

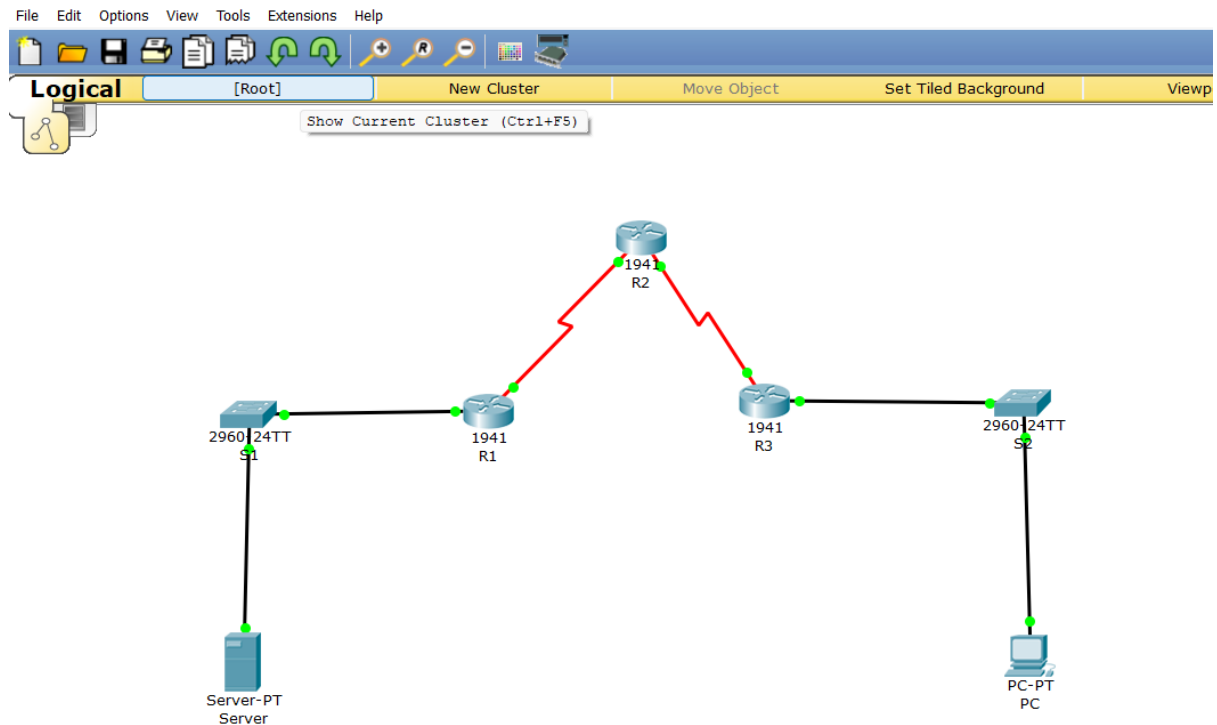
Date: 21/02/2024

Security in Computing

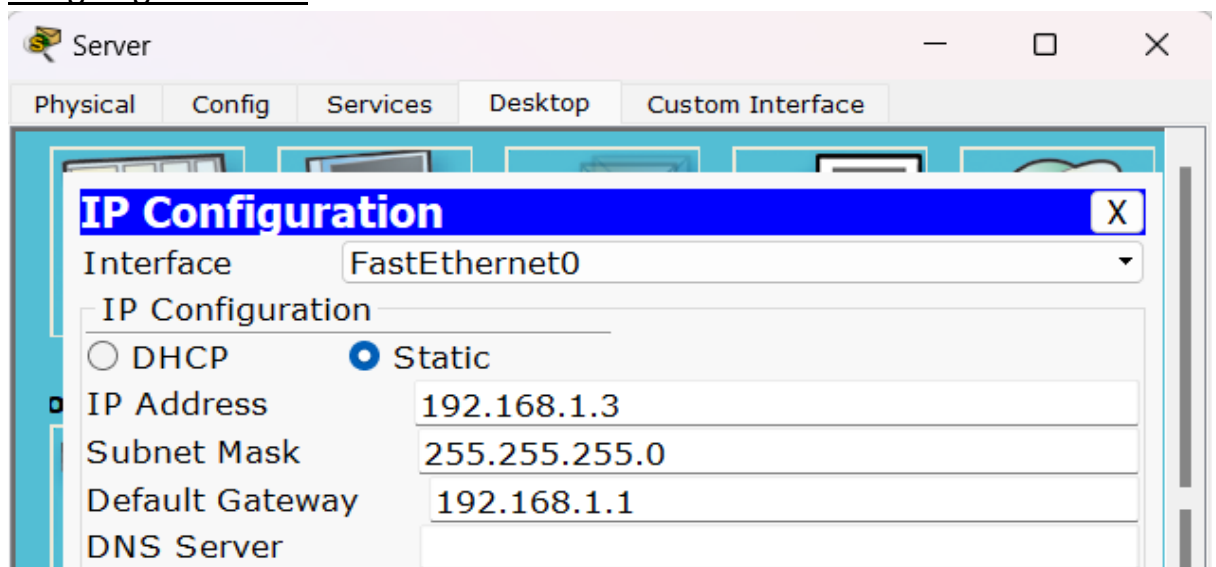
Practical 6:

Aim: Configuring a Zone-Based Policy Firewall.

