpduguard on both interfaces and return to the configuration prompt.

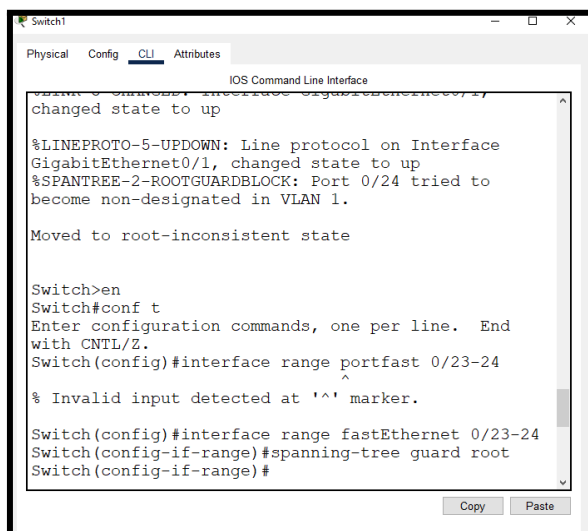
```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#interface range fastEthernet0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports
connected to a single
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)#
```

Switch 1 and Switch 2 Same command

Switch 1 and Switch 2 Configuration

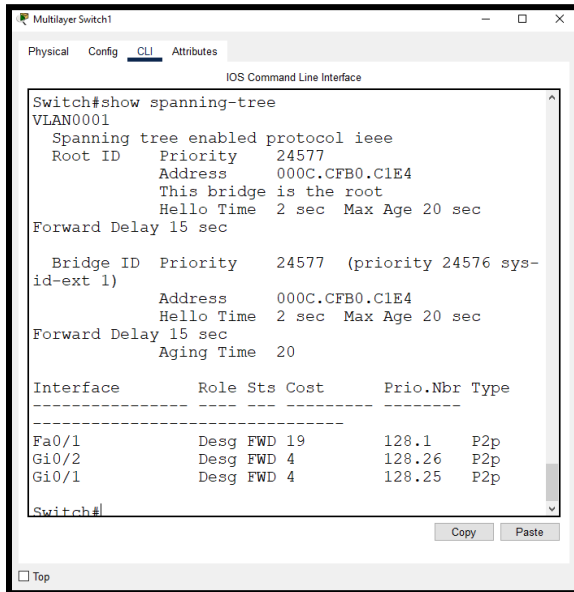
A screenshot of a network switch's CLI interface, titled 'Switch1'. The window has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The main area is labeled 'IOS Command Line Interface'. The text shows various system messages at the top, including line protocol status changes and spanning-tree events. The user then enters 'en' and 'conf t' to enter configuration mode. They attempt to configure interfaces 0/23-24 with 'portfast', but an error occurs due to an invalid input marker. They then successfully configure interfaces 0/23-24 with 'guard root' and return to the configuration prompt.

```
Switch1>
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
%SPANTREE-2-ROOTGUARDBLOCK: Port 0/24 tried to
become non-designated in VLAN 1.
Moved to root-inconsistent state

Switch1>en
Switch1#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch1(config)#interface range portfast 0/23-24
^
% Invalid input detected at '^' marker.

Switch1(config)#interface range fastEthernet 0/23-24
Switch1(config-if-range)#spanning-tree guard root
Switch1(config-if-range)#
```

MultiLayer Switch



The screenshot shows a CLI window titled "MultiLayer Switch1" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the output of the command "Switch#show spanning-tree". The output shows that spanning tree is enabled for VLAN0001, with the root ID being the switch itself (priority 24577, address 000C.CFB0.C1E4). It also lists the bridge ID, priority, address, hello time, max age, forward delay, and aging time. A table at the bottom shows the status of interfaces Fa0/1, Gi0/2, and Gi0/1.

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
    Root ID    Priority    24577
              Address     000C.CFB0.C1E4
              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     000C.CFB0.C1E4
              Hello Time 2 sec  Max Age 20 sec
              Forward Delay 15 sec
              Aging Time 20

