PRACTICAL NO 6

Aim:- IP Security (IPsec) Configuration: Configure IPsec on network devices to provide secure communication and protect against unauthorized access and attacks.

Steps to be followed:

Download Cisco Packet Tracer

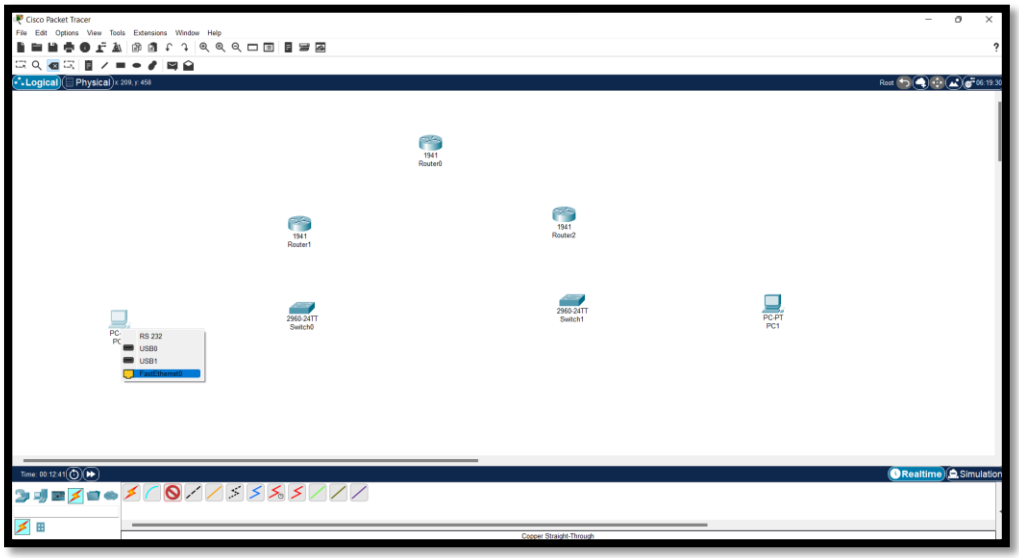
Requirements:

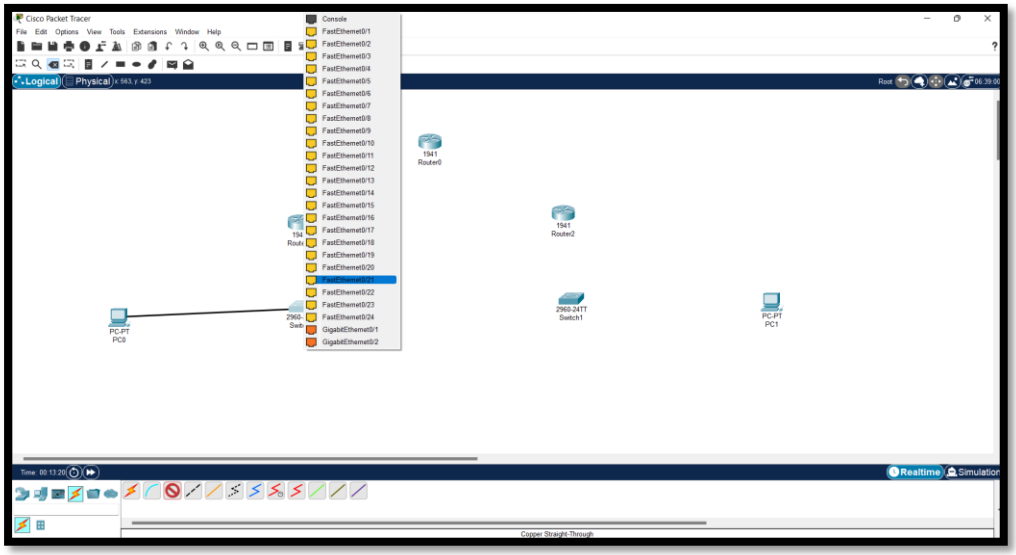
- Take 3 Routers (1941)
- Take 2 Switches (2960)
- Take 2 PC
- Configuration:

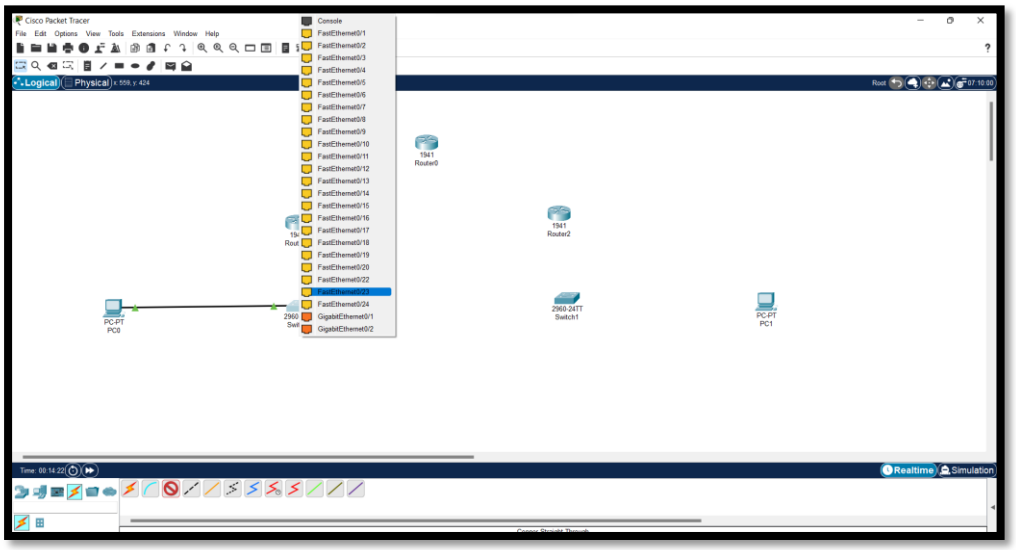
  PC 0 – 192.168.1.2
  PC 1 – 192.168.2.2
  Router 1 (G 0/0) - 20.0.0.1
  Router 1 (G 0/1) - 192.168.1.1
  Router 0 (G 0/0) - 30.0.0.2
  Router 0 (G 0/1) - 20.0.0.2
  Router 2 (G 0/0) - 30.0.0.1
  Router 2 (G 0/1) - 192.168.2.1

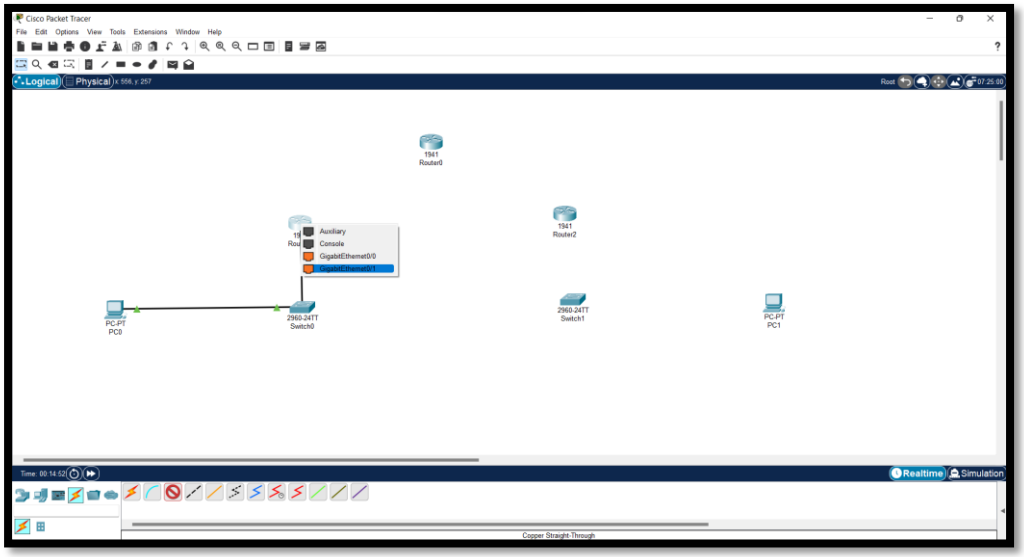
Step 1: Implementing the Topology using Cisco Packet Tracer, configure the IP address and set the IP route.

