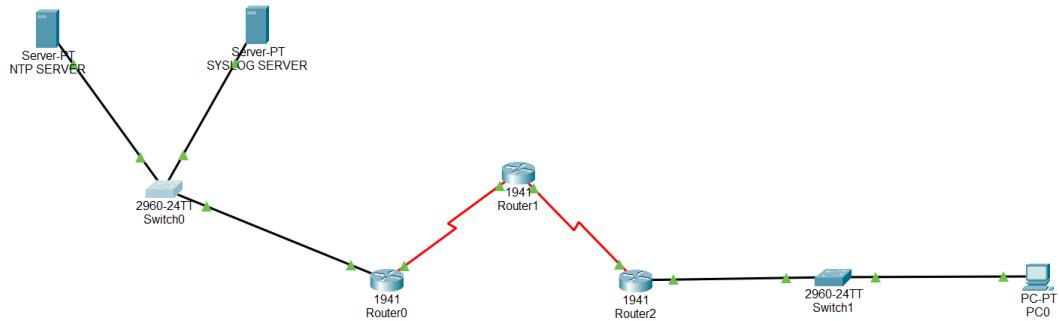


Practical 1

Aim: Configure Routers:

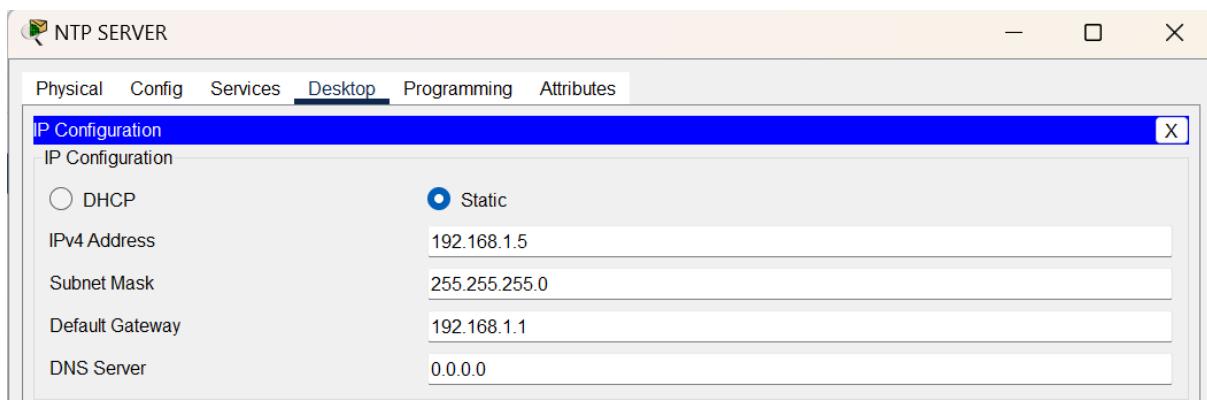
- a. OSPF MD5 Authentication
- b. NTP
- c. To log messages to the SYSLOG server
- d. To support SSH connections

➤ Topology Diagram

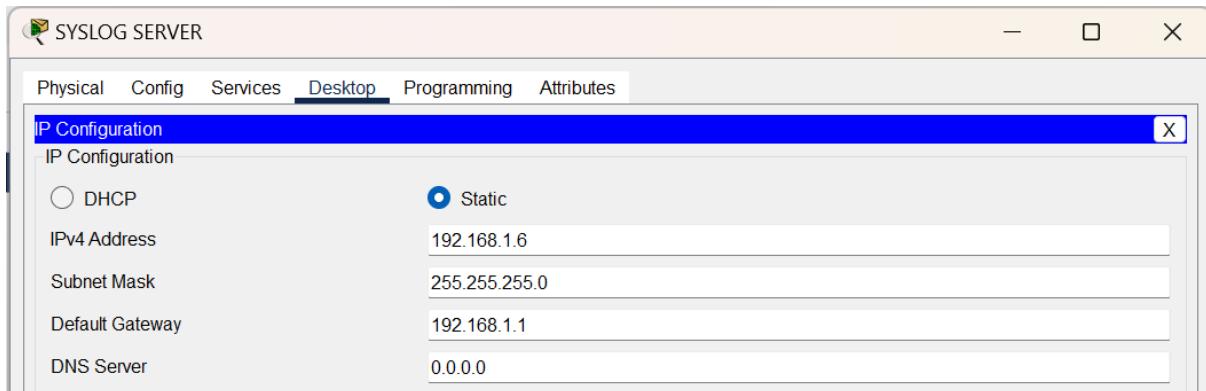


➤ Assigning IP Addresses

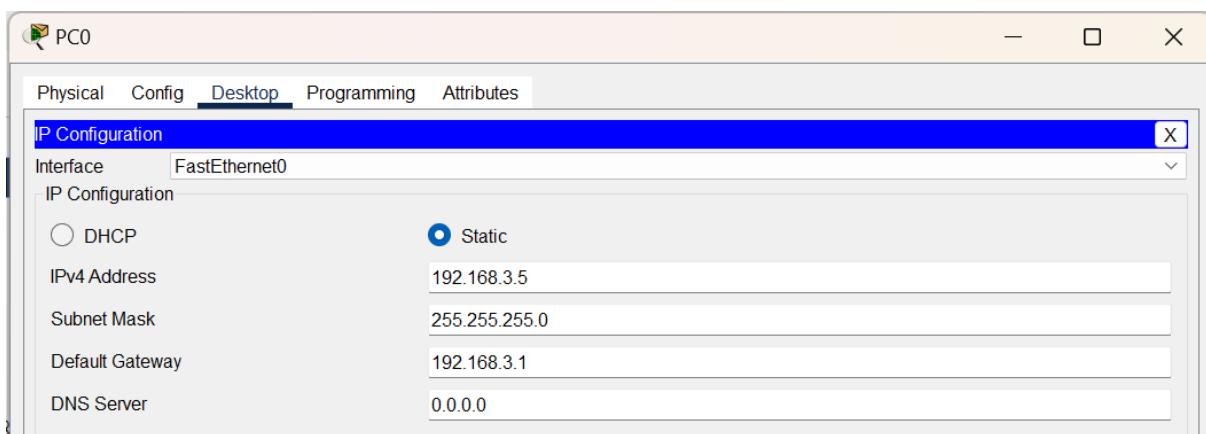
1. NTP Server



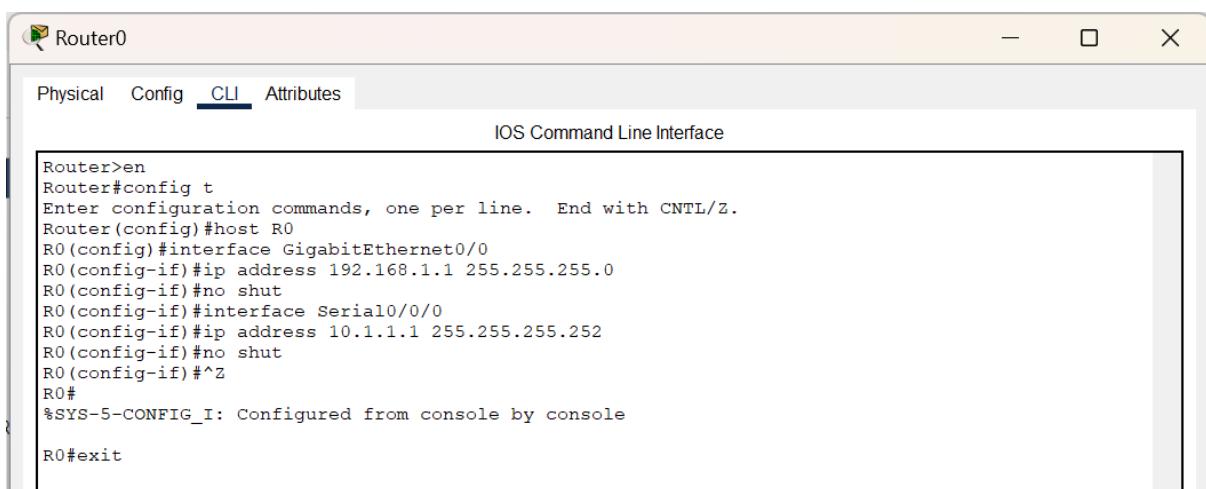
2. SYSLOG Server



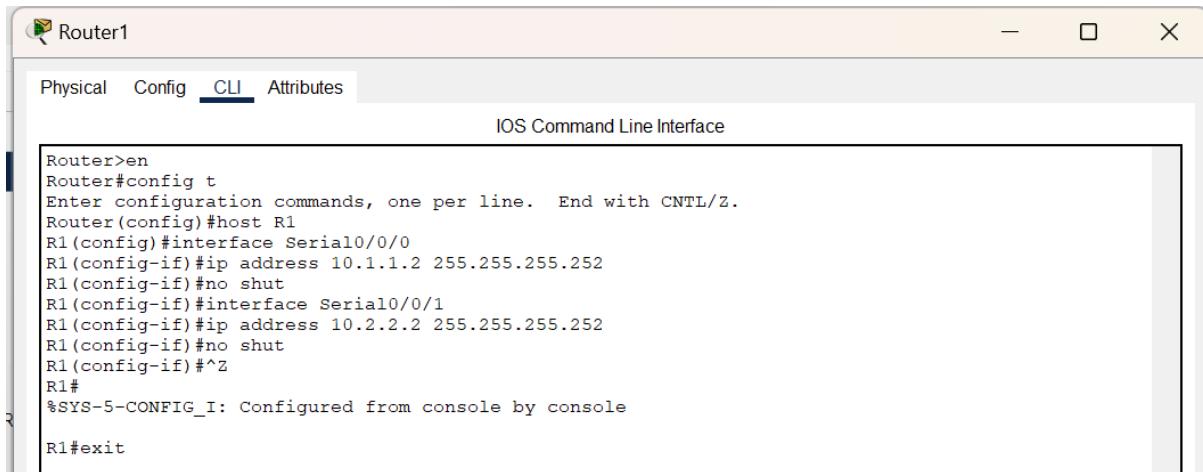
3. PC-0



4. Router 0



5. Router 1



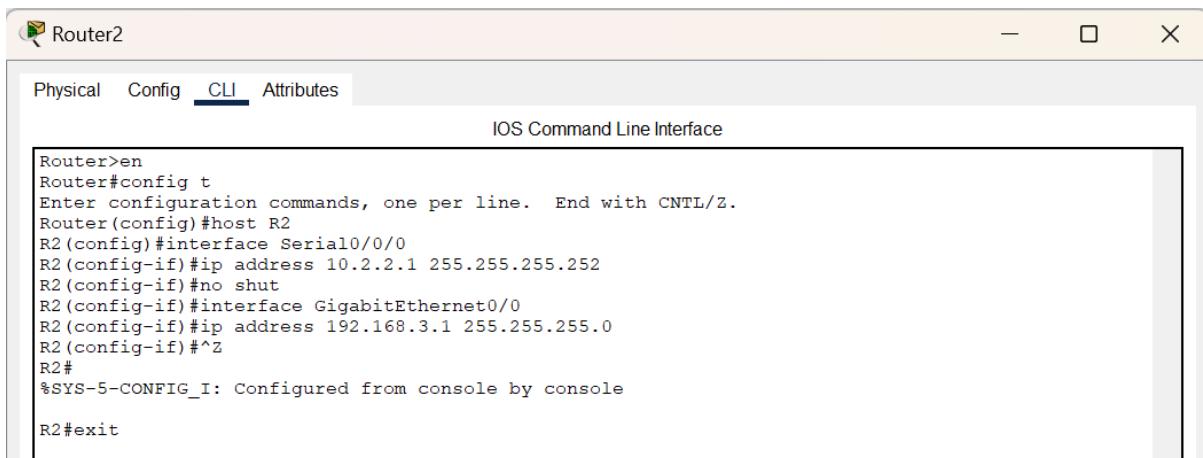
Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.2 255.255.255.252
R1(config-if)#no shut
R1(config-if)#interface Serial0/0/1
R1(config-if)#ip address 10.2.2.2 255.255.255.252
R1(config-if)#no shut
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

6. Router 2



Router2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.2.2.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#interface GigabitEthernet0/0
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ Displaying IP Address Details of Routers

1. Router 0

```
R0>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.1.1    YES manual up       up
GigabitEthernet0/1  unassigned     YES unset administratively down down
Serial0/0/0         10.1.1.1      YES manual up       up
Serial0/0/1         unassigned     YES unset administratively down down
GigabitEthernet0/1/0 unassigned     YES unset administratively down down
Vlan1              unassigned     YES unset administratively down down
```

2. Router 1

```
R1>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  unassigned      YES unset administratively down down
GigabitEthernet0/1  unassigned      YES unset administratively down down
Serial0/0/0         10.1.1.2       YES manual up        up
Serial0/0/1         10.2.2.2       YES manual up        up
GigabitEthernet0/1/0 unassigned      YES unset administratively down down
Vlan1              unassigned      YES unset administratively down down
```

3. Router 2

```
R2>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.3.1    YES manual up        up
GigabitEthernet0/1  unassigned      YES unset administratively down down
Serial0/0/0         10.2.2.1       YES manual up        up
Serial0/0/1         unassigned      YES unset administratively down down
GigabitEthernet0/1/0 unassigned      YES unset administratively down down
Vlan1              unassigned      YES unset administratively down down
```

➤ Configure OSPF on routes

1. Router 0

```
R0>
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#router ospf 1
R0(config-router)#network 192.168.1.0 0.0.0.255 area 0
R0(config-router)#network 10.1.1.0 0.0.0.3 area 0
R0(config-router)#^Z
R0#
%SYS-5-CONFIG_I: Configured from console by console

R0#exit
```

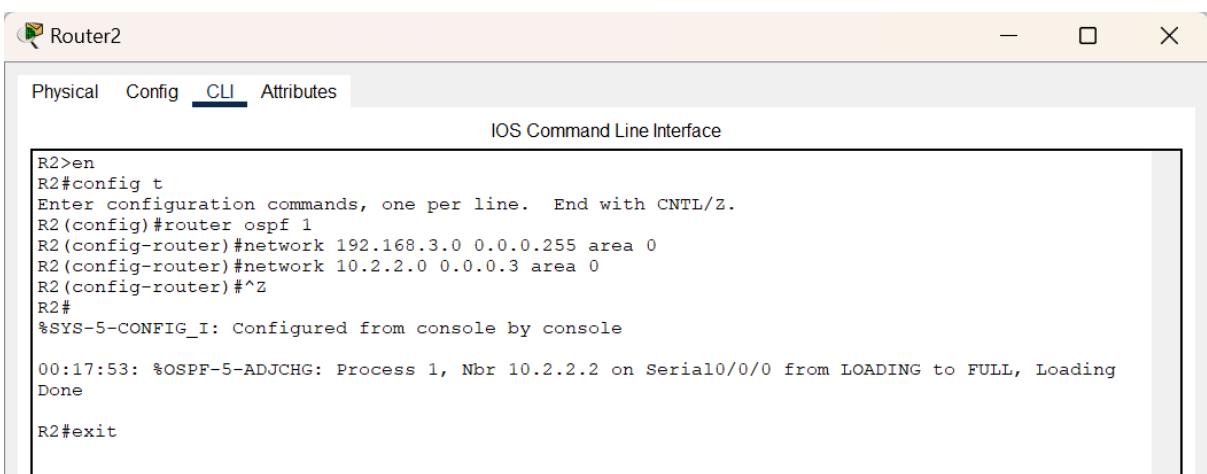
2. Router 1

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#network 10.2.2.0 0.0.0.3 area 0
01:57:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done

R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

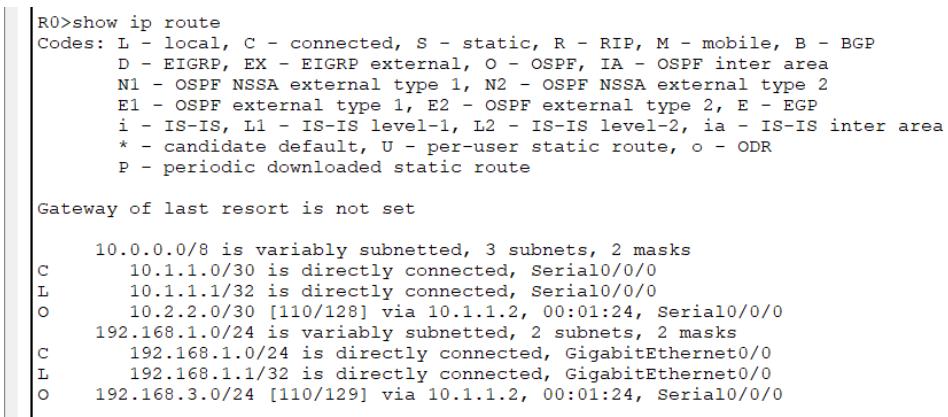
3. Router 2



```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.3.0 0.0.0.255 area 0
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#
R2#
%SYS-5-CONFIG_I: Configured from console by console
00:17:53: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
R2#exit
```

➤ Displaying routing table of routers

1. Router 0



```
R0>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C    10.1.1.0/30 is directly connected, Serial0/0/0
L    10.1.1.1/32 is directly connected, Serial0/0/0
O    10.2.2.0/30 [110/128] via 10.1.1.2, 00:01:24, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.3.0/24 [110/129] via 10.1.1.2, 00:01:24, Serial0/0/0
```

2. Router 1

```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.2/32 is directly connected, Serial0/0/1
O        192.168.1.0/24 [110/65] via 10.1.1.1, 00:02:28, Serial0/0/0
O        192.168.3.0/24 [110/65] via 10.2.2.1, 00:02:28, Serial0/0/1
```

3. Router 2

```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

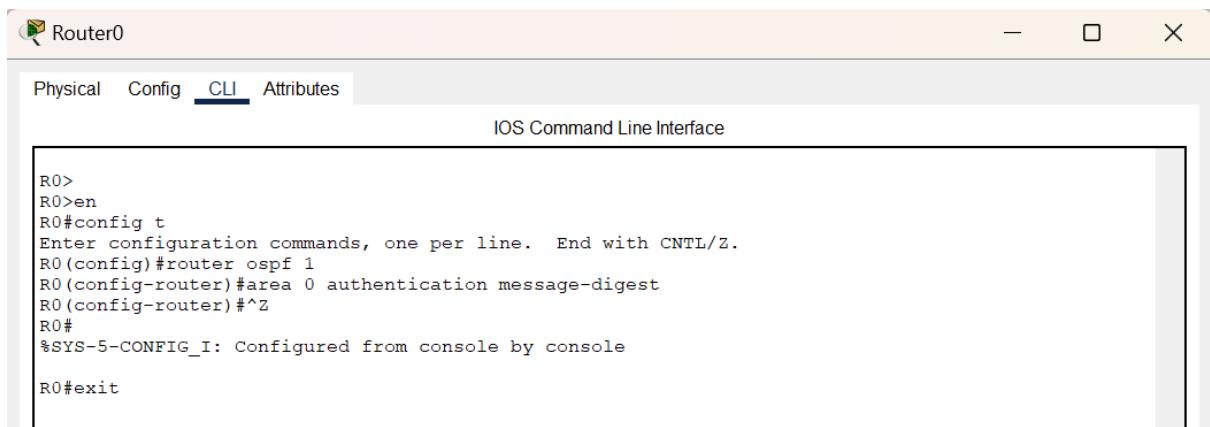
Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O        10.1.1.0/30 [110/128] via 10.2.2.2, 00:02:44, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/0
L        10.2.2.1/32 is directly connected, Serial0/0/0
O        192.168.1.0/24 [110/129] via 10.2.2.2, 00:02:44, Serial0/0/0
          192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

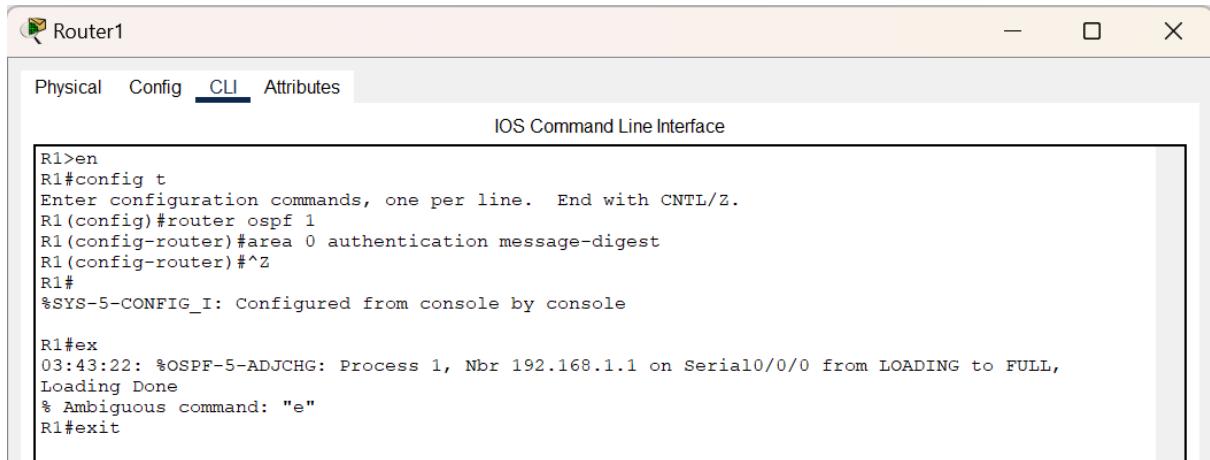
A. OSPF MD5 Authentication

➤ Configure OSPF MD5 authentication on routers

1. Router 0



2. Router 1



Router1

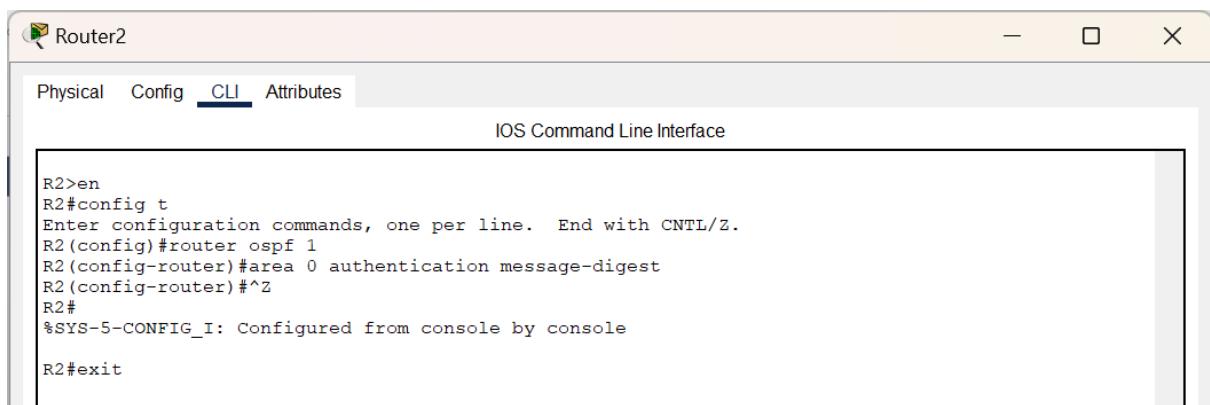
Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
R1(config-router)#+Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#ex
03:43:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done
% Ambiguous command: "e"
R1#exit
```

3. Router 2



Router2

Physical Config **CLI** Attributes

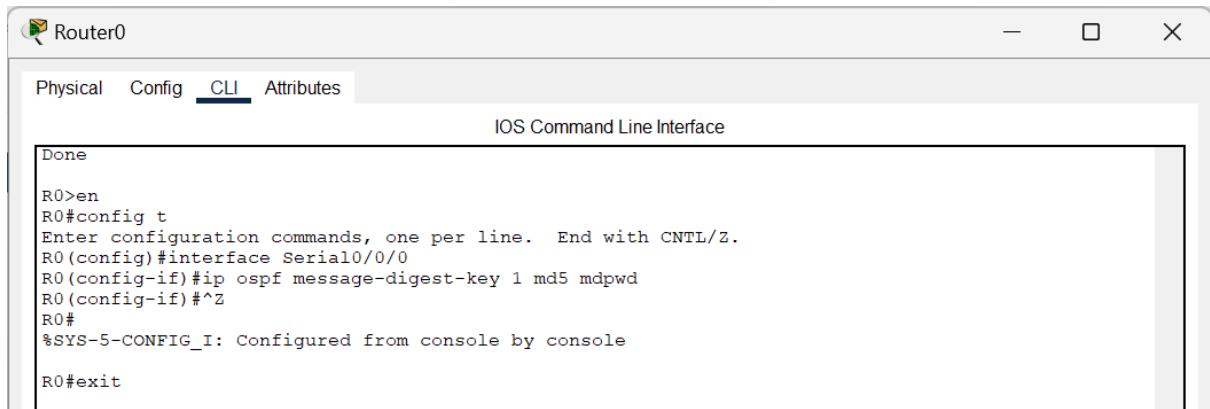
IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
R2(config-router)#+Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

➤ **Configure the MD5 key for all the routers**

1. Router 0



Router0

Physical Config **CLI** Attributes

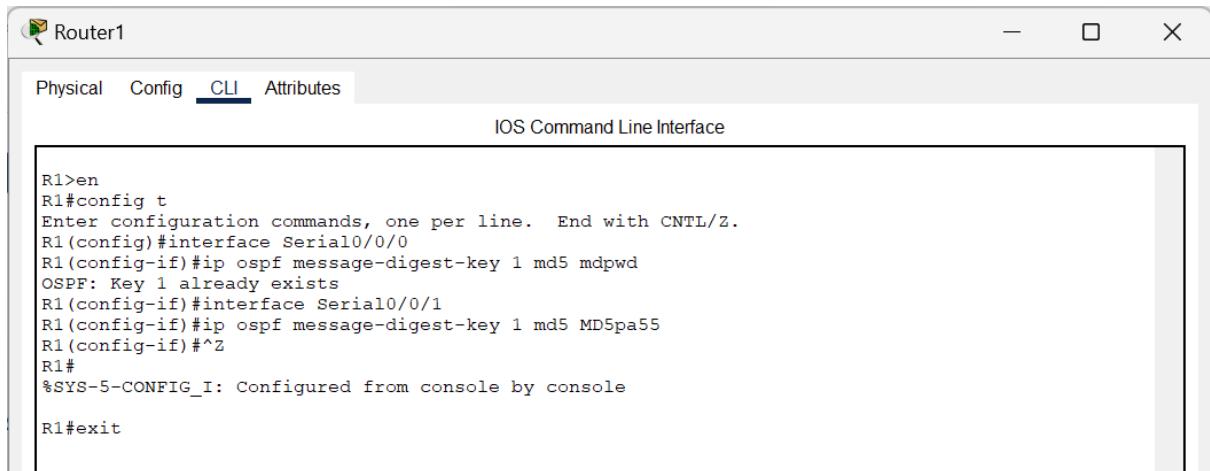
IOS Command Line Interface

```
Done

R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#interface Serial0/0/0
R0(config-if)#ip ospf message-digest-key 1 md5 mdpwd
R0(config-if)#+Z
R0#
%SYS-5-CONFIG_I: Configured from console by console

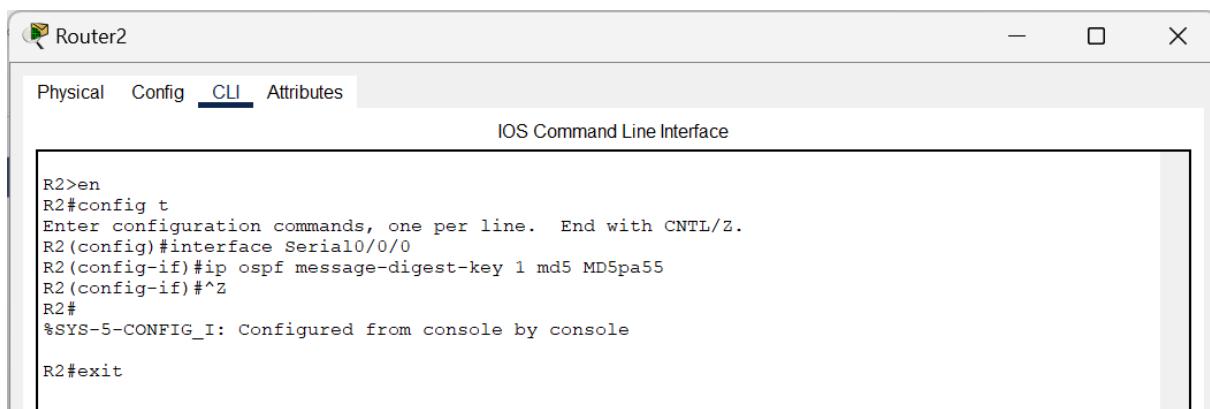
R0#exit
```

2. Router 1



R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Serial0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 mdpwd
OSPF: Key 1 already exists
R1(config-if)#interface Serial0/0/1
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit

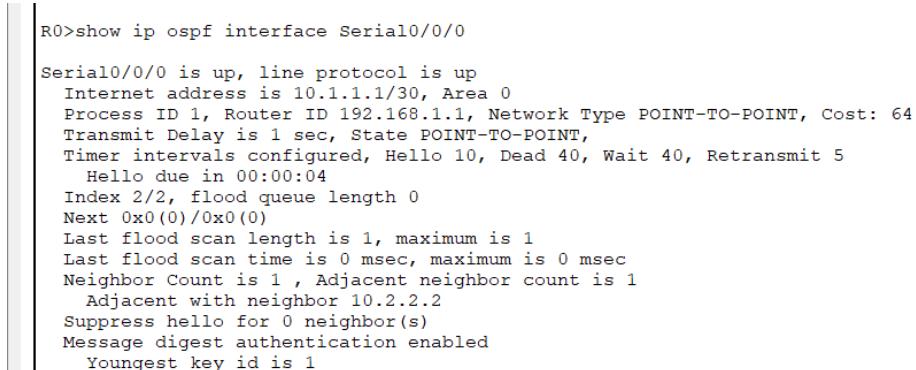
3. Router 2



R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Serial0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit

➤ Displaying OSPF details of all the routers

1. Router 0



```
R0>show ip ospf interface Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

2. Router 1

```
R1>show ip ospf interface Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
R1>show ip ospf interface Serial0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 10.2.2.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.3.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

3. Router 2

```
R2>show ip ospf interface Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.2.2.1/30, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

B. NTP

➤ Check Clock Time in the routers

1. Router 0

```
R0>show clock
*2:36:35.938 UTC Mon Mar 1 1993
```

2. Router 1

```
R1>show clock
*4:11:22.839 UTC Mon Mar 1 1993
```

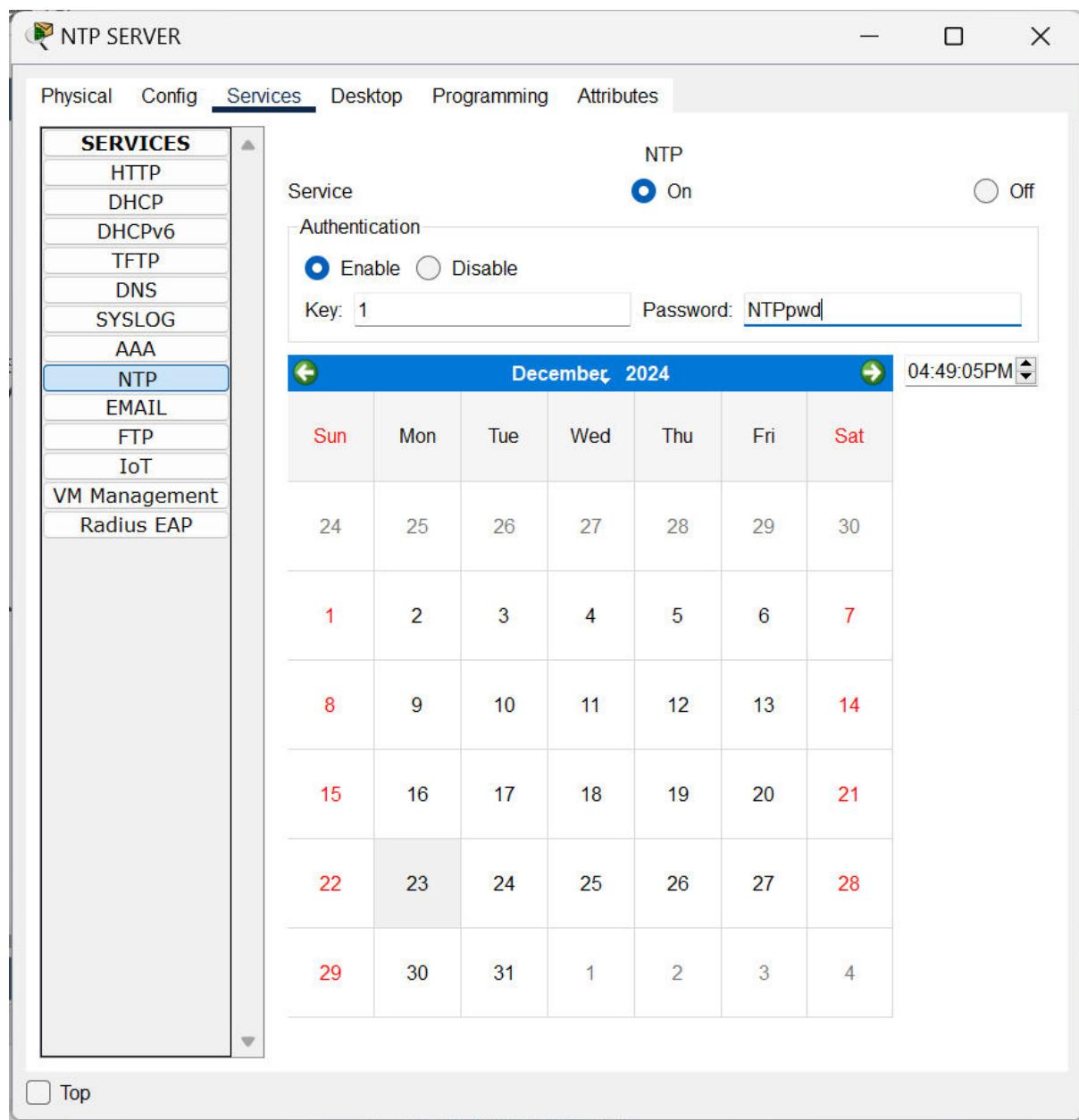
3. Router 2

```
R2>show clock
*0:12:33.21 UTC Mon Mar 1 1993
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 17.12.2024

➤ **Configure NTP Server**



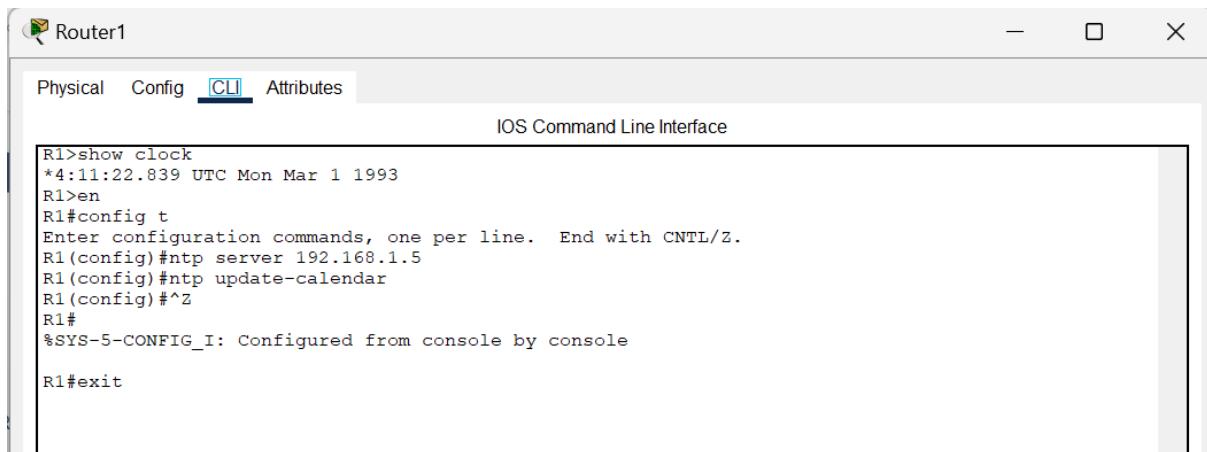
➤ Configure NTP Client

1. Router 0

The screenshot shows the 'Router0' command-line interface (CLI) window. The tab bar indicates the 'CLI' tab is active. Below the tab bar, it says 'IOS Command Line Interface'. The terminal window displays the following configuration commands:

```
R0>show clock
*2:36:35.938 UTC Mon Mar 1 1993
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#ntp server 192.168.1.5
R0(config)#ntp update-calendar
R0(config)#^Z
R0#
%SYS-5-CONFIG_I: Configured from console by console
R0#exit
```

2. Router 1



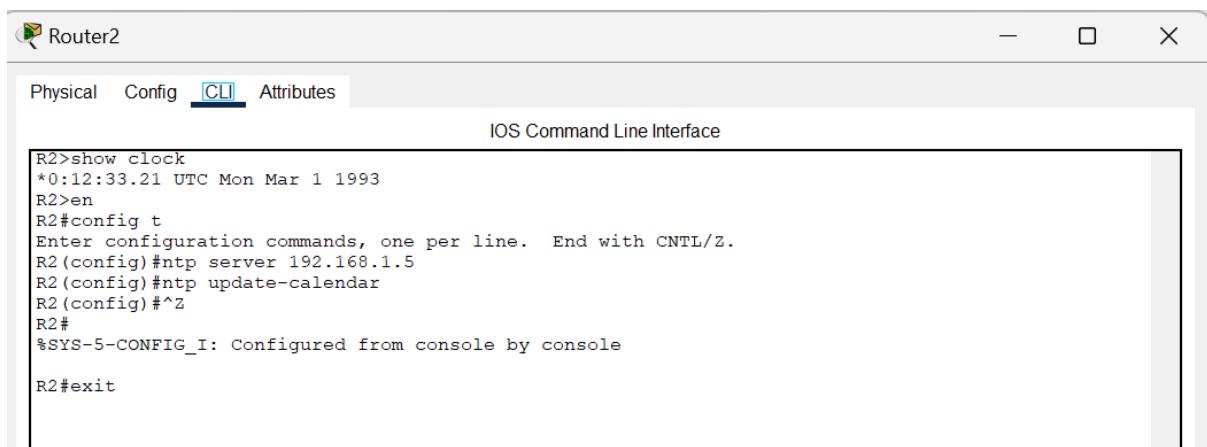
Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>show clock
*4:11:22.839 UTC Mon Mar 1 1993
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
R1(config)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