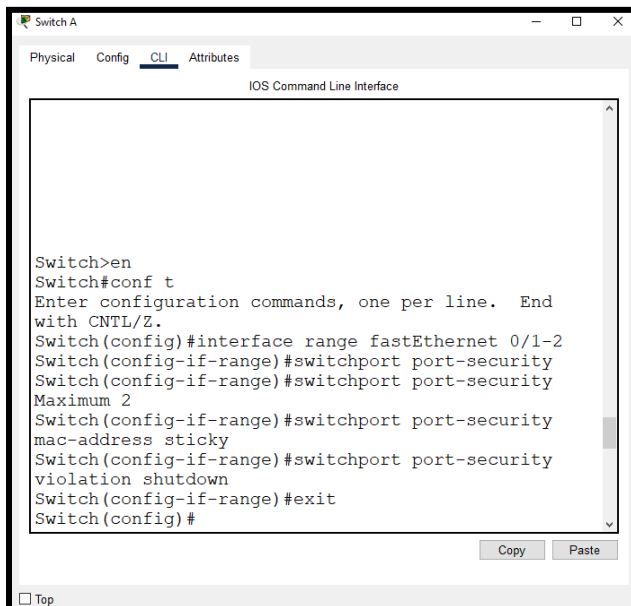
Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/1          Desg FWD 19        128.1    P2p
Gi0/2          Desg FWD 4         128.26   P2p
Gi0/1          Desg FWD 4         128.25   P2p

Switch#
```

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

Part 3 –Port Security and Disable Unused ports

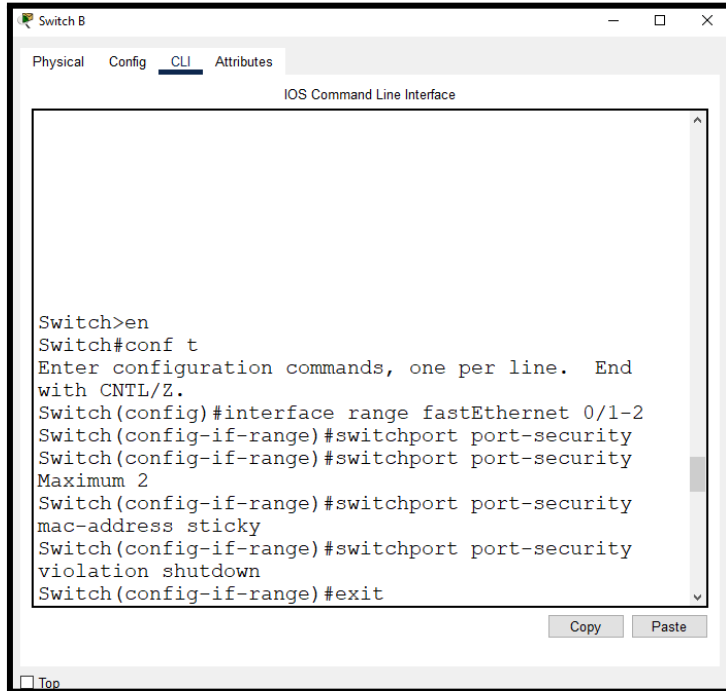
Switch A Configuration



The screenshot shows a CLI window titled "Switch A" with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the configuration commands for enabling port security on interfaces Fa0/1 and Fa0/2. The commands include entering configuration mode, configuring the interface range, enabling port security, setting the maximum number of MAC addresses to 2, and setting the violation action to shutdown.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-2
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)#
```

Switch B Configuration



Switch B

Physical Config CLI Attributes

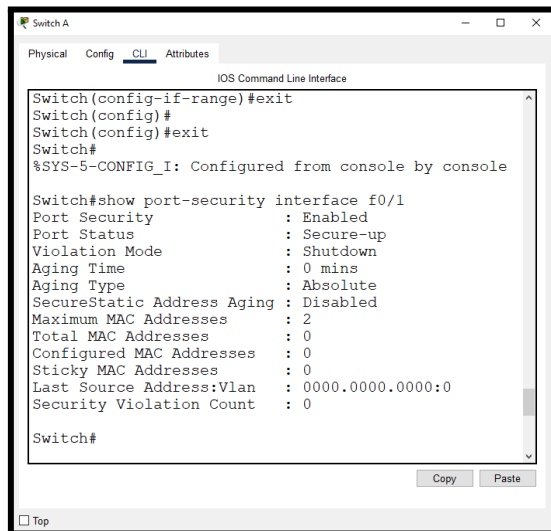
IOS Command Line Interface

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End
with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-2
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
```

Copy Paste

☐ Top

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



Switch A

Physical Config CLI Attributes

IOS Command Line Interface

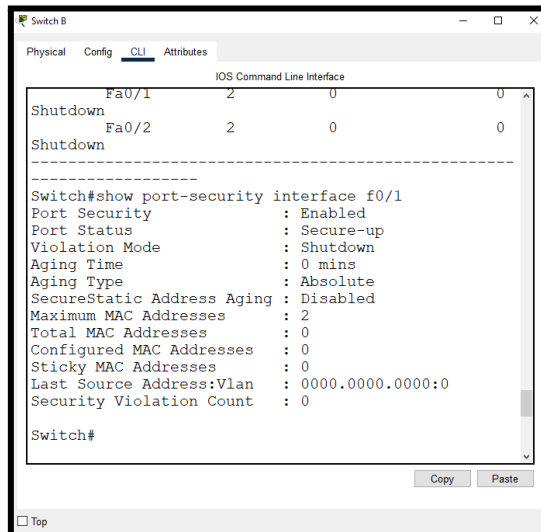
```
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

