

**Practical 6****Configuring a Zone-Based Policy Firewall (ZPF)**

Cisco IOS® Software Release 12.4(6)T introduced Zone-Based Policy Firewall (ZFW), a new configuration model for the Cisco IOS Firewall feature set. This new configuration model offers intuitive policies for multiple-interface routers, increased granularity of firewall policy application, and a default deny-all policy that prohibits traffic between firewall security zones until an explicit policy is applied to allow desirable traffic.

Nearly all classic Cisco IOS Firewall features implemented before Cisco IOS Software Release 12.4(6)T are supported in the new zone-based policy inspection interface:

- 1) Stateful packet inspection
- 2) VRF-aware Cisco IOS Firewall
- 3) URL filtering
- 4) Denial-of-Service (DoS) mitigation

Cisco IOS Software Release 12.4(9)T added ZFW support for per-class session/connection and throughput limits, as well as application inspection and control:

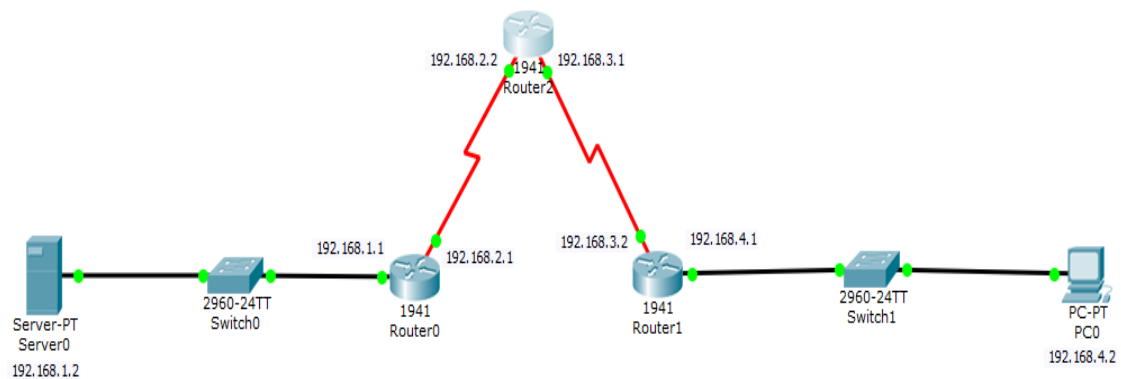
- 1) HTTP
- 2) Post Office Protocol (POP3),
- 3) Internet Mail Access Protocol (IMAP),
- 4) Simple Mail Transfer Protocol/Enhanced Simple Mail Transfer Protocol (SMTP/ESMTP)
- 5) Sun Remote Procedure Call (RPC)
- 6) Instant Messaging (IM) applications:
  - i) Microsoft Messenger
  - ii) Yahoo! Messenger
  - iii) AOL Instant Messenger
- 7) Peer-to-Peer (P2P) File Sharing:
  - i) Bittorrent
  - ii) KaZaA
  - iii) Gnutella
  - iv) eDonkey

Cisco IOS Software Release 12.4(11)T added statistics for easier DoS protection tuning. Some Cisco IOS Classic Firewall features and capabilities are not yet supported in a ZFW in Cisco IOS Software Release 12.4(15)T:

- i) Authentication proxy
- ii) Stateful firewall failover
- iii) Unified firewall MIB
- iv) IPv6 stateful inspection
- v) TCP out-of-order support

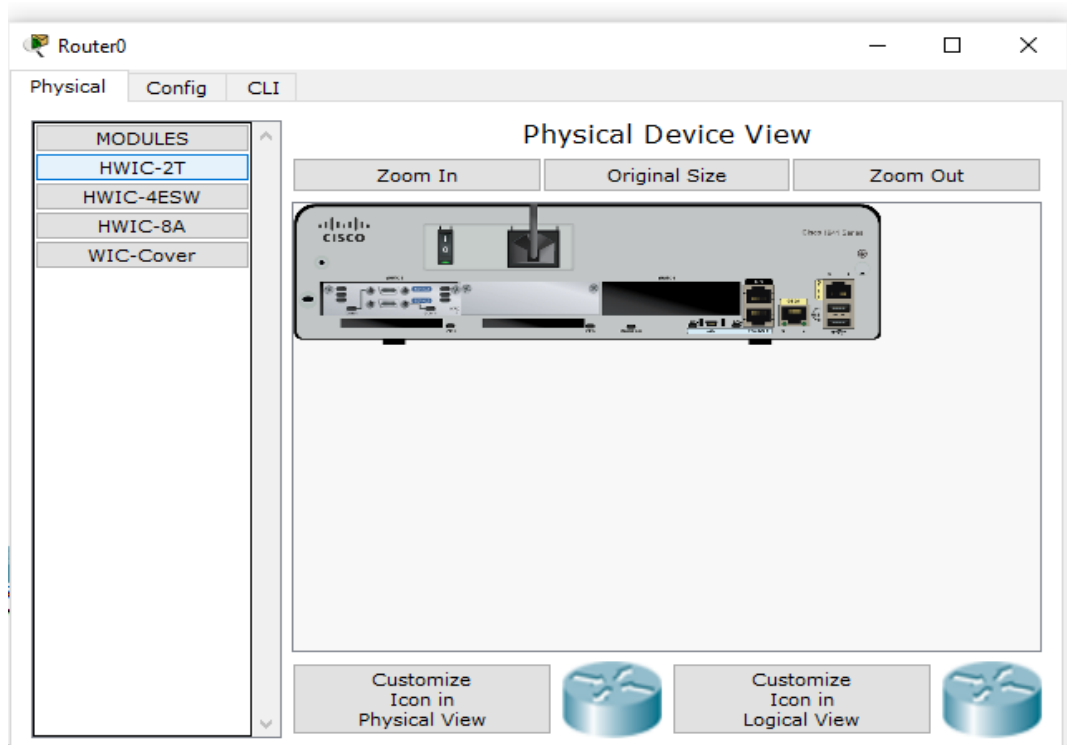
ZFW generally improves Cisco IOS performance for most firewall inspection activities. Neither Cisco IOS ZFW or Classic Firewall include stateful inspection support for multicast traffic.

