Practical 7

Configuring IOS Intrusion Prevention System (IPS) Using the CLI: a) Enable IOS IPS. b) Modify an IPS signature.

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:

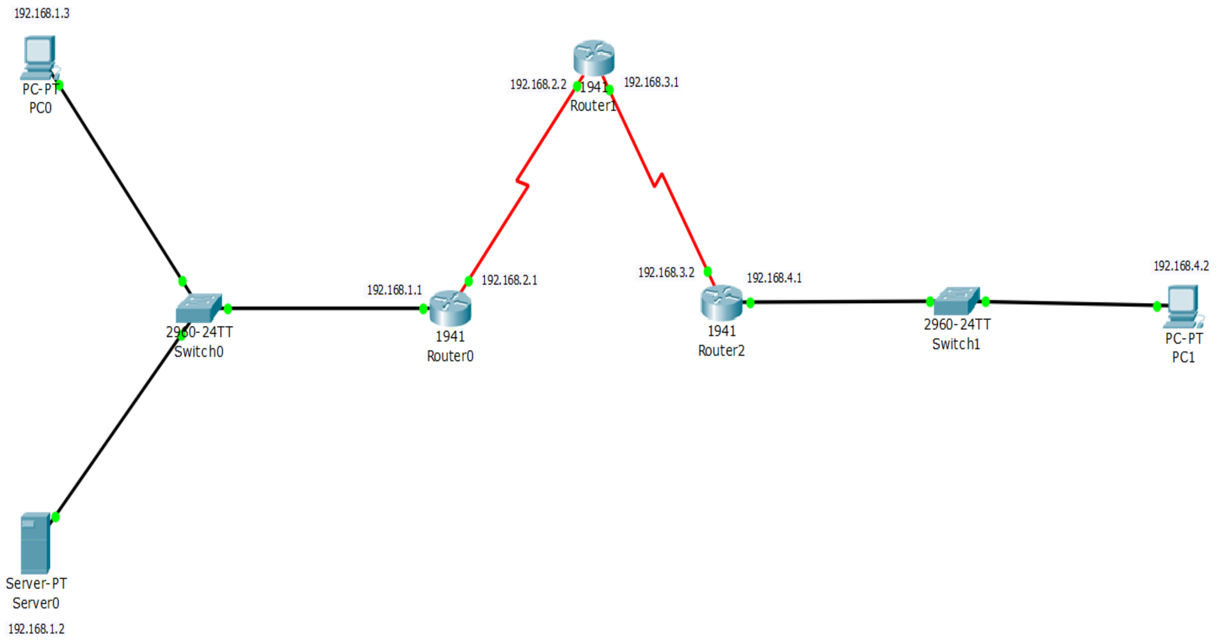
A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks. We can easily install signatures using IDS and IPS management software such as Cisco IDM. Sensors enables us to modify existing signatures and define new ones.

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 define some of the commands which will be used while configuring the Router for IPS.

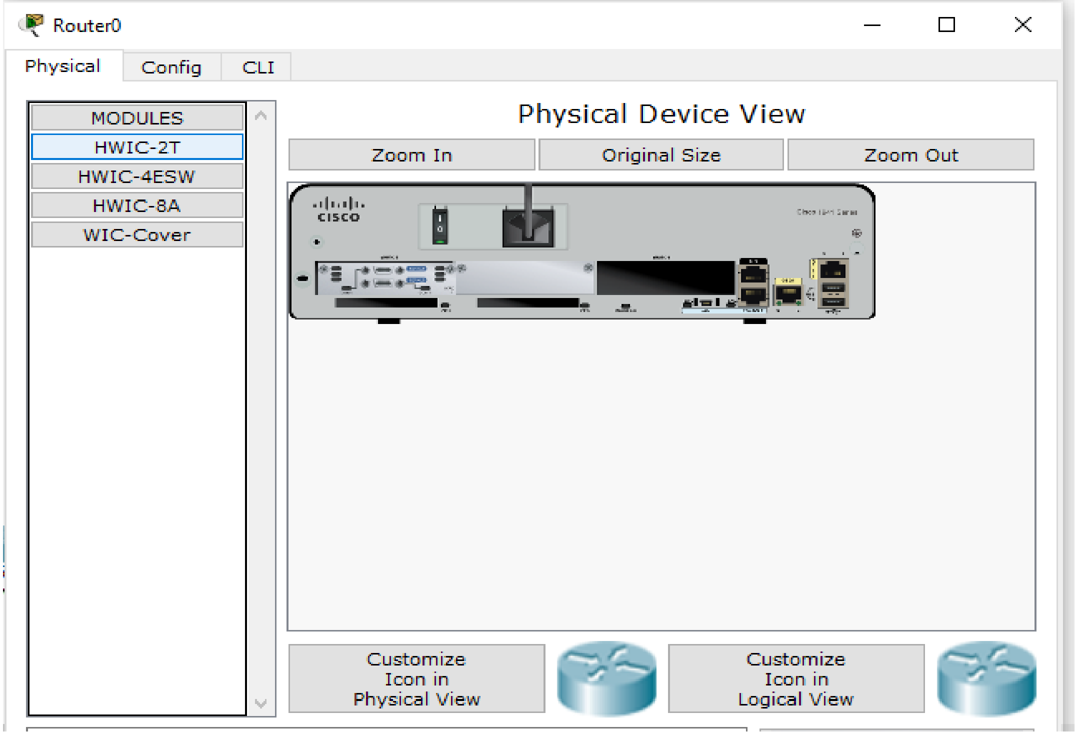
Commands	Function	Example
ip ips signature-category	Enters IPS category configuration mode.	Router(config)# ip ips signature-category
category	Specifies that all categories (and all signatures) are retired in the following step and enters IPS category action configuration mode Specifies the basic category (and a set of signatures) that are to be "unretired" in the following step.	Router(config-ips-category)# category all **Example:** Router(config-ips-category)# category ios_ips basic
retired {**true** | **false**}	Specifies that the device should retire all categories (and all signatures). **true** --Retires all signatures within a given category. **false** --"Unretires" all signatures within a given category.	Router(config-ips-category-action)# retired true
mkdir flash:/ips5	Create a directory for which Cisco IOS IPS saves signature information.	**Example:** Device# mkdir flash:/ips5
ip ips name *ips-name*		**Example:** Device(config)# ip ips name myips
ip ips *ips-name* {**in** | **out**}	Applies an IPS rule at an interface and automatically loads the signatures and builds the signature engines.	**Example:** Device(config-if)# ip ips MYIPS in

