

Date: 06/03/2024

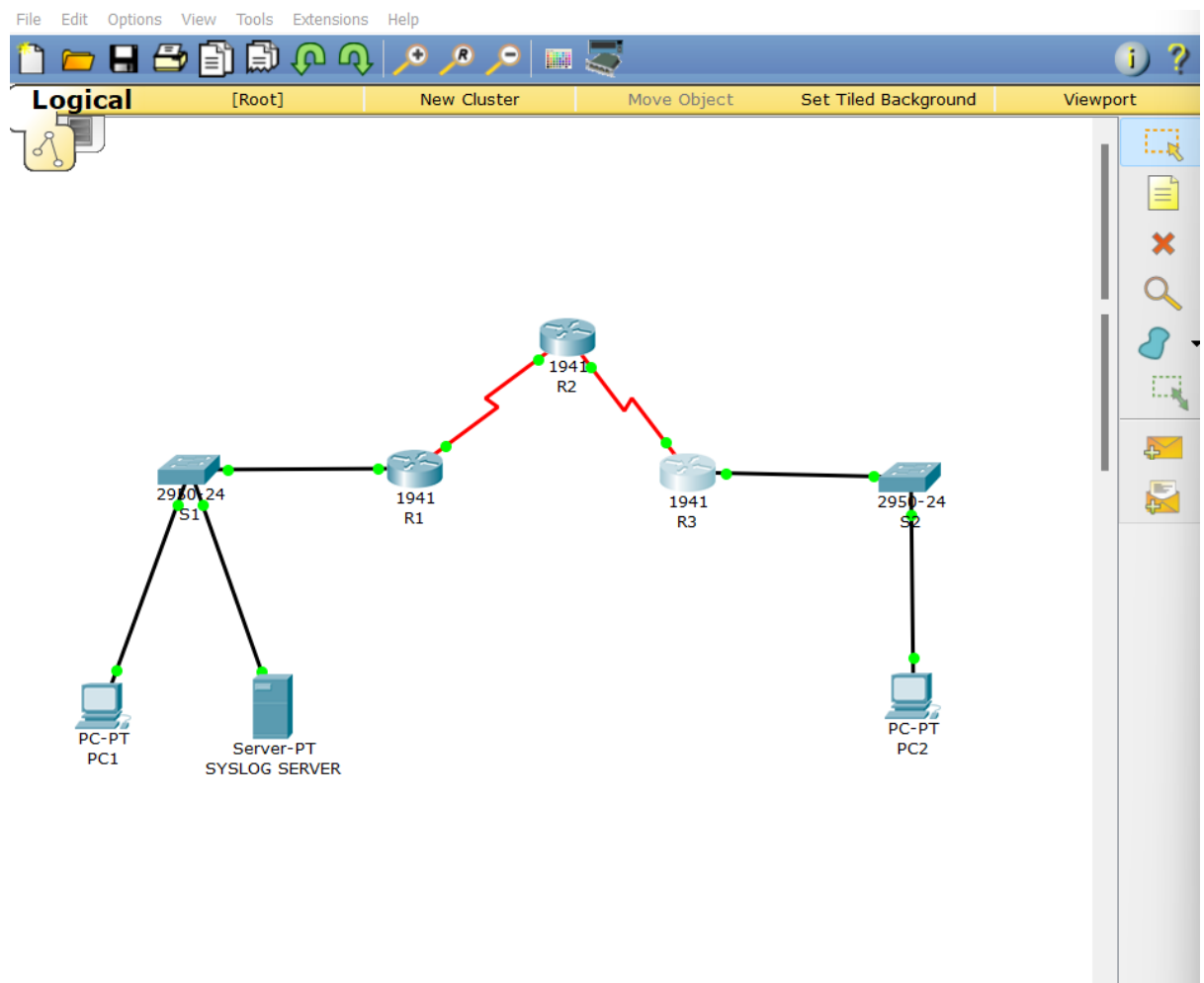
Security in Computing

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:

PC1

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

SYSLOG SERVER

Physical Config Services Desktop Custom Interface

IP Configuration

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.1.50

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server

PC2

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

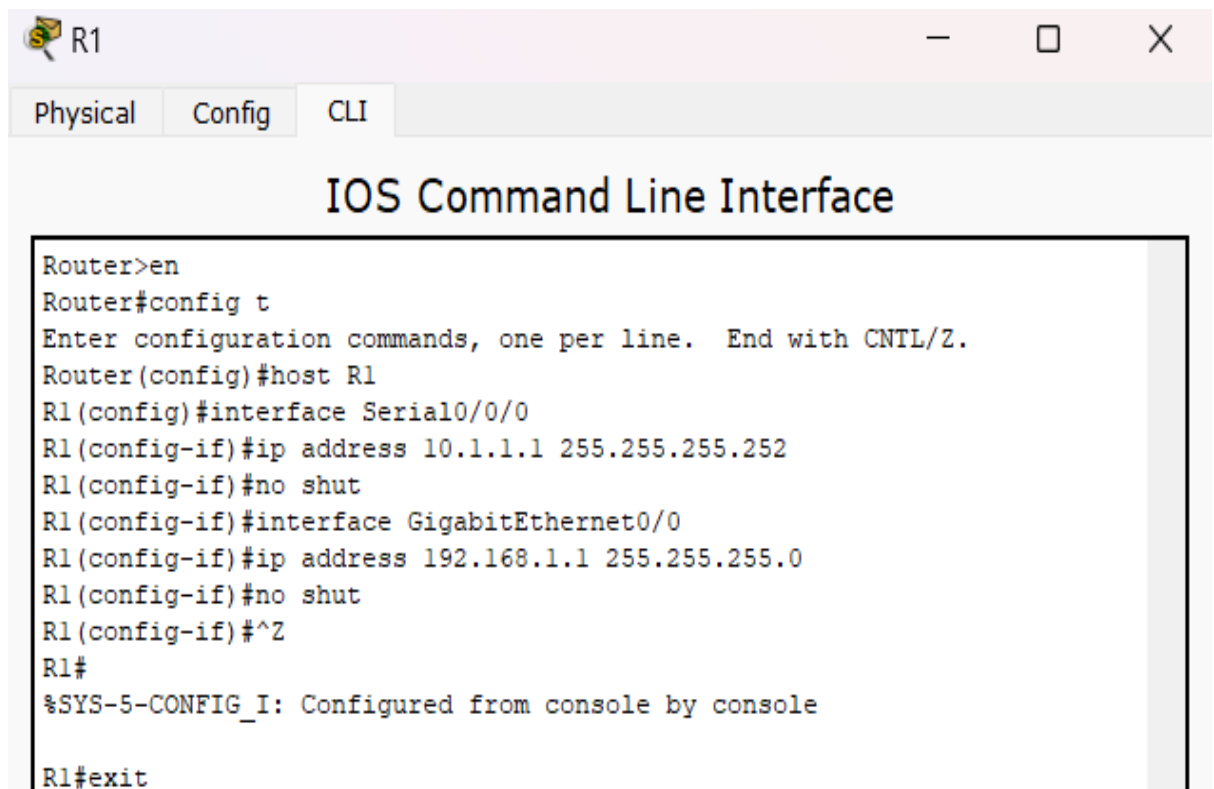
☐ DHCP ☒ Static

IP Address 192.168.3.2

Subnet Mask 255.255.255.0

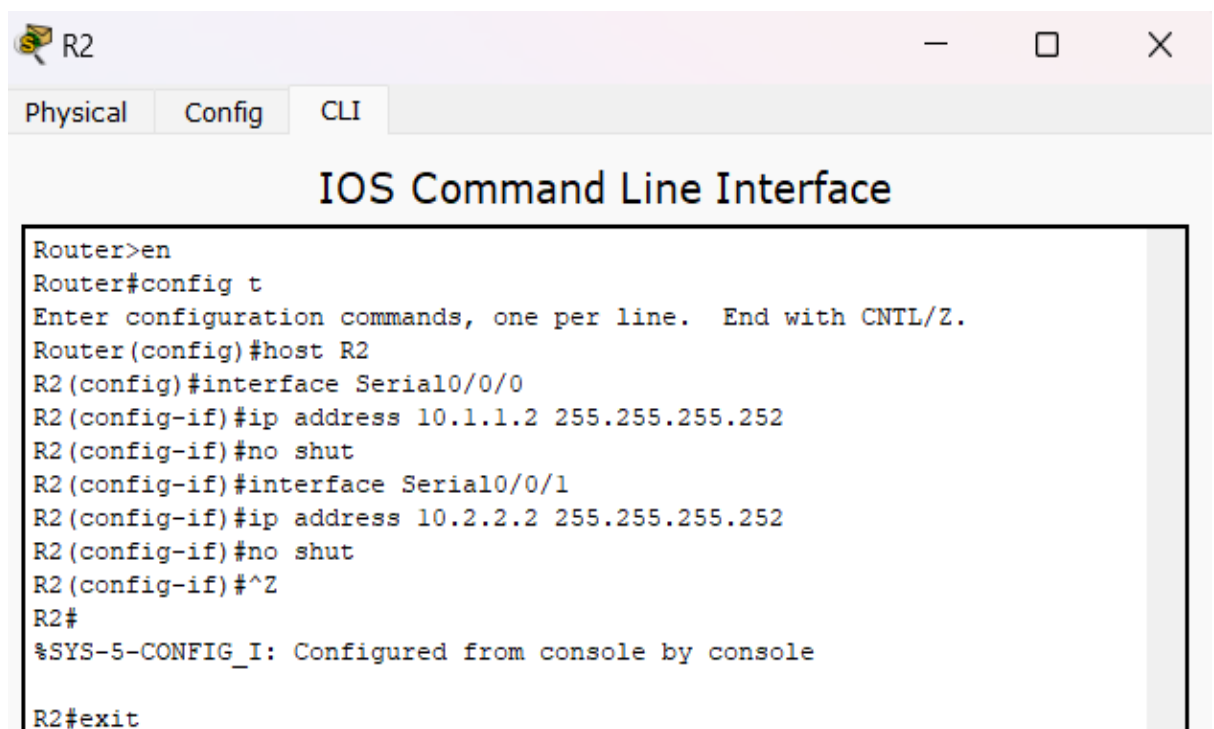
Default Gateway 192.168.3.1

DNS Server 0.0.0.0



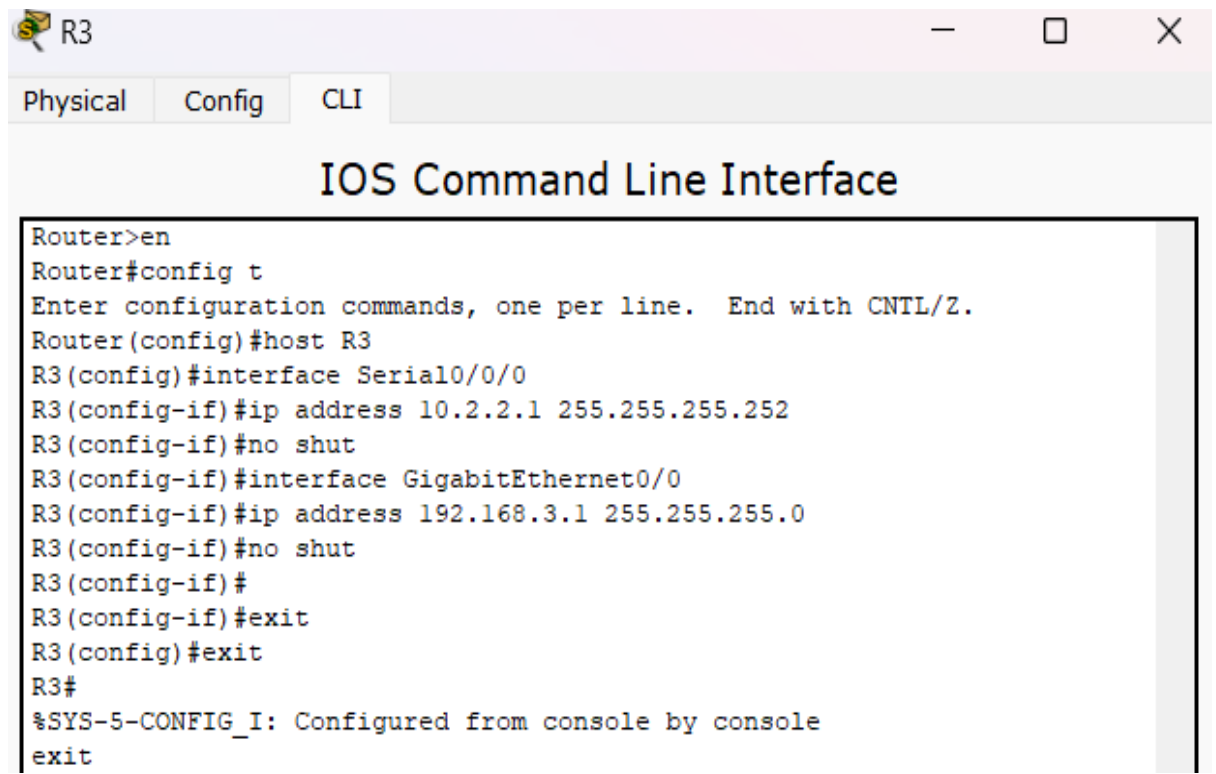
The screenshot shows a window titled 'R1' with three tabs: 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command history shows the following sequence: 'Router>en' to enter enable mode, 'Router#config t' to enter configuration mode, 'Router(config)#host R1' to set the router name, 'R1(config)#interface Serial0/0/0' to enter interface configuration, 'R1(config-if)#ip address 10.1.1.1 255.255.255.252' to assign the IP address, 'R1(config-if)#no shut' to enable the interface, 'R1(config-if)#interface GigabitEthernet0/0' to enter another interface configuration, 'R1(config-if)#ip address 192.168.1.1 255.255.255.0' to assign the IP address, 'R1(config-if)#no shut' to enable it, 'R1(config-if)#^Z' to exit configuration mode, 'R1#' to return to the prompt, a system message '%SYS-5-CONFIG_I: Configured from console by console', and finally 'R1#exit' to exit the CLI.

```
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
```



The screenshot shows a window titled 'R2' with three tabs: 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command history shows the following sequence: 'Router>en' to enter enable mode, 'Router#config t' to enter configuration mode, 'Router(config)#host R2' to set the router name, 'R2(config)#interface Serial0/0/0' to enter interface configuration, 'R2(config-if)#ip address 10.1.1.2 255.255.255.252' to assign the IP address, 'R2(config-if)#no shut' to enable the interface, 'R2(config-if)#interface Serial0/0/1' to enter another interface configuration, 'R2(config-if)#ip address 10.2.2.2 255.255.255.252' to assign the IP address, 'R2(config-if)#no shut' to enable it, 'R2(config-if)#^Z' to exit configuration mode, 'R2#' to return to the prompt, a system message '%SYS-5-CONFIG_I: Configured from console by console', and finally 'R2#exit' to exit the CLI.

```
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
```



