

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:

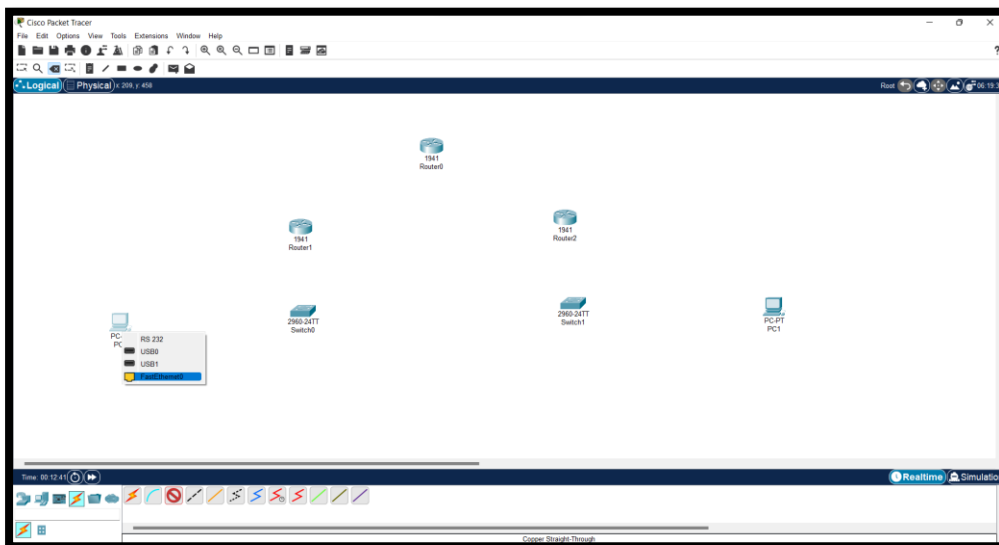
Download Cisco Packet Tracer