Consider the following topology

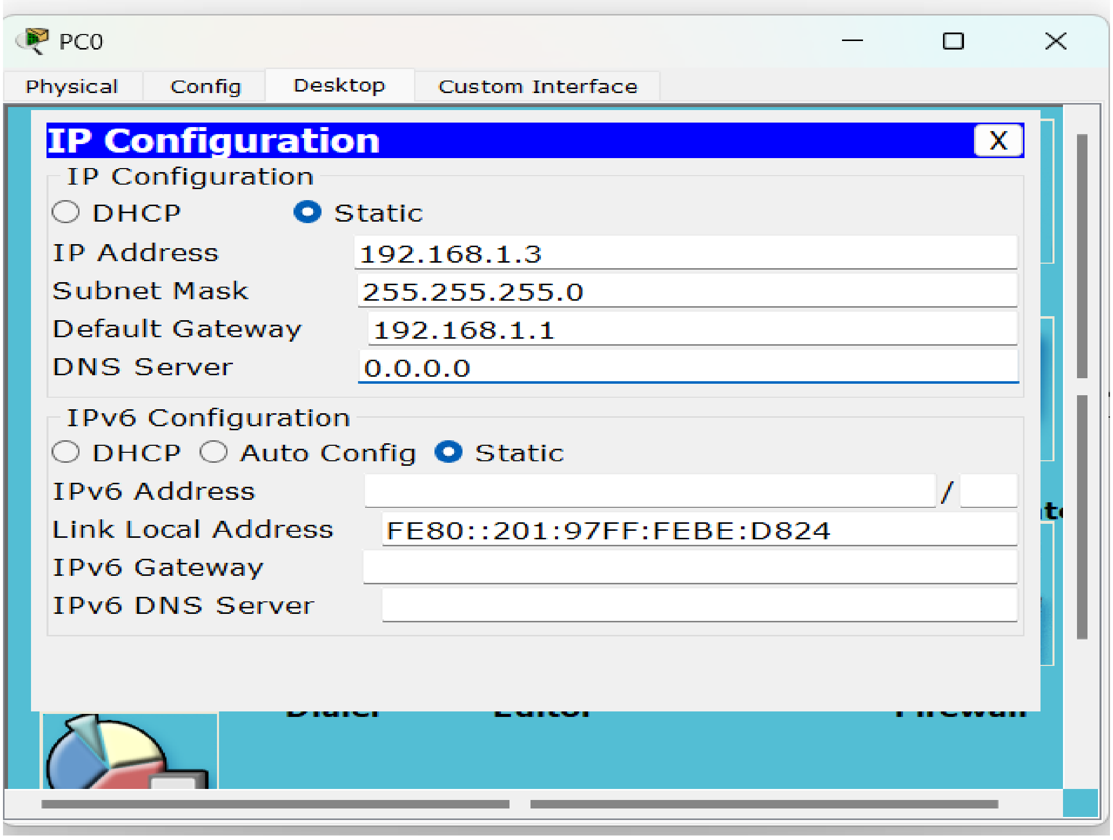


Topology Configuration

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



Configuring PC0



IP Configuration

○ DHCP ● Static

IP Address 192.168.1.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

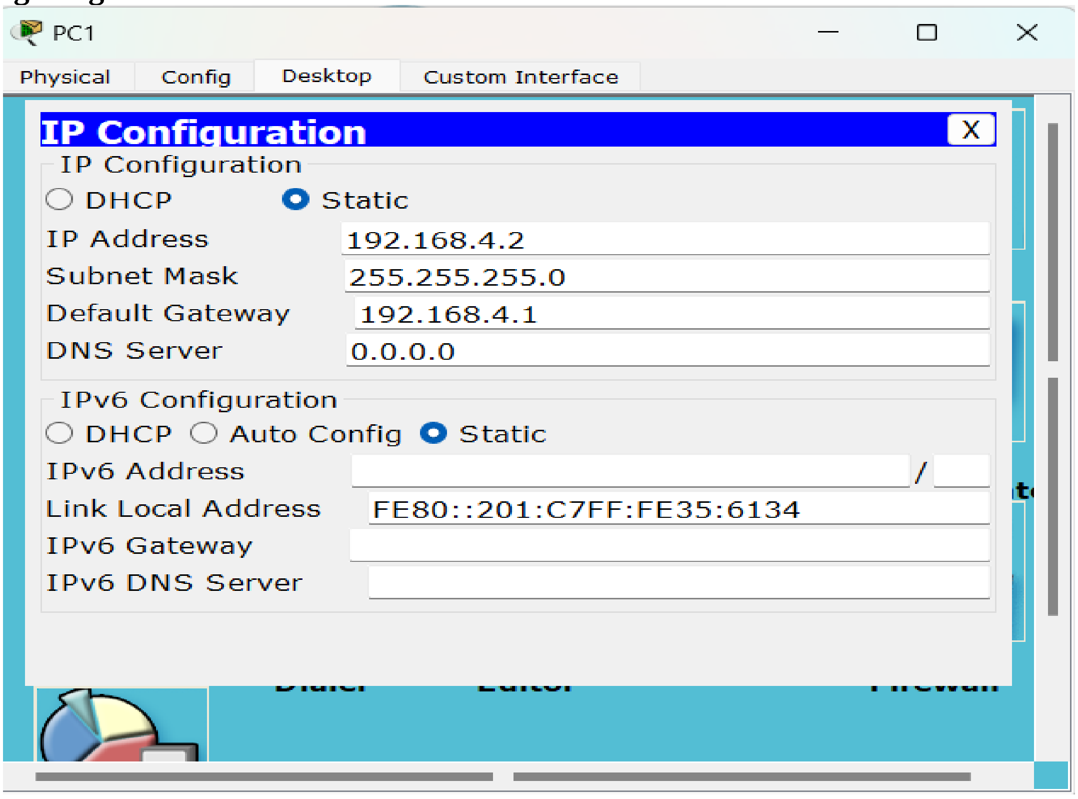
IPv6 Address /

Link Local Address FE80::201:97FF:FEBE:D824

IPv6 Gateway

IPv6 DNS Server

Configuring PC1



IP Configuration

○ DHCP ● 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

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

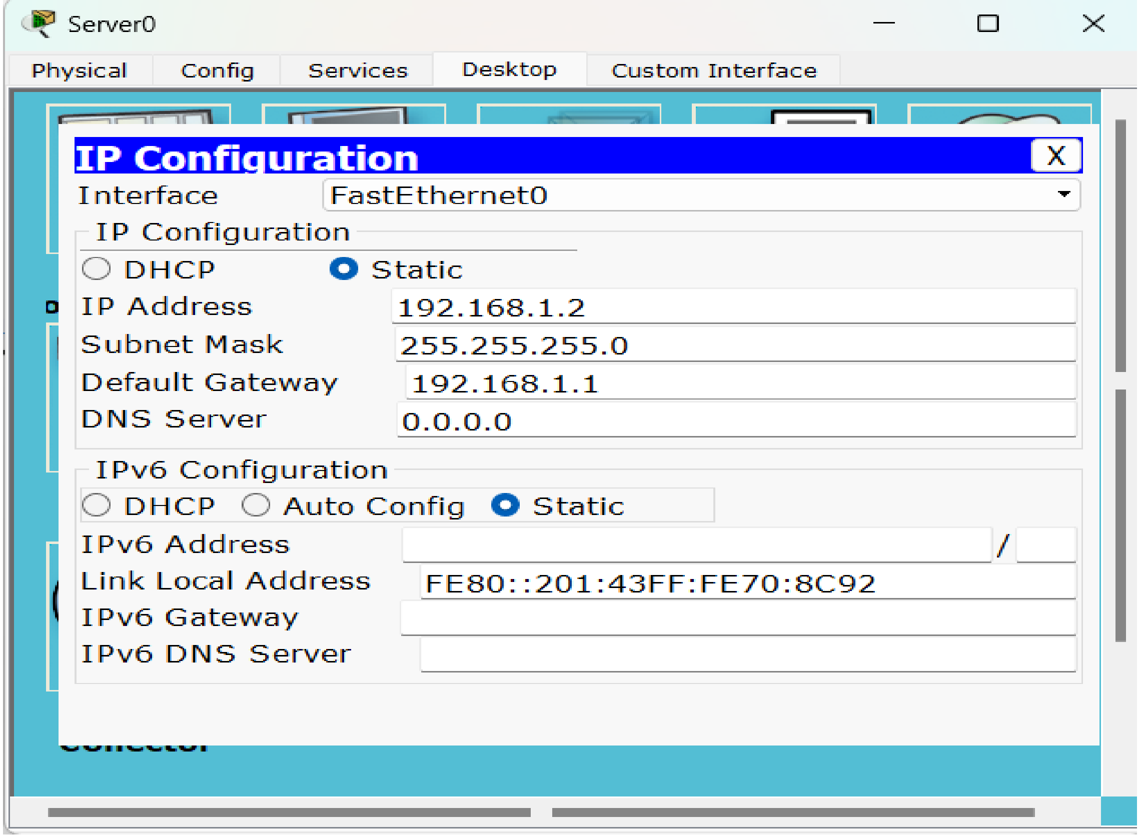
IPv6 Address /

Link Local Address FE80::201:C7FF:FE35:6134

IPv6 Gateway

IPv6 DNS Server

Configuring Server0



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● 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

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

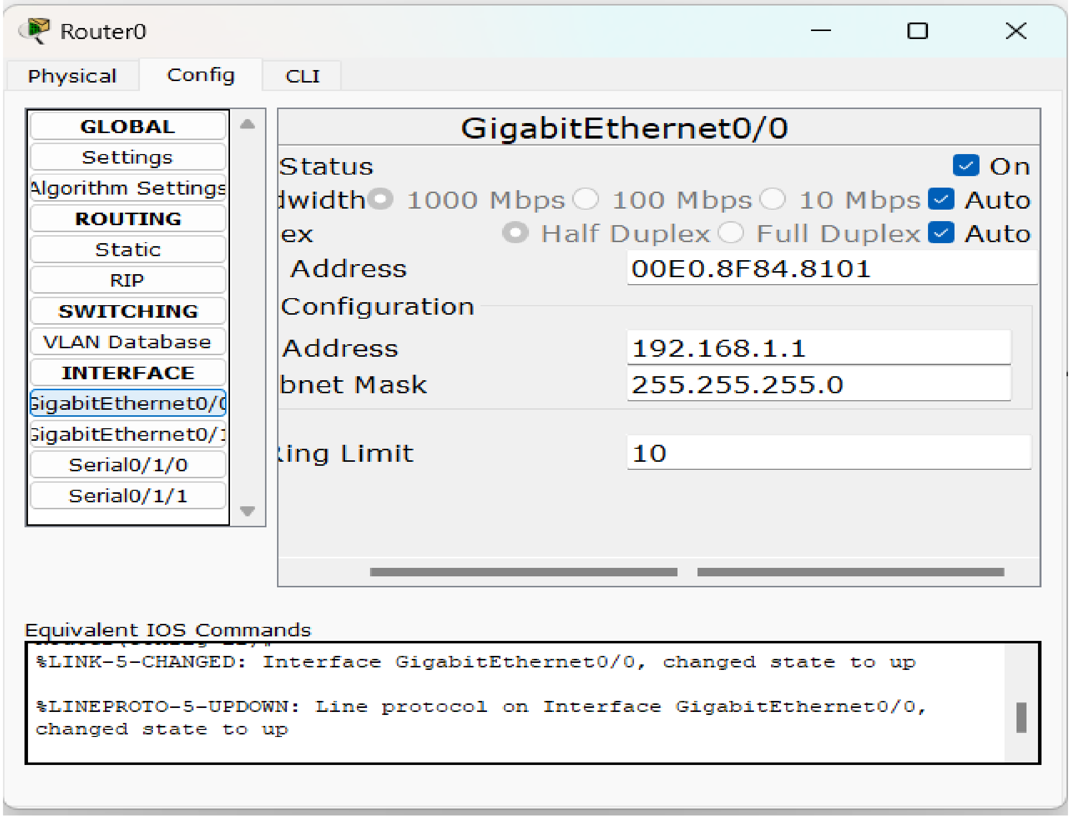
IPv6 Address: /

Link Local Address: FE80::201:43FF:FE70:8C92

IPv6 Gateway:

IPv6 DNS Server:

Configuring Router0



GigabitEthernet0/0

Status ☑ On

dwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

ex ○ Half Duplex ○ Full Duplex ☑ Auto

Address: 00E0.8F84.8101

Configuration

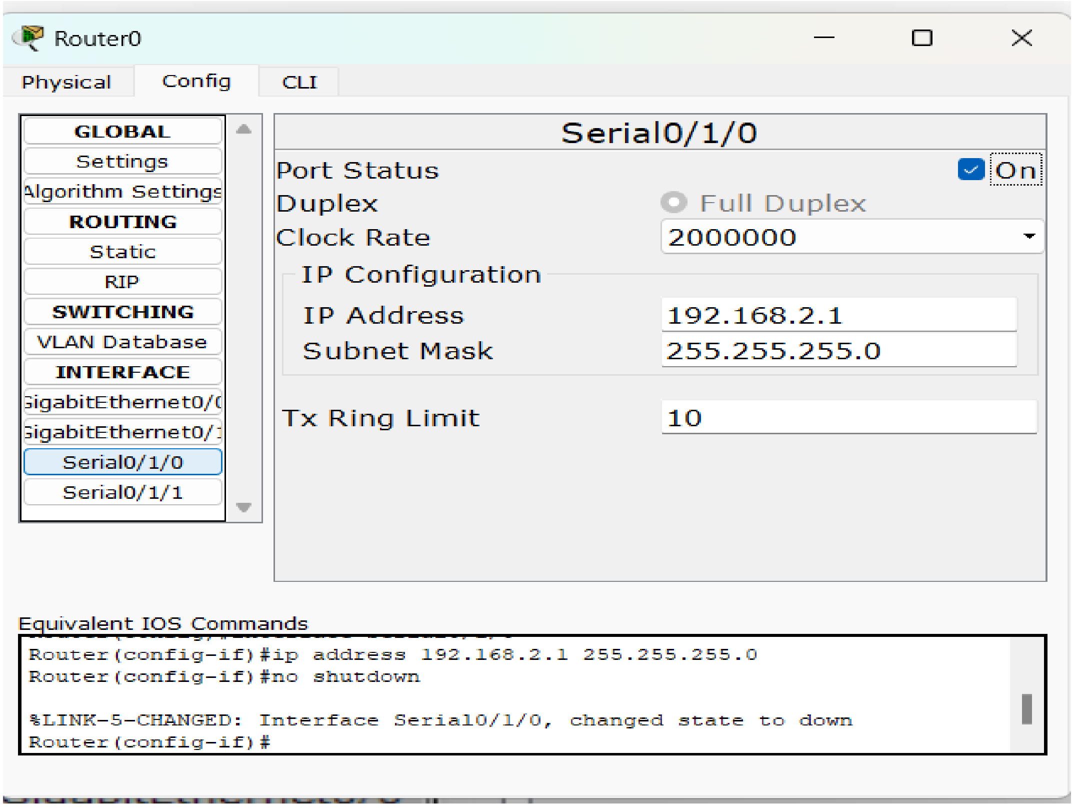
Address: 192.168.1.1

bnet Mask: 255.255.255.0

ing Limit: 10

Equivalent IOS Commands

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```



Serial0/1/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

IP Configuration

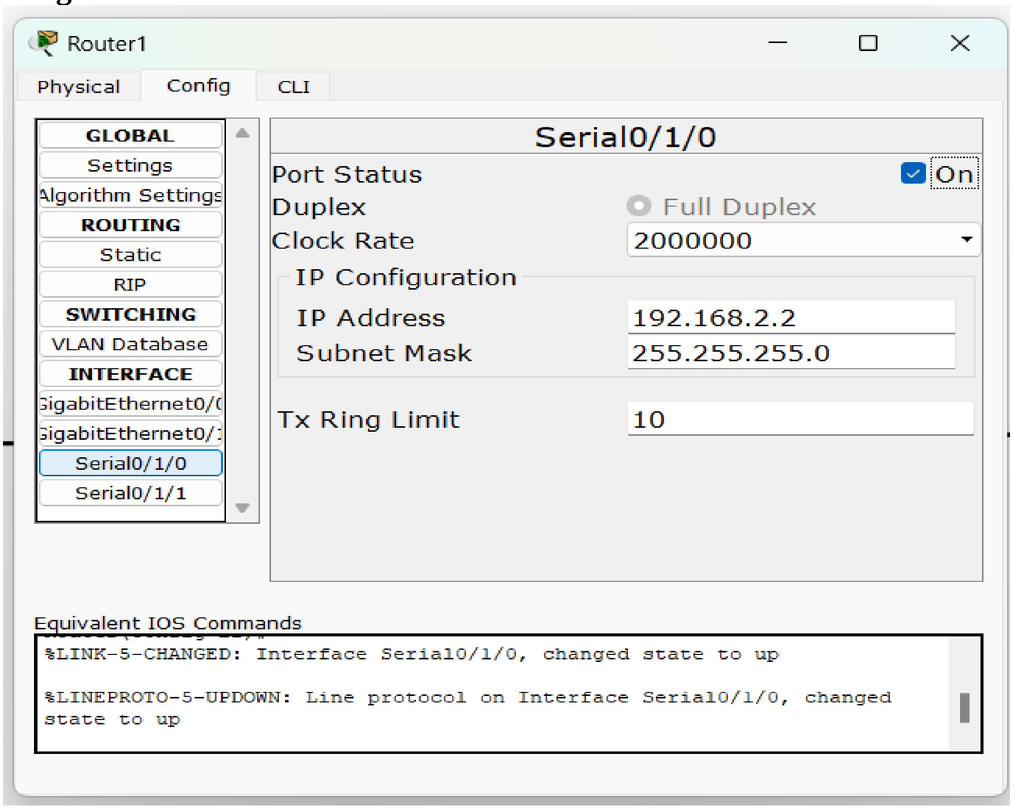
IP Address 192.168.2.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

```
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#
```