3. Router 2



Router2

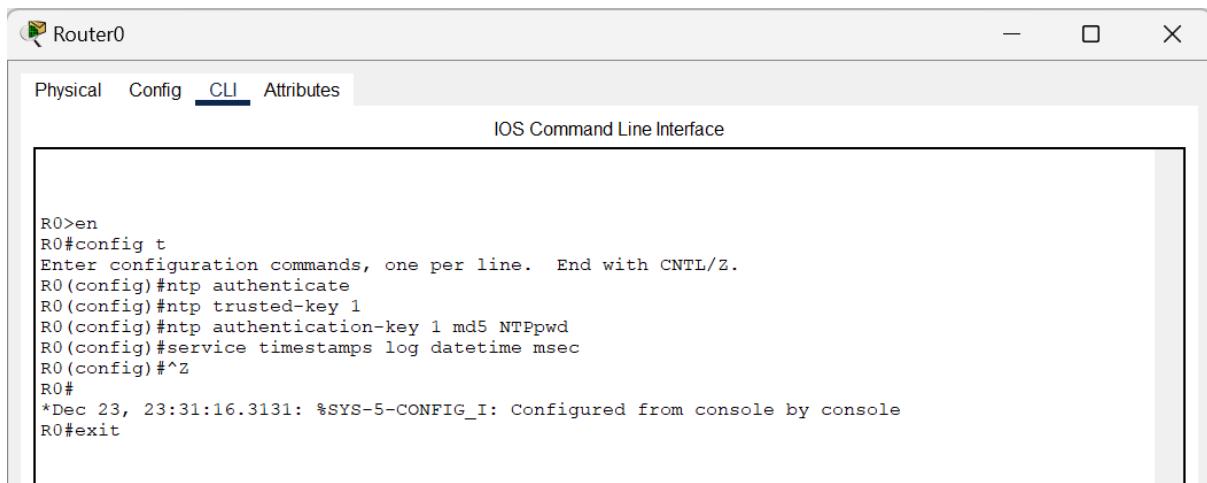
Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>show clock
*0:12:33.21 UTC Mon Mar 1 1993
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#ntp update-calendar
R2(config)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ **Configure NTP authentication and to timestamp log messages on the routers**

1. Router 0



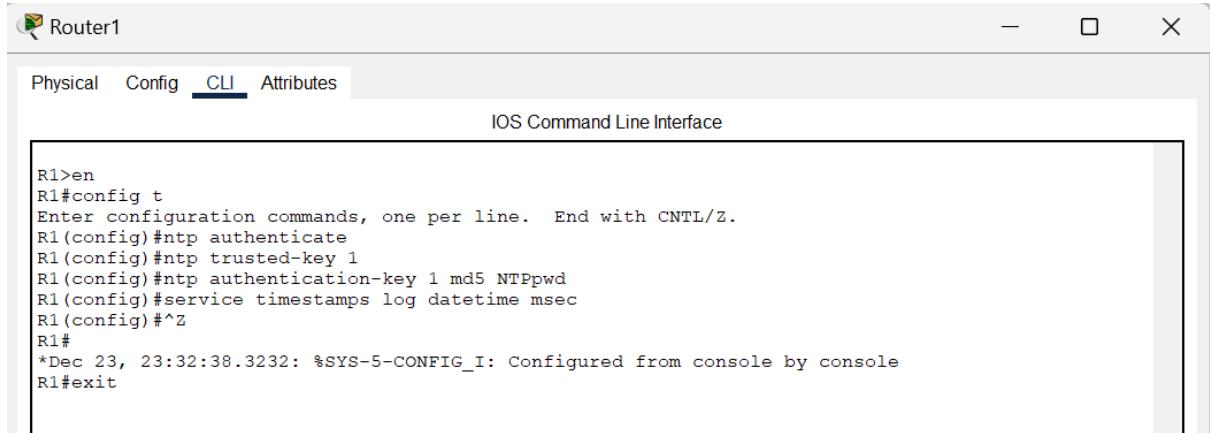
Router0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#ntp authenticate
R0(config)#ntp trusted-key 1
R0(config)#ntp authentication-key 1 md5 NTPpwd
R0(config)#service timestamps log datetime msec
R0(config)#^Z
R0#
*Dec 23, 23:31:16.3131: %SYS-5-CONFIG_I: Configured from console by console
R0#exit
```

2. Router 1



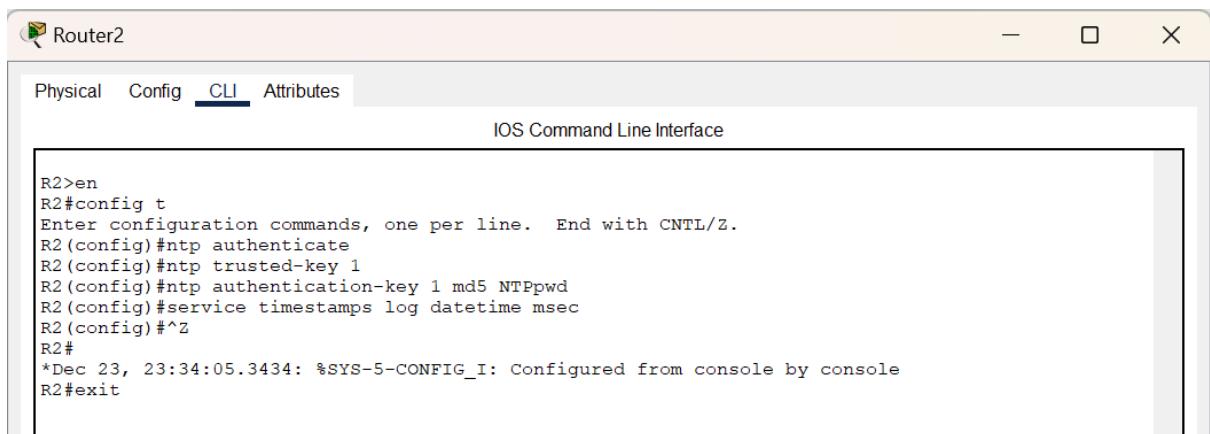
Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp authentication-key 1 md5 NTPpwd
R1(config)#service timestamps log datetime msec
R1(config)#^Z
R1#
*Dec 23, 23:32:38.3232: %SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

3. Router 2



Router2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authentication-key 1 md5 NTPpwd
R2(config)#service timestamps log datetime msec
R2(config)#^Z
R2#
*Dec 23, 23:34:05.3434: %SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ Check updated UTC Clock Time in the routers

1. Router 0

```
R0>show clock
23:34:40.863 UTC Mon Dec 23 2024
```

2. Router 1

```
R1>show clock
23:34:59.541 UTC Mon Dec 23 2024
```

3. Router 2

```
R2>show clock
23:35:18.143 UTC Mon Dec 23 2024
```

C. SYSLOG

➤ Configure routers to log messages to the SYSLOG server

1. Router 0

```
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#logging host 192.168.1.6
R0(config)#^Z
R0#
*Dec 23, 23:37:41.3737: %SYS-5-CONFIG_I: Configured from console by console
*Dec 23, 23:37:41.3737: *Dec 23, 23:37:41.3737: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
R0#exit
```

2. Router 1

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#logging host 192.168.1.6
R1(config)#^Z
R1#
*Dec 23, 23:39:23.3939: %SYS-5-CONFIG_I: Configured from console by console
*Dec 23, 23:39:23.3939: *Dec 23, 23:39:23.3939: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
R1#exit
```

3. Router 2

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#logging host 192.168.1.6
R2(config)#^Z
R2#
*Dec 23, 23:40:03.4040: %SYS-5-CONFIG_I: Configured from console by console
*Dec 23, 23:40:03.4040: *Dec 23, 23:40:03.4040: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host
192.168.1.6 port 514 started - CLI initiated
R2#exit
```

➤ **Verify logging configuration on routers**

1. Router 0

```
R0>show logging
^
% Invalid input detected at '^' marker.

R0>en
R0#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 40 messages logged, xml disabled,
    filtering disabled
Monitor logging: level debugging, 40 messages logged, xml disabled,
    filtering disabled
Buffer logging: disabled, xml disabled,
    filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 40 message lines logged
    Logging to 192.168.1.6 (udp port 514, audit disabled,
        authentication disabled, encryption disabled, link up),
    2 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
```

2. Router 1

```
R1>en
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 89 messages logged, xml disabled,
    filtering disabled
Monitor logging: level debugging, 89 messages logged, xml disabled,
    filtering disabled
Buffer logging: disabled, xml disabled,
    filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 89 message lines logged
    Logging to 192.168.1.6 (udp port 514, audit disabled,
        authentication disabled, encryption disabled, link up),
    2 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
```

3. Router 2

```
R2>en
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 21 messages logged, xml disabled,
    filtering disabled
Monitor logging: level debugging, 21 messages logged, xml disabled,
    filtering disabled
Buffer logging: disabled, xml disabled,
    filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 21 message lines logged
    Logging to 192.168.1.6 (udp port 514, audit disabled,
        authentication disabled, encryption disabled, link up),
    2 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
```

- [Examine logs of the SYSLOG server](#)

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 17.12.2024

SYSLOG SERVER

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG**
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

Syslog

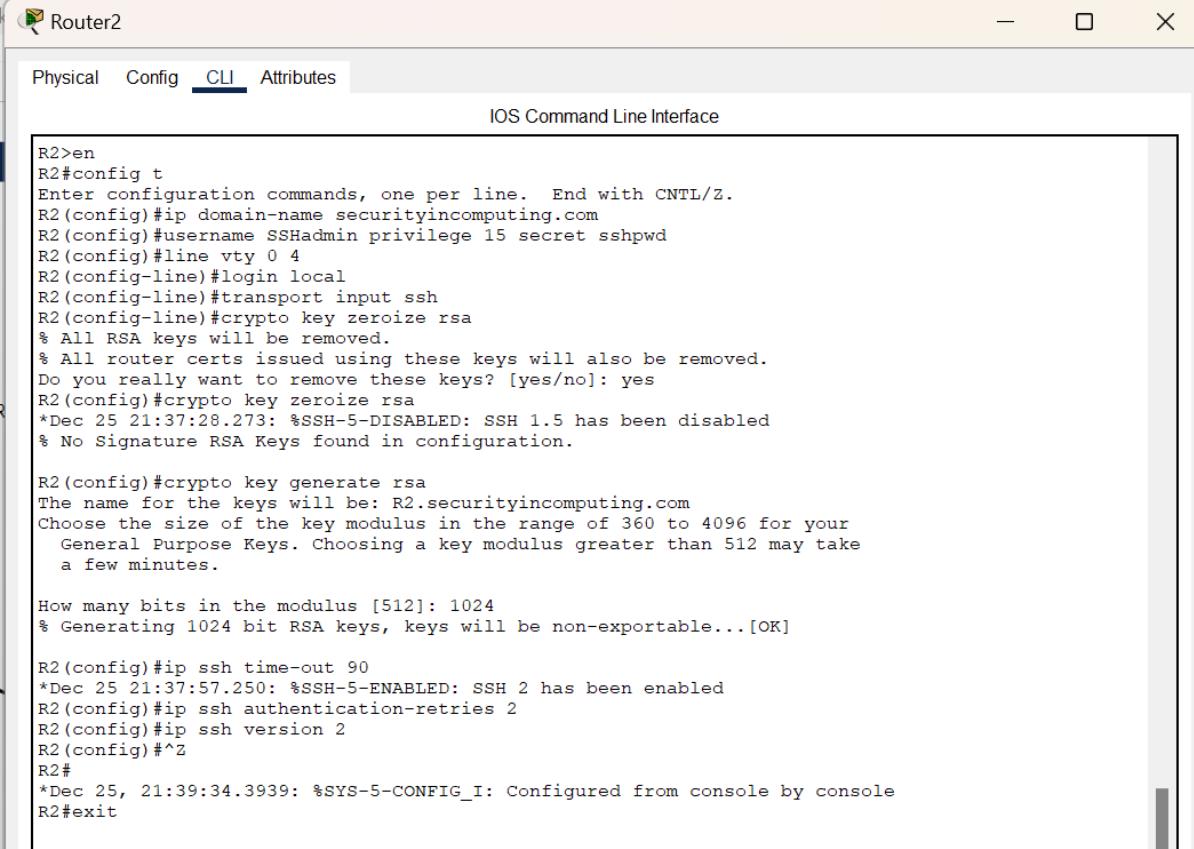
Service

On Off

	Time	HostName	Message
1	12.23.2024 11:39:23.127 PM	10.1.1.2	%SYS-5-CONFIG_I: Configured...
2	12.23.2024 11:39:23.127 PM	10.1.1.2	*Dec 23, 23:39:23.3939: ...
3	12.23.2024 11:40:03.679 PM	10.2.2.1	%SYS-5-CONFIG_I: Configured...
4	12.23.2024 11:40:03.679 PM	10.2.2.1	*Dec 23, 23:40:03.4040: ...

D. SSH

- Configure SSH on R2



The screenshot shows the Cisco IOS Command Line Interface (CLI) for Router2. The window title is "Router2". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area displays the following configuration commands:

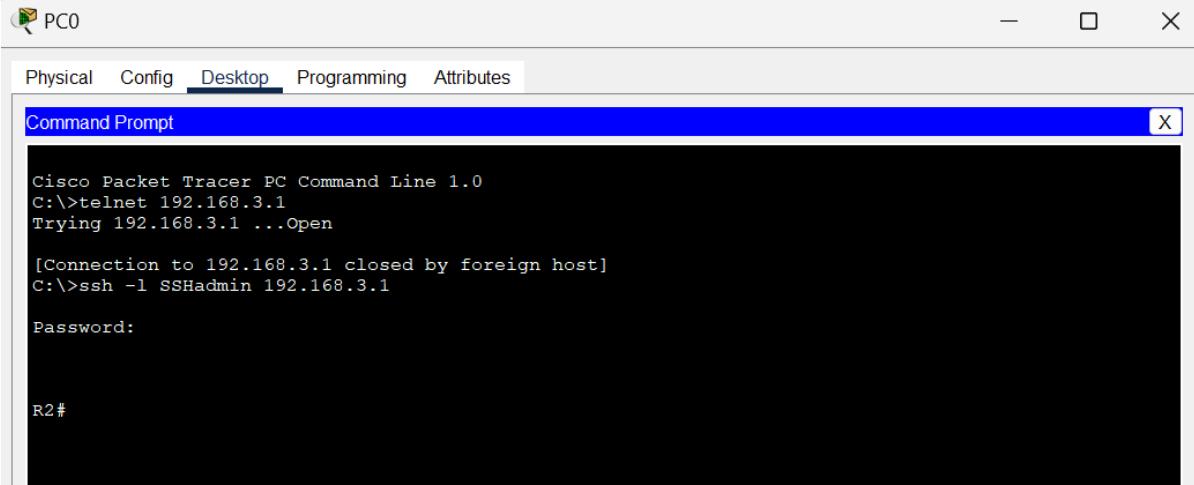
```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip domain-name securityincomputing.com
R2(config)#username SSHadmin privilege 15 secret sshpwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R2(config)#crypto key zeroize rsa
*Dec 25 21:37:28.273: %SSH-5-DISABLED: SSH 1.5 has been disabled
% No Signature RSA Keys found in configuration.

R2(config)#crypto key generate rsa
The name for the keys will be: R2.securityincomputing.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

R2(config)#ip ssh time-out 90
*Dec 25 21:37:57.250: %SSH-5-ENABLED: SSH 2 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
R2(config)#^Z
R2#
*Dec 25, 21:39:34.3939: %SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ Connect to R2 using telnet and SSH on PC



The screenshot shows the Cisco Packet Tracer Command Line interface for PC0. The window title is "PC0". The tabs at the top are "Physical", "Config", "Desktop" (selected), "Programming", and "Attributes". A blue bar labeled "Command Prompt" contains the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open

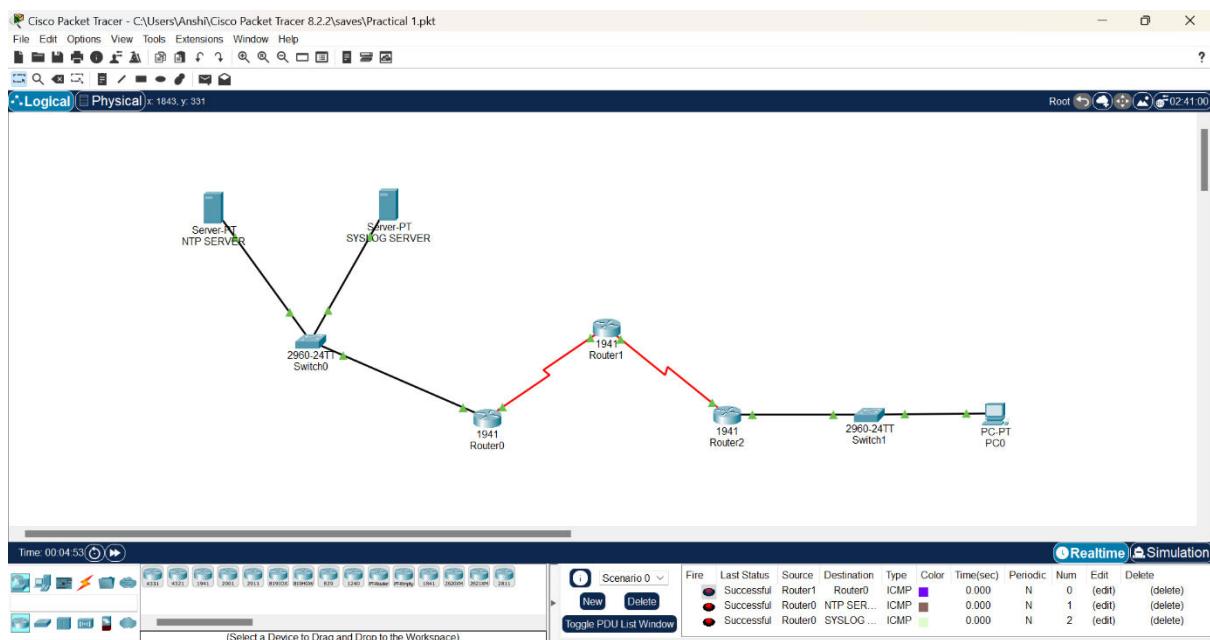
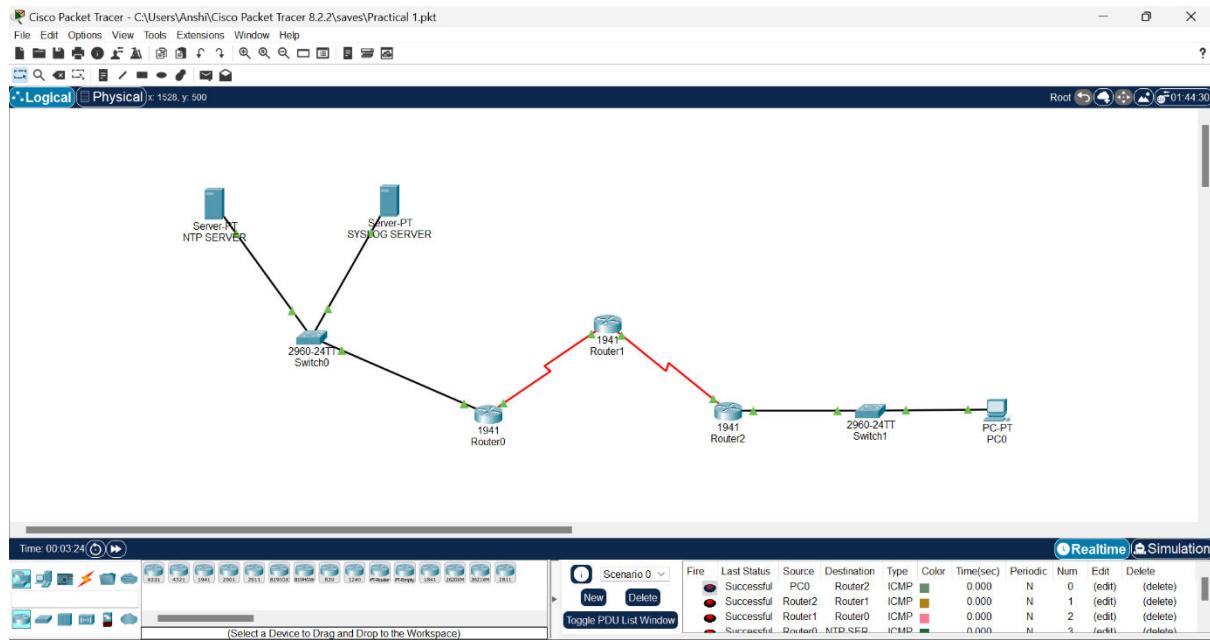
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1

Password:

R2#
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 17.12.2024

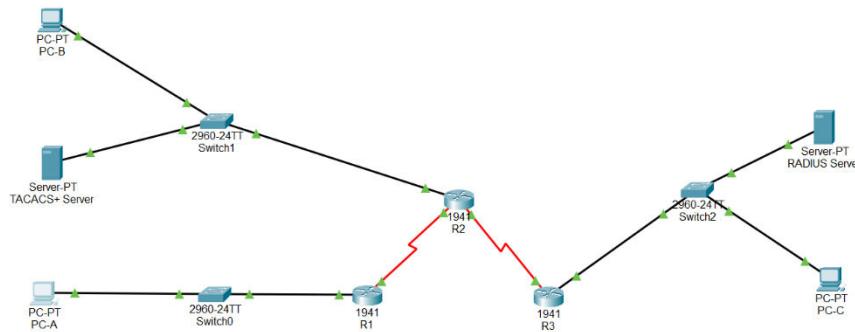


Practical 2

Aim: Configure AAA Authentication

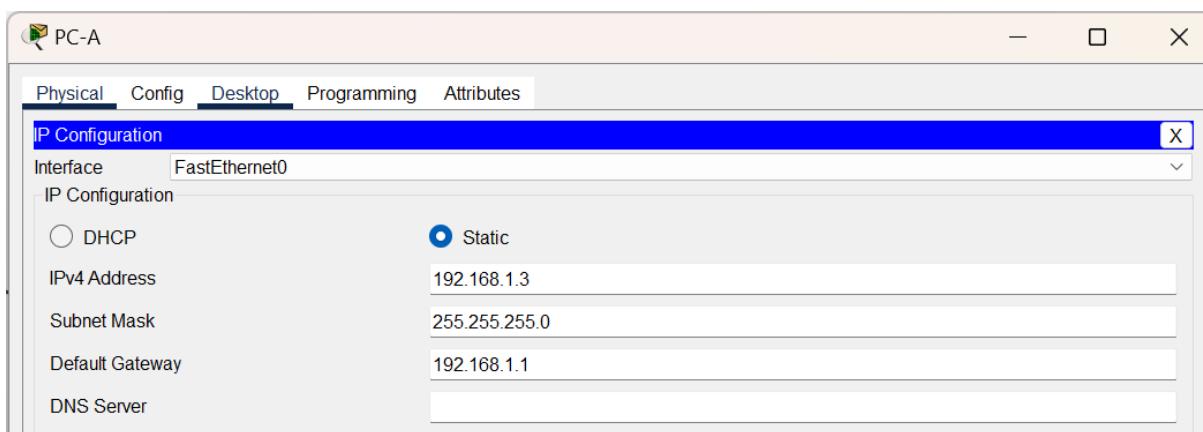
- a. Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA.
- b. Verify local AAA Authentication from the Router console and the PC-A client.

➤ Topology Diagram



➤ Assigning IP Addresses

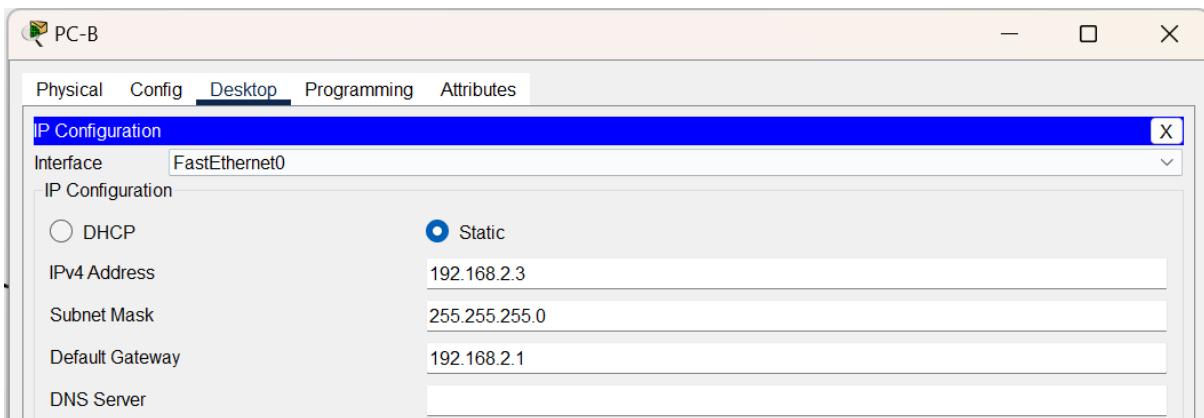
1. PC-A



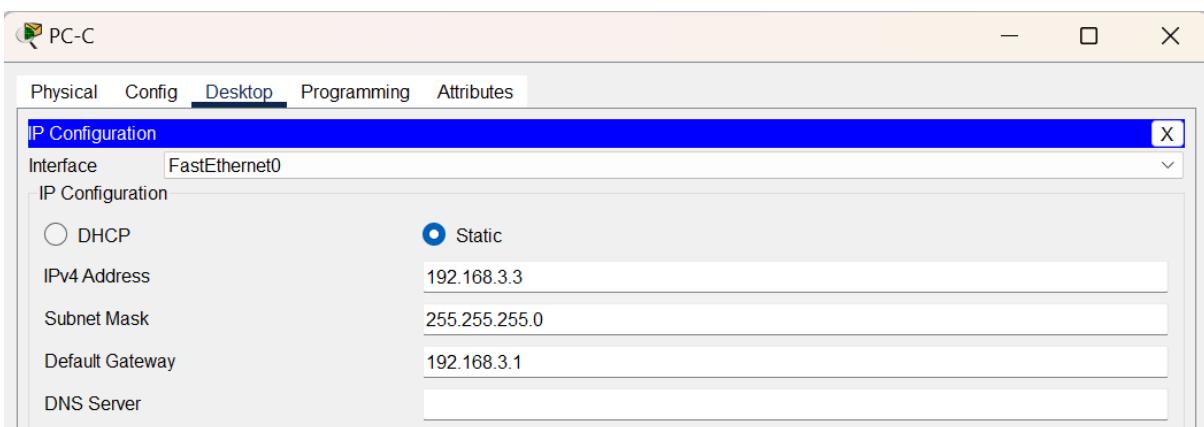
Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 07.01.2025

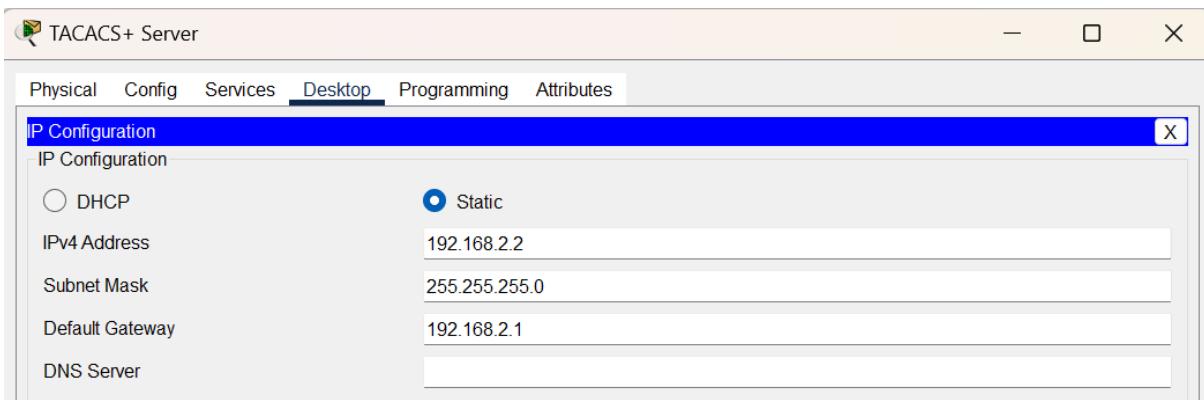
2. PC-B



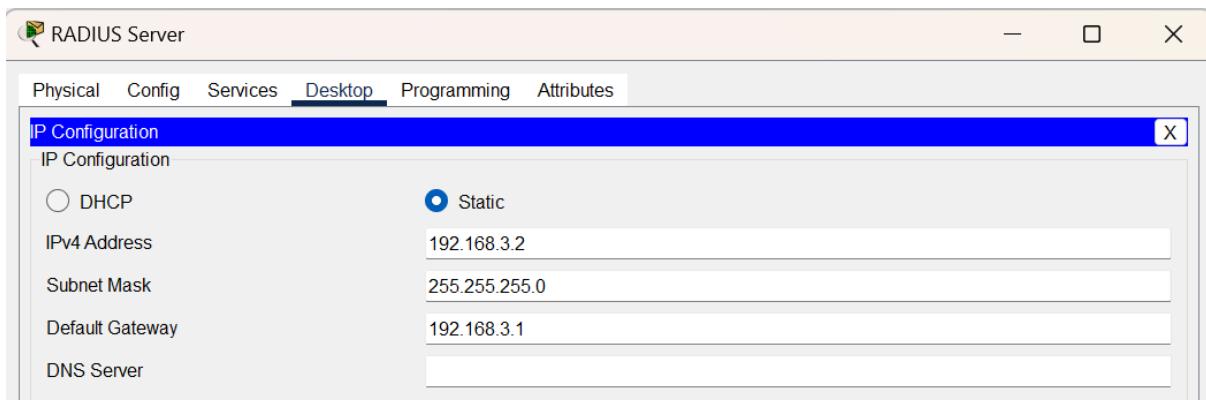
3. PC-C



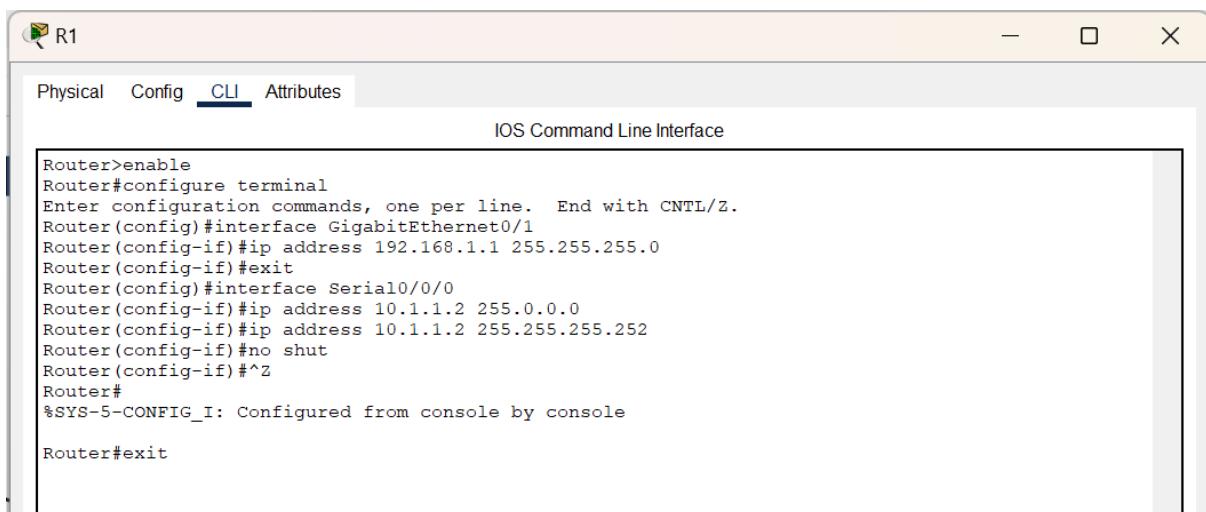
4. TACACS+ Server



5. RADIUS Server



6. R1



7. R2

R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#ip address 10.1.1.1 255.255.255.252
Router(config-if)#exit
Router(config)#interface Serial0/0/1
Router(config-if)#ip address 10.2.2.1 255.255.255.252
Router(config-if)#no shut
Router(config-if)#+Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
```

8. R3

R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 10.2.2.2 255.0.0.0
Router(config-if)#ip address 10.2.2.2 255.255.255.252
Router(config-if)#no shut
Router(config-if)#+Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
```

➤ Displaying IP Address Details of Routers

1. R1

```
R1>show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
GigabitEthernet0/0  unassigned     YES unset  up           up
GigabitEthernet0/1  192.168.1.1   YES manual administratively down down
Serial0/0/0         10.1.1.2      YES manual up            up
Serial0/0/1         unassigned    YES unset  administratively down down
GigabitEthernet0/1/0 unassigned    YES unset  administratively down down
Vlan1              unassigned    YES unset  administratively down down
R1>
```

2. R2

Name: Sahil Kamble

Roll No.: 22093

Class: TYBSc IT

Subject: Information Security

Sem: VI

Date: 07.01.2025

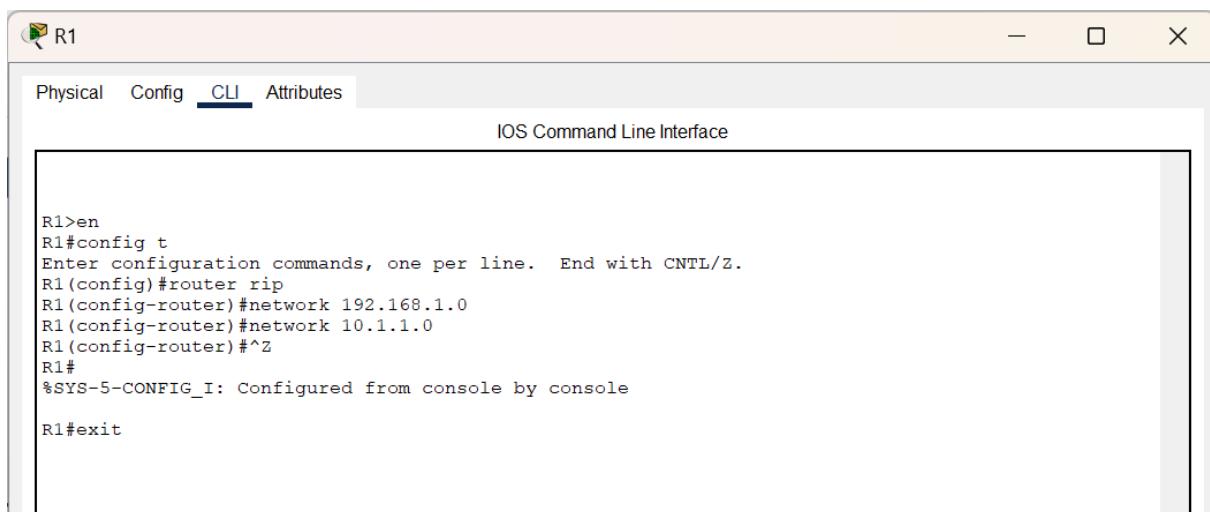
```
R2>show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
GigabitEthernet0/0  192.168.2.1    YES manual up        up
GigabitEthernet0/1  unassigned     YES unset administratively down down
Serial0/0/0         10.1.1.1      YES manual up        up
Serial0/0/1         10.2.2.1      YES manual up        up
GigabitEthernet0/1/0 unassigned     YES unset administratively down down
Vlan1              unassigned     YES unset administratively down down
R2>
```

3. R3

```
R3>show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
GigabitEthernet0/0  192.168.3.1    YES manual up        up
GigabitEthernet0/1  unassigned     YES unset administratively down down
Serial0/0/0         10.2.2.2      YES manual up        up
Serial0/0/1         unassigned     YES unset administratively down down
GigabitEthernet0/1/0 unassigned     YES unset administratively down down
Vlan1              unassigned     YES unset administratively down down
R3>
```

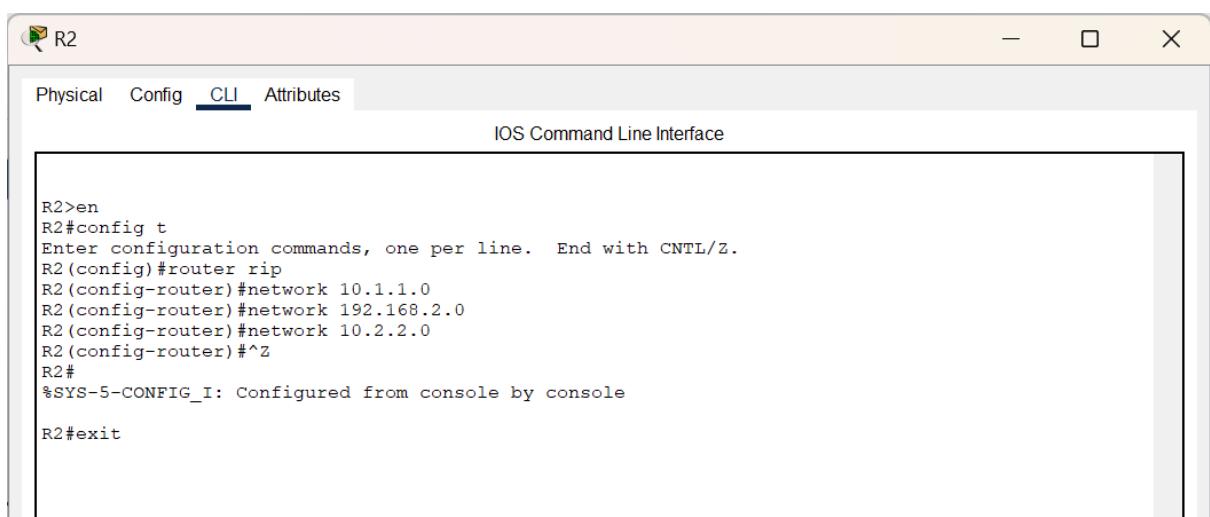
➤ **Configure RIP on routers**

1. R1



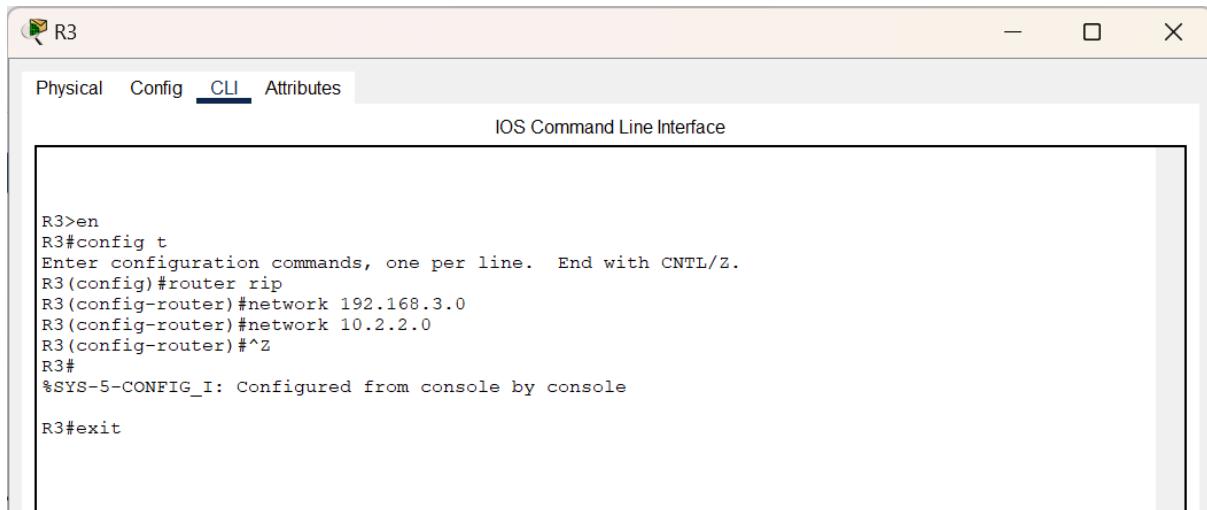
```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

2. R2