➤ **Topology Daigram:**



➤ **Assigning IP Address:**



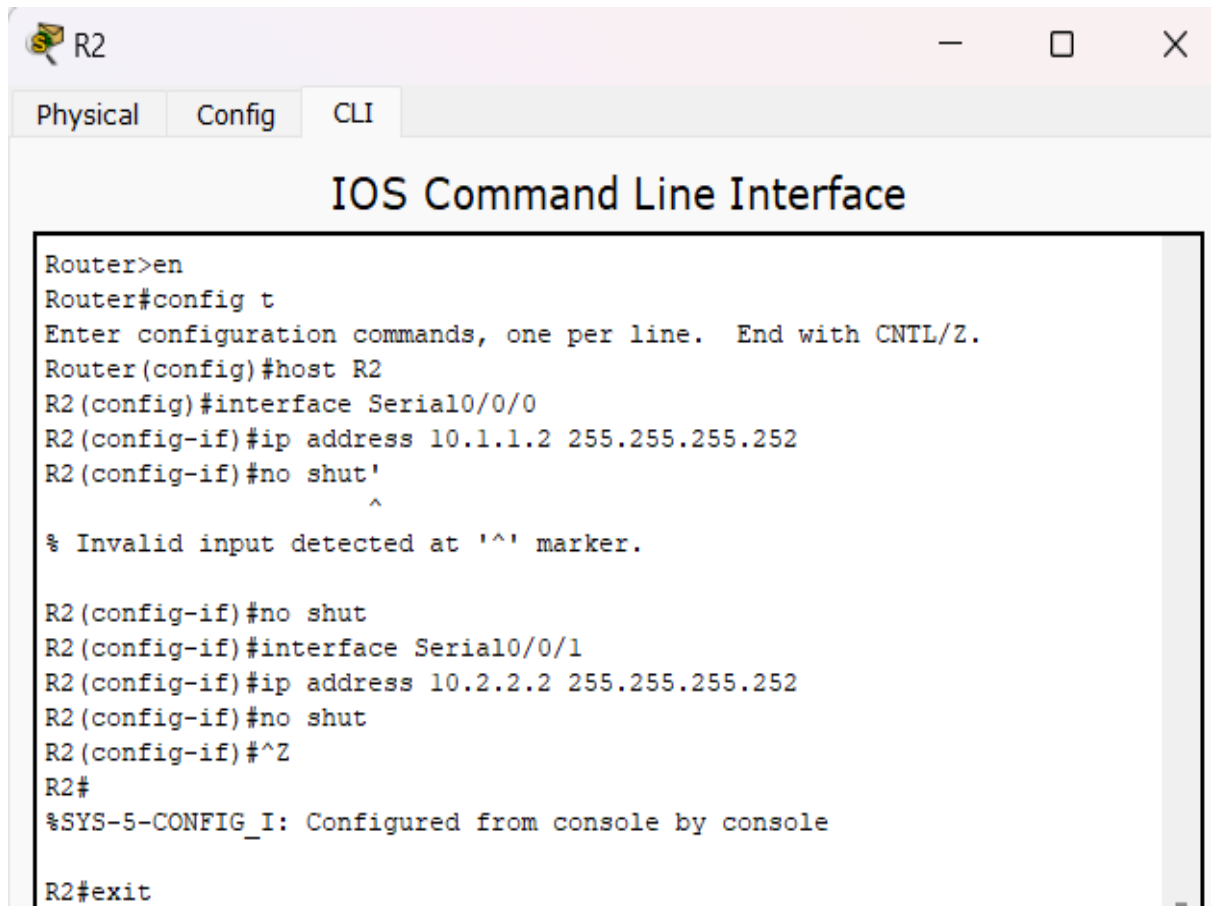
The screenshot displays two windows from a network simulation. The top window, titled 'PC', has tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Config' tab is active, showing the 'IP Configuration' dialog. In this dialog, 'Static' is selected for IP configuration. The fields are filled with: IP Address: 192.168.3.3, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.3.1, and DNS Server: (empty).

The bottom window, titled 'R1', has tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, showing the 'IOS Command Line Interface'. The terminal output shows the configuration of interfaces Serial0/0/0 and GigabitEthernet0/0. The output includes messages about link changes and protocol status, followed by the configuration commands and their execution results.

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

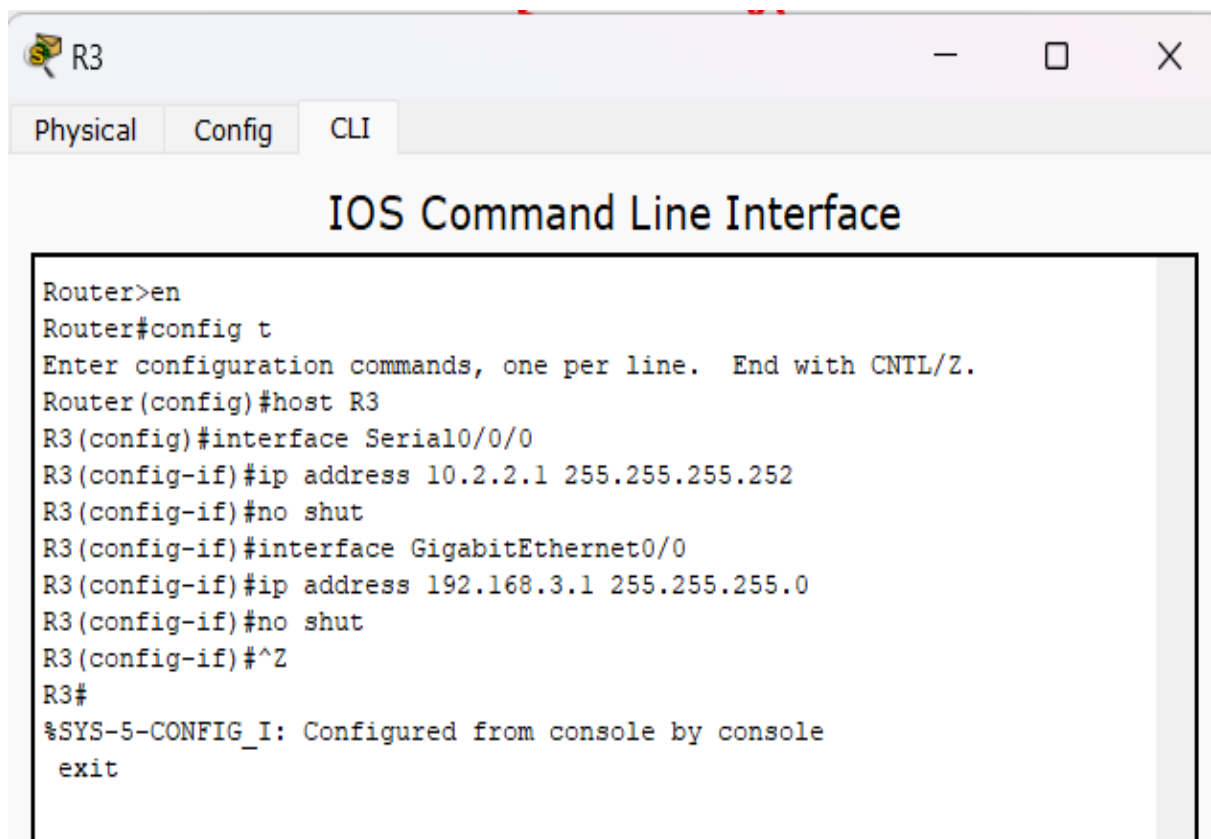
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#ip address 10.1.1.1 255.255.255.252
Router(config-if)#no shut
Router(config-if)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
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 terminal text shows the user entering 'en' to enter enable mode, then 'config t' to enter configuration mode. They configure the host to 'R2'. Under the 'Serial0/0/0' interface, they set the IP address to '10.1.1.2' with a subnet mask of '255.255.255.252' and attempt to shut it down. An error message appears: '% Invalid input detected at '^' marker.' because of a stray single quote. They then correct the command to 'no shut' and configure the 'Serial0/0/1' interface with IP '10.2.2.2' and mask '255.255.255.252', also setting 'no shut'. Finally, they press Ctrl-Z to exit configuration mode, which shows 'R2#' and a system message '%SYS-5-CONFIG_I: Configured from console by console'. The session ends with 'exit'.