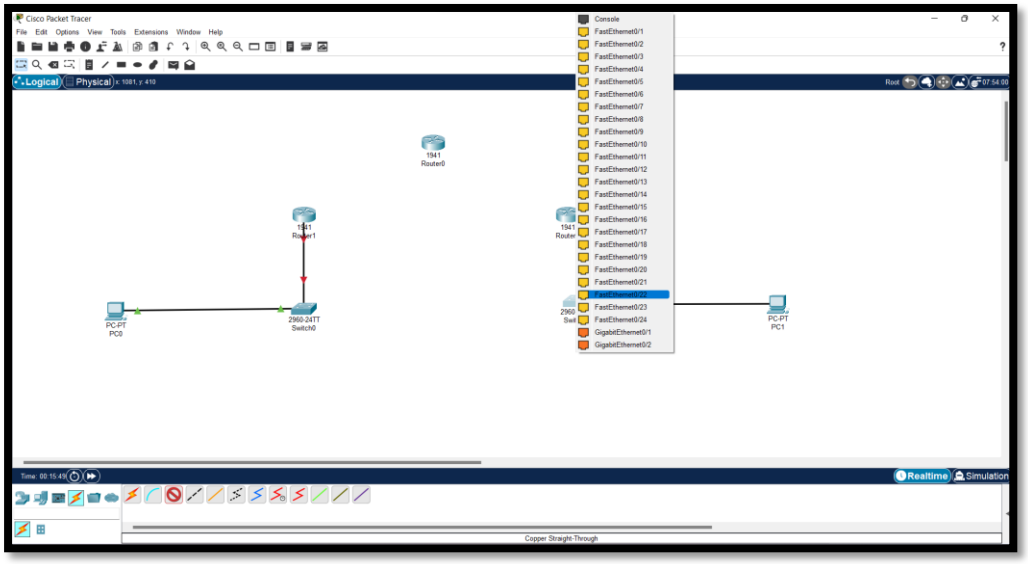
- Connect the PC with Switches and also connect switches with Router using copper straight wire as given below.

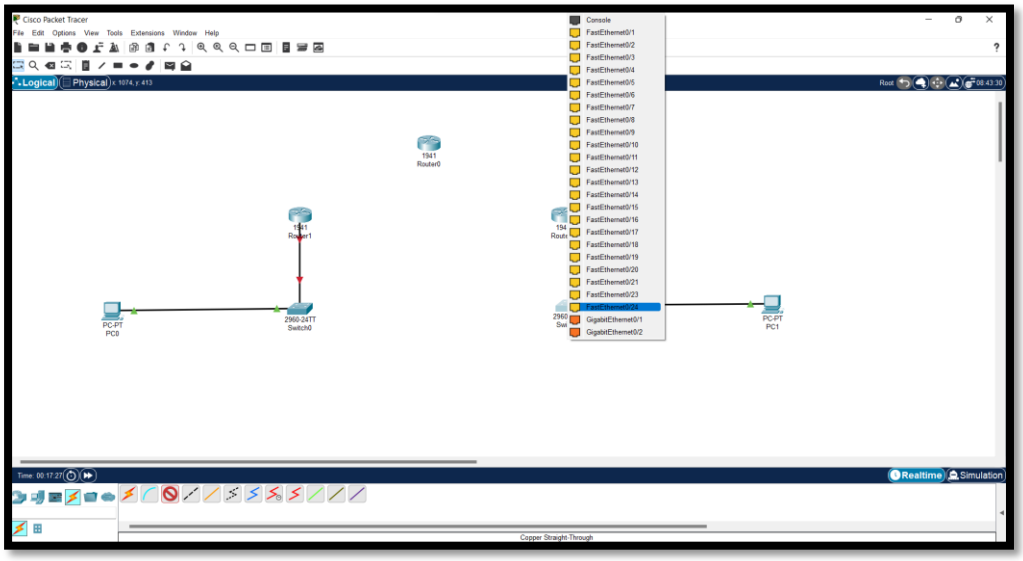



Cisco Packet Tracer
Logical
Physical
1941
Router0
1941
Router2
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
Realtime
Simulation
Copper Straight-Through

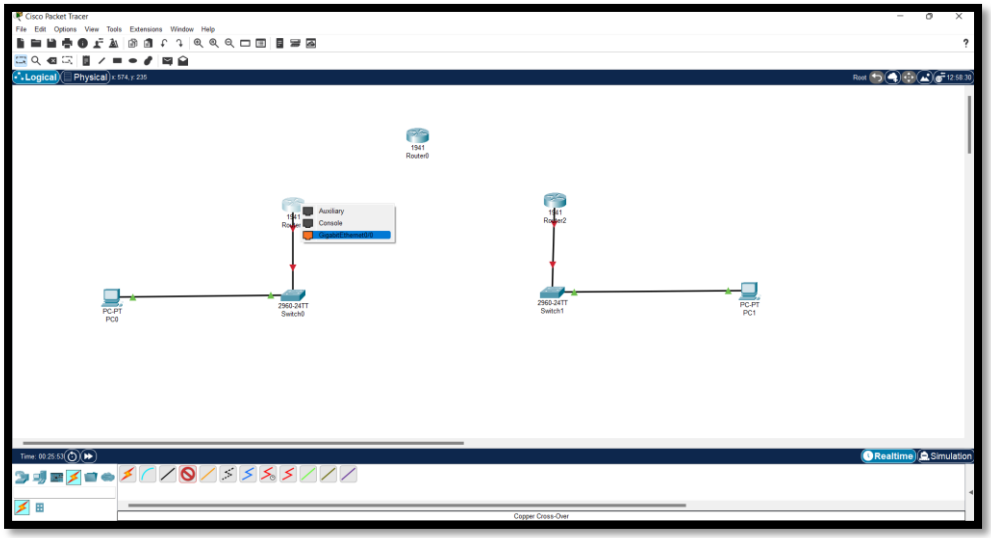

Cisco Packet Tracer
Logical
Physical
1941
Router0
1941
Router2
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
Realtime
Simulation

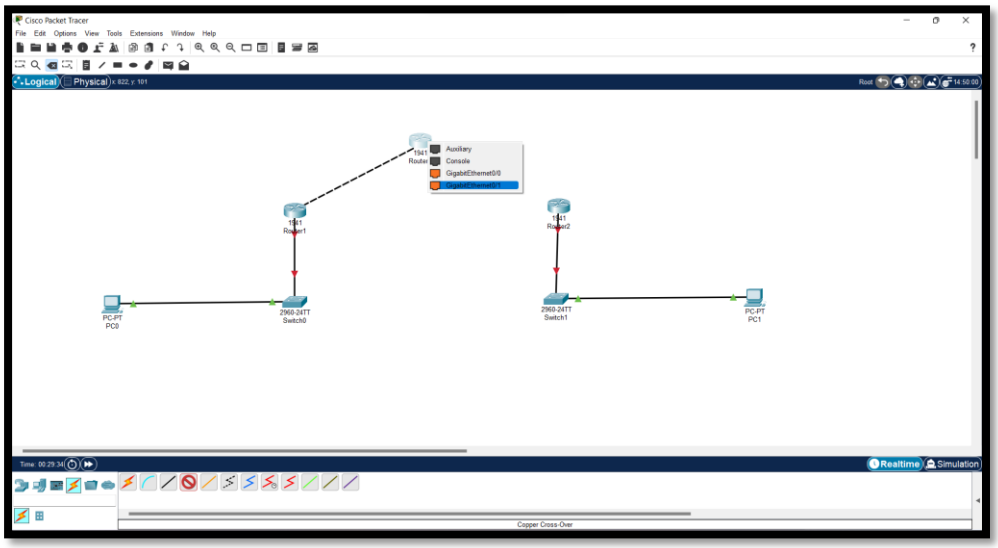

Cisco Packet Tracer
Logical
Physical
1941
Router0
1941
Router2
Auxiliary
Console
GigabitEthernet0/0
2960-24TT
Switch0
2960-24TT
Switch1
PC-PT
PC0
PC-PT
PC1
Realtime
Simulation
Copper Straight-Through

