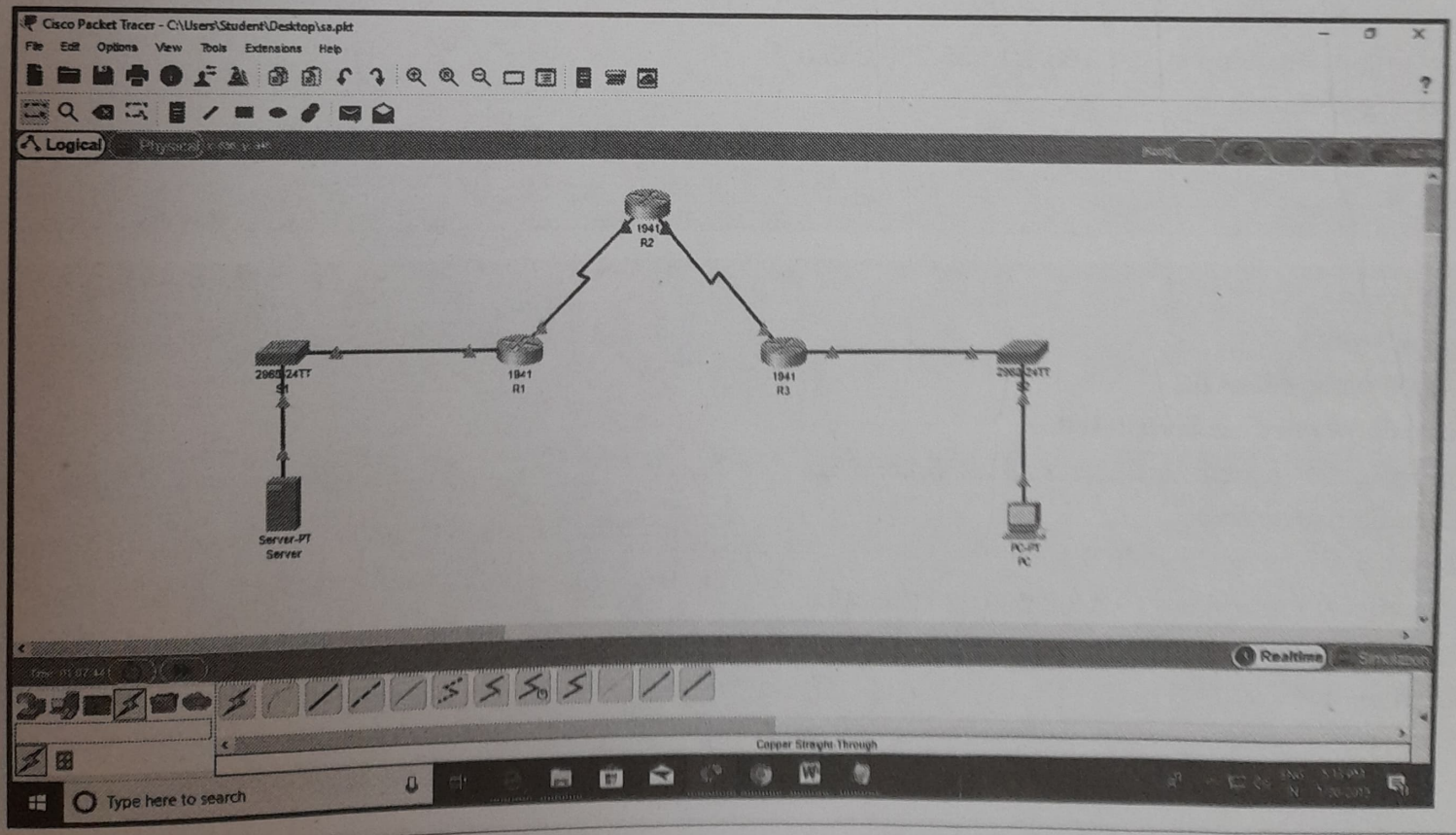
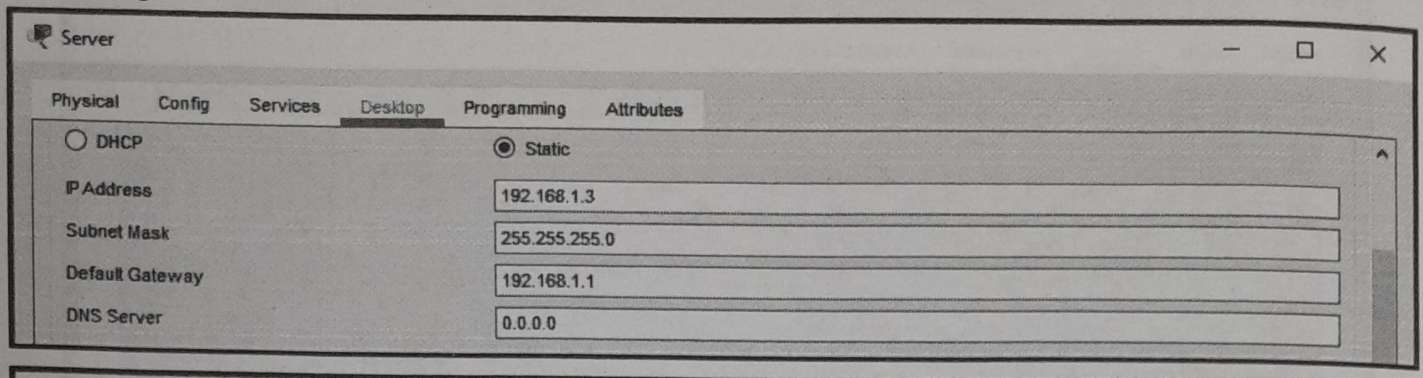
Practical 6

