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.

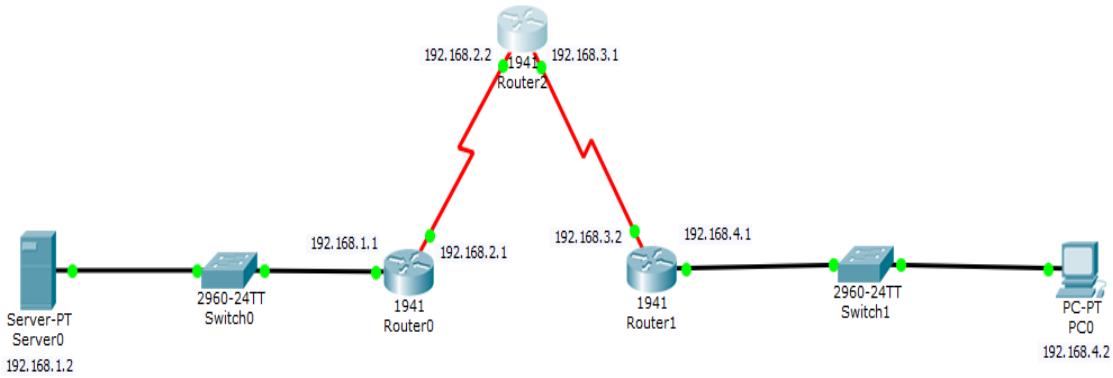
Nearly all classic Cisco IOS Firewall features implemented before Cisco IOS Software Release 12.4(6)T are supported in the new zone-based policy inspection interface:
1) Stateful packet inspection
2) VRF-aware Cisco IOS Firewall
3) URL filtering
4) Denial-of-Service (DoS) mitigation

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

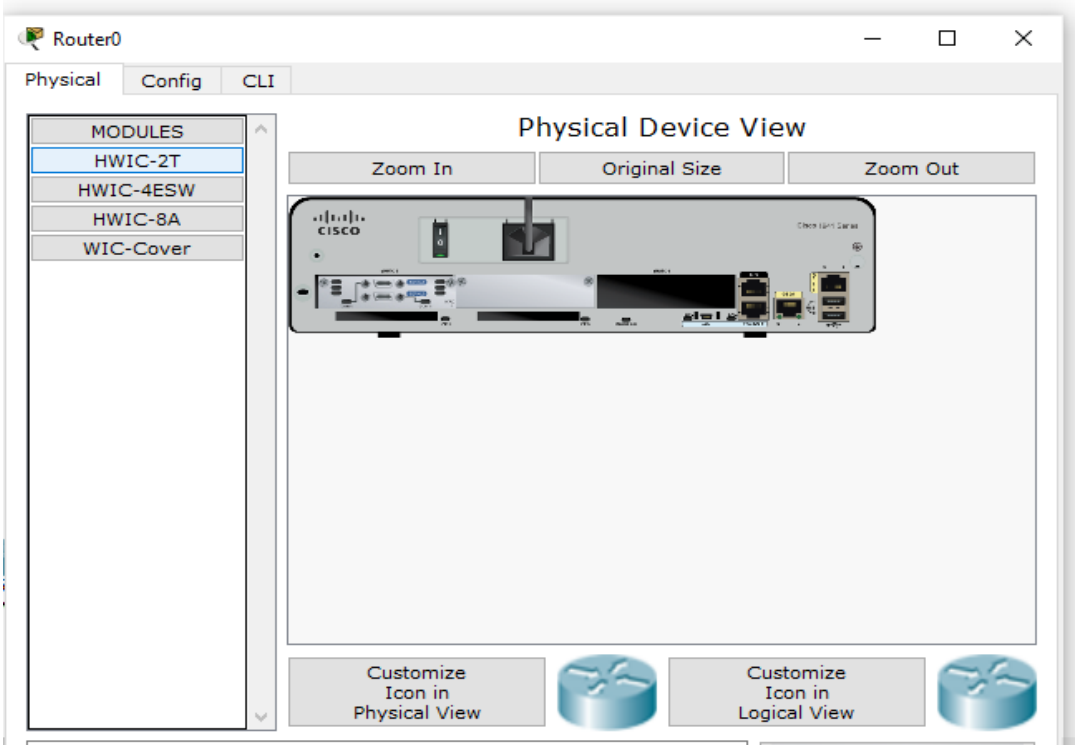
ZFW generally improves Cisco IOS performance for most firewall inspection activities. Neither Cisco IOS ZFW or Classic Firewall include stateful inspection support for multicast traffic.

Consider the following topology

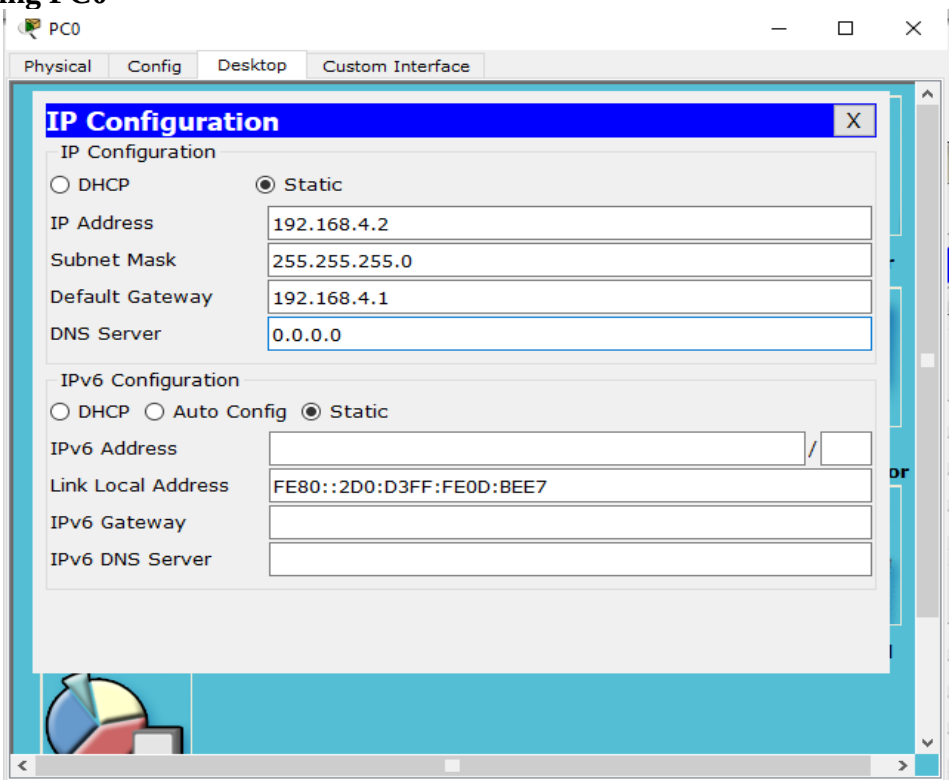


Topology Configuration

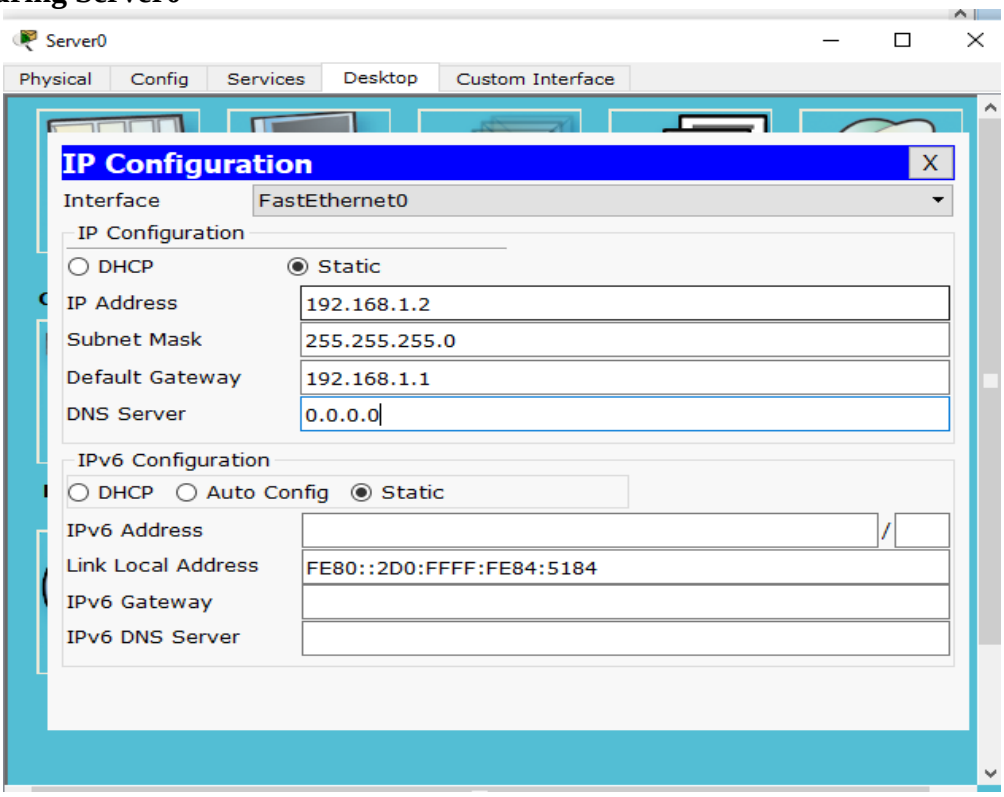
Serial Interface must be added in each Router before configuring it
The serial interface in each Router is added as follows