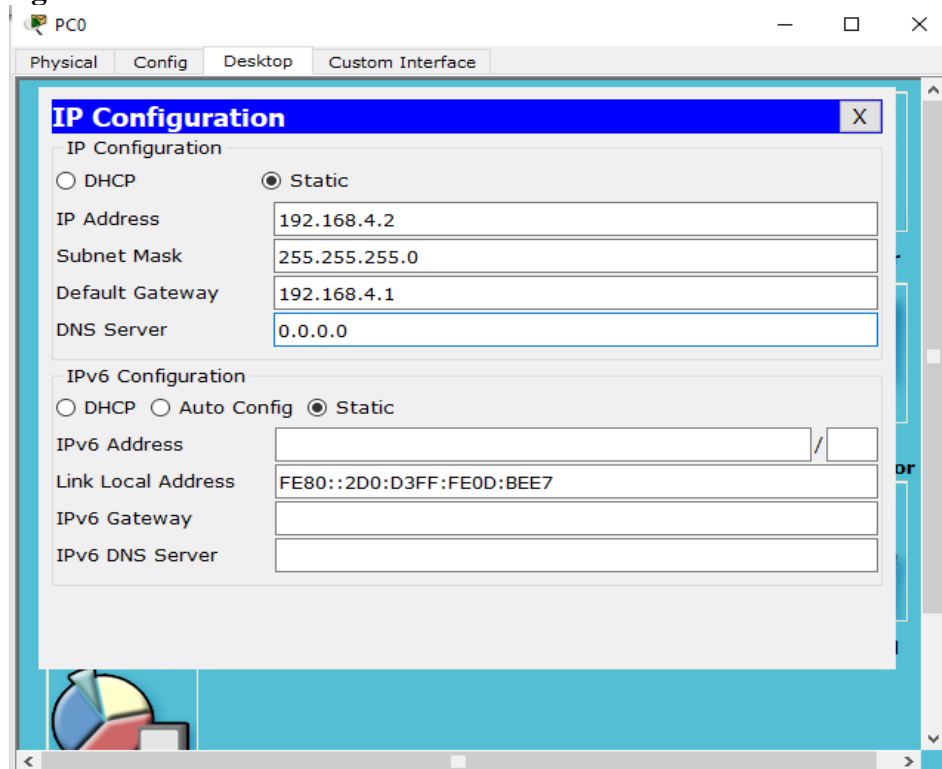
Consider the following topology



## Topology Configuration

Serial Interface must be added in each Router before configuring it  
The serial interface in each Router is added as follows



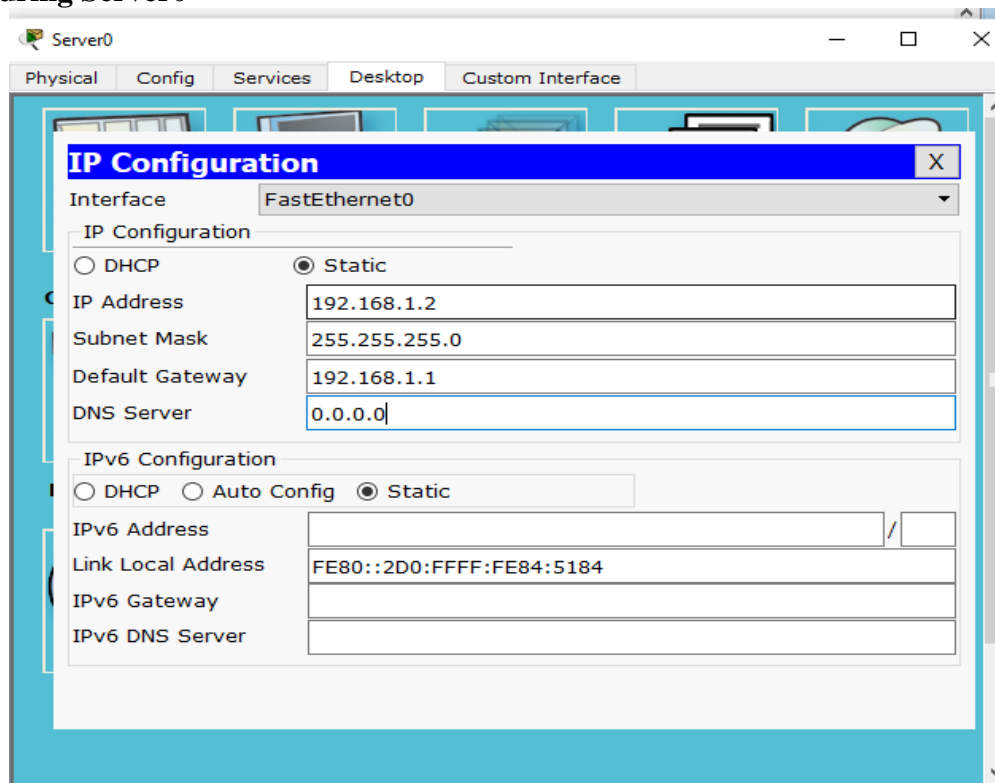
**Configuring PC0**

The screenshot shows the configuration window for PC0. The 'Config' tab is selected. The 'IP Configuration' section is expanded, showing the following settings:

IP Configuration	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IP Address	192.168.4.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.4.1
DNS Server	0.0.0.0

The 'IPv6 Configuration' section is also expanded, showing the following settings:

IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::2D0:D3FF:FE0D:BEE7
IPv6 Gateway	
IPv6 DNS Server	

**Configuring Server0**

The screenshot shows the configuration window for Server0. The 'Config' tab is selected. The 'IP Configuration' section is expanded, showing the following settings:

IP Configuration	
Interface: FastEthernet0	
<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
IP Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

The 'IPv6 Configuration' section is also expanded, showing the following settings:

IPv6 Configuration	
<input type="radio"/> DHCP <input type="radio"/> Auto Config <input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address	FE80::2D0:FFFF:FE84:5184
IPv6 Gateway	
IPv6 DNS Server	

## Configuring Router0

Router0

Physical Config CLI

**GLOBAL**

Settings

Algorithm Settings

**ROUTING**

Static

RIP

**SWITCHING**

VLAN Database

**INTERFACE**

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

**GigabitEthernet0/0**

Port Status ☒ On

Bandwidth ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☒ Half Duplex ☐ Full Duplex ☒ Auto