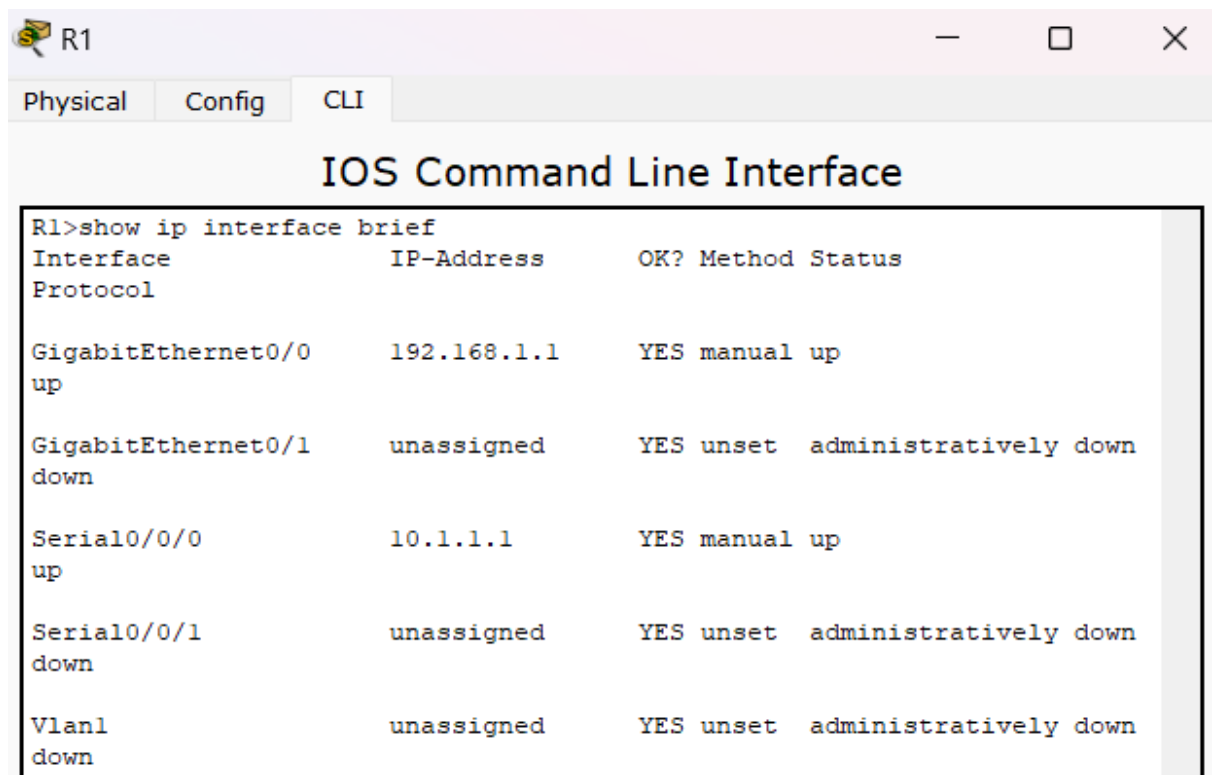
The screenshot shows the CLI of router R3. The user has entered the configuration mode and configured the host name as R3. Two interfaces have been configured: Serial0/0/0 with IP address 10.2.2.1 and GigabitEthernet0/0 with IP address 192.168.3.1. Both interfaces are in the 'no shut' state. The user has exited the configuration mode and the router has confirmed the configuration.

```

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:**



The screenshot shows the CLI of router R1. The user has entered the command 'show ip interface brief', which displays a table of interface details. The table includes columns for Interface, IP-Address, OK?, Method, and Status. The interfaces listed are GigabitEthernet0/0, GigabitEthernet0/1, Serial0/0/0, Serial0/0/1, and Vlan1.

```

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

```

R2

Physical Config CLI

IOS Command Line Interface

```
R2>show ip interface brief
```

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

R2>

R3

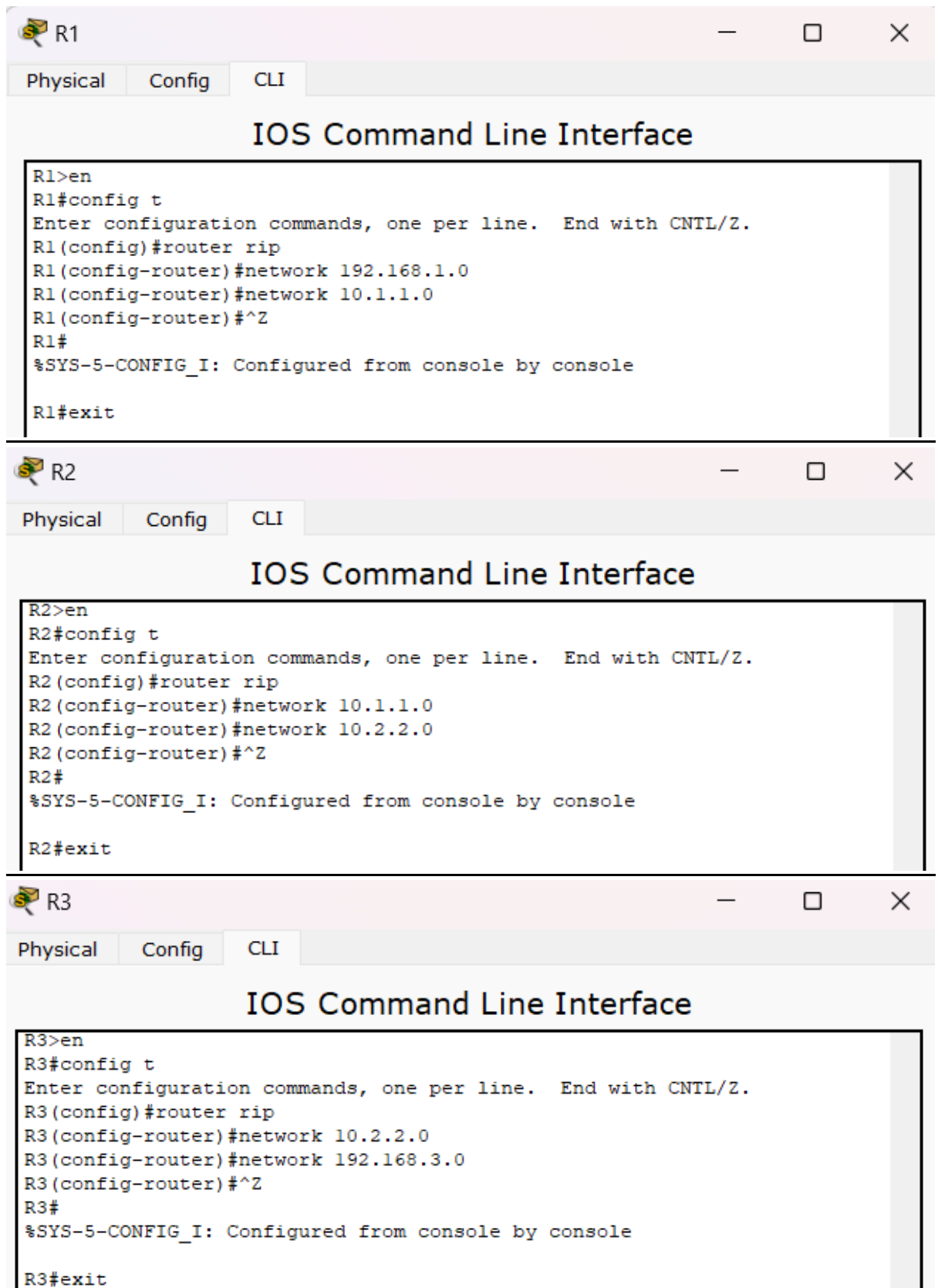
Physical Config CLI

IOS Command Line Interface

```
R3>show ip interface brief
```

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

➤ **Configure RIP on Routers:**



The image displays three sequential screenshots of a network simulator's CLI interface for three routers, R1, R2, and R3. Each window has a title bar with the router name and standard window controls. Below the title bar are tabs for 'Physical', 'Config', and 'CLI', with 'CLI' being the active tab. The main area is titled 'IOS Command Line Interface' and contains a text box with the command history.

R1 Configuration:

```
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
```

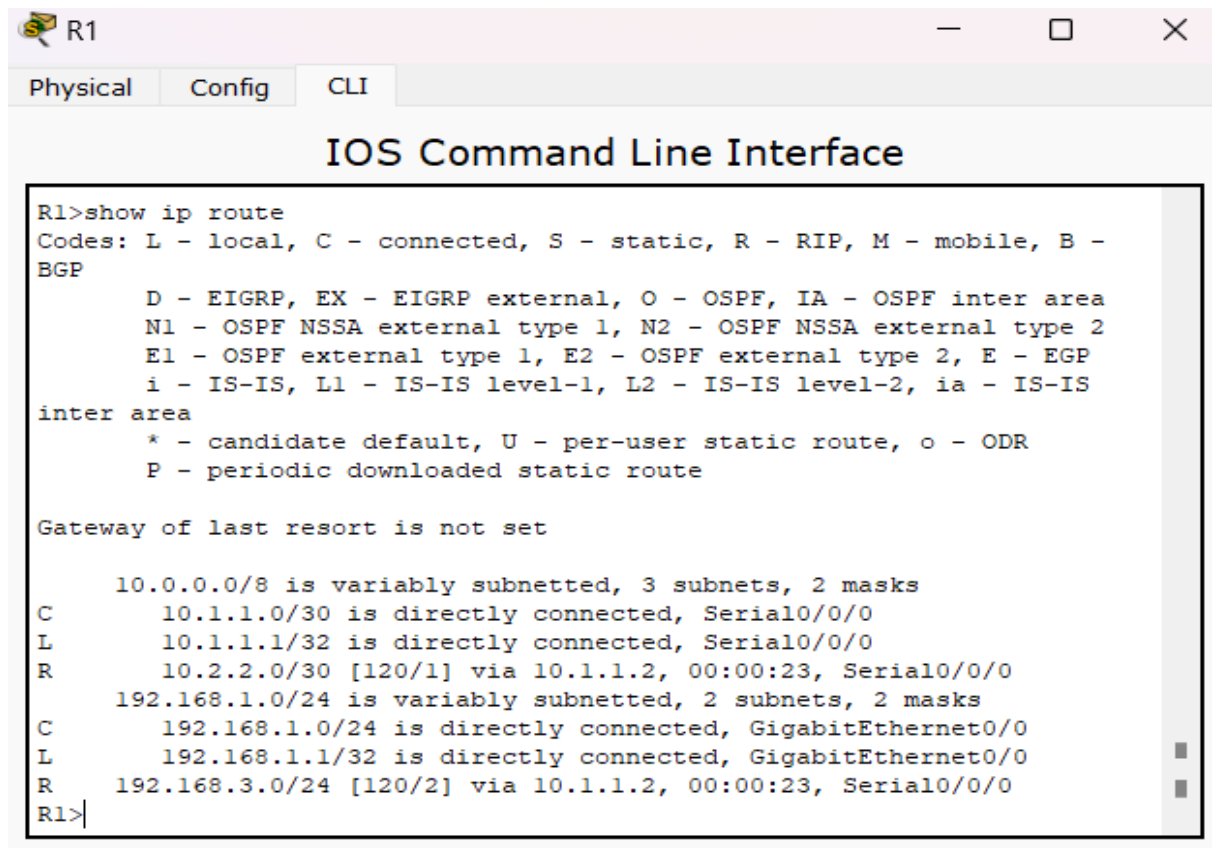
R2 Configuration:

```
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 Configuration:

```
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

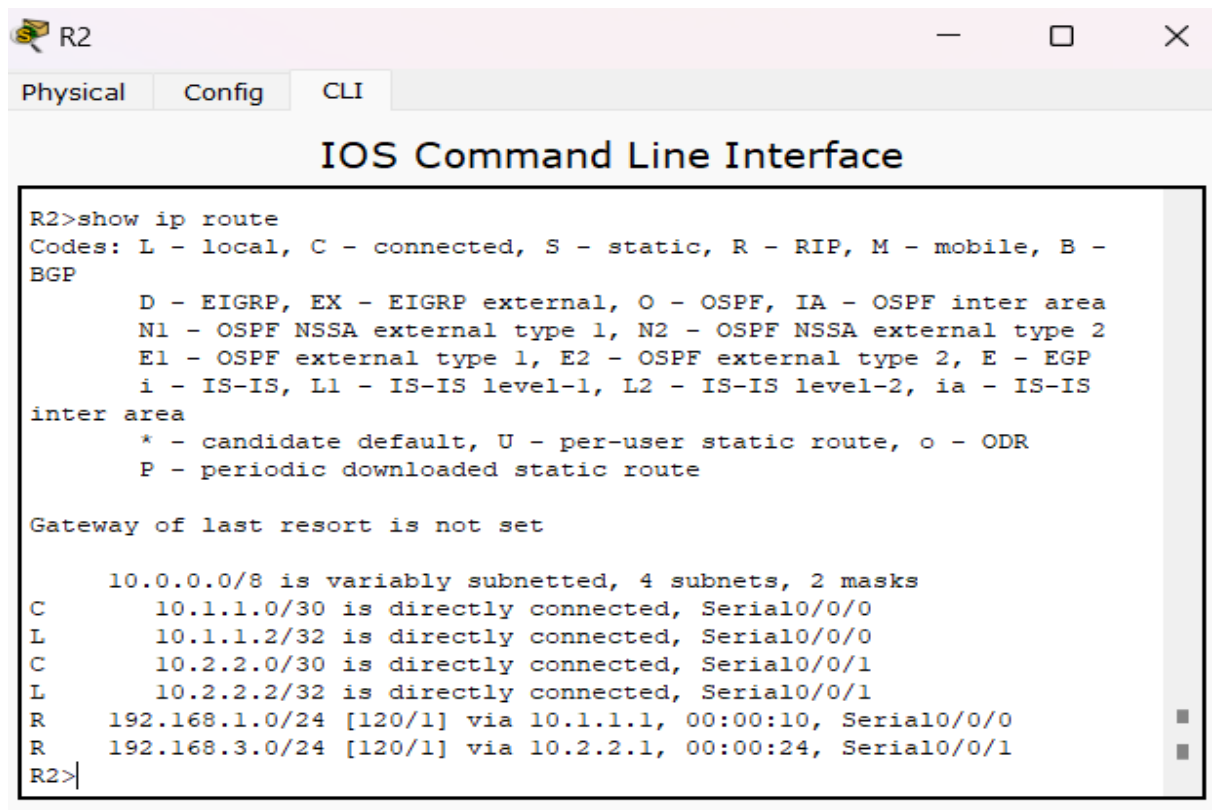
Physical Config CLI

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

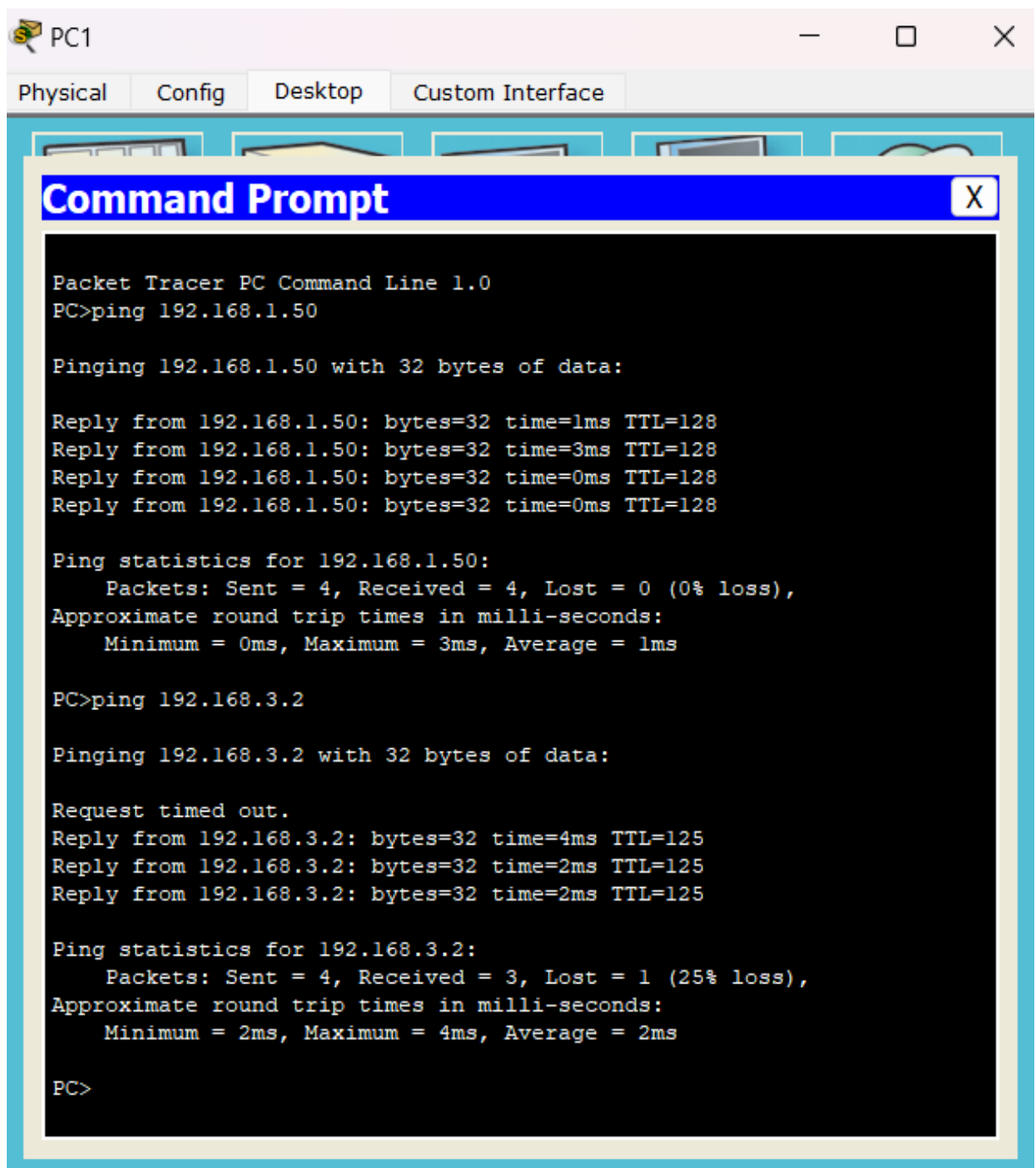
```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E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