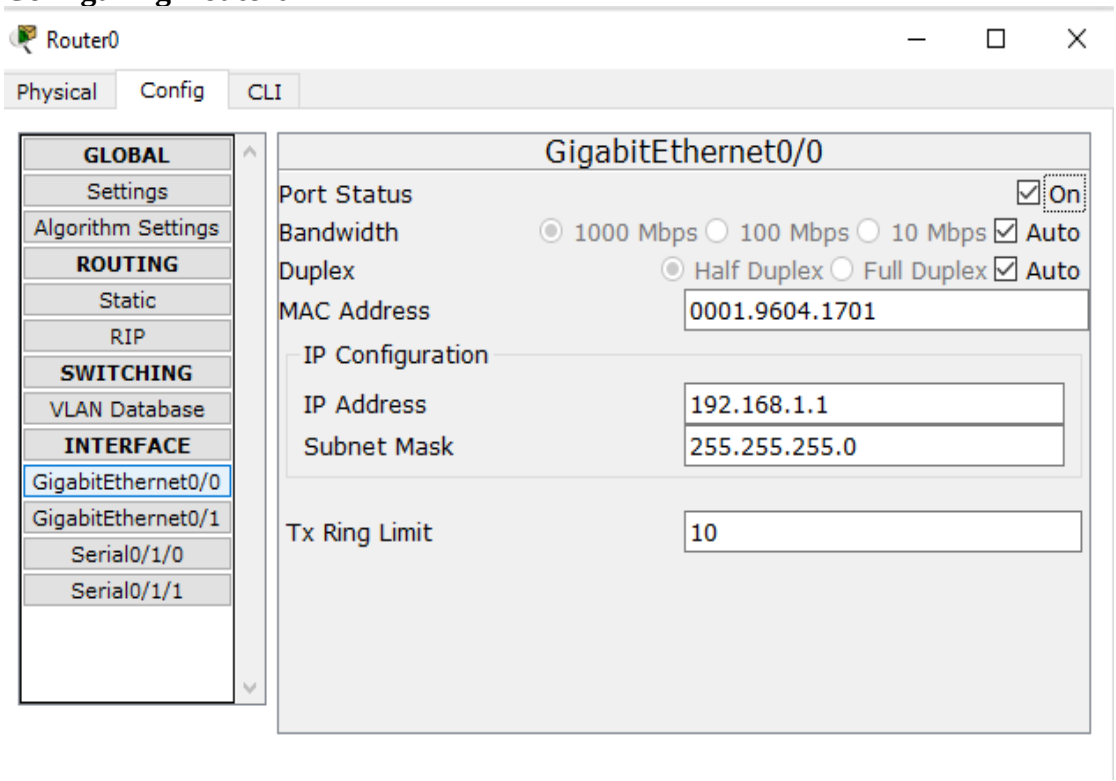
Configuring PC0

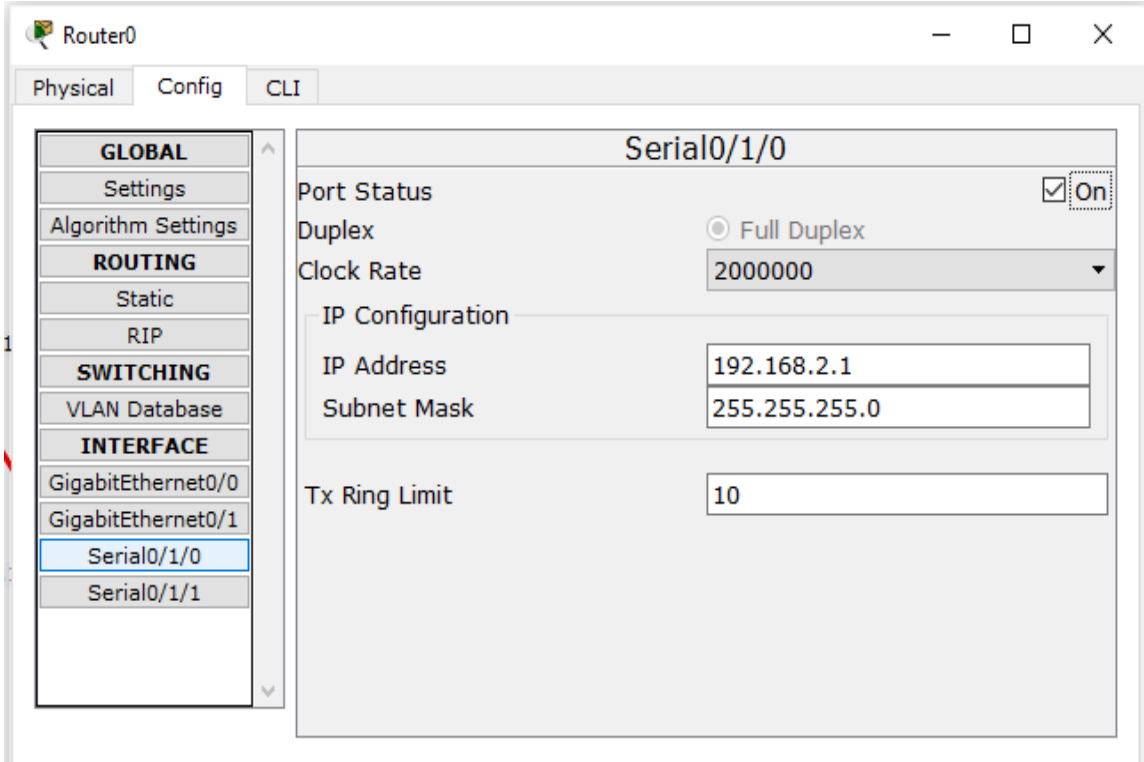


Configuring Server0

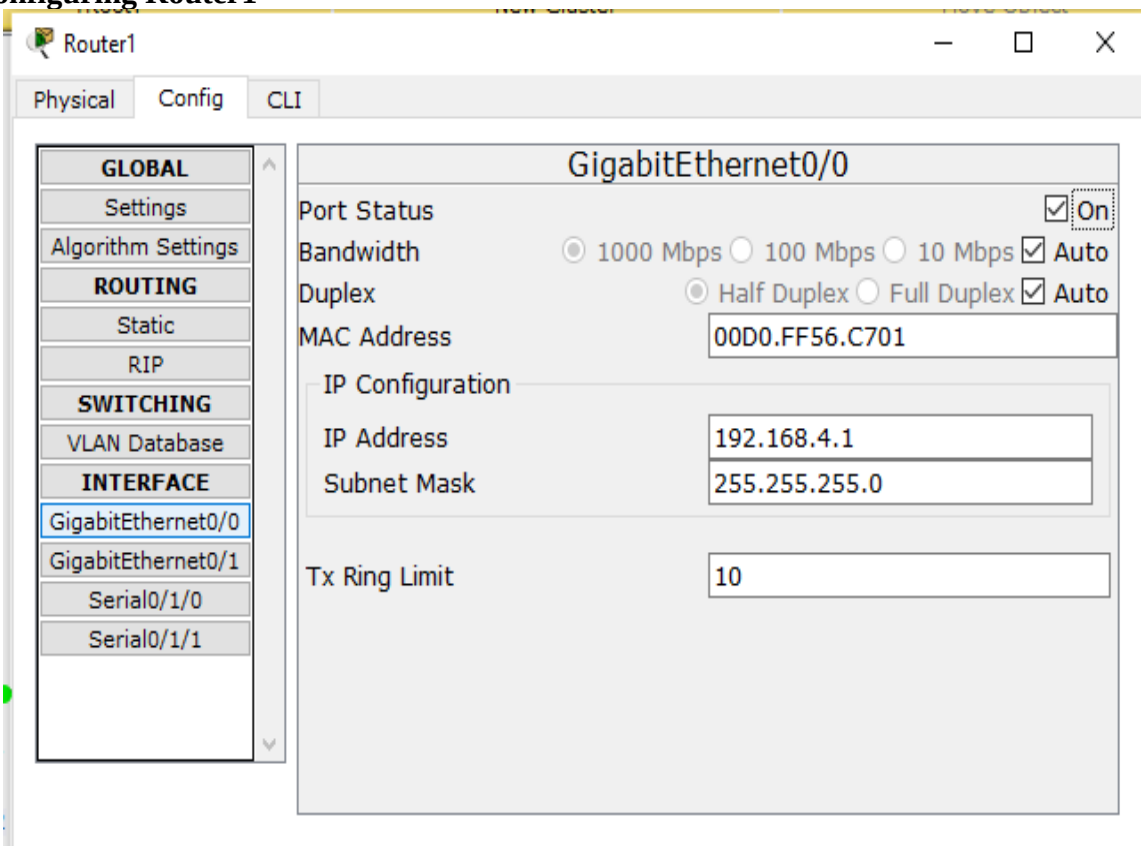


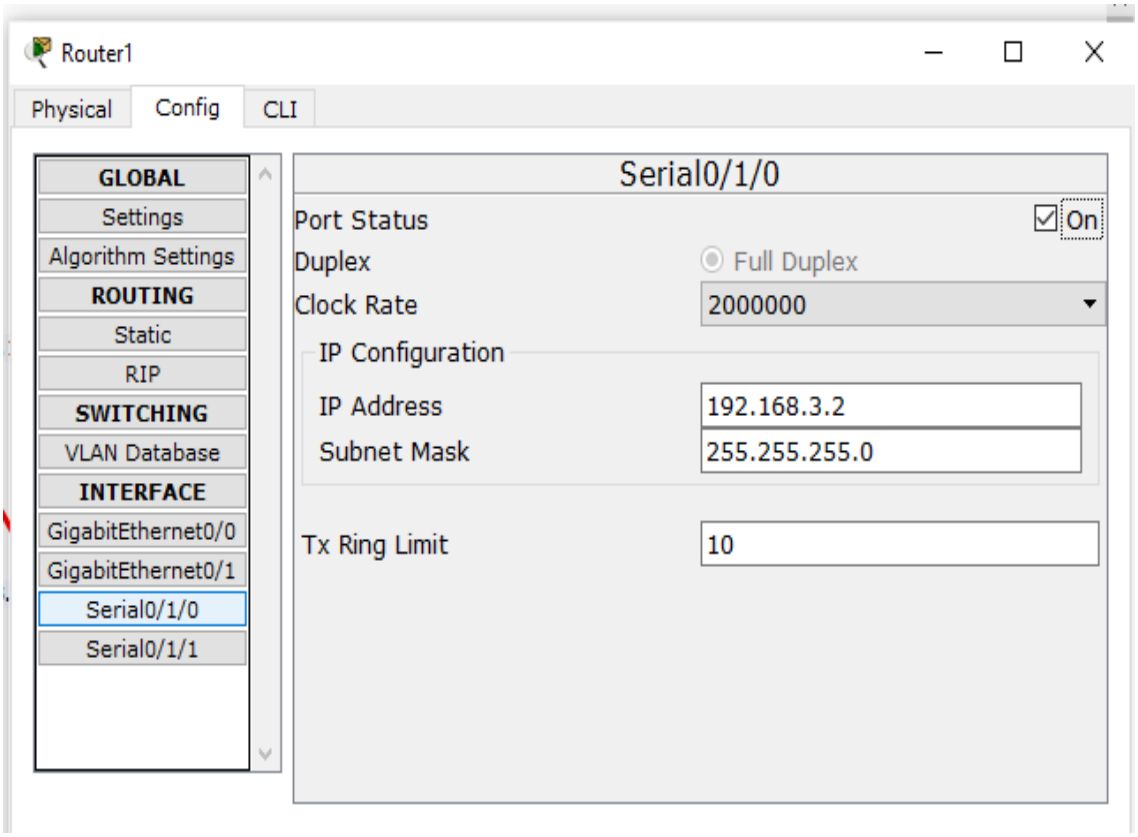
Configuring Router0