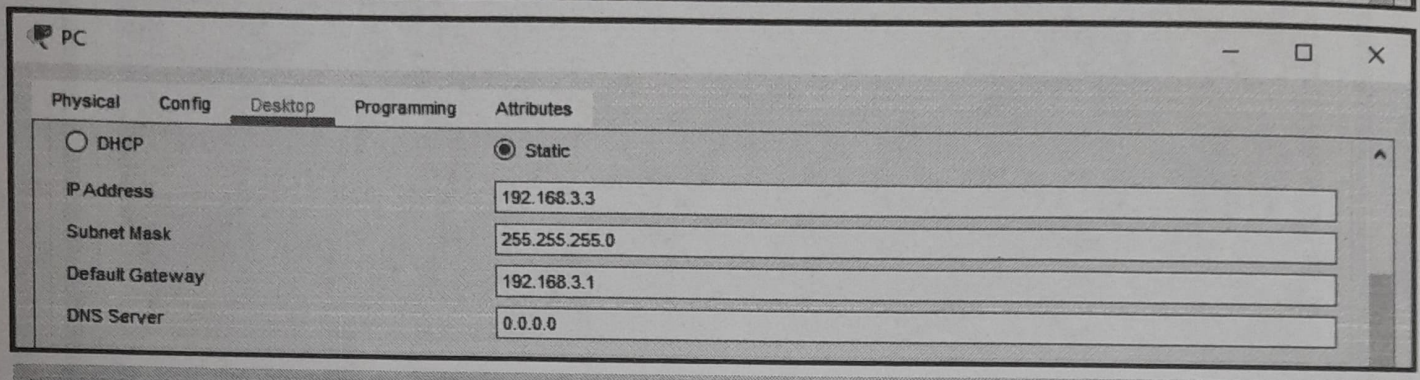
▶ **Aim : Configuring a Zone-Based Policy Firewall**

☞ **Topology Diagram**



Assign IP Addresses






```
Router>en
Router#conf t
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)#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#exit
```

```
Router>en
Router#conf t
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)#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#exit
```

```
Router>en
Router#conf t
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)#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#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
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
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
Vlan1 unassigned YES unset administratively down down
```

☞ Configure RIP on routers

```
R1>en
R1#conf t
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#exit
```

```
R2>en
R2#conf t
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#exit
```

```
R3>en
R3#conf t
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#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, 00:00:01, 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, 00:00:01, 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, 00:00:10, Serial0/0/0
R 192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:28, 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, 00:00:11, 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, 00:00:11, 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
```