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

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 a window titled 'R3' with three tabs: 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal text shows the user entering 'en' to enter enable mode, then 'config t' to enter configuration mode. They configure the host to 'R3'. Under the 'Serial0/0/0' interface, they set the IP address to '10.2.2.1' with a subnet mask of '255.255.255.252' and set 'no shut'. Then, under the 'GigabitEthernet0/0' interface, they set the IP address to '192.168.3.1' with a subnet mask of '255.255.255.0' and set 'no shut'. Finally, they press Ctrl-Z to exit configuration mode, which shows 'R3#' and a system message '%SYS-5-CONFIG_I: Configured from console by console'. The session ends with 'exit'.

```
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
exit
```

➤ Displaying IP Address details in routers

R1

Physical Config CLI

IOS Command Line Interface

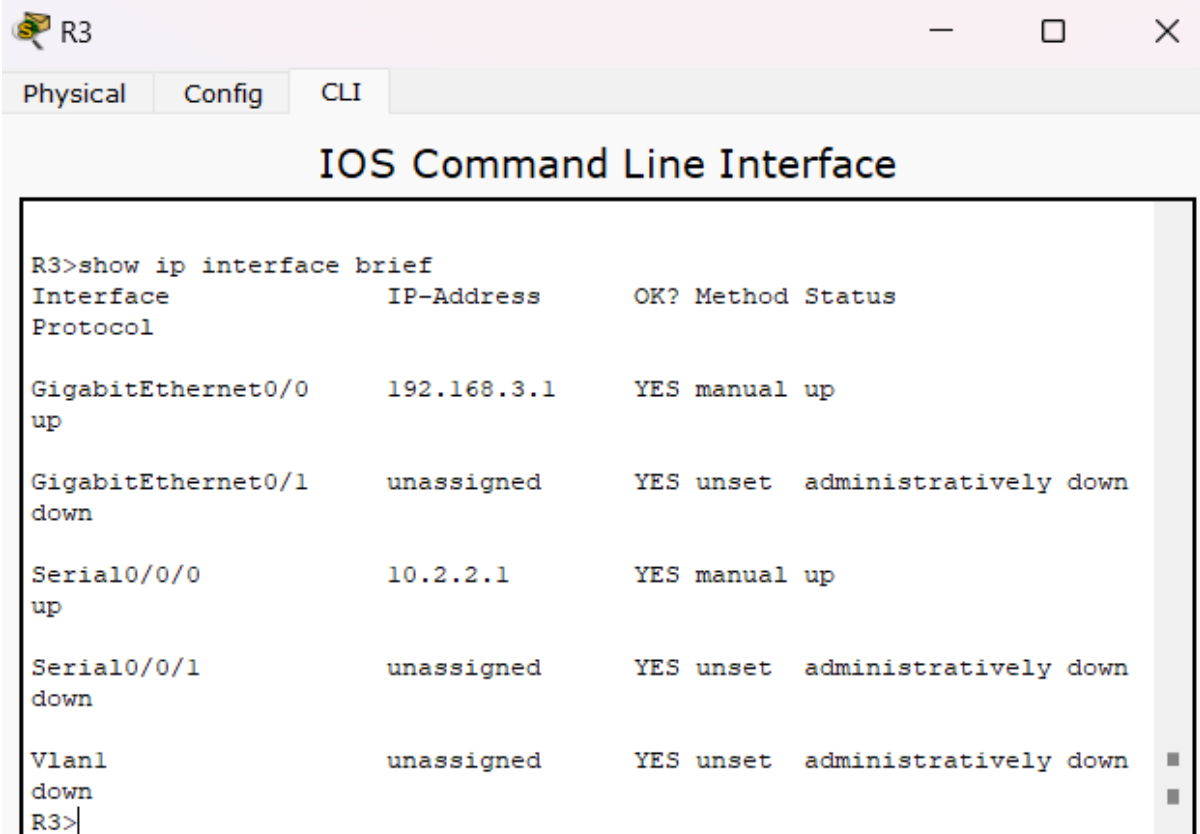
```
Router>show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 192.168.1.1     YES manual up
up
GigabitEthernet0/1 unassigned      YES unset  administratively down
down
Serial0/0/0        10.1.1.1        YES manual up
up
Serial0/0/1        unassigned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

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  up
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

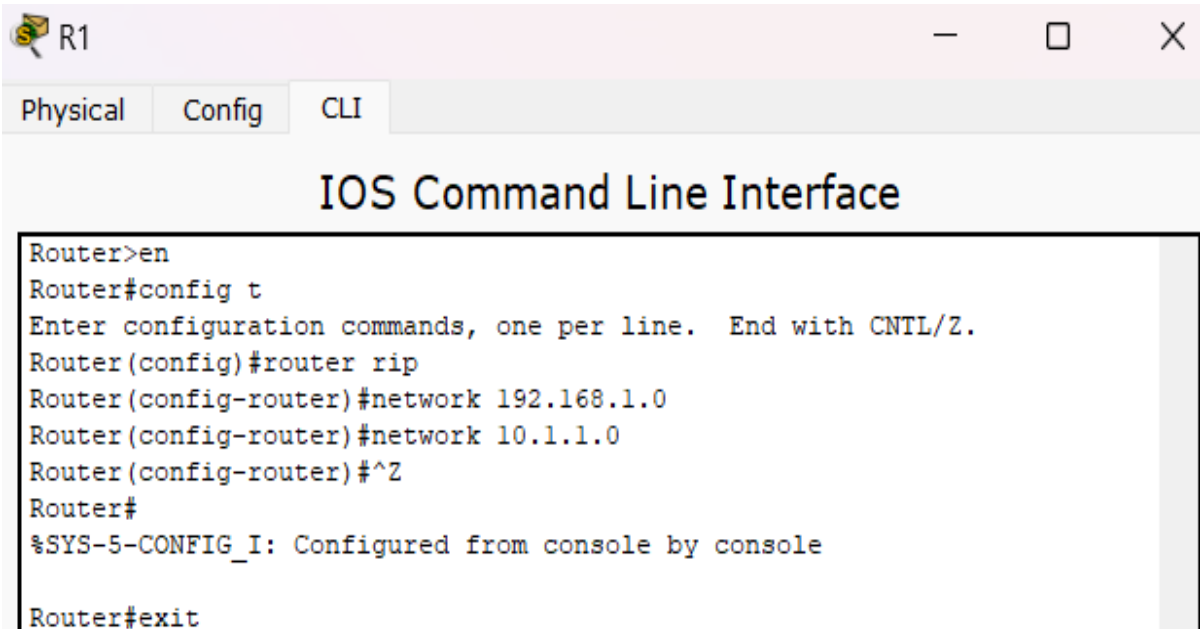
GigabitEthernet0/1  unassigned      YES unset  administratively down
down

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
R3>
```

➤ Configuring router




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)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 10.1.1.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#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 — □ ×