The screenshot shows a Packet Tracer PC interface for PC1. The 'Command Prompt' window is open, displaying the results of two ping commands. The first command, 'ping 192.168.1.50', shows successful results with 0% loss. The second command, 'ping 192.168.3.2', shows a 25% loss (1 packet lost) and a request timeout.

```
Packet Tracer PC Command Line 1.0
PC>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=3ms TTL=128
Reply from 192.168.1.50: bytes=32 time=0ms TTL=128
Reply from 192.168.1.50: bytes=32 time=0ms 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 = 3ms, Average = 1ms

PC>ping 192.168.3.2

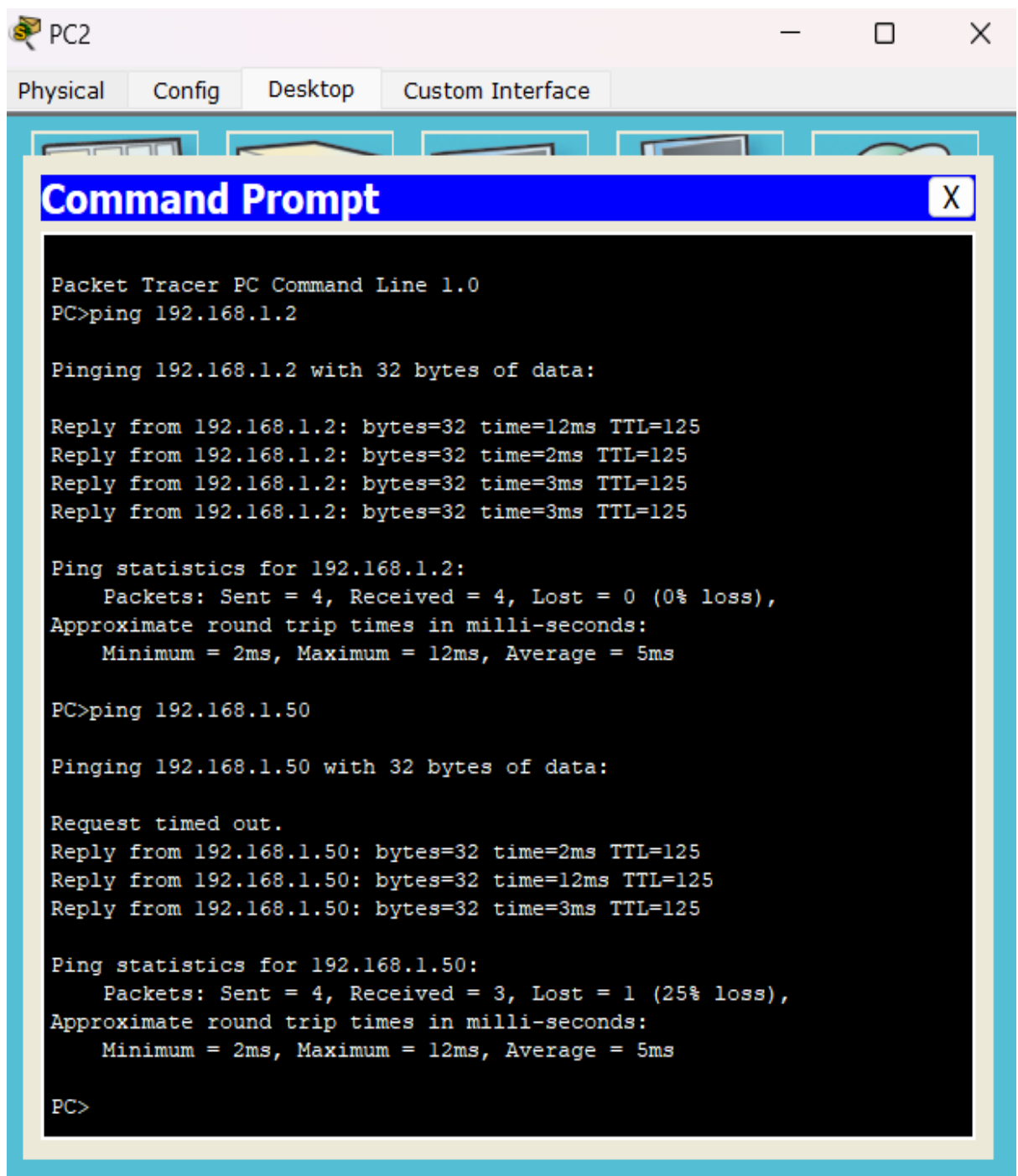
Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=4ms 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

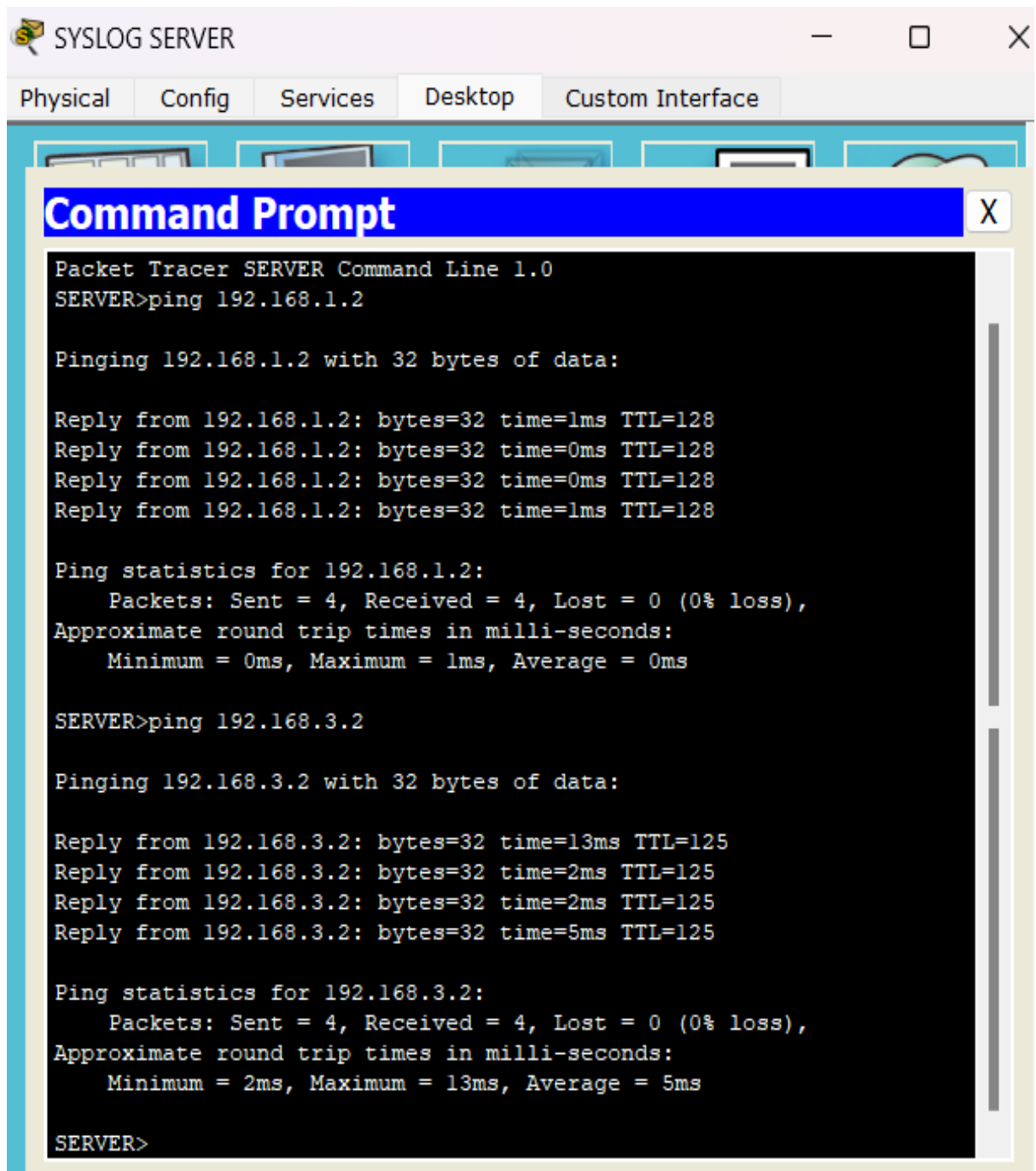
Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

PC>
```