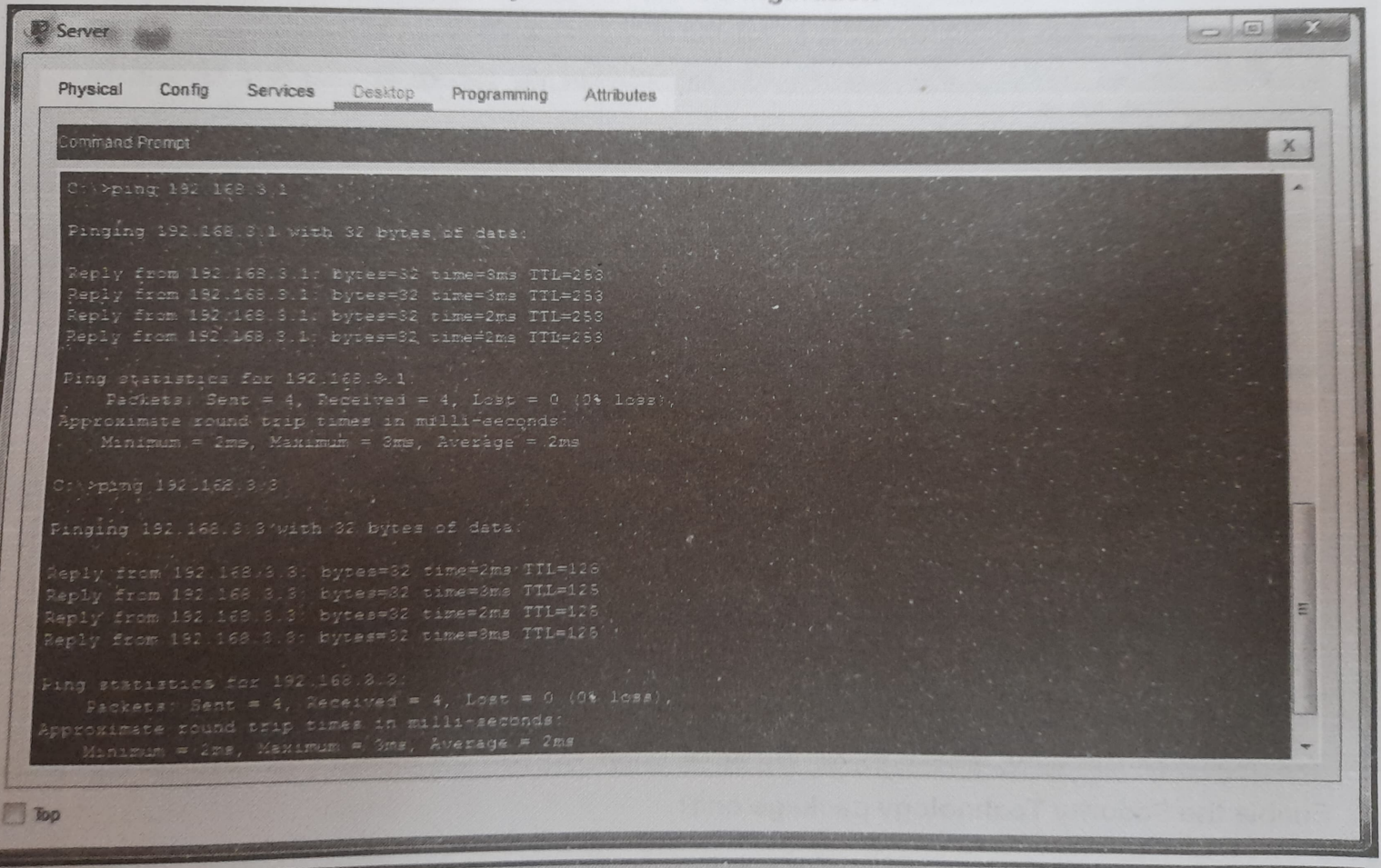
☞ **Configure SSH on R2**

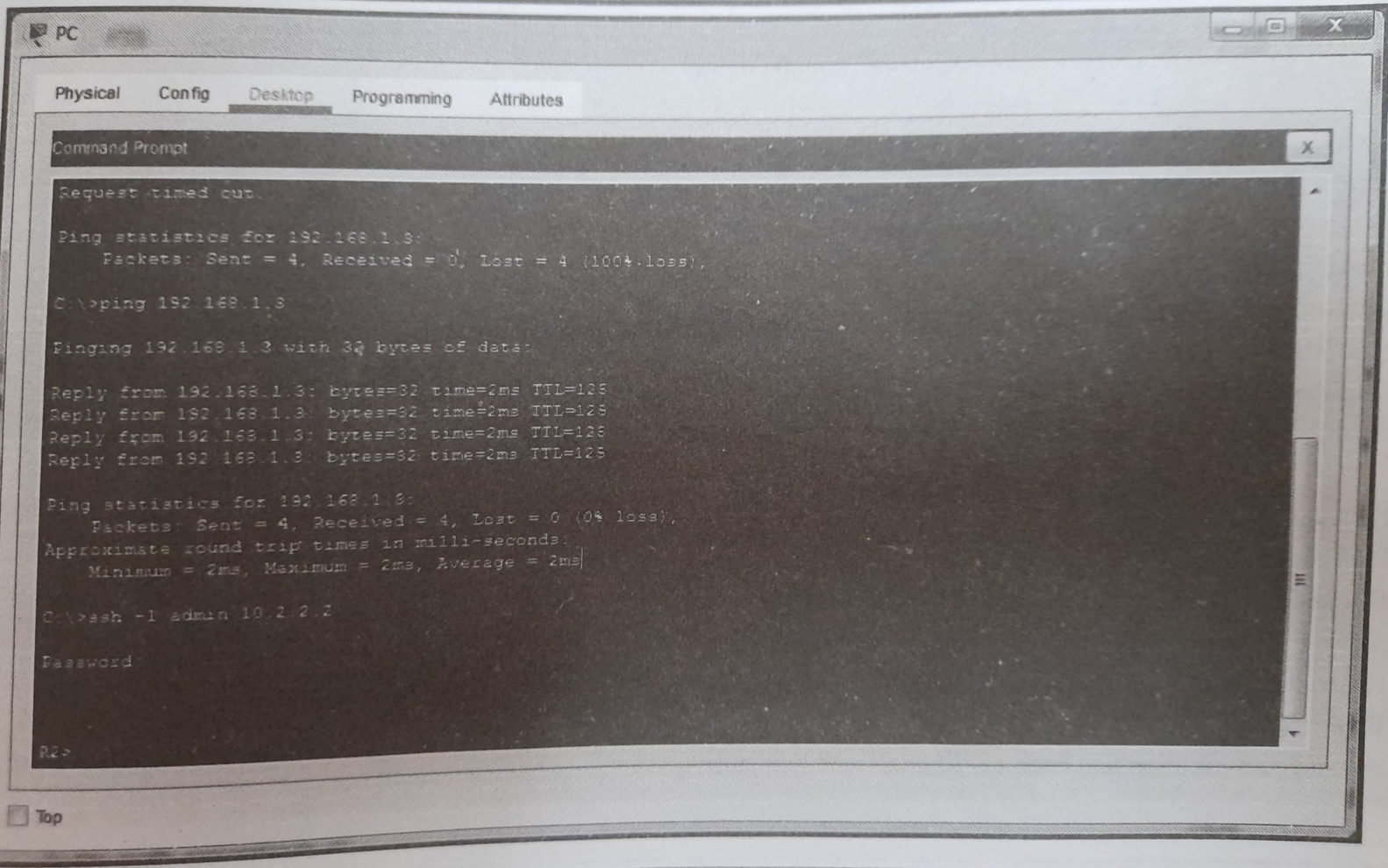
```
R2>en
R2#conf t
R2(config)#ip domain-name securityincomputing.com
R2(config)#username admin secret pwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key zeroizersa
% No Signature RSA Keys found in configuration.
R2(config)#crypto key generate rsa
```

