PRACTICAL NO 7: Configure IOS Intrusion Prevention System (IPS) Using the CLI

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE). The network administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. These parameters have default values but can also be configured through CLI. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

1) Send an alarm to a syslog server or a centralized management interface
2) Drop the packet
3) Reset the connection
4) Deny traffic from the source IP address of the attacker for a specified amount of time
5) Deny traffic on the connection for which the signature was seen for a specified amount of time

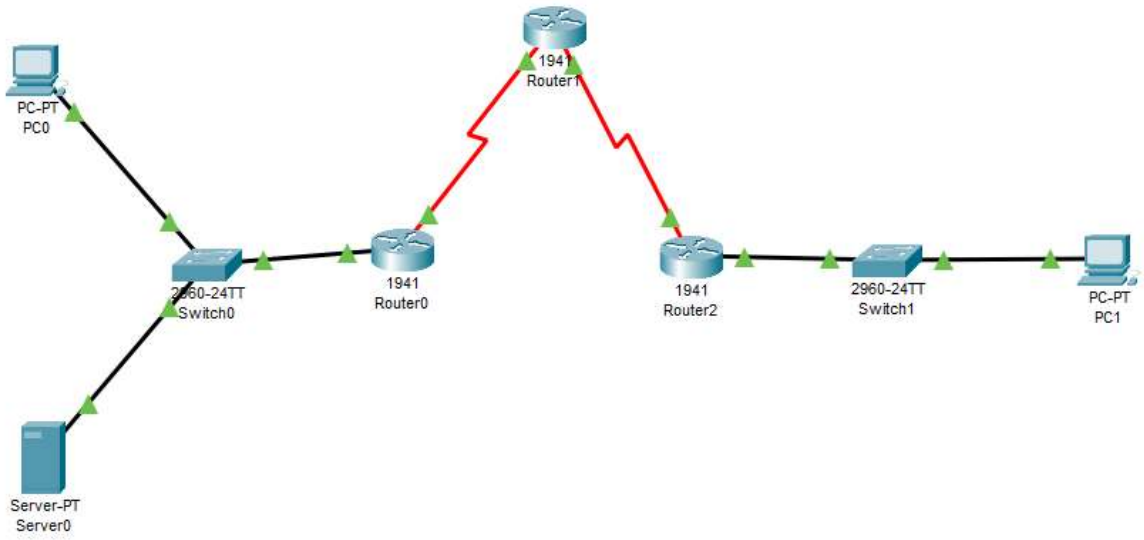
Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features may be enabled independently and on different router interfaces.

Signatures:

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks. We can easily install signatures using IDS and IPS management software such as Cisco IDM. Sensors enables us to modify existing signatures and define new ones.

As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. A malicious packet flow has a specific type of activity and signature, and an IDS or IPS sensor examines the data flow using many different signatures. When an IDS or IPS sensor matches a signature with a data flow, the sensor takes action, such as logging the event or sending an alarm to IDS or IPS management software, such as the Cisco SDM

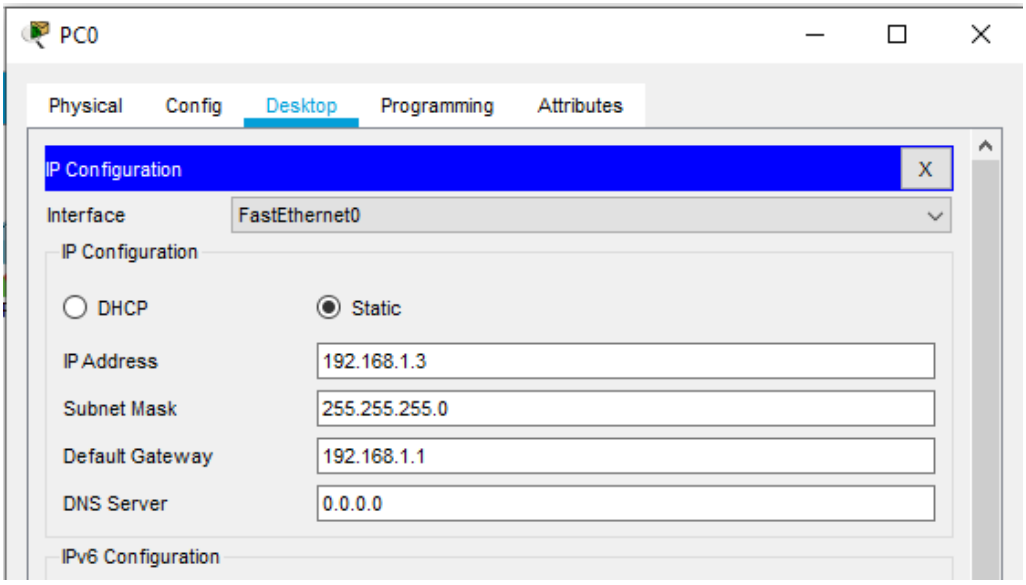
We us the following topology for the present case:



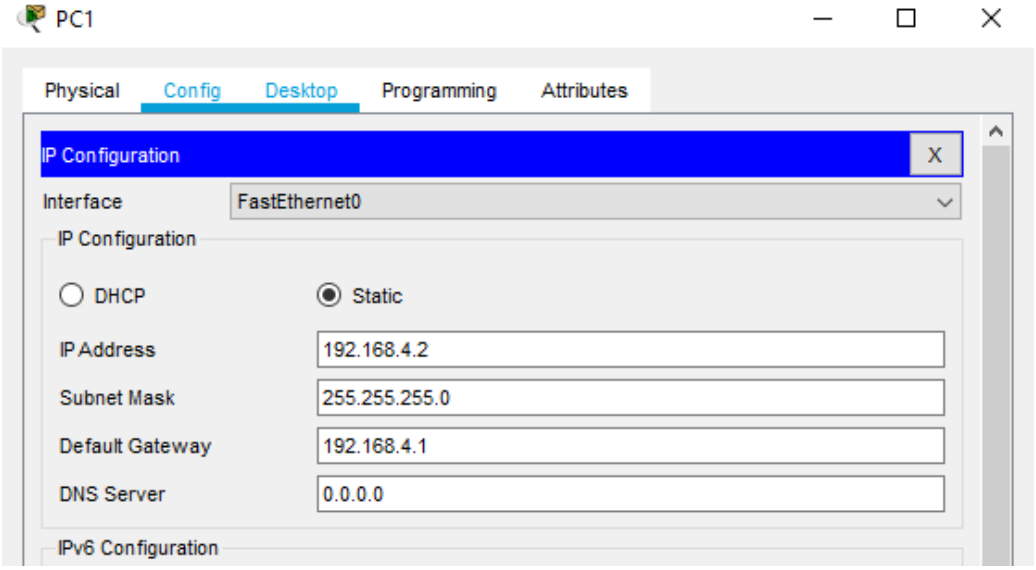
Let us consider the following Address table to configure the network devices:

