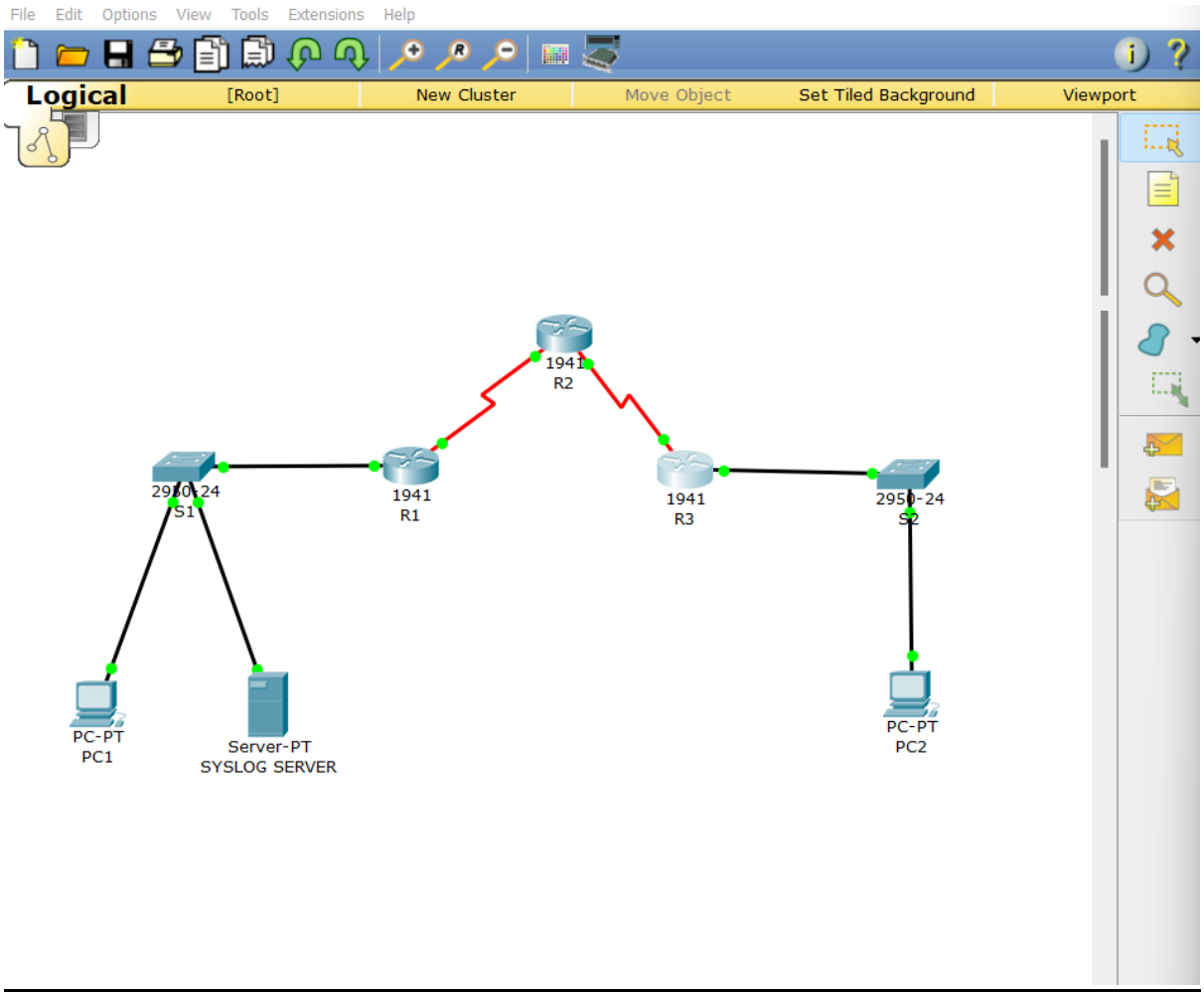
**Date:** 06/03/2024 **Security in Computing**