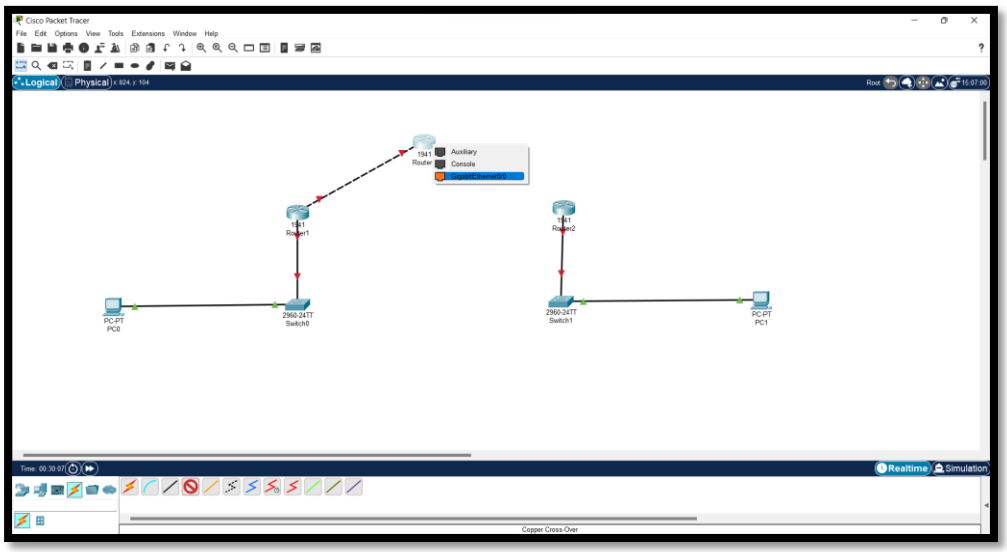


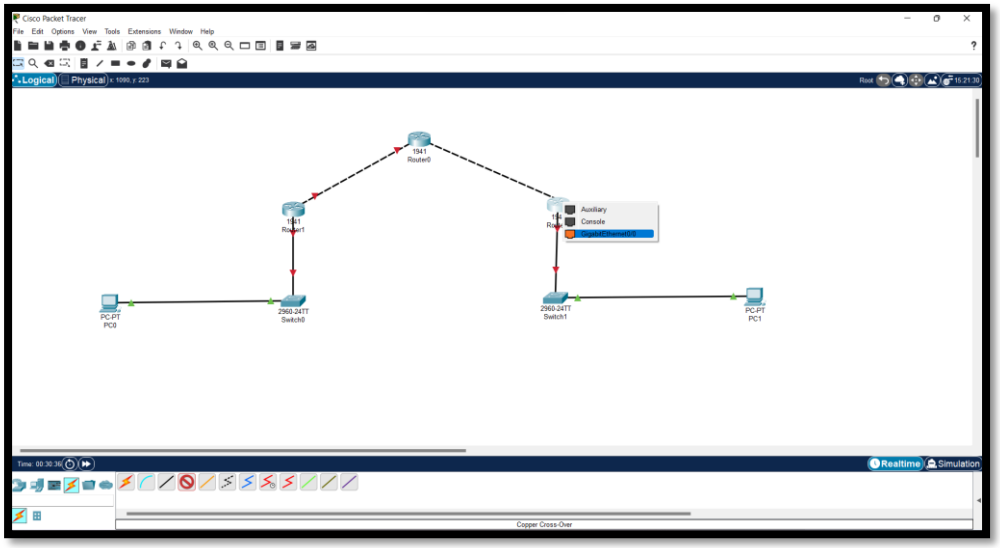


- Connect the Router 1 with Router 0 and Router 0 with Router 2 using copper cross wire as given below.

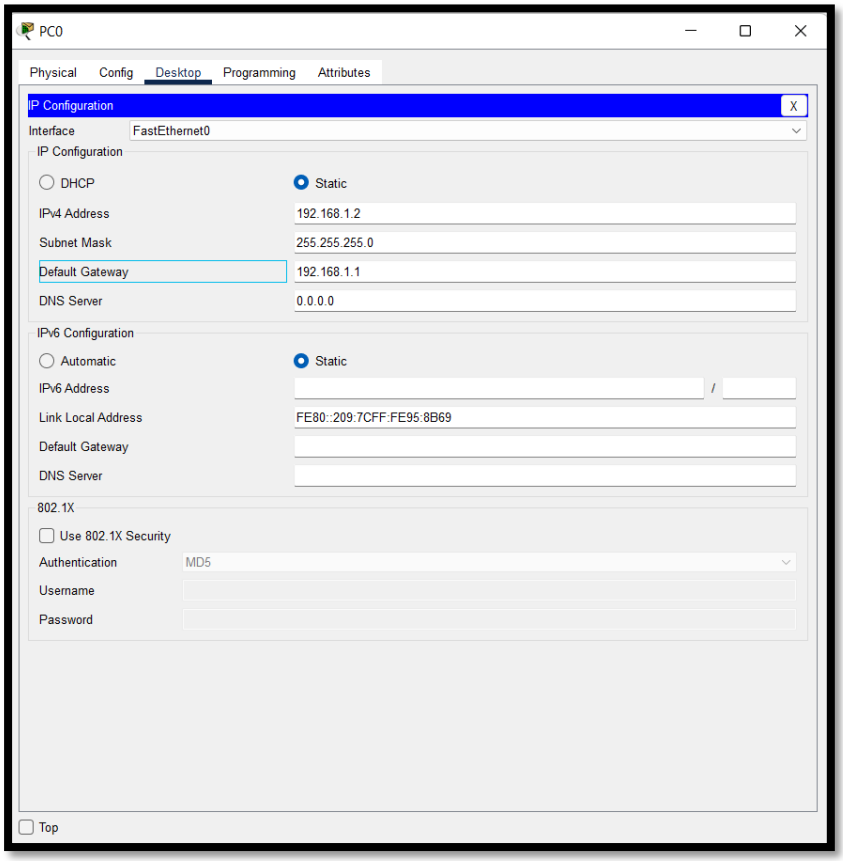

Cisco Packet Tracer
Logical
Physical
Auxiliary
Console
Realtime
Simulation
Copper Cross-Over

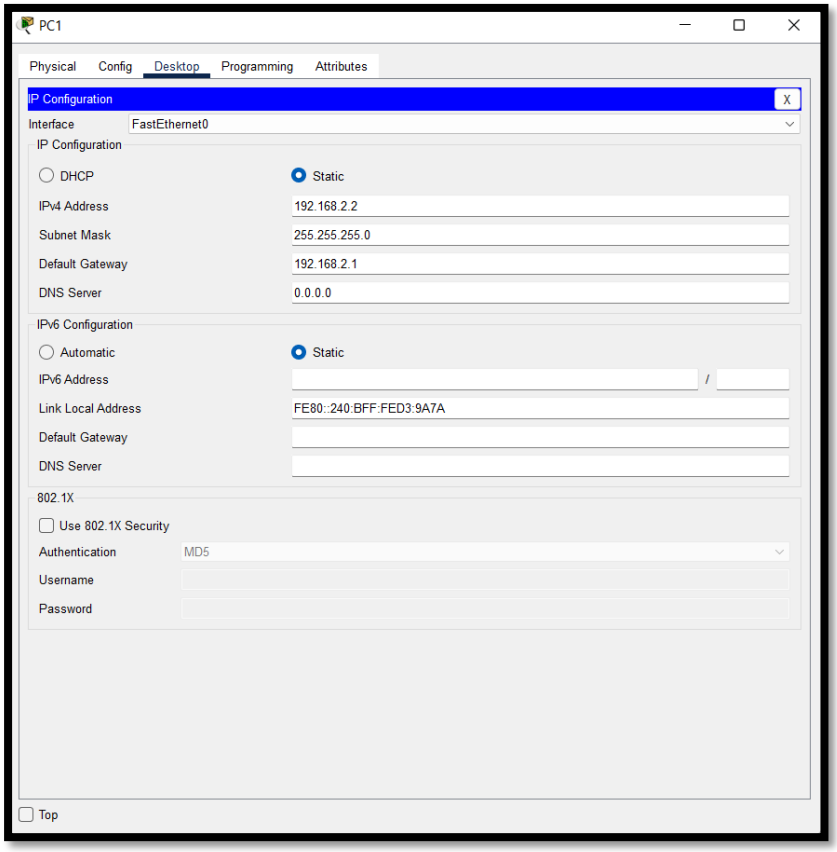

Cisco Packet Tracer
Logical
Physical
Auxiliary
Console
Realtime
Simulation
Copper Cross-Over


Cisco Packet Tracer
Logical
Physical
Auxiliary
Console
Realtime
Simulation
Copper Cross-Over