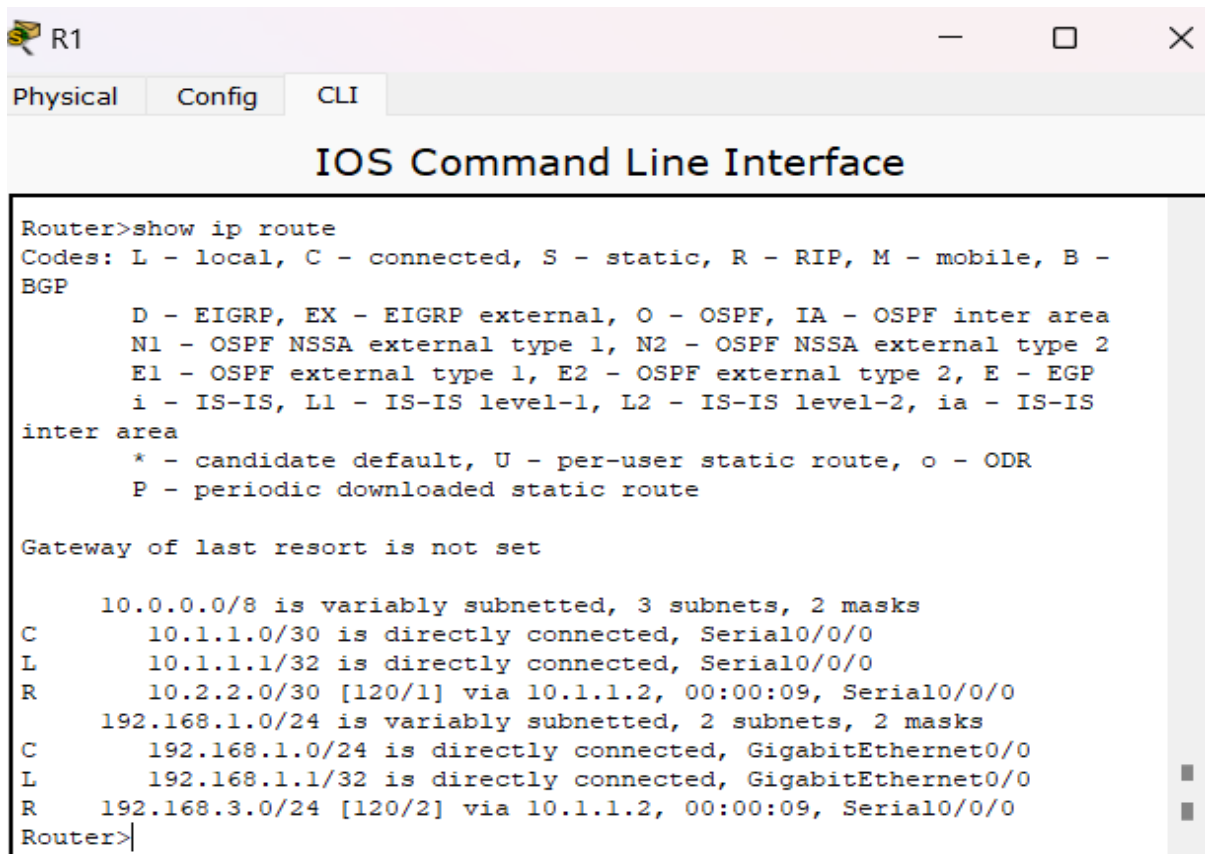
Physical Config CLI

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
```

➤ Showing IP route:



R1

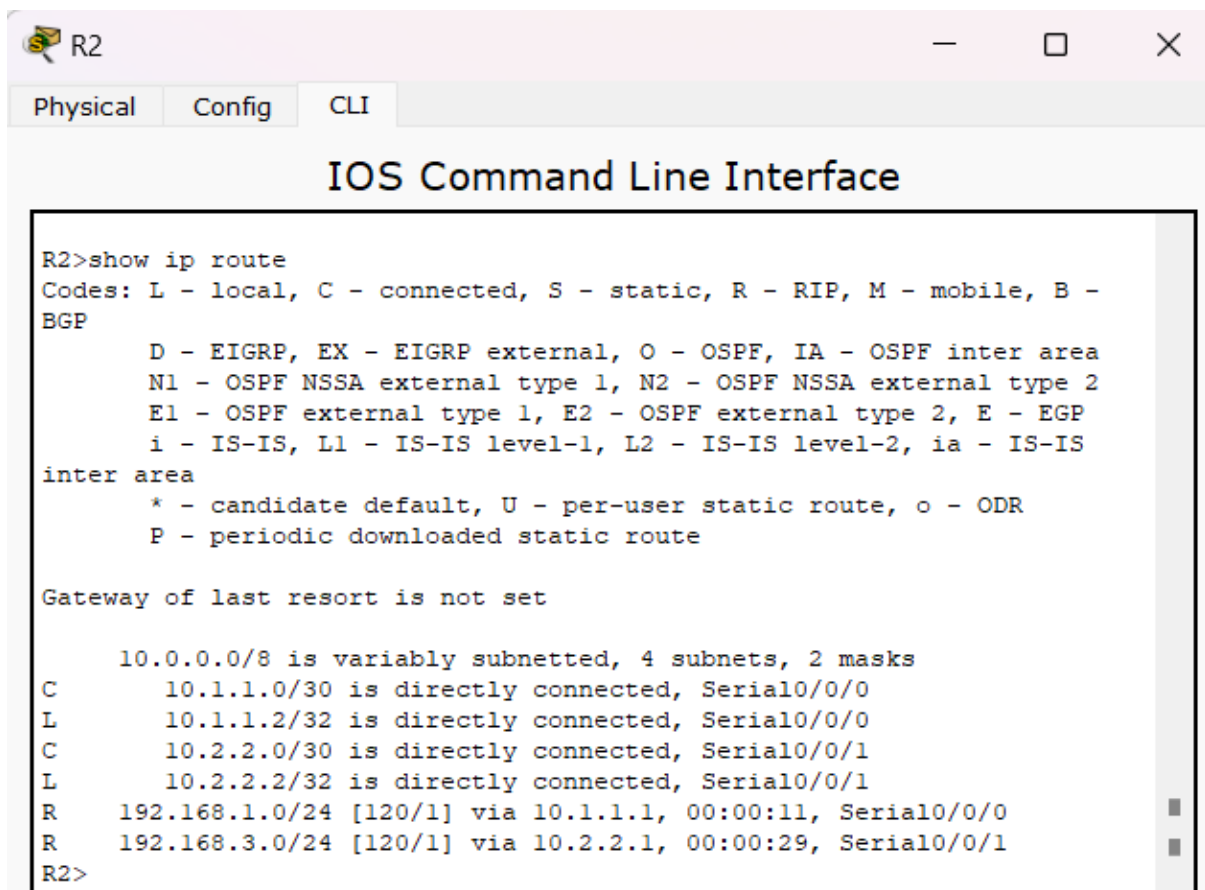
Physical Config CLI

IOS Command Line Interface