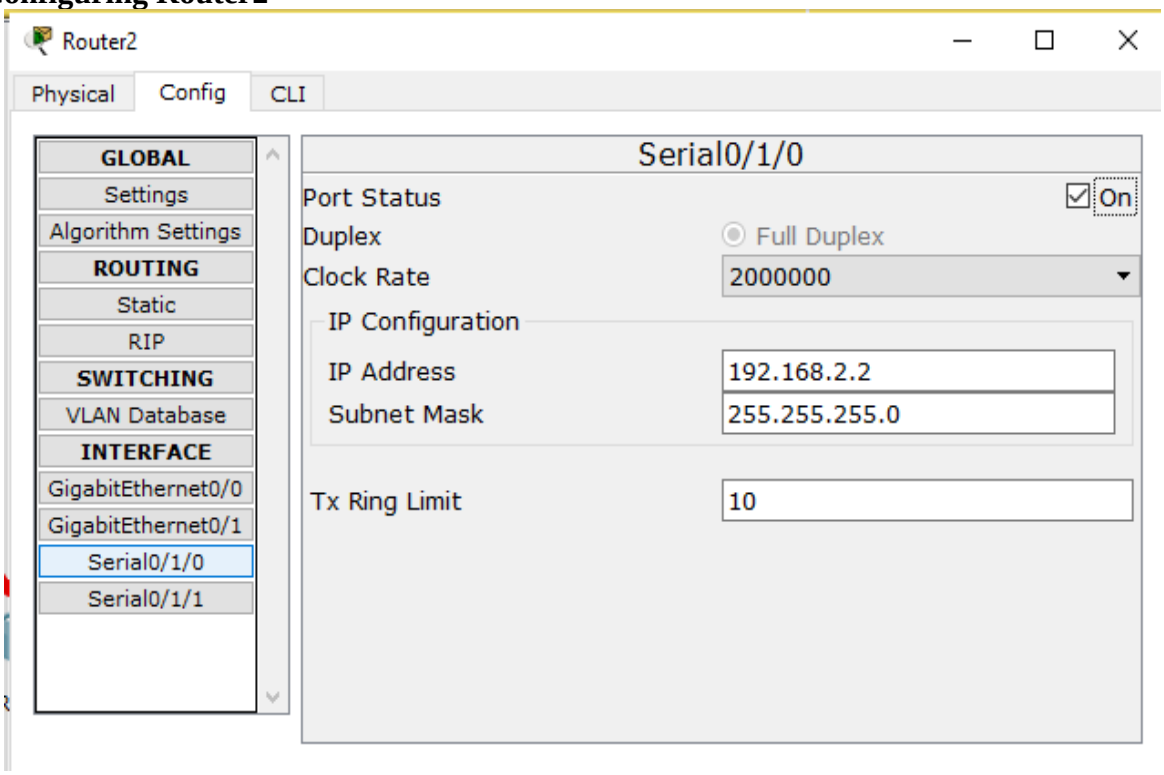


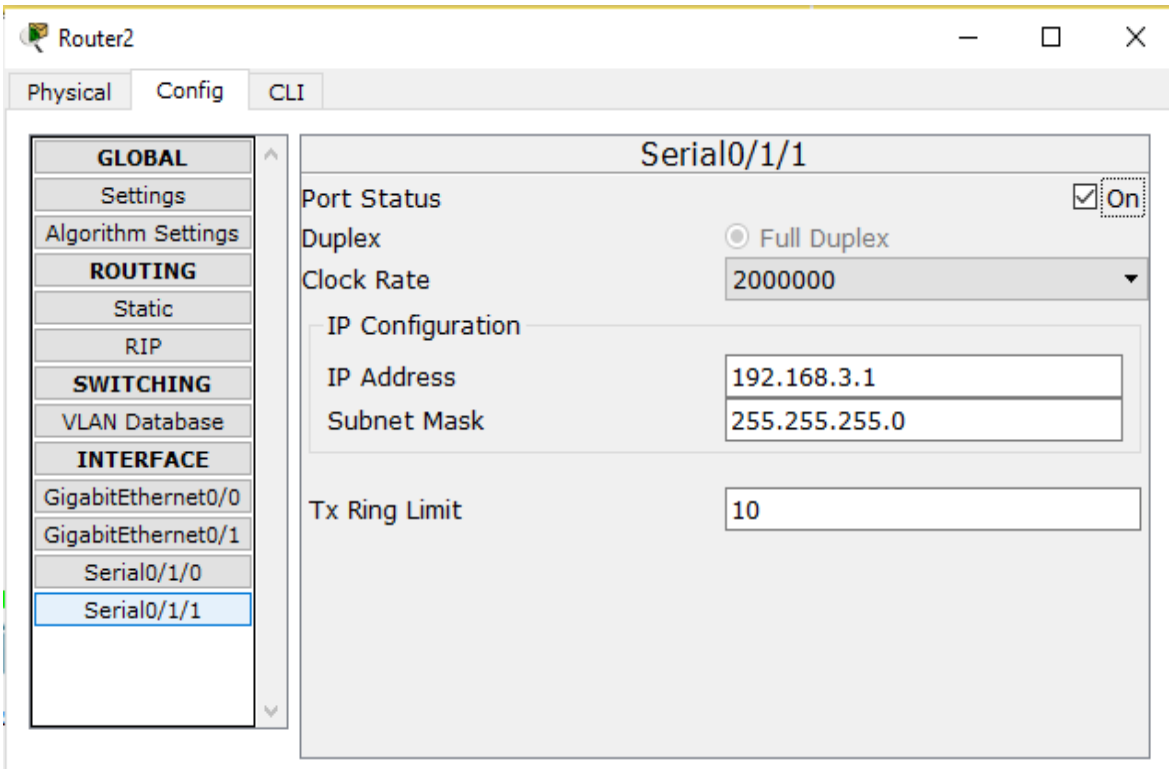
Configuring Router1





Configuring Router2

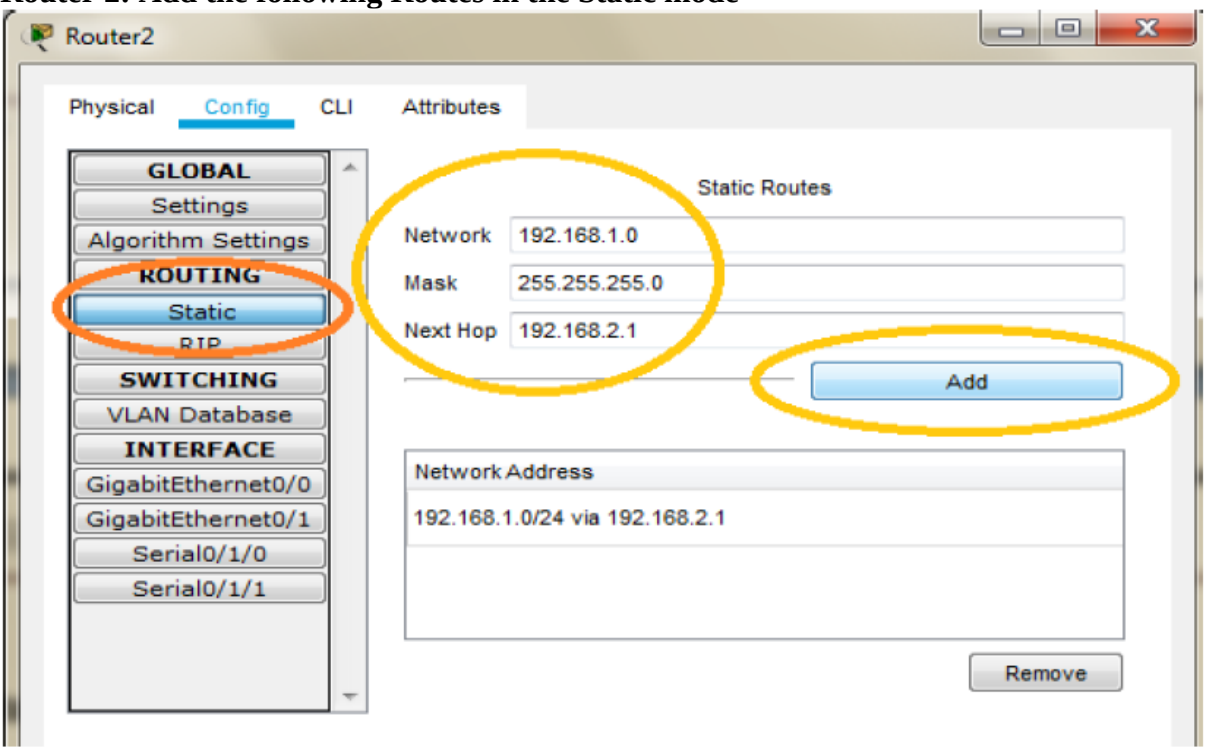


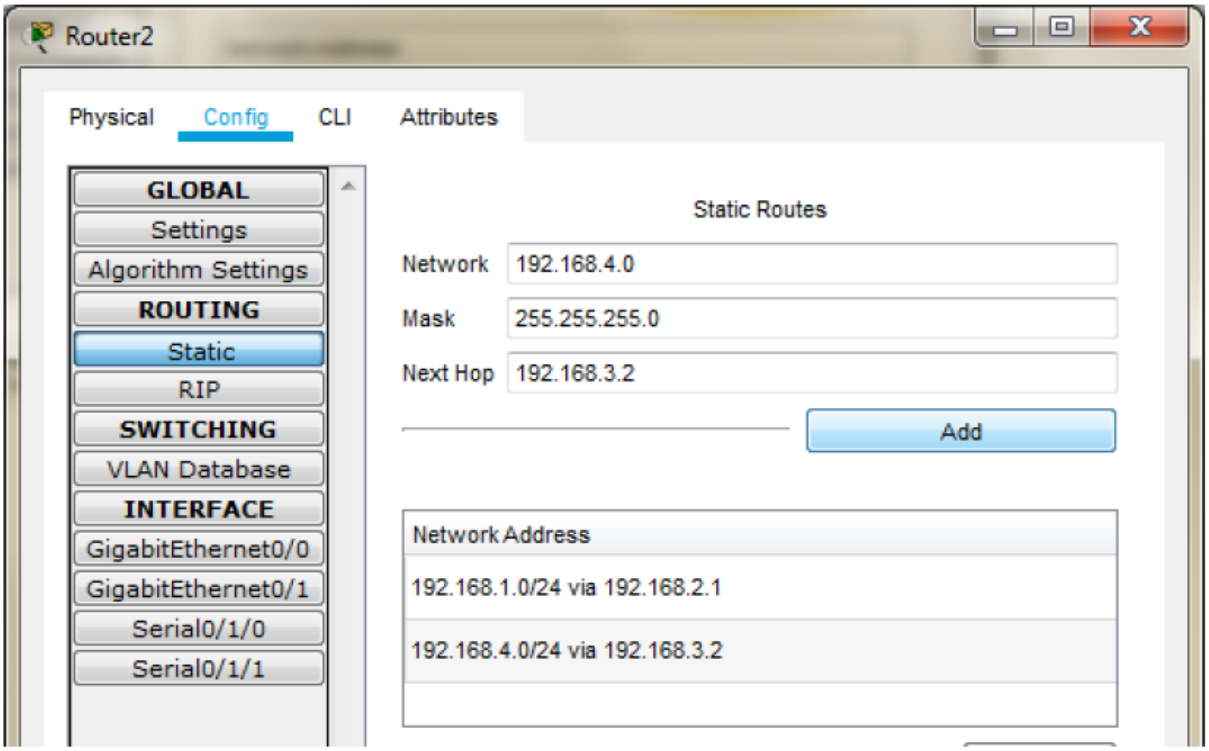