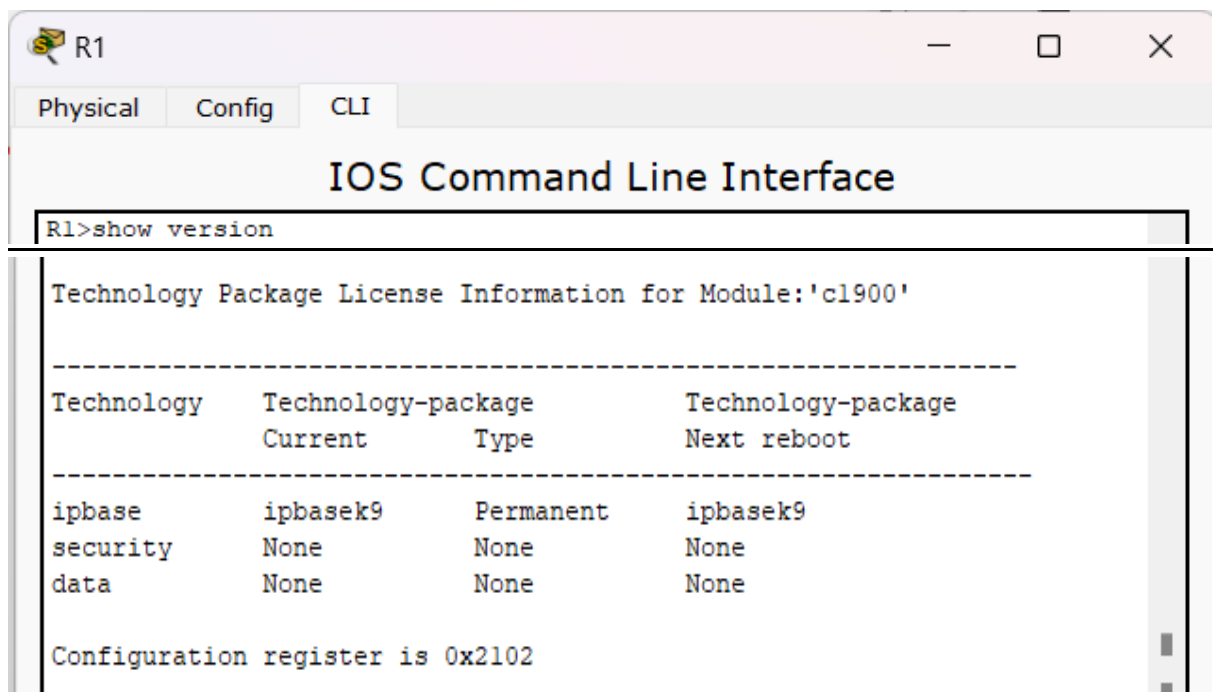
- PC 2



- SYSLOG SERVER



➤ **Enable the Secure Technology Package on R1 :**

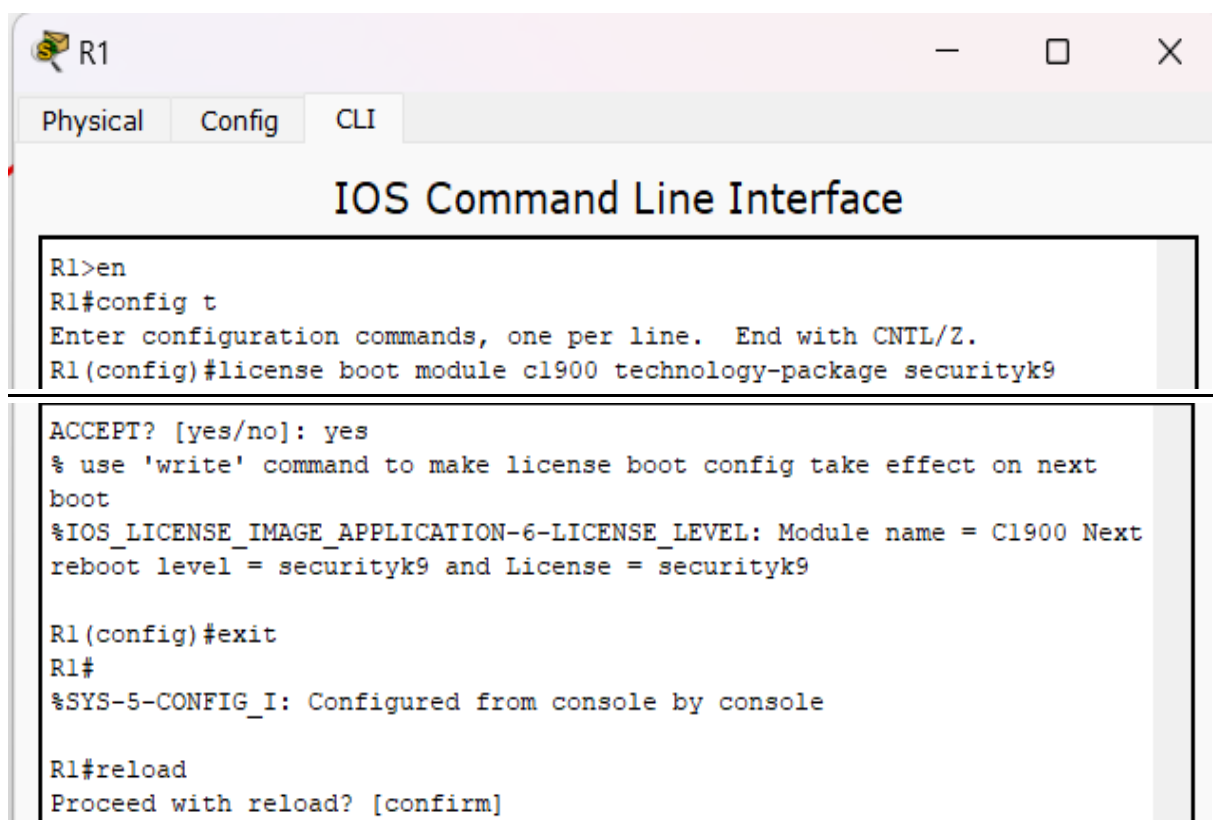


```
R1>show version
```

Technology Package License Information for Module:'cl900'

Technology	Technology-package Current	Technology-package Type	Technology-package 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 cl900 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:'cl900'
```

Technology	Technology-package Current	Type	Technology-package 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

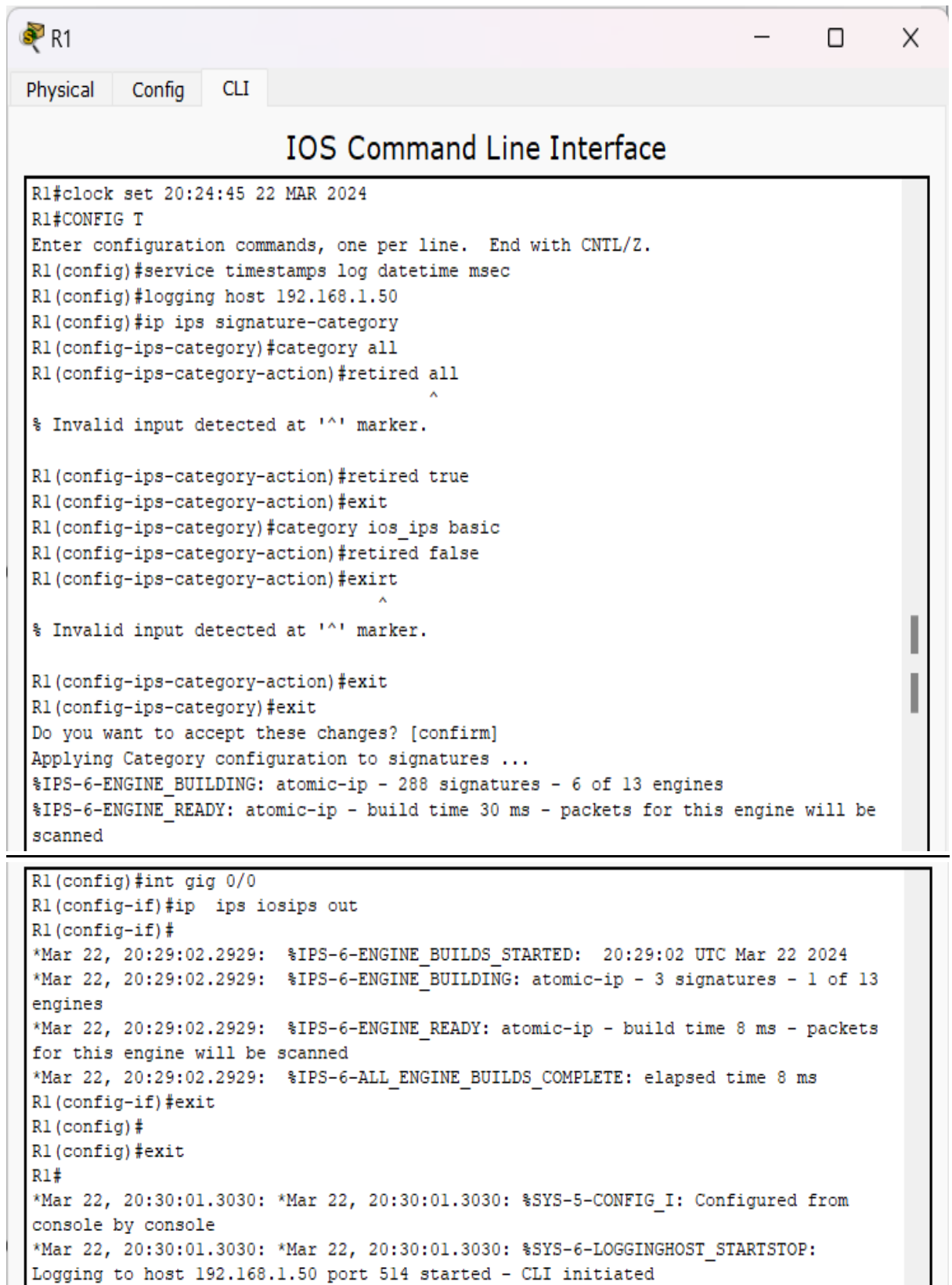
Config

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#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
```