Switch#
```

Copy Paste

☐ Top



Switch B

Physical Config CLI Attributes

IOS Command Line Interface

```

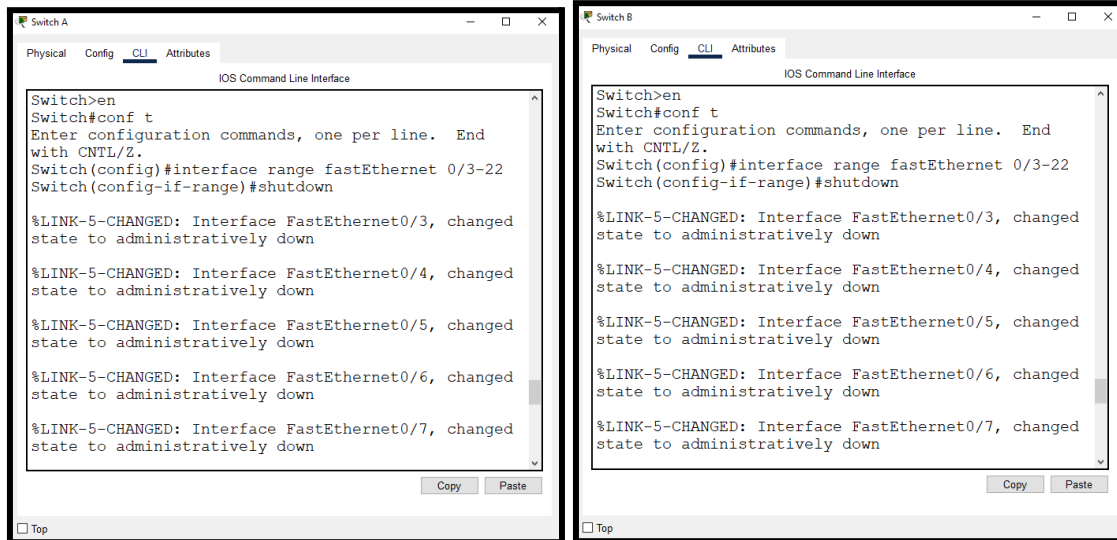
Fa0/1      2      0      0
Shutdown
Fa0/2      2      0      0
Shutdown
-----
Switch#show port-security interface f0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 2
Total MAC Addresses    : 0
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Switch#
```

Copy Paste

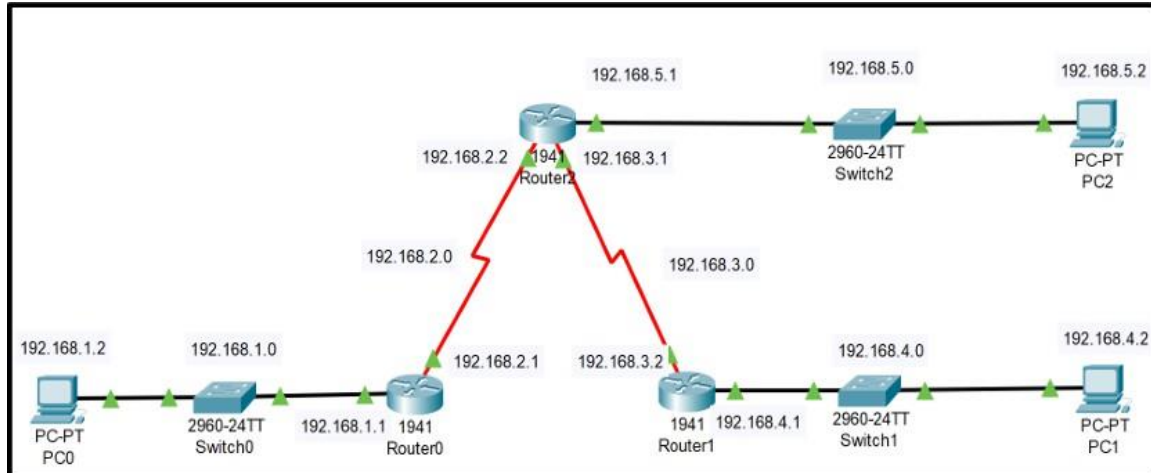