```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 10.2.2.0
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

3. R3



The screenshot shows a window titled "R3" with a tab bar containing "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tab bar, it says "IOS Command Line Interface". The main area of the window displays the following CLI session:

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 192.168.3.0
R3(config-router)#network 10.2.2.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ Displaying routing table of routers

1. R1

```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.1, 00:00:16, Serial0/0/0
R        192.168.2.0/24 [120/1] via 10.1.1.1, 00:00:16, Serial0/0/0
R        192.168.3.0/24 [120/2] via 10.1.1.1, 00:00:16, Serial0/0/0

R1>
```

2. R2

```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0
R        192.168.3.0/24 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1

R2>
```

3. R3

```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        10.1.1.0/30 [120/1] via 10.2.2.1, 00:00:06, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/0
L        10.2.2.2/32 is directly connected, Serial0/0/0
R        192.168.2.0/24 [120/1] via 10.2.2.1, 00:00:06, Serial0/0/0
  192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0

R3>
```

➤ Configure Local AAA Authentication for Console Line on R1

The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a device named R1. The window title is "R1". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main pane displays the following configuration commands:

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/z.
R1(config)#username aaaAdmin secret aaapwd
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

Below the main pane, a separate window titled "User Access Verification" shows the authentication process:

```
User Access Verification
Username: aaaAdmin
Password:
R1>
```

➤ Configure Local AAA Authentication for vty Lines on R1

The screenshot shows the Cisco IOS Command Line Interface (CLI) running on a device named R1. The window title is "R1". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main pane displays the following configuration commands:

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/z.
R1(config)#ip domain-name sic.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.sic.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

R1(config)#aaa authentication login SSH-LOGIN local
*Mar 1 1:39:41.682: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input ssh
R1(config-line)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

PC-A

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l aaaAdmin 192.168.1.1
Password:
R1>exit
[Connection to 192.168.1.1 closed by foreign host]
C:\>
```

➤ Configure Server-Based AAA Authentication Using TACACS+ on R2

AAA

Service	On / Off	Radius Port
AAA	On	1645

Network Configuration

Client Name	Client IP	ServerType	Radius
R2	192.168.2.1	Tacacs	tacacspwd

User Setup

Username	Password
admin2	pwd2

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 07.01.2025

The screenshot shows a Windows application window titled "R2". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs, it says "IOS Command Line Interface". The main text area contains the following configuration commands:

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username admin2 secret pwd2
R2(config)#tacacs-server host 192.168.2.2
R2(config)#tacacs-server key tacacspwd
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#line console 0
R2(config-line)#login authentication default
R2(config-line)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

Below this, there is a separate text box containing a "User Access Verification" prompt:

```
User Access Verification
Username: admin2
Password:
R1>
```

➤ Configure Server-Based AAA Authentication Using RADIUS on R3

RADIUS Server

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA**
- NTP
- EMAIL
- FTP
- IoT

VM Management

- Radius EAP

AAA

Service On Off Radius Port 1645

Network Configuration

Client Name	Client IP	Server Type	Key
1 R3	192.168.3.1	Radius	radiuspwd

Add Save Remove

User Setup

Username Password

Username	Password
1 admin3	pwd3

Add Save Remove

Top

R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username admin3 secret pwd3
R3(config)#radius-server host 192.168.3.2
R3(config)#radius-server key radiuspwd
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#{^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

Name: Sahil Kamble

Roll No.: 22093

Class: TYBSc IT

Subject: Information Security

Sem: VI

Date: 07.01.2025

User Access Verification

Username: admin3

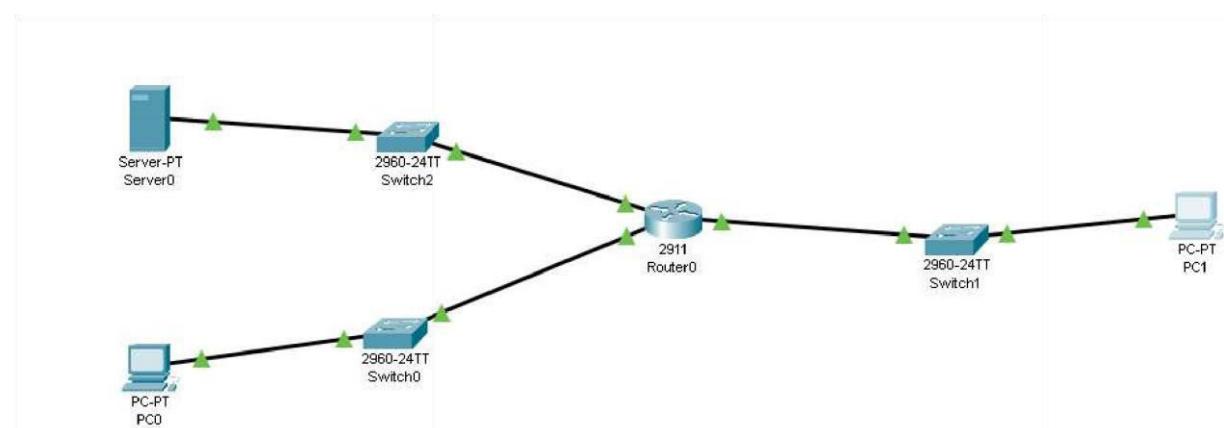
Password:

R3>

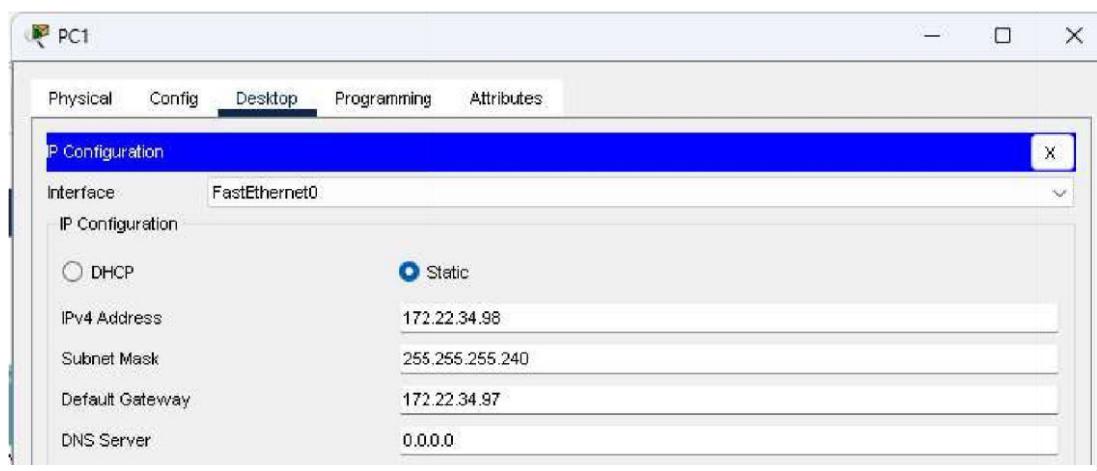
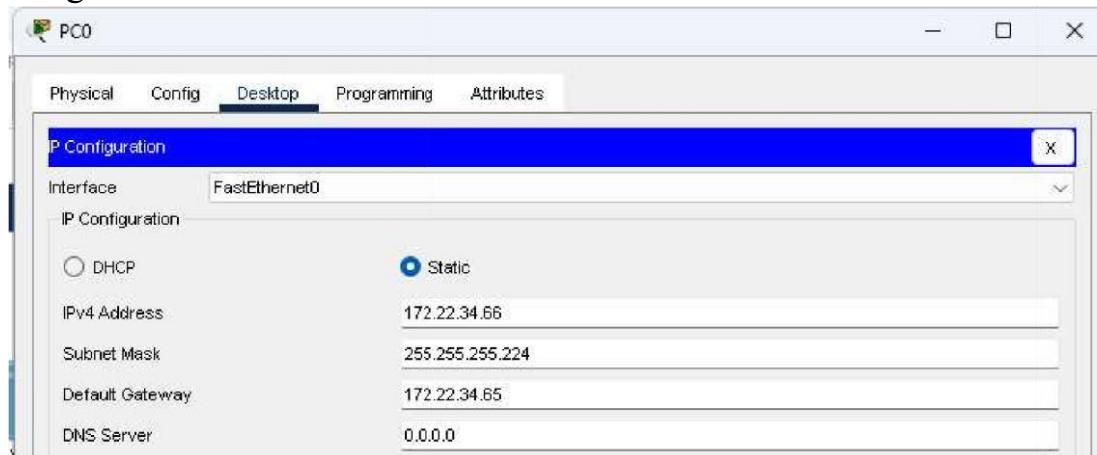
Practical 3:

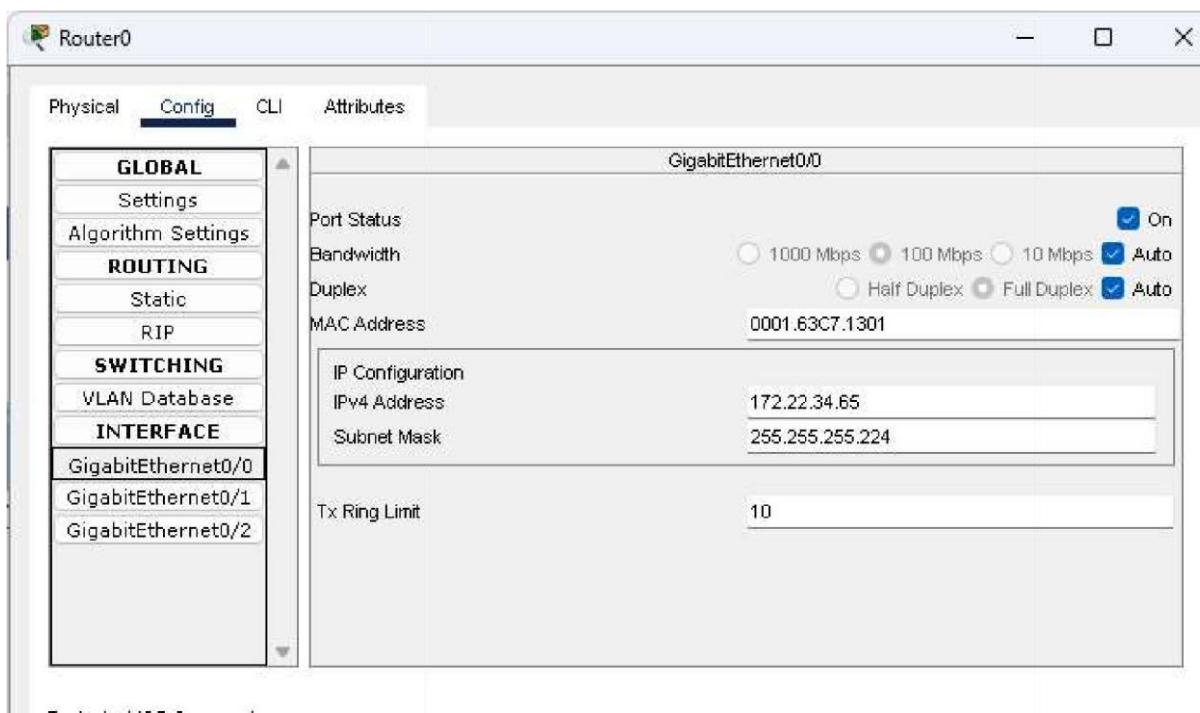
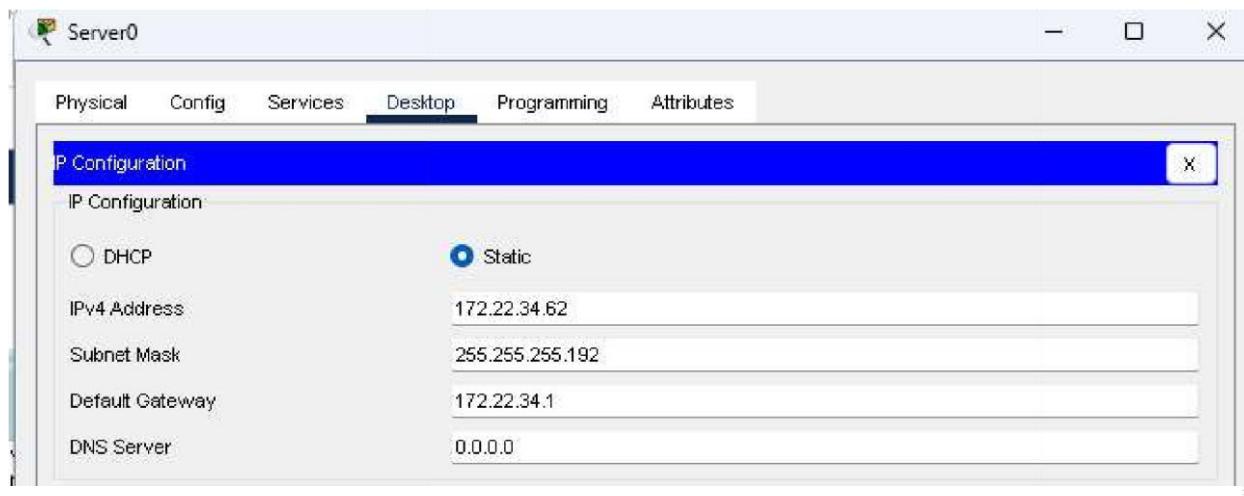
Aim: Configure extended ACLs.

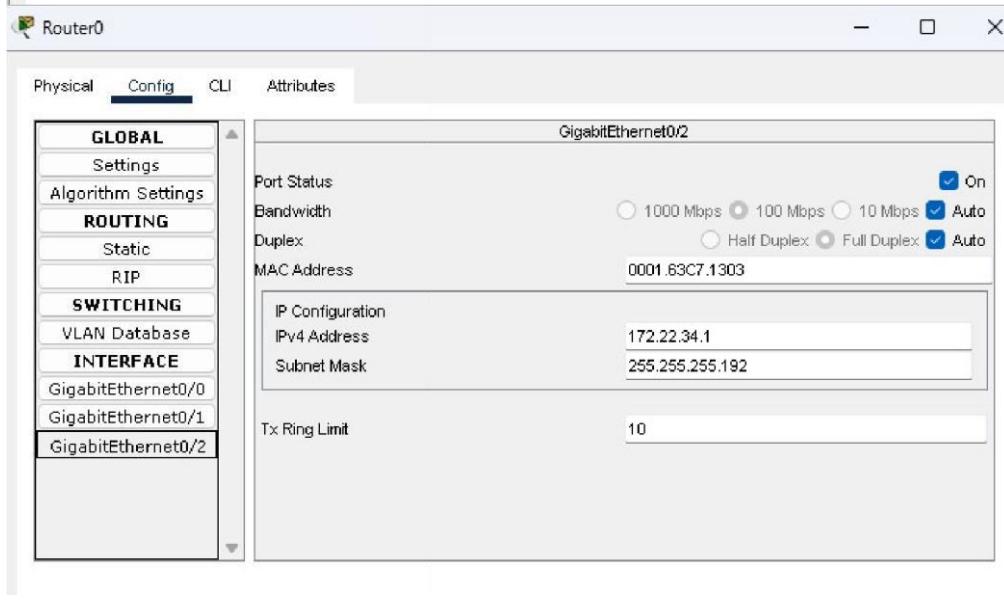
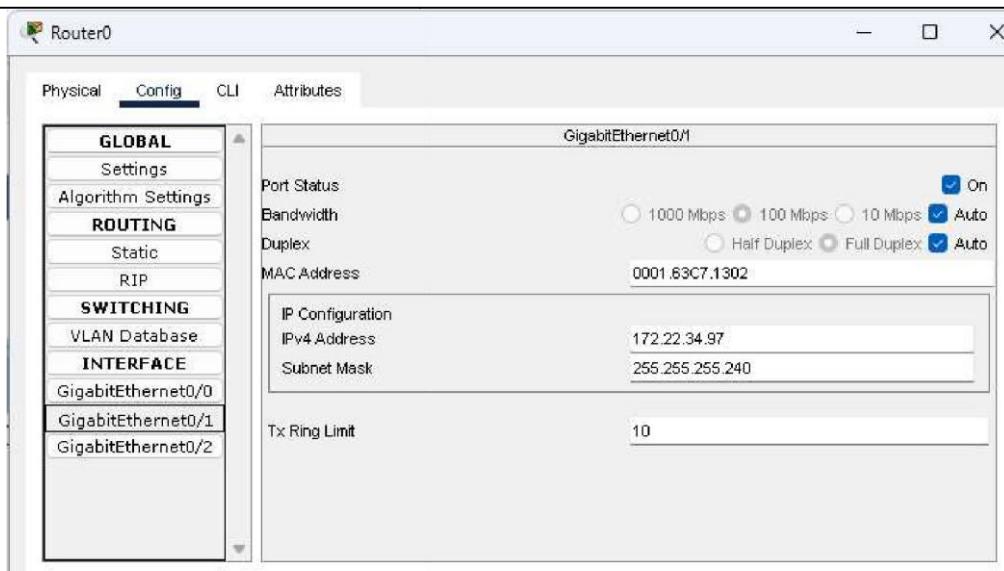
Topology:



Assign IP address:





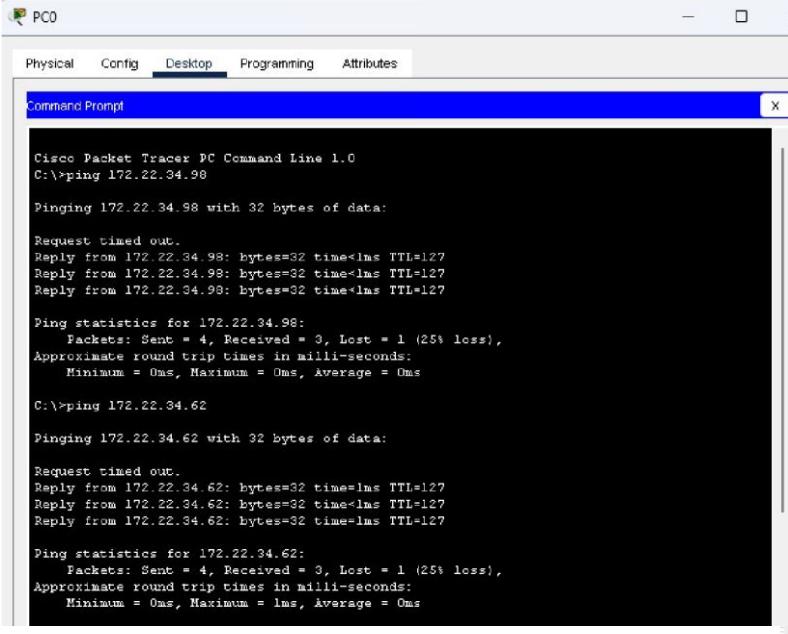


Displaying IP address details of R1

The screenshot shows the IOS Command Line Interface for Router0. The command entered was 'Router#show ip interface brief'. The output displays the following table:

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	172.22.34.65	YES	manual	up	up
GigabitEthernet0/1	172.22.34.97	YES	manual	up	up
GigabitEthernet0/2	172.22.34.1	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

Performing ping from PC-0 to server and PC 1



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.98

Pinging 172.22.34.98 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127
Reply from 172.22.34.98: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

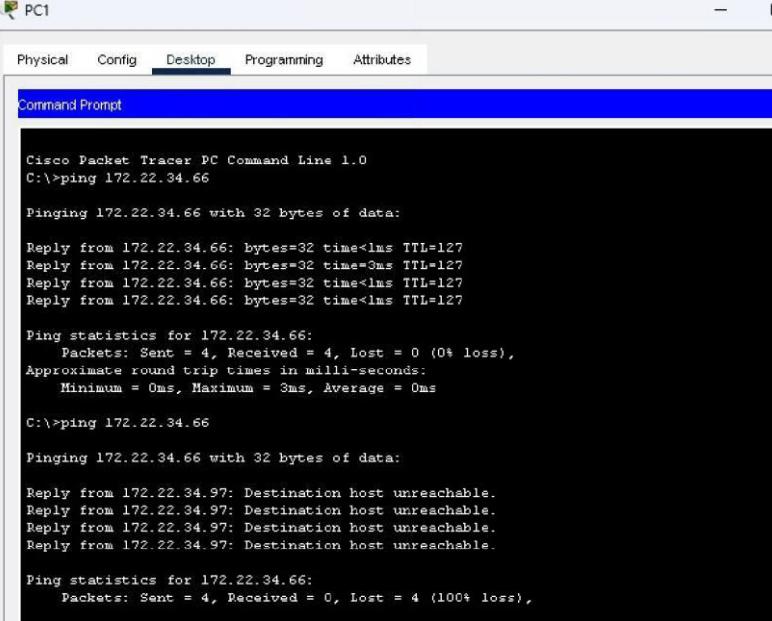
C:\>ping 172.22.34.62

Pinging 172.22.34.62 with 32 bytes of data:

Request timed out.
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Performing ping from PC-1 to server and PC 0



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127
Reply from 172.22.34.66: bytes=32 time=0ms TTL=127
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127

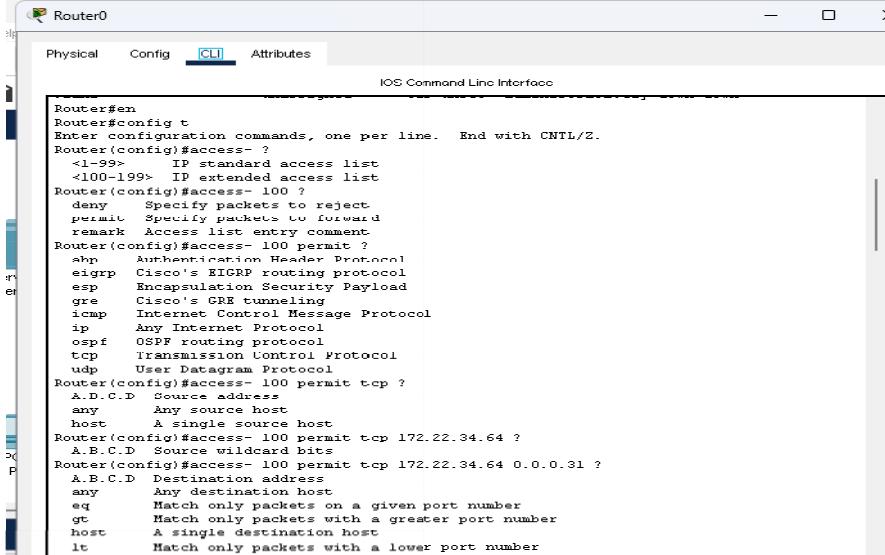
Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.22.34.66

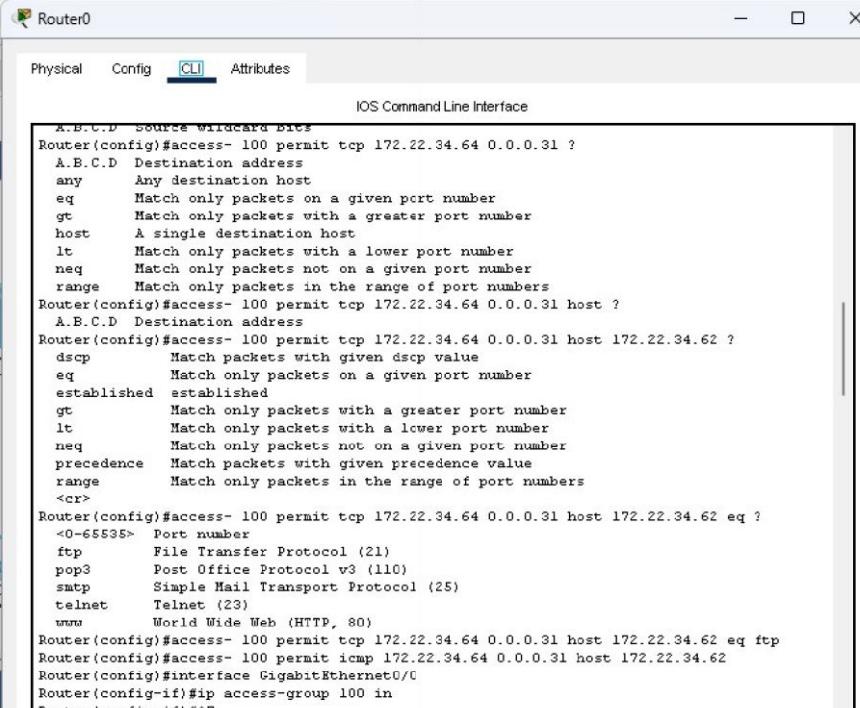
Pinging 172.22.34.66 with 32 bytes of data:
Reply from 172.22.34.97: Destination host unreachable.

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Configure, Apply and verify an extended numbered ACL (PC-0 needs only FTP access and should be able to ping the server, but not PC-1)



Router#en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access- ?
<1-99> IP standard access list
<100-199> IP extended access list
Router(config)#access- 100 ?
deny Specify packets to reject
permit Specify packets to forward
remark Access list entry comment
Router(config)#access- 100 permit ?
ah Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
Router(config)#access- 100 permit tcp ?
A.B.C.D Source address
any Any source host
host A single source host
Router(config)#access- 100 permit tcp 172.22.34.64 ?
A.B.C.D Source standard mask
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host ?
A.B.C.D Destination address
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
dscp Match packets with given dscp value
eq Match only packets on a given port number
established established
gt Match only packets with a greater port number
lt Match only packets with a lower port number
neq Match only packets not on a given port number
precedence Match packets with given precedence value
range Match only packets in the range of port numbers
<cr>
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
<0-65535> Port number
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
Router(config)#access- 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#^Z



A.B.C.D source wildcard bits:
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host ?
A.B.C.D Destination address
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?
dscp Match packets with given dscp value
eq Match only packets on a given port number
established established
gt Match only packets with a greater port number
lt Match only packets with a lower port number
neq Match only packets not on a given port number
precedence Match packets with given precedence value
range Match only packets in the range of port numbers
<cr>
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?
<0-65535> Port number
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)
Router(config)#access- 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp
Router(config)#access- 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#^Z

Performing ping from PC-0 to Server and PC-1 to check the working of ACL

```
Request timed out.  
Reply from 172.22.34.62: bytes=32 time=1ms TTL=127  
Reply from 172.22.34.62: bytes=32 time<1ms TTL=127  
Reply from 172.22.34.62: bytes=32 time=1ms TTL=127  
Ping statistics for 172.22.34.62:  
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 1ms, Average = 0ms  
  
C:\>ftp 172.22.34.62  
Trying to connect... 172.22.34.62  
Connected to 172.22.34.62  
220- Welcome to PT Ftp server  
Username:cisco  
331- Username ok, need password  
Password:  
230- Logged in  
(passive mode On)  
ftp>quit  
  
221- Service closing control connection.  
C:\>ping 172.22.34.98  
  
Pinging 172.22.34.98 with 32 bytes of data:  
  
Reply from 172.22.34.98: Destination host unreachable.  
  
Ping statistics for 172.22.34.98:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\>
```

Configure, Apply and verify an extended numbered ACL (PC-1 needs only FTP access and should be able to ping the server, but not PC-0)

```
Router#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#ip access-list ?  
  extended Extended Access List  
  standard Standard Access List  
Router(config)#ip access-list extended ?  
  <100-199> Extended IP access-list number  
  WORD      name  
Router(config)#ip access-list extended HTTP_ACL  
Router(config-ext-nacl)#  
* Unknown command or computer name, or unable to find computer address  
  
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?  
  A.B.C.D Destination address  
  any      Any destination host  
  eq       Match only packets on a given port number  
  gt       Match only packets with a greater port number  
  host     A single destination host  
  lt       Match only packets with a lower port number  
  neq     Match only packets not on a given port number  
  range   Match only packets in the range of port numbers  
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?  
  A.B.C.D Destination address  
  any      Any destination host  
  eq       Match only packets on a given port number  
  gt       Match only packets with a greater port number  
  host     A single destination host  
  lt       Match only packets with a lower port number  
  neq     Match only packets not on a given port number  
  range   Match only packets in the range of port numbers  
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host ?  
  A.B.C.D Destination address  
  Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 ?  
    eq      Match only packets on a given port number
```

The screenshot shows a Windows application window titled "Router0" with the tab "CLI" selected. The main area displays the IOS Command Line Interface (CLI) configuration for an ACL. The commands shown include permit rules for TCP port 172.22.34.96, ICMP, and HTTP, along with interface and access-group configurations. The configuration ends with the message "#SYS-5-CONFIG_I: Configured from console by console".

```
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 ?
A.B.C.D Destination address
any Any destination host
eq Match only packets on a given port number
gt Match only packets with a greater port number
host A single destination host
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host ?
A.B.C.D Destination address
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 ?
eq Match only packets on a given port number
established established
gt Match only packets with a greater port number
lt Match only packets with a lower port number
neq Match only packets not on a given port number
range Match only packets in the range of port numbers
<cr>
Router(config-ext-nacl)#permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq ?
<0-65535> Port number
domain Domain Name Service (DNS, 53)
ftp File Transfer Protocol (21)
pop3 Post Office Protocol v3 (110)
smtp Simple Mail Transport Protocol (25)
telnet Telnet (23)
www World Wide Web (HTTP, 80)
Router(config-ext-nacl)#permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
Router(config-ext-nacl)#interface GigabitEthernet0/1
Router(config-if)#ip access-group HTTP_ACL in
Router(config-if)#^Z
Router#
#SYS-5-CONFIG_I: Configured from console by console
```

Performing ping from PC-1 to Server and PC-0 to check the working of ACL.

The screenshot shows a Windows application window titled "PC1" with the tab "Desktop" selected. A "Command Prompt" window is open, displaying the results of a ping test to 172.22.34.66 and an attempt to connect via FTP to 172.22.34.62. The output shows that the ping test was successful, while the FTP connection attempt failed due to a timeout.

```
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127
Reply from 172.22.34.66: bytes=32 time=2ms TTL=127
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127
Reply from 172.22.34.66: bytes=32 time<1ms TTL=127

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>ping 172.22.34.66

Pinging 172.22.34.66 with 32 bytes of data:
Reply from 172.22.34.97: Destination host unreachable.

Ping statistics for 172.22.34.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp 172.22.34.62
Trying to connect...172.22.34.62
*Error opening ftp://172.22.34.62/ (Timed out)

.

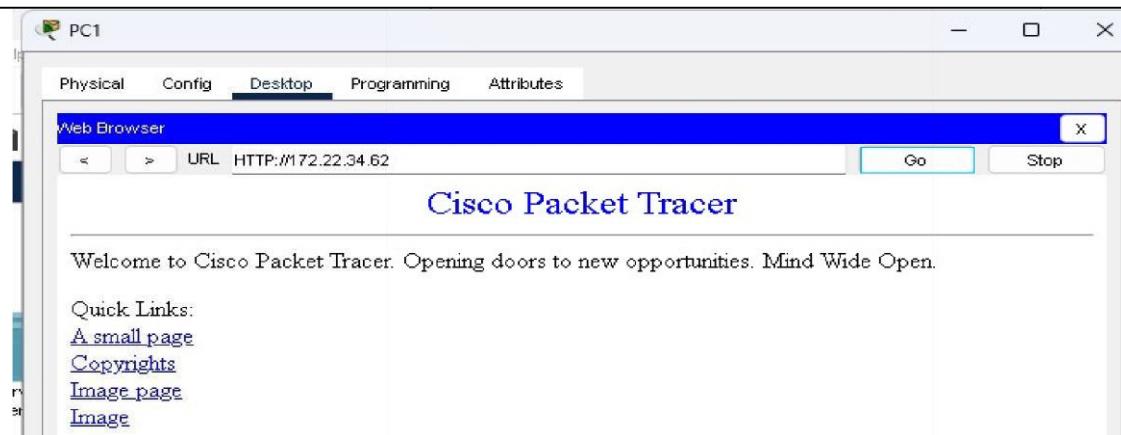
(Disconnecting from ftp server)