**PRACTICAL 7**

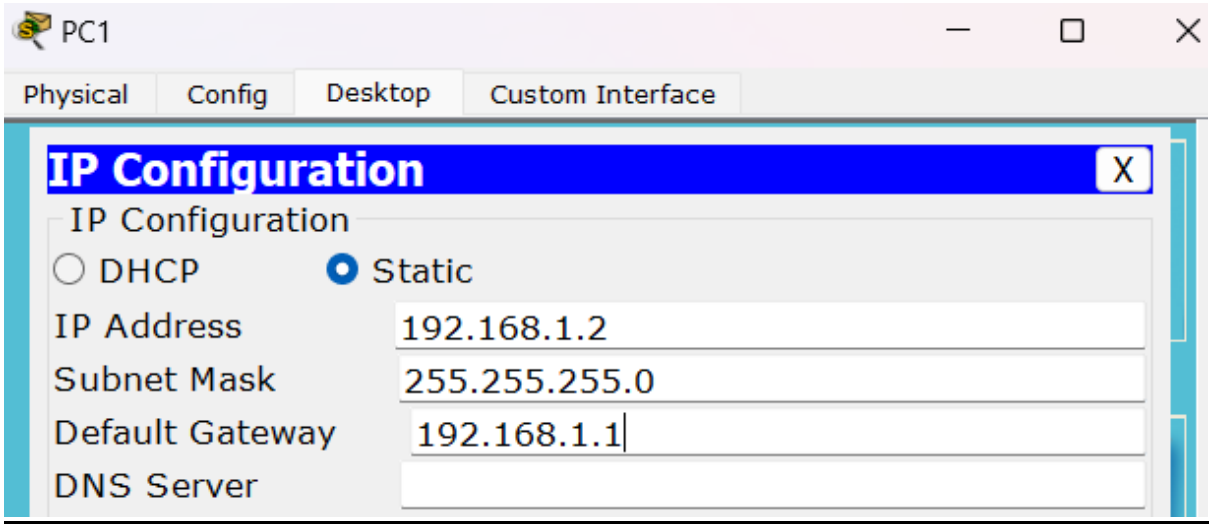
**Aim: Configure IOS Intrusion Prevention System (IPS) using the CLI.**

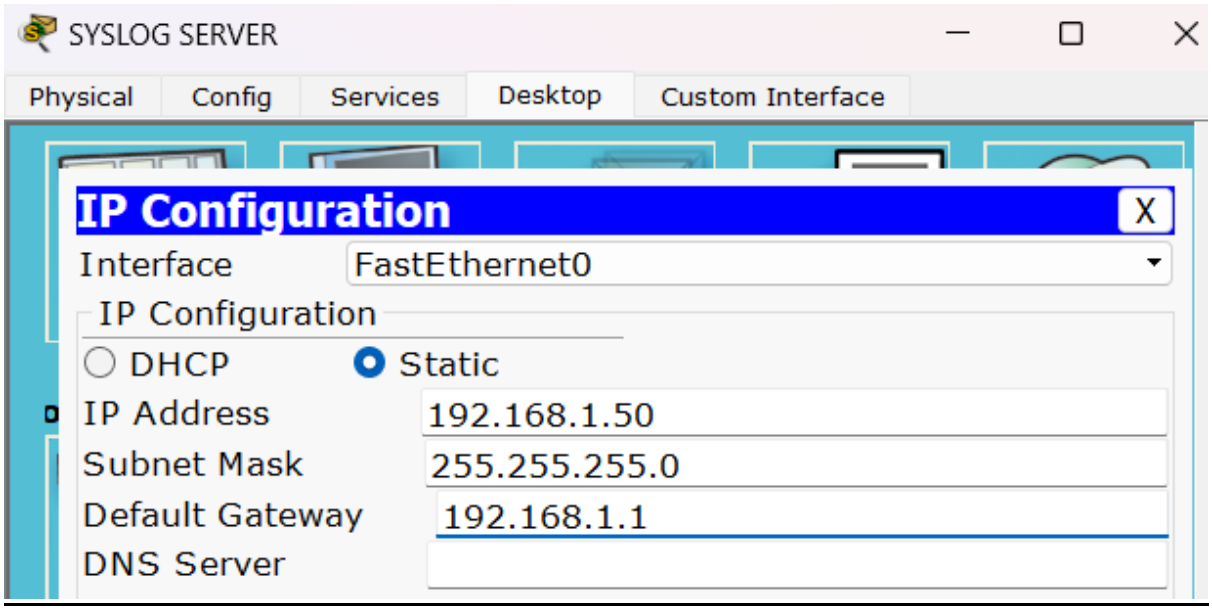
a. **Enable IOS IPS.**
b. **Modify an IPS Signature.**