Device	Interface	IP Address	Subnet Mask	Default gateway	Switch Port
PC 0	NA	192.168.1.3	255.255.255.0	192.168.1.1	Switch0 F0/1
PC 1	NA	192.168.4.2	255.255.255.0	192.168.4.1	Switch1 F0/1
Server0	NA	192.168.1.2	255.255.255.0	192.168.1.1	Switch0 F0/2
Router0	GE0/0	192.168.1.1	255.255.255.0	NA	Switch0 F0/5
	S0/1/0	192.168.2.1	255.255.255.0	NA	NA
Router1	S0/1/0	192.168.2.2	255.255.255.0	NA	NA
	S0/1/1	192.168.3.1	255.255.255.0	NA	NA
Router2	S0/1/1	192.168.3.2	255.255.255.0	NA	NA
	GE0/0	192.168.4.1	255.255.255.0	NA	Switch1 F0/5

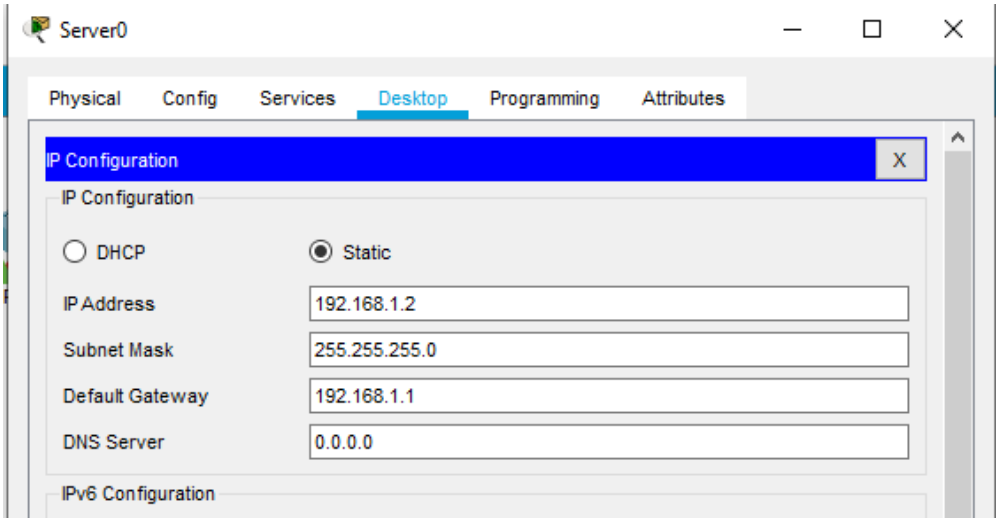
Configuring PC0



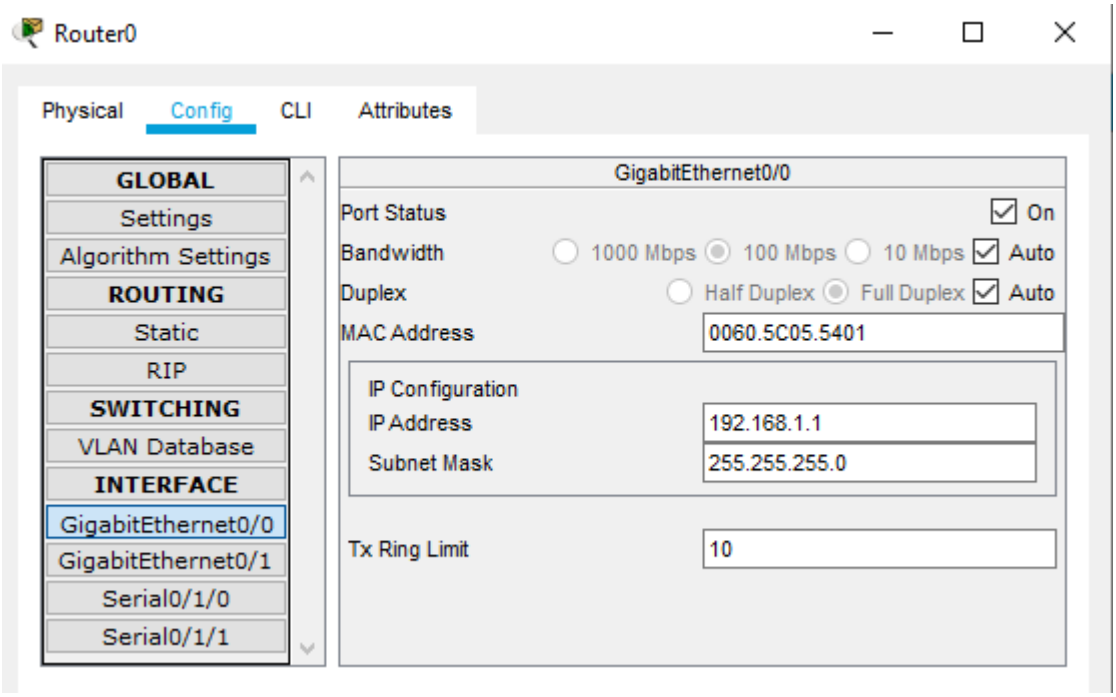