```
Router>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, 00:00:09, 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, 00:00:09, Serial0/0/0
Router>
```



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, 00:00:11, Serial0/0/0
R       192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:29, Serial0/0/1
R2>
```

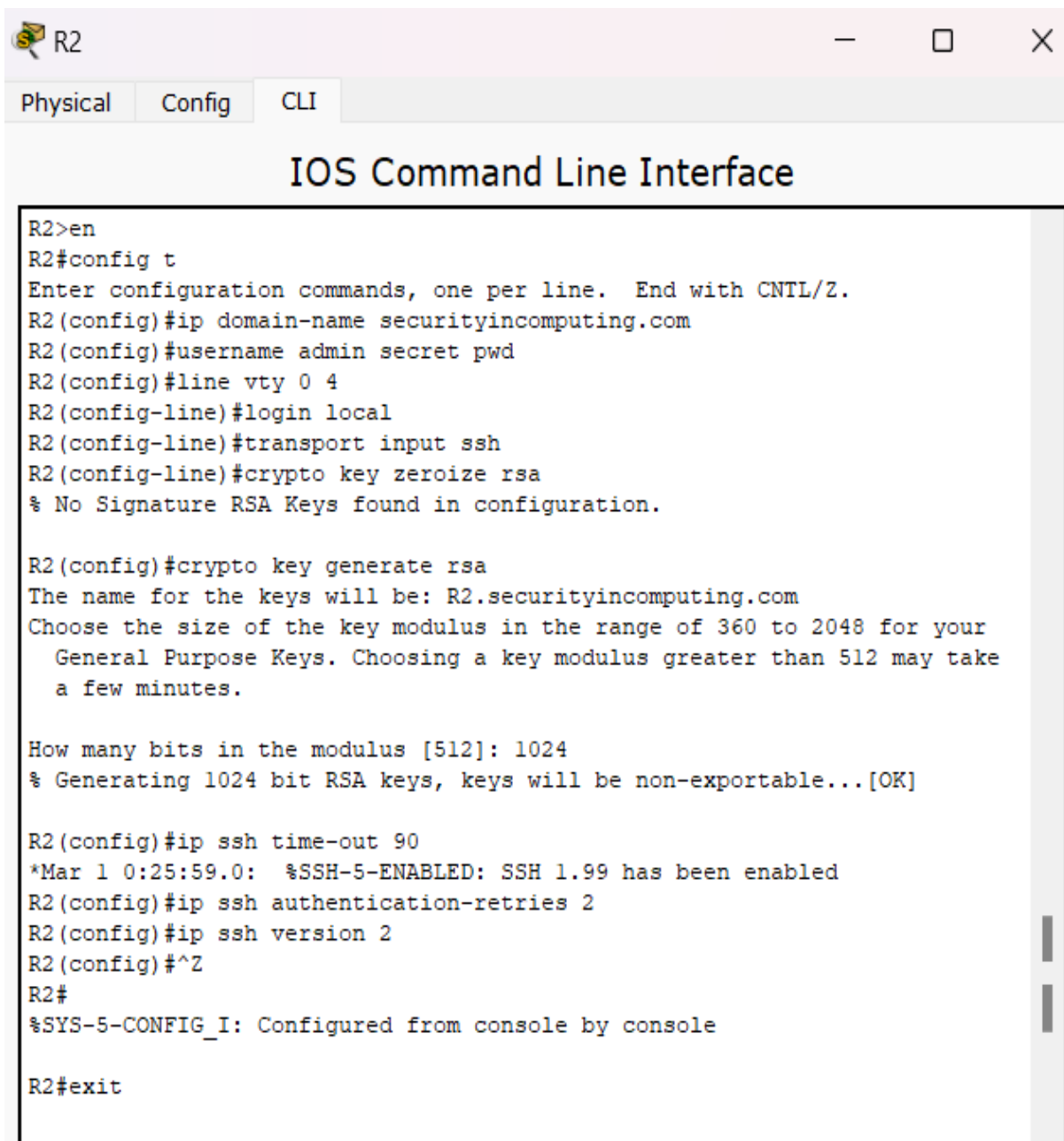


```
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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, 00:00:02, 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, 00:00:02, 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 SSH on R2



The screenshot shows a network device named R2 with three tabs: Physical, Config, and CLI. The CLI tab is active, displaying the 'IOS Command Line Interface'. The user enters the command 'en' to enter enable mode, followed by 'config t' to enter global configuration mode. The user then configures the domain name to 'securityincomputing.com', sets the username 'admin' with password 'secret', and enables VTY lines 0 to 4 for local login. The transport input is set to 'ssh', and the crypto key is set to 'zeroize rsa'. A message indicates that no signature RSA keys were found in the configuration. The user then generates RSA keys with the command 'crypto key generate rsa'. The system prompts for the key modulus size, and the user enters '1024'. A message indicates that the keys will be non-exportable. The user then sets the SSH time-out to 90, enables SSH, sets the authentication retries to 2, and sets the SSH version to 2. Finally, the user exits configuration mode with '^Z' and the CLI shows the configuration summary: '%SYS-5-CONFIG_I: Configured from console by console'. The user then exits the CLI with 'exit'.

```
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.