Configuring Router1



Serial0/1/0

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

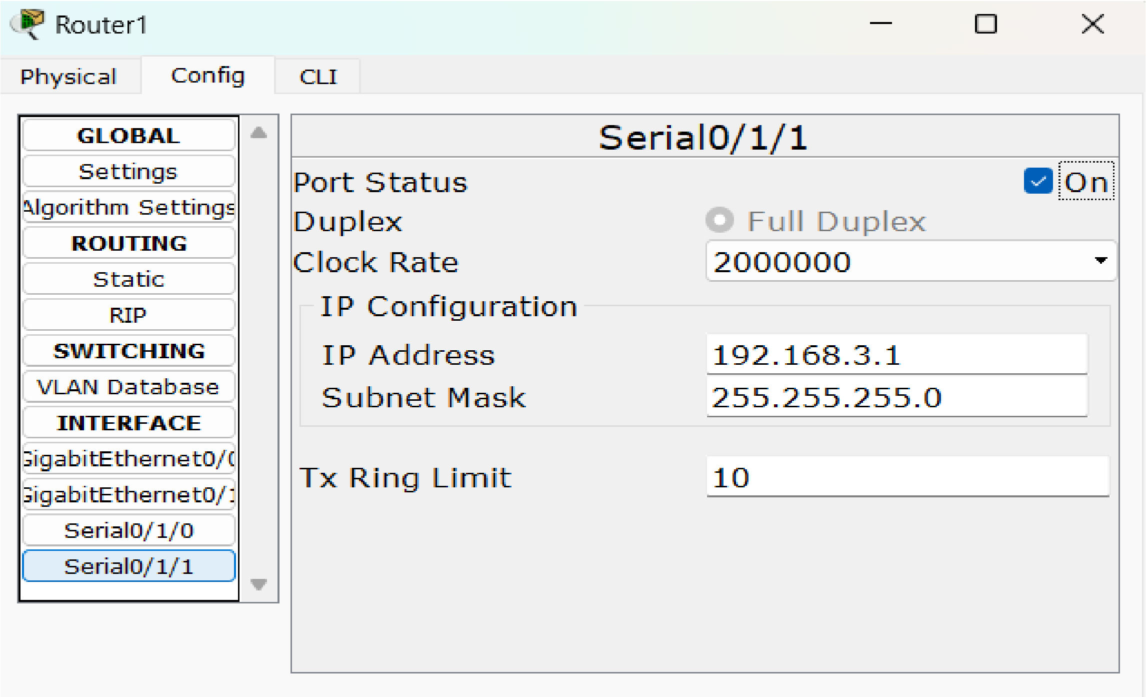
IP Configuration

IP Address 192.168.2.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up
```



Router1

Serial0/1/1

Port Status ☑ On

Duplex ○ Full Duplex

Clock Rate 2000000

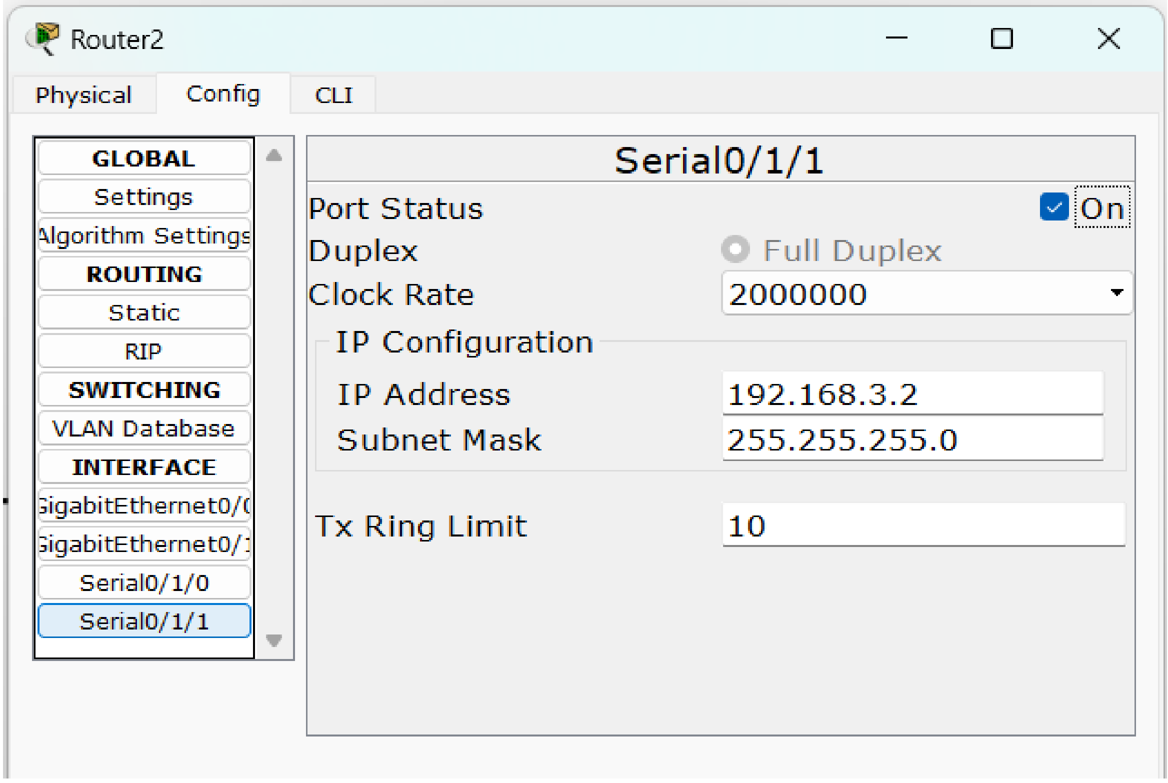
IP Configuration

IP Address 192.168.3.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Configuring Router2