Part 1: Static Routing

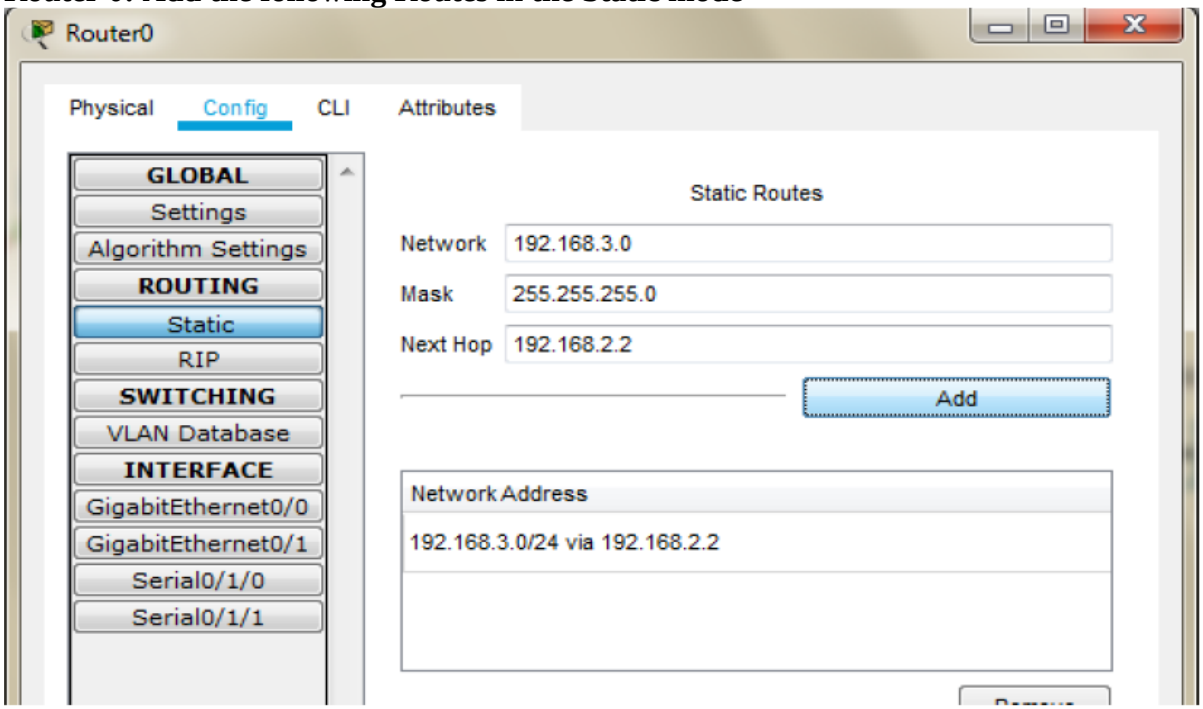
Static Routing is done using the following procedure for each Router

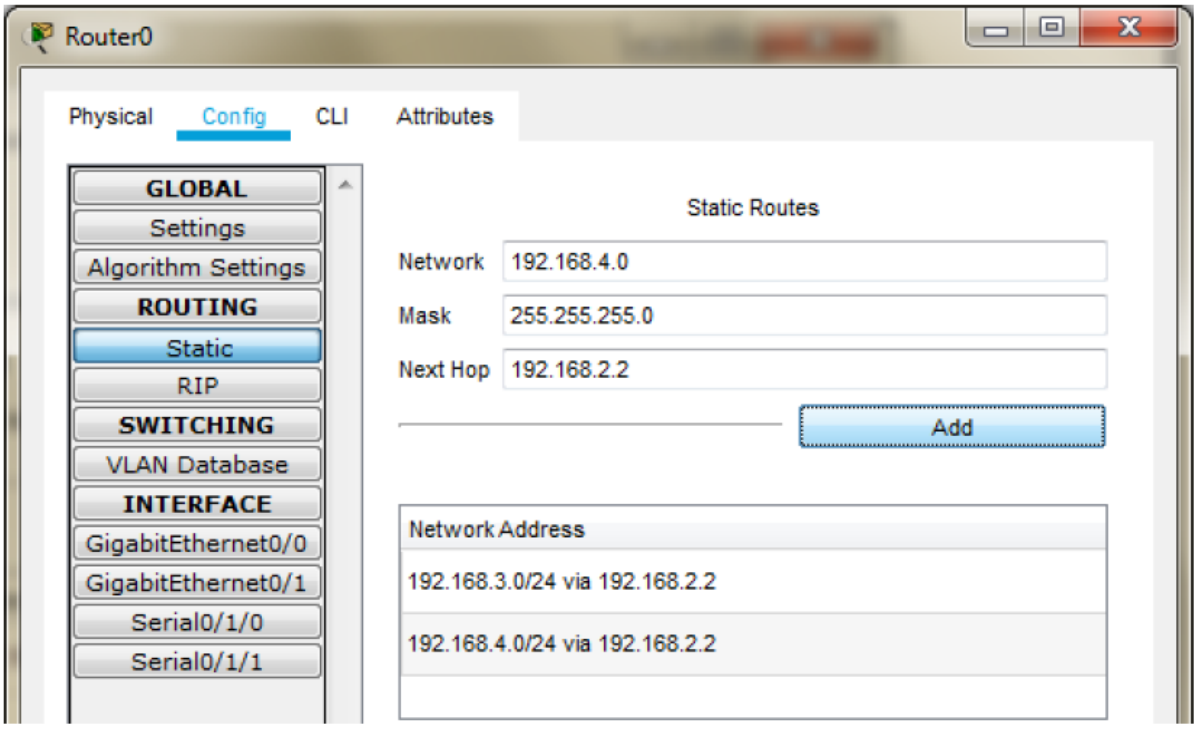
Router 2: Add the following Routes in the Static mode