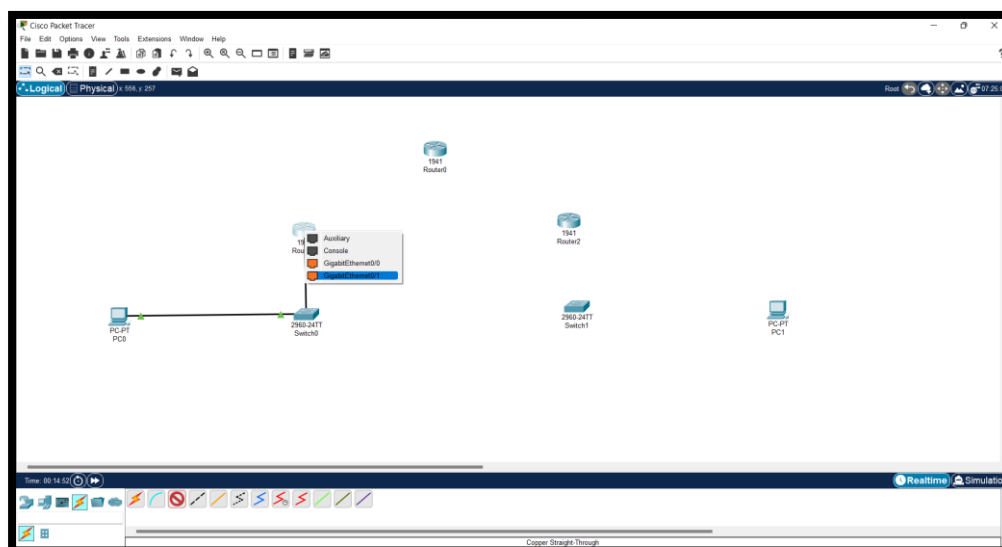
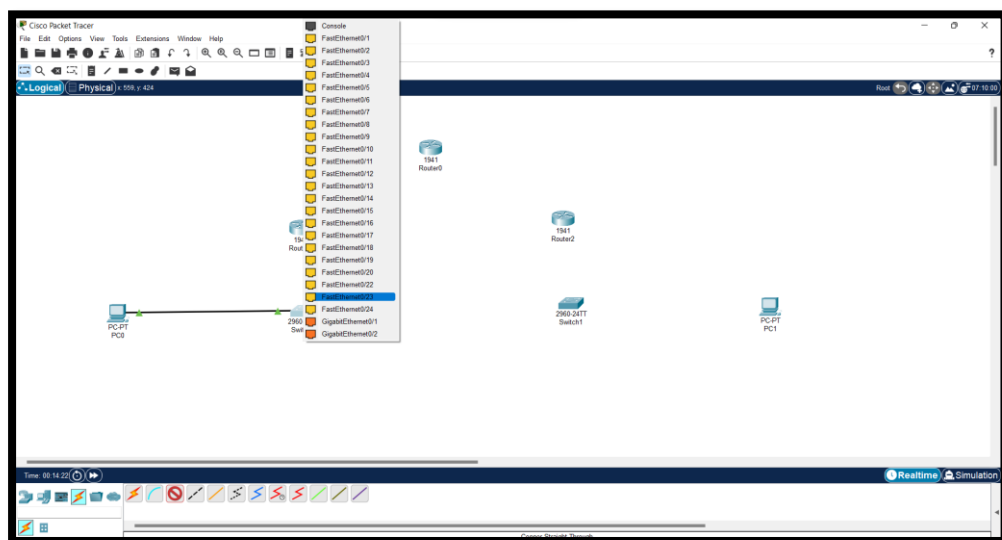
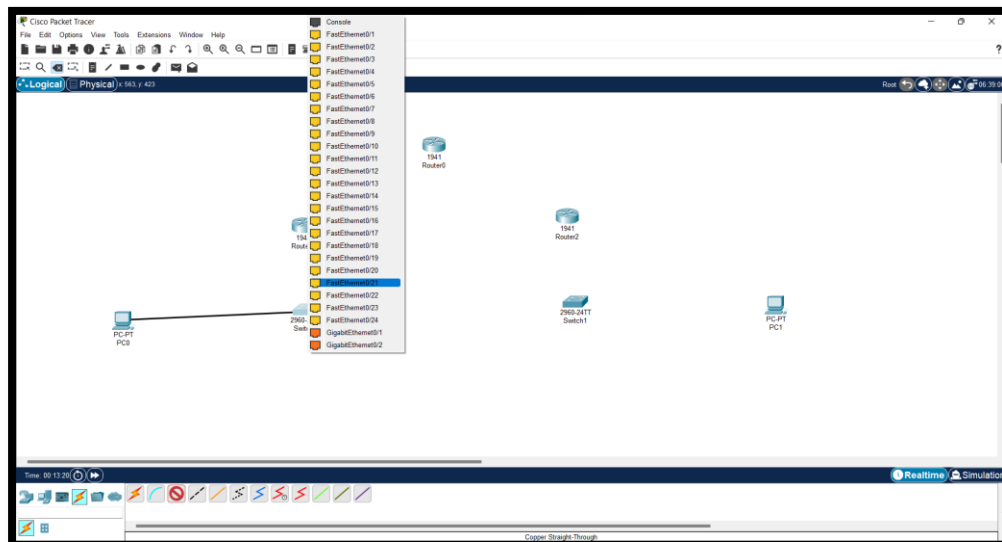
Requirements:

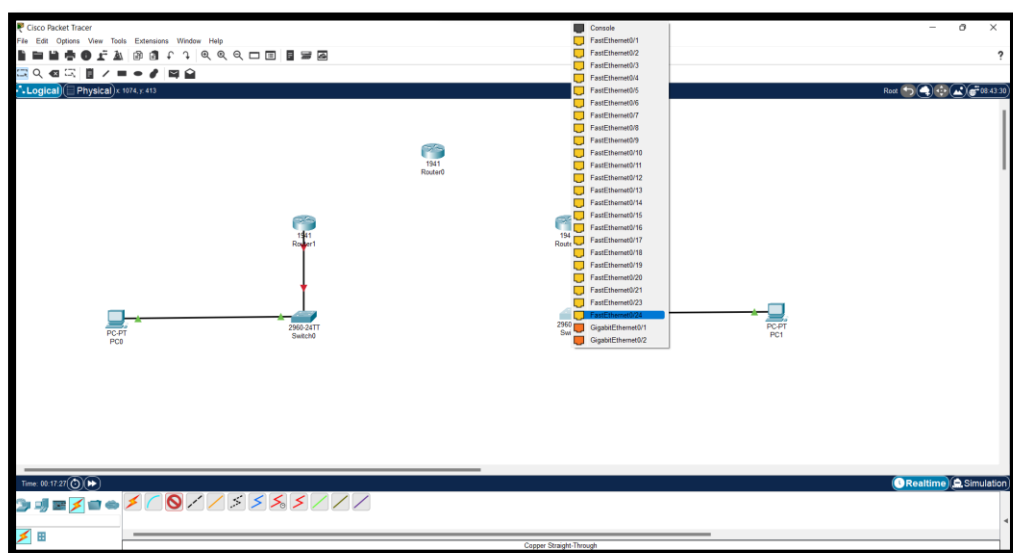
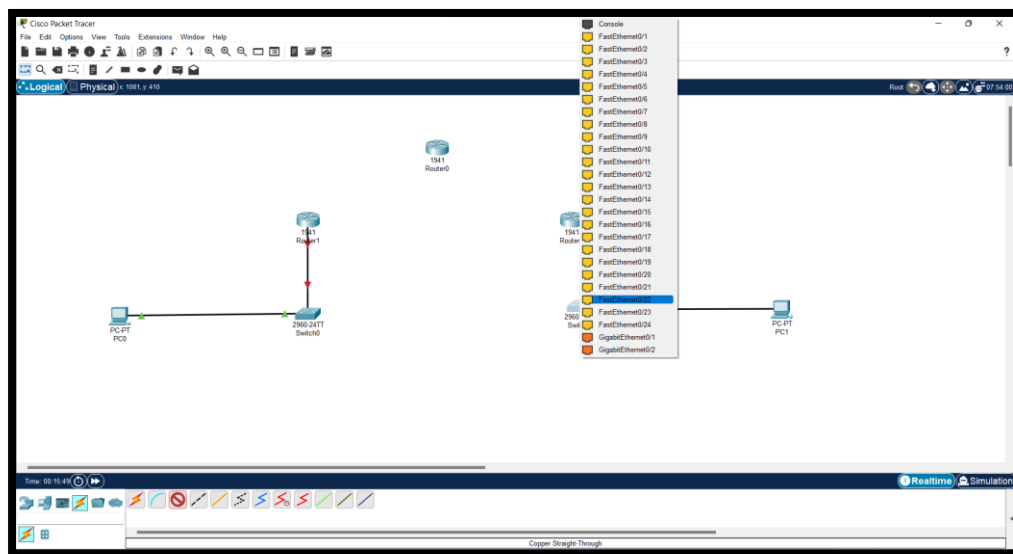
- Take 3 Routers (1941)
- Take 2 Switches (2960)
- Take 2 PC
- Configuration:
 - PC 0 – 192.168.1.2
 - PC 1 – 192.168.2.2
 - Router 1 (G 0/0) - 20.0.0.1
 - Router 1 (G 0/1) - 192.168.1.1
 - Router 0 (G 0/0) - 30.0.0.2
 - Router 0 (G 0/1) - 20.0.0.2
 - Router 2 (G 0/0) - 30.0.0.1
 - Router 2 (G 0/1) - 192.168.2.1