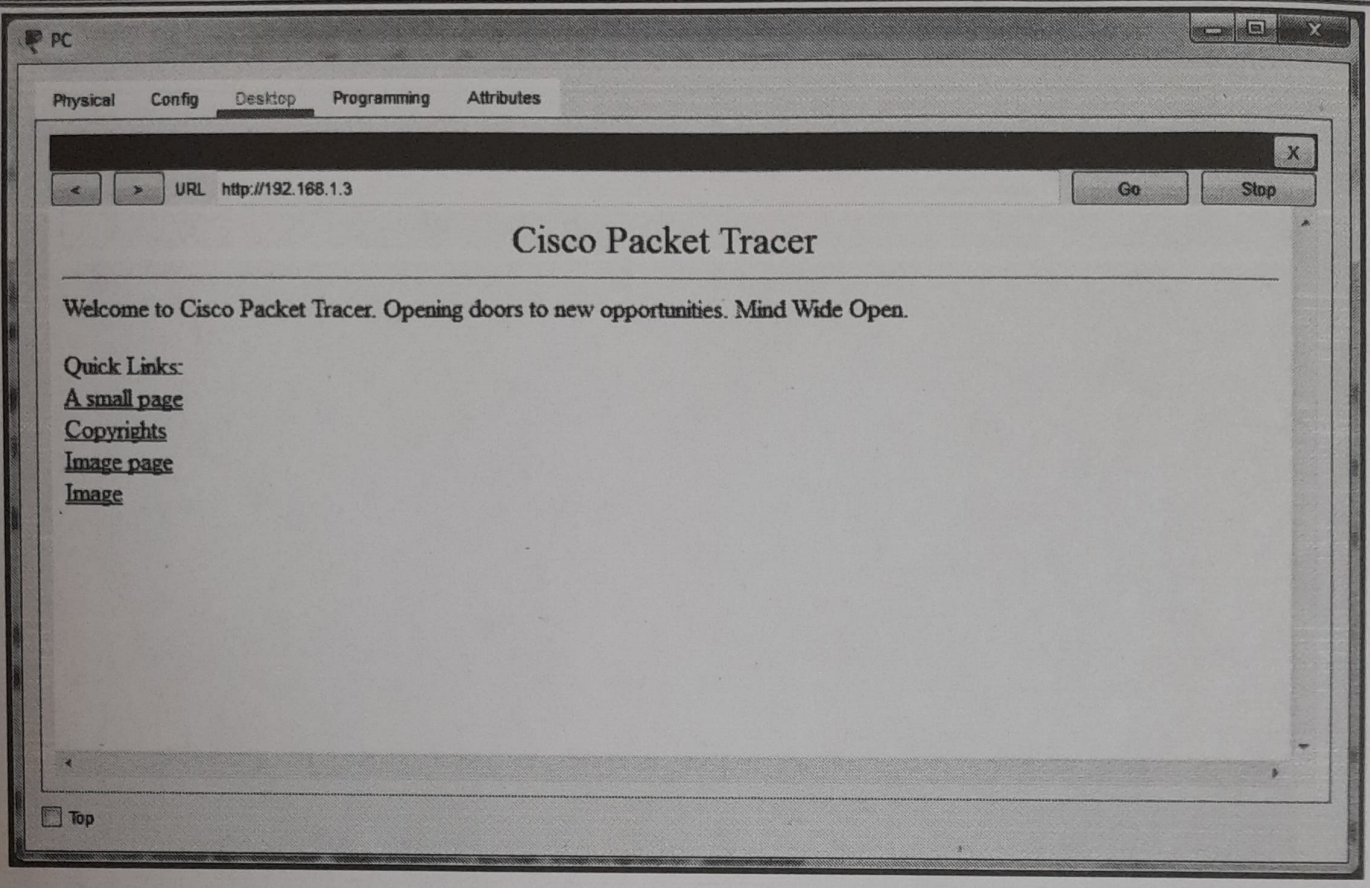
- The name for the keys will be: R2.securityincomputing.com
- Choose the size of the key modulus in the range of 360 to 2048 for yourGeneral Purpose Keys. Choosing a key modulus greater than 512 may takea few minutes.
- How many bits in the modulus [512]: 1024

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#ipssh time-out 90
*Mar 1 0:21:14.577: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ipssh authentication-retries 2
R2(config)#ipssh version 2
R2(config)# ^ Z
R2#exit
```

☞ Verify Basic Network Connectivity before ACL Configuration




PC
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Request timed out.
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=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 = 2ms, Average = 2ms
C:\>ssh -l admin 10.2.2.2
Password:
R2>
Top



☞ **Enable the Security Technology package on R**