Router2

Serial0/1/1

Port Status ☑ On

Duplex ○ Full Duplex

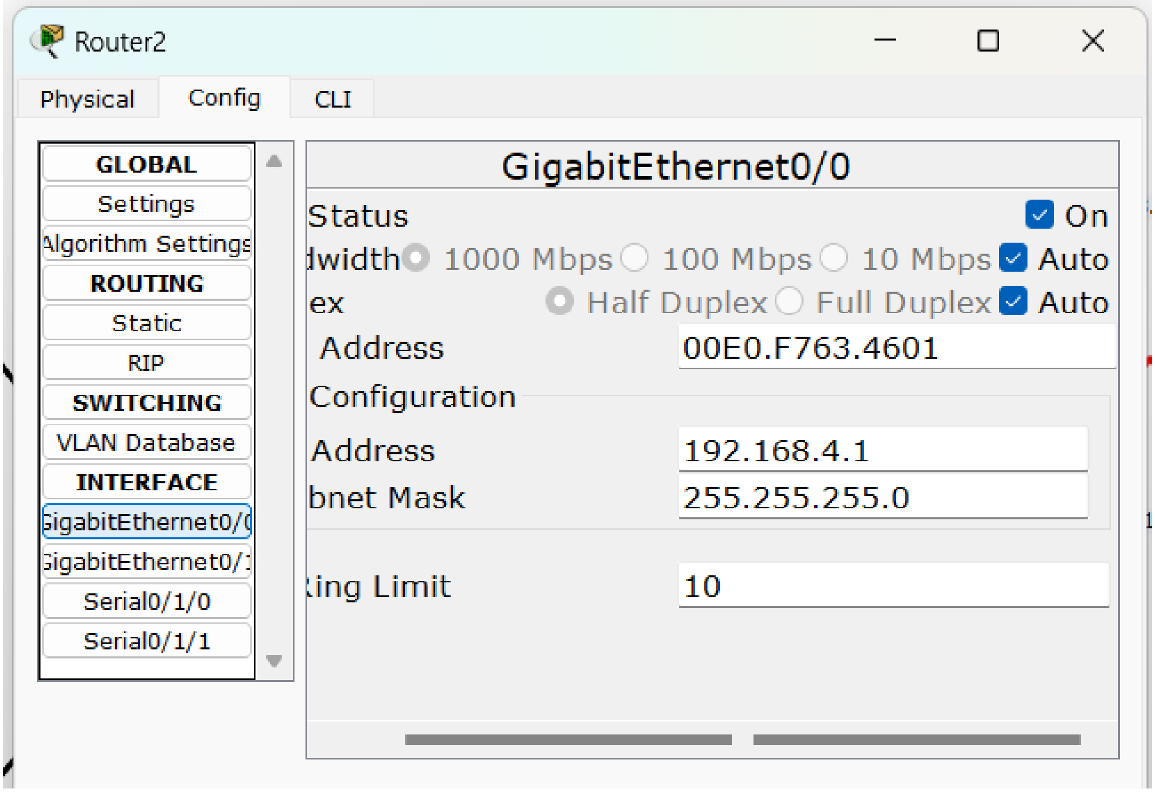
Clock Rate 2000000

IP Configuration

IP Address 192.168.3.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10



GigabitEthernet0/0

Status ☑ On

dwidth ○ 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

ex ○ Half Duplex ○ Full Duplex ☑ Auto

Address 00E0.F763.4601

Configuration

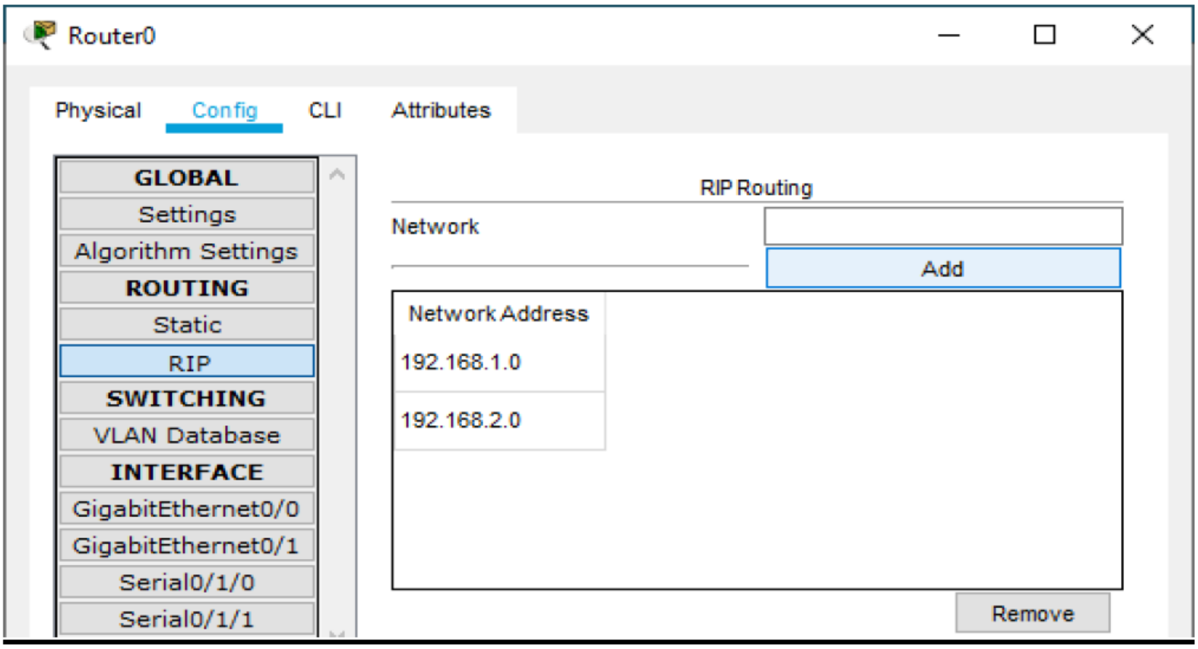
Address 192.168.4.1

bnet Mask 255.255.255.0