S
```

Checking http connection from pc-1

Name - Sahil Kamble
Sub- Information security
Sem- VI

Date- 14/01/25
Class- TYBSC-IT
Roll.No- IT-22093

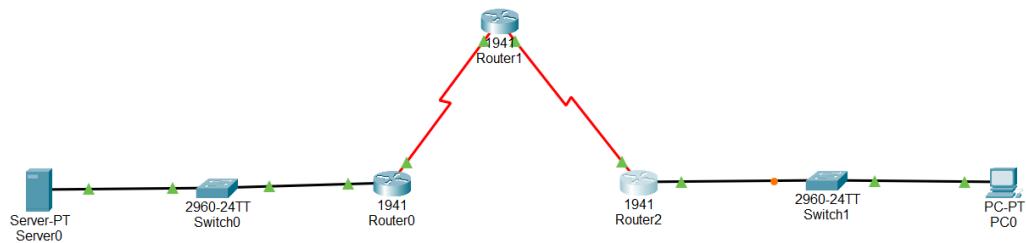


Practical 4

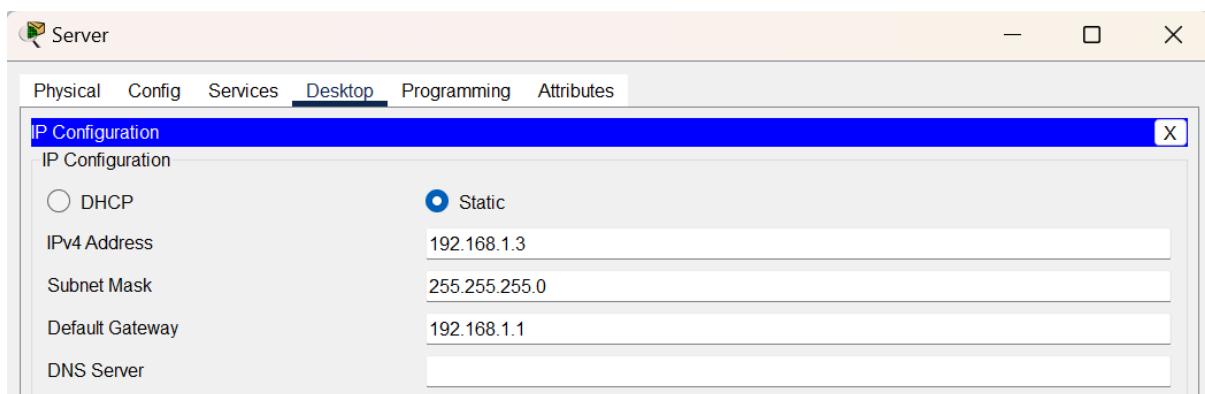
Aim: Configure IP ACLs to Mitigate Attacks

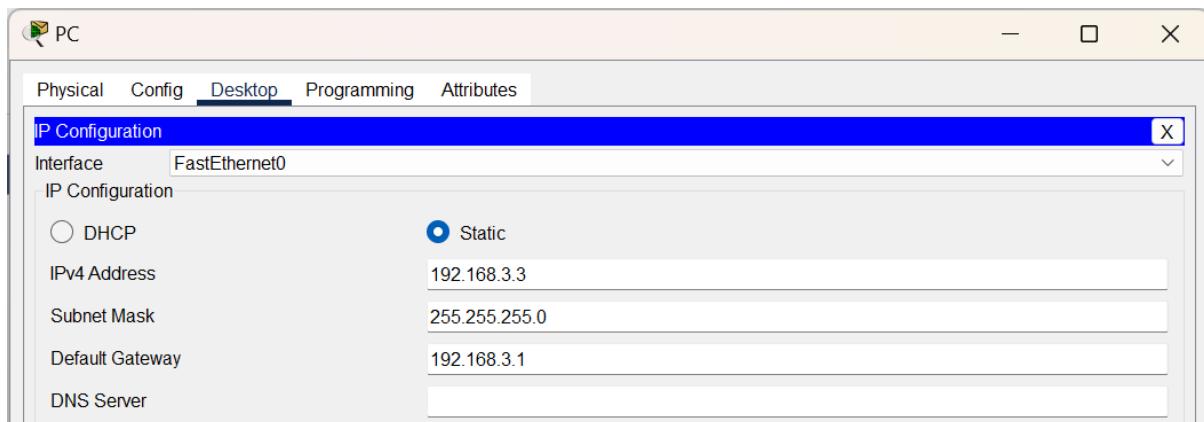
- A. Verify connectivity among devices before firewall configuration.
- B. Use ACLs to ensure remote access to the routers is available only from management station PC-c.
- C. Configure ACLs on to mitigate attacks.
- D. Configure IPv6 ACLs

➤ Topology Diagram



➤ Assigning IP Addresses





R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/z.
Router(config)#host R1
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

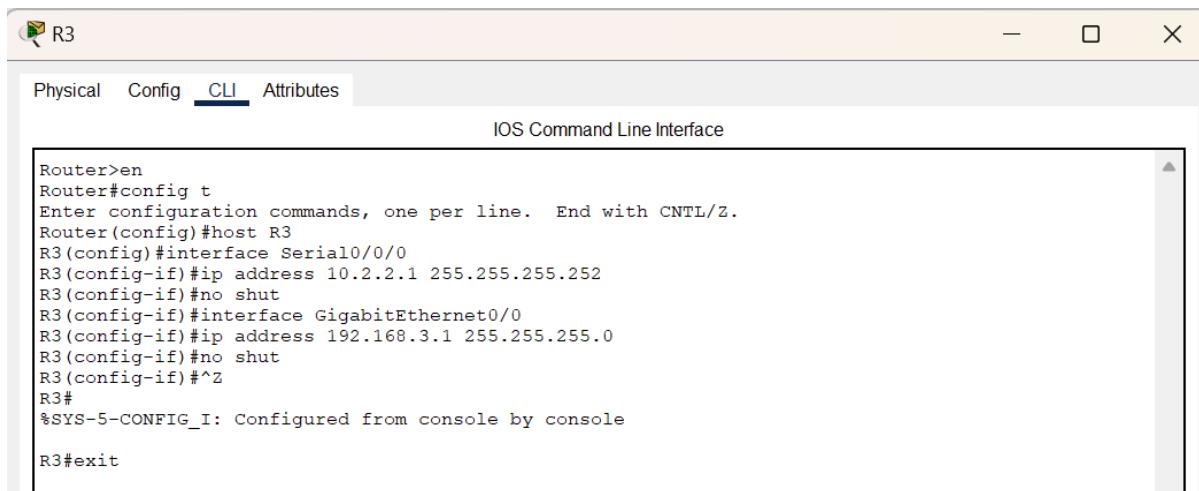
R2

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/z.
Router(config)#host R2
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#int loopback1

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```



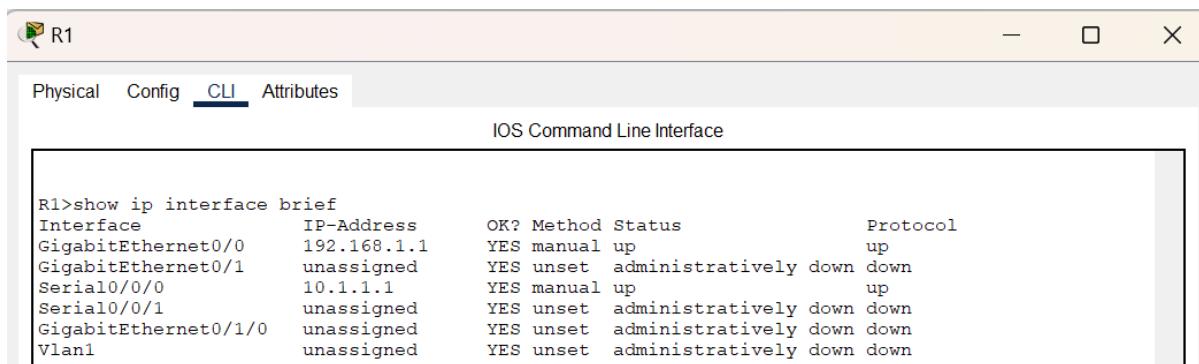
R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R3
R3(config)#interface Serial0/0/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#{^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ Displaying IP Address Details of Routers

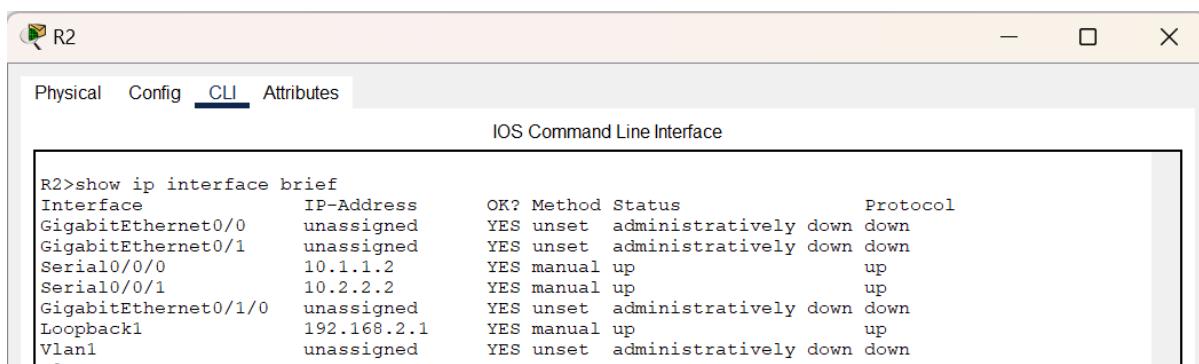


R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0  192.168.1.1    YES manual up           up
GigabitEthernet0/1  unassigned      YES unset administratively down down
Serial0/0/0         10.1.1.1       YES manual up           up
Serial0/0/1         unassigned      YES unset administratively down down
GigabitEthernet0/1/0 unassigned      YES unset administratively down down
Vlan1              unassigned      YES unset administratively down down
````
```

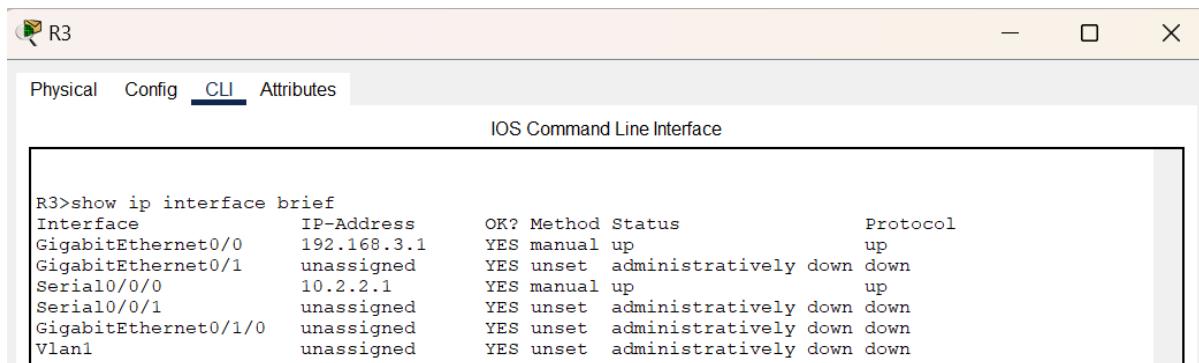


R2

Physical Config **CLI** Attributes

IOS Command Line Interface

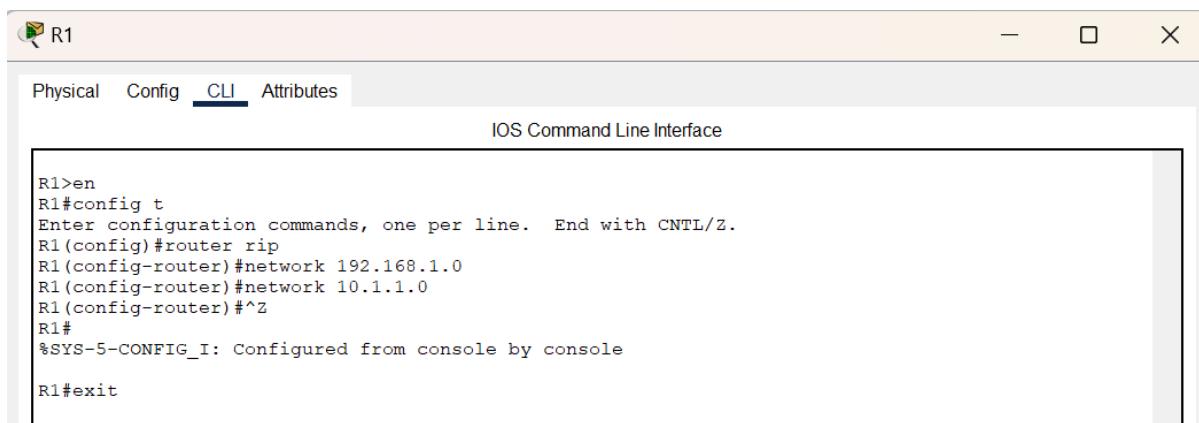
```
R2>show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset administratively down down
GigabitEthernet0/1 unassigned YES unset administratively down down
Serial0/0/0 10.1.1.2 YES manual up up
Serial0/0/1 10.2.2.2 YES manual up up
GigabitEthernet0/1/0 unassigned YES unset administratively down down
Loopback1 192.168.2.1 YES manual up up
Vlan1 unassigned YES unset administratively down down
````
```



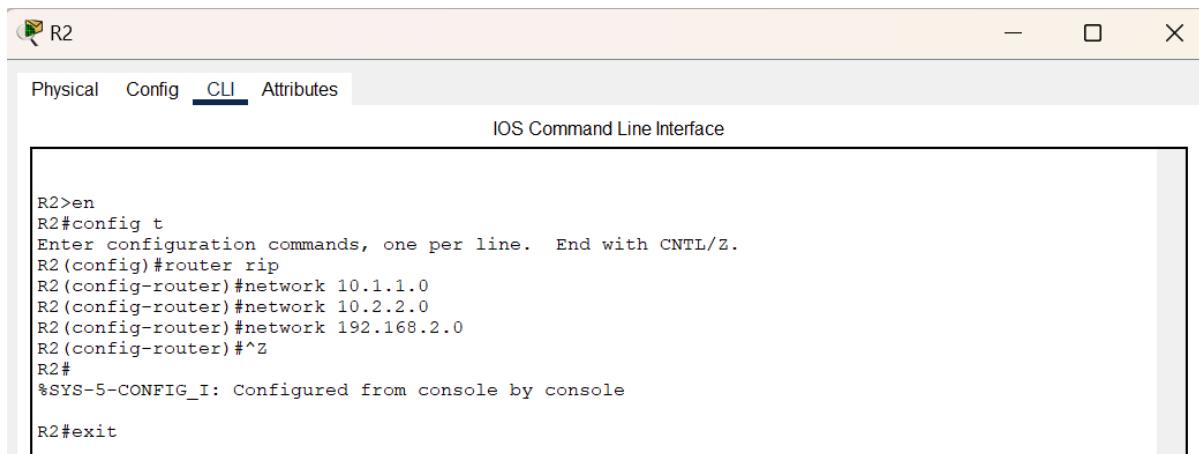
R3>show ip interface brief

| Interface | IP-Address | OK? | Method | Status | Protocol |
|----------------------|-------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0 | 192.168.3.1 | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.2.2.1 | YES | manual | up | up |
| Serial0/0/1 | unassigned | YES | unset | administratively down | down |
| GigabitEthernet0/1/0 | unassigned | YES | unset | administratively down | down |
| Vlan1 | unassigned | YES | unset | administratively down | down |

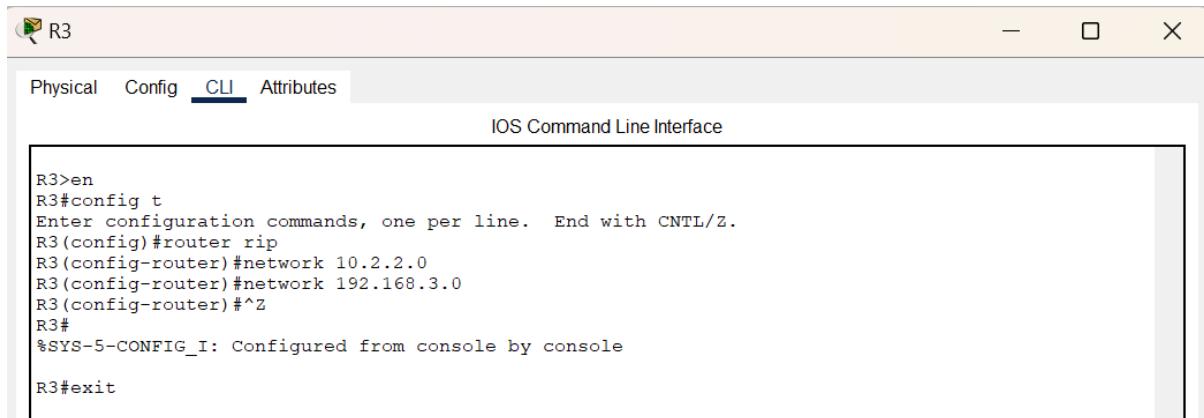
➤ Configure RIP on routers



```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#+Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

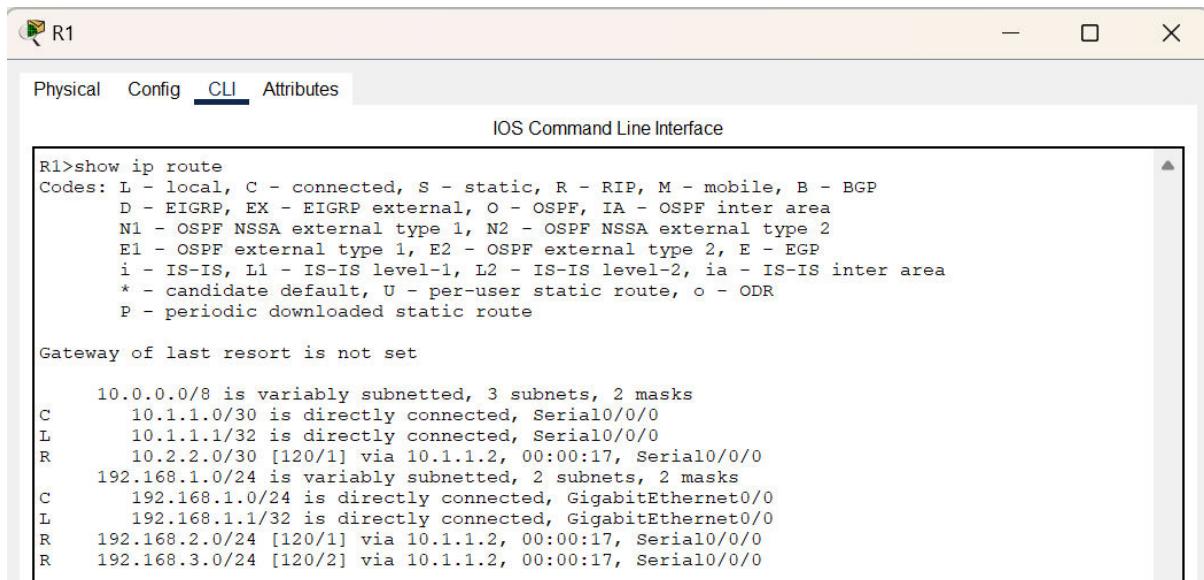


```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#network 192.168.2.0
R2(config-router)#+Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```



R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

➤ Displaying routing table of routers



```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:17, Serial0/0/0
          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.1.0/24 is directly connected, GigabitEthernet0/0
L          192.168.1.1/32 is directly connected, GigabitEthernet0/0
R          192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:17, Serial0/0/0
R          192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:17, Serial0/0/0
```

R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.2/32 is directly connected, Serial0/0/1
R        192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
          192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback1
L        192.168.2.1/32 is directly connected, Loopback1
R        192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:11, Serial0/0/1
```

R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:08, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/0
L        10.2.2.1/32 is directly connected, Serial0/0/0
R        192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:08, Serial0/0/0
R        192.168.2.0/24 [120/1] via 10.2.2.2, 00:00:08, Serial0/0/0
          192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

➤ **Configure SSH on R2**

R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/z.
R2(config)#ip domain-name securityincomputing.com
R2(config)#username admin secret pwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

R2(config)#crypto key generate rsa
The name for the keys will be: R2.securityincomputing.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

R2(config)#ip ssh time-out 90
*Mar 1 2:52:48.794: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
R2(config)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit

➤ Verify Basic Network Connectivity before ACL Configuration

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=23ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 23ms, Average = 7ms

C:\>ssh -l admin 192.168.2.1
Password:

R2>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

Cisco 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=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=23ms TTL=125
Reply from 192.168.1.3: bytes=32 time=11ms TTL=125
Reply from 192.168.1.3: bytes=32 time=17ms TTL=125

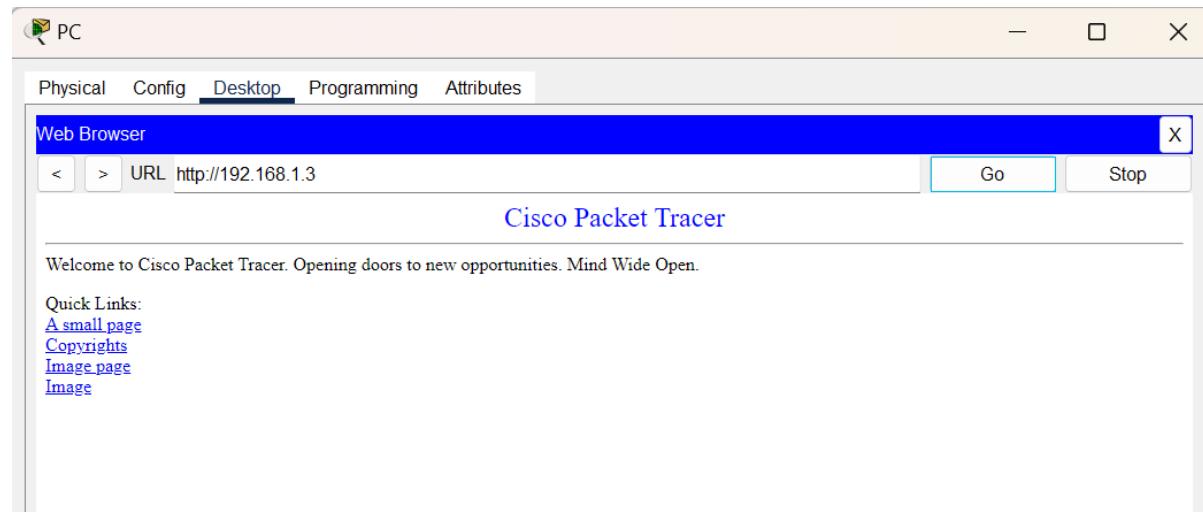
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 23ms, Average = 13ms

C:\>ssh -l admin 192.168.2.1

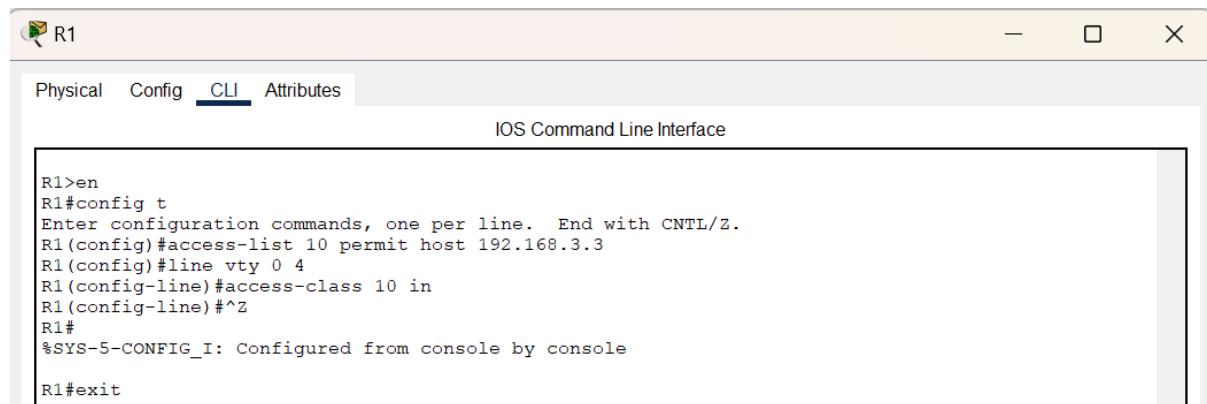
Password:

R2>exit

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



- **Configure ACL on routers (block all remote access to the routers except from PC)**

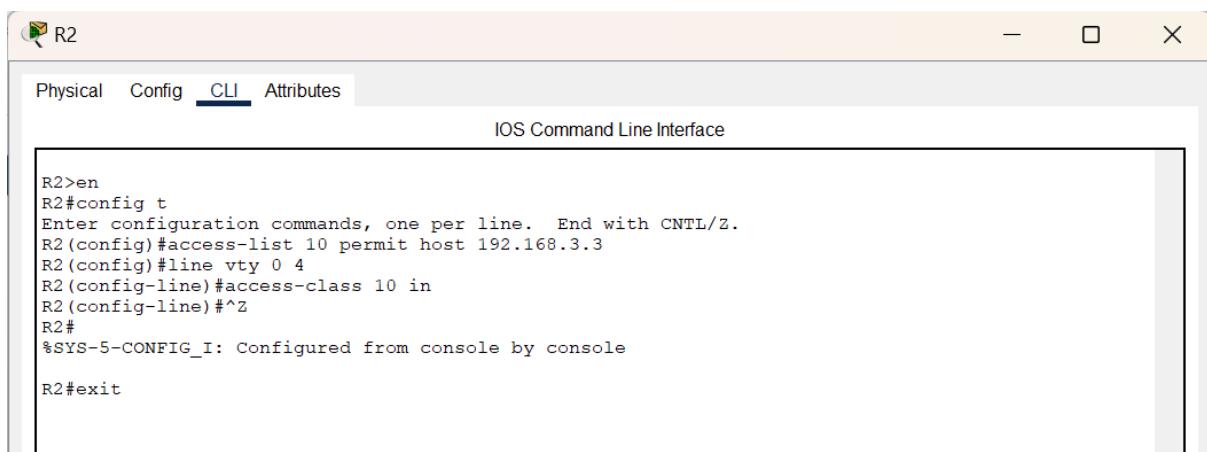


R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 10 permit host 192.168.3.3
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
R1(config-line)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

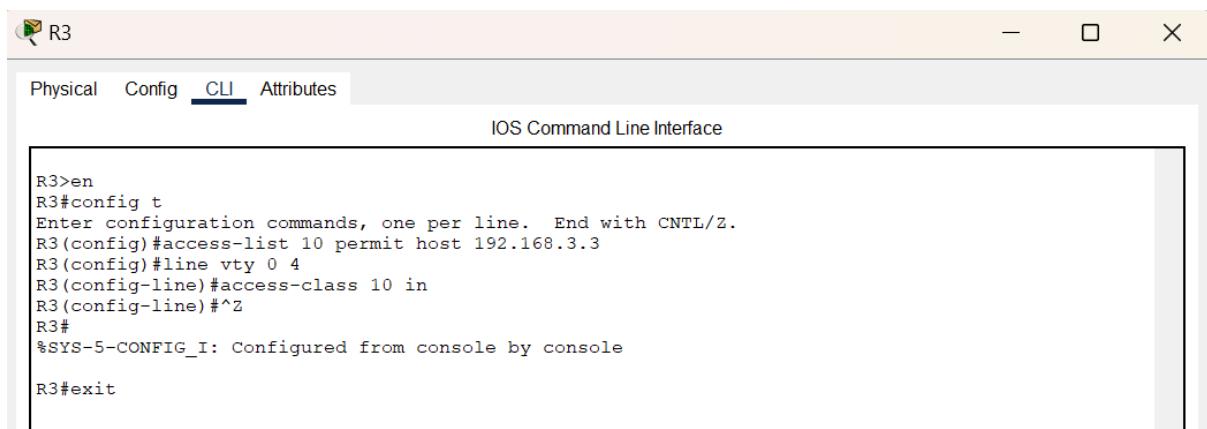


R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 10 permit host 192.168.3.3
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in
R2(config-line)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```



R3

Physical Config **CLI** Attributes

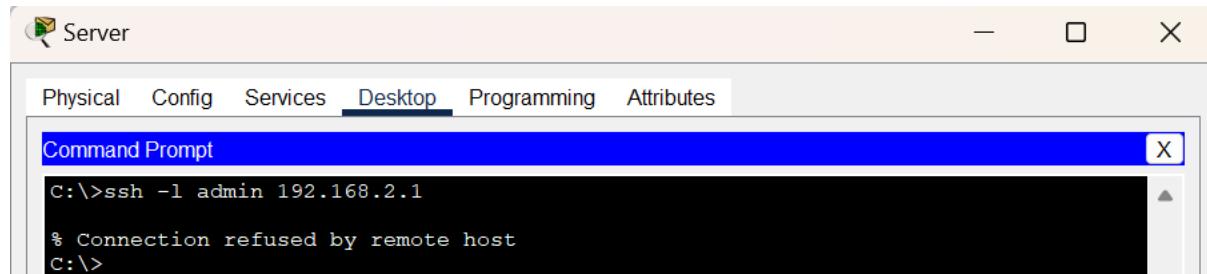
IOS Command Line Interface

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 10 permit host 192.168.3.3
R3(config)#line vty 0 4
R3(config-line)#access-class 10 in
R3(config-line)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ **Verifying the working of ACL**

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

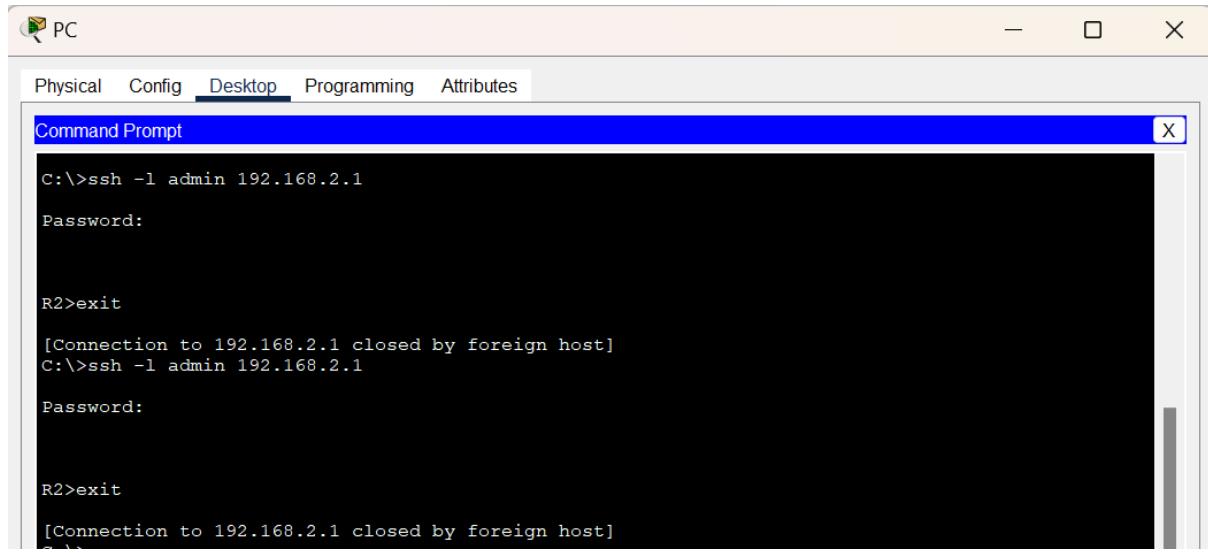


Server

Physical Config Services Desktop Programming Attributes

Command Prompt

```
C:\>ssh -l admin 192.168.2.1
% Connection refused by remote host
C:\>
```



PC

Physical Config Desktop Programming Attributes

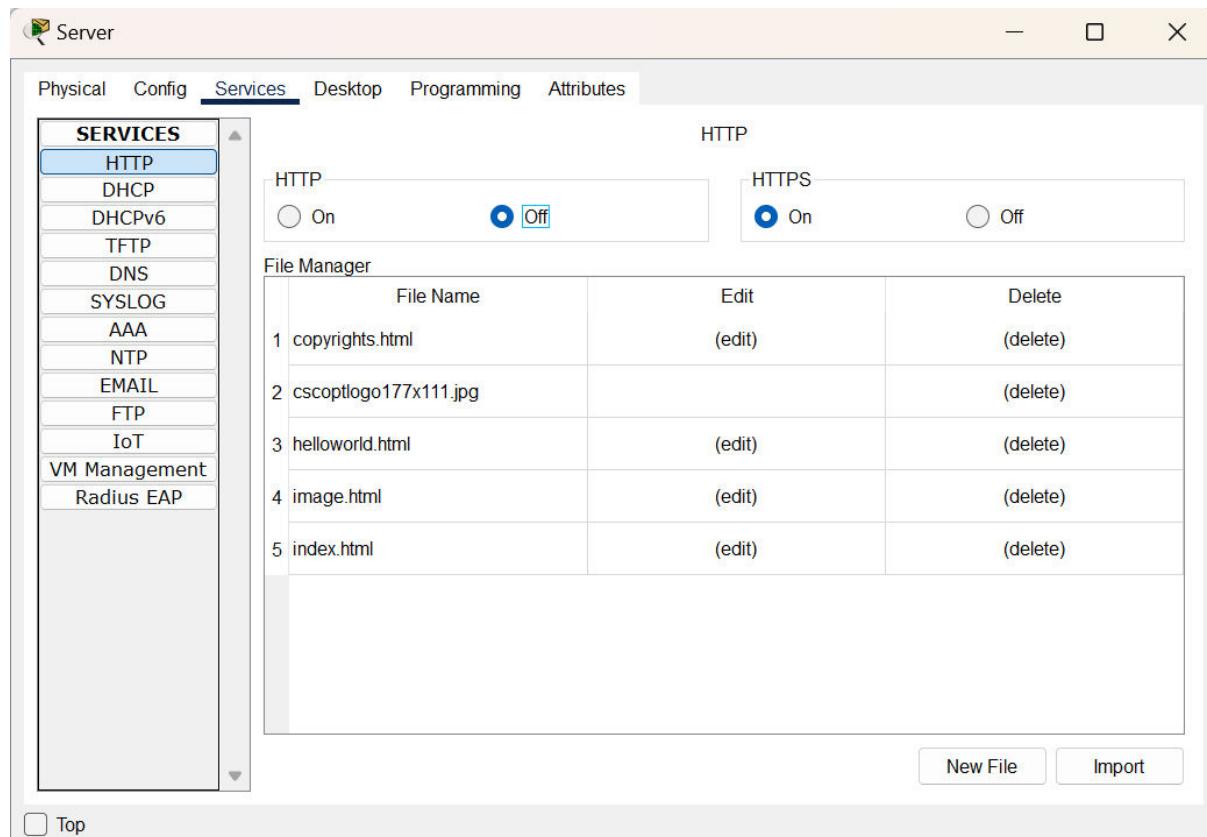
Command Prompt

```
C:\>ssh -l admin 192.168.2.1
Password:

R2>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l admin 192.168.2.1
Password:

R2>exit
[Connection to 192.168.2.1 closed by foreign host]
```

- **Disable HTTP and enable HTTPS on server**

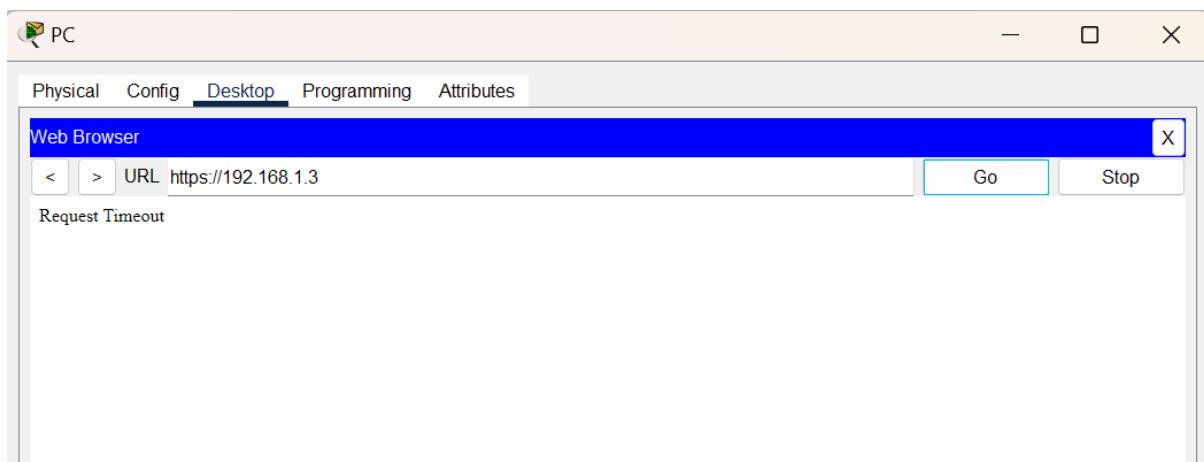


➤ **Configure ACL on routers**

- Permit any outside host to access DNS, SMTP, and FTP services on Server
- Deny any outside host access to HTTPS services on Server.
- Permit PC to access RI via SSH.

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 120 permit udp any host 192.168.1.3 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq smtp
R1(config)#access-list 120 permit tcp any host 192.168.1.3 eq ftp
R1(config)#access-list 120 deny tcp any host 192.168.1.3 eq 443
R1(config)#access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
R1(config)#interface Serial0/0/0
R1(config-if)#ip access-group 120 in
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

➤ Verifying the working of ACL



➤ Verifying the network connectivity before ACL implementation

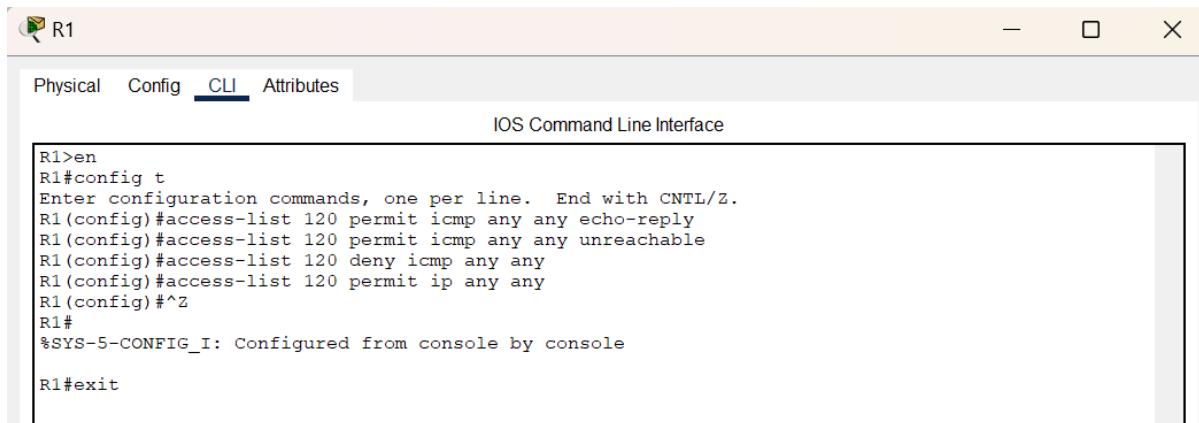
```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

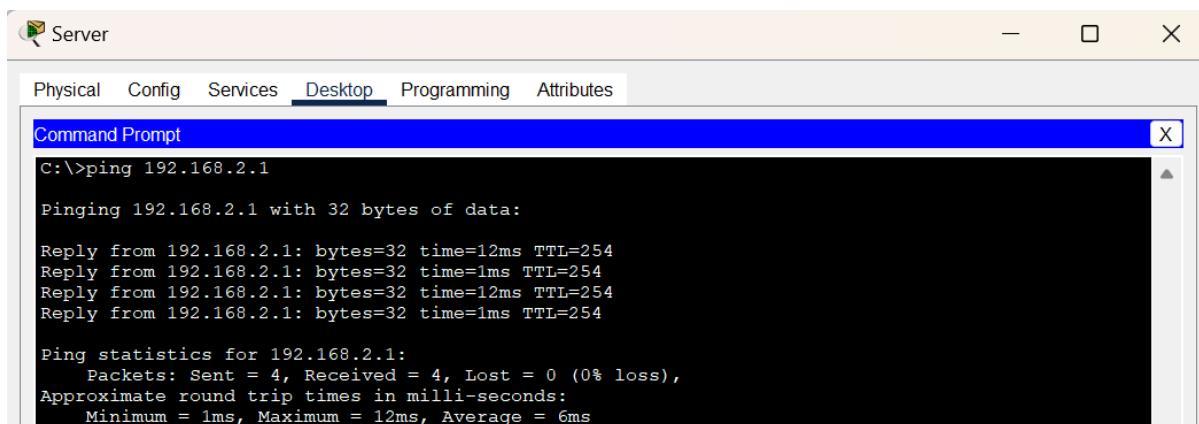
➤ Modify an Existing ACL on R1

- **(Permit ICMP echo replies and destination unreachable messages from the outside network. Deny all the other incoming ICMP packets.**



R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 120 permit icmp any any echo-reply
R1(config)#access-list 120 permit icmp any any unreachable
R1(config)#access-list 120 deny icmp any any
R1(config)#access-list 120 permit ip any any
R1(config)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit

➤ Verifying the working of ACL

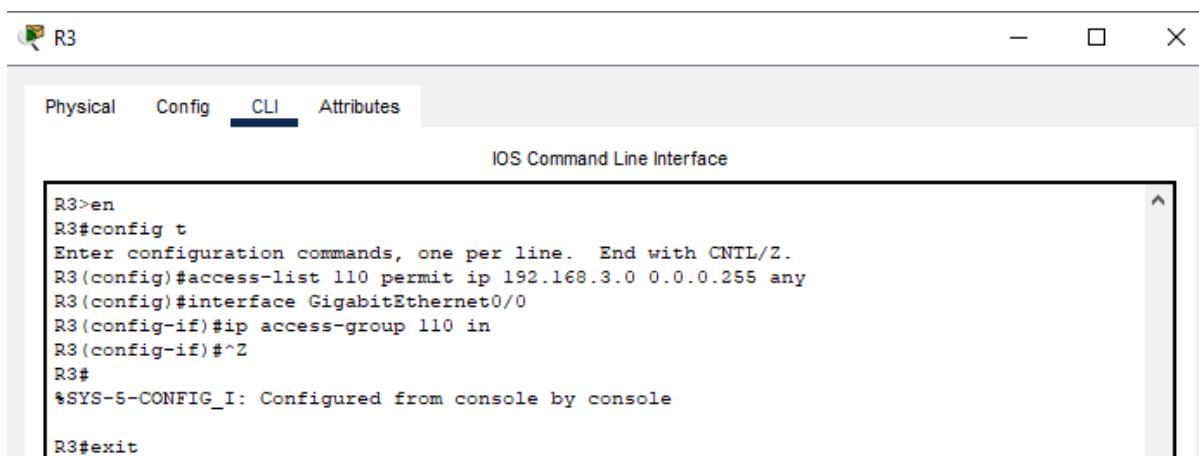


C:\>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=12ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254
Reply from 192.168.2.1: bytes=32 time=12ms TTL=254
Reply from 192.168.2.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.2.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 12ms, Average = 6ms