MAC Address 0001.9604.1701

IP Configuration

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Router0

Physical Config CLI

**GLOBAL**

Settings

Algorithm Settings

**ROUTING**

Static

RIP

**SWITCHING**

VLAN Database

**INTERFACE**

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/1/0

Serial0/1/1

**Serial0/1/0**

Port Status ☒ On

Duplex ☒ Full Duplex

Clock Rate 2000000

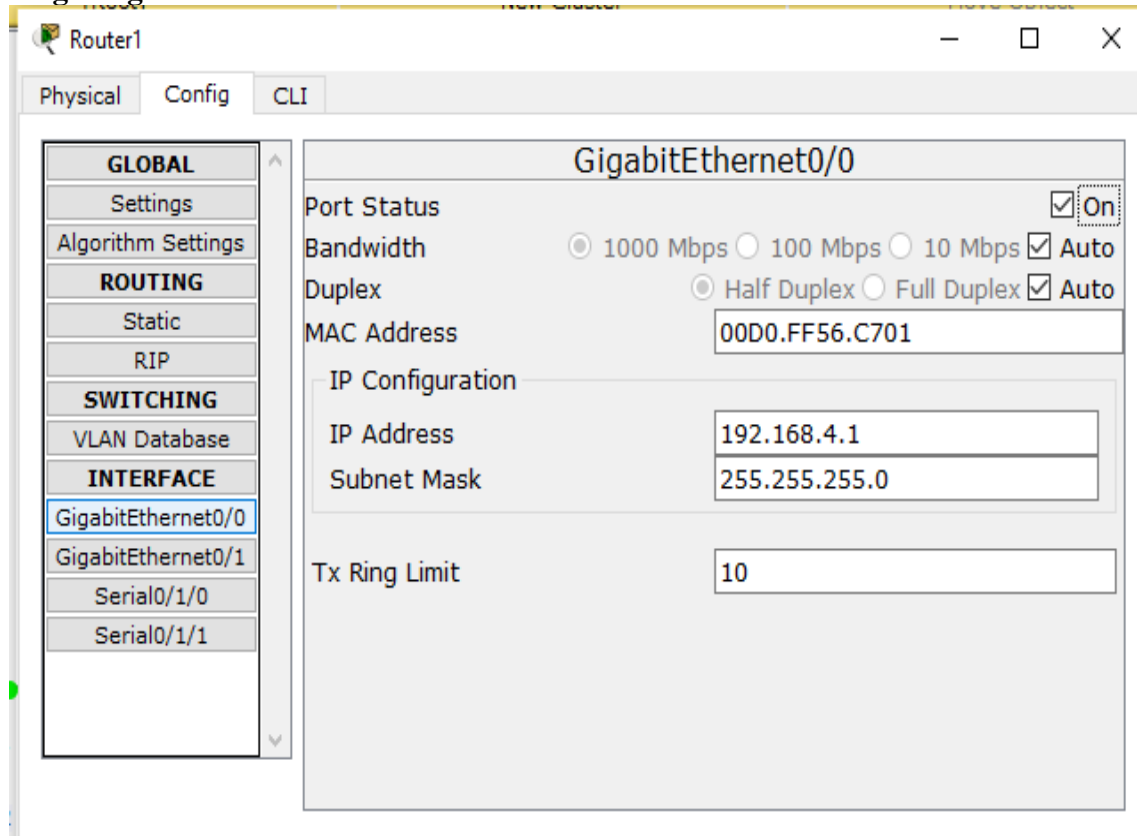
IP Configuration

IP Address 192.168.2.1

Subnet Mask 255.255.255.0

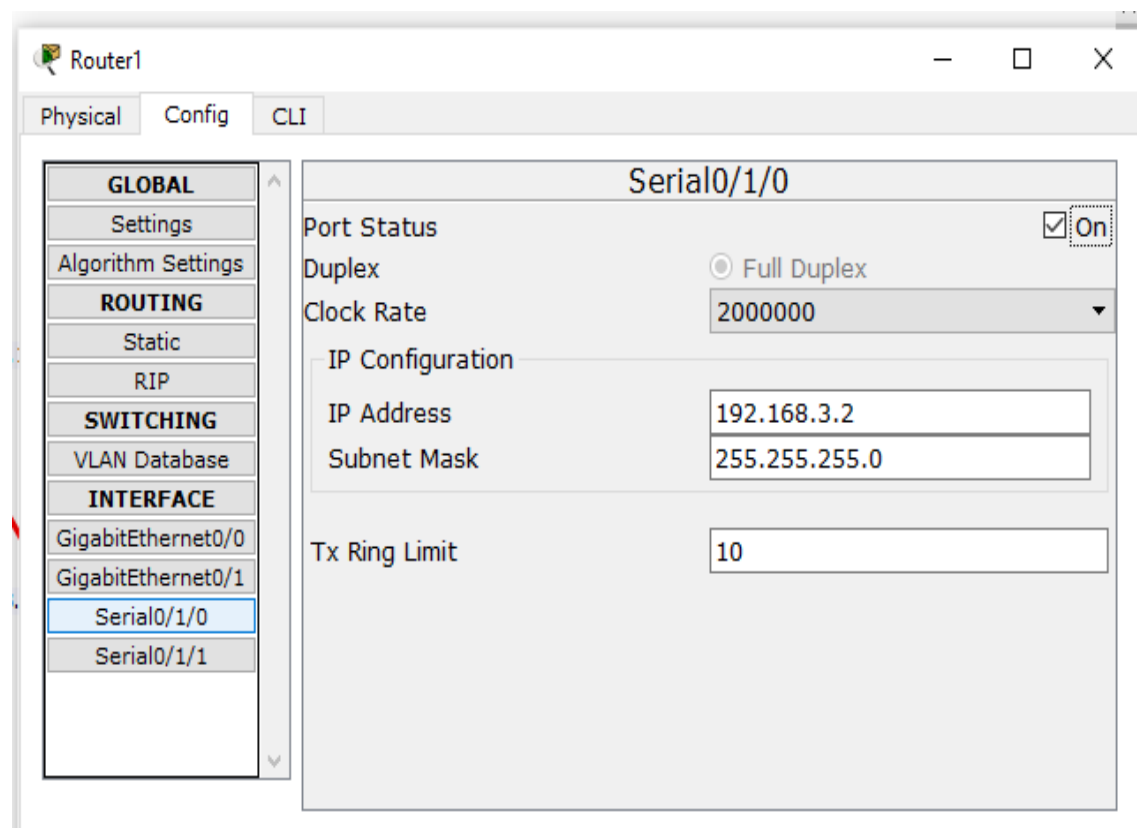
Tx Ring Limit 10

## Configuring Router1



The screenshot shows the configuration window for Router1, specifically the GigabitEthernet0/0 interface. The left sidebar contains a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING (Static, RIP), SWITCHING (VLAN Database), and INTERFACE (GigabitEthernet0/0, GigabitEthernet0/1, Serial0/1/0, Serial0/1/1). The main area displays the configuration for GigabitEthernet0/0. The Port Status is checked and set to On. Bandwidth is set to 1000 Mbps, and Duplex is set to Half Duplex. The MAC Address is 00D0.FF56.C701. The IP Configuration section shows the IP Address as 192.168.4.1 and the Subnet Mask as 255.255.255.0. The Tx Ring Limit is set to 10.

GigabitEthernet0/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input checked="" type="radio"/> Half Duplex <input type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	00D0.FF56.C701
IP Configuration	
IP Address	192.168.4.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10



The screenshot shows the configuration window for Router1, specifically the Serial0/1/0 interface. The left sidebar is the same as the previous screenshot. The main area displays the configuration for Serial0/1/0. The Port Status is checked and set to On. Duplex is set to Full Duplex. The Clock Rate is set to 2000000. The IP Configuration section shows the IP Address as 192.168.3.2 and the Subnet Mask as 255.255.255.0. The Tx Ring Limit is set to 10.

Serial0/1/0	
Port Status	<input checked="" type="checkbox"/> On
Duplex	<input checked="" type="radio"/> Full Duplex
Clock Rate	2000000
IP Configuration	
IP Address	192.168.3.2
Subnet Mask	255.255.255.0
Tx Ring Limit	10

## Configuring Router2

The screenshot shows the configuration window for Router2, specifically for the Serial0/1/0 interface. The window has tabs for Physical, Config, and CLI. The left sidebar shows a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING (Static, RIP), SWITCHING (VLAN Database), and INTERFACE (GigabitEthernet0/0, GigabitEthernet0/1, Serial0/1/0, Serial0/1/1). The Serial0/1/0 interface is selected. The main area shows the following configuration:

Serial0/1/0	
Port Status	<input checked="" type="checkbox"/> On
Duplex	<input type="radio"/> Full Duplex
Clock Rate	2000000
IP Configuration	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Tx Ring Limit	10