ing Limit 10

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)

Router0

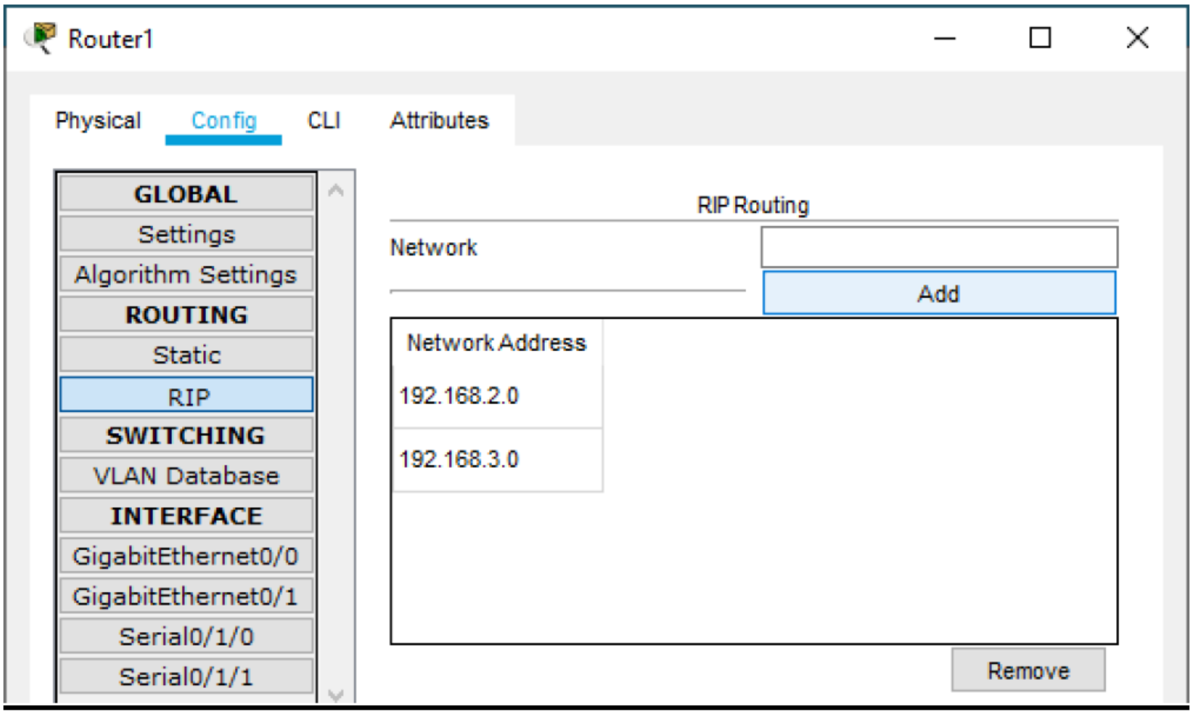


RIP Routing

Network

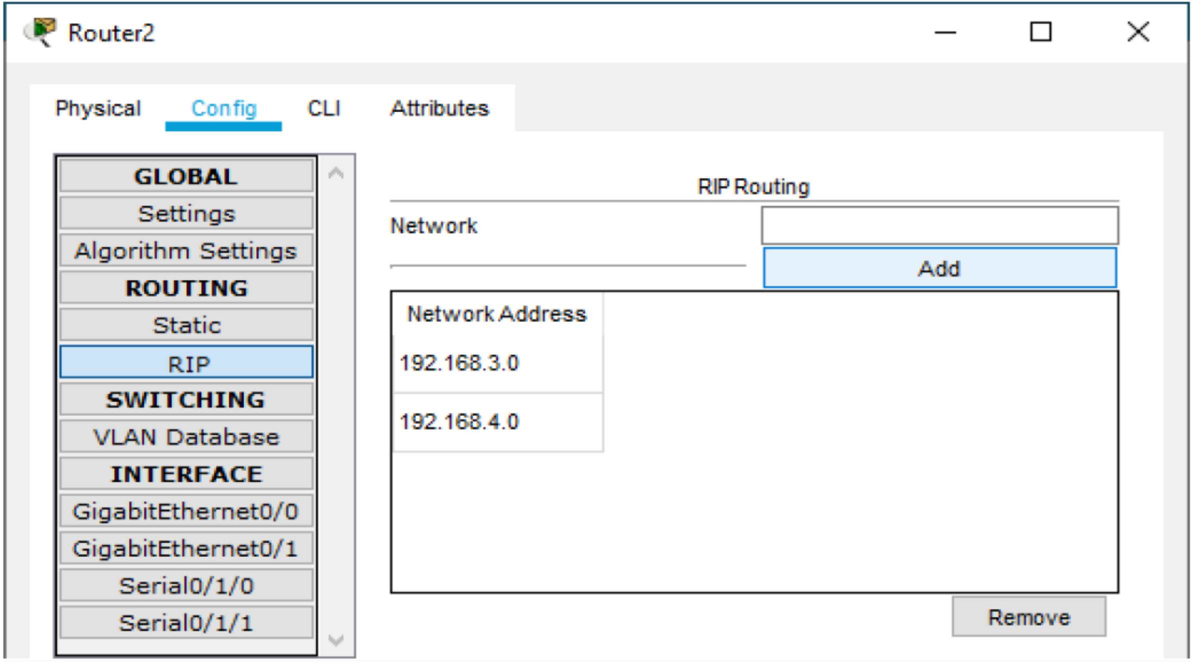
Network Address
192.168.1.0
192.168.2.0

Router1



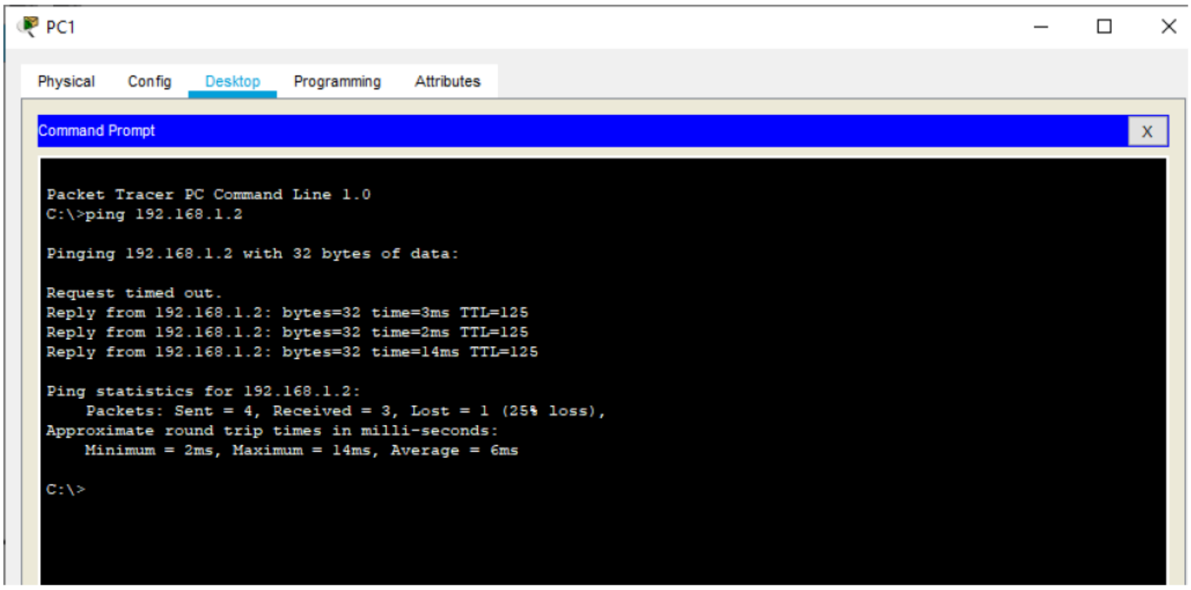
Network Address
192.168.2.0
192.168.3.0

Router2



Network Address
192.168.3.0
192.168.4.0

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

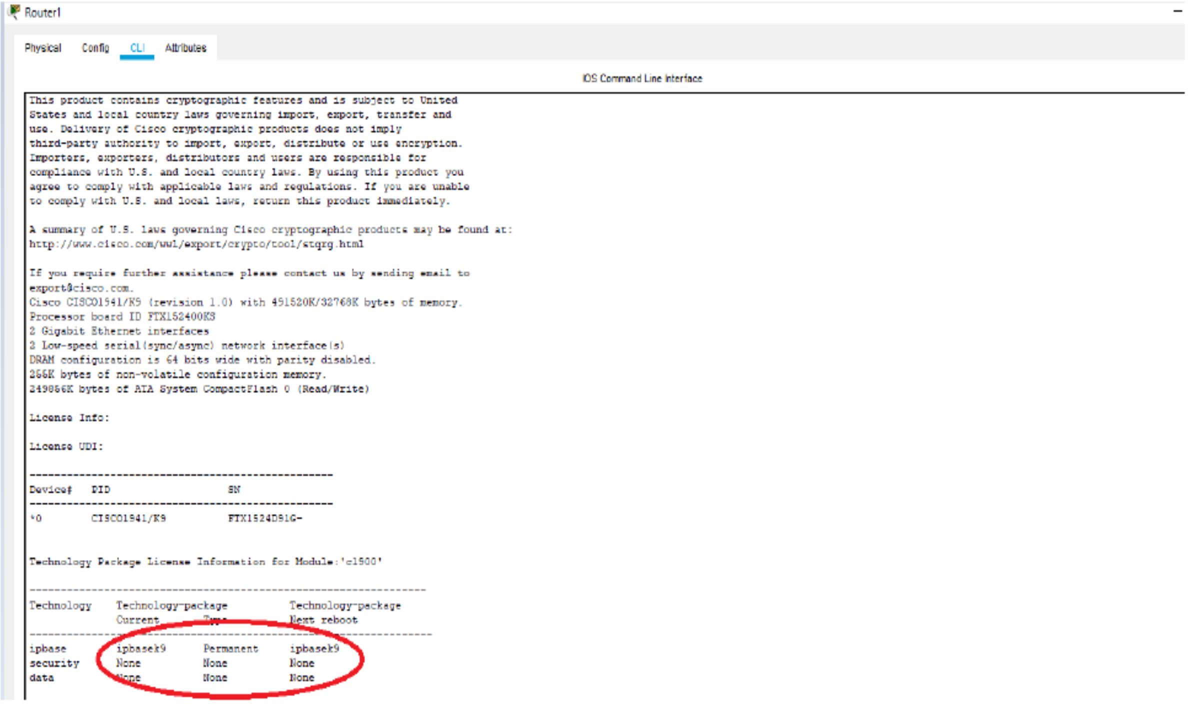