```
R3>show version
Technology Package License Information for Module:'c1900'
-----------------------------------------------------------------
Technology Technology-package Technology-package
Current Type Next reboot
-----------------------------------------------------------------
ipbase ipbasek9 Permanent ipbasek9
security None NoneNone
data None NoneNone
Configuration register is 0x2102
```

```
R3>en
R3#conf t
R3(config)# license boot module c1900 technology-package securityk9
ACCEPT? [yes/no]: Yes
R3(config)#exit
R3#reload
System configuration has been modified. Save? [yes/no]:yes
```

```
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
```

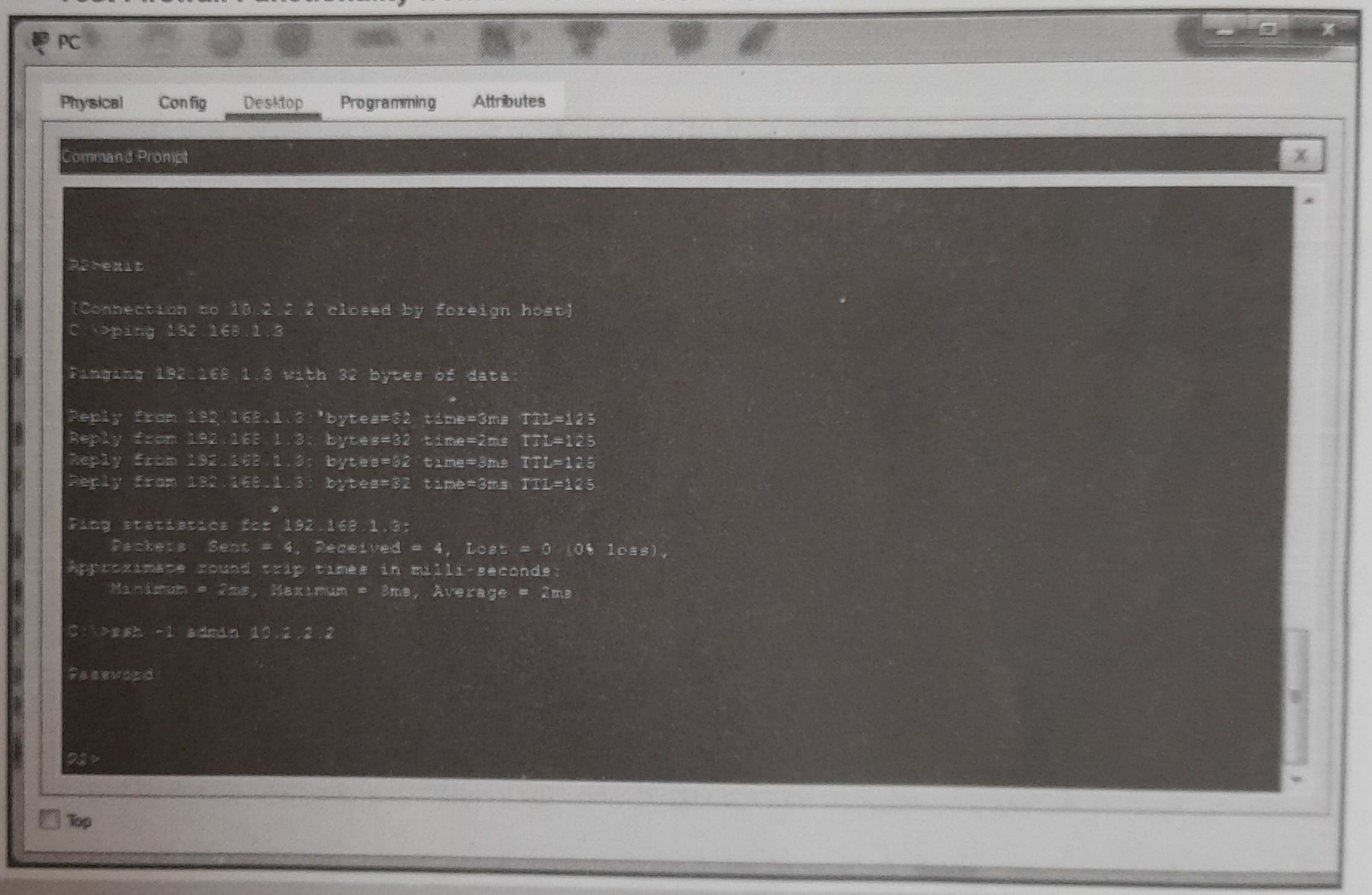
☞ **Create the Firewall Zones, Class Maps and ACLs on R3:-**

(Permit all IP protocols from the 192.168.3.0/24 source network to any destination.)

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

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

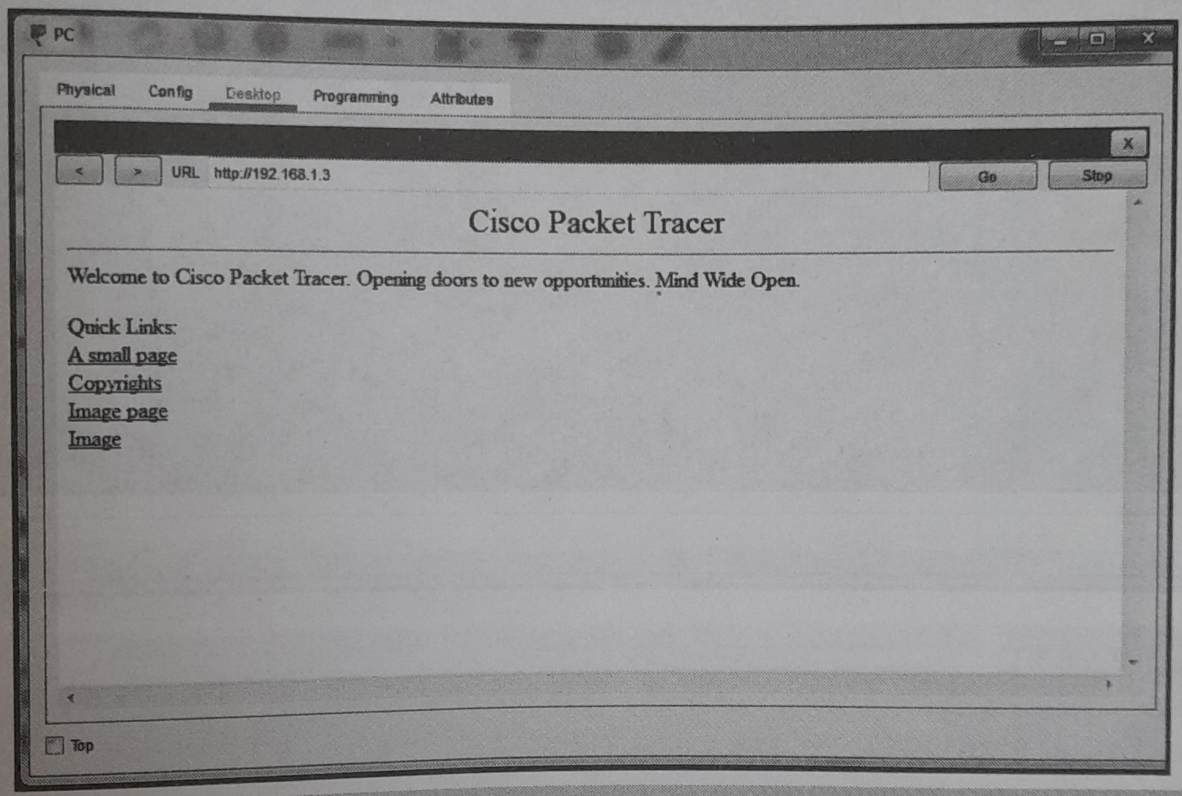



```
R3>en
R3#show policy-map type inspect zone-pair sessions
policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR
Service-policy inspect : IN-2-OUT-PMAP
Class-map: IN-NET-CLASS-MAP (match-all)
```

- **Match :** access-group 101
- Inspect
- Number of Established Sessions = 1
- Established Sessions