➤ Configure ACL on routers

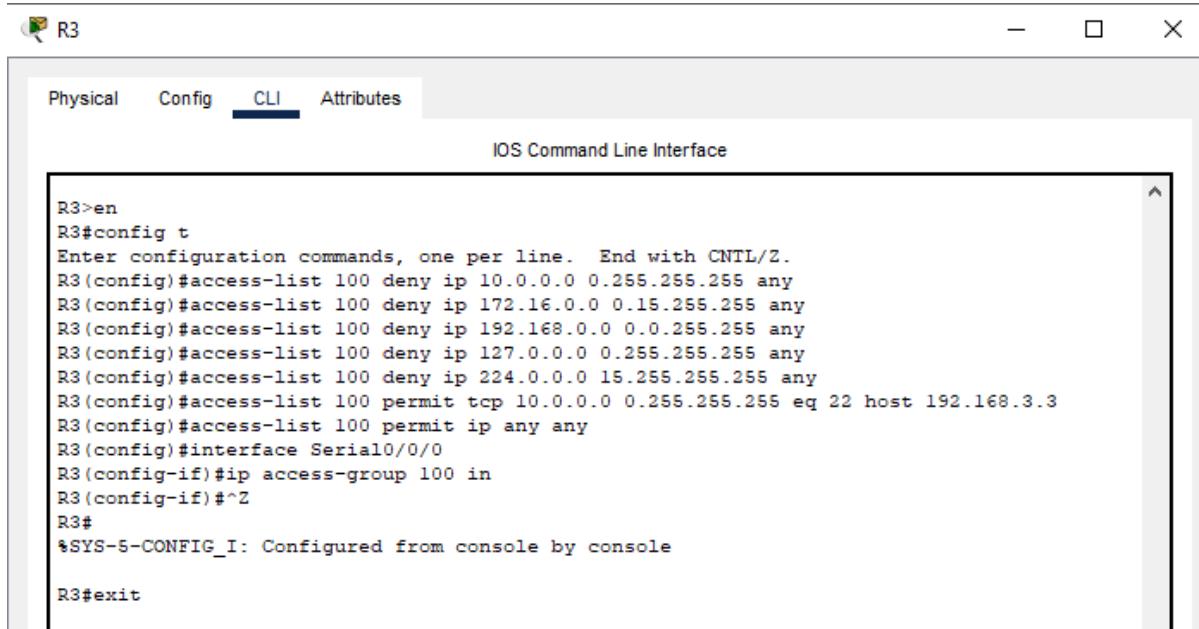
- **(Deny all outbound packets with source address outside the range of internal IP addresses on R3)**



R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip access-group 110 in
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

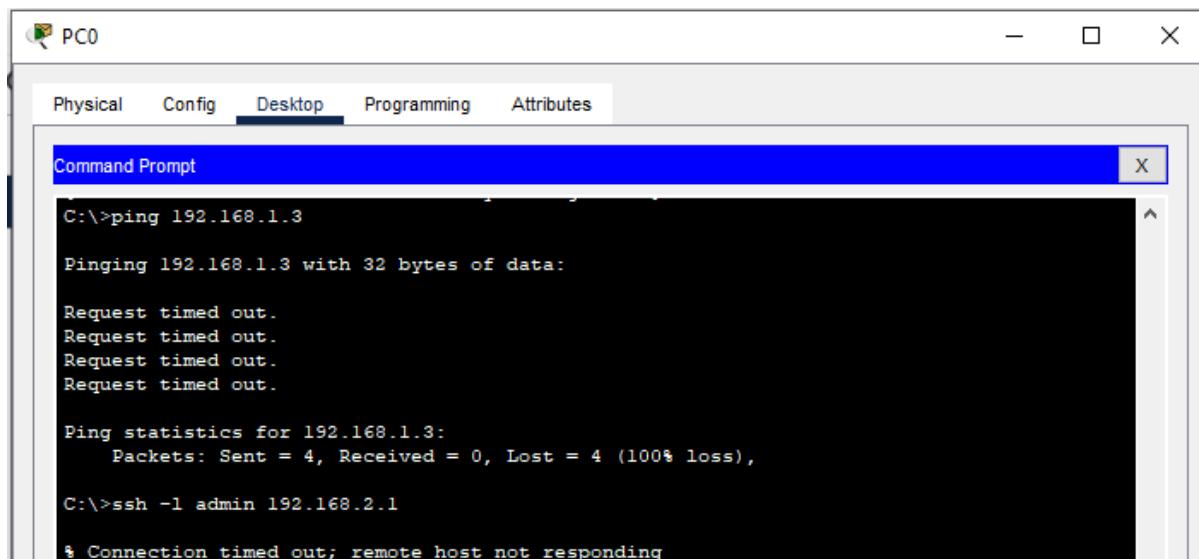
➤ **Configure ACL on routers**

- **(On R3, block all packets containing the source IP address from the following pool of addresses: private addresses, 127.0.0.0/8, and any IP multicast address. Permit SSH traffic from the 10.0.0.0/8 network to return to the host PC)**



R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)#access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)#access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host 192.168.3.3
R3(config)#access-list 100 permit ip any any
R3(config)#interface Serial0/0/0
R3(config-if)#ip access-group 100 in
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit



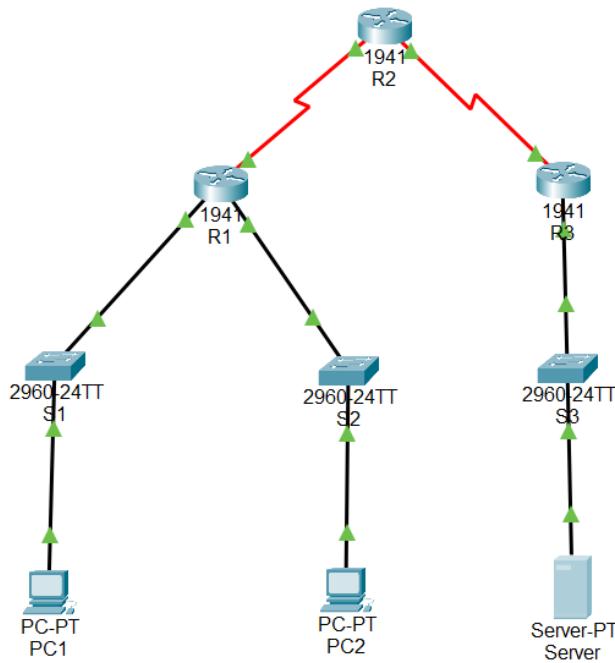
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

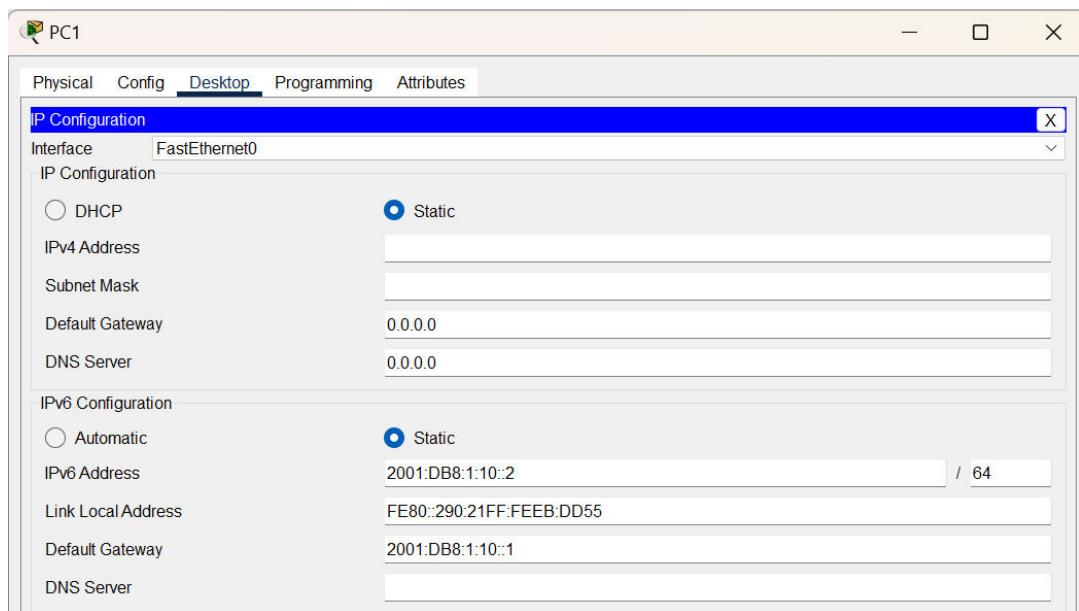
C:\>ssh -l admin 192.168.2.1
* Connection timed out; remote host not responding

Configuring IPv6 ACLs

➤ Topology Diagram

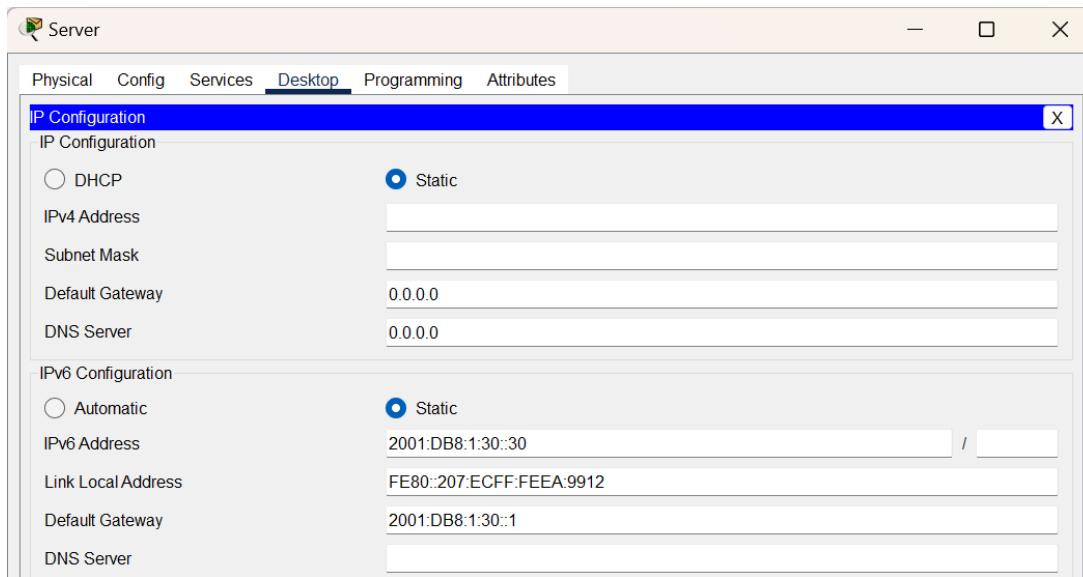
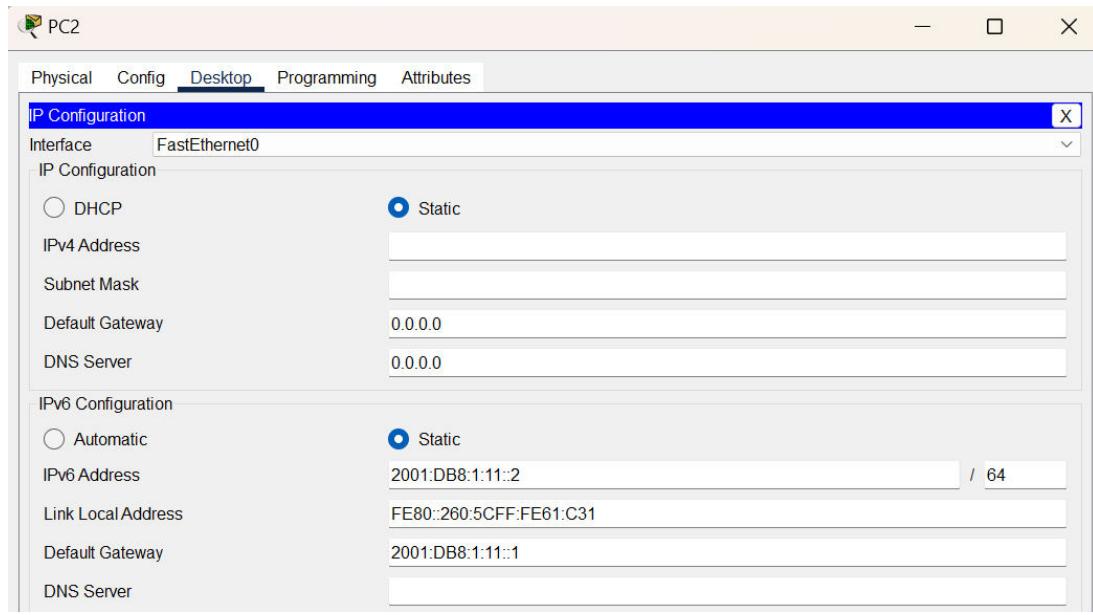


➤ Assign IP Address



Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025



Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#ipv6 unicast-routing
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:10::1/64
R1(config-if)#no shut
R1(config-if)#interface GigabitEthernet0/1
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:11::1/64
R1(config-if)#no shut
R1(config-if)#interface Serial0/0/0
R1(config-if)#ipv6 enable
R1(config-if)#ipv6 address 2001:DB8:1:28::1/64
R1(config-if)#no shut
R1(config-if)^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#ipv6 unicast-routing
R2(config)#interface Serial0/0/0
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:28::2/64
R2(config-if)#no shut
R2(config-if)#interface Serial0/0/1
R2(config-if)#ipv6 enable
R2(config-if)#ipv6 address 2001:DB8:1:29::2/64
R2(config-if)#no shut
R2(config-if)^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

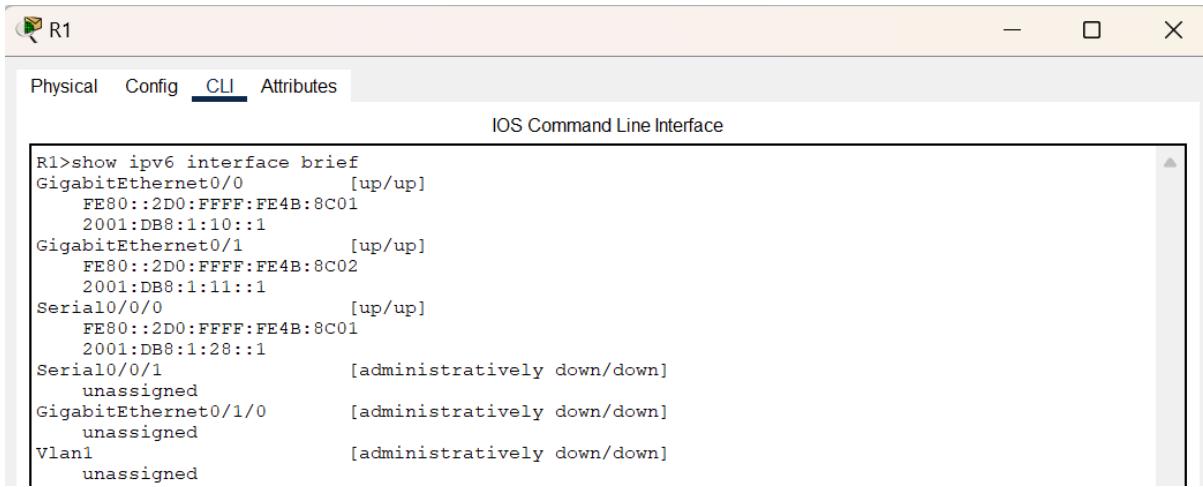
R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R3
R3(config)#ipv6 unicast-routing
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2001:DB8:1:30::1/64
R3(config-if)#no shut
R3(config-if)#interface Serial0/0/0
R3(config-if)#ipv6 enable
R3(config-if)#ipv6 address 2001:DB8:1:29::1/64
R3(config-if)#no shut
R3(config-if)^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ Displaying IP Address Details of Routers



R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::2D0:FFFF:FE4B:8C01
  2001:DB8:1:10::1
GigabitEthernet0/1      [up/up]
  FE80::2D0:FFFF:FE4B:8C02
  2001:DB8:1:11::1
Serial0/0/0             [up/up]
  FE80::2D0:FFFF:FE4B:8C01
  2001:DB8:1:28::1
Serial0/0/1             [administratively down/down]
  unassigned
GigabitEthernet0/1/0    [administratively down/down]
  unassigned
Vlan1                  [administratively down/down]
  unassigned
```



R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>show ipv6 interface brief
GigabitEthernet0/0      [administratively down/down]
  unassigned
GigabitEthernet0/1      [administratively down/down]
  unassigned
Serial0/0/0             [up/up]
  FE80::207:ECFF:FE76:A01
  2001:DB8:1:28::2
Serial0/0/1             [up/up]
  FE80::207:ECFF:FE76:A01
  2001:DB8:1:29::2
GigabitEthernet0/1/0    [administratively down/down]
  unassigned
Vlan1                  [administratively down/down]
  unassigned
```



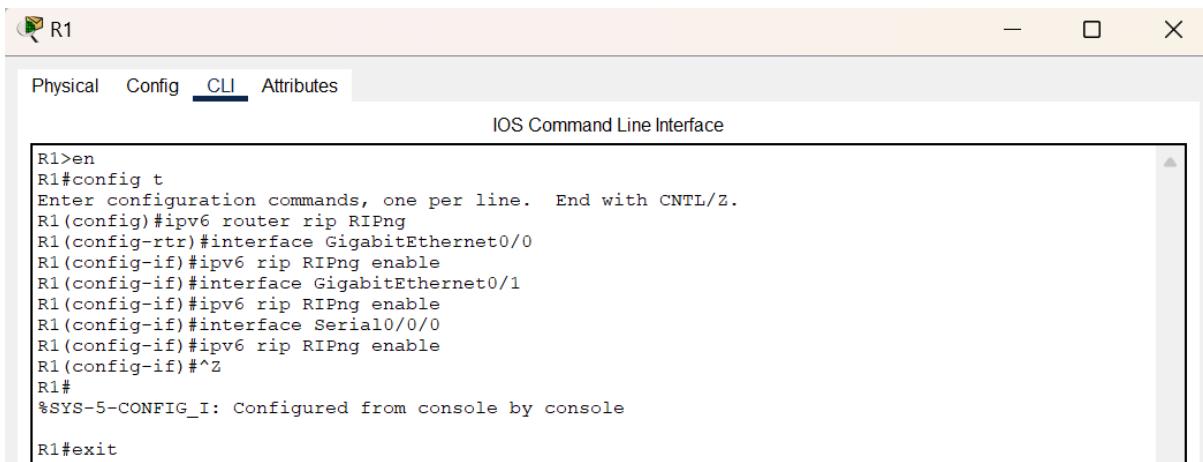
R3

Physical Config **CLI** Attributes

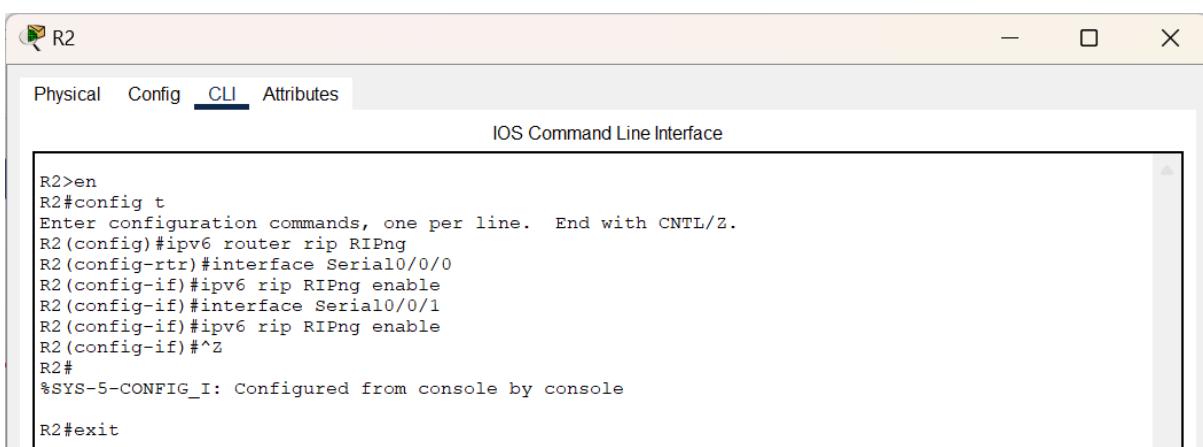
IOS Command Line Interface

```
R3>show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::2E0:F7FF:FE60:7401
  2001:DB8:1:30::1
GigabitEthernet0/1      [administratively down/down]
  unassigned
Serial0/0/0             [up/up]
  FE80::2E0:F7FF:FE60:7401
  2001:DB8:1:29::1
Serial0/0/1             [administratively down/down]
  unassigned
GigabitEthernet0/1/0    [administratively down/down]
  unassigned
Vlan1                  [administratively down/down]
  unassigned
```

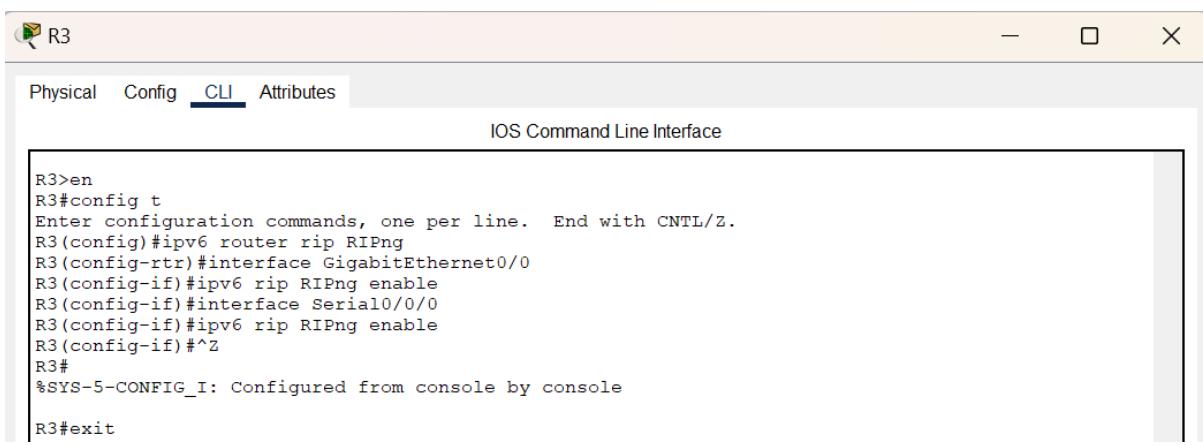
➤ Configure RIPng on routers



R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router rip RIPng
R1(config-rtr)#interface GigabitEthernet0/0
R1(config-if)#ipv6 rip RIPng enable
R1(config-if)#interface GigabitEthernet0/1
R1(config-if)#ipv6 rip RIPng enable
R1(config-if)#interface Serial0/0/0
R1(config-if)#ipv6 rip RIPng enable
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit



R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ipv6 router rip RIPng
R2(config-rtr)#interface Serial0/0/0
R2(config-if)#ipv6 rip RIPng enable
R2(config-if)#interface Serial0/0/1
R2(config-if)#ipv6 rip RIPng enable
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit



R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router rip RIPng
R3(config-rtr)#interface GigabitEthernet0/0
R3(config-if)#ipv6 rip RIPng enable
R3(config-if)#interface Serial0/0/0
R3(config-if)#ipv6 rip RIPng enable
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

➤ **Displaying routing table of routers**

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

R1

Physical Config **CLI** Attributes

IOS Command Line Interface

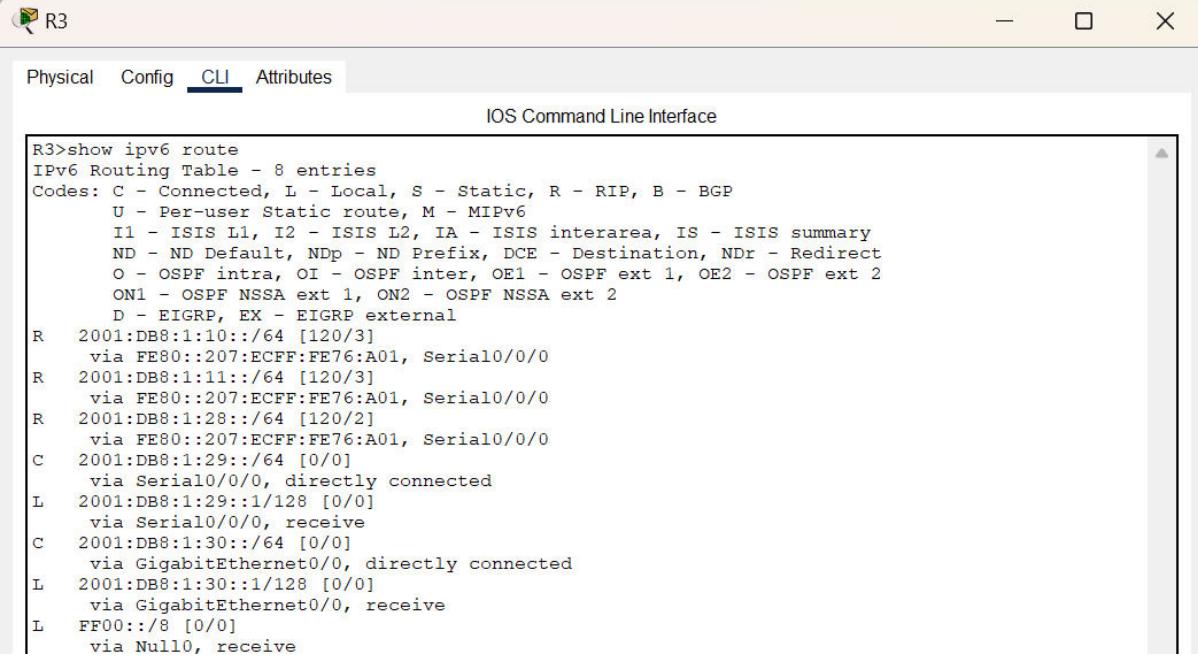
```
R1>show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
C  2001:DB8:1:10::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:1:10::1/128 [0/0]
   via GigabitEthernet0/0, receive
C  2001:DB8:1:11::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L  2001:DB8:1:11::1/128 [0/0]
   via GigabitEthernet0/1, receive
C  2001:DB8:1:28::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:1:28::1/128 [0/0]
   via Serial0/0/0, receive
R  2001:DB8:1:29::/64 [120/2]
   via FE80::207:ECFF:FE76:A01, Serial0/0/0
R  2001:DB8:1:30::/64 [120/3]
   via FE80::207:ECFF:FE76:A01, Serial0/0/0
L  FF00::/8 [0/0]
   via Null0, receive
```

R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
R  2001:DB8:1:10::/64 [120/2]
   via FE80::2D0:FFFF:FE4B:8C01, Serial0/0/0
R  2001:DB8:1:11::/64 [120/2]
   via FE80::2D0:FFFF:FE4B:8C01, Serial0/0/0
C  2001:DB8:1:28::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:1:28::2/128 [0/0]
   via Serial0/0/0, receive
C  2001:DB8:1:29::/64 [0/0]
   via Serial0/0/1, directly connected
L  2001:DB8:1:29::2/128 [0/0]
   via Serial0/0/1, receive
R  2001:DB8:1:30::/64 [120/2]
   via FE80::2E0:F7FF:FE60:7401, Serial0/0/1
L  FF00::/8 [0/0]
   via Null0, receive
```



The screenshot shows a terminal window titled "R3" with the following interface:

- Top menu bar: Physical, Config, **CLI**, Attributes.
- Title bar: IOS Command Line Interface.
- Output area:

```
R3>show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
      U - Per-user Static route, M - MIPv6
      I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
      D - EIGRP, EX - EIGRP external
R    2001:DB8:1:10::/64 [120/3]
      via FE80::207:ECFF:FE76:A01, Serial0/0/0
R    2001:DB8:1:11::/64 [120/3]
      via FE80::207:ECFF:FE76:A01, Serial0/0/0
R    2001:DB8:1:28::/64 [120/2]
      via FE80::207:ECFF:FE76:A01, Serial0/0/0
C    2001:DB8:1:29::/64 [0/0]
      via Serial0/0/0, directly connected
L    2001:DB8:1:29::1/128 [0/0]
      via Serial0/0/0, receive
C    2001:DB8:1:30::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:DB8:1:30::1/128 [0/0]
      via GigabitEthernet0/0, receive
L    FF00::8 [0/0]
      via Null0, receive
```

➤ **Displaying IP Address Details of Routers**

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
c:\>ping 2001:DB8:1:11::2
Pinging 2001:DB8:1:11::2 with 32 bytes of data:
Reply from 2001:DB8:1:11::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:1:11::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=22ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=10ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 22ms, Average = 9ms
```

PC2

Physical Config Desktop Programming Attributes

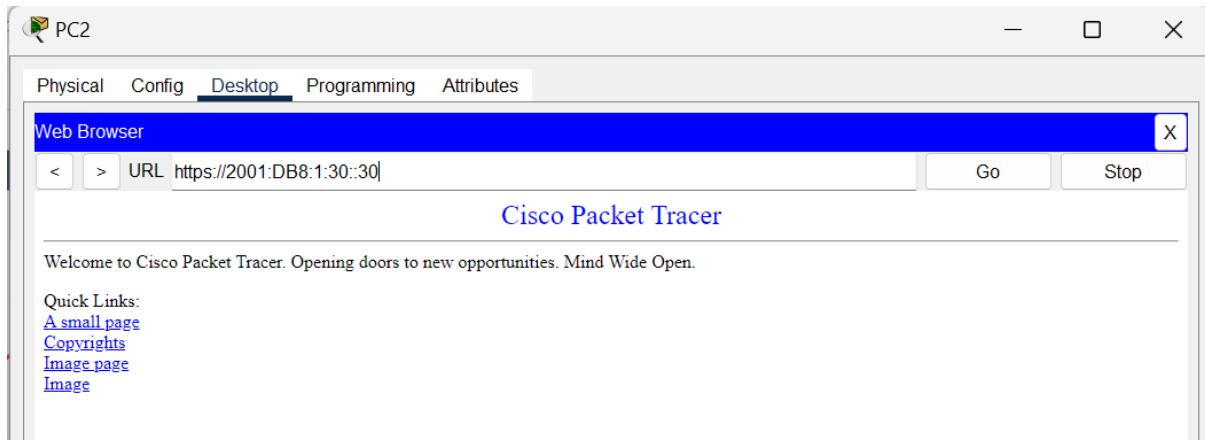
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
c:\>ping 2001:DB8:1:10::2
Pinging 2001:DB8:1:10::2 with 32 bytes of data:
Reply from 2001:DB8:1:10::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:1:10::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

c:\>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Reply from 2001:DB8:1:30::30: bytes=32 time=30ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=16ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 30ms, Average = 12ms
```



➤ **Configuring ACL**
(Block HTTP and HTTPS access and Allow all other IPv6 traffic to pass)

The screenshot shows a window titled 'R1' with a tab bar at the top. The 'CLI' tab is selected. Below it is a terminal window titled 'IOS Command Line Interface'. The command history shows the configuration of an IPv6 access-list named 'BLOCK_HTTPS_ACL' on interface GigabitEthernet0/0. The configuration includes deny rules for ports 80 and 443, and a permit rule for all other traffic.

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 access-list BLOCK_HTTPS_ACL
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq www
R1(config-ipv6-acl)#deny tcp any host 2001:DB8:1:30::30 eq 443
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#interface GigabitEthernet0/0
R1(config-if)#ipv6 traffic-filter BLOCK_HTTPS_ACL in
R1(config-if)^(Z)
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

➤ **Verifying the working of ACL**

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

PC1

Physical Config Desktop Programming Attributes

Command Prompt X

```
C:\>ping 2001:DB8:1:11::2
Pinging 2001:DB8:1:11::2 with 32 bytes of data:
Reply from 2001:DB8:1:11::2: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:1:11::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:1:11::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 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=16ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=21ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 21ms, Average = 10ms
```

PC2

Physical Config Desktop Programming Attributes

Command Prompt X

```
C:\>ping 2001:DB8:1:10::2
Pinging 2001:DB8:1:10::2 with 32 bytes of data:
Reply from 2001:DB8:1:10::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:1:10::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

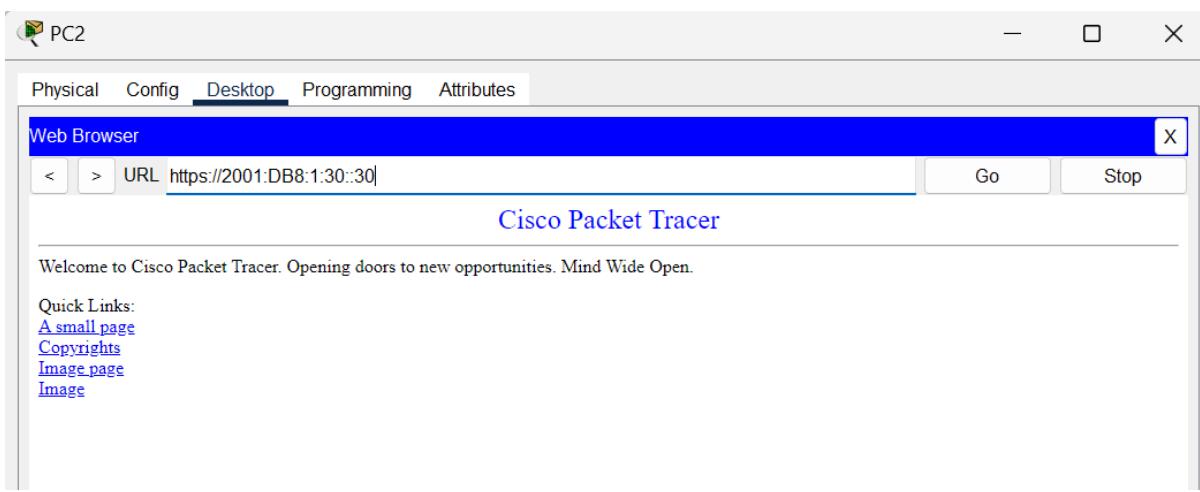
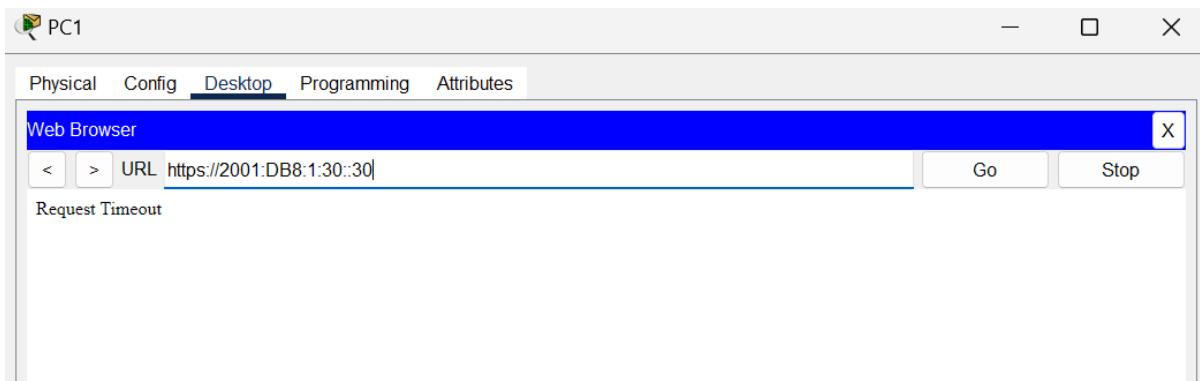
C:\>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:

Reply from 2001:DB8:1:30::30: bytes=32 time=26ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:1:30::30: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:1:30::30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 26ms, Average = 8ms
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025



➤ **Configuring ACL**
(Block ICMP access and Allow all other IPv6 traffic to pass)

A screenshot of a terminal window titled "R3". The top menu bar includes "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected. The window title is "IOS Command Line Interface". The terminal output shows the configuration of an IPv6 ACL named "BLOCK_ICMP_ACL" on interface GigabitEthernet0/0:

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 access-list BLOCK_ICMP_ACL
R3(config-ipv6-acl)#deny icmp any any
R3(config-ipv6-acl)#permit ipv6 any any
R3(config-ipv6-acl)#interface GigabitEthernet0/0
R3(config-if)#ipv6 traffic-filter BLOCK_ICMP_ACL in
R3(config-if)#+^z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ **Verifying the working of ACL**

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 21.01.2025

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:1:30::30:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PC2