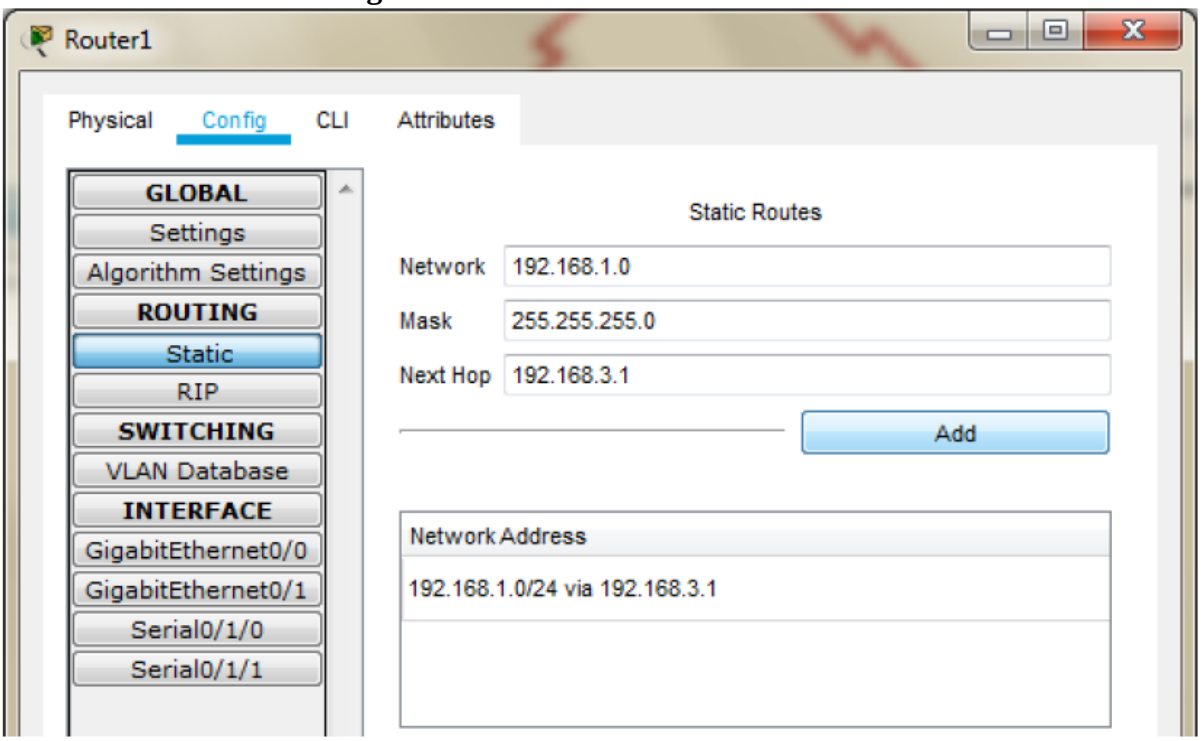


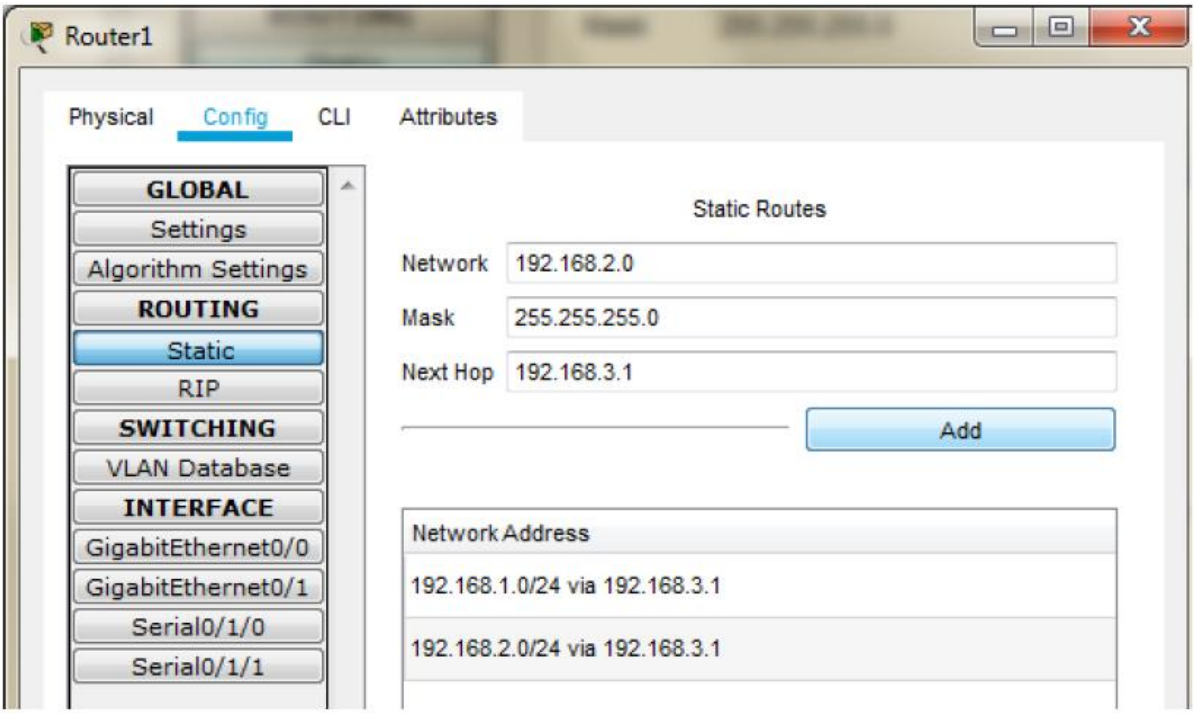
Router 0: Add the following Routes in the Static mode