Configuring PC1

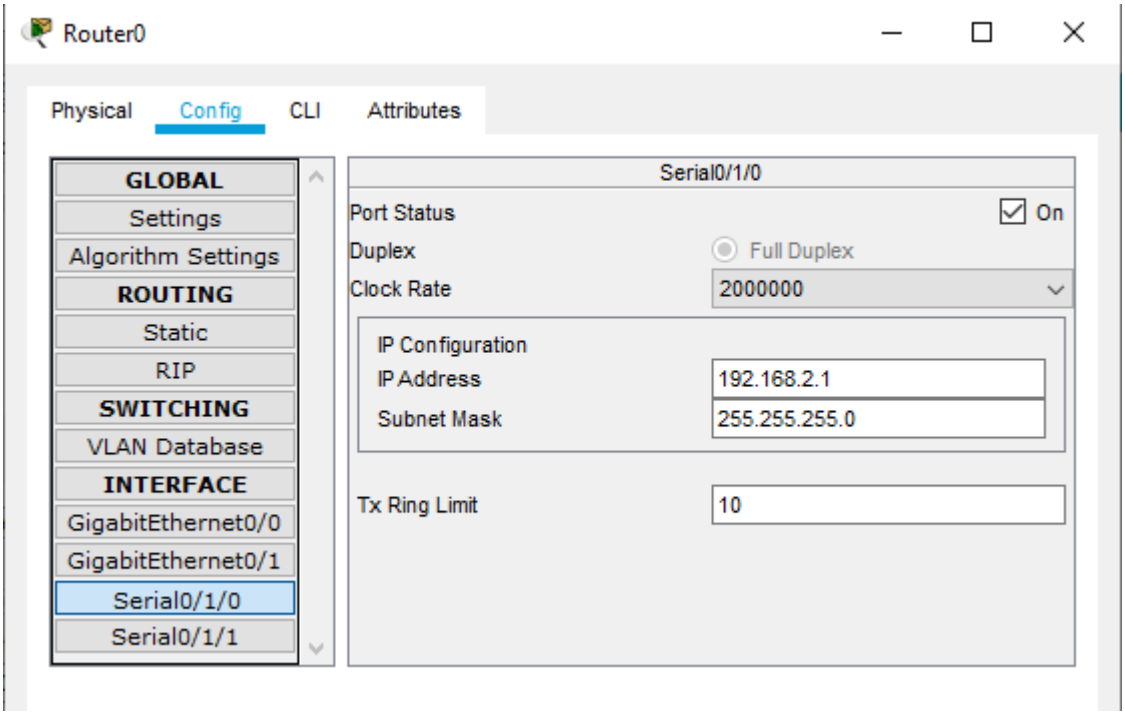


Configuring Server0

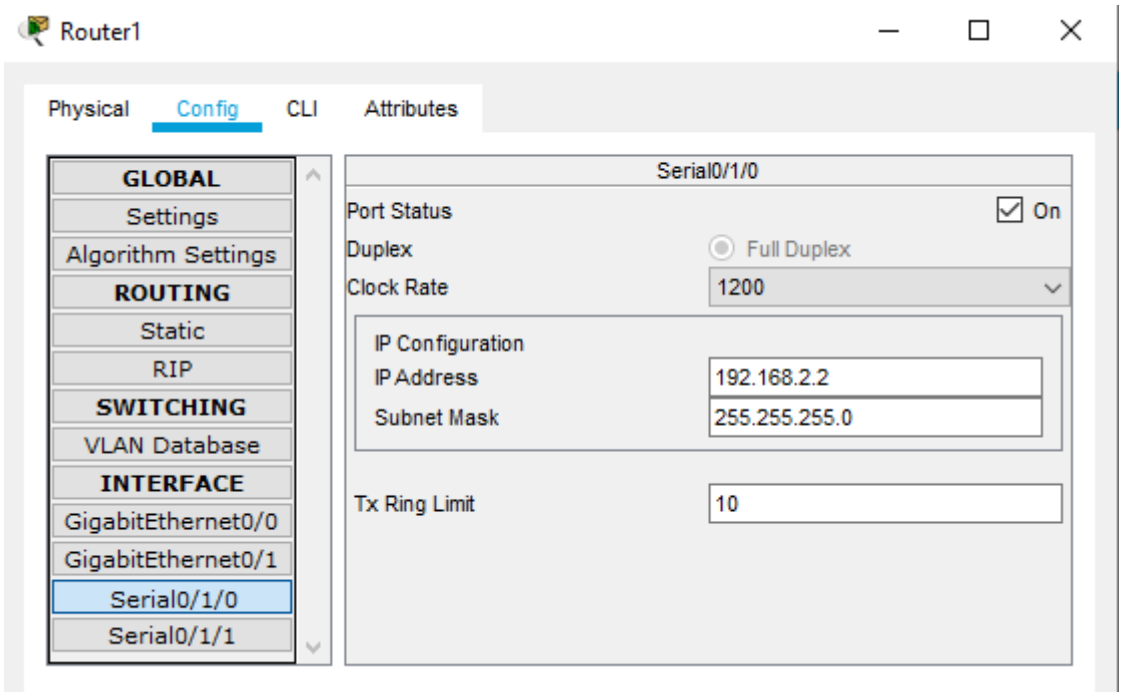


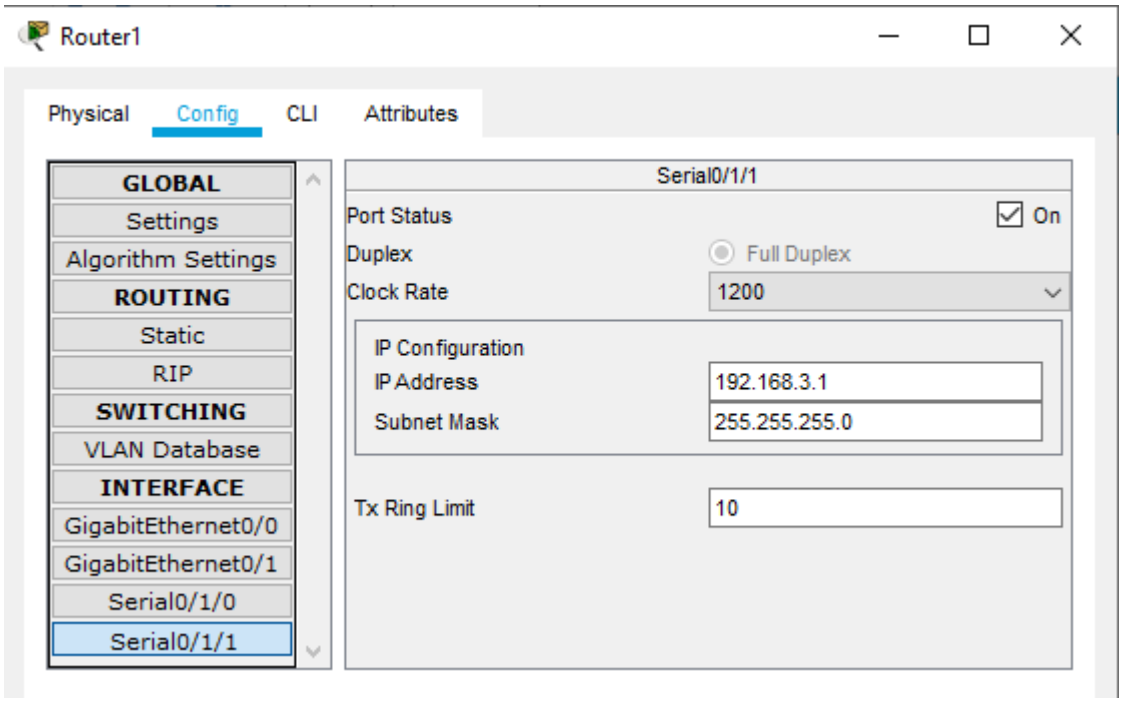
Configuring Router0



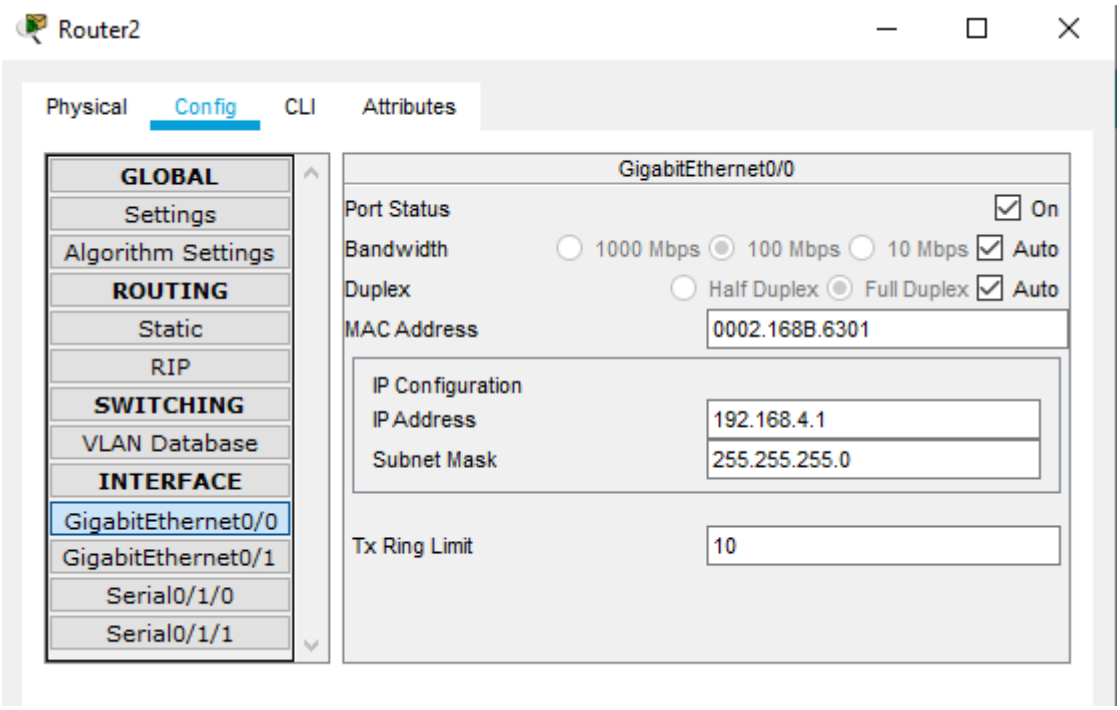


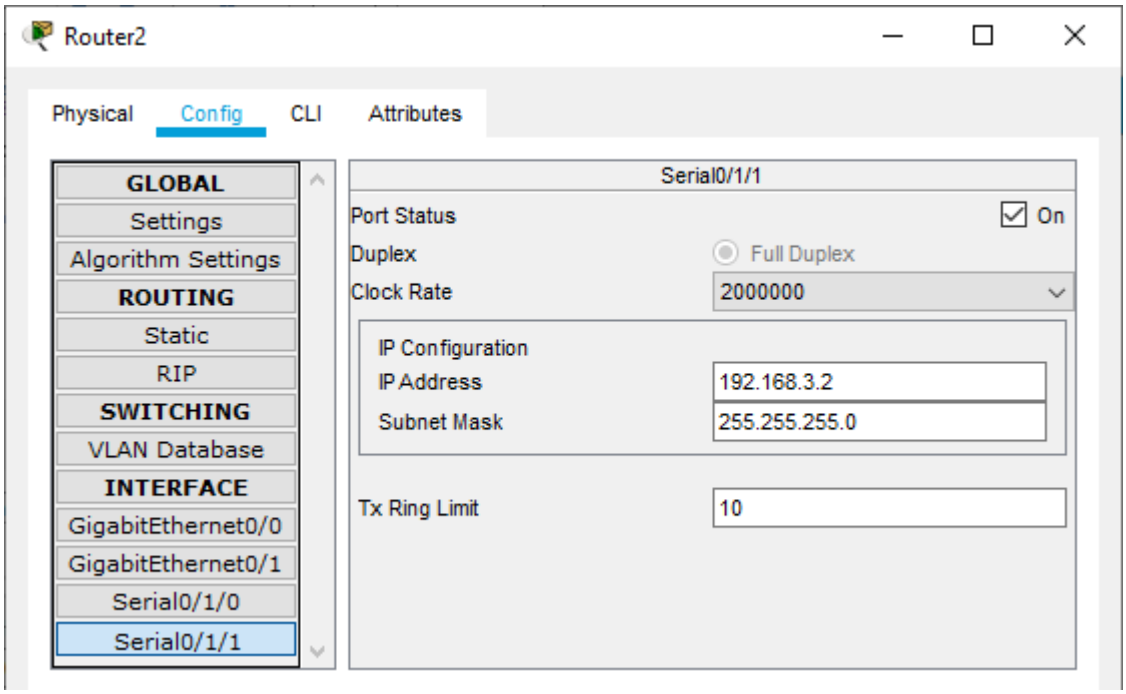
Configuring Router1



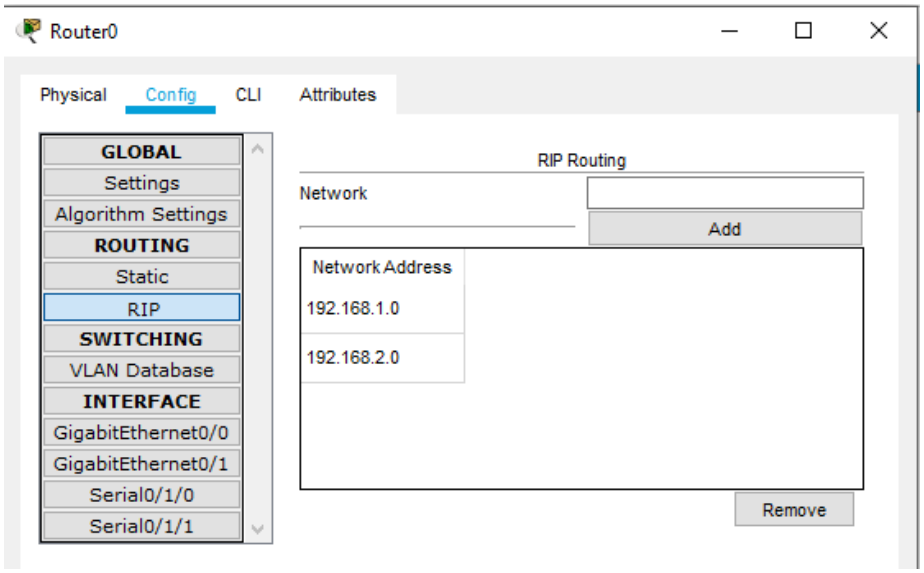