☐ Top

Shutting down all the unused ports

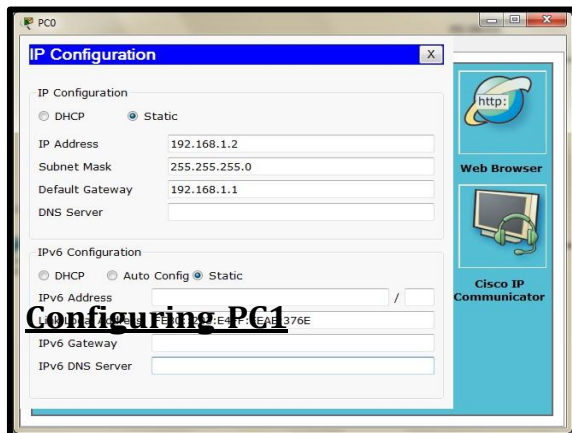


Practical

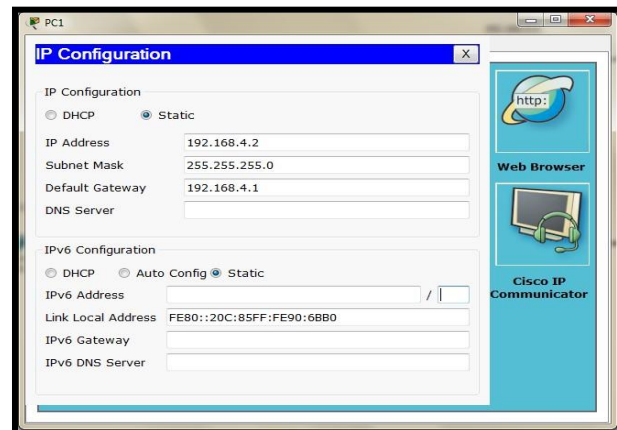
Configure and Verify a Site-to-Site IPsec VPN Using CLI



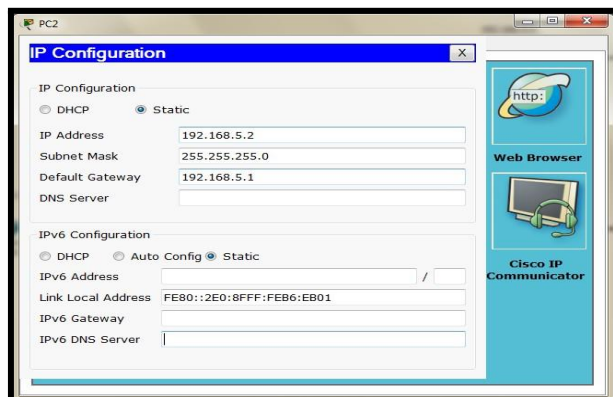
Configuring PC0 and PC1



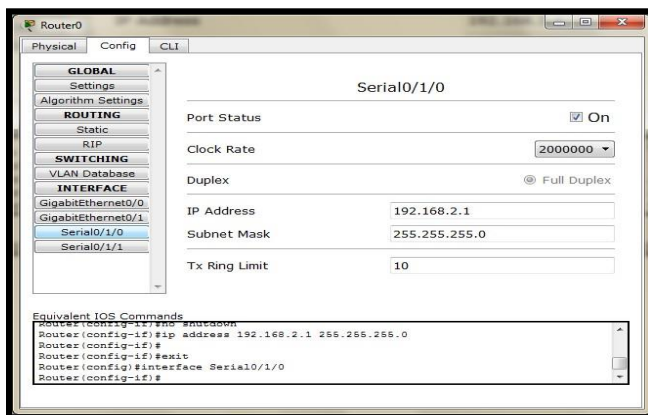
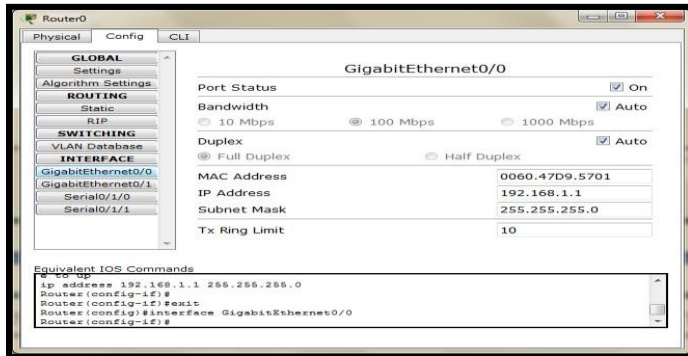
Configuring PC1



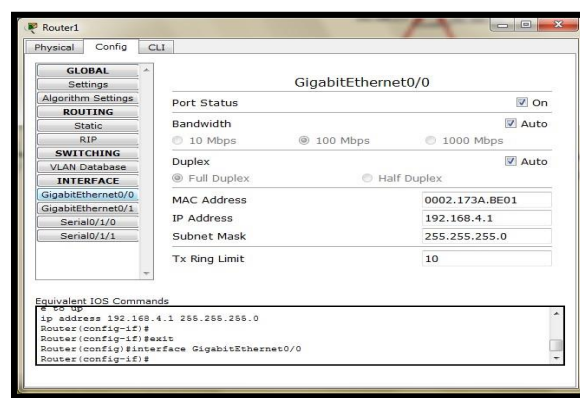
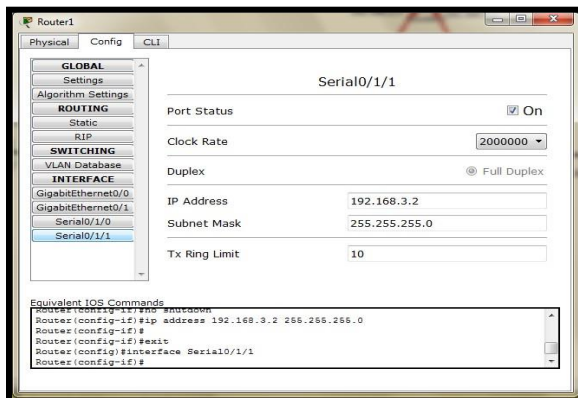
Configuring PC2