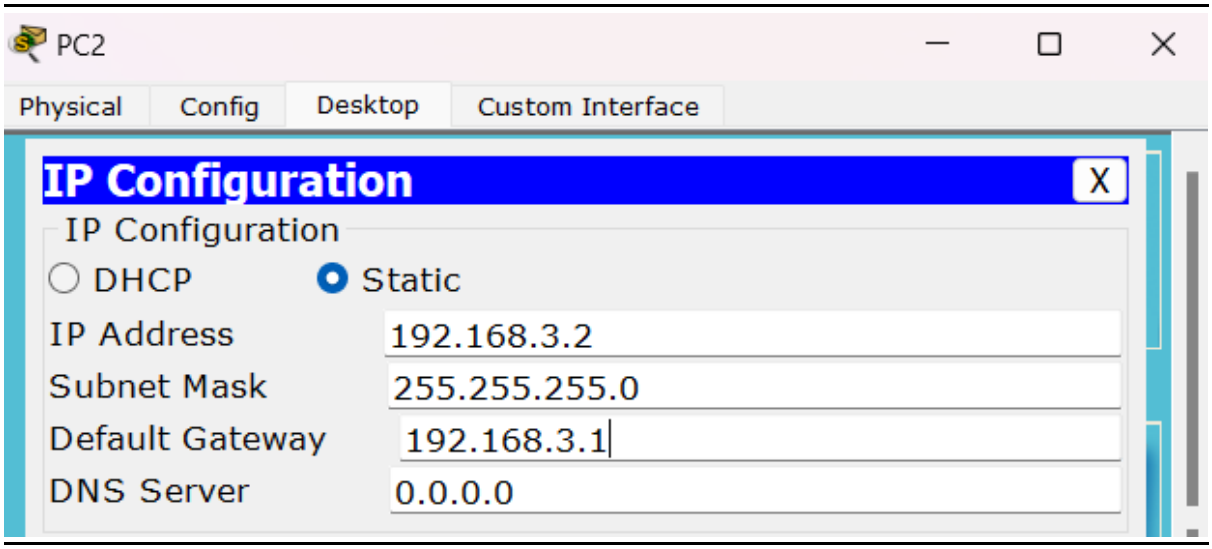
➢ **Topology Diagram:**



## ➢ Assign IP Addresses:



R1

Physical Config CLI

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

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)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

R3

Physical Config CLI

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)#
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

- **Displaying IP Address Details of Routers:**

R1

Physical Config CLI

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

Vlan1                  unassigned      YES unset  administratively down
down
```

R2

Physical Config CLI

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

Vlan1                  unassigned      YES unset  administratively down
down
R2>
```

R3

Physical Config CLI

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

Vlan1                  unassigned      YES unset  administratively down
down
```

## ➢ Configure RIP on Routers:

R1

Physical | Config | CLI

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

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

Physical | Config | CLI

IOS Command Line Interface

```
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

Physical | Config | CLI

IOS Command Line Interface

```
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, 00:00:23, 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, 00:00:23, Serial0/0/0
R1>
```