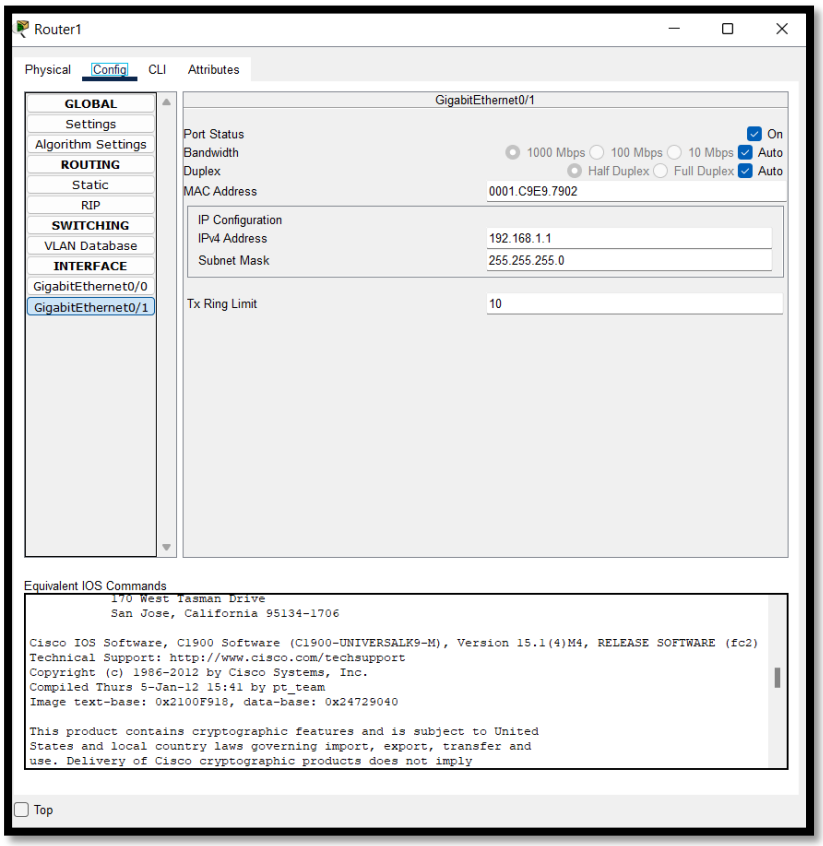


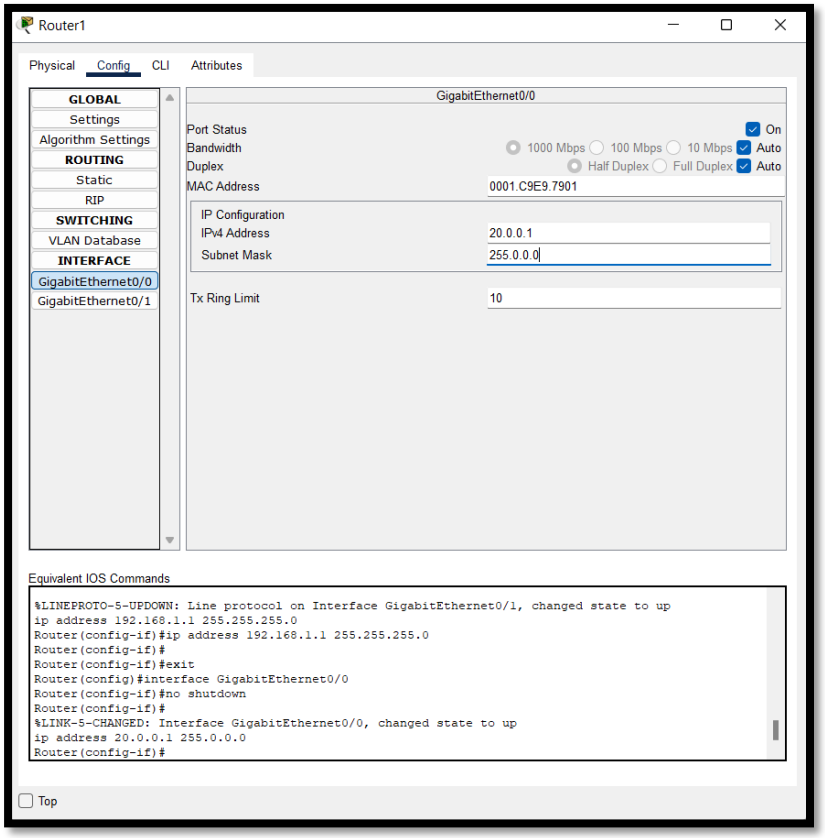
- Provide the IP address to PC 0 and PC 1