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

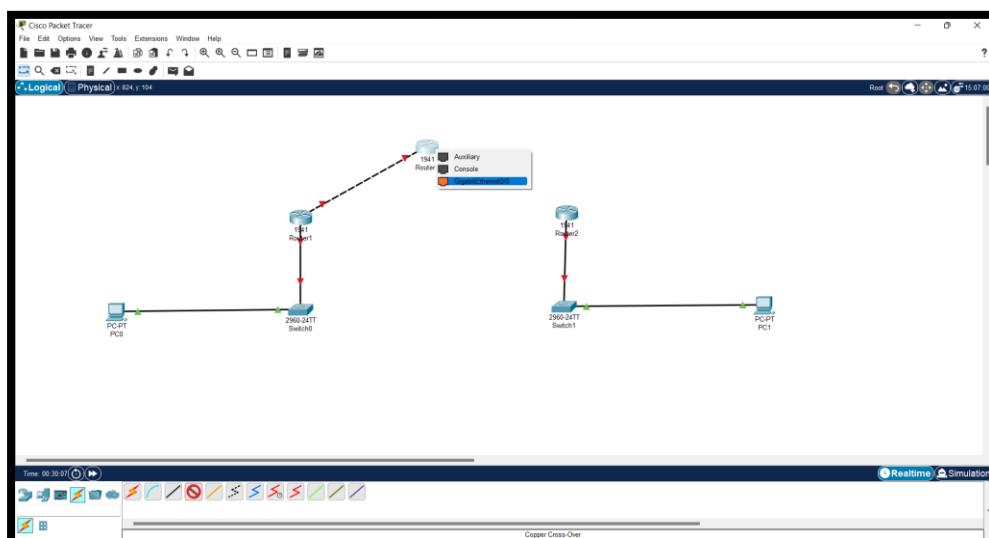
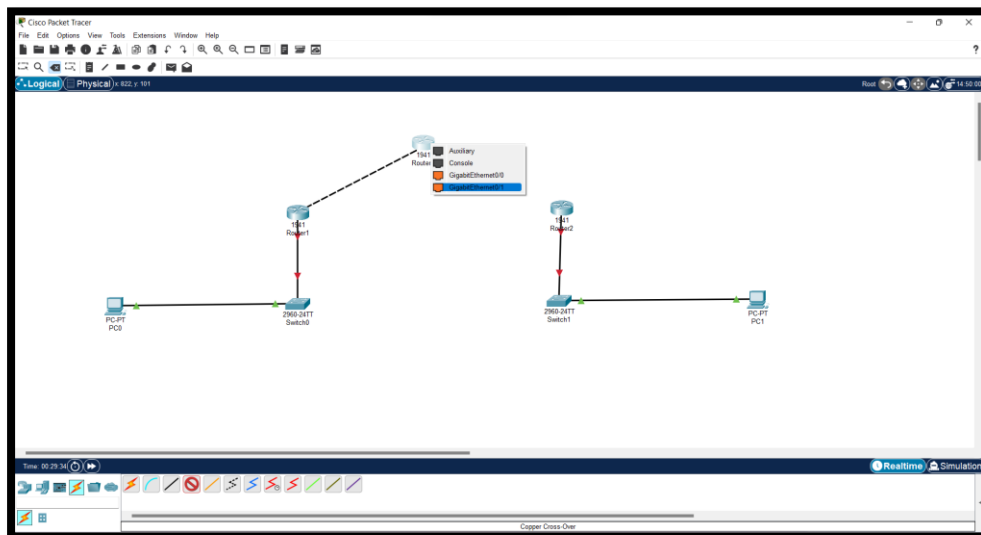
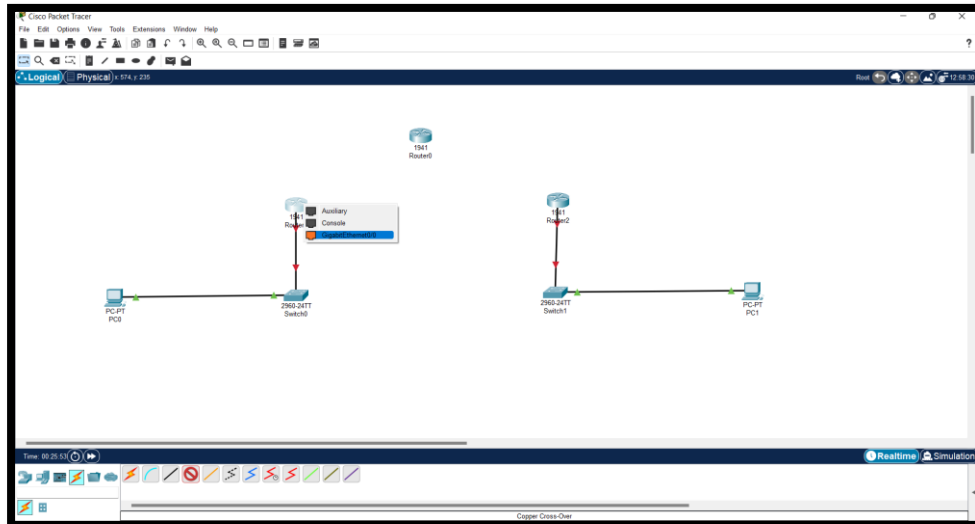
- Connect the PC with Switches and also connect switches with Router using copper straight wire as given below.