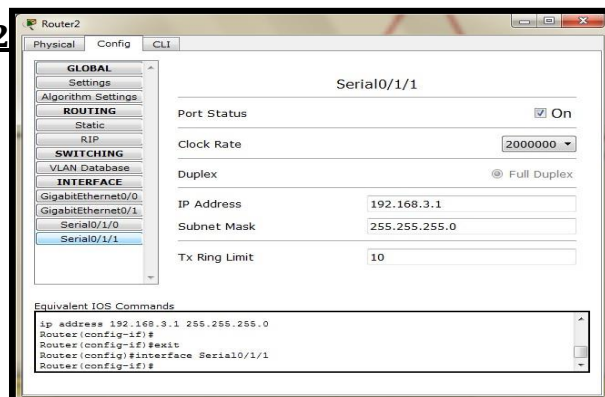
Configuring Router 0

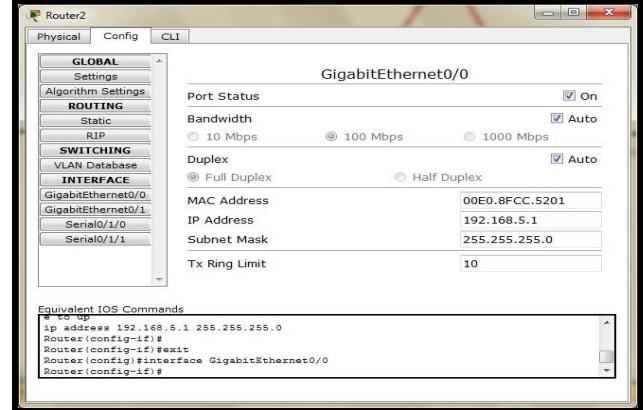
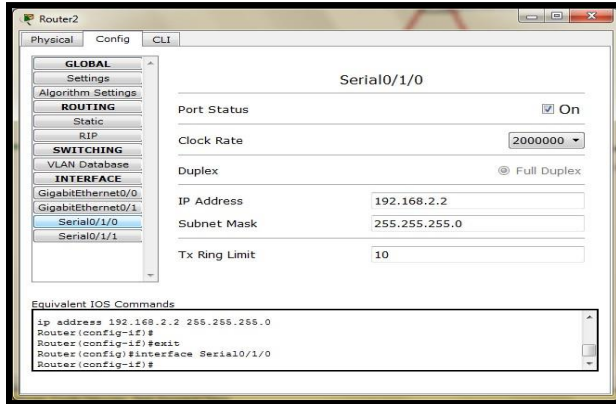


Configuring Router1



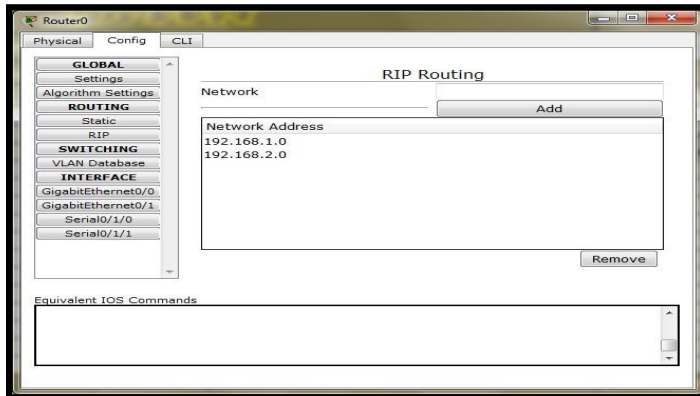
Configuring Router2



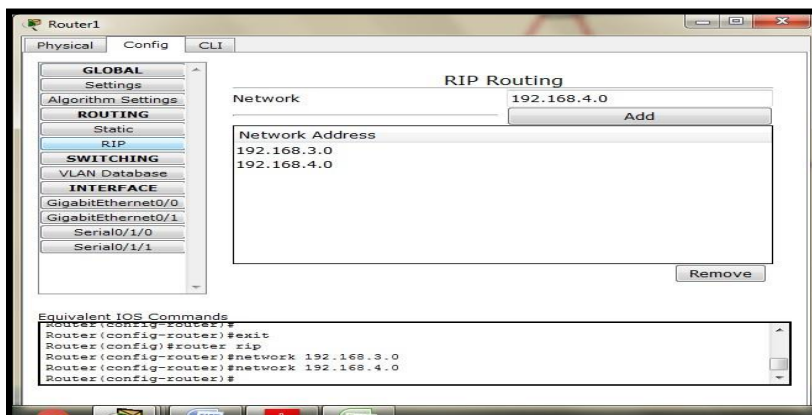


Part 1: Configuring RIP on each Router

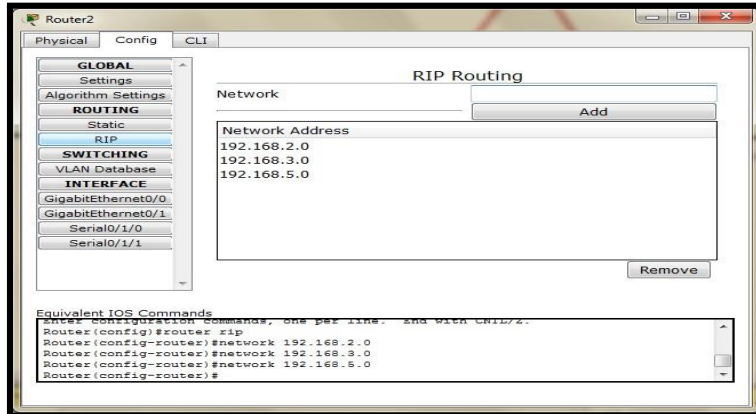
Router 0: Add the following networks



Router 1: Add the following networks

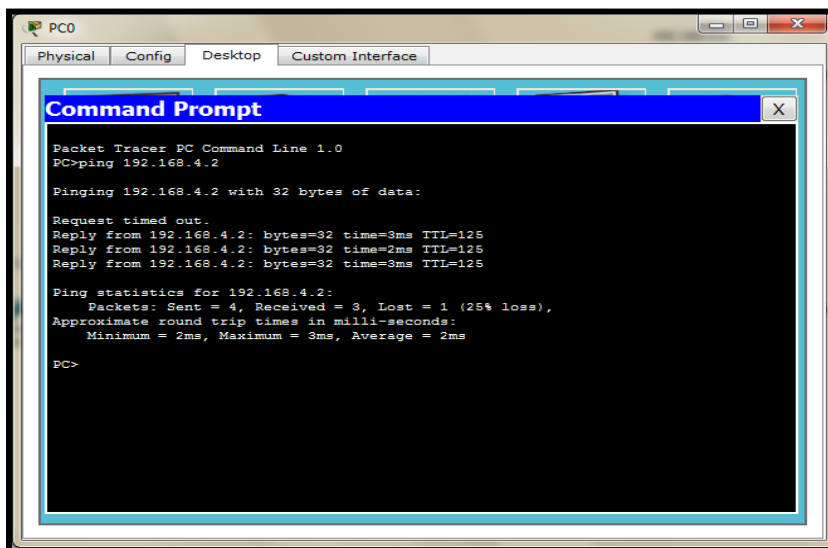


Router 2: Add the following networks

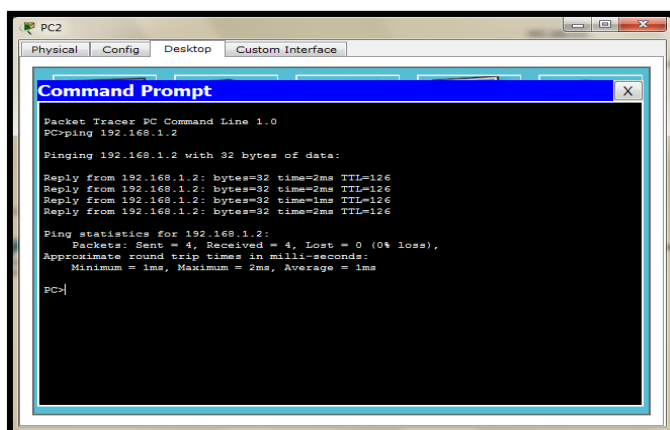


Now check the connectivity by ping command

PC0 to PC1 (it should be successful)



PC2 to PC0 (it should be successful)



Part 2: Configure IPSec Parameters on Router0

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

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

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

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