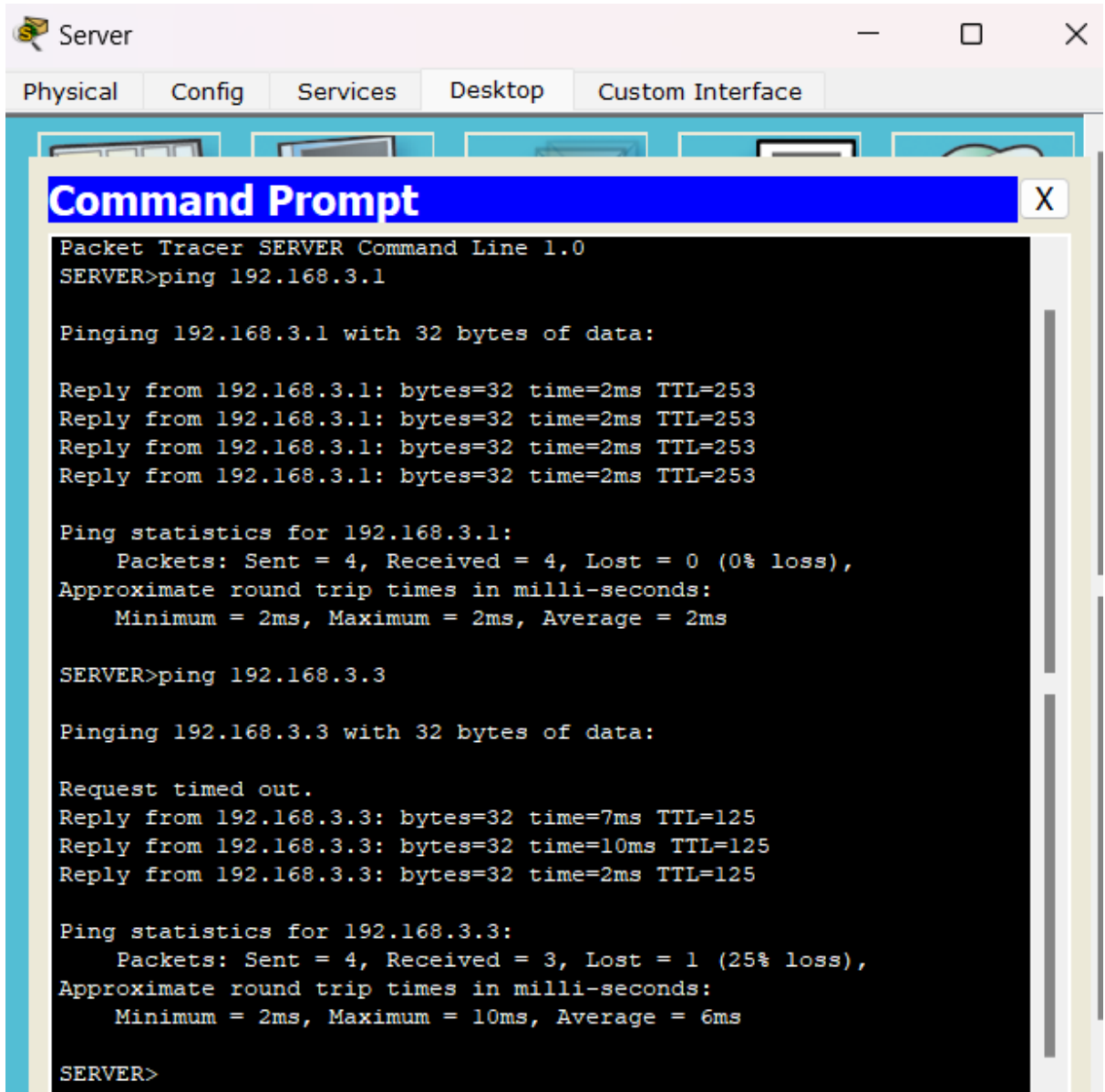
R2(config)#crypto key generate rsa
The name for the keys will be: R2.securityincomputing.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

R2(config)#ip ssh time-out 90
*Mar 1 0:25:59.0: %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 the 'Server' window in Packet Tracer with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the output of two ping commands. The first command, 'ping 192.168.3.1', shows successful connectivity with 4 packets received and 0% loss. The second command, 'ping 192.168.3.3', shows a 25% packet loss (1 packet lost) and a higher round trip time.

```
Packet Tracer SERVER Command Line 1.0
SERVER>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=2ms 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 = 2ms, Average = 2ms

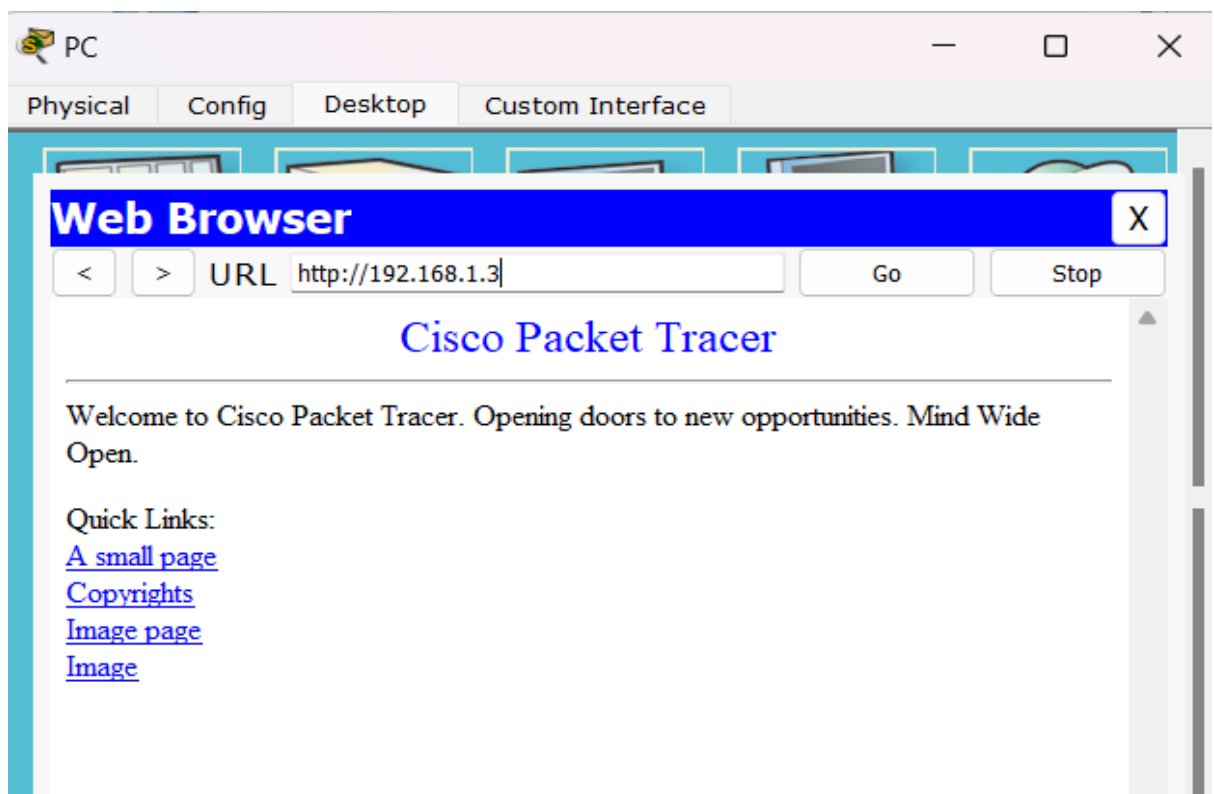
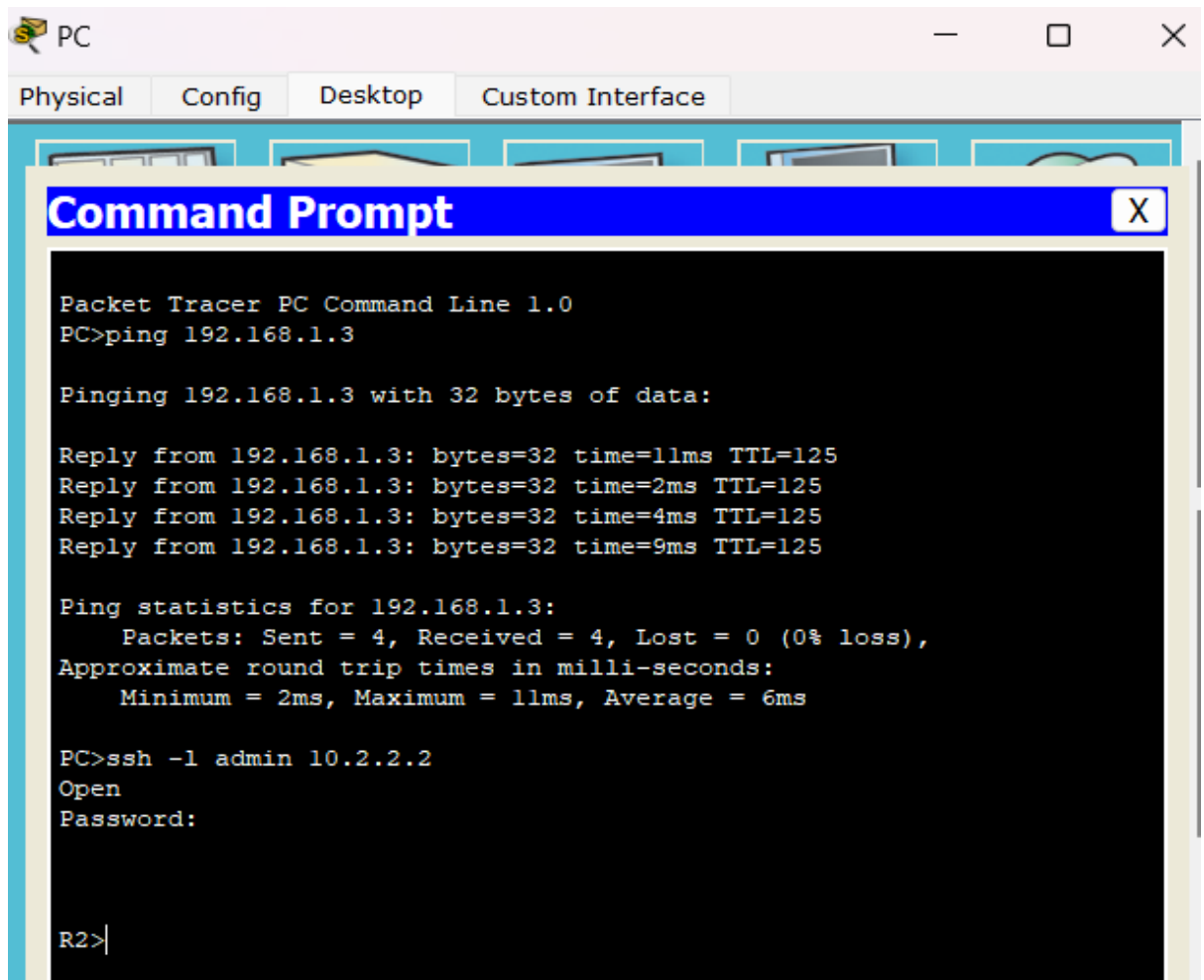
SERVER>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time=7ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 6ms

SERVER>
```