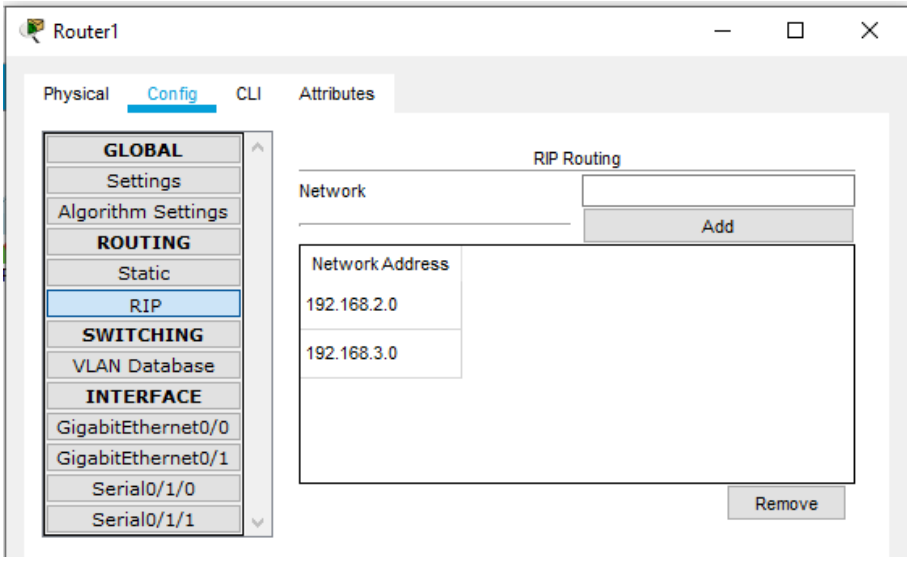
Configuring Router2

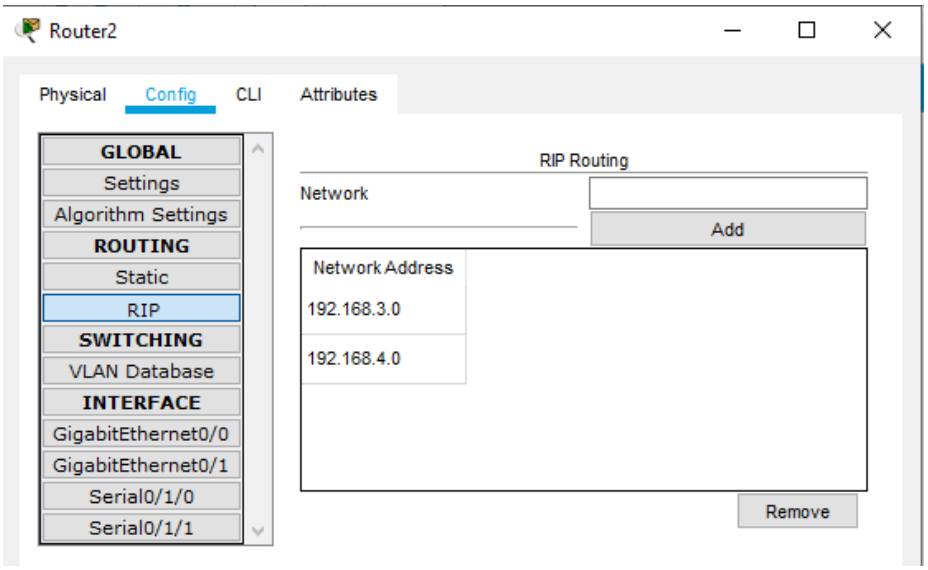




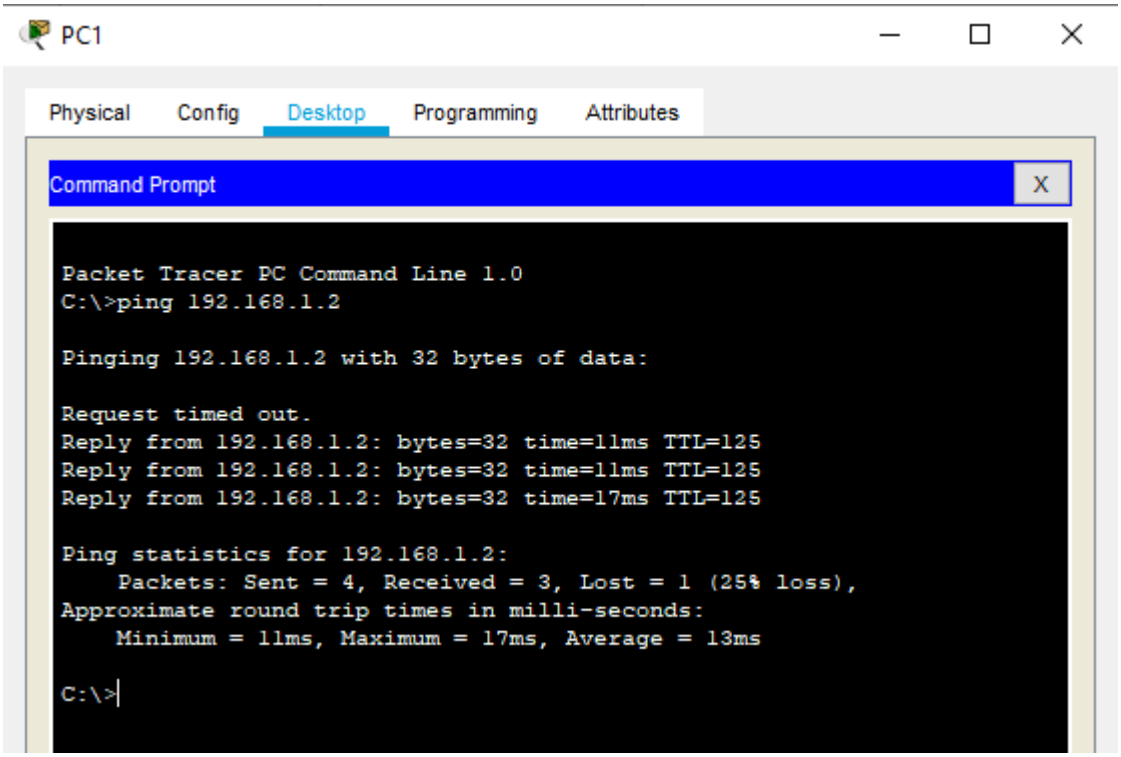
We need to set the Routing table in all the Routers so that each node could send and receive packets from others (RIP is set in all the Routers as follows)