```
Router#show version
```

Step 2: Configuring IKA phase 1 ISAKMP policy on Router0

Type the following commands in the CLI mode of Router0

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

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

Part 3: Configure IPSec Parameters on Router1

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

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

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

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

```
Router#show version
```

Step 2: Configuring IKA phase 1 ISAKMP policy on Router1

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

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

```

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

```

Part 4: Verify the IPsec VPN

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

```

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

```



```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router>enable
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: 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

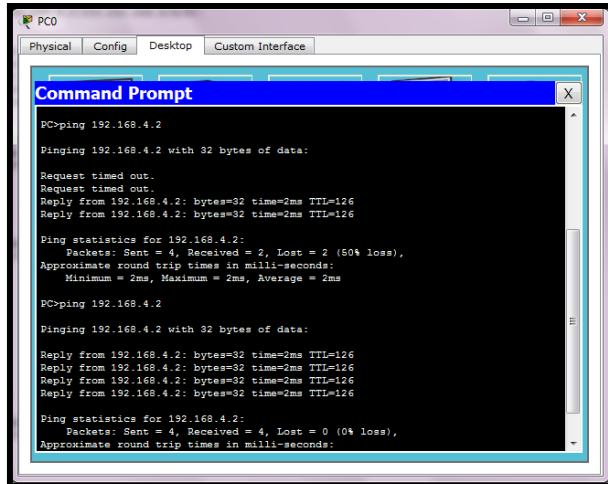
  local crypto endpt.: 192.168.2.1, remote crypto endpt.: 192.168.3.2
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
  current outbound spi: 0x0(0)

inbound esp sas:
inbound ah sas:
inbound pcg sas:
outbound esp sas:
outbound ah sas:
outbound pcg sas:
Router#

```

Step 2: Ping PC1 from PC0 (Creating interesting traffic)

We ping PC1 from PC0 (which is the interesting traffic)



```
PC0
Physical Config Desktop Custom Interface

Command Prompt

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.4.2: bytes=32 time=2ms TTL=126
Reply from 192.168.4.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>ping 192.168.4.2

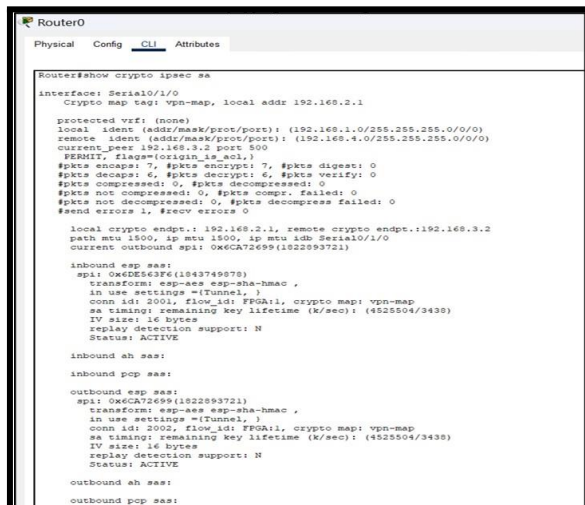
Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=2ms TTL=126
Reply from 192.168.4.2: bytes=32 time=2ms TTL=126
Reply from 192.168.4.2: bytes=32 time=2ms TTL=126
Reply from 192.168.4.2: bytes=32 time=2ms 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:
```

And now we check the Router0 by typing the following Command

Router#show crypto ipsec sa



```
Router0
Physical Config CLI Attributes

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 192.168.4.2 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 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: 0x6CA72699(1822893721)

inbound esp sas:
  spi: 0x6DE6437F(1843749578)
    transform: esp-aes esp-sha-hmac ,
    in use settings = (Tunnel, 1)
    conn id: 2001, flow_id: FFGA11, crypto map: vpn-map
    sa timing: remaining key lifetime (k/sec): (4525504/3438)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