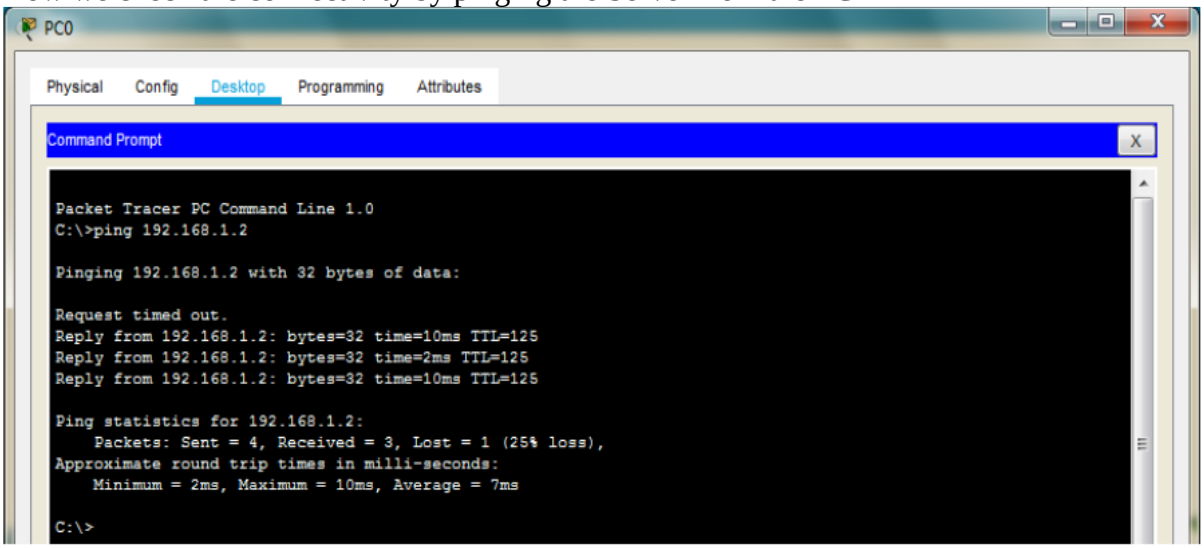


Router 1: Add the following Routes in the Static mode





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



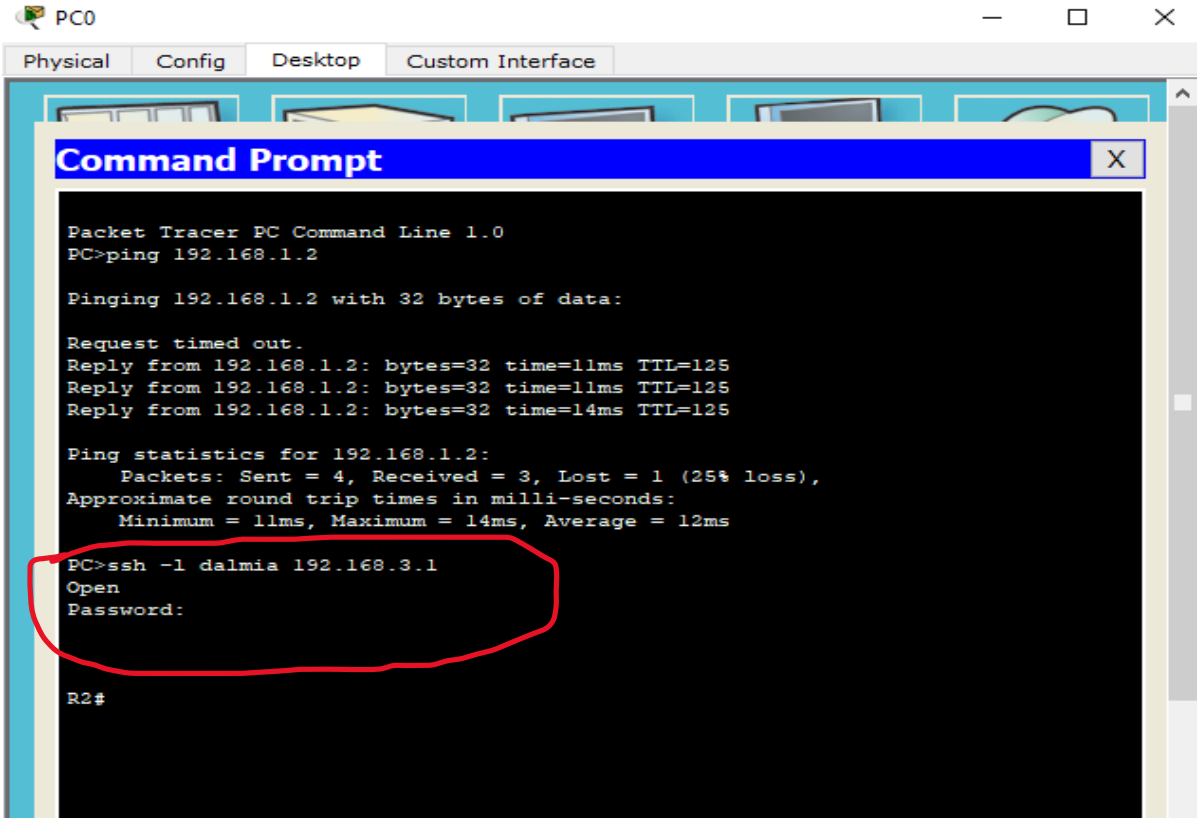
Part 2: Configuring SSH on Router 2

Type the following commands in the CLI mode of Router2

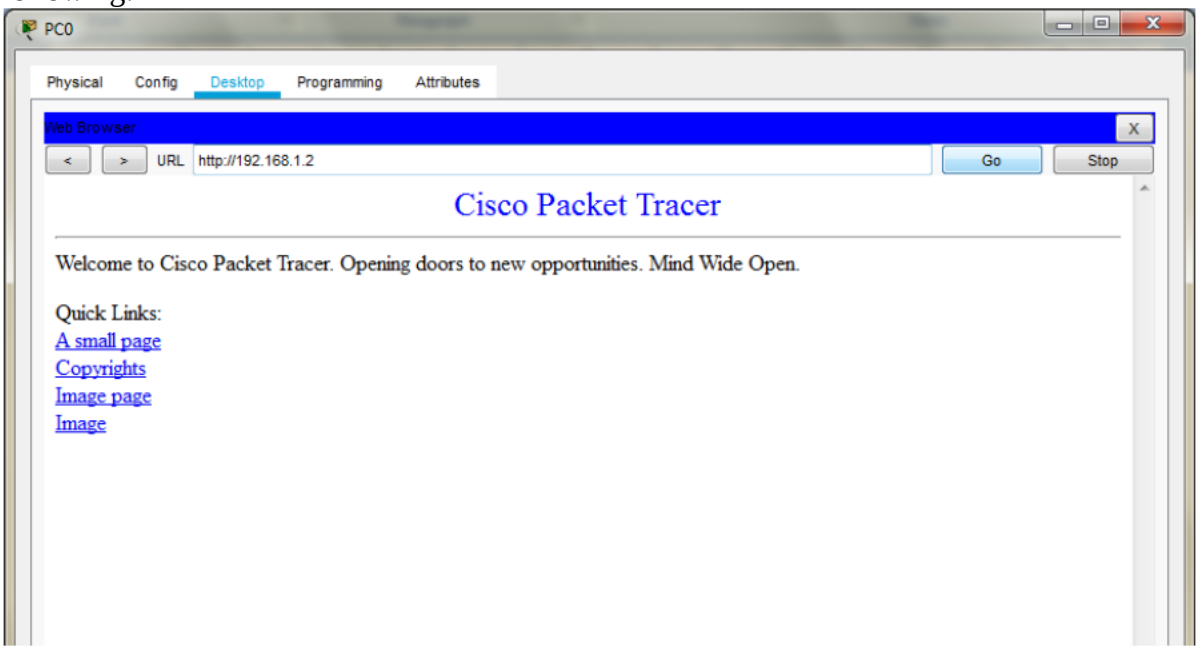
```
Router>en
Router#conf t
Router(config)#ip domain-name dalmia.com
Router(config)#hostname R2
R2(config)#crypto key generate rsa
The name for the keys will be: R2.dalmia.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater 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: -