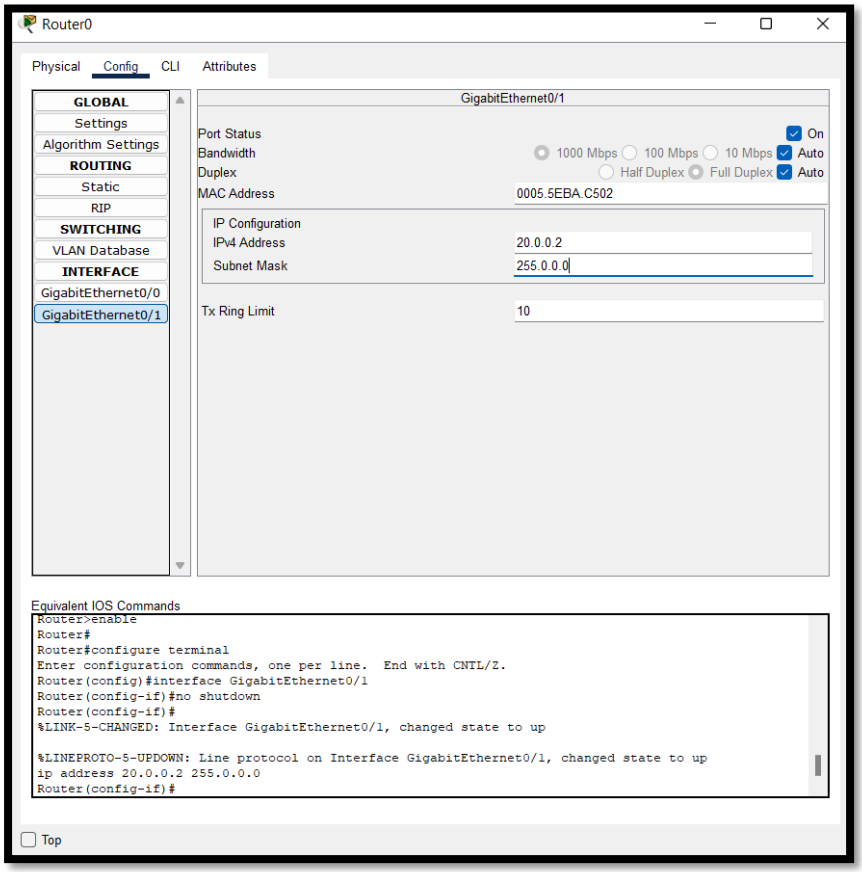


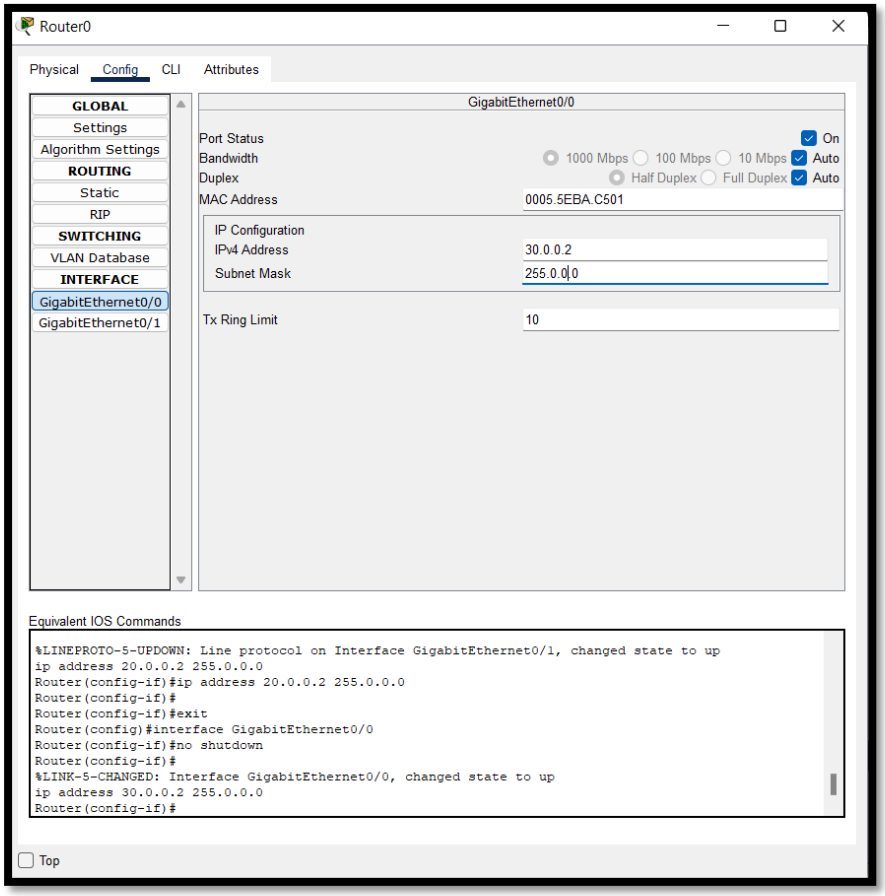


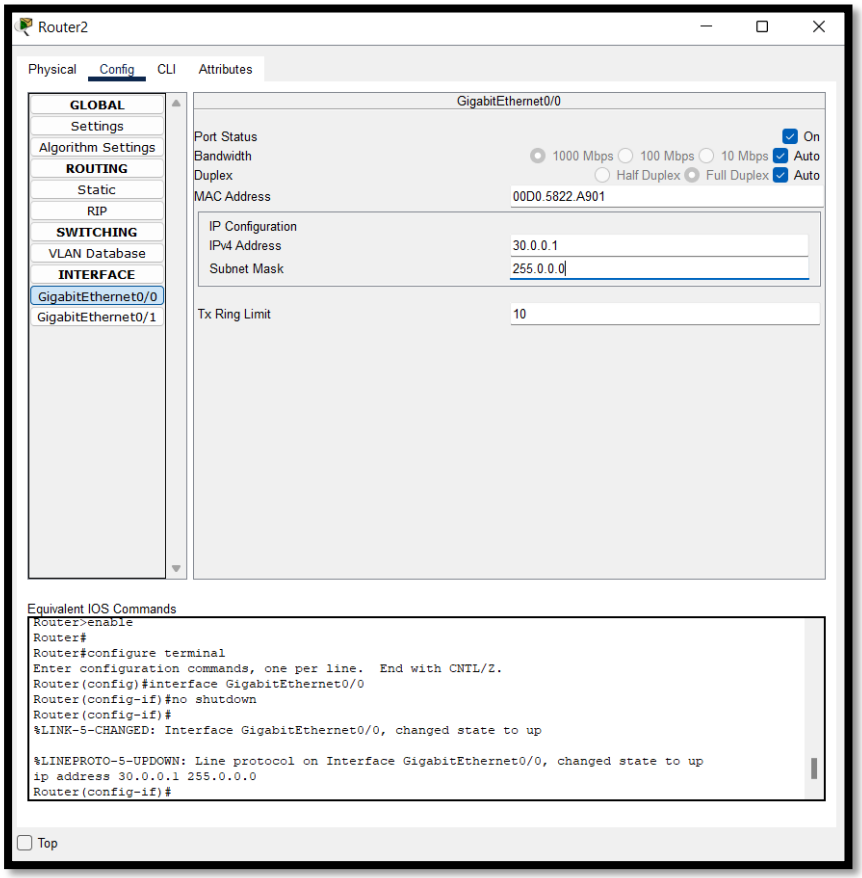
- Provide the IP Configuration to the Routers.

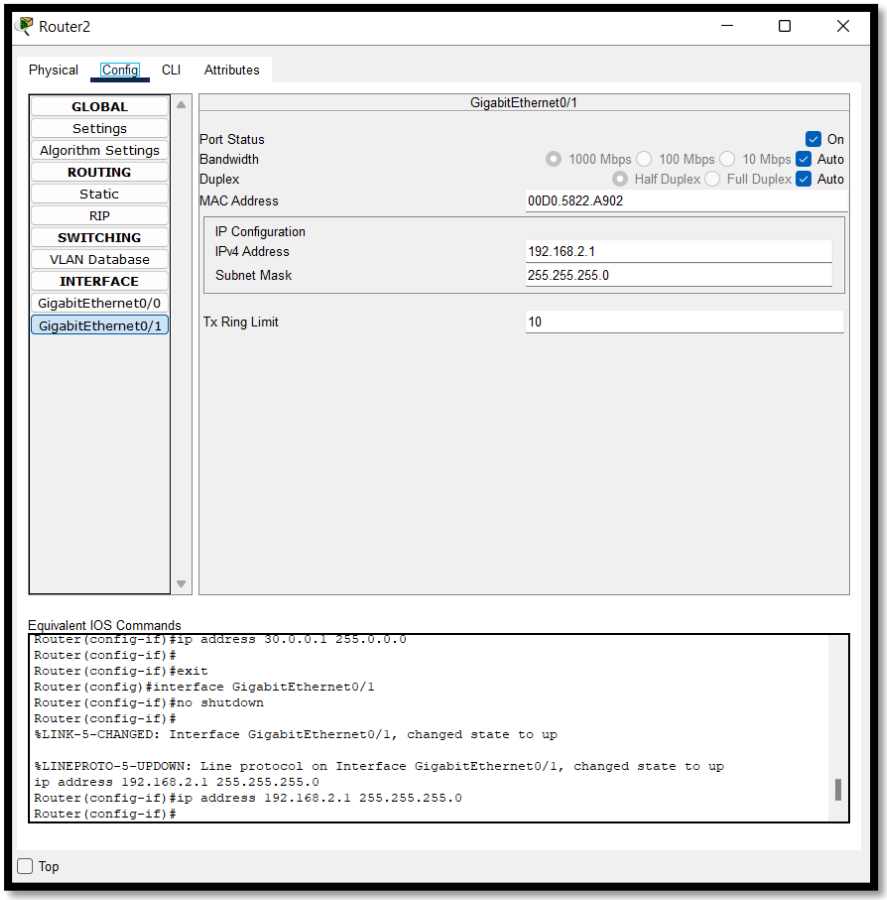



Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C9E9.7901
IP Configuration
IPv4 Address
20.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
ip address 20.0.0.1 255.0.0.0
Router(config-if)#
Top

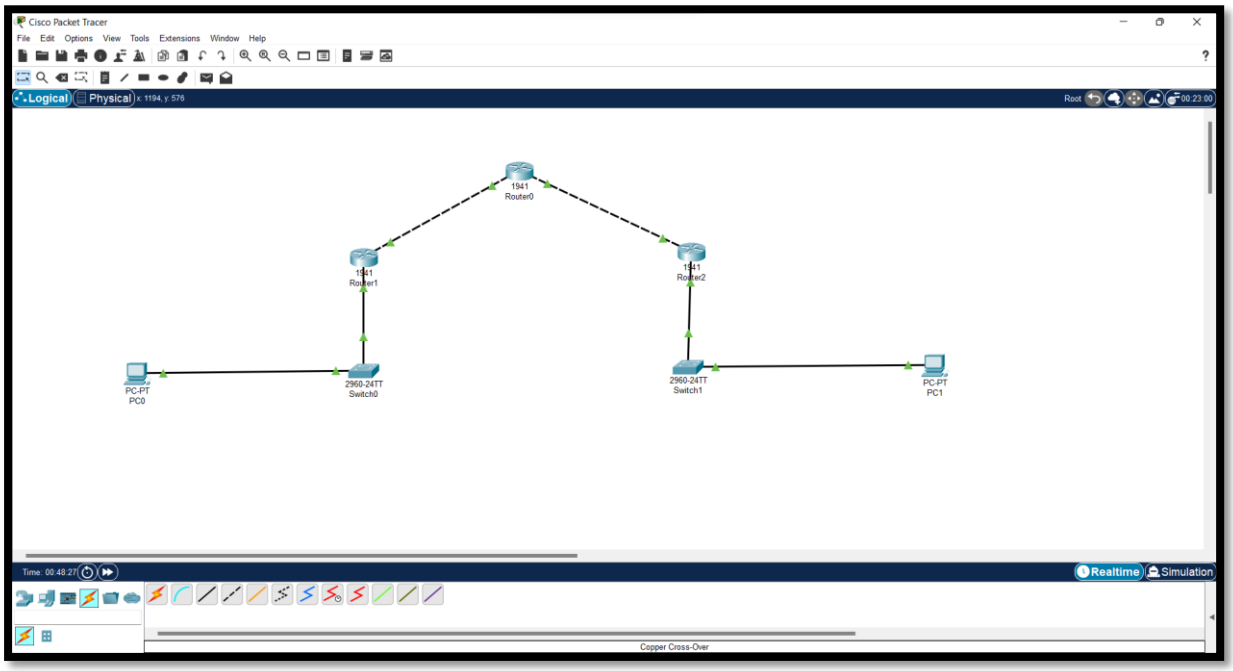

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0005.5EBA.C502
IP Configuration
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
ip address 20.0.0.2 255.0.0.0
Router(config-if)#
Top


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0005.5EBA.C501
IP Configuration
IPv4 Address
30.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
ip address 20.0.0.2 255.0.0.0
Router(config-if)#ip address 20.0.0.2 255.0.0.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
ip address 30.0.0.2 255.0.0.0
Router(config-if)#
Top


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.5822.A901
IP Configuration
IPv4 Address
30.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
ip address 30.0.0.1 255.0.0.0
Router(config-if)#
Top