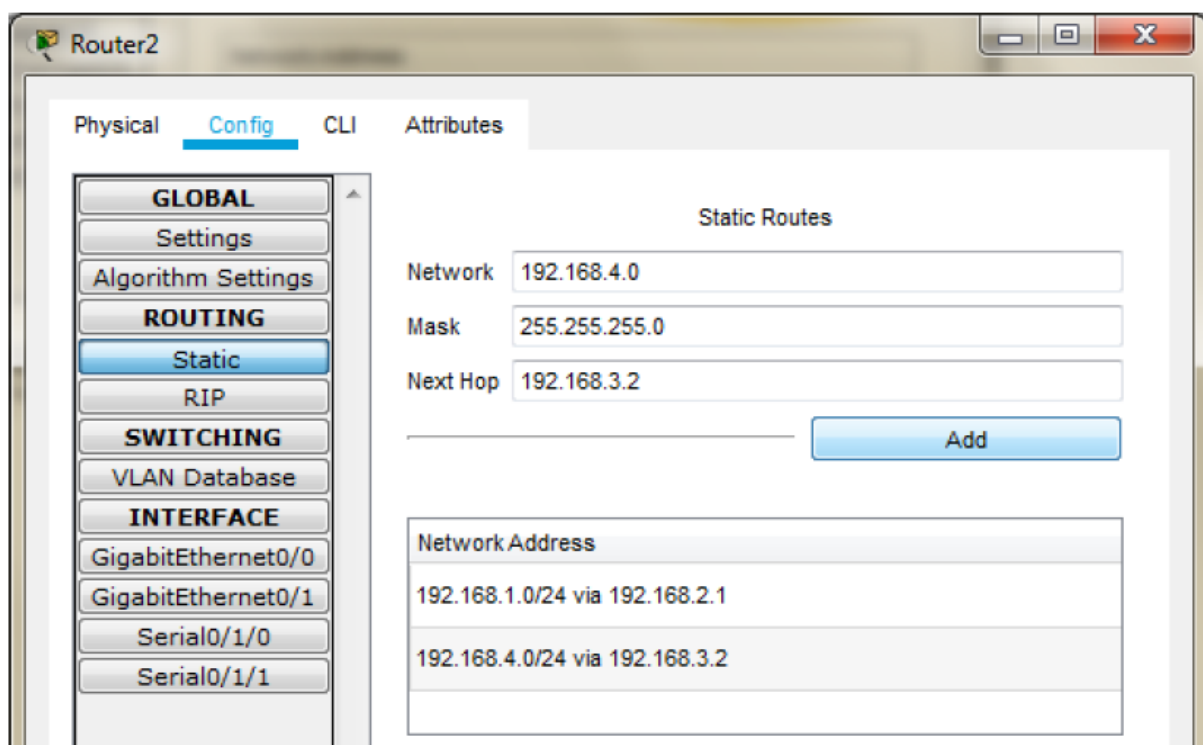
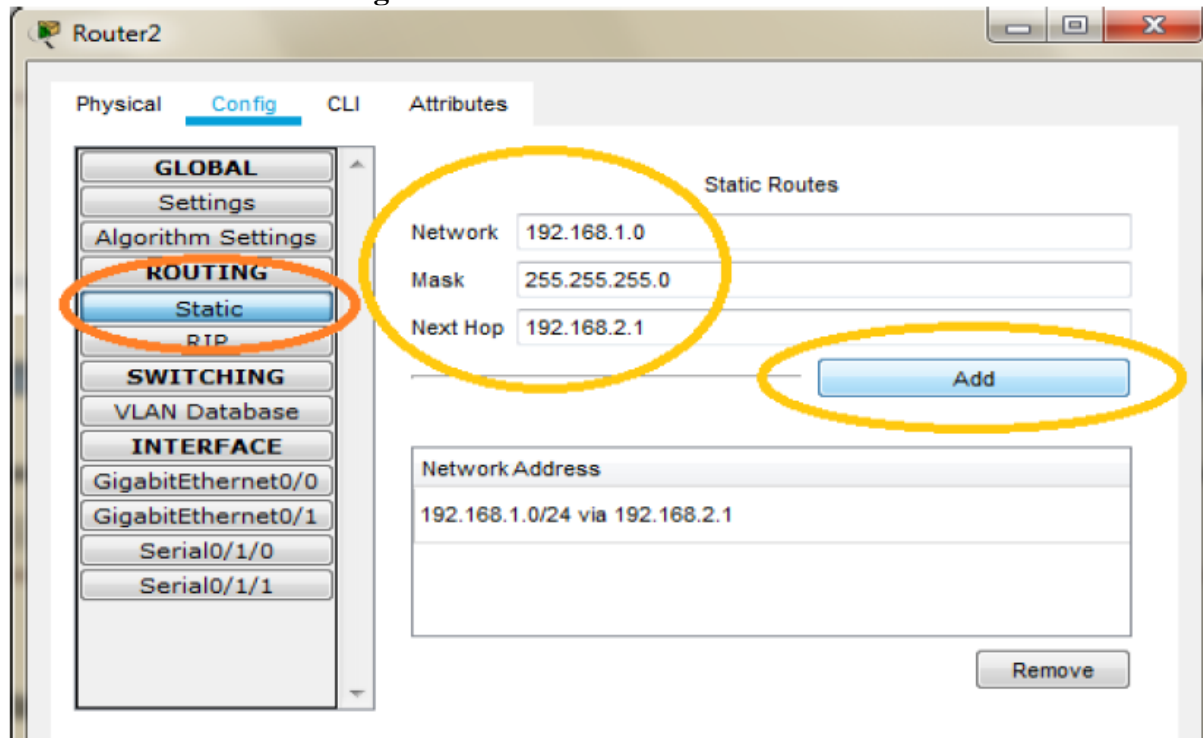
The screenshot shows the configuration window for Router2, specifically for the Serial0/1/1 interface. The window has tabs for Physical, Config, and CLI. The left sidebar shows a tree view with categories: GLOBAL, Settings, Algorithm Settings, ROUTING (Static, RIP), SWITCHING (VLAN Database), and INTERFACE (GigabitEthernet0/0, GigabitEthernet0/1, Serial0/1/0, Serial0/1/1). The Serial0/1/1 interface is selected. The main area shows the following configuration:

Serial0/1/1	
Port Status	<input checked="" type="checkbox"/> On
Duplex	<input type="radio"/> Full Duplex
Clock Rate	2000000
IP Configuration	
IP Address	192.168.3.1
Subnet Mask	255.255.255.0
Tx Ring Limit	10

**Part 1: Static Routing**

Static Routing is done using the following procedure for each Router

**Router 2: Add the following Routes in the Static mode**



**Router 0: Add the following Routes in the Static mode**

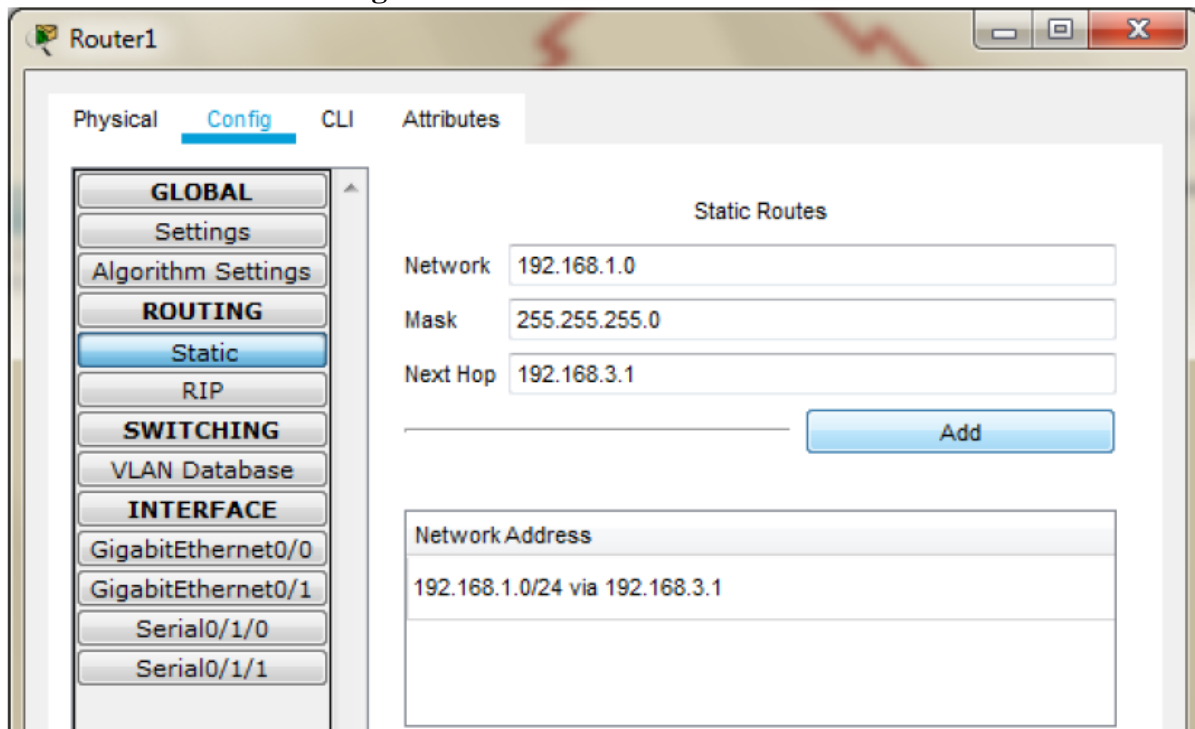
The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under ROUTING, 'Static' is selected. The main area is titled 'Static Routes' and contains input fields for 'Network' (192.168.3.0), 'Mask' (255.255.255.0), and 'Next Hop' (192.168.2.2). An 'Add' button is visible. Below these fields, a table titled 'Network Address' shows the added route: 192.168.3.0/24 via 192.168.2.2.