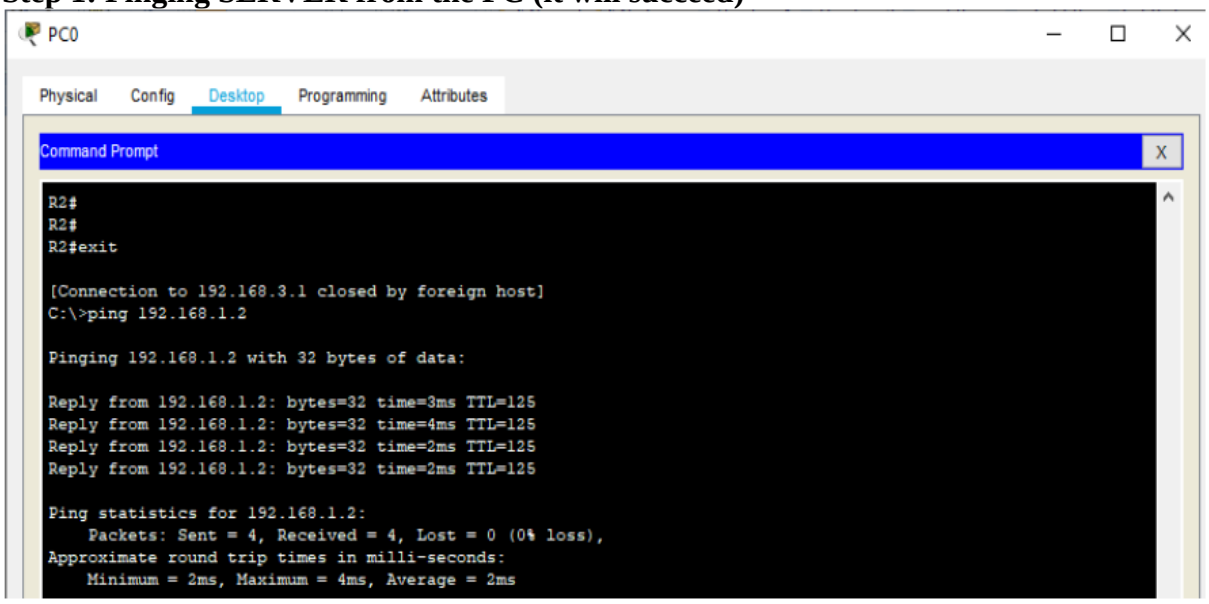
Part 3: Create the Firewall Zones on Router1

Type the following commands in the CLI mode of Router1

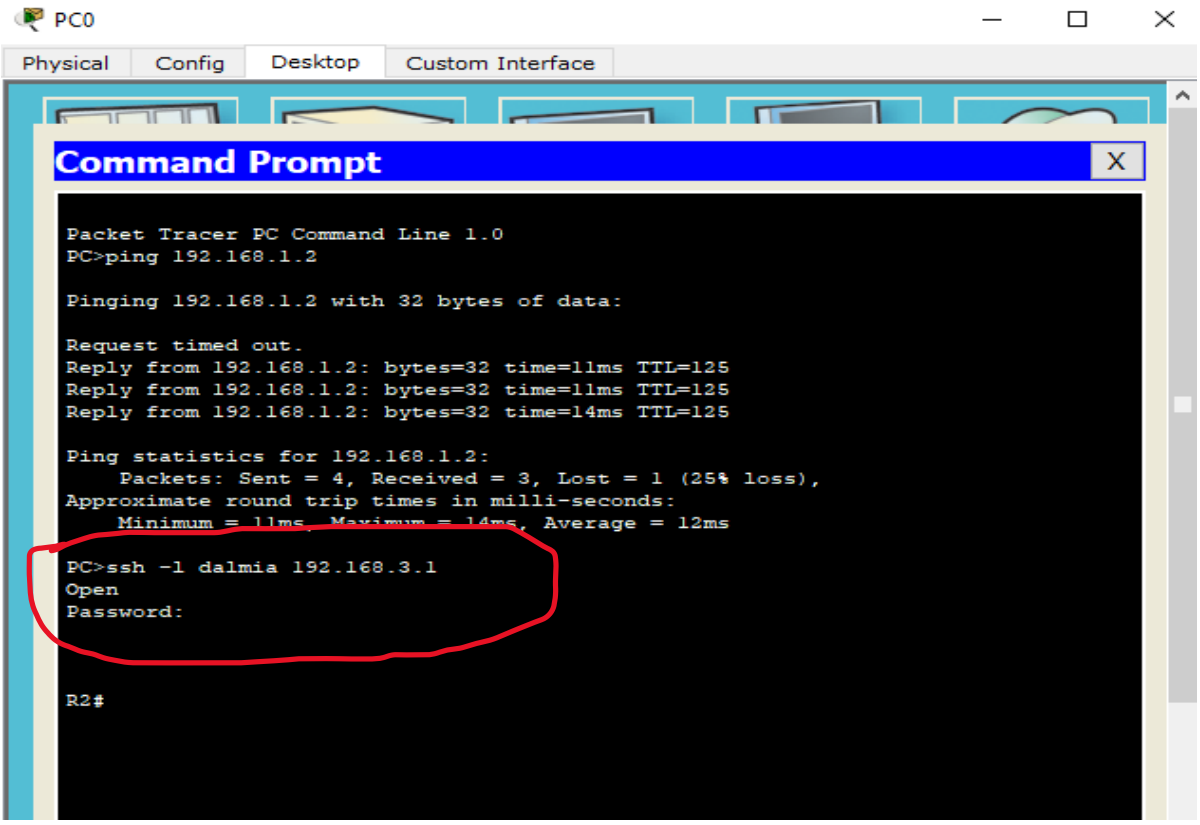
```
Router>en
Router#conf t
Router(config)#license boot module c1900 technology-package securityk9
ACCEPT? [yes/no]: y
Router(config)#exit
Router#copy run start
Press enter when prompted
Router#reload
Continue with configuration dialog? [yes/no]: n
Router>en
Router#conf t
Router(config)#zone security 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)