Physical Config Desktop Programming Attributes

Command Prompt

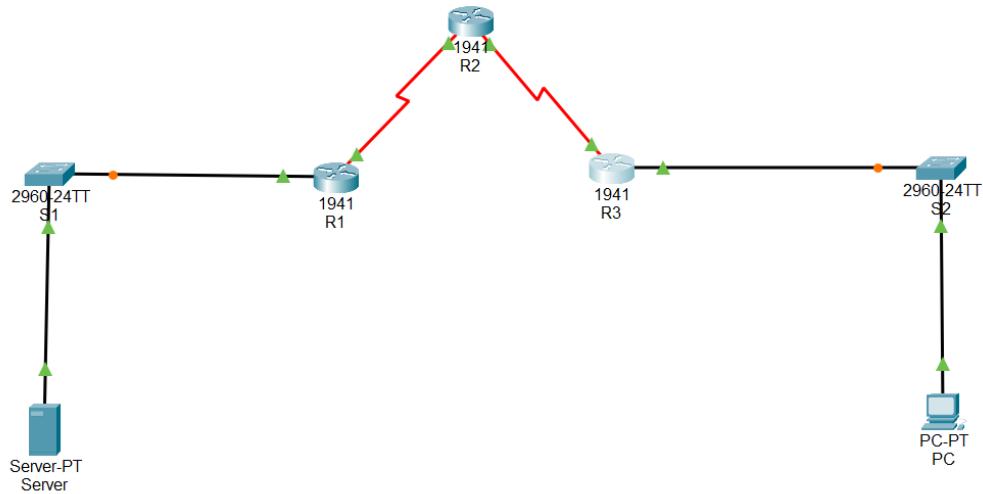
```
C:\>ping 2001:DB8:1:30::30
Pinging 2001:DB8:1:30::30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:1:30::30:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

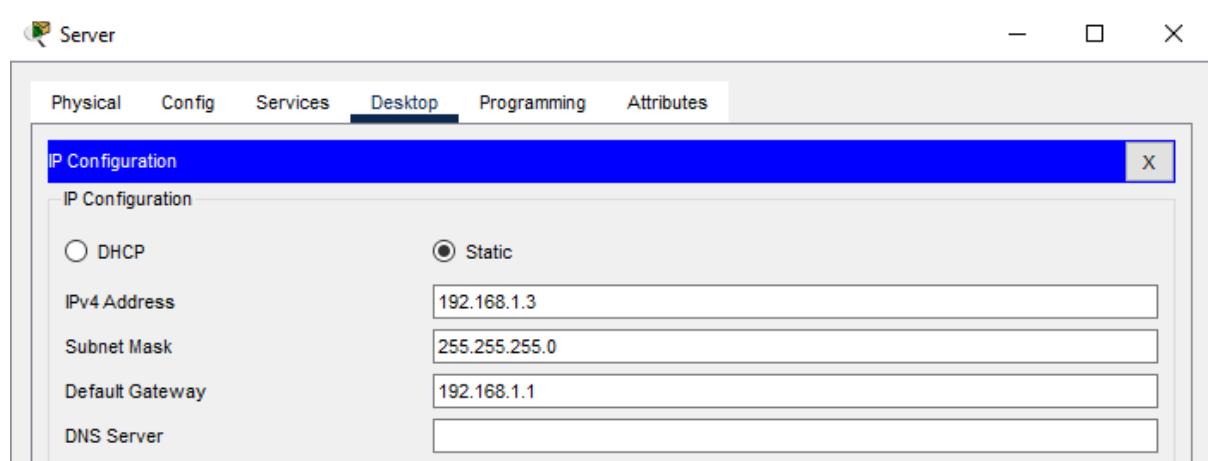
Practical 5

Aim: Configuring a Zone-Based Policy Firewall.

➤ Topology Diagram

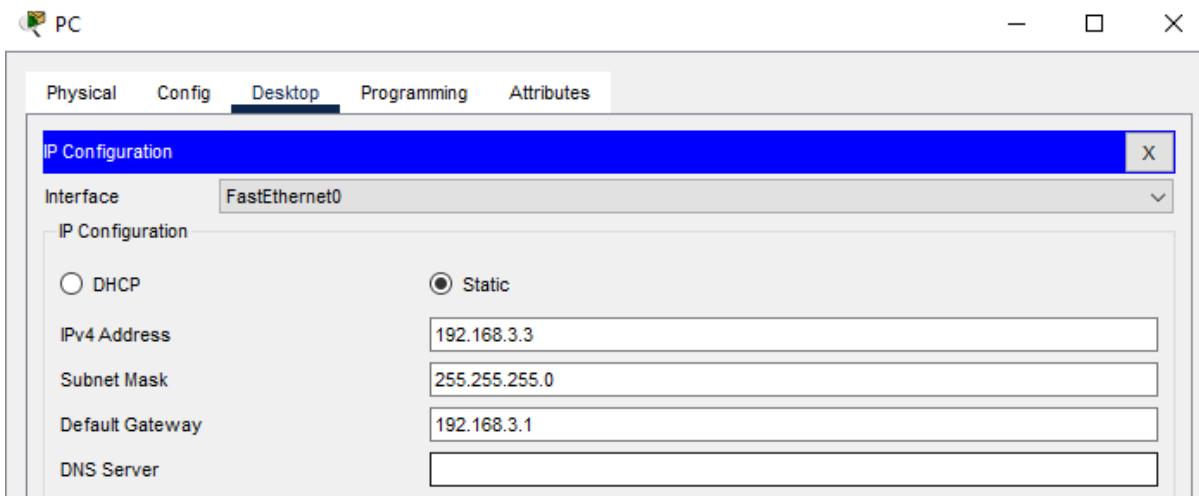


➤ Assigning IP Addresses



Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 28.01.2025

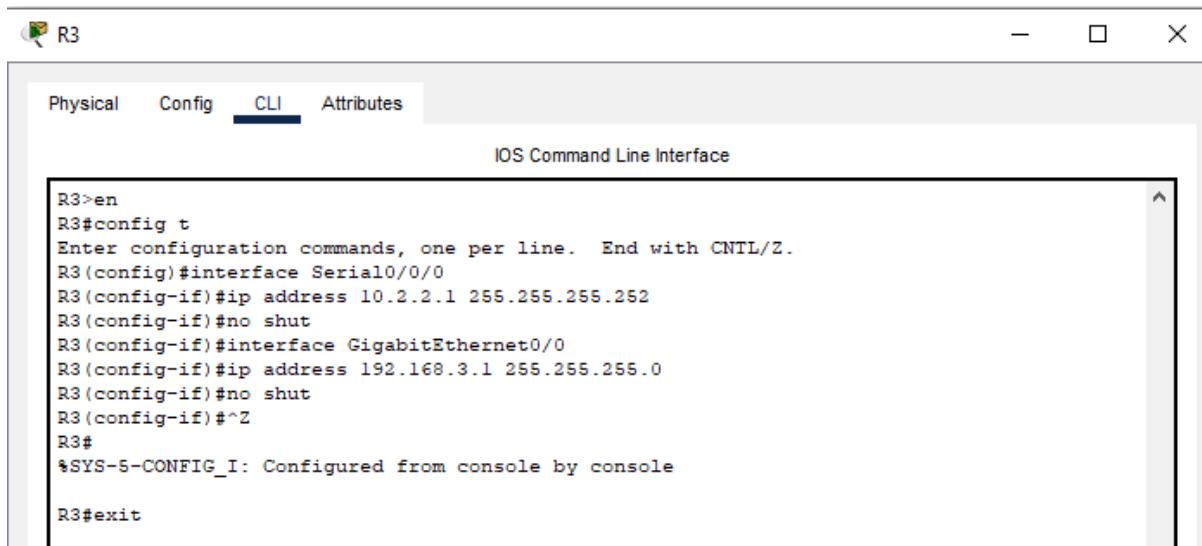


The screenshot shows the "IOS Command Line Interface" for a device named "R1". The "CLI" tab is selected. The configuration commands entered are:

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

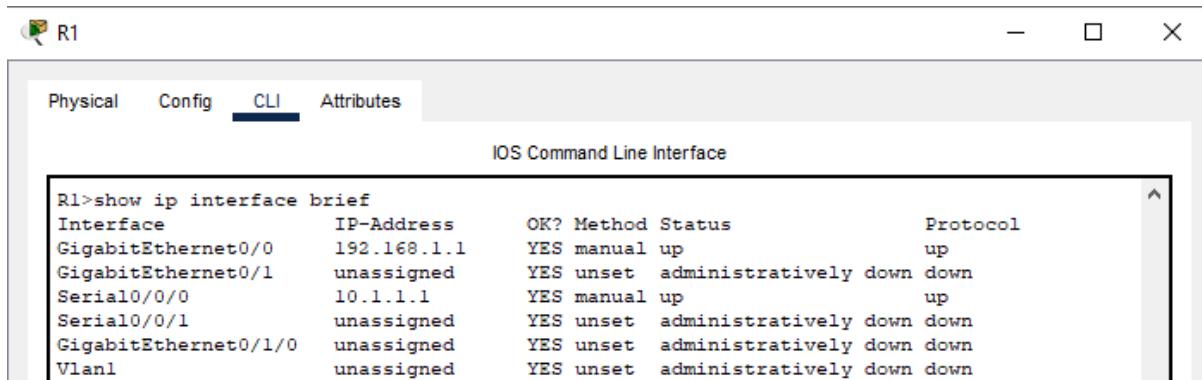
The screenshot shows the "IOS Command Line Interface" for a device named "R2". The "CLI" tab is selected. The configuration commands entered are:

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#interface Serial0/0/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```



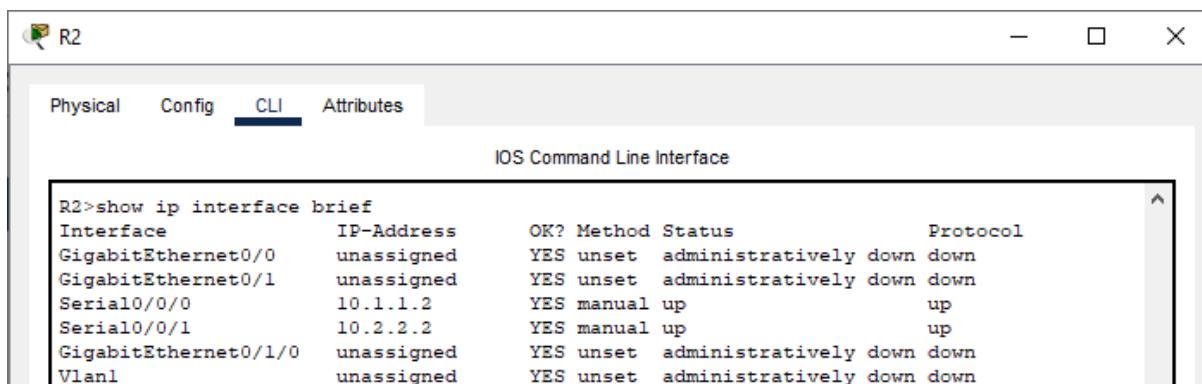
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface Serial0/0/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

➤ Displaying IP Address details in routers



R1>show ip interface brief

| Interface | IP-Address | OK? | Method | Status | Protocol |
|----------------------|-------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0 | 192.168.1.1 | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.1.1.1 | YES | manual | up | up |
| Serial0/0/1 | unassigned | YES | unset | administratively down | down |
| GigabitEthernet0/1/0 | unassigned | YES | unset | administratively down | down |
| Vlan1 | unassigned | YES | unset | administratively down | down |



R2>show ip interface brief

| Interface | IP-Address | OK? | Method | Status | Protocol |
|----------------------|------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0 | unassigned | YES | unset | administratively down | down |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.1.1.2 | YES | manual | up | up |
| Serial0/0/1 | 10.2.2.2 | YES | manual | up | up |
| GigabitEthernet0/1/0 | unassigned | YES | unset | administratively down | down |
| Vlan1 | unassigned | YES | unset | administratively down | down |

R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R3>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.3.1    YES manual up        up
GigabitEthernet0/1  unassigned     YES unset administratively down down
Serial0/0/0         10.2.2.1      YES manual up        up
Serial0/0/1         unassigned     YES unset administratively down down
GigabitEthernet0/1/0 unassigned     YES unset administratively down down
Vlan1              unassigned     YES unset administratively down down
```

➤ Configuring router

R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#^Z
R1#
*SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#^Z
R2#
*SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

➤ Showing IP route

R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:14, Serial0/0/0
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
R 192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:14, Serial0/0/0

R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.2/32 is directly connected, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.2/32 is directly connected, Serial0/0/1
R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:22, Serial0/0/0
R 192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:09, Serial0/0/1

```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:06, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/0
L        10.2.2.1/32 is directly connected, Serial0/0/0
R        192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:06, Serial0/0/0
          192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

➤ Configure SSH on R2

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip domain-name securityincomputing.com
R2(config)#username admin secret pwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

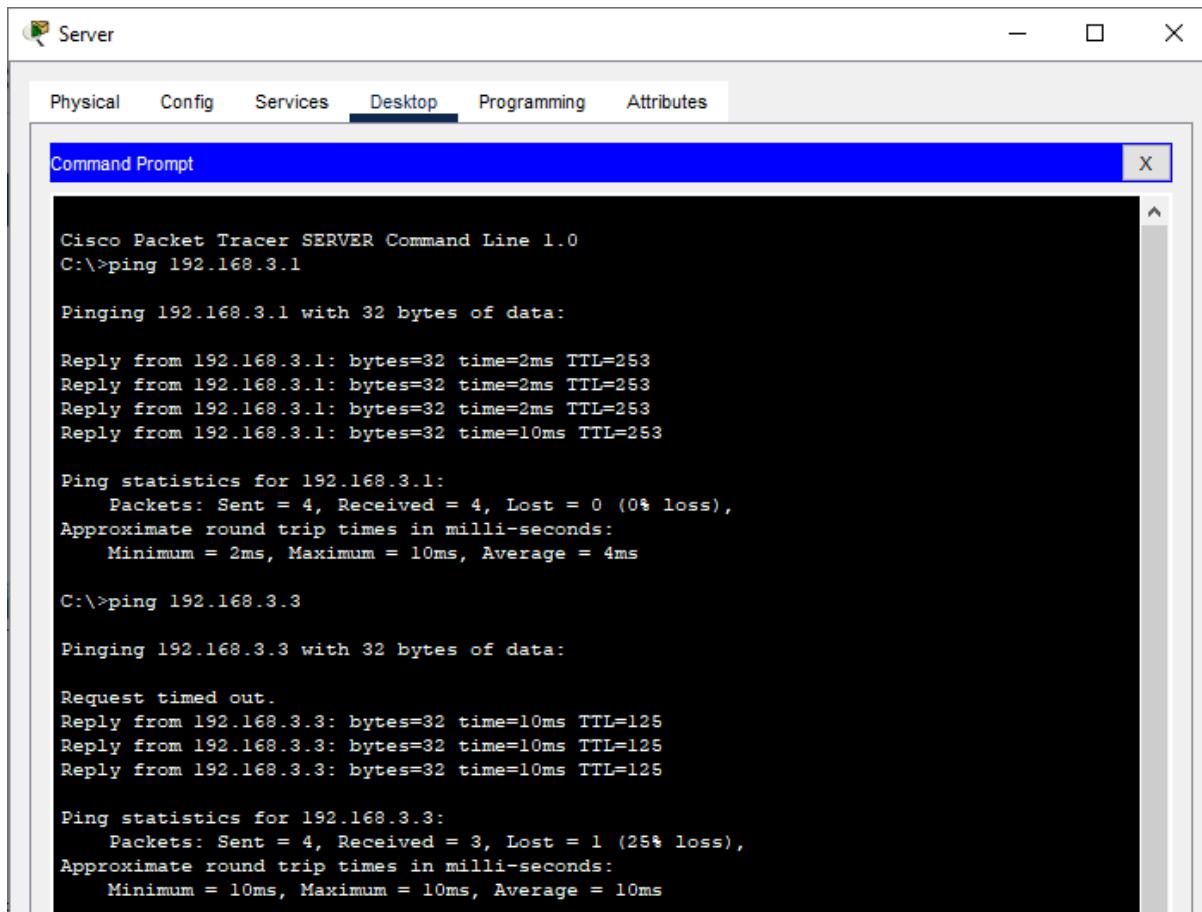
R2(config)#crypto key generate rsa
The name for the keys will be: R2.securityincomputing.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

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

R2(config)#ip ssh time-out 90
*Mar 1 0:7:55.157: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
R2(config)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

➤ **Verify basic network connectivity before ACL configuration**



The screenshot shows a Cisco Packet Tracer SERVER Command Line window. It displays the output of several ping commands. The first set of pings is to 192.168.3.1, showing four successful replies with times ranging from 2ms to 10ms. The second set of pings is to 192.168.3.3, showing three successful replies with times ranging from 10ms to 10ms, and one request timed out. The third set of pings is to 192.168.3.3, showing three successful replies with times ranging from 10ms to 10ms, and one lost packet (25% loss).

```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=2ms TTL=253
Reply from 192.168.3.1: bytes=32 time=10ms TTL=253

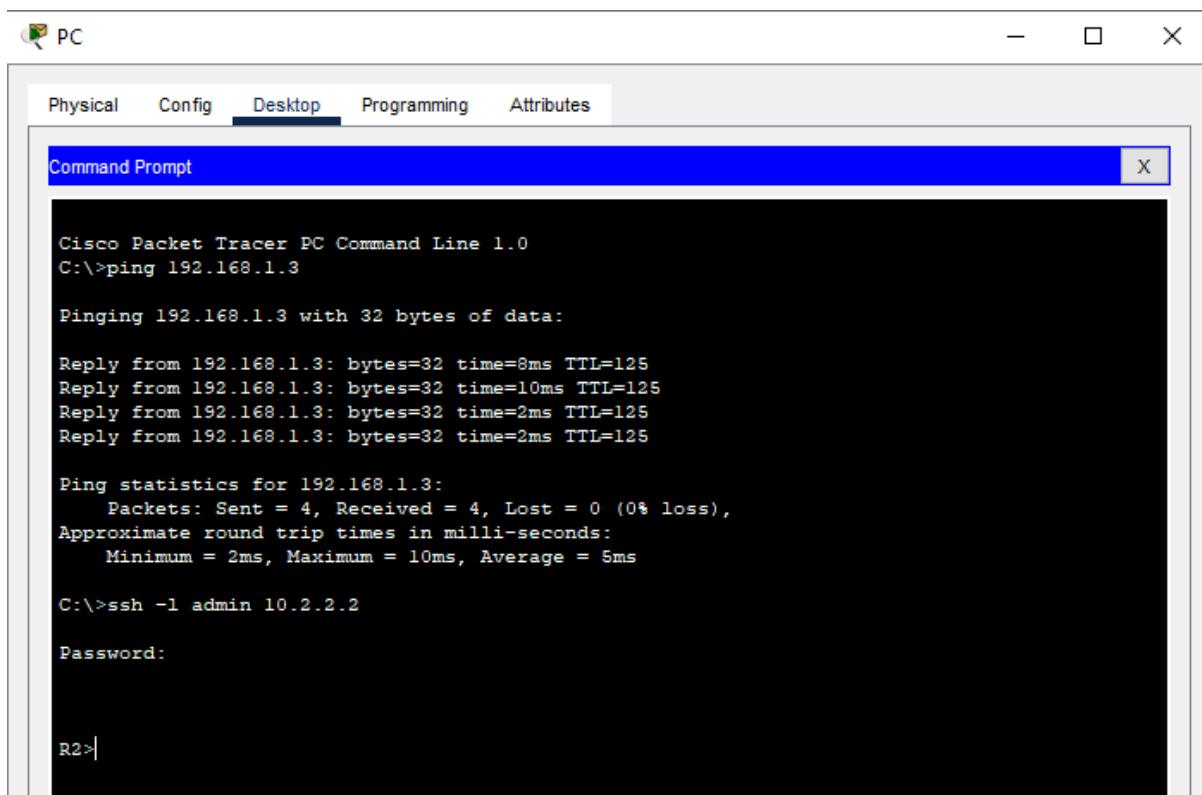
Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 4ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```



The screenshot shows a Cisco Packet Tracer PC Command Line window. It displays the output of a ping command to 192.168.1.3 and an SSH session attempt to 10.2.2.2. The ping command shows four successful replies with times ranging from 8ms to 10ms. The SSH session attempt shows a password prompt and a partially visible R2> prompt.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

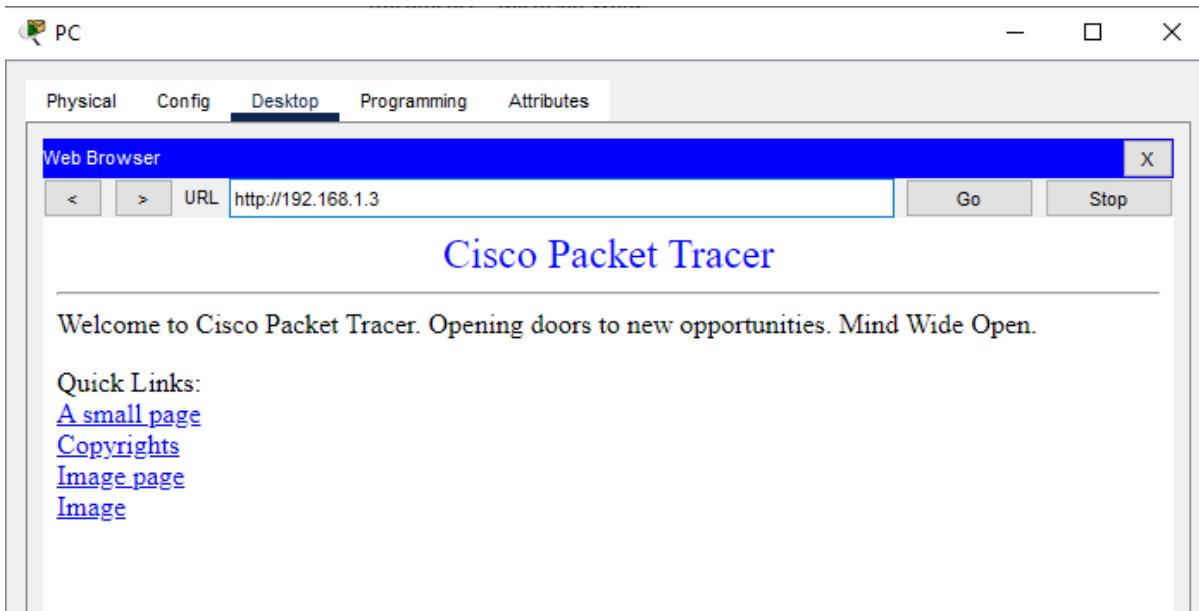
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=8ms TTL=125
Reply from 192.168.1.3: bytes=32 time=10ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125

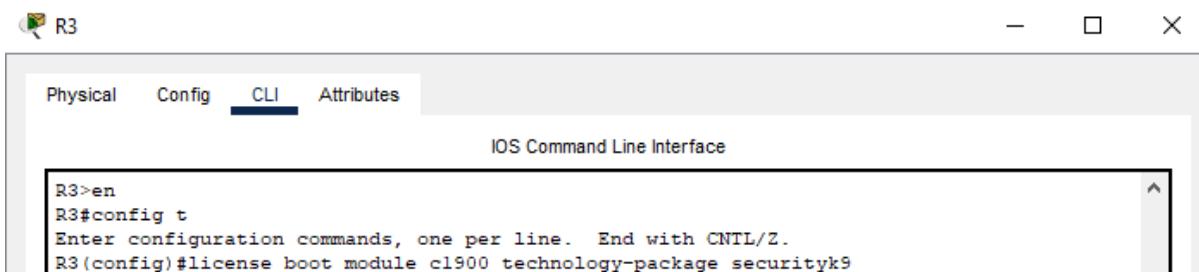
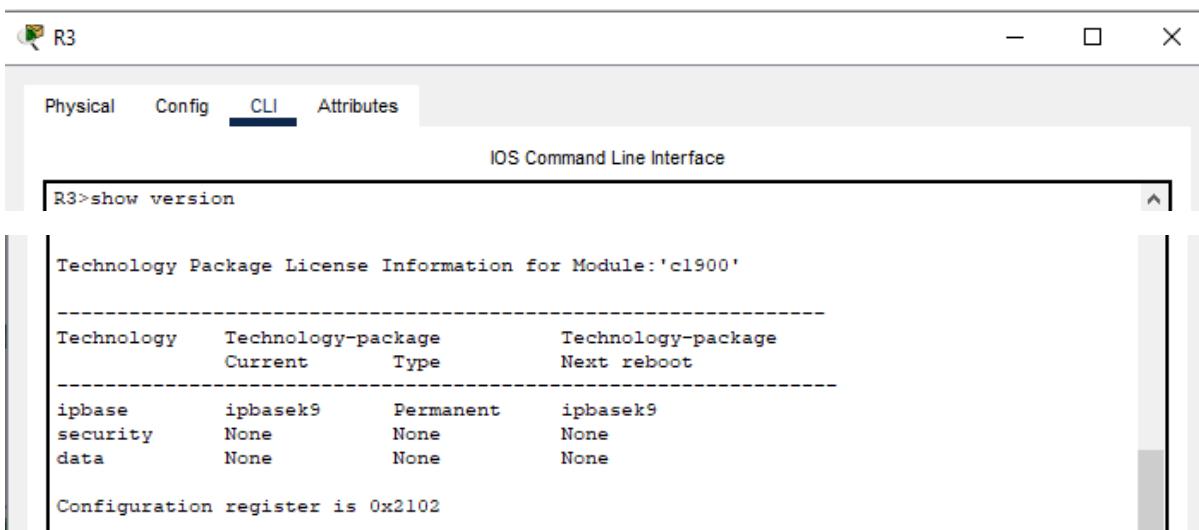
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 5ms

C:\>ssh -l admin 10.2.2.2
Password:

R2>
```



➤ **Enable the security technology package on R**



```
ACCEPT? [yes/no]: yes
# use 'write' command to make license boot config take effect on next boot

R3(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next
reboot level = securityk9 and License = securityk9

R3(config)#exit
R3#
*SYS-5-CONFIG_I: Configured from console by console

R3#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

R3

Physical Config **CLI** Attributes

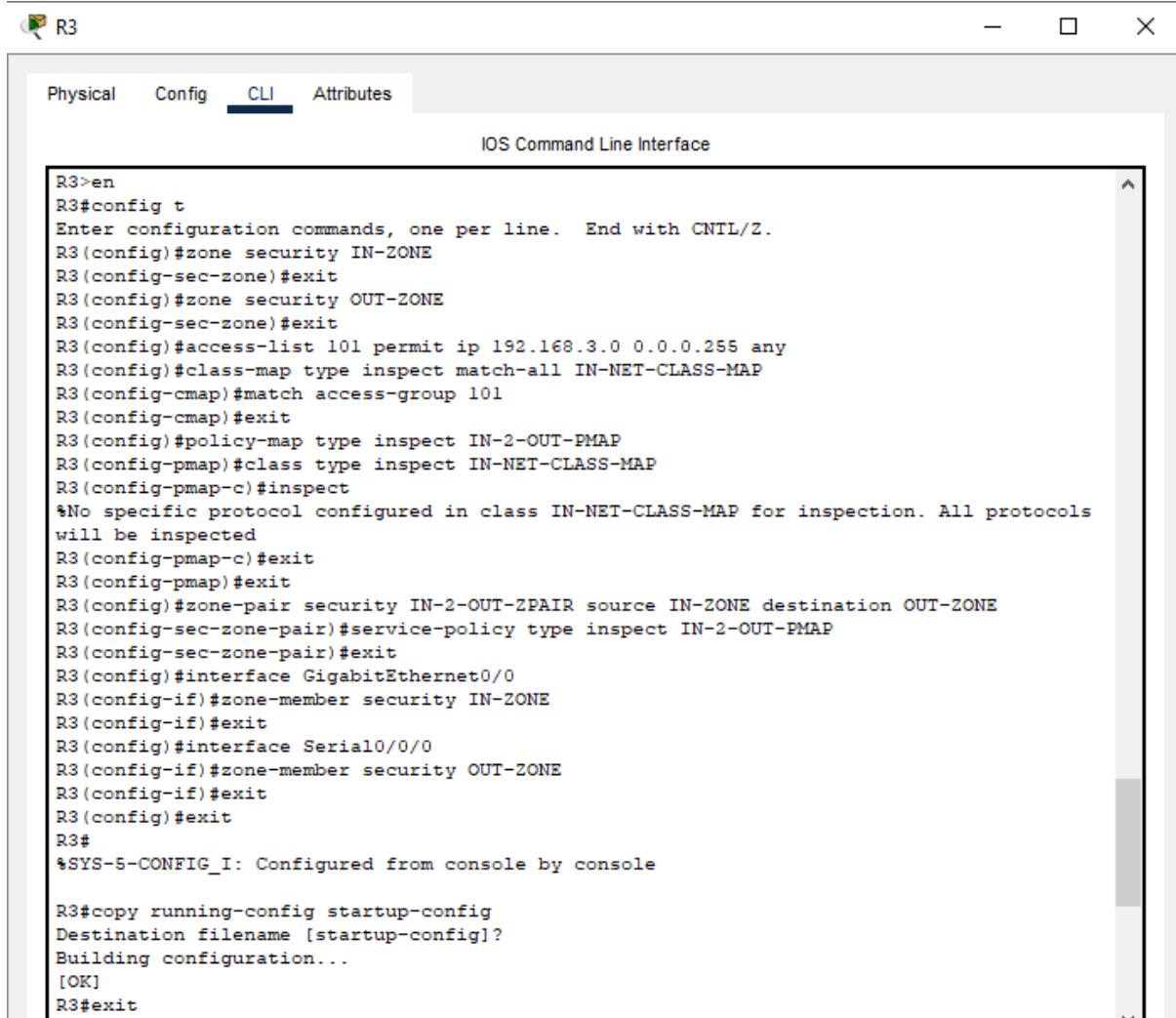
IOS Command Line Interface

```
R3>show version

Technology Package License Information for Module:'c1900'
-----
Technology      Technology-package          Technology-package
                Current        Type            Next reboot
-----
ipbase         ipbasek9      Permanent      ipbasek9
security       securityk9     Evaluation    securityk9
data           disable       None          None

Configuration register is 0x2102
```

➤ **Create the Firewall Zones , Class Maps and ACLs on R3**

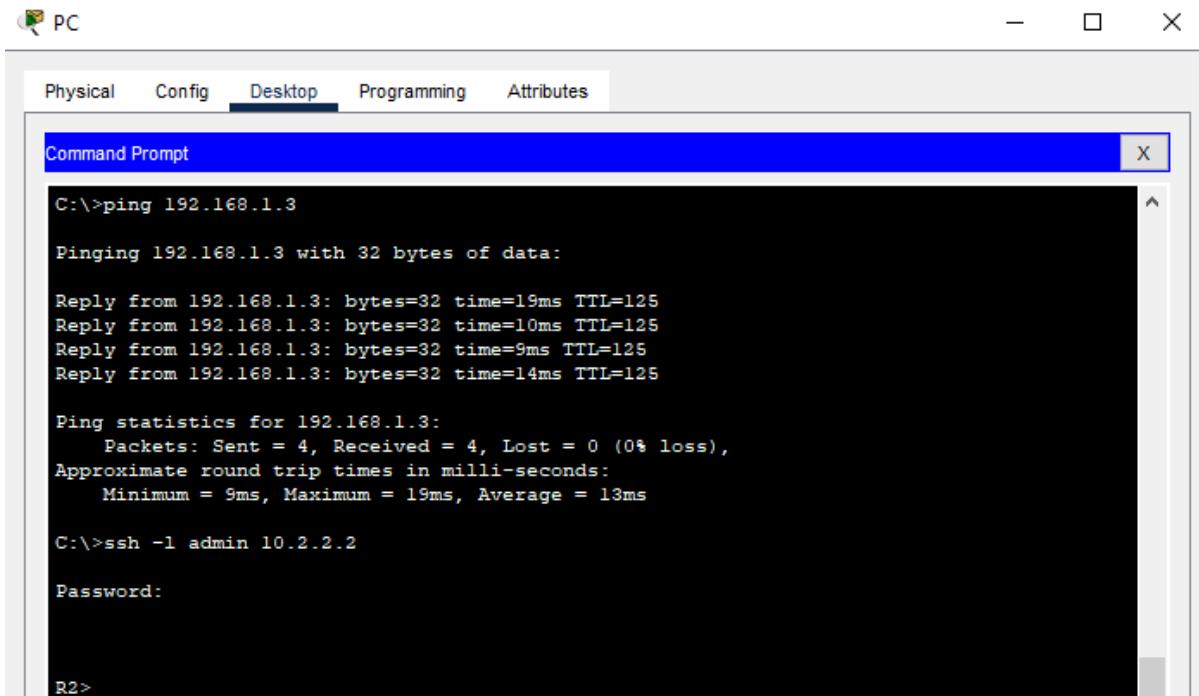


The screenshot shows the CLI interface for a Cisco router named R3. The window title is "R3". The tabs at the top are "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area is titled "IOS Command Line Interface". The configuration commands entered are:

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#zone security IN-ZONE
R3(config-sec-zone)#exit
R3(config)#zone security OUT-ZONE
R3(config-sec-zone)#exit
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
R3(config)#class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)#match access-group 101
R3(config-cmap)#exit
R3(config)#policy-map type inspect IN-2-OUT-PMAP
R3(config-pmap)#class type inspect IN-NET-CLASS-MAP
R3(config-pmap-c)#inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols
will be inspected
R3(config-pmap-c)#exit
R3(config-pmap)#exit
R3(config)#zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
R3(config-sec-zone-pair)#service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)#exit
R3(config)#interface GigabitEthernet0/0
R3(config-if)#zone-member security IN-ZONE
R3(config-if)#exit
R3(config)#interface Serial0/0/0
R3(config-if)#zone-member security OUT-ZONE
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

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

➤ **Test Firewall Functionality from IN-ZONE to OUT-ZONE**



PC

Physical Config Desktop Programming Attributes

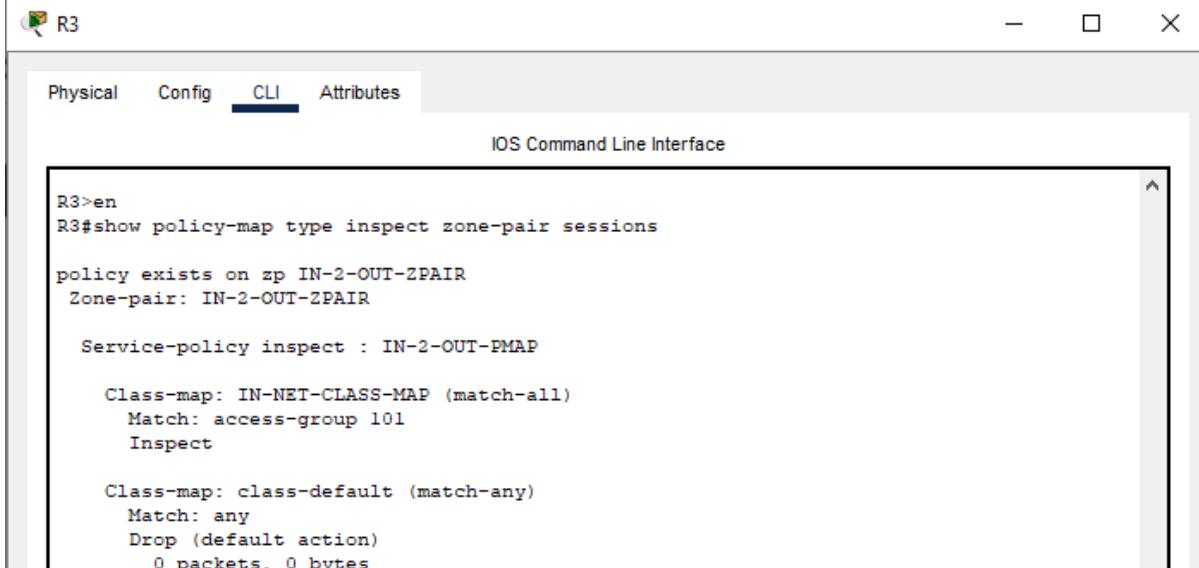
Command Prompt

```
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=19ms TTL=125
Reply from 192.168.1.3: bytes=32 time=10ms TTL=125
Reply from 192.168.1.3: bytes=32 time=9ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms 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 = 9ms, Maximum = 19ms, Average = 13ms

C:\>ssh -l admin 10.2.2.2
Password:

R2>
```