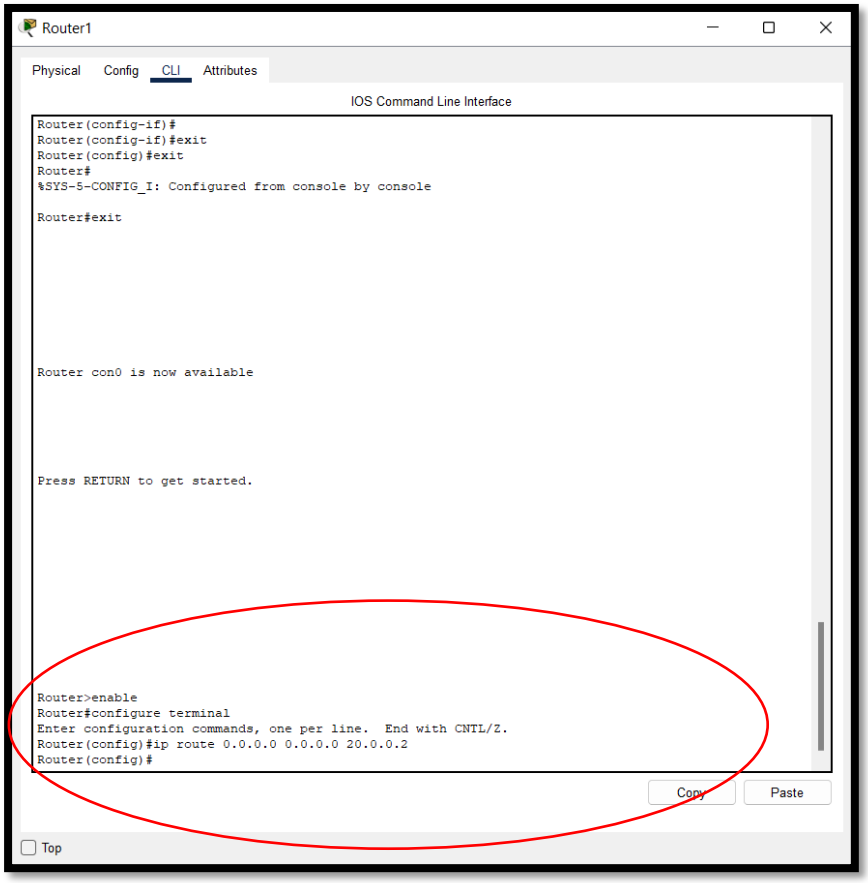


- Now we can see all the connections are properly configured as given below (Green Arrow).

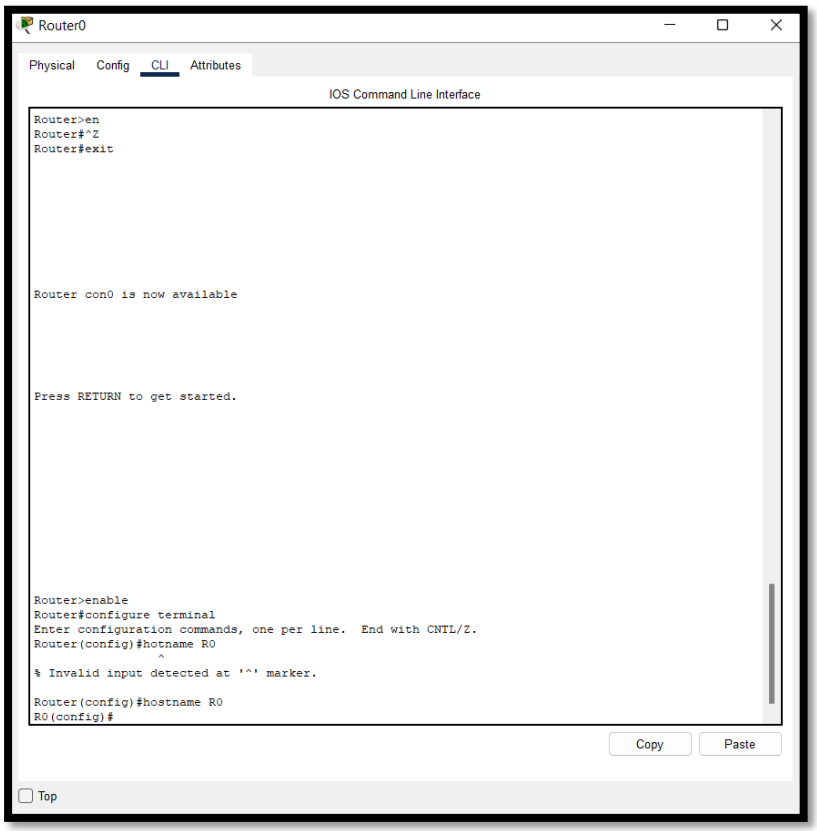


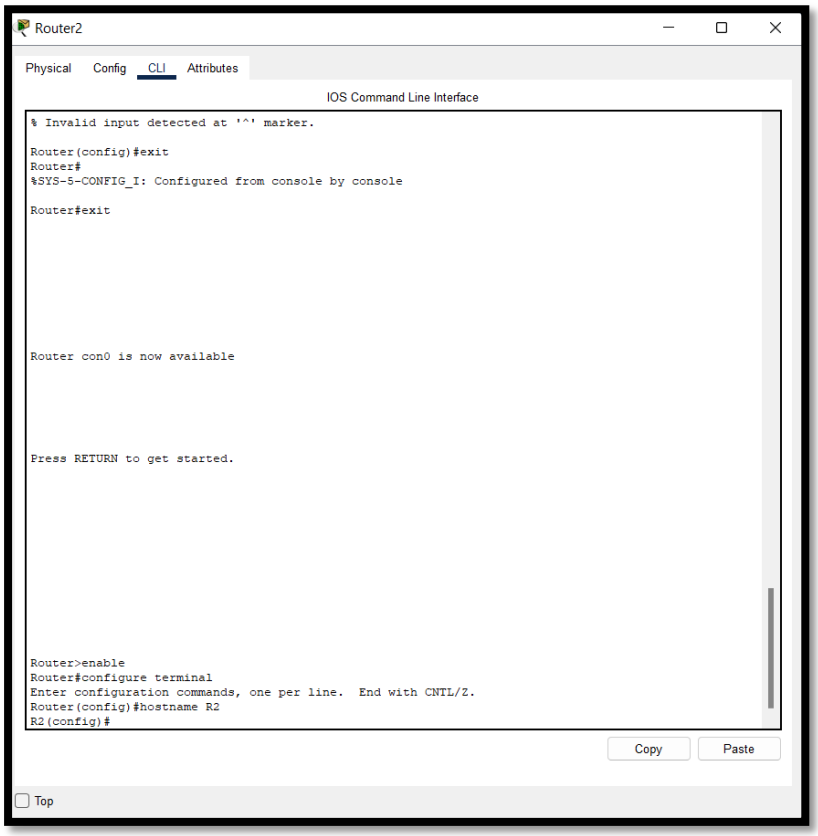
- We have to set the path from Router 0 - 20.0.0.2 to Router 1 and Router 0 – 30.0.0.2 to Router 2 as shown below.

- Click on the Router 1 and go to CLI mode follow the below steps.

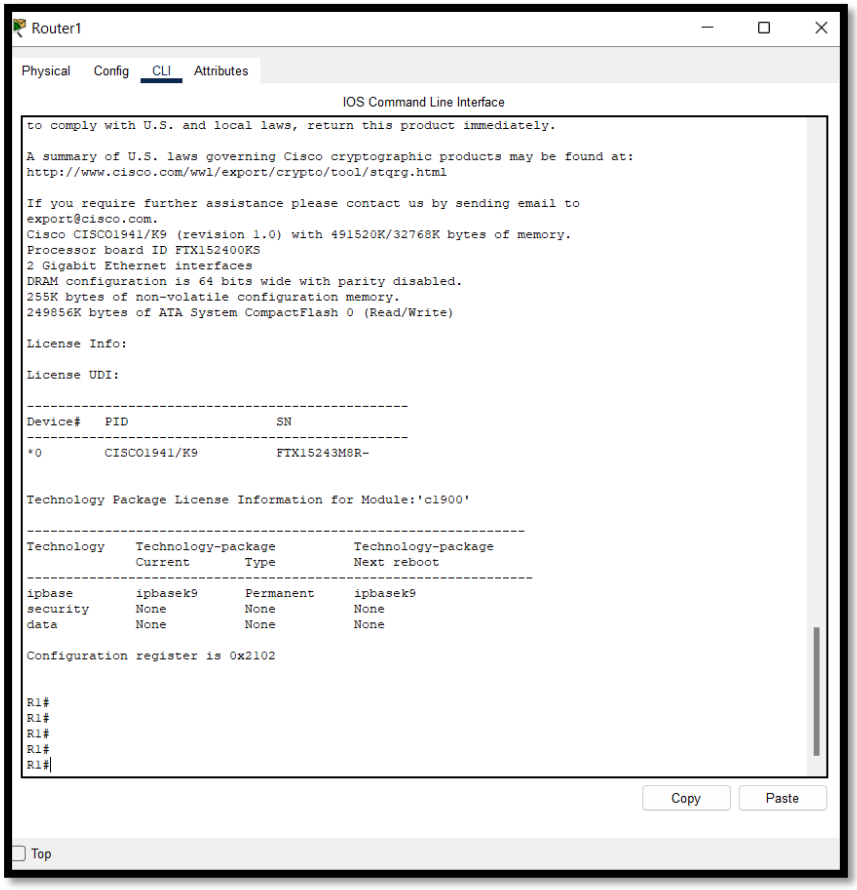


Step 2: Configure the Hostname on all Routers and enable the security package on R1 and R2, ping one PC from the other (all packets are lost).