- Enable the security technology package on R



The screenshot shows a window titled 'R3' with tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command 'R3>show version' has been entered, resulting in the following output:

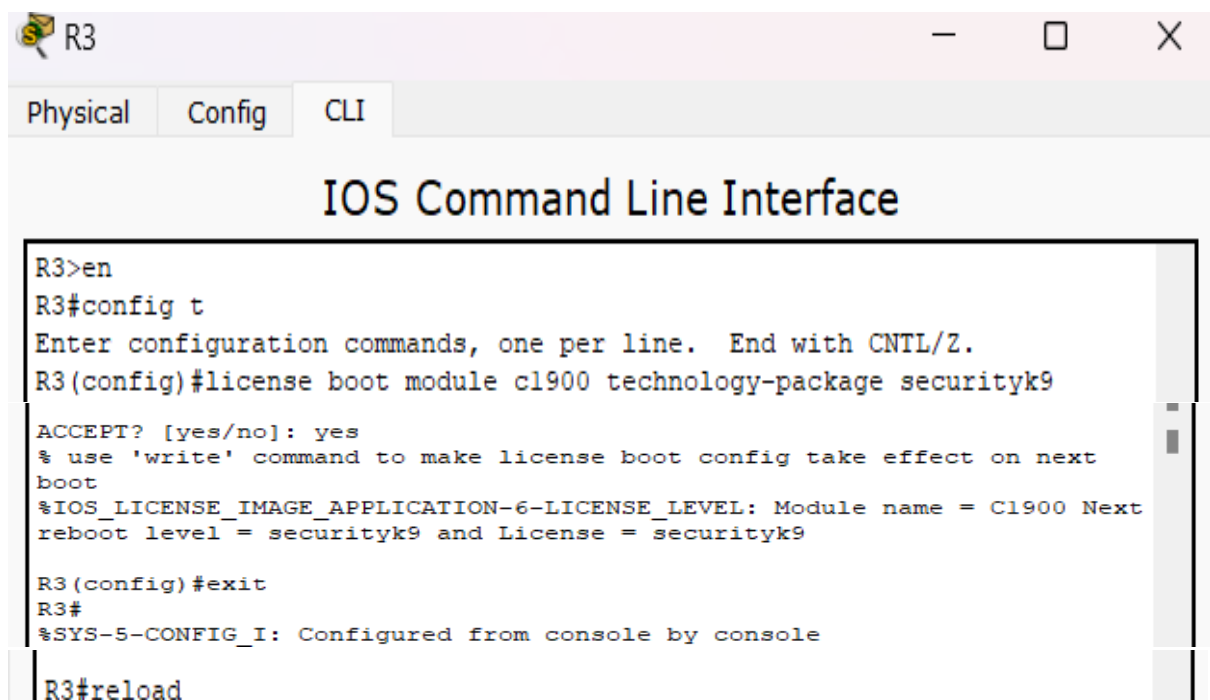
```

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