R3

Physical Config CLI Attributes

IOS Command Line Interface

```
R3>en
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR

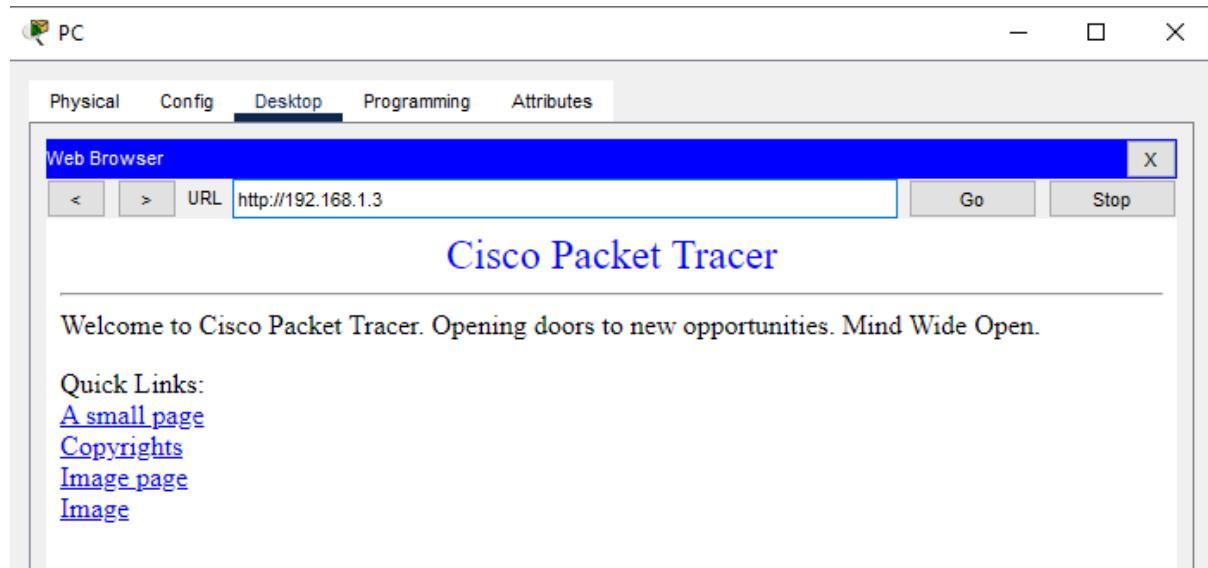
Service-policy inspect : IN-2-OUT-PMAP

Class-map: IN-NET-CLASS-MAP (match-all)
Match: access-group 101
Inspect

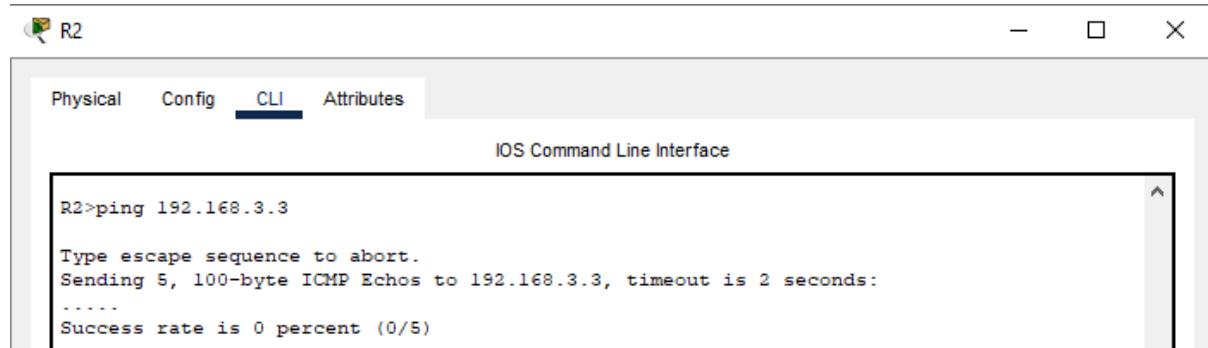
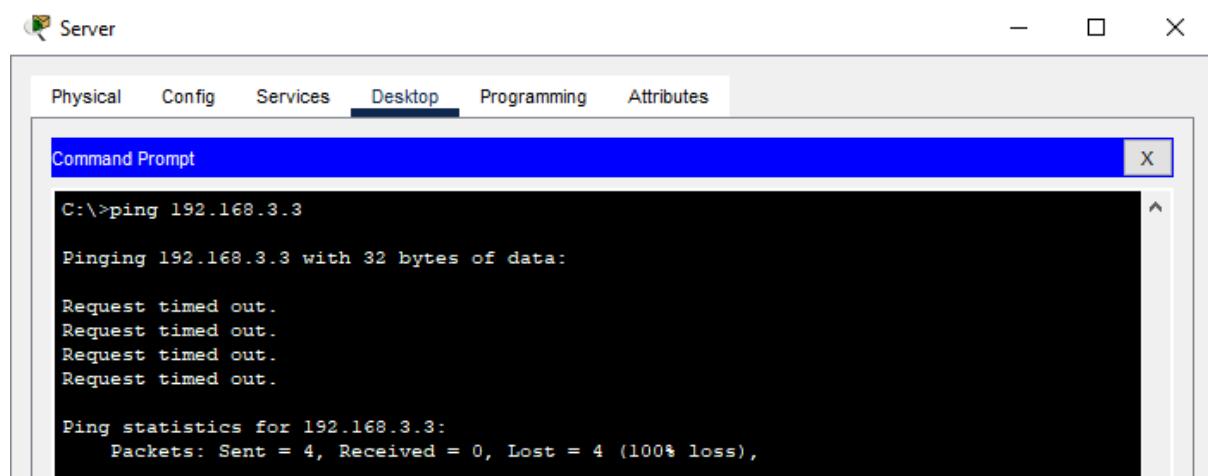
Class-map: class-default (match-any)
Match: any
Drop (default action)
  0 packets, 0 bytes
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 28.01.2025



➤ Test Firewall Functionality from OUT-ZONE to IN-ZONE

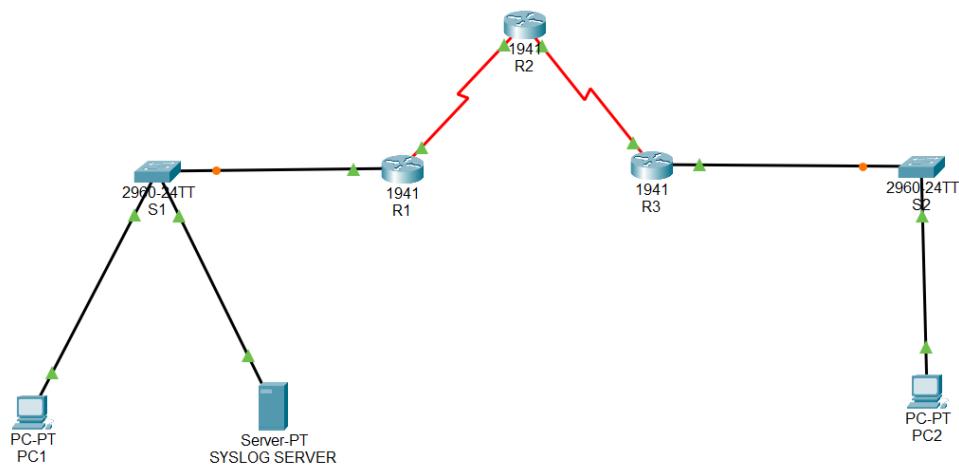


Practical 6

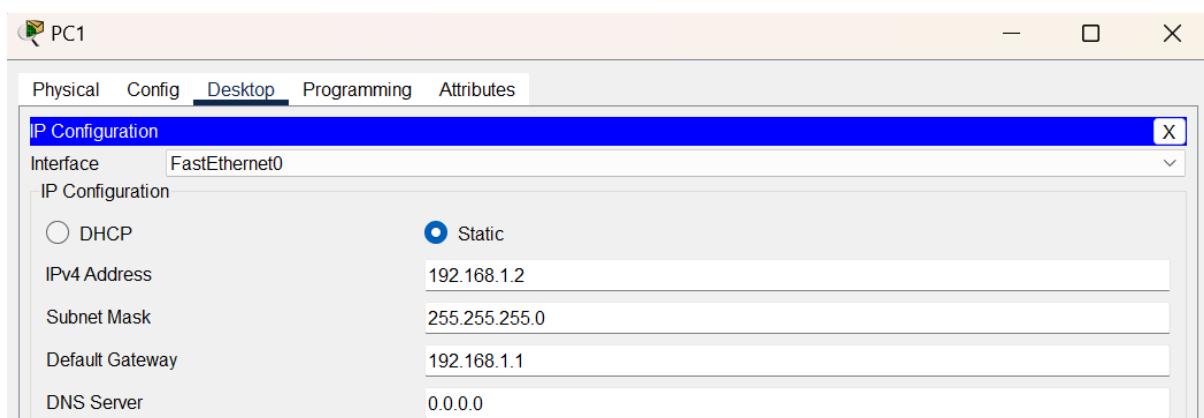
Aim: Configure IOS Intrusion Prevention System (IPS) using the CLI.

- Enable IOS IPS.
- Modify an IPS Signature.

➤ Topology Diagram

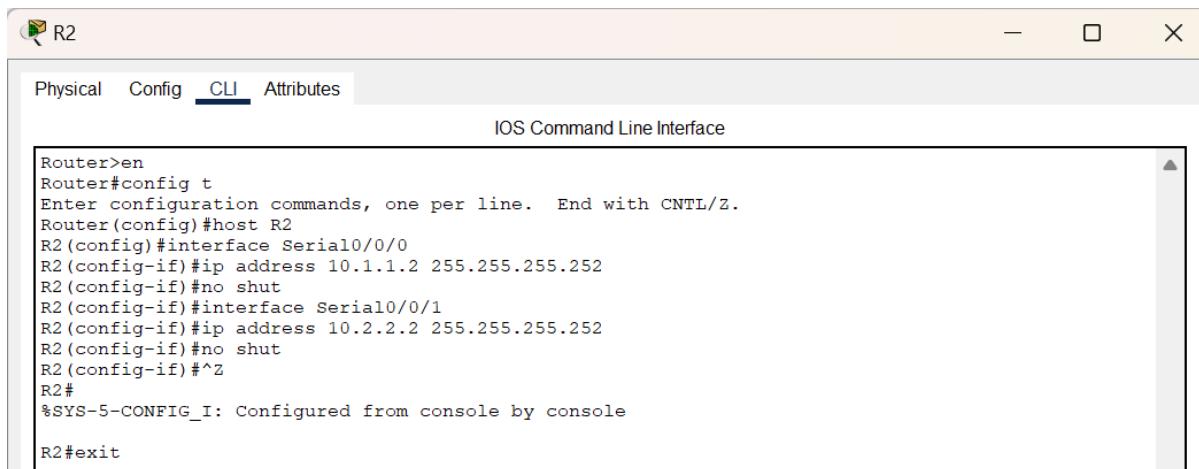
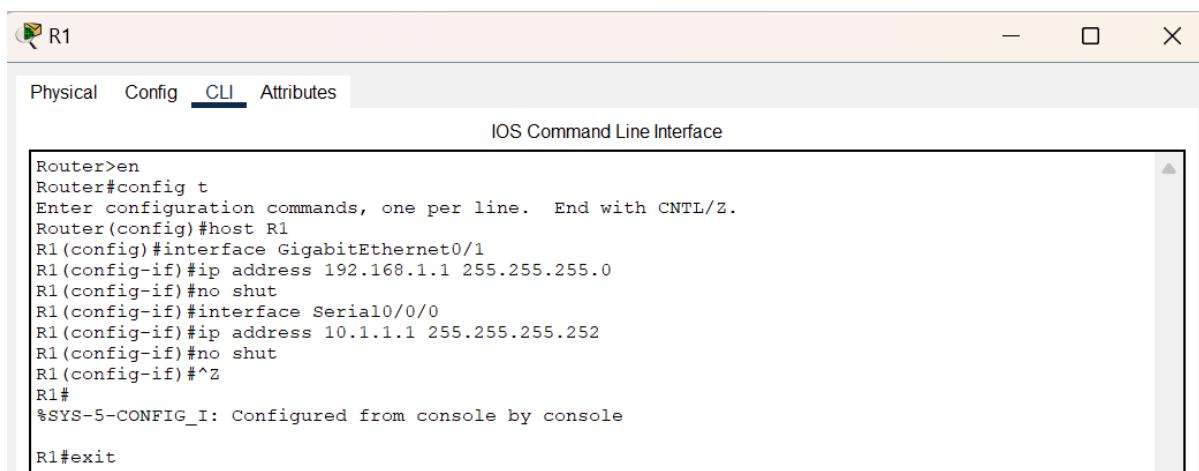
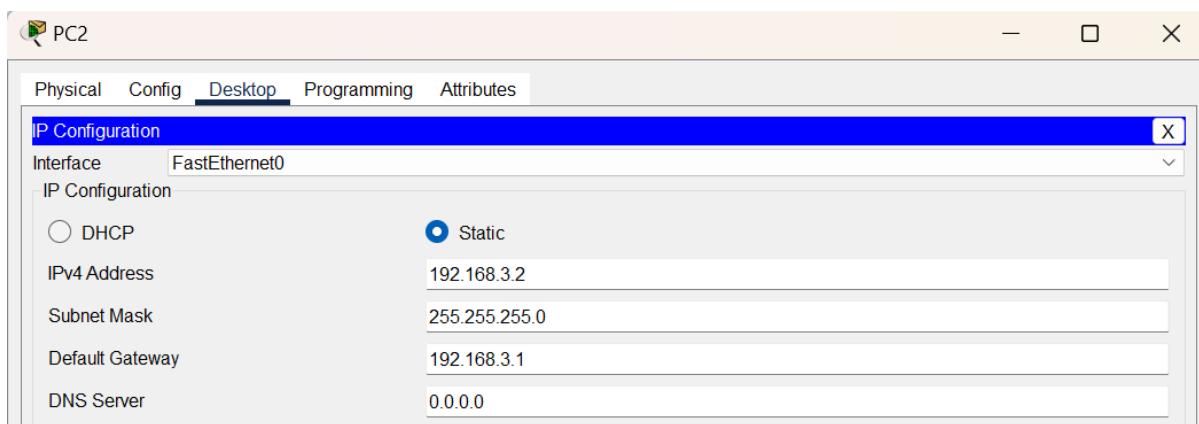
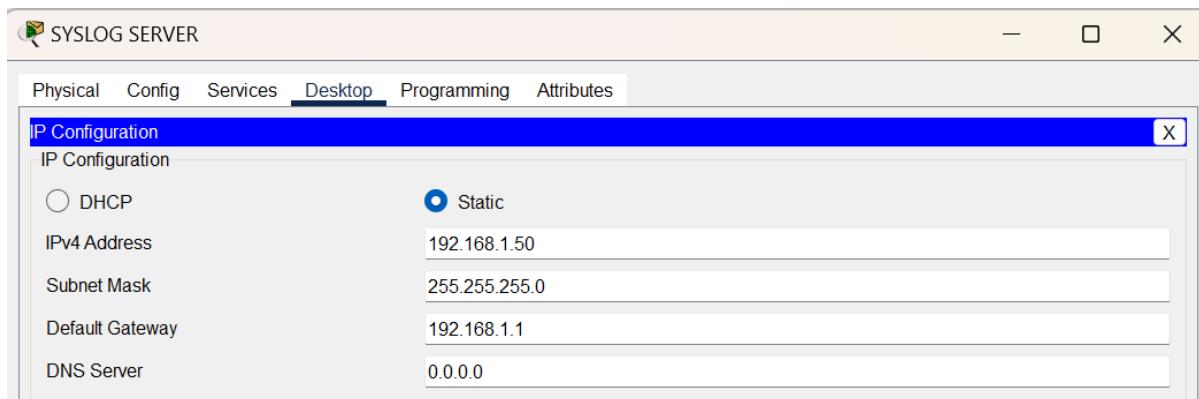


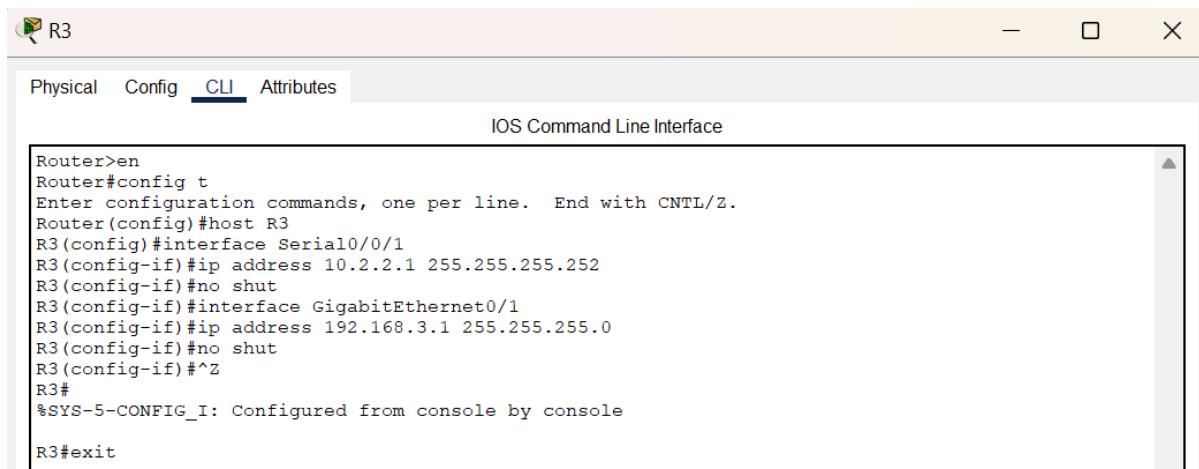
➤ Assigning IP Addresses



Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 04.02.2025





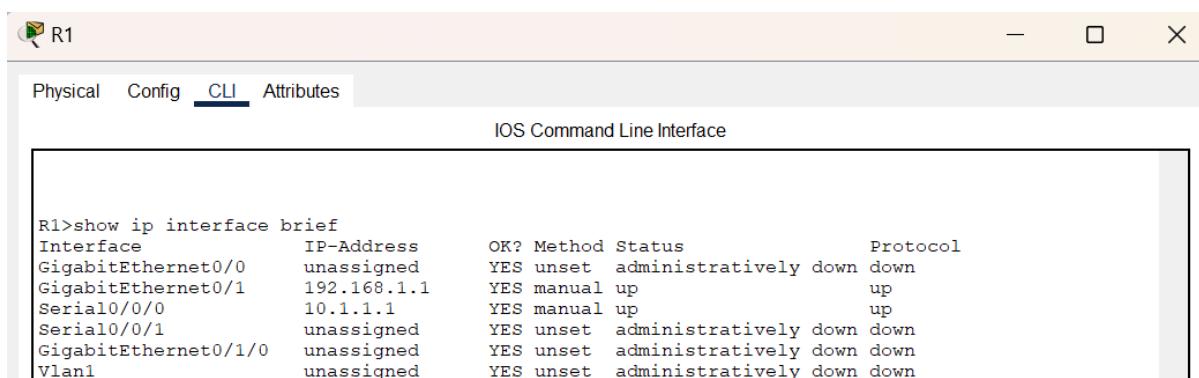
R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R3
R3(config)#interface Serial0/0/1
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#interface GigabitEthernet0/1
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ Displaying IP Address Details of Routers

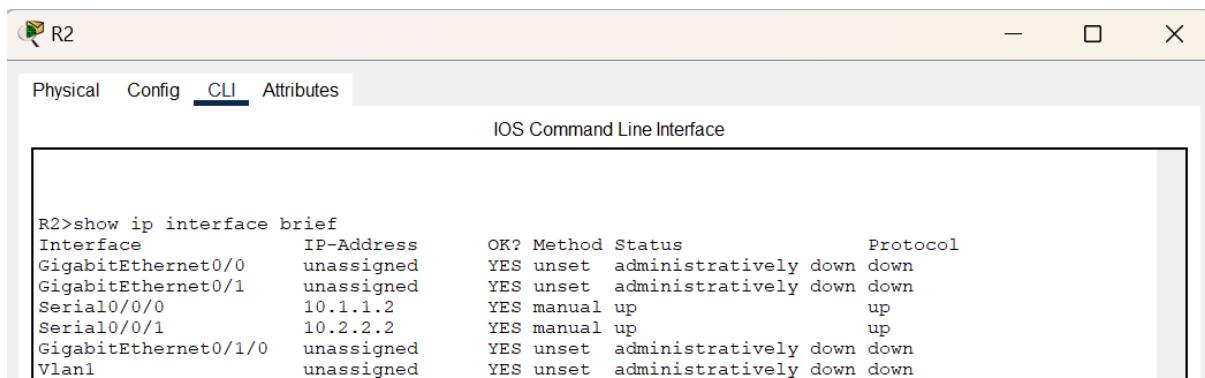


R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>show ip interface brief
Interface          IP-Address      OK? Method Status           Protocol
GigabitEthernet0/0  unassigned     YES unset administratively down down
GigabitEthernet0/1  192.168.1.1   YES manual up             up
Serial0/0/0         10.1.1.1     YES manual up             up
Serial0/0/1         unassigned    YES unset administratively down down
GigabitEthernet0/1/0 unassigned    YES unset administratively down down
Vlan1              unassigned    YES unset administratively down down
```

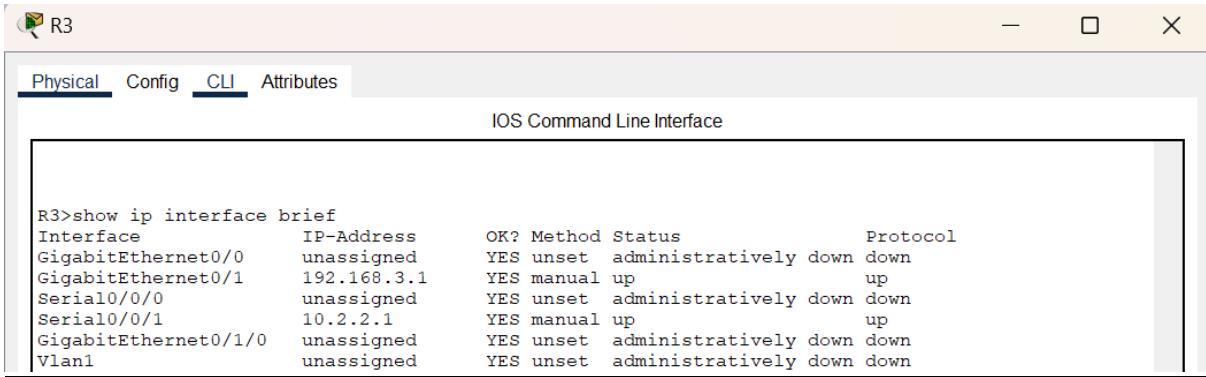


R2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R2>show ip interface brief
Interface          IP-Address      OK? Method Status           Protocol
GigabitEthernet0/0  unassigned     YES unset administratively down down
GigabitEthernet0/1  unassigned    YES unset administratively down down
Serial0/0/0         10.1.1.2     YES manual up             up
Serial0/0/1         10.2.2.2     YES manual up             up
GigabitEthernet0/1/0 unassigned    YES unset administratively down down
Vlan1              unassigned    YES unset administratively down down
```



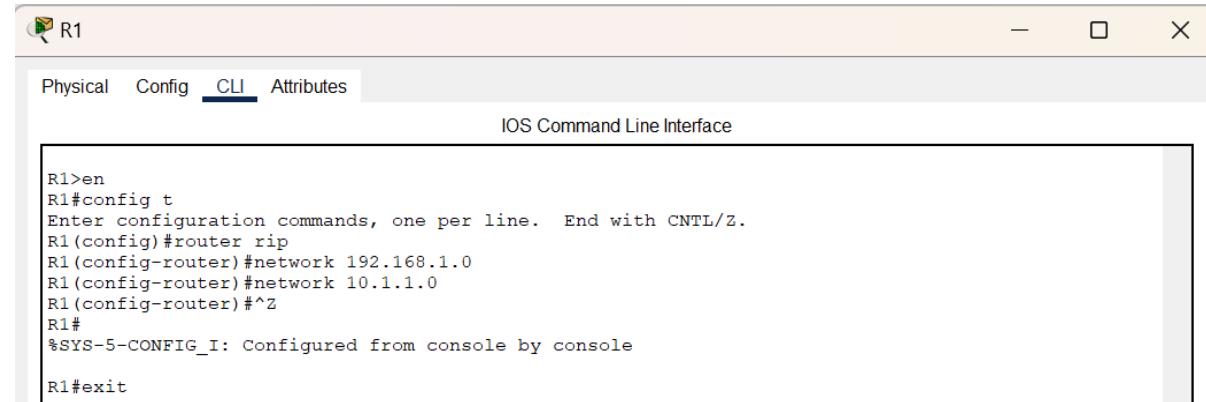
R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R3>show ip interface brief
Interface          IP-Address      OK? Method Status       Protocol
GigabitEthernet0/0  unassigned      YES unset administratively down down
GigabitEthernet0/1  192.168.3.1    YES manual up        up
Serial0/0/0         unassigned      YES unset administratively down down
Serial0/0/1         10.2.2.1      YES manual up        up
GigabitEthernet0/1/0 unassigned      YES unset administratively down down
Vlan1              unassigned      YES unset administratively down down
```

➤ Configuring RIP on Routers

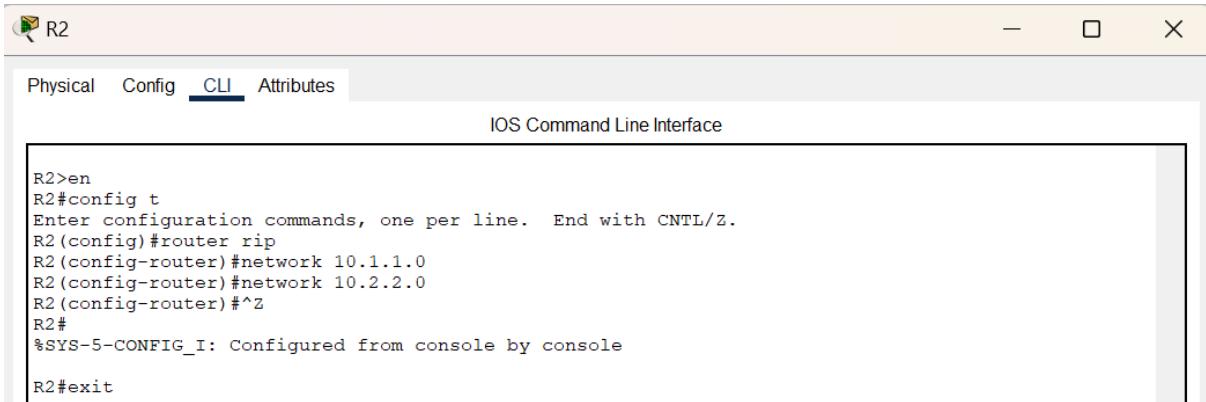


R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#+Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

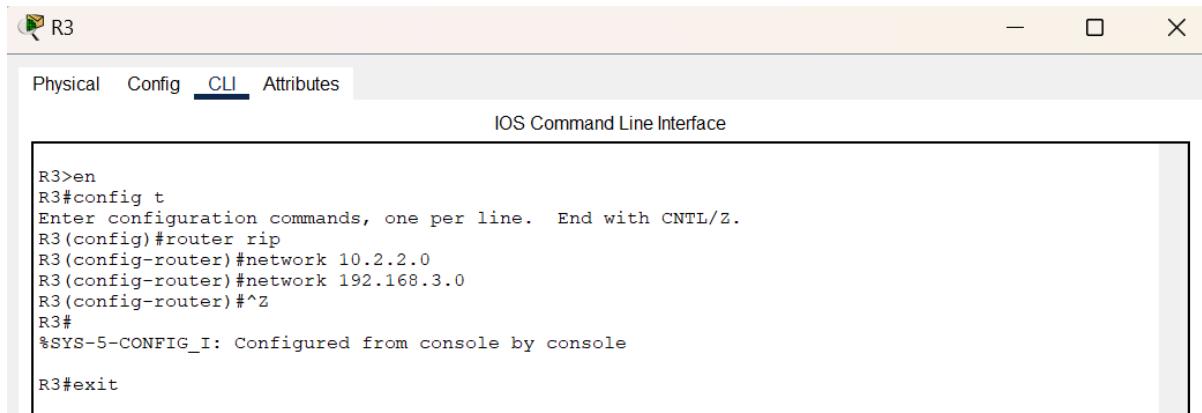


R2

Physical Config **CLI** Attributes

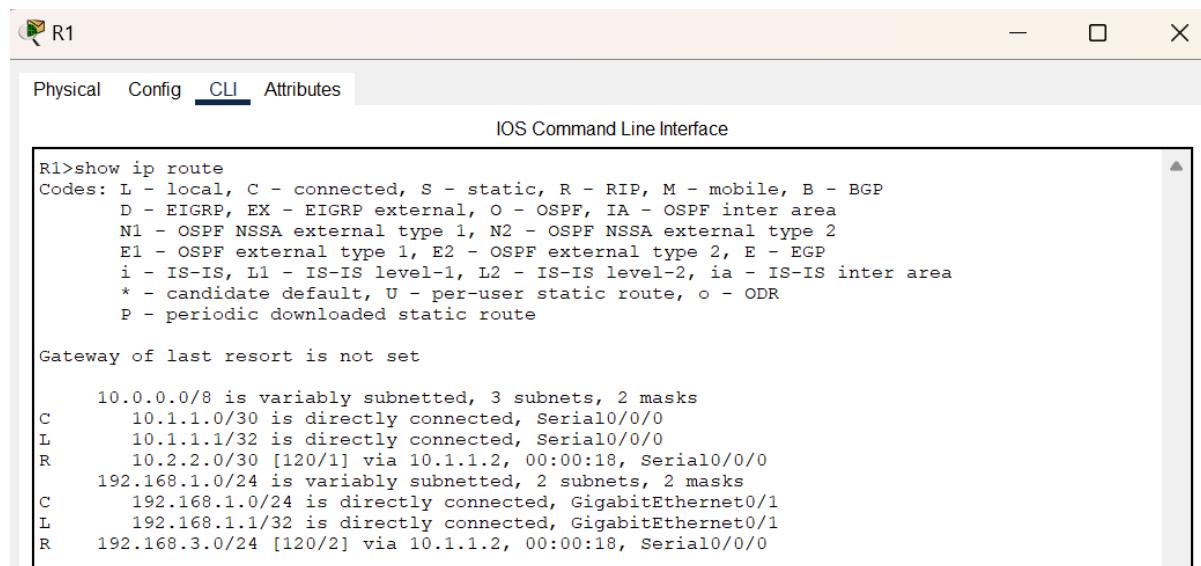
IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#+Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```



R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

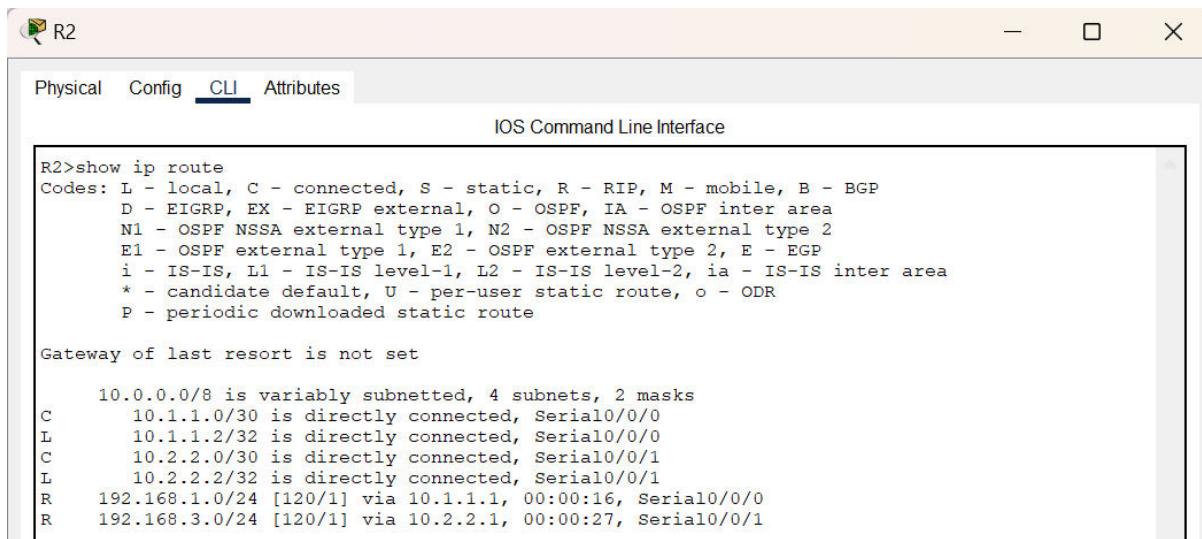
➤ Displaying Routing Table of Routers



R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:18, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
R 192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:18, Serial0/0/0



R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.2/32 is directly connected, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.2/32 is directly connected, Serial0/0/1
R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:16, Serial0/0/0
R 192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:27, Serial0/0/1

```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:07, Serial0/0/1
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
R        192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:07, Serial0/0/1
          192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C          192.168.3.0/24 is directly connected, GigabitEthernet0/1
L          192.168.3.1/32 is directly connected, GigabitEthernet0/1
```

➤ Verifying Full Network Connectivity

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

Reply from 192.168.1.50: bytes=32 time<1ms TTL=128
Reply from 192.168.1.50: bytes=32 time=4ms TTL=128
Reply from 192.168.1.50: bytes=32 time<1ms TTL=128
Reply from 192.168.1.50: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.50:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```



```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=21ms TTL=125
Reply from 192.168.3.2: bytes=32 time=10ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 8ms
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 04.02.2025

PC2

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:

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=3ms 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 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

Reply from 192.168.1.50: bytes=32 time=27ms TTL=125
Reply from 192.168.1.50: bytes=32 time=3ms TTL=125
Reply from 192.168.1.50: bytes=32 time=3ms TTL=125
Reply from 192.168.1.50: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 27ms, Average = 8ms
```

SYSLOG SERVER

Physical Config Services Desktop Programming Attributes

Command Prompt

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

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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 = 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=14ms TTL=125
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 5ms
```

➤ Enable the Secure Technology Package on R1

```
R1>show version
```

```
Technology Package License Information for Module:'c1900'  
-----  
Technology      Technology-package      Technology-package  
    Current        Type            Next reboot  
-----  
ipbase         ipbasek9       Permanent     ipbasek9  
security        None           None          None  
data            None           None          None  
  
Configuration register is 0x2102
```

R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9

ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config) #: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot
level = securityk9 and License = securityk9

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#reload

Proceed with reload? [confirm] . . .
```

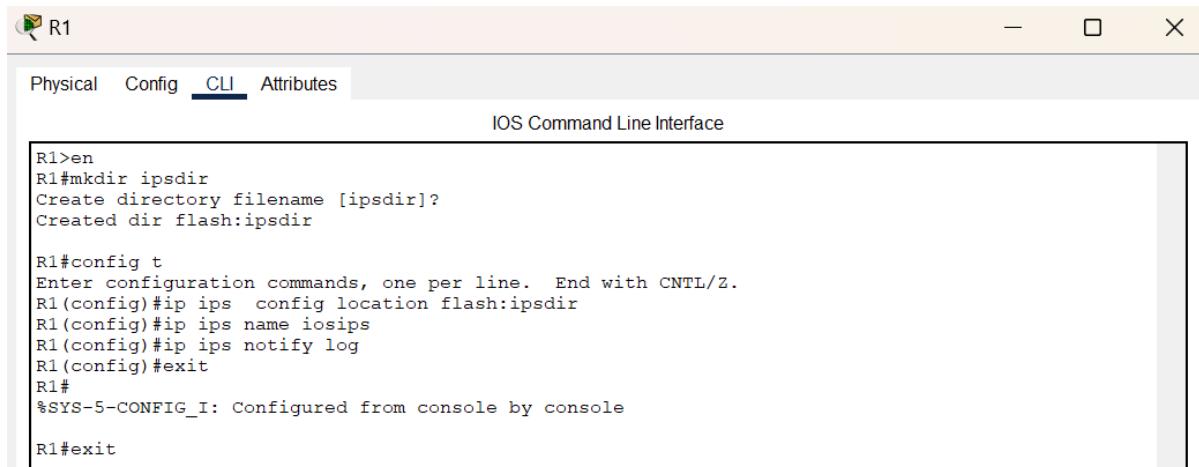
R1>show version

```
Technology Package License Information for Module:'c1900'  
-----  
Technology      Technology-package      Technology-package  
    Current        Type            Next reboot  
-----  
ipbase         ipbasek9       Permanent     ipbasek9
security        securityk9     Evaluation   securityk9
data            disable        None          None  
  
Configuration register is 0x2102
```

➤ **1. Enable IOS IPS on R1**

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

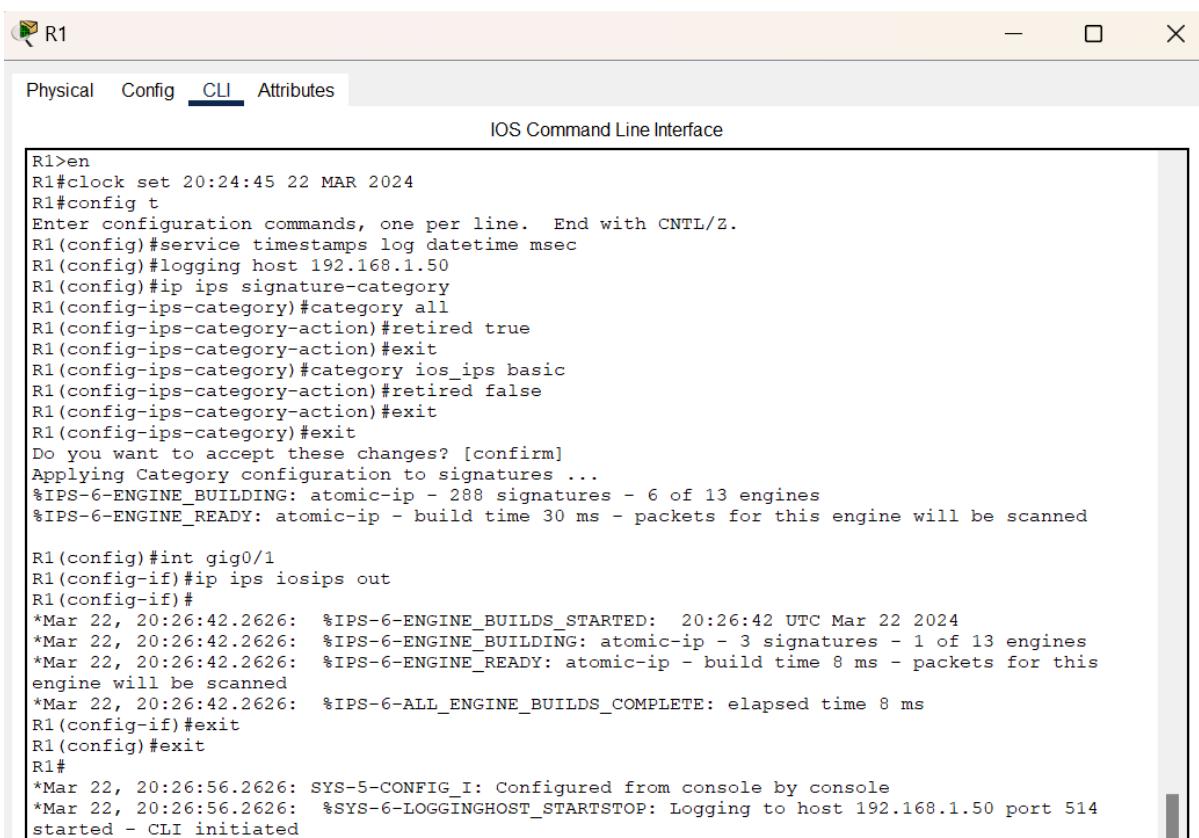
Subject: Information Security
Sem: VI
Date: 04.02.2025



R1>en
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit



R1>en
R1#clock set 20:24:45 22 MAR 2024
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.50
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

R1(config)#int gig0/1
R1(config-if)#ip ips iosips out
R1(config-if)#
*Mar 22, 20:26:42.2626: %IPS-6-ENGINE_BUILDS_STARTED: 20:26:42 UTC Mar 22 2024
*Mar 22, 20:26:42.2626: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Mar 22, 20:26:42.2626: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Mar 22, 20:26:42.2626: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
R1(config-if)#exit
R1(config)#exit
R1#
*Mar 22, 20:26:56.2626: SYS-5-CONFIG_I: Configured from console by console
*Mar 22, 20:26:56.2626: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port 514 started - CLI initiated

```
R1#show ip ips all
IPS Signature File Configuration Status
  Configured Config Locations: flash:ipsdir
  Last signature default load time:
  Last signature delta load time:
  Last event action (SEAP) load time: -none-

  General SEAP Config:
  Global Deny Timeout: 3600 seconds
  Global Overrides Status: Enabled
  Global Filters Status: Enabled

  IPS Auto Update is not currently configured

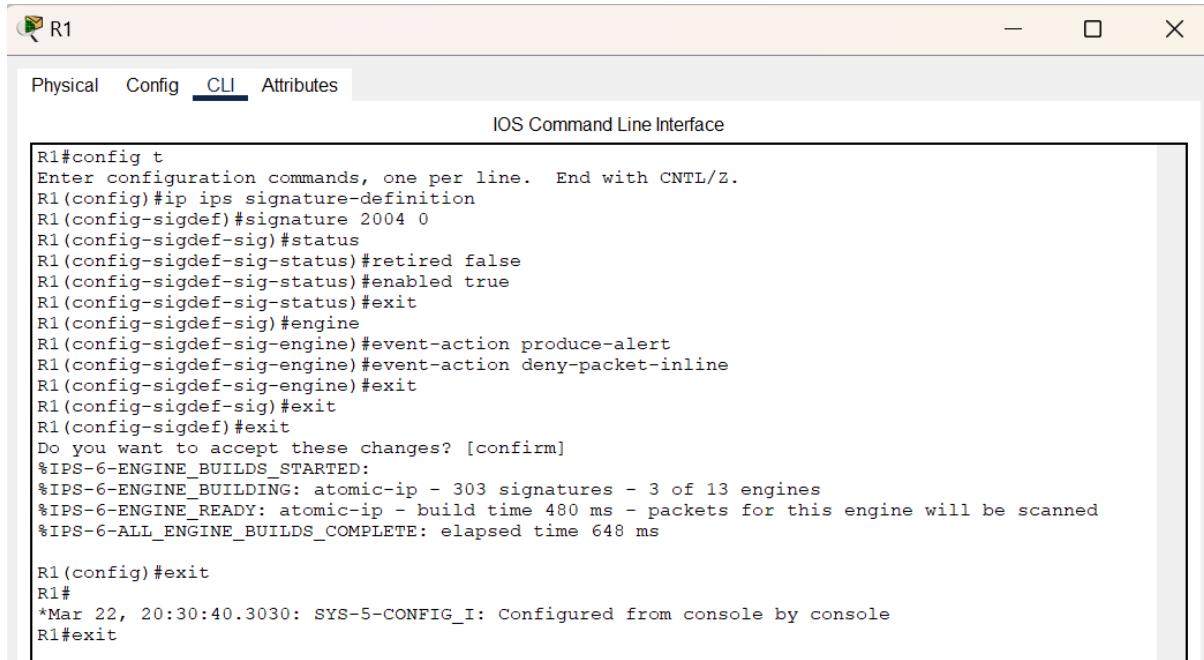
  IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

  IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

  IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
      IPS fail closed is disabled
      IPS deny-action ips-interface is false
      Fastpath ips is enabled
      Quick run mode is enabled
      Interface Configuration
        Interface GigabitEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

  IPS Category CLI Configuration:
    Category all
      Retire: True
    Category ios_ips basic
      Retire: False
```