R2

Physical | Config | CLI

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, 00:00:10, Serial0/0/0
R    192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:24, Serial0/0/1
R2>
```

R3

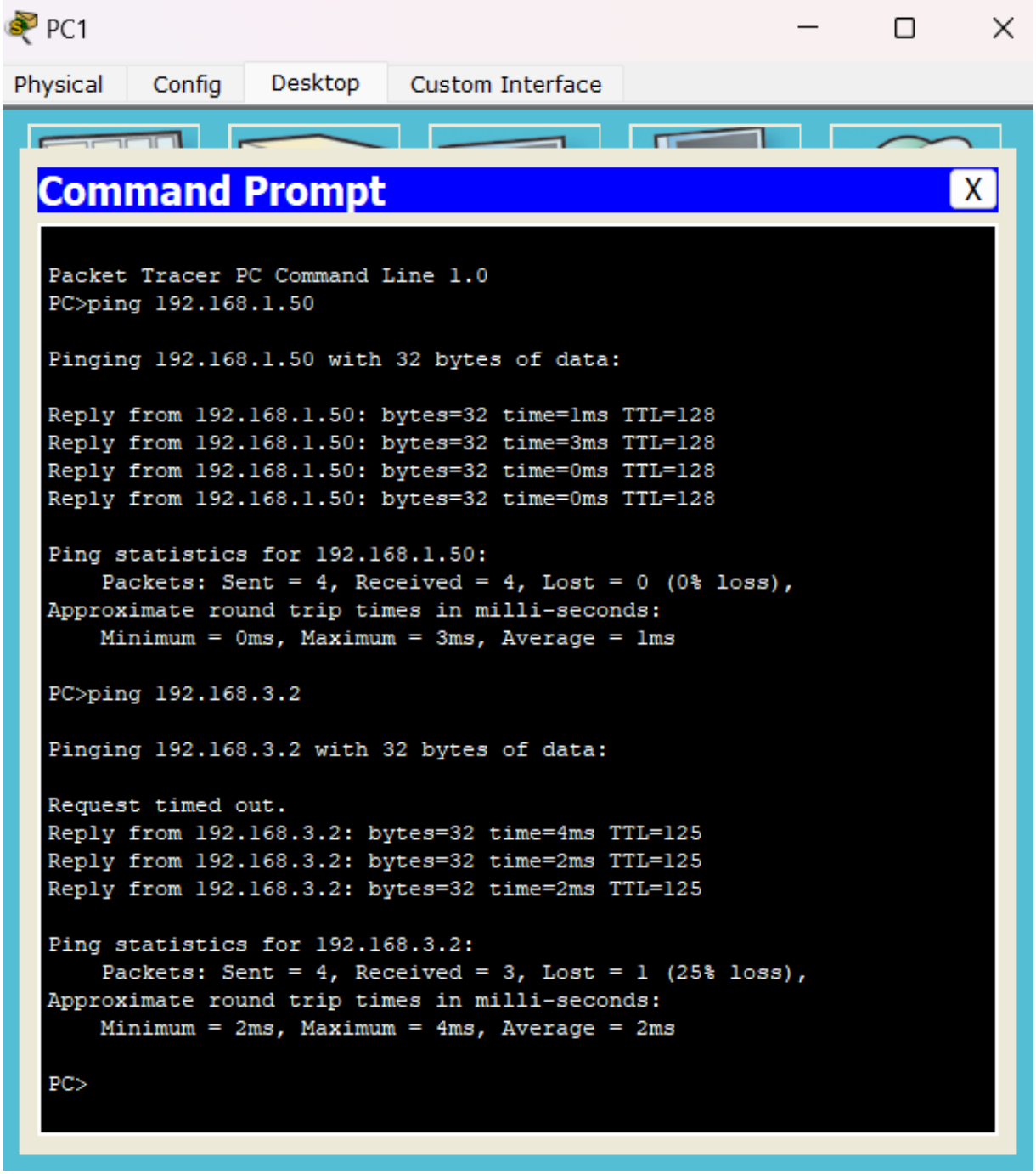
Physical | Config | CLI

IOS Command Line Interface

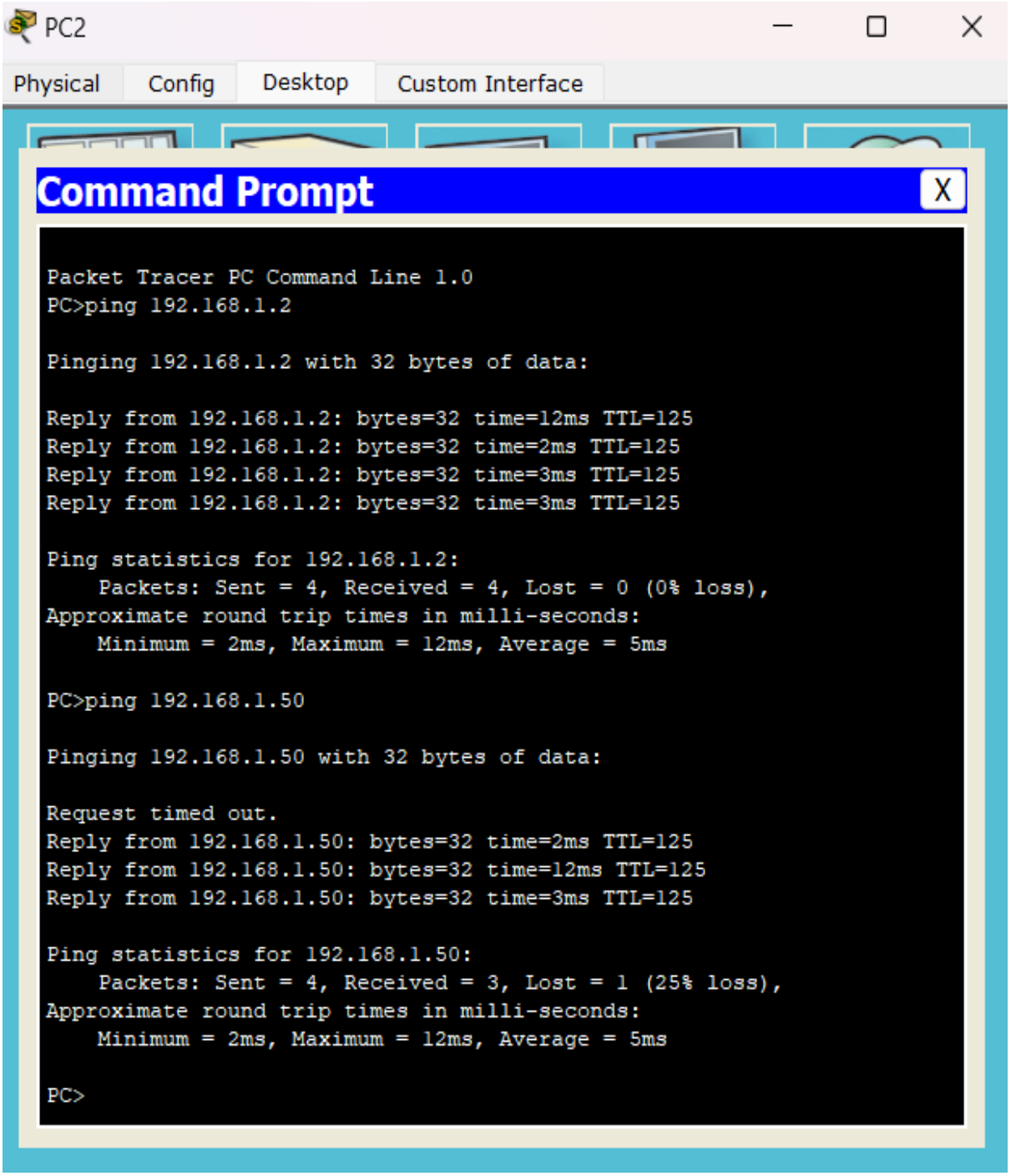
```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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
     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>
```

## ➢ Verifying Full Network Connectivity:

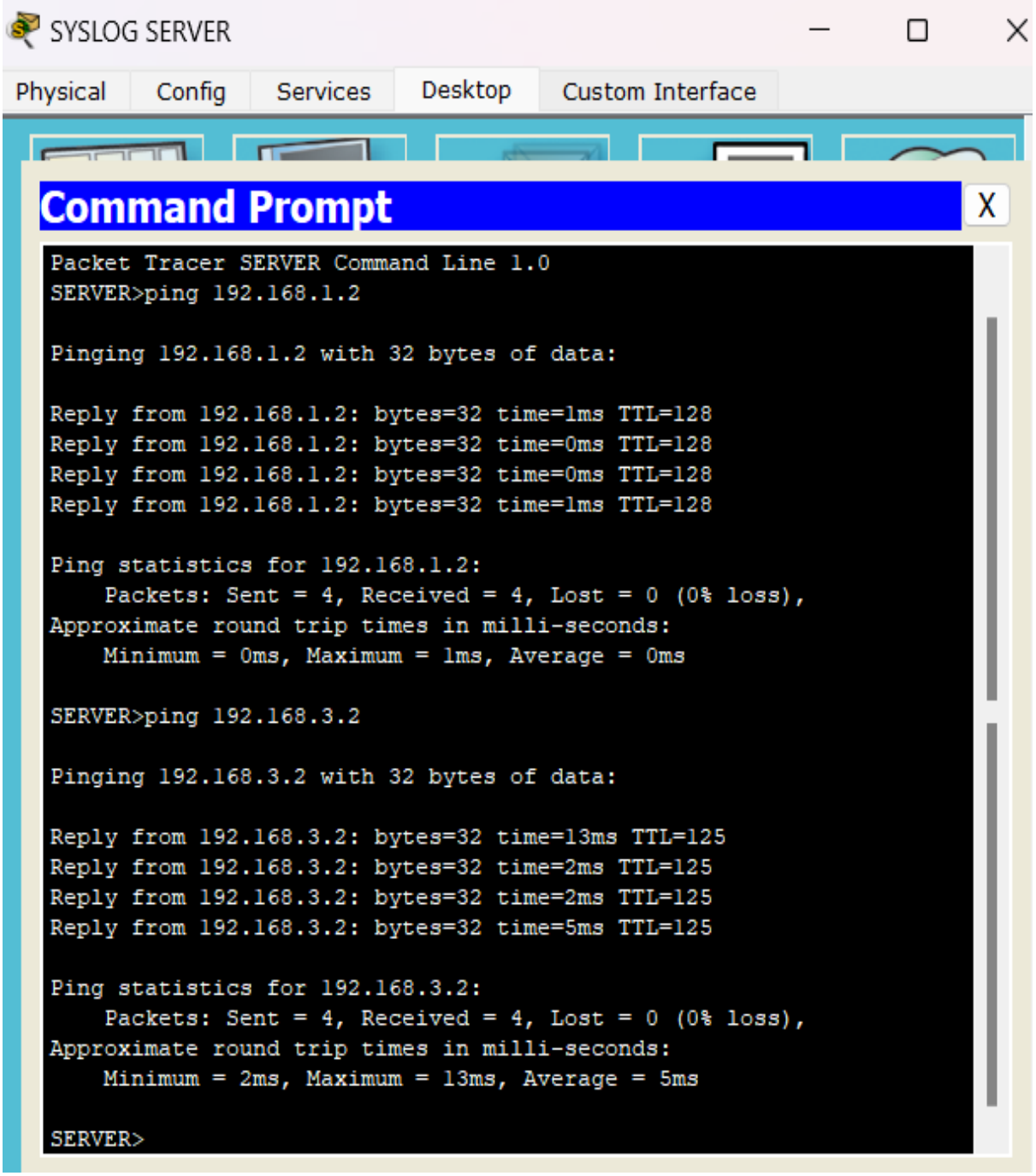
- PC 1



- PC 2


PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 12ms, Average = 5ms
PC>ping 192.168.1.50
Pinging 192.168.1.50 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.50: bytes=32 time=2ms TTL=125
Reply from 192.168.1.50: bytes=32 time=12ms TTL=125
Reply from 192.168.1.50: bytes=32 time=3ms TTL=125
Ping statistics for 192.168.1.50:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 12ms, Average = 5ms
PC>

- SYSLOG SERVER



## ➢ Enable the Secure Technology Package on R1 :

R1

Physical Config CLI

IOS Command Line Interface