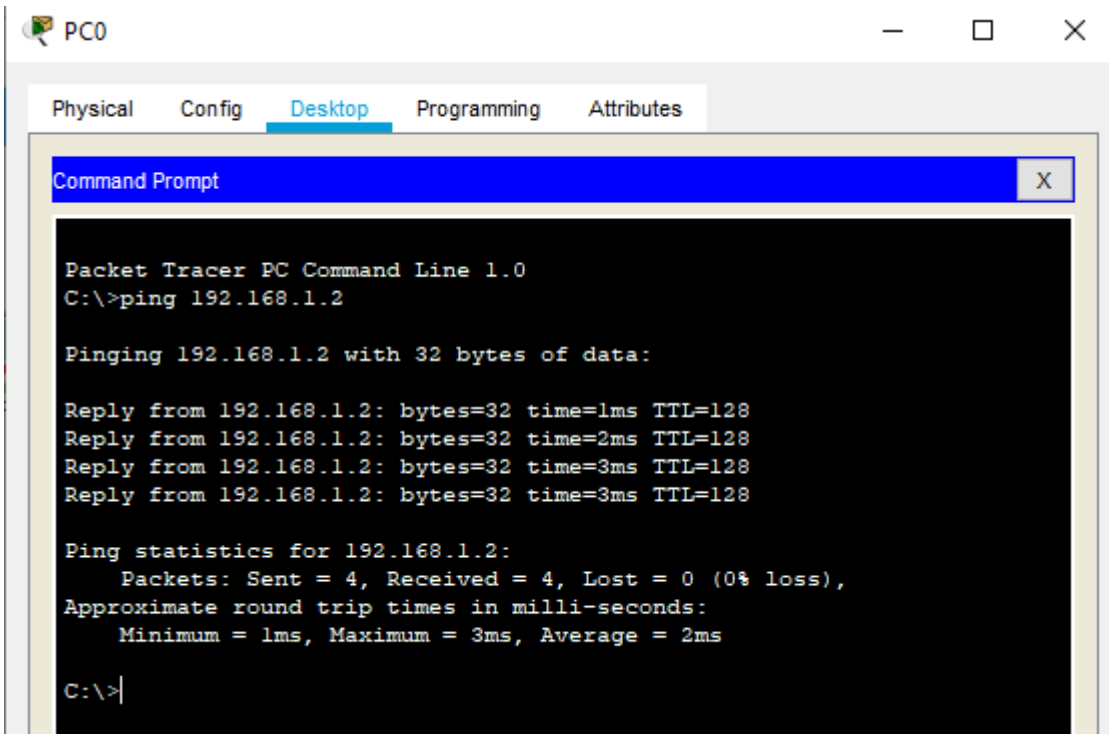






Now we can check the connectivity by sending ping commands from any node to any other node





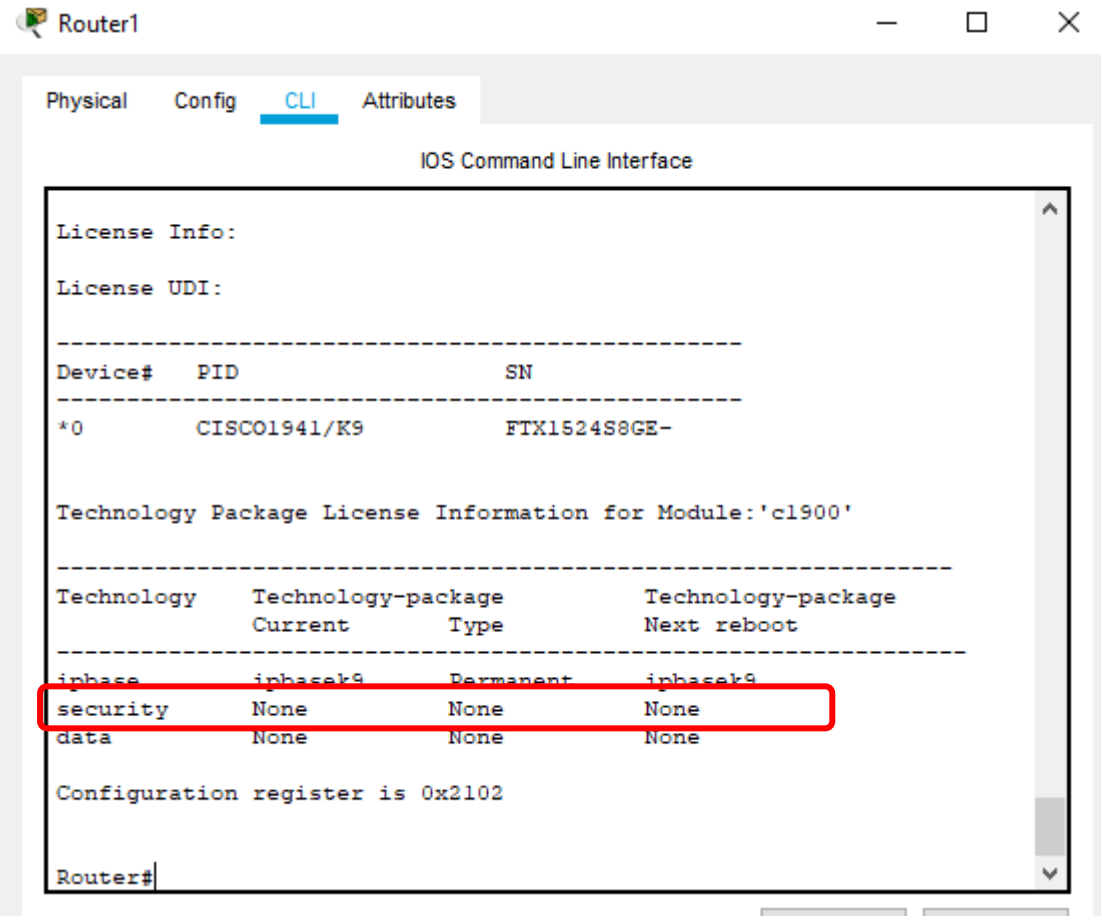
So, we conclude that the connectivity has been established