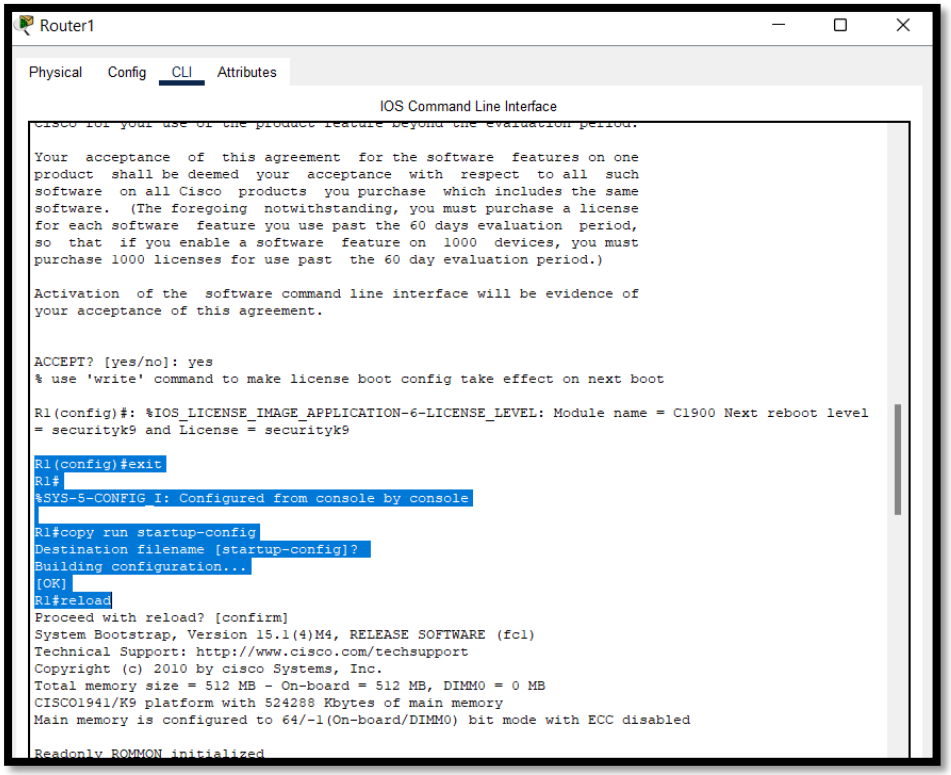


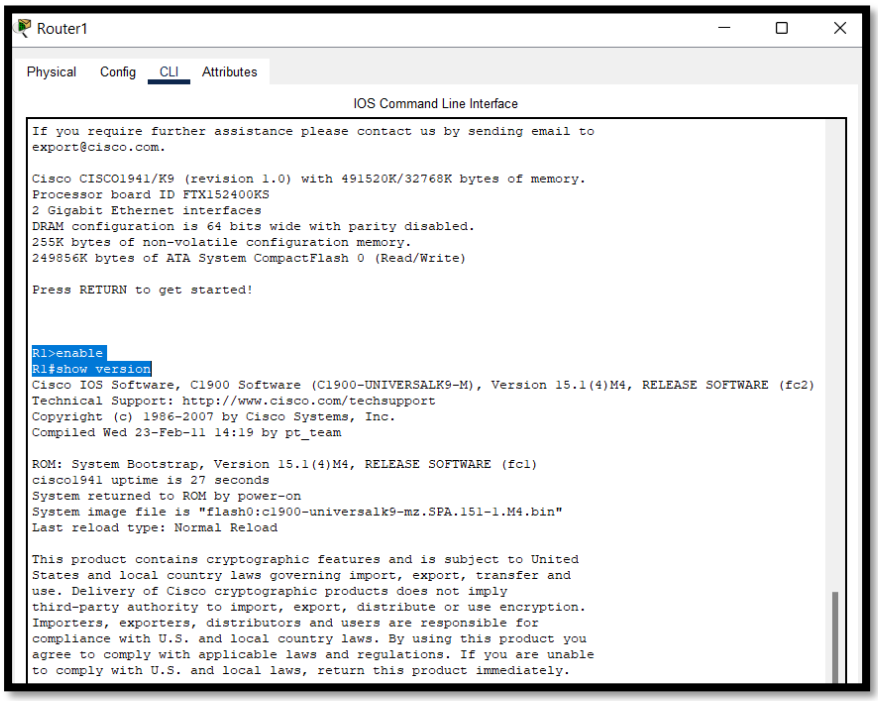


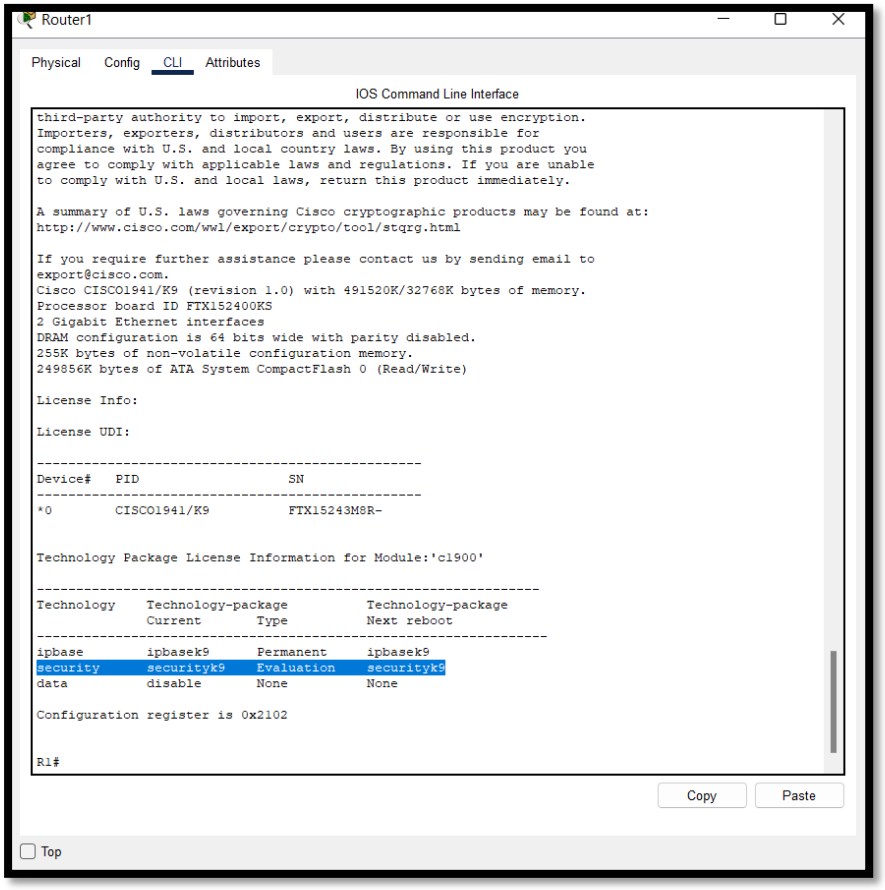
- Enable the security packages on the Router 1 and Router 2.
- First of all, let us check whether the security version is enabled or not.