```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=3ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms 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 = 2ms, Maximum = 14ms, Average = 6ms

C:\>
```

So, we conclude that the connectivity has been established

Part 1: 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

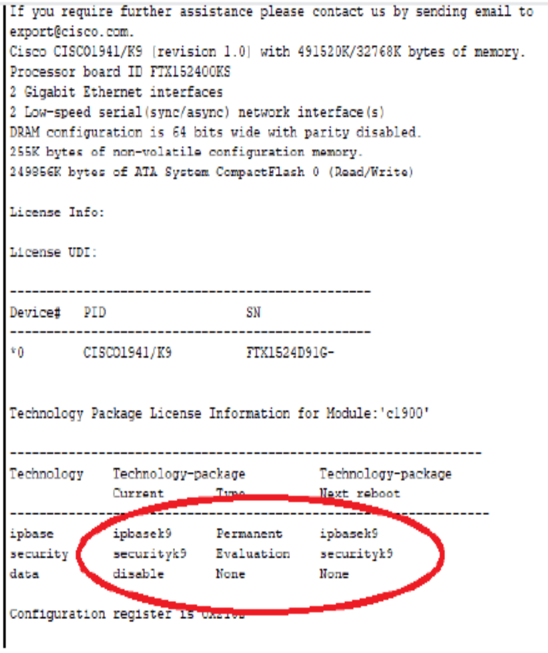


```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524D81G-


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
```

As seen above the security package is not enabled, to enable the security feature, type the following command in 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#show version
```

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



```
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524D91G-


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

Configuration register is 0x2102
```

As seen above now the security package has been enabled

Now, type the following commands in the CLI mode of Router1

```
Router>en
Router#mkdir dalmia
Create directory filename [dalmia]?
Created dir flash:dalmia
Router#conf t
Router(config)#ip ips config location flash:dalmia
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]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

Router(config)#int Se0/1/0
Router(config-if)#ip ips iosips out

Router(config-if)#exit
Router(config)#exit
Router#
```