Network Address
192.168.3.0/24 via 192.168.2.2

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The left sidebar has a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under ROUTING, 'Static' is selected. The main area is titled 'Static Routes' and contains input fields for 'Network' (192.168.4.0), 'Mask' (255.255.255.0), and 'Next Hop' (192.168.2.2). An 'Add' button is visible. Below these fields, a table titled 'Network Address' shows two added routes: 192.168.3.0/24 via 192.168.2.2 and 192.168.4.0/24 via 192.168.2.2.

Network Address
192.168.3.0/24 via 192.168.2.2
192.168.4.0/24 via 192.168.2.2



**Router 1: Add the following Routes in the Static mode**

The screenshot shows the Router1 configuration window with the 'Config' tab selected. The left sidebar contains a tree view with the following categories and items:

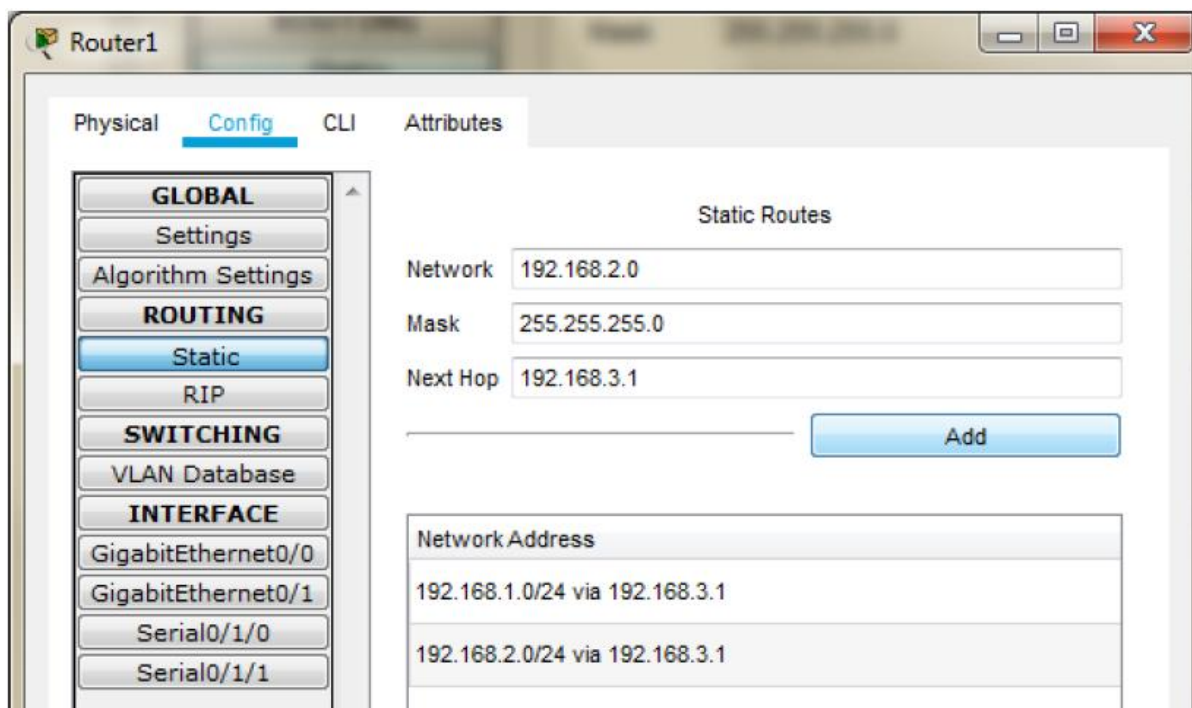
- GLOBAL**
  - Settings
  - Algorithm Settings
- ROUTING**
  - Static** (selected)
  - RIP
- SWITCHING**
  - VLAN Database
- INTERFACE**
  - GigabitEthernet0/0
  - GigabitEthernet0/1
  - Serial0/1/0
  - Serial0/1/1

The main area is titled 'Static Routes' and contains the following fields:

- Network: 192.168.1.0
- Mask: 255.255.255.0
- Next Hop: 192.168.3.1

Below these fields is an 'Add' button. At the bottom, there is a table for 'Network Address' with one entry:

Network Address
192.168.1.0/24 via 192.168.3.1



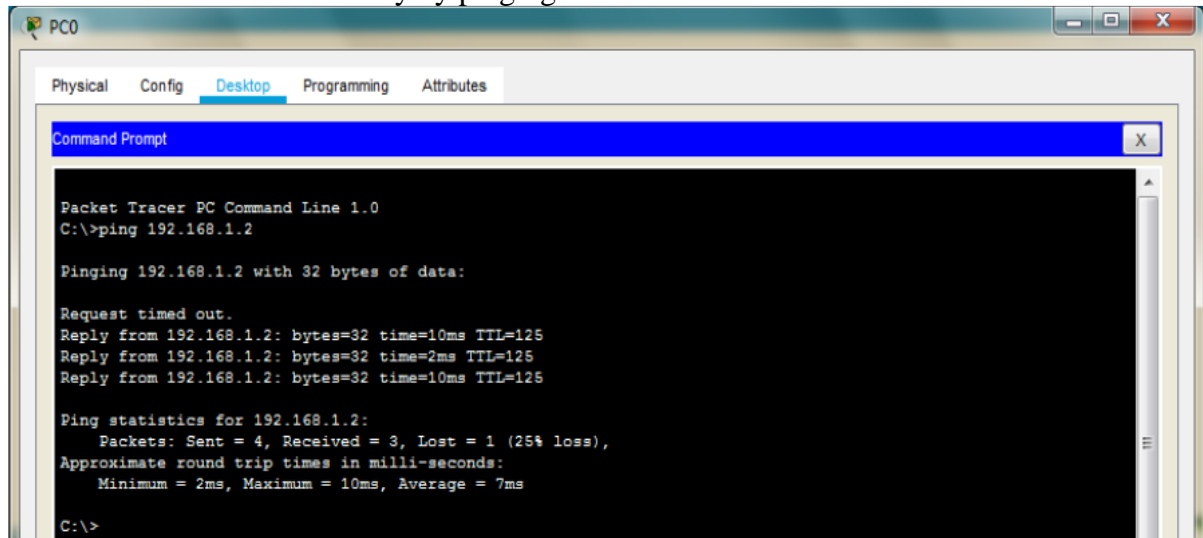
The screenshot shows the Router1 configuration window with the 'Config' tab selected. The left sidebar is identical to the previous screenshot. The main area is titled 'Static Routes' and contains the following fields:

- Network: 192.168.2.0
- Mask: 255.255.255.0
- Next Hop: 192.168.3.1

Below these fields is an 'Add' button. At the bottom, there is a table for 'Network Address' with two entries:

Network Address
192.168.1.0/24 via 192.168.3.1
192.168.2.0/24 via 192.168.3.1

Now we check the connectivity by pinging the Server from the PC



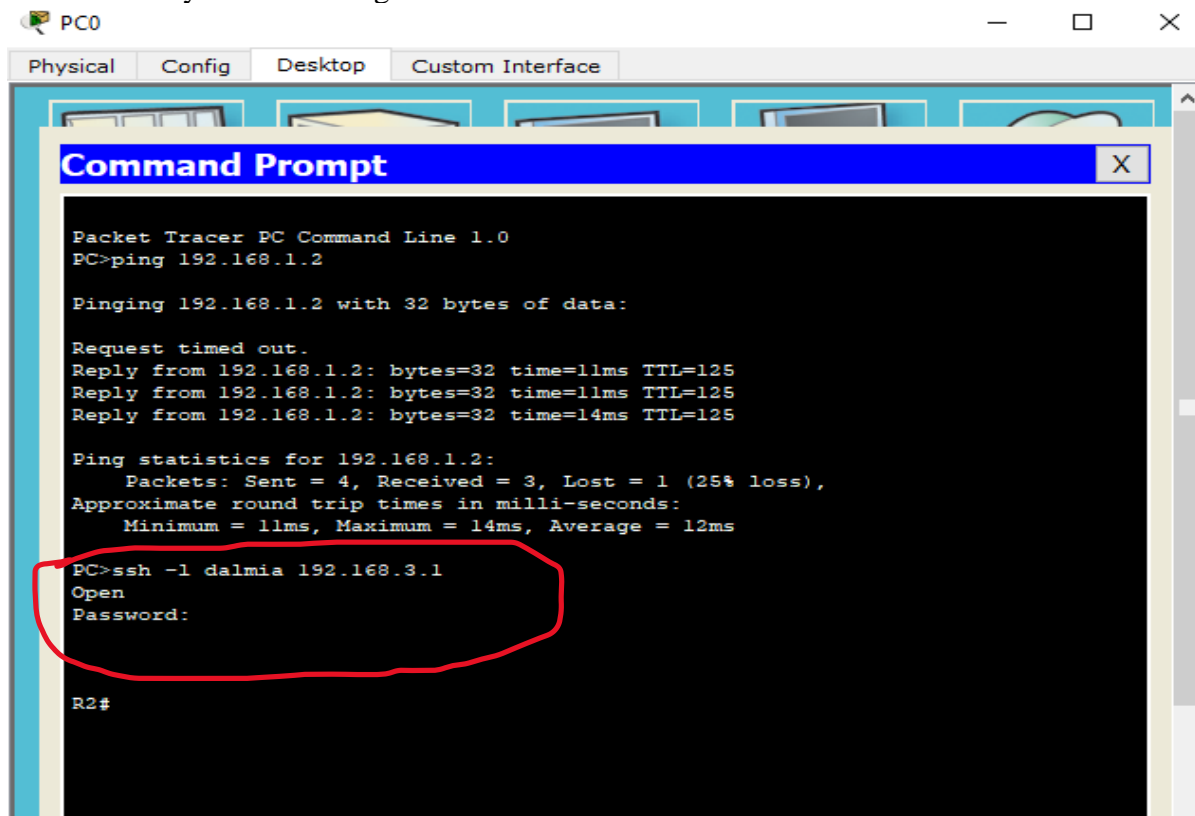
## Part 2: Configuring SSH on Router 2

Type the following commands in the CLI mode of Router2

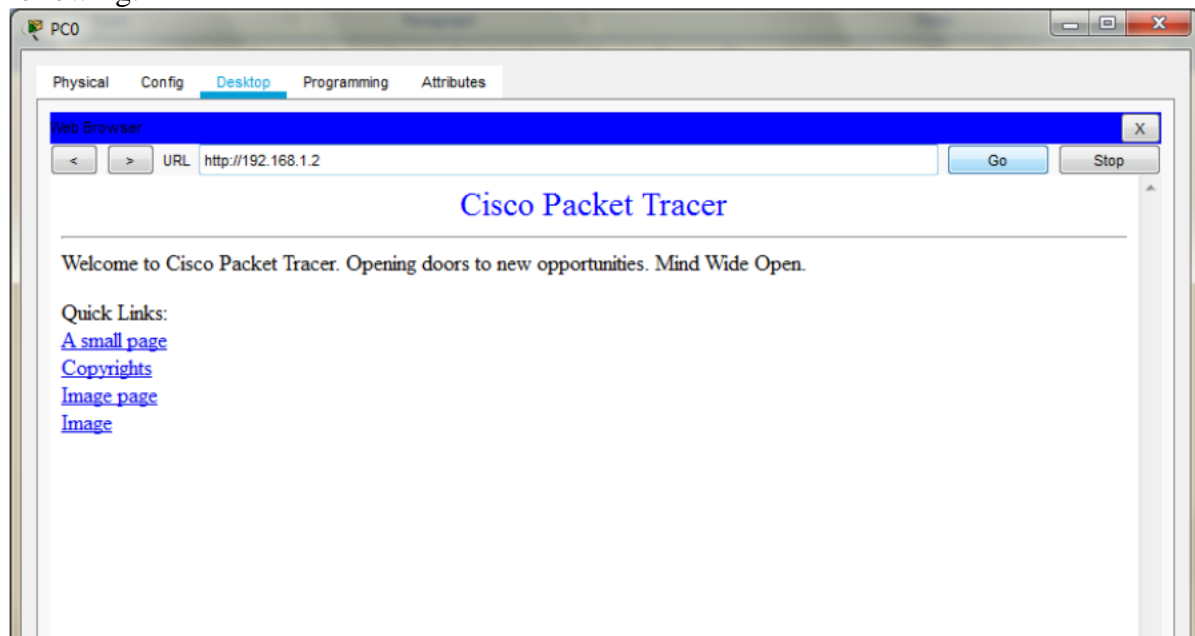
```
Router>en
Router#conf t
Router(config)#ip domain-name dalmia.com
Router(config)#hostname R2
R2(config)#crypto key generate rsa
The name for the keys will be: R2.dalmia.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater 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)#line vty 0 4
*Mar 2 0:52:50.777: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#exit
R2(config)#username dalmia privilege 15 password cisco
```

Now we verify the SSH using PC as follows



Next, we access the web services of the Server using the web browser of PC using the following: -