```



The screenshot shows the same 'R3' window with the 'CLI' tab active. The following commands have been entered to enable the security technology package:

```

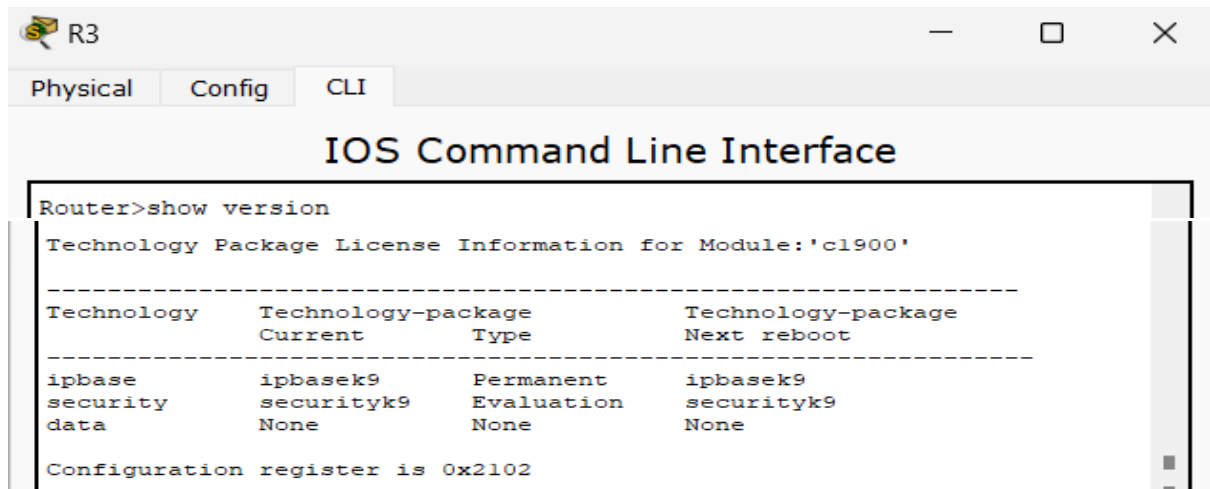
R3>en
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#license boot module c1900 technology-package securityk9

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

```



R3

Physical Config CLI

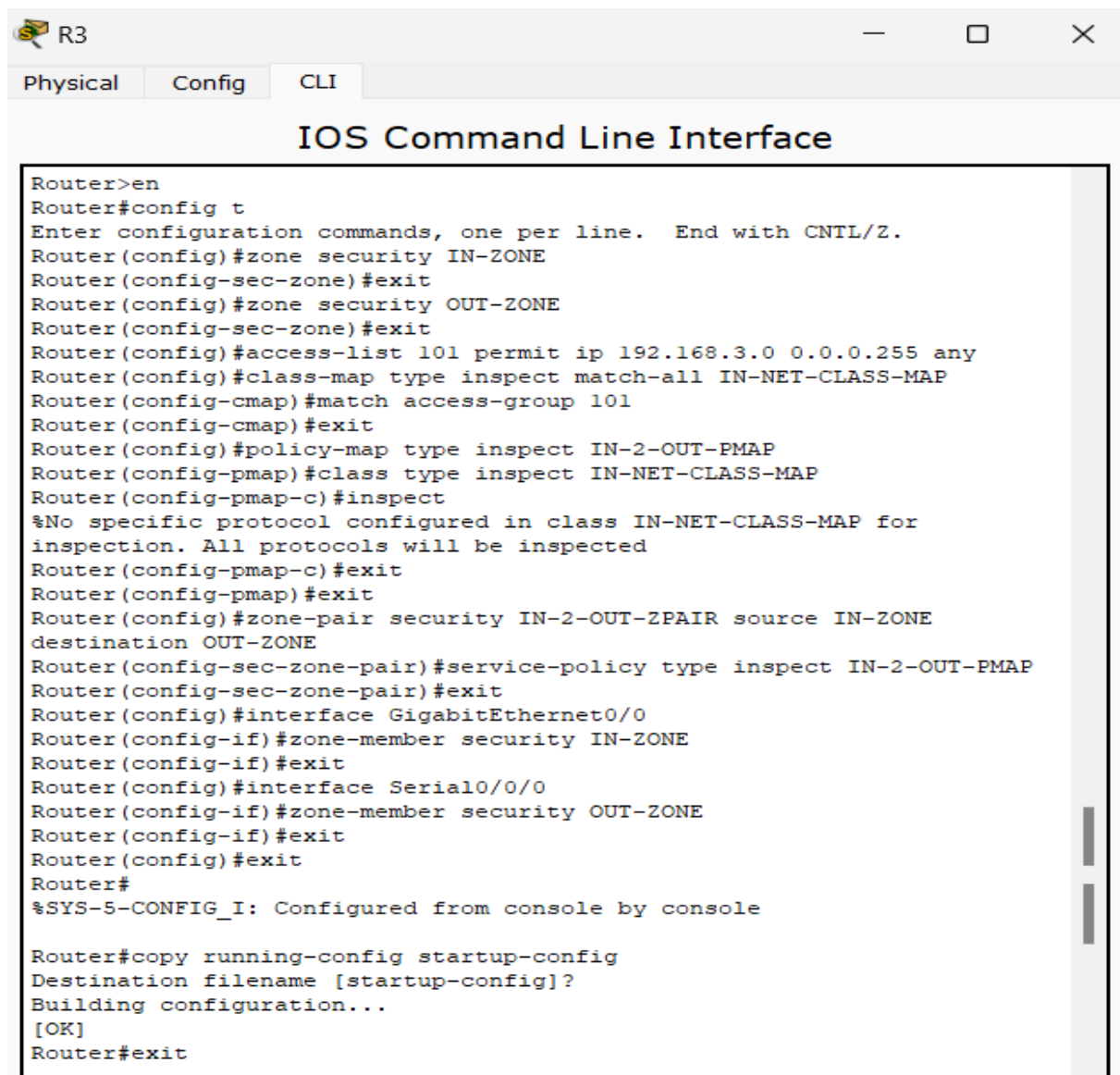
IOS Command Line Interface

```
Router>show version

Technology Package License Information for Module:'c1900'

-----
Technology      Technology-package      Technology-package
Current         Type                    Next  reboot
-----
ipbase          ipbasek9                Permanent
security        securityk9              Evaluation
data            None                    None
Configuration register is 0x2102
```

- Create the Firewall Zones , Class Maps and ACLs on R3:



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

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

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

The screenshot displays two windows from the Packet Tracer application. The top window is titled 'PC' and has tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Desktop' tab is active, showing a 'Command Prompt' window. The command prompt text is as follows:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=11ms 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=9ms 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 = 11ms, Average = 6ms

PC>ssh -l admin 10.2.2.2
Open
Password:

R2>
```

The bottom window is titled 'R3' and has tabs for 'Physical', 'Config', and 'CLI'. The 'CLI' tab is active, showing the 'IOS Command Line Interface'. The command prompt text is as follows:

```
Router>en
Router#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
Router#
```

The image shows two overlapping windows from the Cisco Packet Tracer application. The top window is titled 'Web Browser' and displays the Cisco Packet Tracer homepage. The bottom window is titled 'R3' and shows the 'IOS Command Line Interface' for a router.

Web Browser Window:

- Address bar: `http://192.168.1.3`
- Page Title: Cisco Packet Tracer
- Content: Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open. Quick Links: [A small page](#), [Copyrights](#), [Image page](#), [Image](#)

R3 Window (IOS Command Line Interface):

```
Router>en
Router#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
Router#
```

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