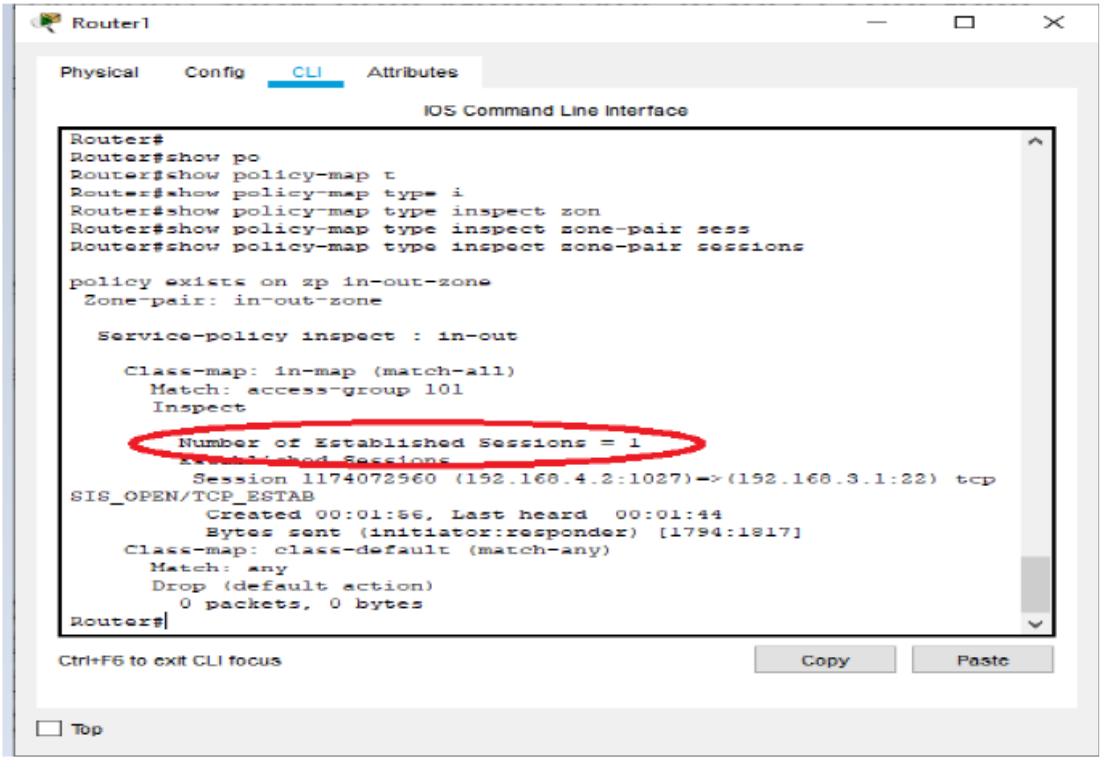
Step 2: Start an SSH session from PC to Router 2 (ip 192.168.1.2)



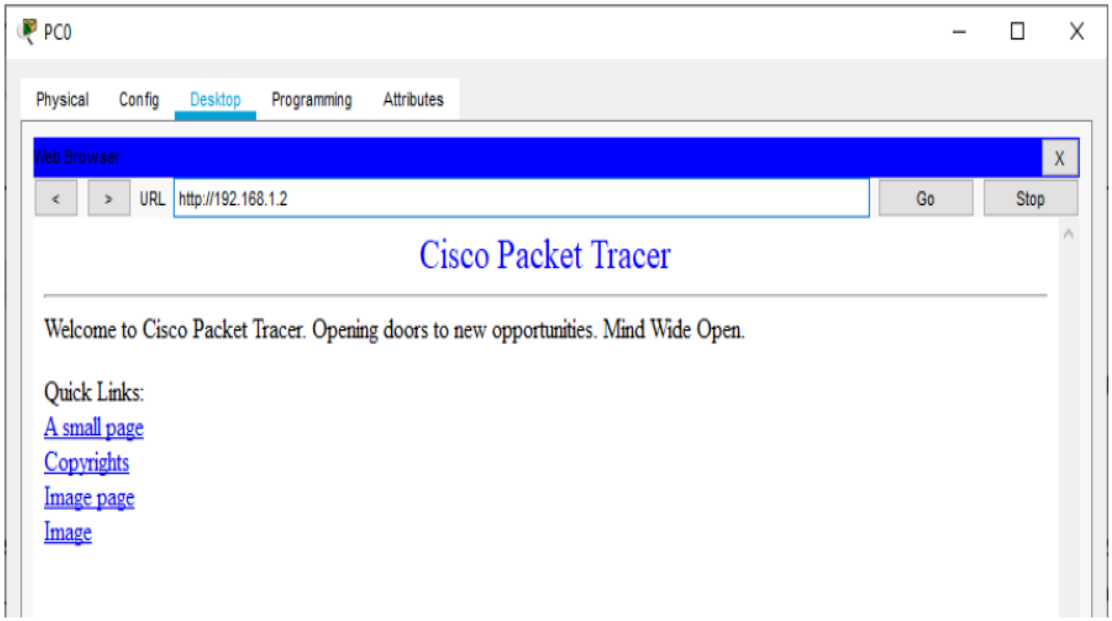
As seen above the session becomes active and we get access to Router2 (Do not exit and the session and continue to Step 3)

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

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

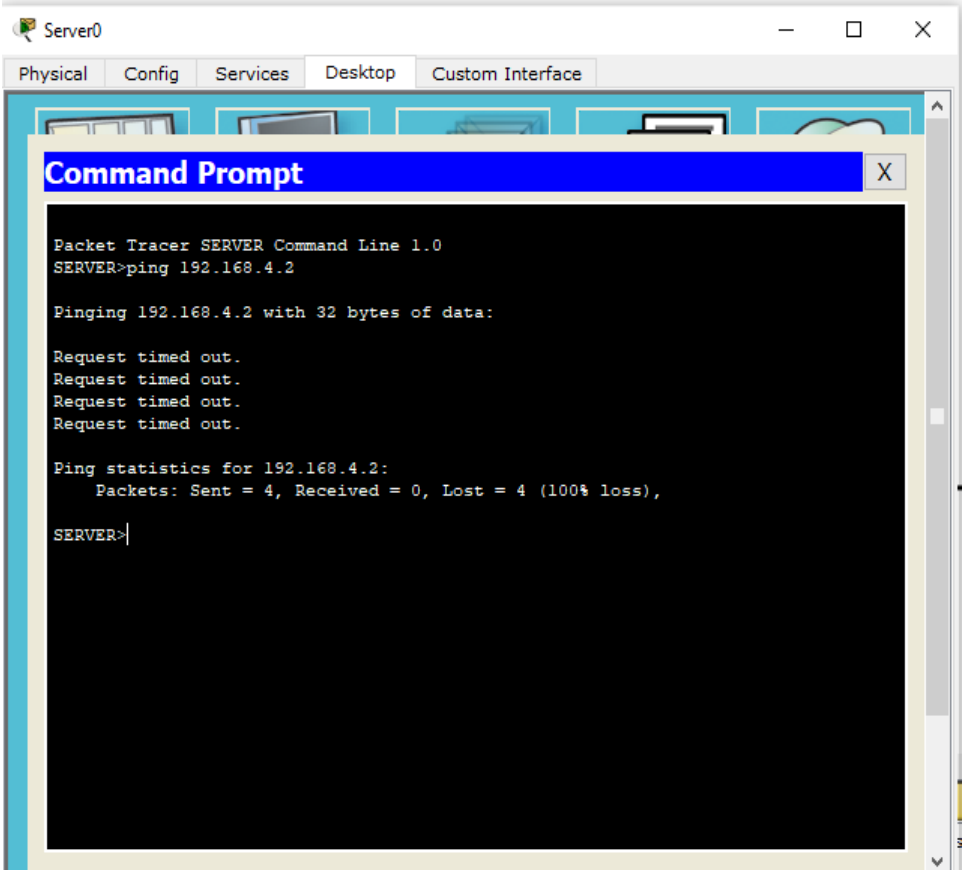


Step 4: We close the SSH connection and open the web browser and access the server address (192.168.1.2) and get the following



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.

****