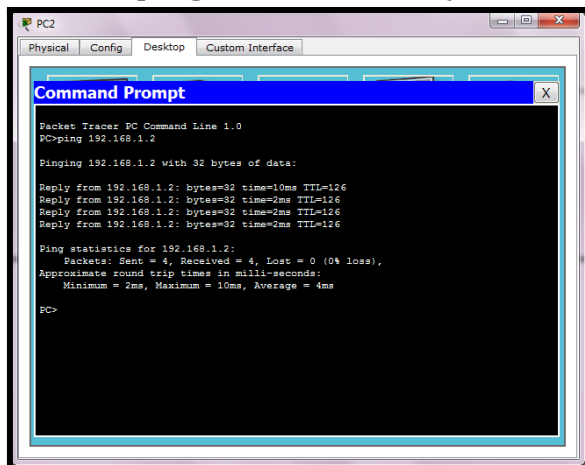
outbound esp sas:
  spi: 0x6CA72699(1822893721)
    transform: esp-aes esp-sha-hmac ,
    in use settings = (Tunnel, 1)
    conn id: 2002, flow_id: FFGA11, crypto map: vpn-map
    sa timing: remaining key lifetime (k/sec): (4525504/3438)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

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

Now we ping PC0 from PC0 (which is interesting traffic)



```
PC2
Physical Config Desktop Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

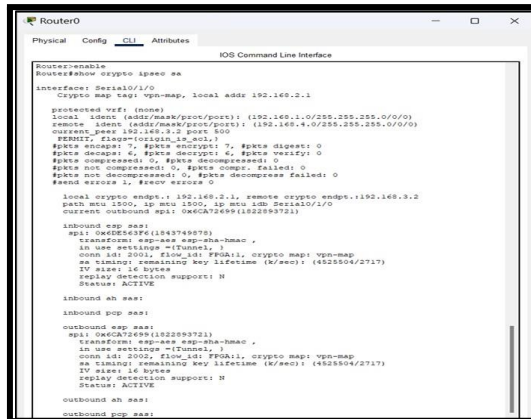
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms 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 = 2ms, Maximum = 10ms, Average = 4ms

PC>
```

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



```
Router0#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): (192.168.1.0/255.255.0.0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.0.0/0)
current_peer 192.168.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp. failed: 0
#pkts not decompressed: 0, #pkts decomp. 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: 0x6CA72699(1822893721)

inbound esp sas:
spi: 0x6DE563F6(1843749878)
transform: esp-esp esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2001, flow_id: FFD11, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/2717)
IV size: 16 bytes
 replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

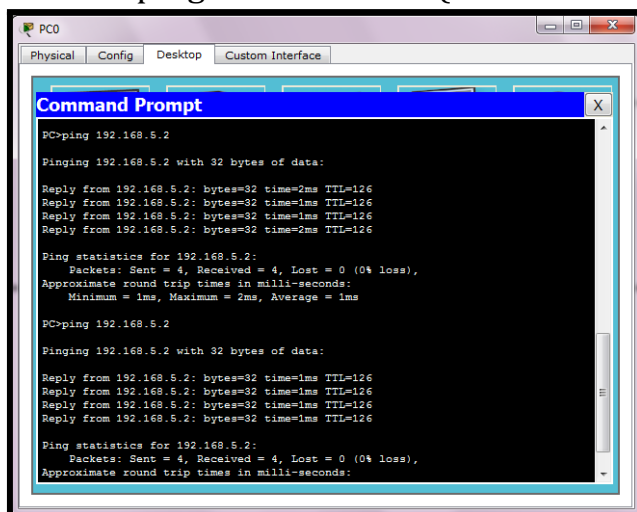
outbound esp sas:
spi: 0x6CA72699(1822893721)
transform: esp-esp esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2002, flow_id: FFD11, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/2717)
IV size: 16 bytes
 replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

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

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



```
PC0#ping 192.168.5.2
Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=2ms TTL=126
Reply from 192.168.5.2: bytes=32 time=1ms TTL=126
Reply from 192.168.5.2: bytes=32 time=1ms TTL=126
Reply from 192.168.5.2: bytes=32 time=2ms 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 = 1ms, Maximum = 2ms, Average = 1ms

PC0#ping 192.168.5.2
Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=1ms TTL=126
Reply from 192.168.5.2: bytes=32 time=1ms TTL=126
Reply from 192.168.5.2: bytes=32 time=1ms TTL=126
Reply from 192.168.5.2: bytes=32 time=1ms 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:
```

And now we check the Router0 by typing the following Command

Router#show crypto ipsec sa



```
Router0#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): (192.168.1.0/255.255.0.0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.0.0/0)
current_peer 192.168.3.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp. failed: 0
#pkts not decompressed: 0, #pkts decomp. 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: 0x6CA72699(1822893721)

inbound esp sas:
spi: 0x6DE563F6(1843749878)
transform: esp-esp esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2001, flow_id: FFD11, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/2717)
IV size: 16 bytes
 replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x6CA72699(1822893721)
transform: esp-esp esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2002, flow_id: FFD11, crypto map: vpn-map
sa timing: remaining key lifetime (k/sec): (4525504/2717)
IV size: 16 bytes
 replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```