PART1: Enable the IOS IPS (on Router1)

Type the following command in the CLI mode of Router1

Router#show version

We will get a message informing whether the security Package is enabled or not



As seen above the security package is not enabled, to enable the security feature, type the following command in Router1

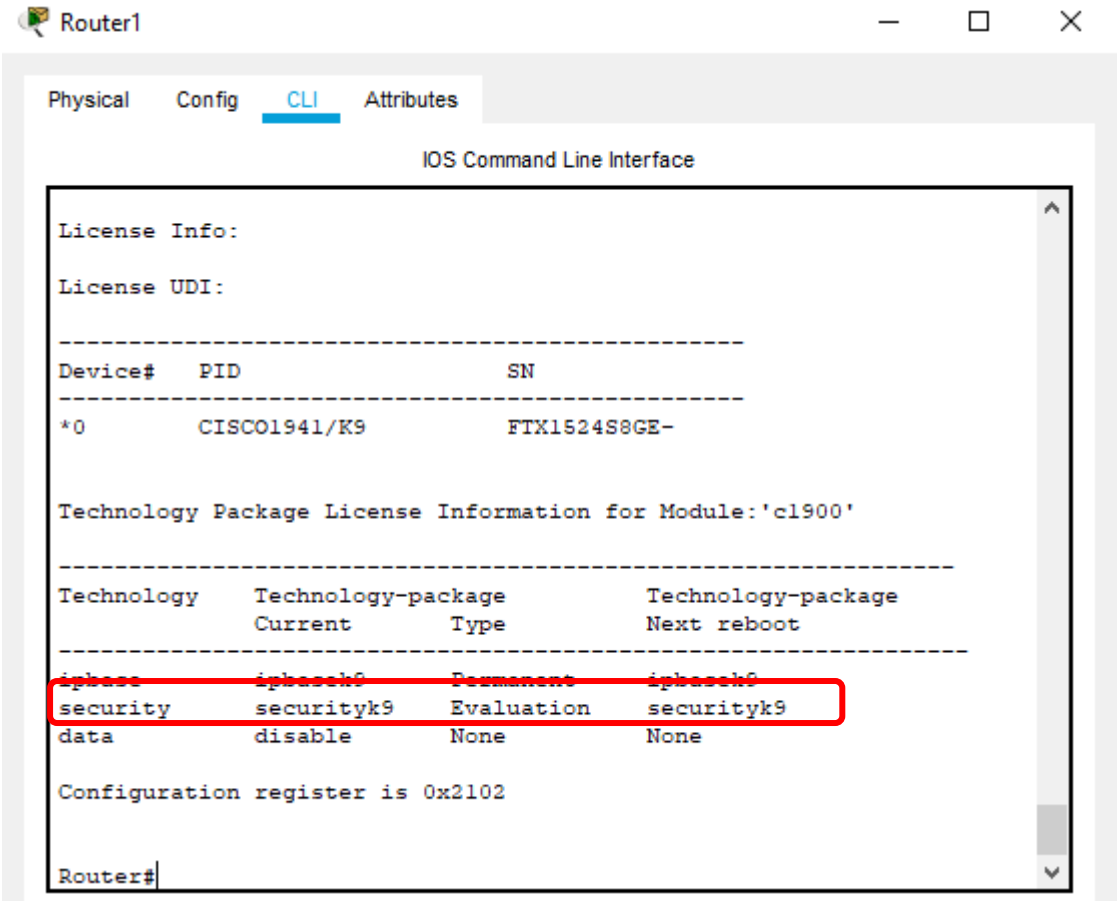
Router#configure terminal
Router(config)#license boot module c1900 technology-package securityk9
ACCEPT? [yes/no]: y

Press enter key

Router#
Router#reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm] Press Enter key
Press RETURN to get started! Press Enter key

Router>enable
Router# Router#show version

We will get a message informing whether the security package is enabled or not



As seen above now the security package has been enabled

Now type the following commands in the CLI mode of Router1

Router#
Router#clock set 10:30:45 march 3 2022
Router#mkdir smile
Create directory filename [smile]? Press enter key
Created dir flash:smile

Router#

Router#configure terminal
Router(config)#ip ips config location flash:smile
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#ip ips signature-category
Router(config-ips-category)#category all

```
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit

Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y

Router(config)#interface Serial0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#
Press enter key
Router(config-if)#exit
Router(config)#
```