➤ 2. Modify the Signatures of the IPS

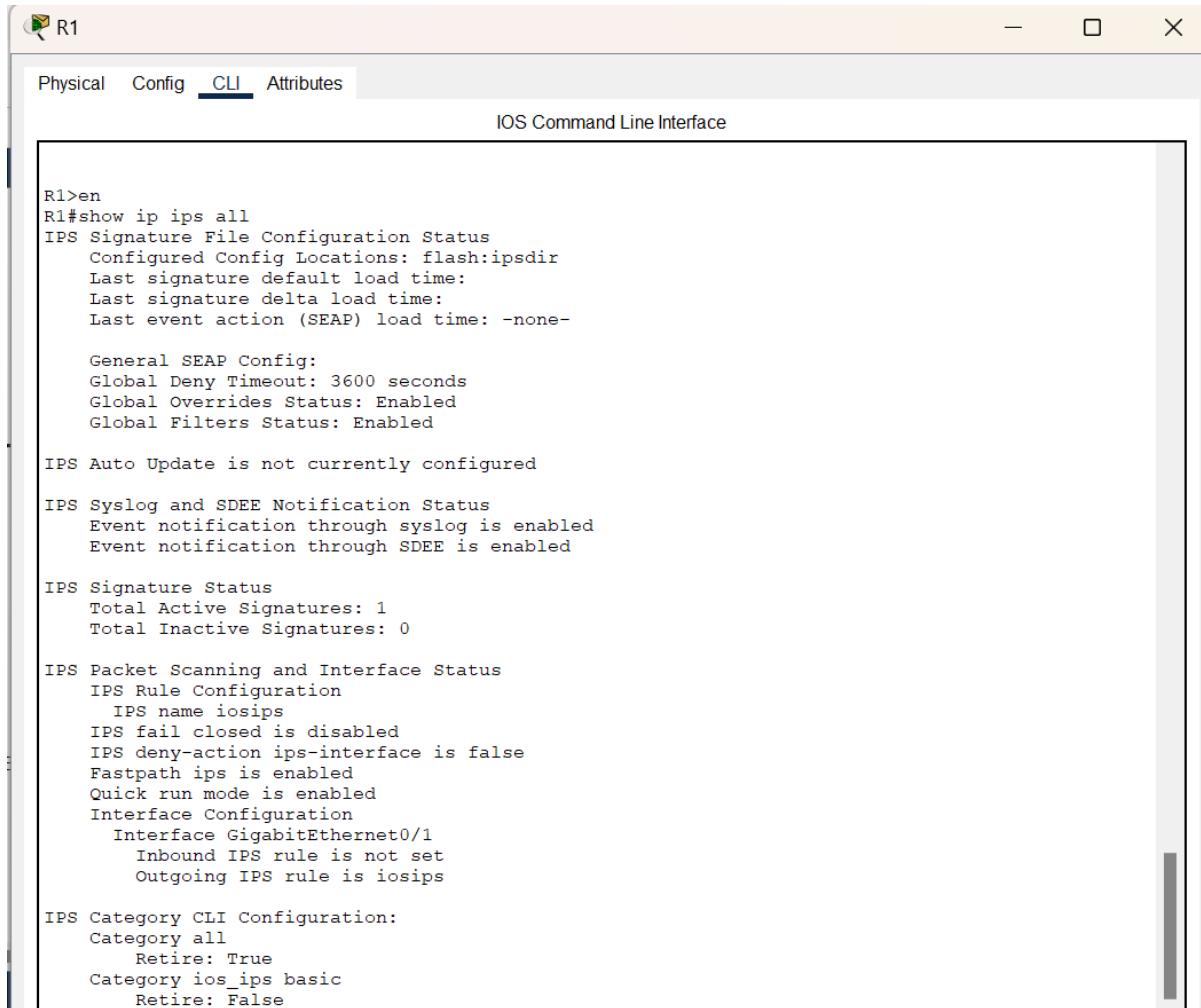


The screenshot shows a terminal window titled "R1". The window has tabs at the top: "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main area of the window displays the following command-line session:

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#exit
R1(config-sigdef-sig)#engine
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILD_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILD_COMPLETE: elapsed time 648 ms

R1(config)#exit
R1#
*Mar 22, 20:30:40.3030: SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

➤ Displaying the IPS Configuration Status Summary



R1>en
R1#show ip ips all
IPS Signature File Configuration Status
Configured Config Locations: flash:ipsdir
Last signature default load time:
Last signature delta load time:
Last event action (SEAP) load time: -none-

General SEAP Config:
Global Deny Timeout: 3600 seconds
Global Overrides Status: Enabled
Global Filters Status: Enabled

IPS Auto Update is not currently configured

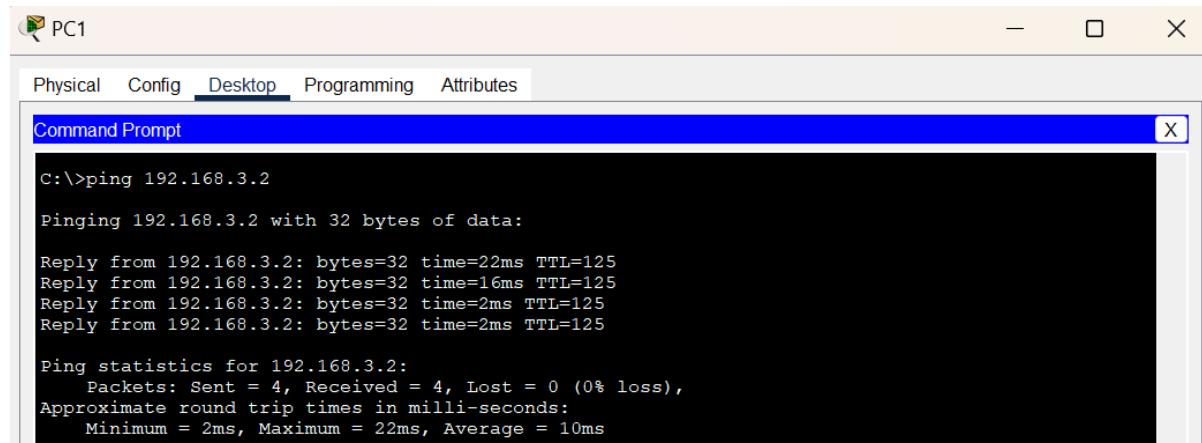
IPS Syslog and SDEE Notification Status
Event notification through syslog is enabled
Event notification through SDEE is enabled

IPS Signature Status
Total Active Signatures: 1
Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
IPS Rule Configuration
IPS name iosips
IPS fail closed is disabled
IPS deny-action ips-interface is false
Fastpath ips is enabled
Quick run mode is enabled
Interface Configuration
Interface GigabitEthernet0/1
Inbound IPS rule is not set
Outgoing IPS rule is iosips

IPS Category CLI Configuration:
Category all
Retire: True
Category ios_ips basic
Retire: False

➤ Verifying the Working of IPS

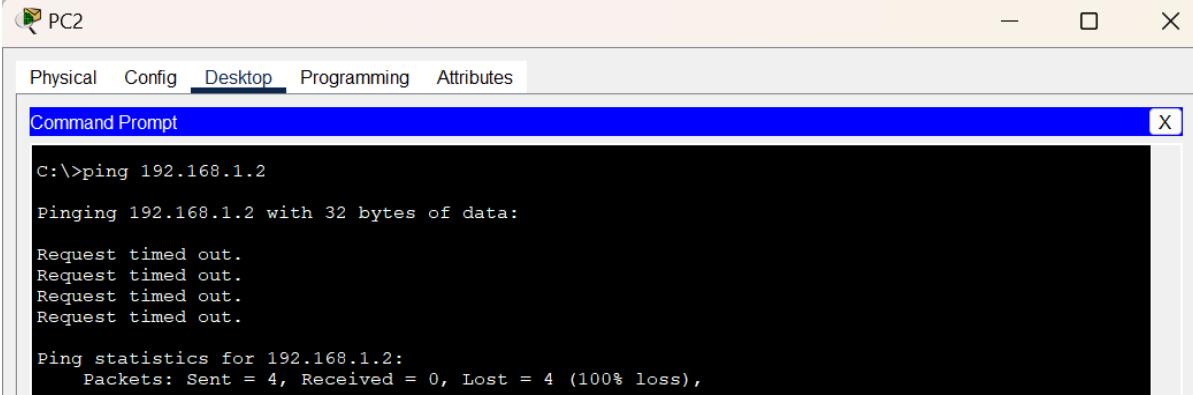


C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=22ms TTL=125
Reply from 192.168.3.2: bytes=32 time=16ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 22ms, Average = 10ms

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 04.02.2025



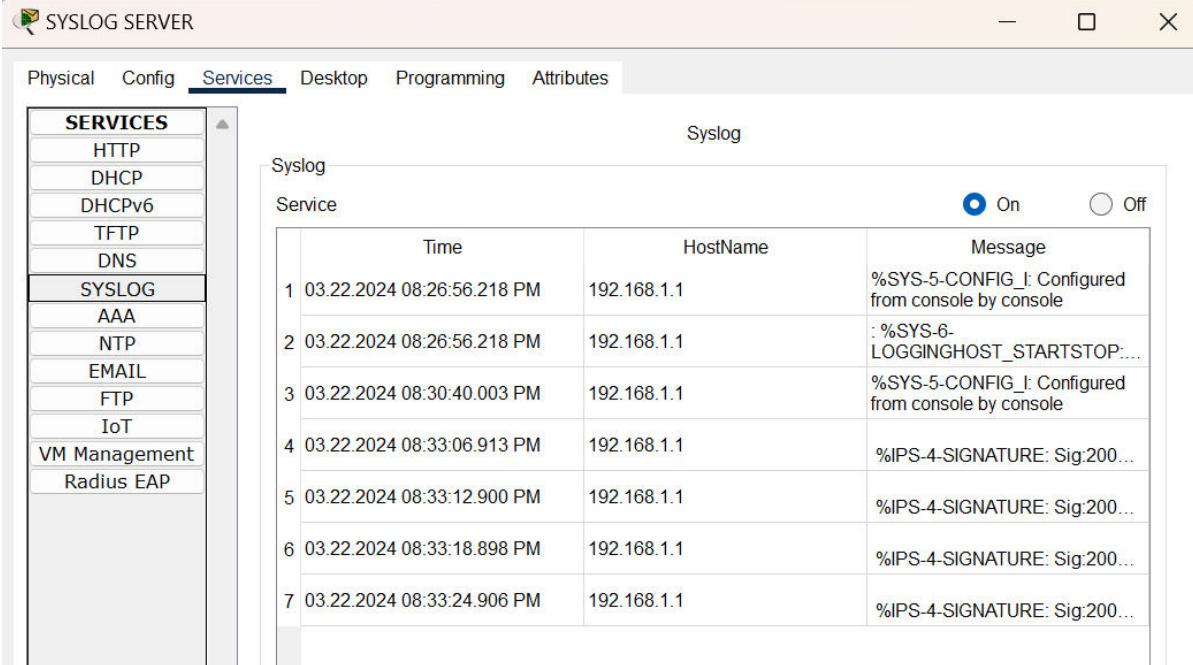
PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
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),
```



SYSLOG SERVER

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG**
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

Syslog

Service

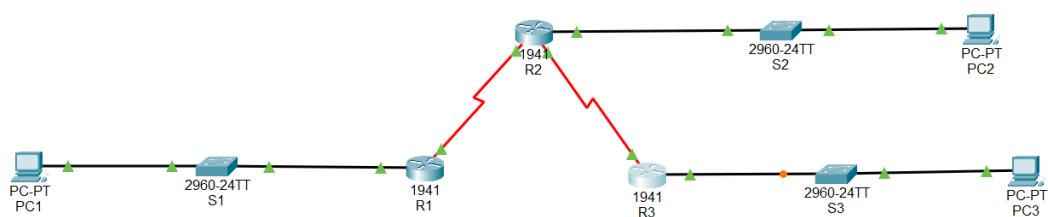
On Off

| | Time | HostName | Message |
|---|----------------------------|-------------|---|
| 1 | 03.22.2024 08:26:56.218 PM | 192.168.1.1 | %SYS-5-CONFIG_I: Configured from console by console |
| 2 | 03.22.2024 08:26:56.218 PM | 192.168.1.1 | : %SYS-6-LOGGINGHOST_STARTSTOP:... |
| 3 | 03.22.2024 08:30:40.003 PM | 192.168.1.1 | %SYS-5-CONFIG_I: Configured from console by console |
| 4 | 03.22.2024 08:33:06.913 PM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 5 | 03.22.2024 08:33:12.900 PM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 6 | 03.22.2024 08:33:18.898 PM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |
| 7 | 03.22.2024 08:33:24.906 PM | 192.168.1.1 | %IPS-4-SIGNATURE: Sig:200... |

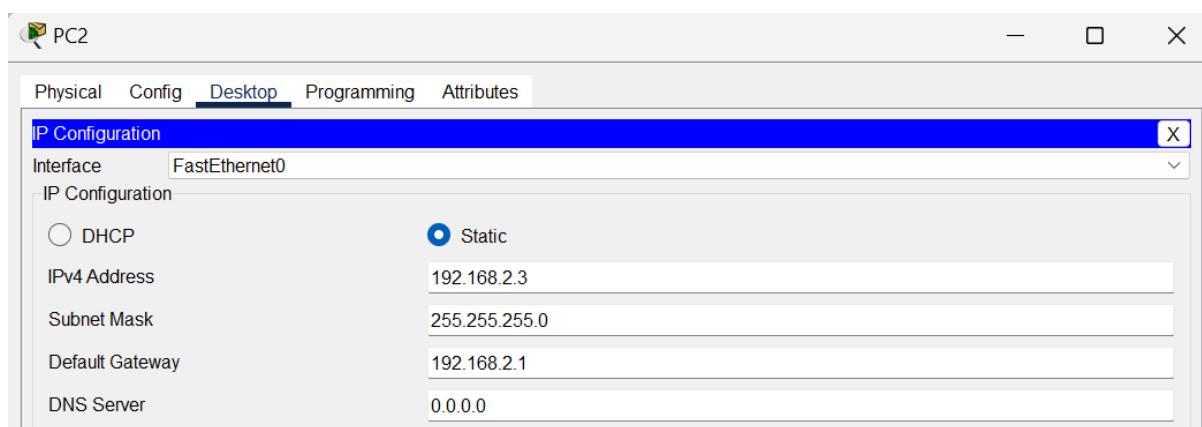
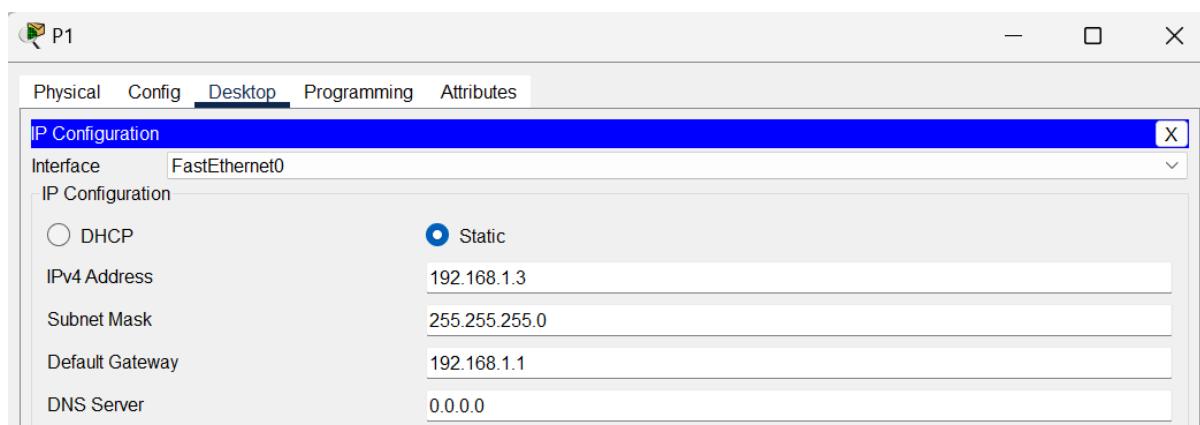
Practical 7

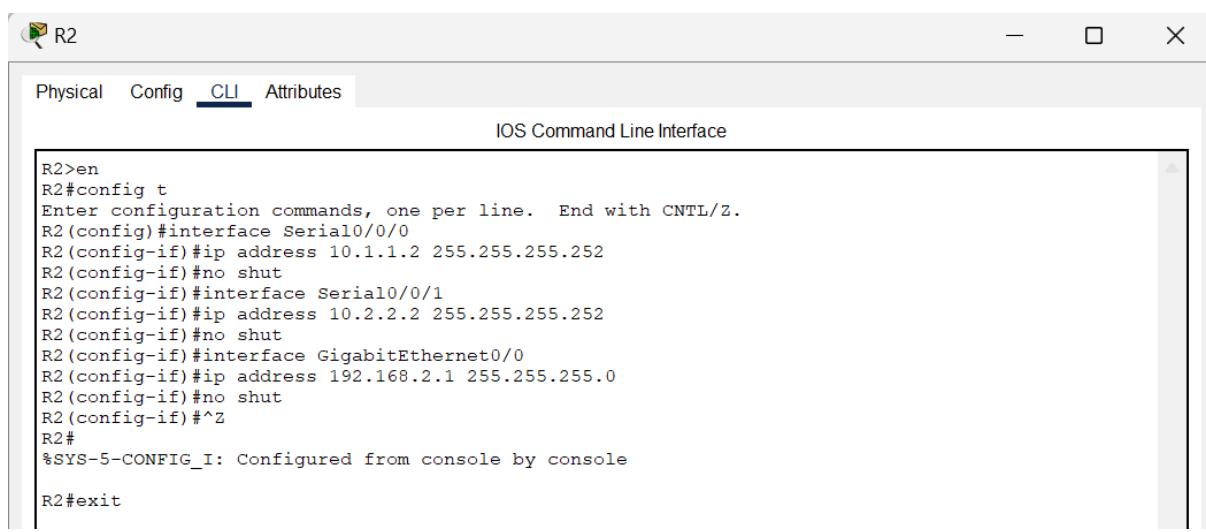
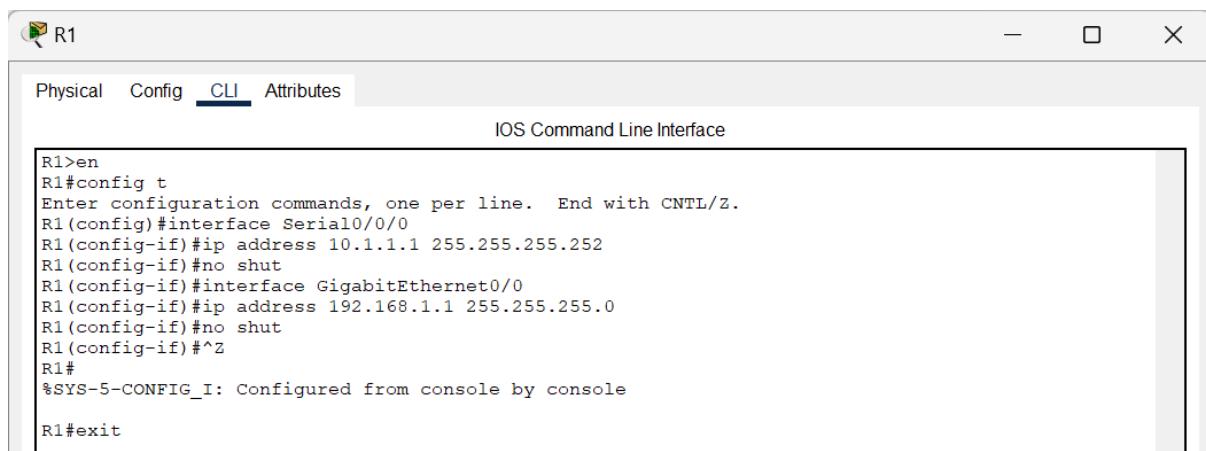
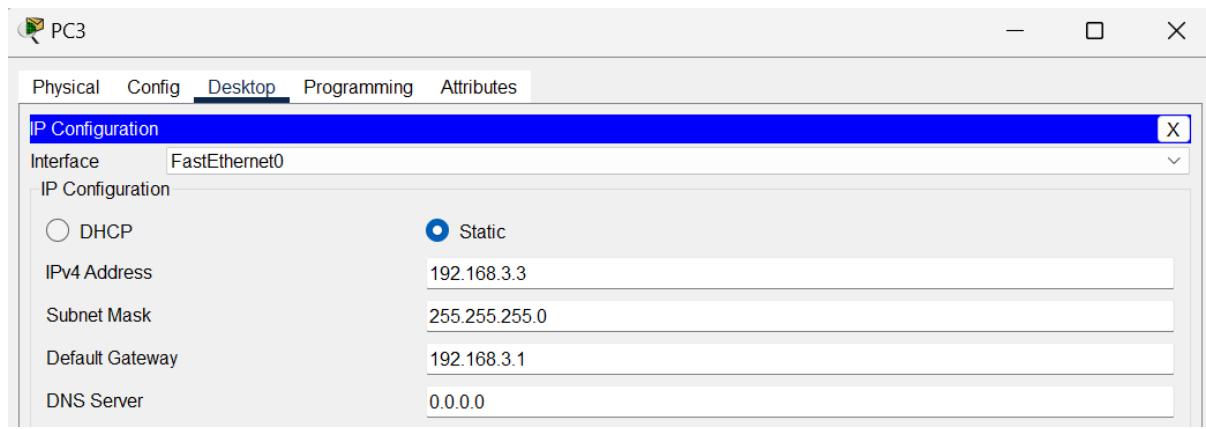
Aim: Configure and Verify a Site-to-Site IPsec VPN using CLI Topology

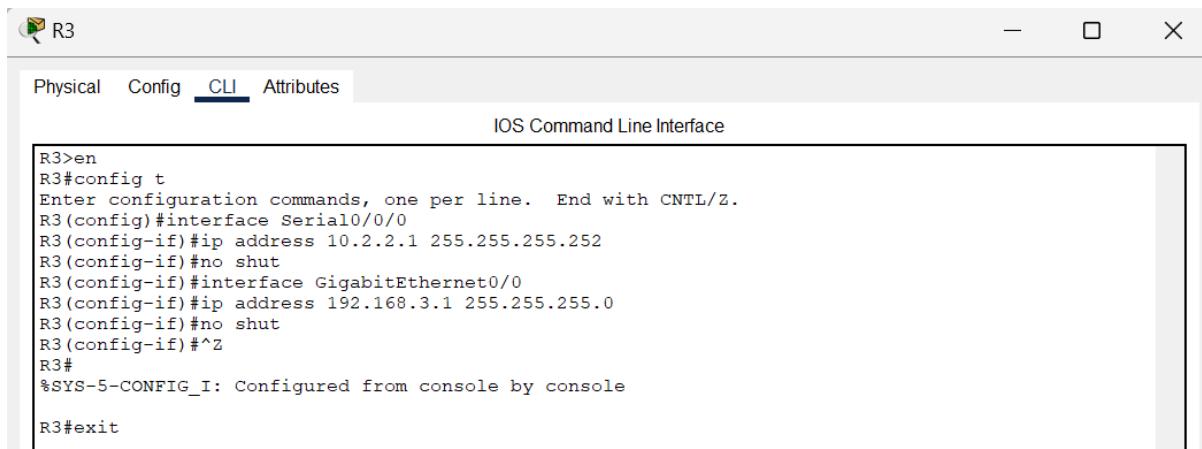
➤ Topology Diagram



➤ Assign IP Addresses

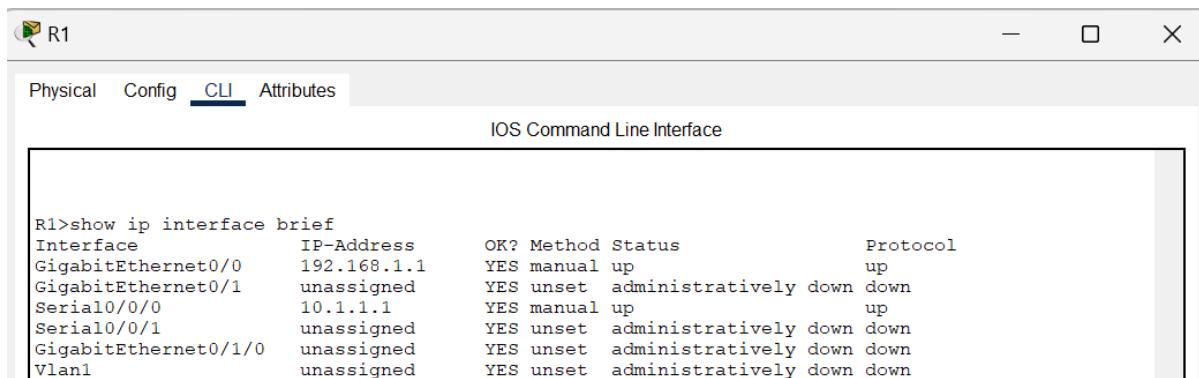






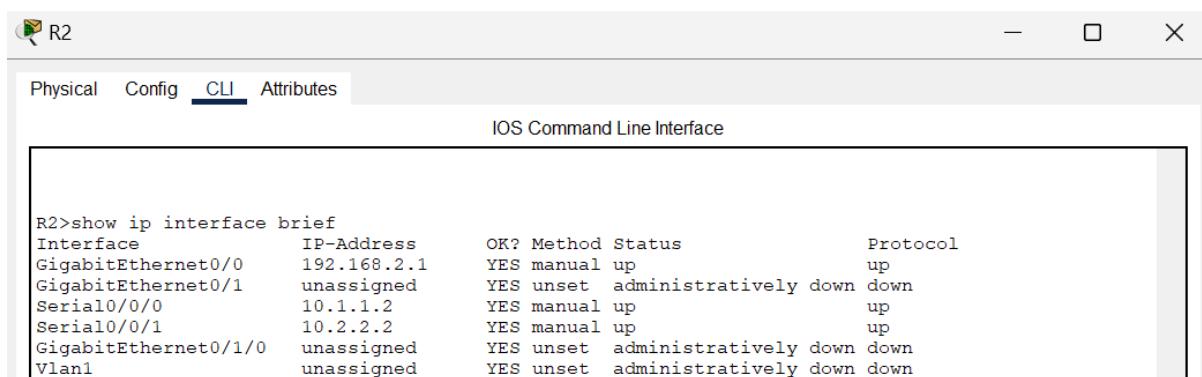
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface Serial0/0/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

➤ Displaying IP Address Details of Routers



R1>show ip interface brief

| Interface | IP-Address | OK? | Method | Status | Protocol |
|----------------------|-------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0 | 192.168.1.1 | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.1.1.1 | YES | manual | up | up |
| Serial0/0/1 | unassigned | YES | unset | administratively down | down |
| GigabitEthernet0/1/0 | unassigned | YES | unset | administratively down | down |
| Vlan1 | unassigned | YES | unset | administratively down | down |



R2>show ip interface brief

| Interface | IP-Address | OK? | Method | Status | Protocol |
|----------------------|-------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0 | 192.168.2.1 | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.1.1.2 | YES | manual | up | up |
| Serial0/0/1 | 10.2.2.2 | YES | manual | up | up |
| GigabitEthernet0/1/0 | unassigned | YES | unset | administratively down | down |
| Vlan1 | unassigned | YES | unset | administratively down | down |

R3>show ip interface brief

| Interface | IP-Address | OK? | Method | Status | Protocol |
|----------------------|-------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0 | 192.168.3.1 | YES | manual | up | up |
| GigabitEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0/0 | 10.2.2.1 | YES | manual | up | up |
| Serial0/0/1 | unassigned | YES | unset | administratively down | down |
| GigabitEthernet0/1/0 | unassigned | YES | unset | administratively down | down |
| Vlan1 | unassigned | YES | unset | administratively down | down |

➤ Configure RIP on Routers

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 192.168.2.0
R2(config-router)#network 10.2.2.0
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
```

➤ Displaying Routing Table of Routers

R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
R 10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:29, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
R 192.168.2.0/24 [120/1] via 10.1.1.2, 00:00:29, Serial0/0/0
R 192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:29, Serial0/0/0

R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.2/32 is directly connected, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.2/32 is directly connected, Serial0/0/1
R 192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:12, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0
L 192.168.2.1/32 is directly connected, GigabitEthernet0/0
R 192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:03, Serial0/0/1

R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R 10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:06, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/0
L 10.2.2.1/32 is directly connected, Serial0/0/0
R 192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:06, Serial0/0/0
R 192.168.2.0/24 [120/1] via 10.2.2.2, 00:00:06, Serial0/0/0
192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.3.0/24 is directly connected, GigabitEthernet0/0
L 192.168.3.1/32 is directly connected, GigabitEthernet0/0

➤ Verifying full network connectivity

C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=9ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 9ms, Average = 3ms

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=17ms TTL=125
Reply from 192.168.3.3: bytes=32 time=12ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 2ms, Maximum = 17ms, Average = 8ms

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco 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=12ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=17ms 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 = 1ms, Maximum = 17ms, Average = 7ms

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=13ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 13ms, Average = 4ms
```

PC3

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco 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=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=4ms 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 = 4ms, Average = 2ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=21ms TTL=126
Reply from 192.168.2.3: bytes=32 time=20ms TTL=126
Reply from 192.168.2.3: bytes=32 time=13ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 13ms
```

- Enable the Security Technology package on R1 and R3

R1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R1>show version
```

```
Technology Package License Information for Module:'c1900'

Technology      Technology-package      Technology-package
Current        Type                  Next reboot
-----
```

| Technology | Technology-package | Type | Next reboot |
|------------|--------------------|-----------|-------------|
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | None | None | None |
| data | None | None | None |

```
Configuration register is 0x2102
```



```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#license boot module c1900 technologyv-package securityvk9
```



```
ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot
level = securityvk9 and License = securityvk9

R1(config)# exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#reload
System configuration has been modified. Save? [yes/no]:yes
```



```
R1>show version
```

```
Technology Package License Information for Module:'c1900'

Technology      Technology-package      Technology-package
Current        Type                  Next reboot
-----
```

| Technology | Technology-package | Type | Next reboot |
|------------|--------------------|------------|-------------|
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Evaluation | securityk9 |
| data | disable | None | None |

```
Configuration register is 0x2102
```

R3

Physical Config **CLI** Attributes

IOS Command Line Interface

```
R3>show version
```

```
Technology Package License Information for Module:'c1900'

Technology      Technology-package      Technology-package
Current        Type                  Next reboot
-----
```

| Technology | Technology-package | Type | Next reboot |
|------------|--------------------|-----------|-------------|
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | None | None | None |
| data | None | None | None |

```
Configuration register is 0x2102
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 18.02.2025

```
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#license boot module c1900 technology-package securityk9
```

```
ACCEPT? [yes/no]: yes
* use 'write' command to make license boot config take effect on next boot

R3(config) #: %IOS LICENSE IMAGE APPLICATION-6-LICENSE LEVEL: Module name = C1900 Next reboot
level = securityk9 and License = securityk9

R3(config)#exit
R3#
*SYS-5-CONFIG_I: Configured from console by console

R3#reload
System configuration has been modified. Save? [yes/no]:yes
```

```
R3>show version
```

```
Technology Package License Information for Module:'c1900'
```

| Technology | Technology-package
Current | Type | Technology-package
Next reboot |
|------------|-------------------------------|------------|-----------------------------------|
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Evaluation | securityk9 |
| data | disable | None | None |

```
Configuration register is 0x2102
```

➤ Configure ACL, IKE Phase 1 ISAKMP policy and IKE Phase 2 IPsec policy on R1 and R3

The screenshot shows the Cisco IOS CLI interface for router R1. The window title is 'R1'. The tab bar at the top includes 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs, it says 'IOS Command Line Interface'. The main area displays the following configuration commands:

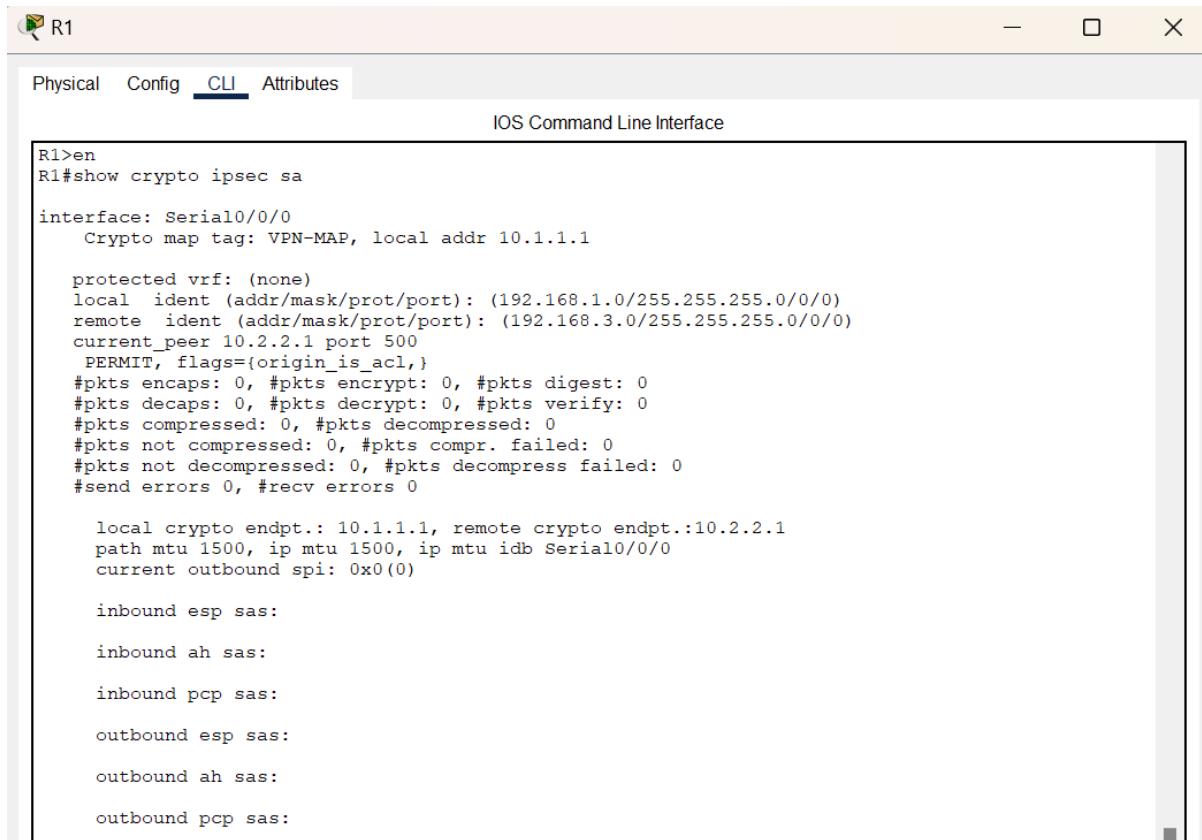
```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key vnpwd address 10.2.2.1
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#description VPN connection to R3
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#exit
R1(config)#interface Serial0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#^Z
R1#
*SYS-5-CONFIG_I: Configured from console by console

R1#exit
```



R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key vpnpwd address 10.1.1.1
R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R3(config-crypto-map)#description VPN connection to R1
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set transform-set VPN-SET
R3(config-crypto-map)#match address 110
R3(config-crypto-map)#exit
R3(config)#interface Serial0/0/0
R3(config-if)#crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit

➤ **Verify the working of IPsec VPN for interesting traffic on R1**



R1>en
R1#show crypto ipsec sa

| interface: | Serial0/0/0 |
|-------------------------------------|---|
| Crypto map tag: | VPN-MAP, local addr 10.1.1.1 |
| 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): | (192.168.3.0/255.255.255.0/0/0) |
| current_peer | 10.2.2.1 port 500 |
| PERMIT, flags={origin_is_acl,} | |
| #pkts encaps: | 0, #pkts encrypt: 0, #pkts digest: 0 |
| #pkts decaps: | 0, #pkts decrypt: 0, #pkts verify: 0 |
| #pkts compressed: | 0, #pkts decompressed: 0 |
| #pkts not compressed: | 0, #pkts compr. failed: 0 |
| #pkts not decompressed: | 0, #pkts decompress failed: 0 |
| #send errors 0, #recv errors 0 | |
| local crypto endpt.: | 10.1.1.1, remote crypto endpt.:10.2.2.1 |
| path mtu | 1500, ip mtu 1500, ip mtu idb Serial0/0/0 |
| current outbound spi: | 0x0(0) |
| inbound esp sas: | |
| inbound ah sas: | |
| inbound pcp sas: | |
| outbound esp sas: | |
| outbound ah sas: | |
| outbound pcp sas: | |

PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

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=12ms TTL=126
Reply from 192.168.3.3: bytes=32 time=7ms TTL=126
Reply from 192.168.3.3: bytes=32 time=3ms TTL=126
Reply from 192.168.3.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 12ms, Average = 6ms
```

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
R1#show crypto ipsec sa

interface: Serial0/0/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.1
  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): (192.168.3.0/255.255.255.0/0/0)
  current_peer 10.2.2.1 port 500
    PERMIT, flags=(origin_is_acl,)
  #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
  #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 1, #recv errors 0

  local crypto endpt.: 10.1.1.1, remote crypto endpt.:10.2.2.1
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
  current outbound spi: 0xB14DFBC4(2974677956)

  inbound esp sas:
    spi: 0x05925F39(93478713)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
      sa timing: remaining key lifetime (k/sec): (4525504/3575)
      IV size: 16 bytes
      replay detection support: N
    Status: ACTIVE
```

Name: Sahil Kamble
Roll No.: 22093
Class: TYBSc IT

Subject: Information Security
Sem: VI
Date: 18.02.2025

```
inbound ah sas:  
inbound pcp sas:  
  
outbound esp sas:  
    spi: 0xB14DFBC4(2974677956)  
        transform: esp-aes esp-sha-hmac ,  
        in use settings ={Tunnel, }  
        conn id: 2007, flow_id: FPGA:1, crypto map: VPN-MAP  
        sa timing: remaining key lifetime (k/sec): (4525504/3575)  
        IV size: 16 bytes  
        replay detection support: N  
        Status: ACTIVE  
  
outbound ah sas:  
outbound pcp sas:
```