```
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

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
%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          None          None          None

Configuration register is 0x2102
```

## 1. Enable IOS IPS on R1:

R1

Physical | Config | CLI

IOS Command Line Interface

```
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

Physical Config CLI

## IOS Command Line Interface

```
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 all
                                      ^
% Invalid input detected at '^' marker.

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)#exirt
                                  ^
% Invalid input detected at '^' marker.

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 gig 0/0
R1(config-if)#ip  ips iosips out
R1(config-if)#
*Mar 22, 20:29:02.2929:  %IPS-6-ENGINE_BUILDS_STARTED:  20:29:02 UTC Mar 22 2024
*Mar 22, 20:29:02.2929:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13
engines
*Mar 22, 20:29:02.2929:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets
for this engine will be scanned
*Mar 22, 20:29:02.2929:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
R1(config-if)#exit
R1(config)#
R1(config)#exit
R1#
*Mar 22, 20:30:01.3030: *Mar 22, 20:30:01.3030: %SYS-5-CONFIG_I: Configured from
console by console
*Mar 22, 20:30:01.3030: *Mar 22, 20:30:01.3030: %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 iosipd
      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 GigabitEthernet0/0
        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
R1#
```

## 2. Modify the Signatures of the IPS:

R1

Physical Config CLI

IOS Command Line Interface

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips signature-defination
                                      ^
% Invalid input detected at '^' marker.

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 product-alert
                                                  ^
% Invalid input detected at '^' marker.

R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be
scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