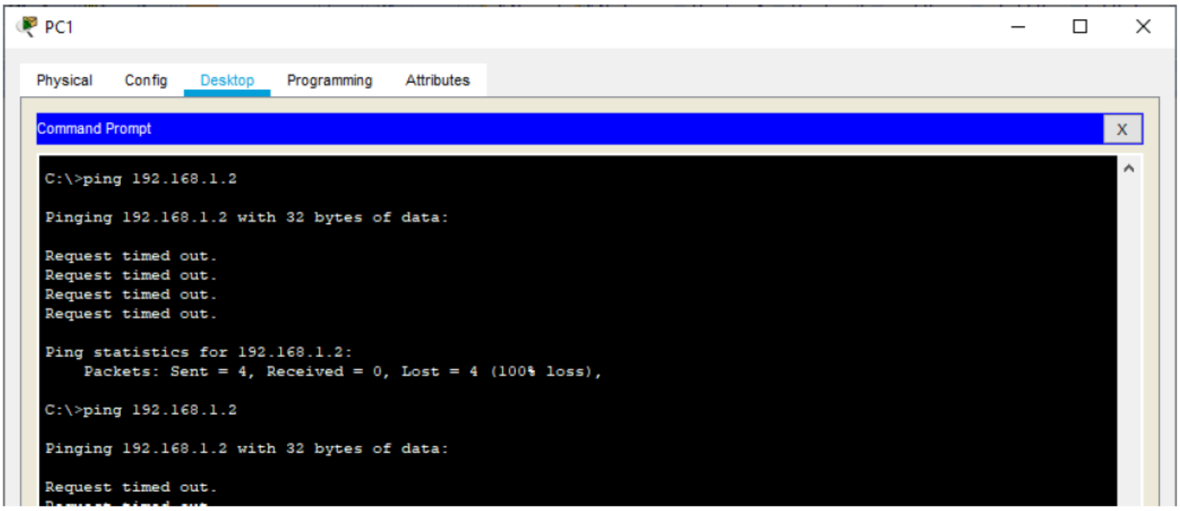
Part 2: Modify the Signature

Type the following commands in the CLI mode of Router1

```
Router#conf t
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] <Enter>
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

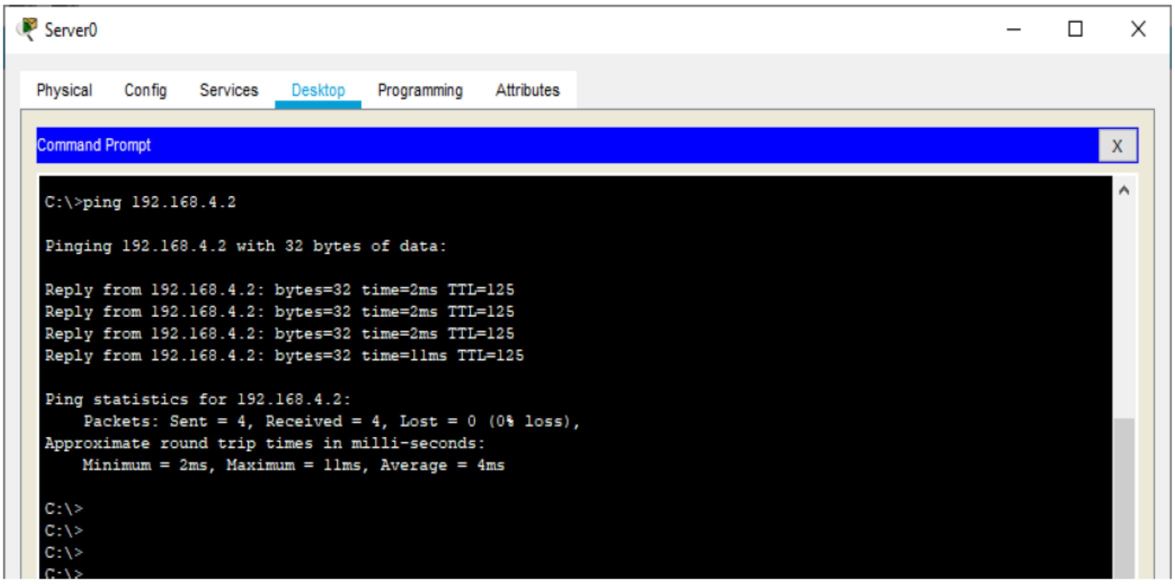
PC1 to SERVER



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
```

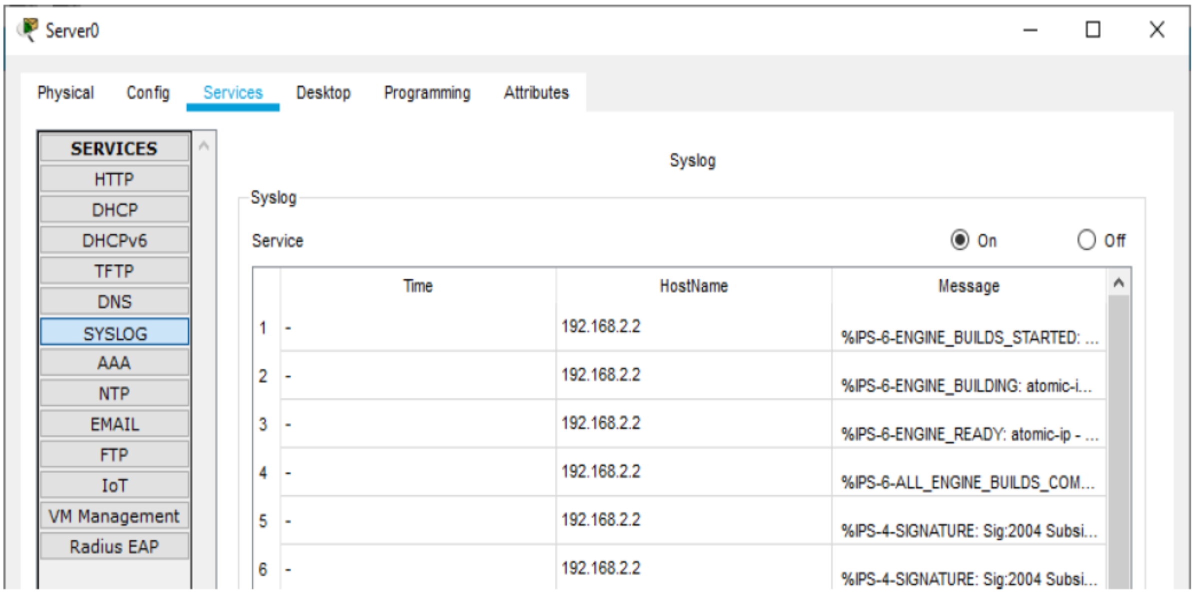
The ping FAILS

SERVER to PC1



```
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\>
C:\>
C:\>
C:\>
```

Also, we can observe the Syslog service in the SERVER to check the log activities



Service ● On ○ Off

	Time	HostName	Message
1	-	192.168.2.2	%IPS-6-ENGINE_BUILDS_STARTED: ...
2	-	192.168.2.2	%IPS-6-ENGINE_BUILDING: atomic-i...
3	-	192.168.2.2	%IPS-6-ENGINE_READY: atomic-ip - ...
4	-	192.168.2.2	%IPS-6-ALL_ENGINE_BUILDS_COM...
5	-	192.168.2.2	%IPS-4-SIGNATURE: Sig:2004 Subsi...
6	-	192.168.2.2	%IPS-4-SIGNATURE: Sig:2004 Subsi...

Use show commands to verify IPS on Router1

```
Router#show ip ips all
```

Hence we set the IPS and also verified it on Router1

****