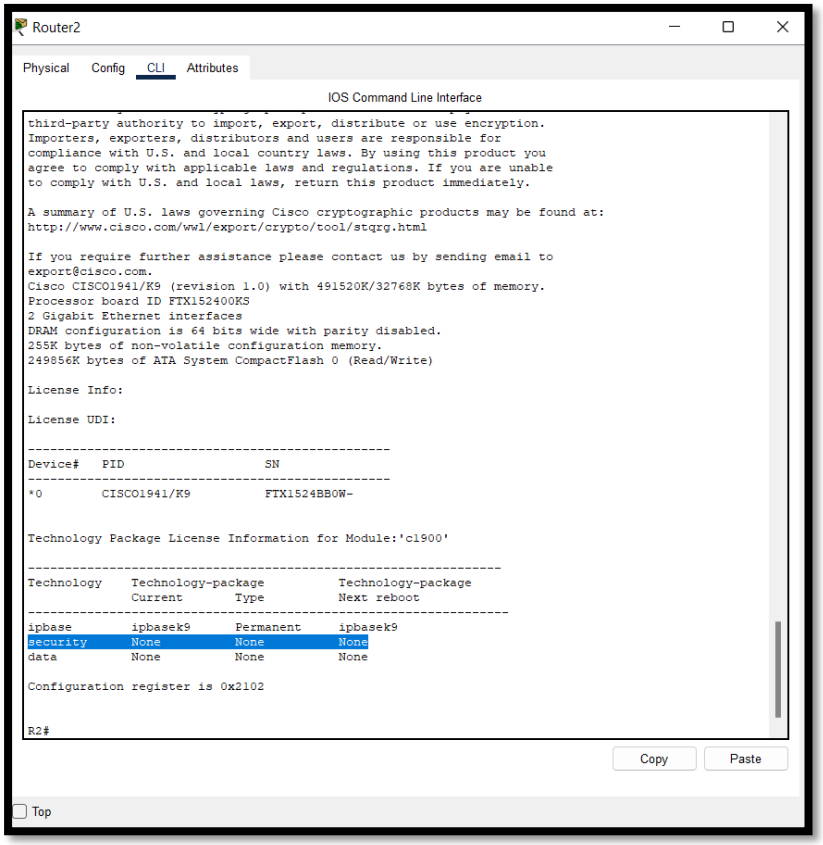
- To enable the security package, follow the below commands.

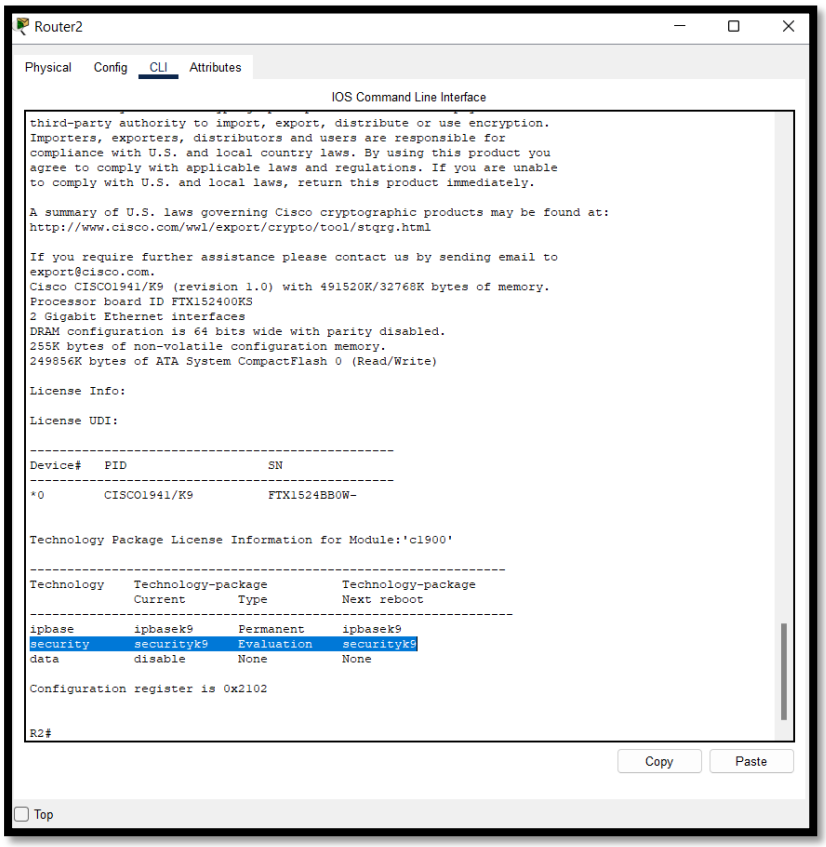

Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Your acceptance of this agreement for the software features on one product shall be deemed your acceptance with respect to all such software on all Cisco products you purchase which includes the same software. (The foregoing notwithstanding, you must purchase a license for each software feature you use past the 60 days evaluation period, so that if you enable a software feature on 1000 devices, you must purchase 1000 licenses for use past the 60 day evaluation period.)
Activation of the software command line interface will be evidence of your acceptance of this agreement.
ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled
Readonly ROMMON initialized


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
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
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)
Press RETURN to get started!
R1>enable
R1#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team
ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 27 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload
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.



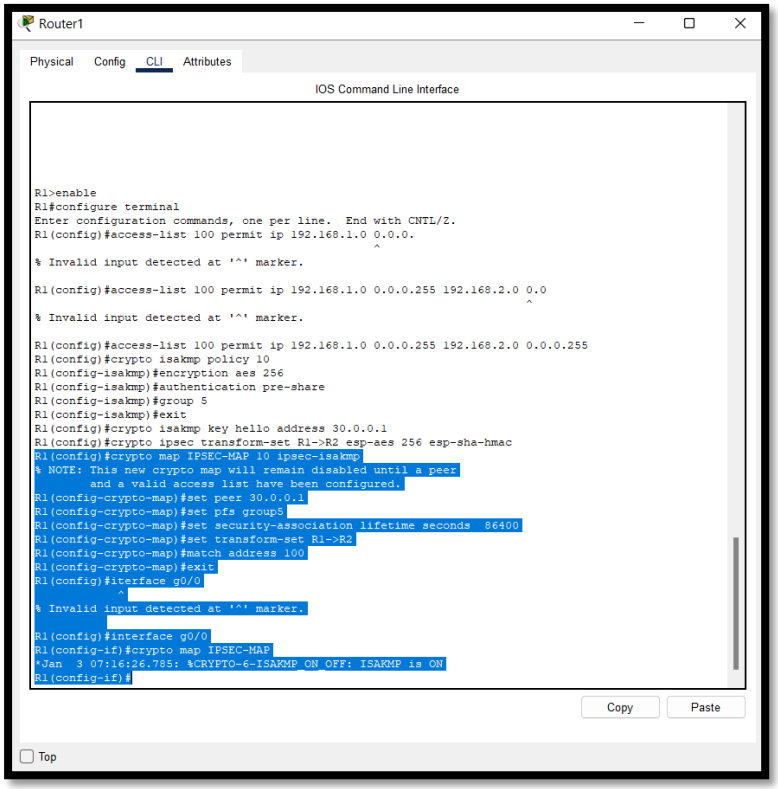
- Follow the same steps for Router 2.

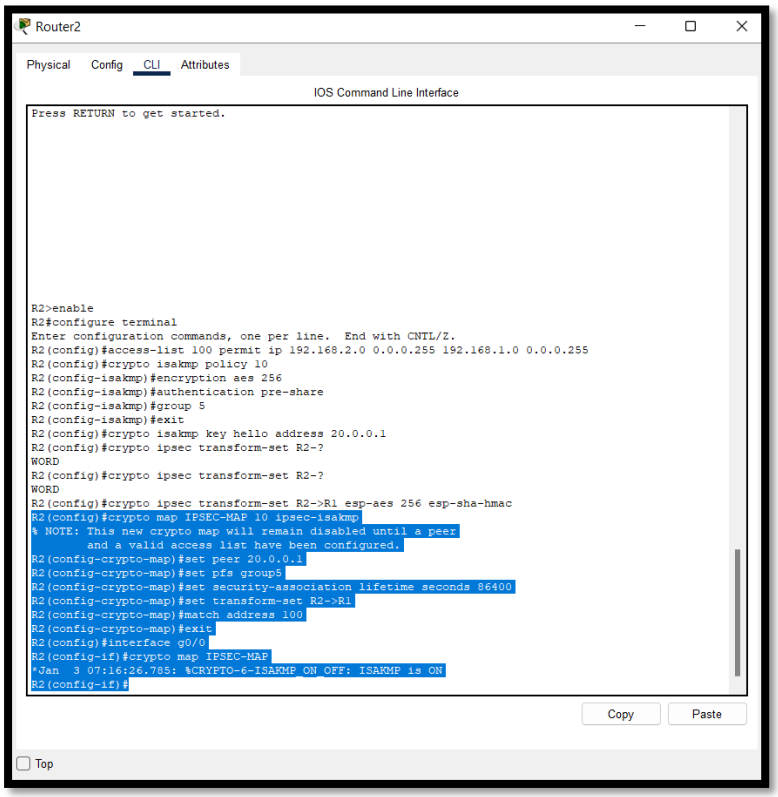




Step 3: Apply the Access Control List (ACL) at Router 1 and Router 2, Set the ISAKMP policy and ISAKMP key, Set IPsec transform set.

Step 4: Create the Crypto map. Apply the Crypto map to the required interface.





Step 5: Verify the output by pinging one PC from other (ping is successful)

- Now go to command prompt of PC0 and ping 192.168.2.2
- It will successfully generate the output now.