R1(config)#exit
R1#
*Mar 22, 20:38:16.3838: *Mar 22, 20:38:16.3838: %SYS-5-CONFIG_I: Configured from
console by console
R1#
```

## ➢ Displaying the IPS Configuration Status Summary:

R1

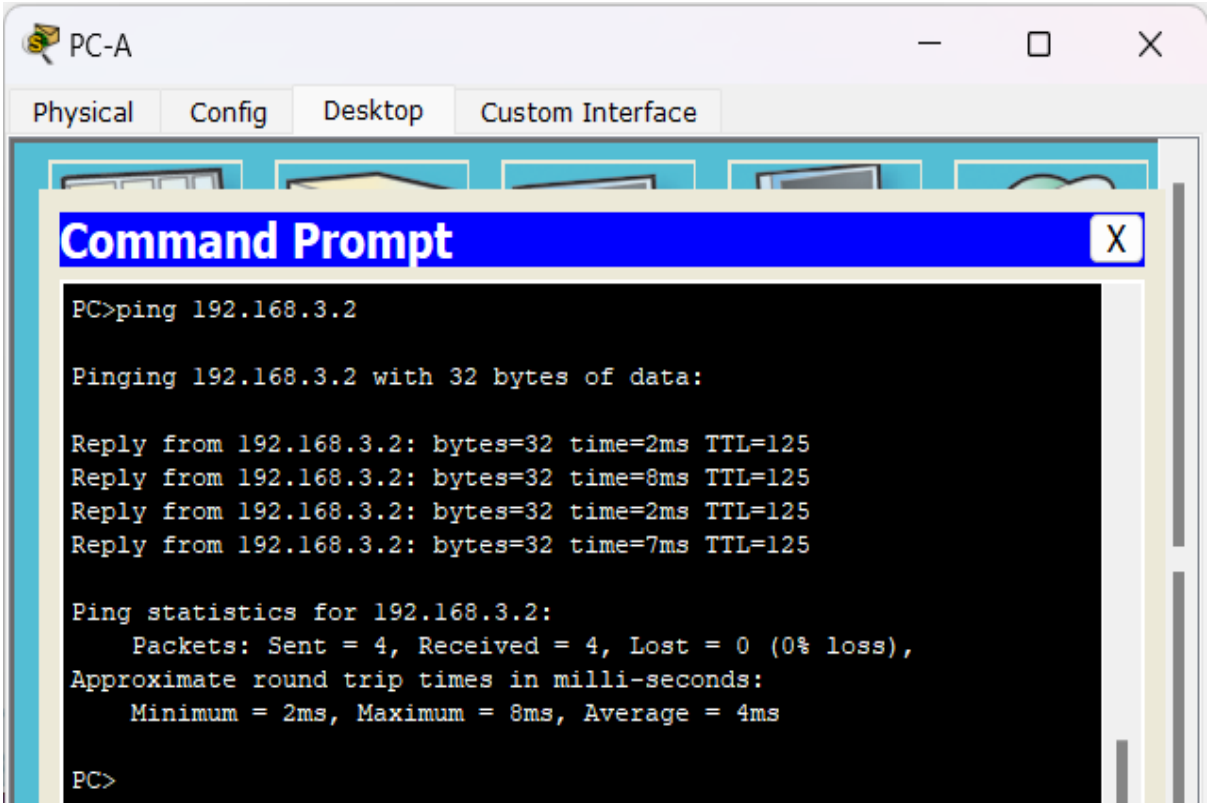
Physical Config CLI

IOS Command Line Interface

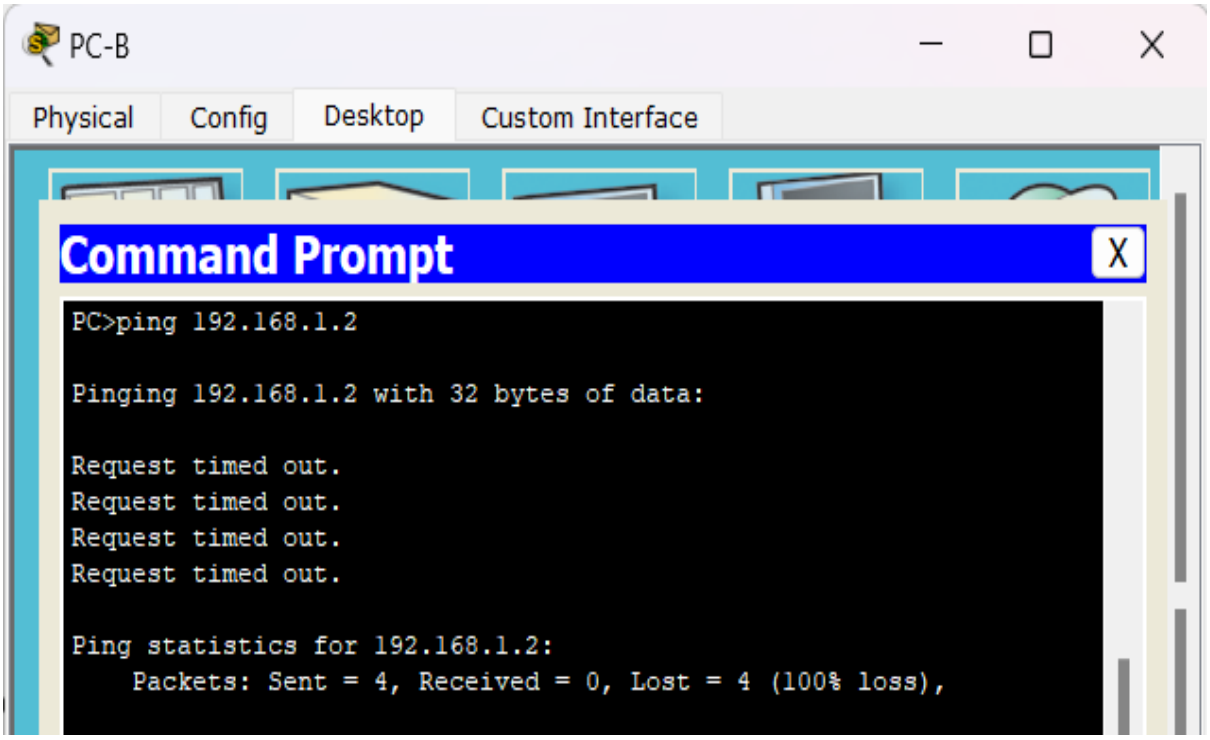
```
Router>en
Router#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    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 GigabitEthernet0/0
        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
Router#
```

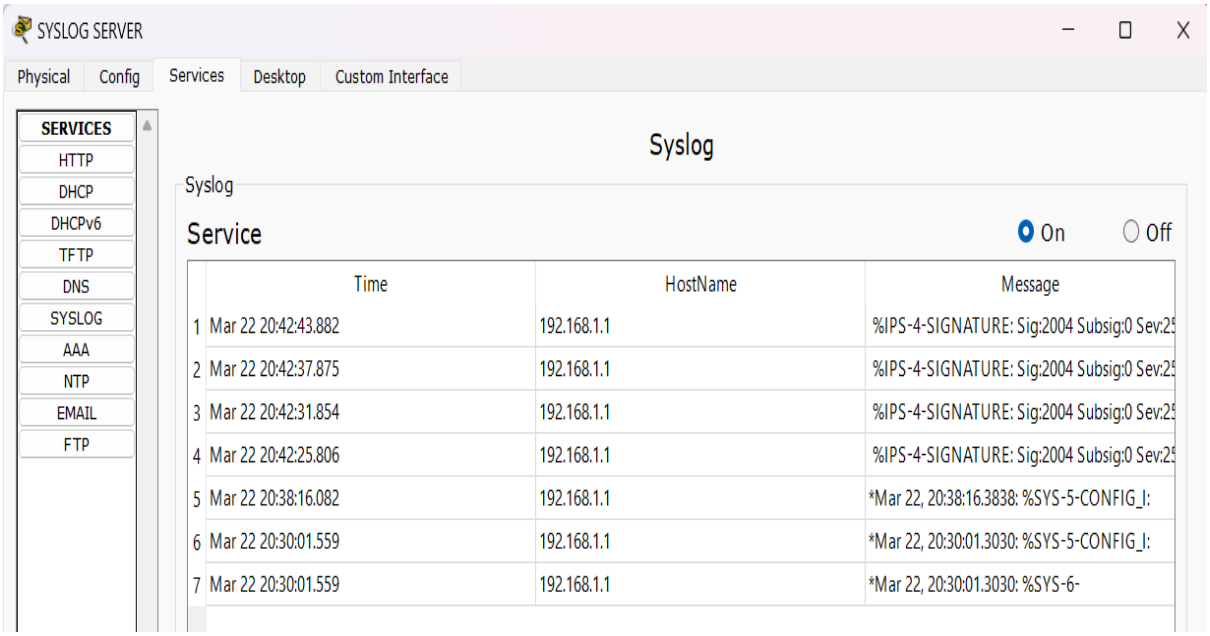
## ➢ Verifying the Working of IPS:

- PC 1




- PC 2




SYSLOG SERVER
Physical
Config
Services
Desktop
Custom Interface
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
Syslog
Syslog
Service
On
Off
Time
HostName
Message
1 Mar 22 20:42:43.882 192.168.1.1 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25
2 Mar 22 20:42:37.875 192.168.1.1 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25
3 Mar 22 20:42:31.854 192.168.1.1 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25
4 Mar 22 20:42:25.806 192.168.1.1 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25
5 Mar 22 20:38:16.082 192.168.1.1 *Mar 22, 20:38:16.3838: %SYS-5-CONFIG_I:
6 Mar 22 20:30:01.559 192.168.1.1 *Mar 22, 20:30:01.3030: %SYS-5-CONFIG_I:
7 Mar 22 20:30:01.559 192.168.1.1 *Mar 22, 20:30:01.3030: %SYS-6-