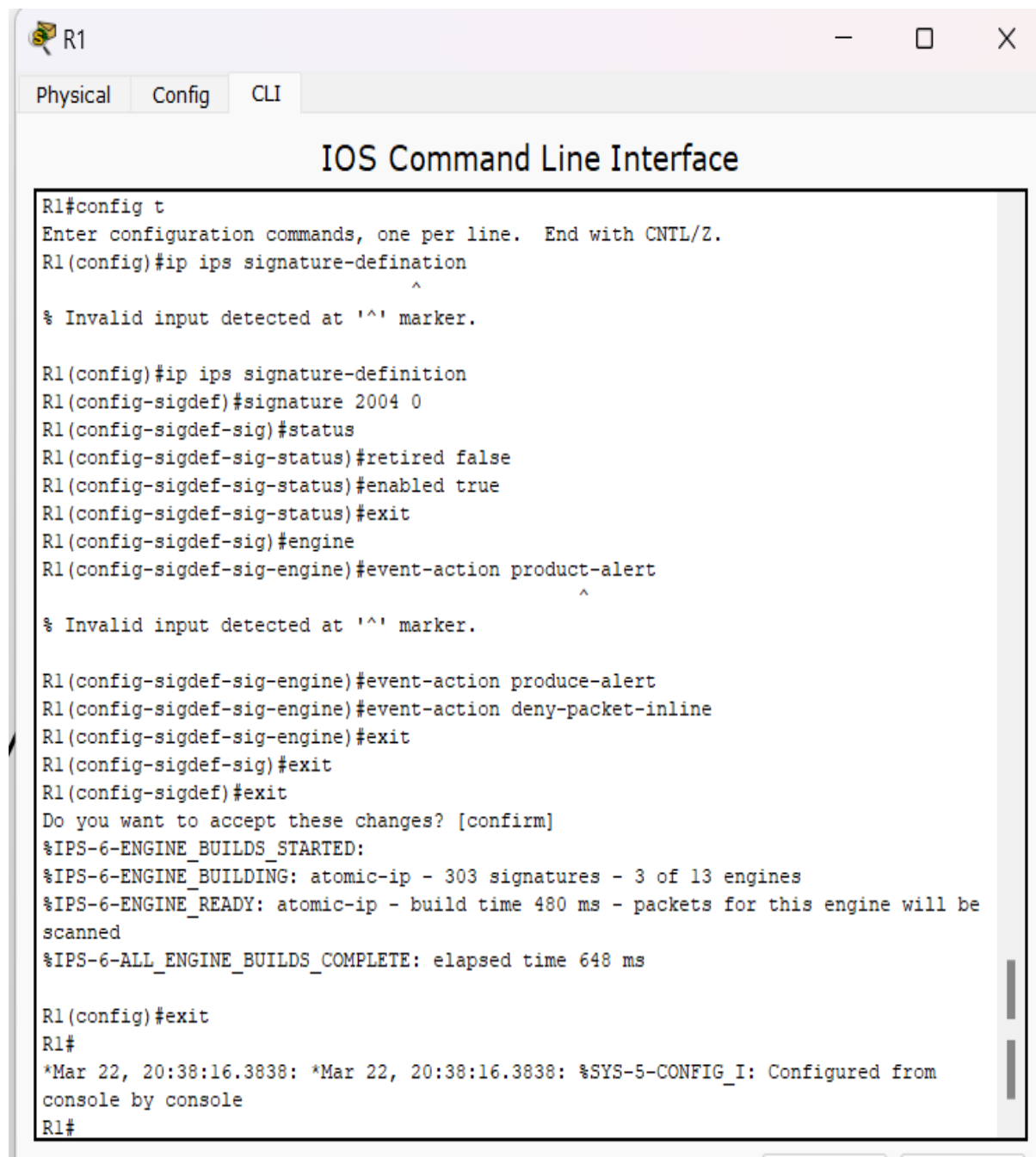
```
Interface GigabitEthernet0/0  
Inbound IPS rule is not set  
Outgoing IPS rule is iosips
```

```
IPS Category CLI Configuration:
```

```
Category all  
Retire: True  
Category ios_ips basic  
Retire: False
```

```
R1#
```

2. Modify the Signatures of the IPS:



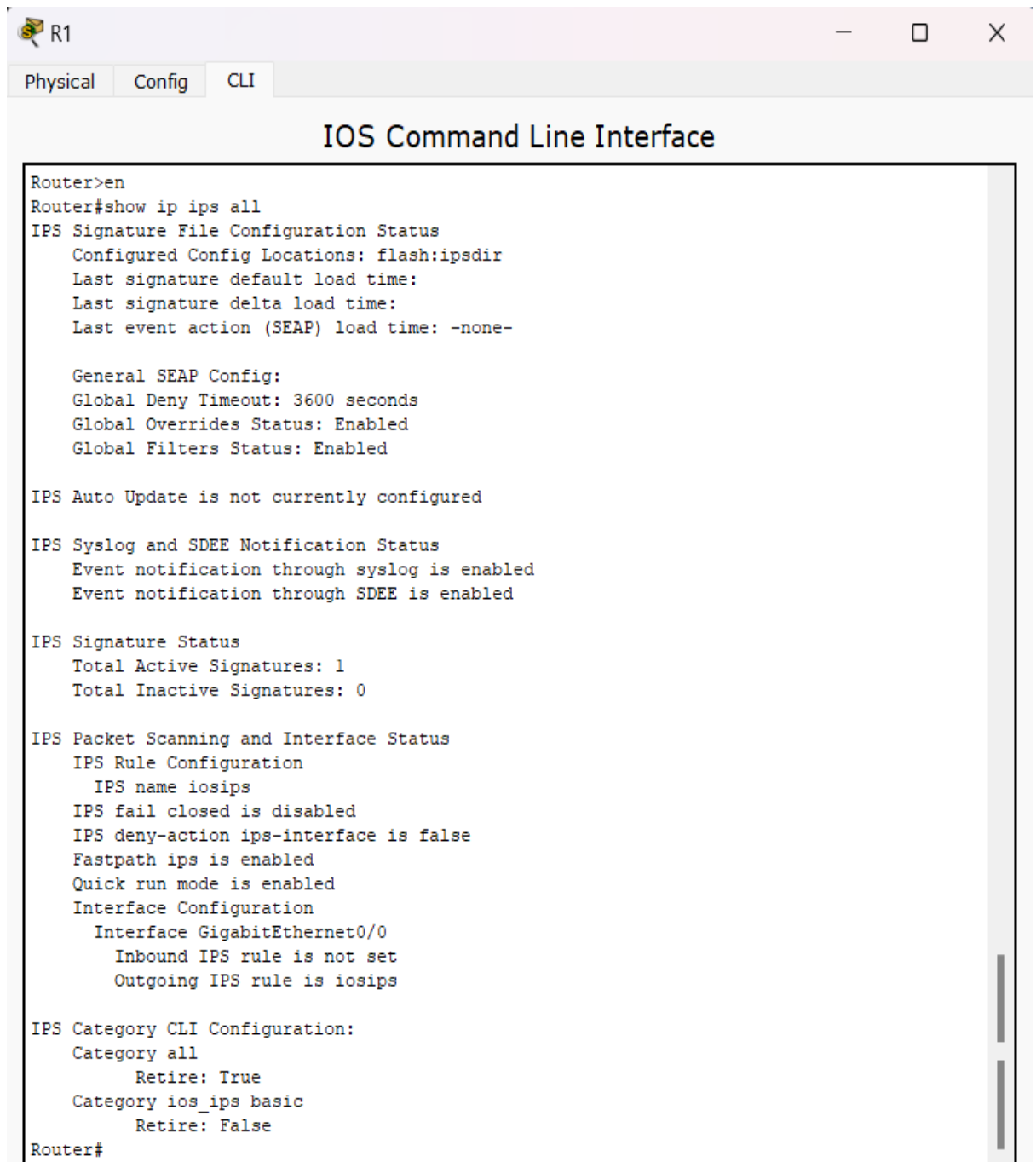
```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ips signature-definition
      ^
% Invalid input detected at '^' marker.

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:**



The screenshot shows a window titled 'R1' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command 'Router>en' has been entered, followed by 'Router#show ip ips all'. The output displays the IPS configuration status, including file configuration, SEAP config, auto update status, syslog and SDEE notification status, signature status, packet scanning and interface status, and category CLI configuration.