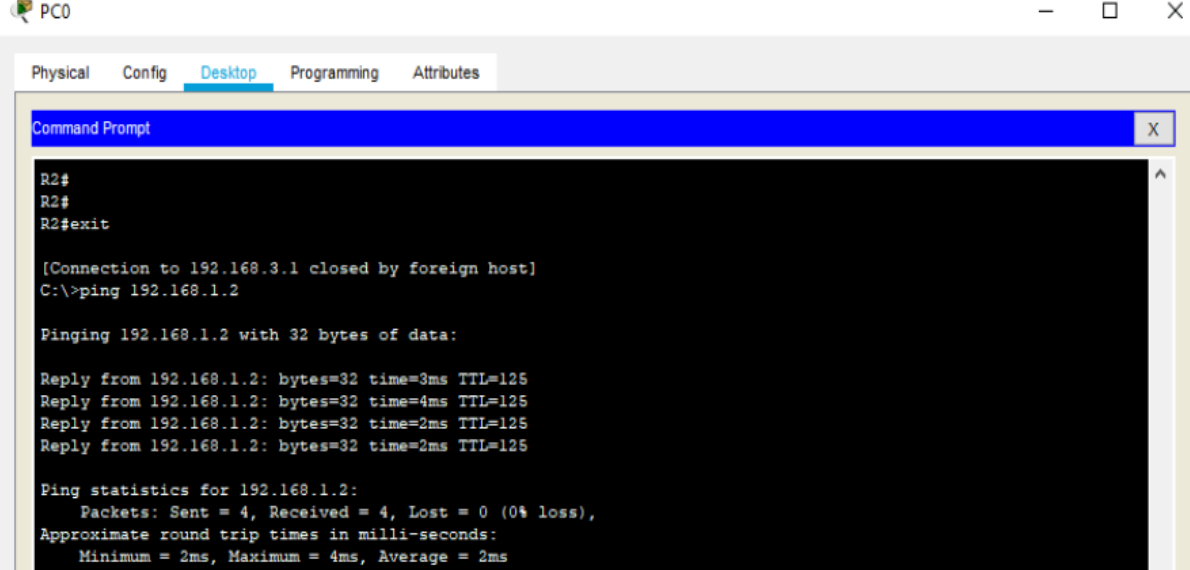
**Part 3: Create the Firewall Zones on Router1**

Type the following commands in the CLI mode of Router1

```
Router>en
Router#conf t
Router(config)#license boot module c1900 technology-package securityk9
ACCEPT? [yes/no]: y
Router(config)#exit
Router#copy run start
Press enter when prompted
Router#reload
Continue with configuration dialog? [yes/no]: n
Router>en
Router#conf t
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 192.168.4.0 0.0.0.255 any
Router(config)#class-map type inspect match-all in-map
Router(config-cmap)#match access-group 101
Router(config-cmap)#exit
Router(config)#policy-map type inspect in-out
Router(config-pmap)#class type inspect in-map
Router(config-pmap-c)#inspect
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#
Router(config)#zone-pair security in-out-zone source in-zone destination out-zone
Router(config-sec-zone-pair)#service-policy type inspect in-out
Router(config-sec-zone-pair)#exit
Router(config)#
Router(config)#int G0/0
Router(config-if)#zone-member security in-zone
Router(config-if)#exit
Router(config)#
Router(config)#int Se0/1/1
Router(config-if)#zone-member security out-zone
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

## Part 4: Testing the Firewall Functionality (from in-zone to out-zone) by the following steps

### Step 1: Pinging SERVER from the PC (it will succeed)



The screenshot shows the Packet Tracer interface for PC0. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt shows the following output:

```
R2#
R2#
R2#exit

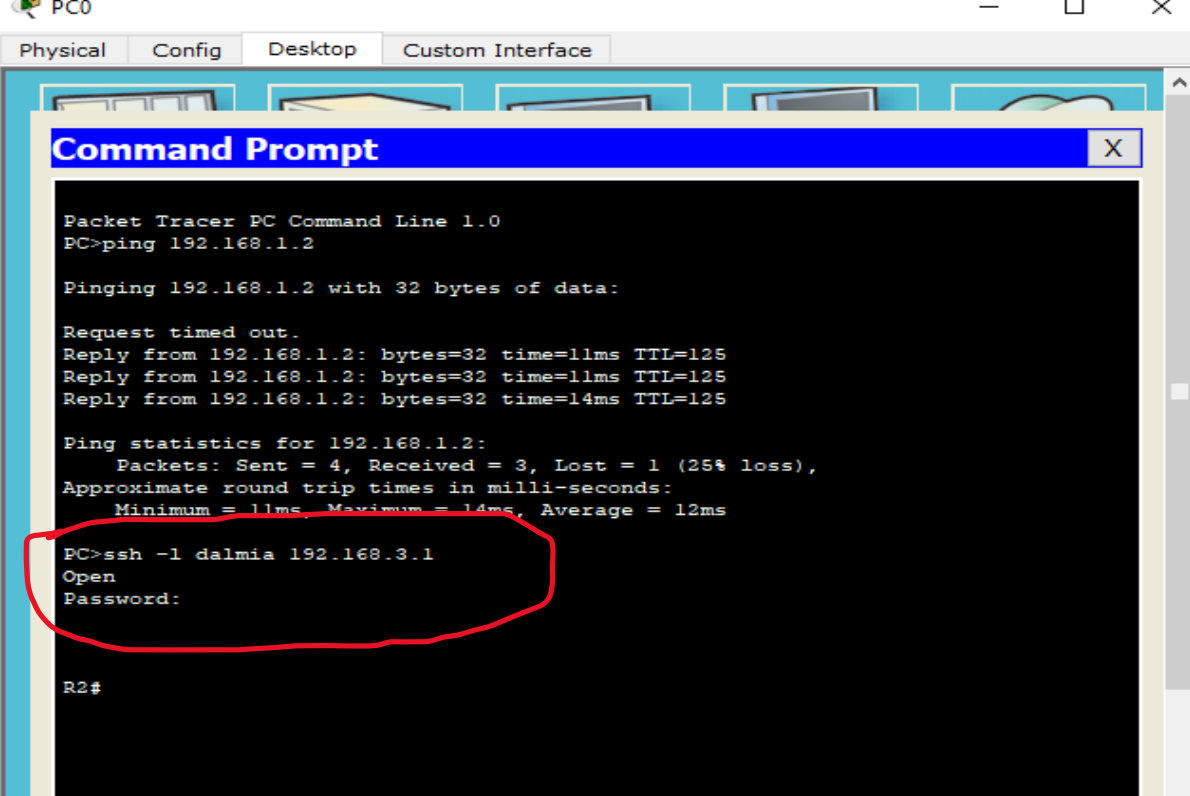
[Connection to 192.168.3.1 closed by foreign host]
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=4ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms 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 = 4ms, Average = 2ms
```

### Step 2: Start an SSH session from PC to Router 2 (ip 192.168.1.2)



The screenshot shows the Packet Tracer interface for PC0. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=11ms TTL=125
Reply from 192.168.1.2: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 14ms, Average = 12ms

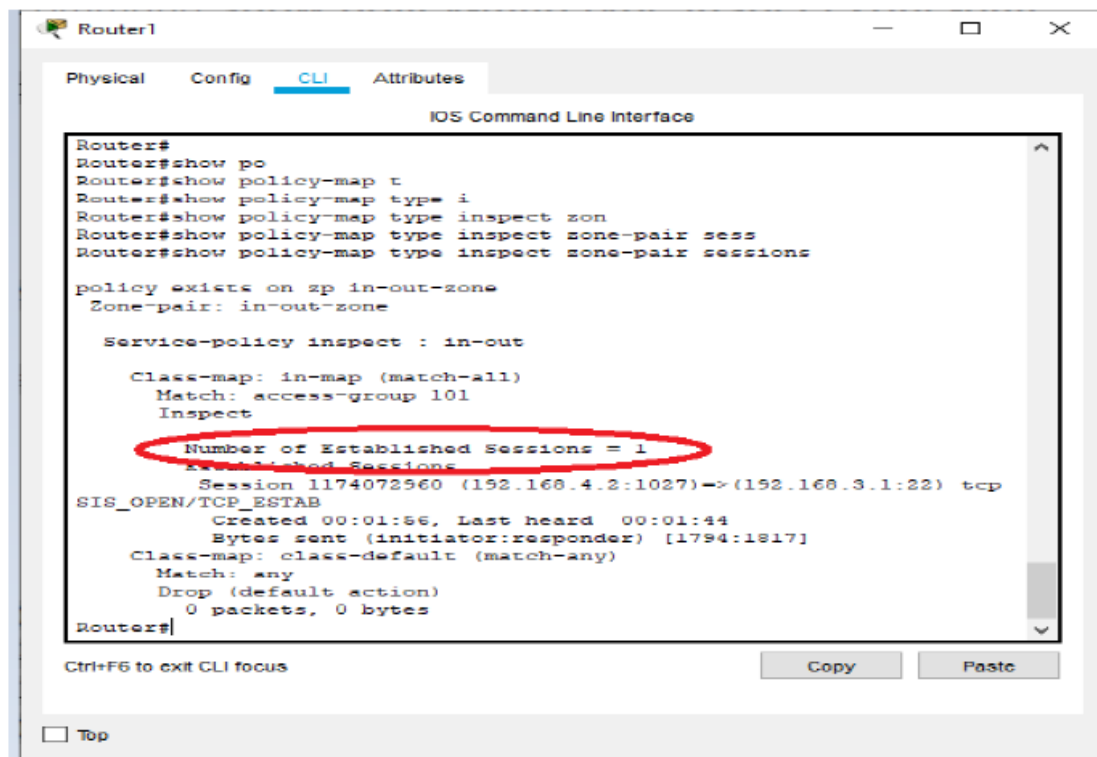
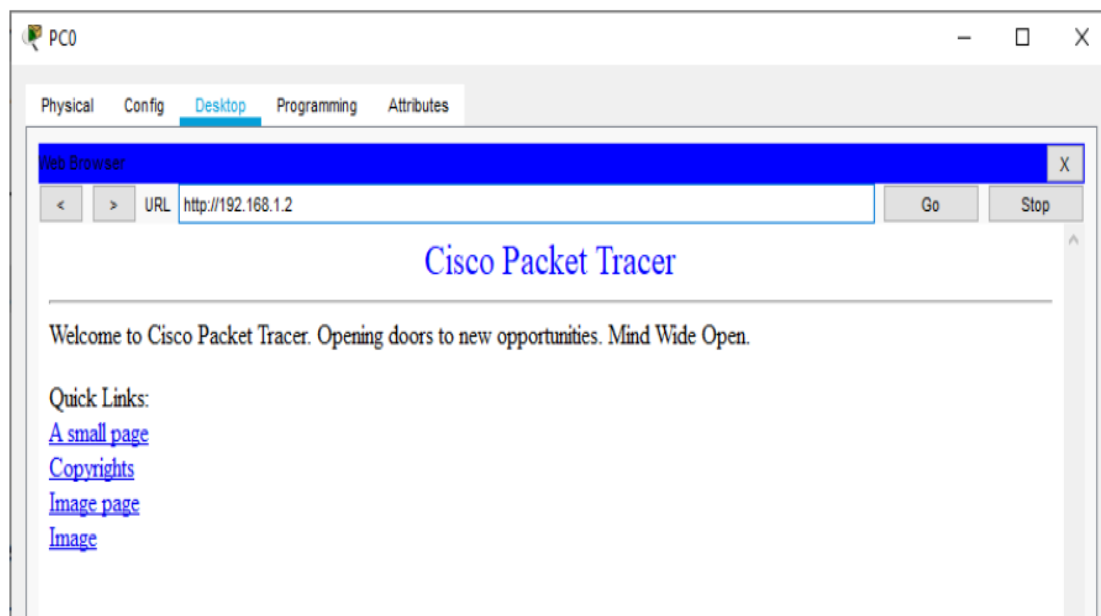
PC>ssh -l dalmia 192.168.3.1
Open
Password:

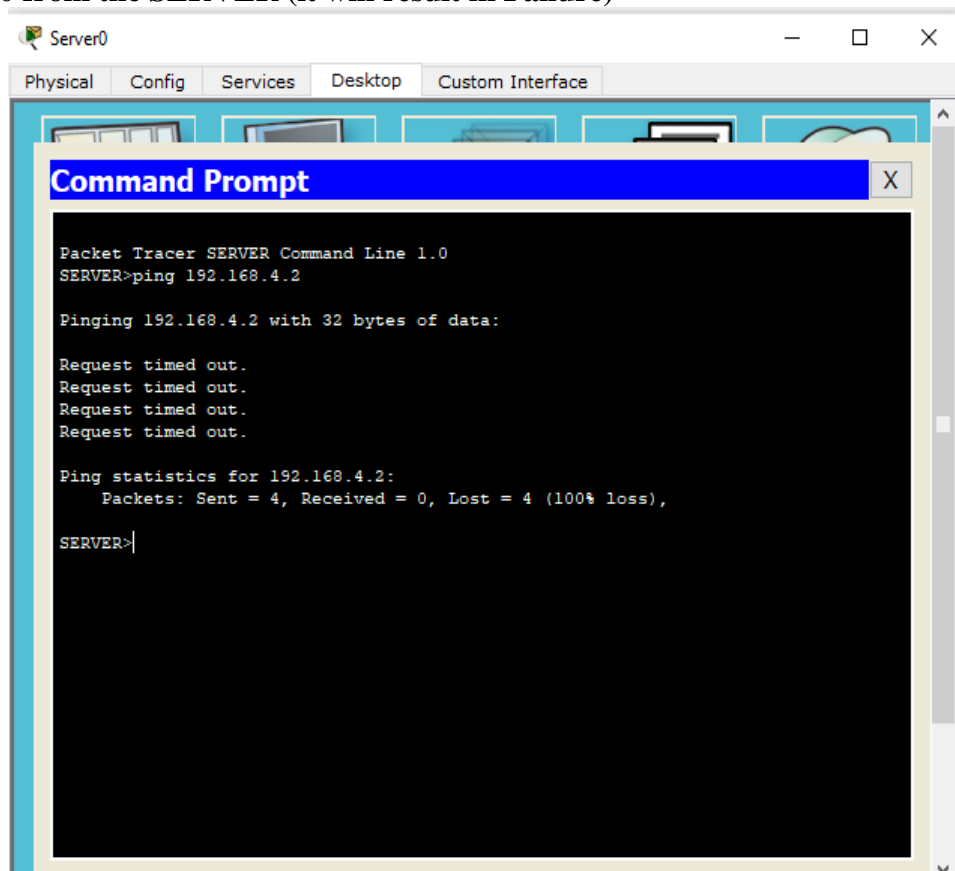
R2#
```

As seen above the session becomes active and we get access to Router2 (Do not exit the session and continue to Step 3)

**Step 3: Type the following command in the CLI mode of Router1**

Router#show policy-map type inspect zone-pair sessions

**Step 4: We close the SSH connection and open the web browser and access the server address (192.168.1.2) and get the following**

**Part 5: Testing the Firewall Functionality (from out-zone to in-zone) by the following step: -****Ping PC0 from the SERVER (it will result in Failure)**

Hence the Firewall functionality has been verified.

\*\*\*\*\*