```
Session 235150144 (192.168.3.3:1029)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
Created 00:00:13, Last heard 00:00:10
Bytes sent (initiator:responder) [578:656]
```

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

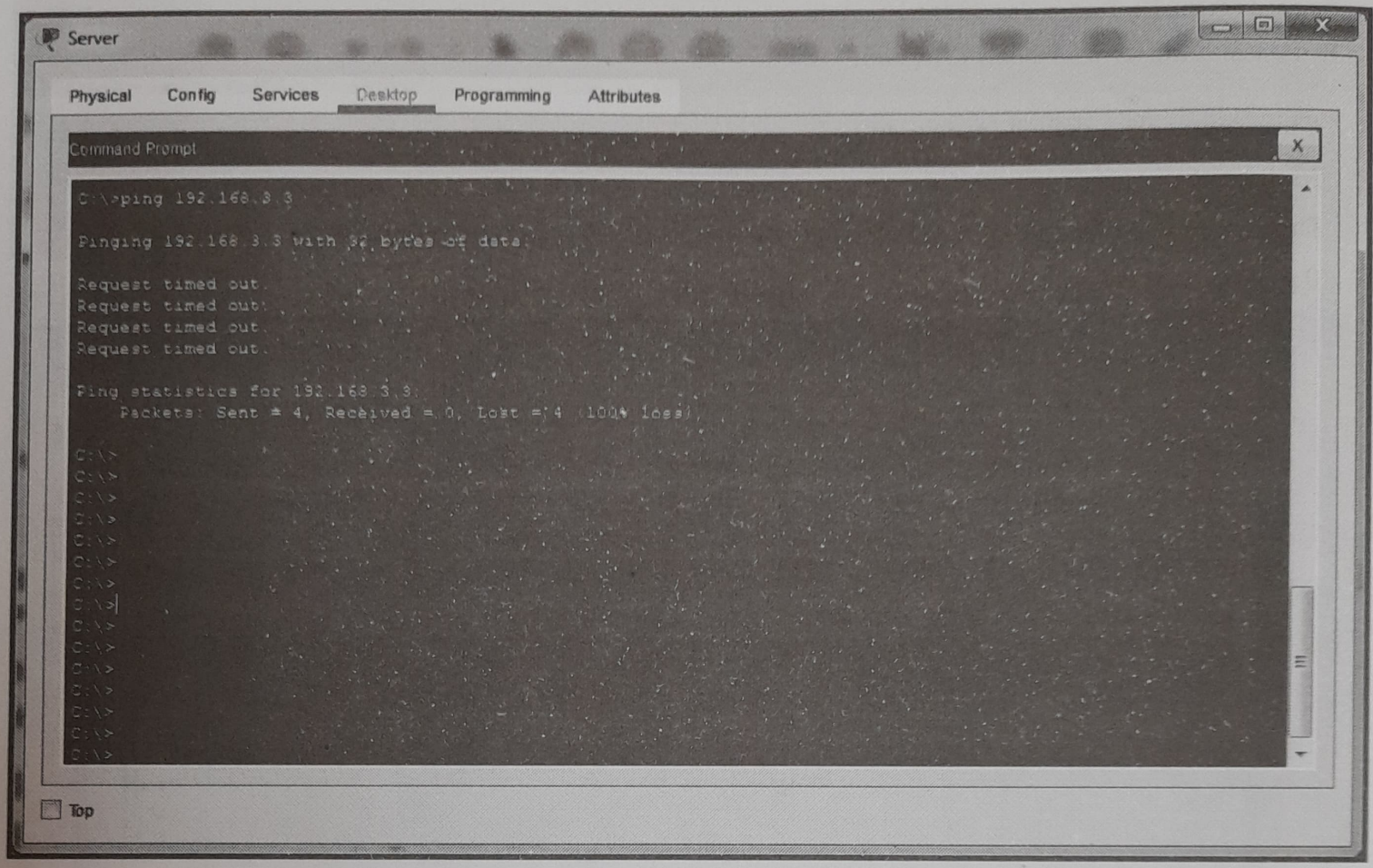



```
R3#show policy-map type inspect zone-pair sessions
policy exists on zp IN-2-OUT-ZPAIR
Zone-pair: IN-2-OUT-ZPAIR

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
```

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



R2>ping 192.168.3.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)