```
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

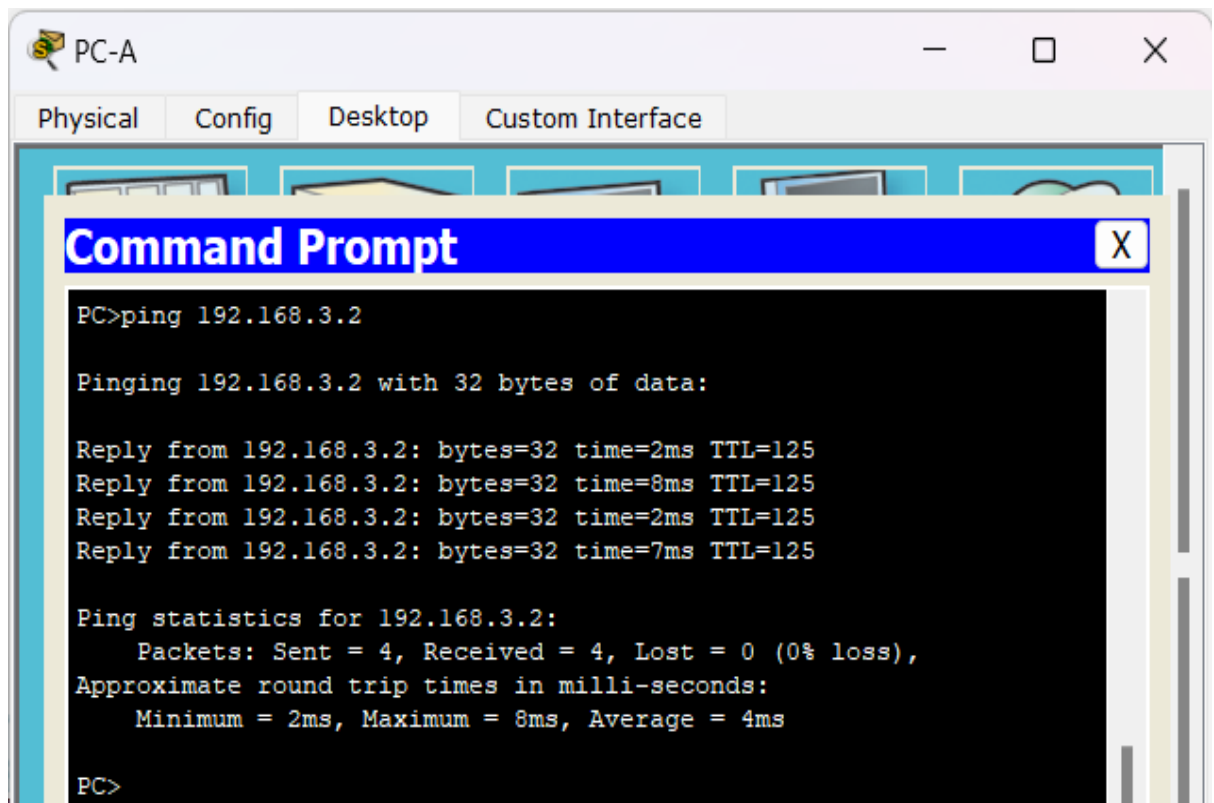
IPS Signature Status
  Total Active Signatures: 1
  Total Inactive Signatures: 0

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



The screenshot shows a window titled 'PC-A' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 192.168.3.2'. The output indicates that the ping was successful, with 4 packets sent and received, and a 0% loss. The round trip times are listed as 2ms, 8ms, 2ms, and 7ms.

```
PC>ping 192.168.3.2

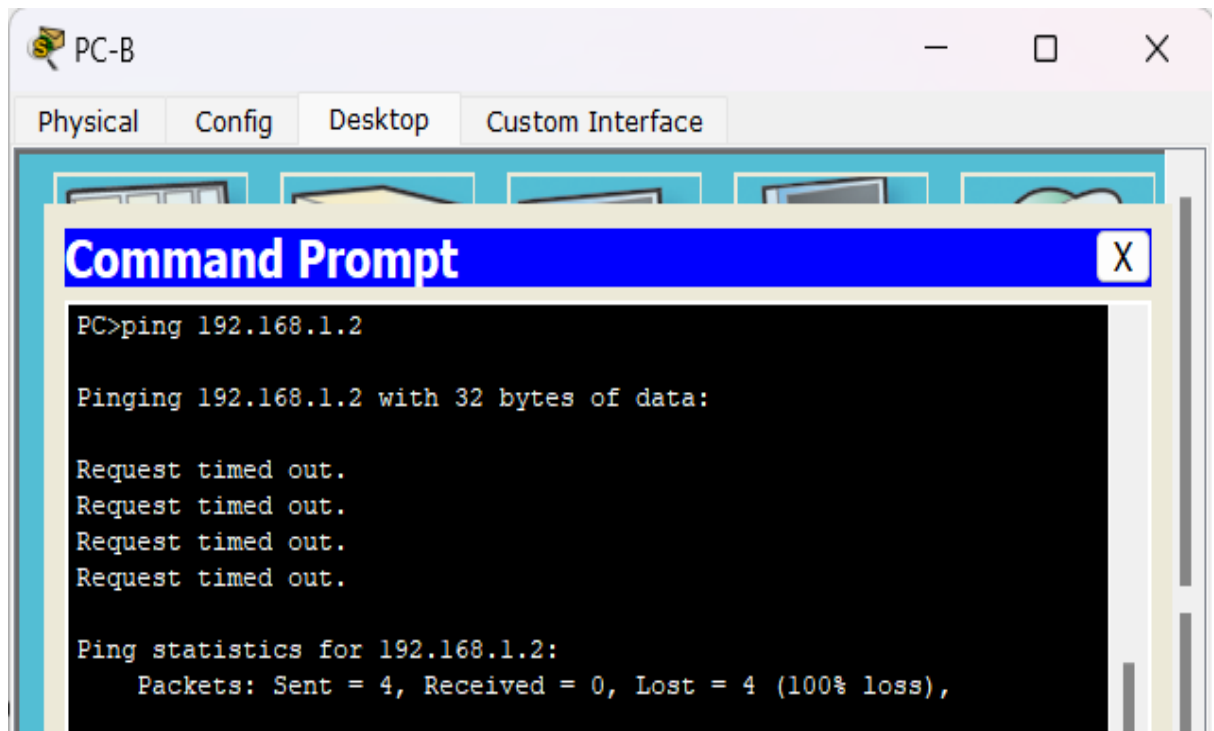
Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=8ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=7ms 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 = 8ms, Average = 4ms

PC>
```

- PC 2




The screenshot shows a window titled 'PC-B' with tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 192.168.1.2'. The output indicates that the ping failed, with 4 packets sent and 0 received, resulting in a 100% loss. The output also shows 'Request timed out.' for each of the four attempts.

```
PC>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

Custom Interface

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

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-