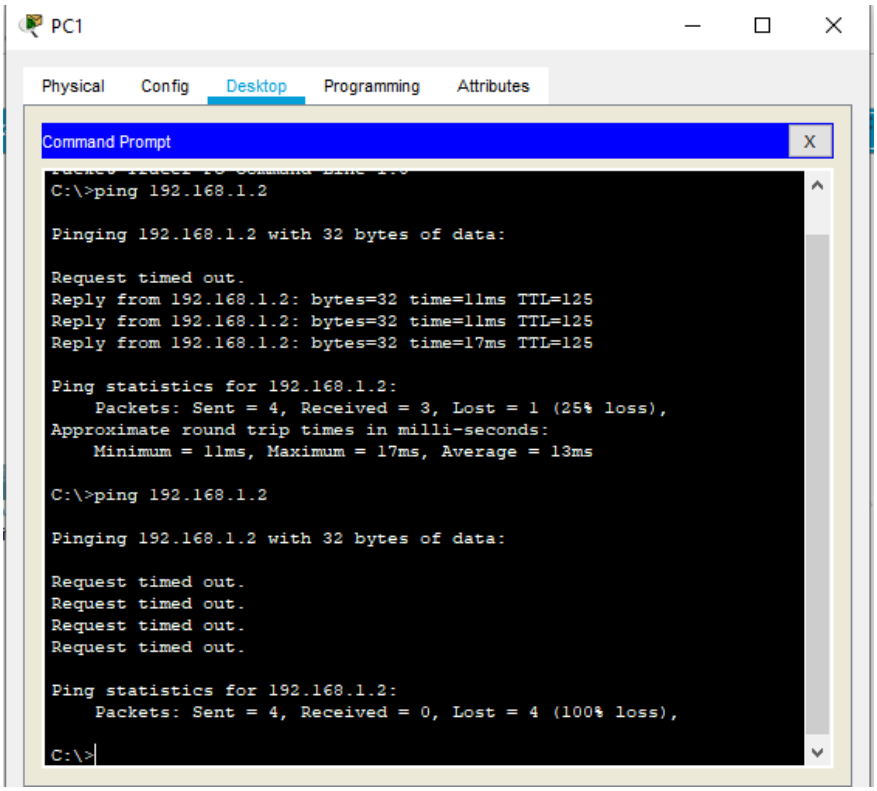
Part 2: Modify the Signature

Type the following commands in the CLI mode of Router1

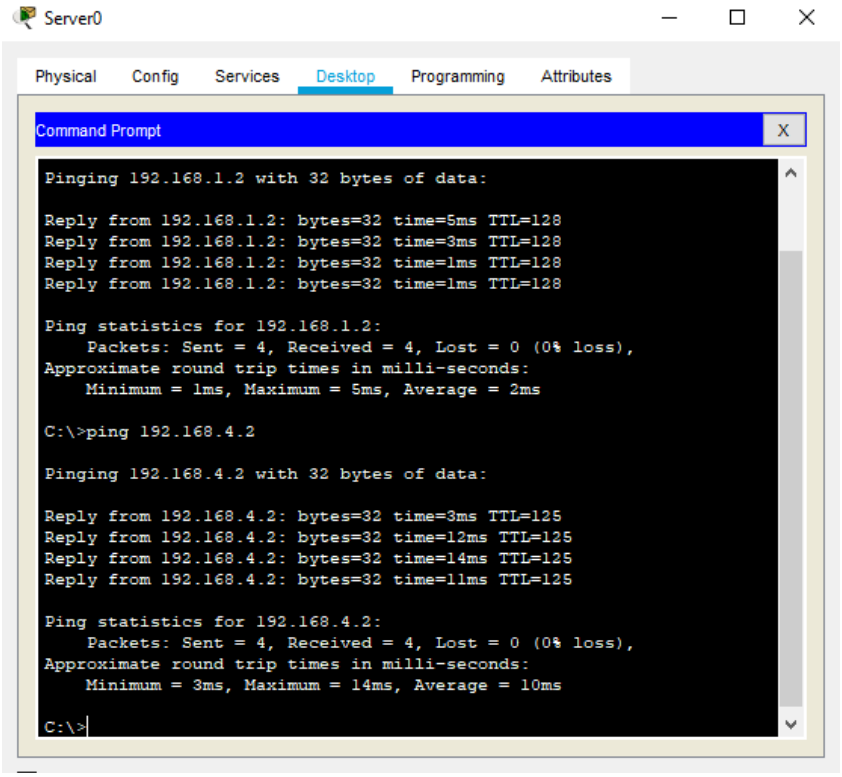
```
Router(config)#
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
Router(config)#
```

Now we need to verify the above IPS configuration, we do it first by pinging PC1 to SERVER and then from SERVER to PC1

PC1 to SERVER – The ping fails



Server to PC1 – The Ping is successful



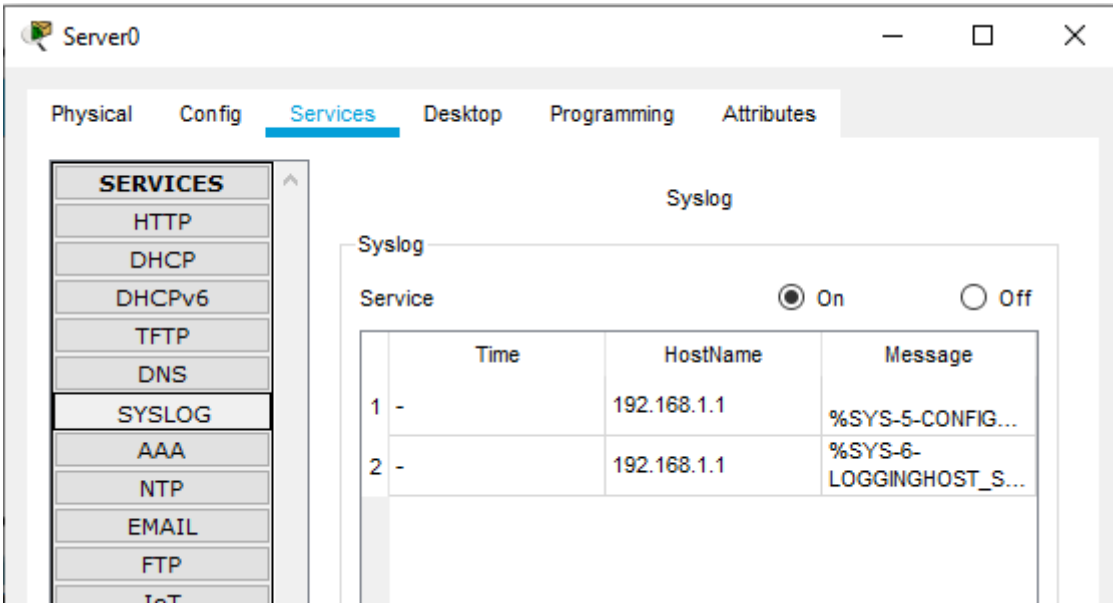
We check the Syslog service on the server to check the logging activity, by typing the following commands in Router0

```
Router>enable
Router#configure terminal
Router(config)#logging 192.168.1.2
Router(config)#
Router(config)#
Router(config)#exit
Router#

Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms

Router#
```



Hence, we set the IPS and also verified it on Router1