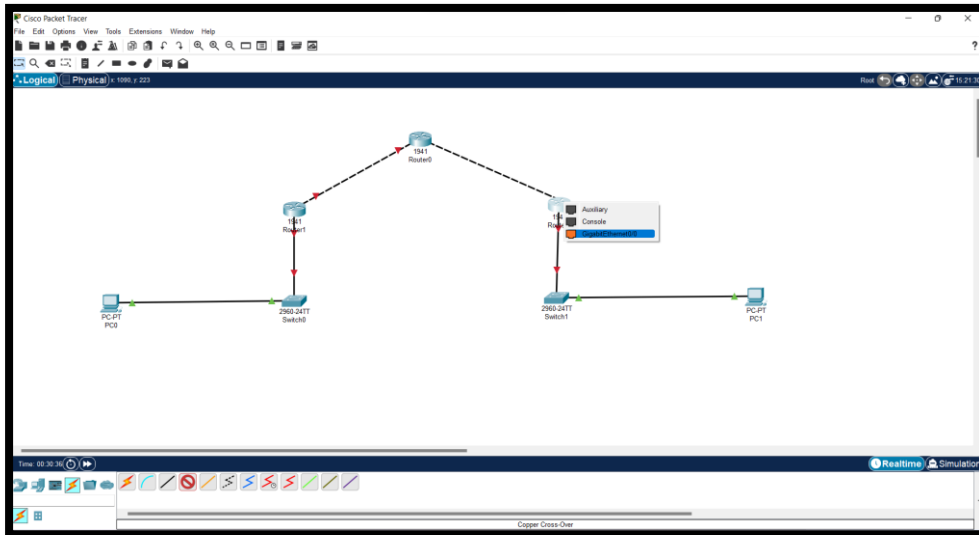






- Connect the Router 1 with Router 0 and Router 0 with Router 2 using copper cross wire as given below.





- Provide the IP address to PC 0 and PC 1

The screenshot shows the configuration window for PC0. The 'Desktop' tab is selected. Under 'IP Configuration', the 'Interface' is 'FastEthernet0'. The 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

Under 'IPv6 Configuration', the 'Static' radio button is selected. The fields are empty:

Field	Value
IPv6 Address	
Link Local Address	FE80::209:7CFF:FE95:8B69
Default Gateway	
DNS Server	

Under '802.1X', the 'Use 802.1X Security' checkbox is unchecked. The 'Authentication' dropdown is set to 'MD5'. The 'Username' and 'Password' fields are empty.

The screenshot shows the 'PC1' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing settings for 'FastEthernet0'. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). Below these are fields for 'IPv4 Address' (192.168.2.2), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.2.1), and 'DNS Server' (0.0.0.0). The 'IPv6 Configuration' section also has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). Below these are fields for 'IPv6 Address' (empty), 'Link Local Address' (FE80::240:BFF:FED3:9A7A), 'Default Gateway' (empty), and 'DNS Server' (empty). The '802.1X' section has a checkbox 'Use 802.1X Security' (unchecked), a dropdown 'Authentication' (MD5), and fields for 'Username' and 'Password'.

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::240:BFF:FED3:9A7A

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

Top

➤ Provide the IP Configuration to the Routers.

The screenshot shows the 'Router1' configuration window with the 'Config' tab selected. The 'GigabitEthernet0/1' interface is selected in the left sidebar. The 'GigabitEthernet0/1' configuration section shows 'Port Status' (On), 'Bandwidth' (1000 Mbps), 'Duplex' (Half Duplex), and 'MAC Address' (0001.C9E9.7902). The 'IP Configuration' section shows 'IPv4 Address' (192.168.1.1) and 'Subnet Mask' (255.255.255.0). The 'Tx Ring Limit' is set to 10. The 'Equivalent IOS Commands' section at the bottom shows the following commands: '170 West Tasman Drive', 'San Jose, California 95134-1706', '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) 1986-2012 by Cisco Systems, Inc.', 'Compiled Thurs 5-Jan-12 15:41 by pt_team', 'Image text-base: 0x2100F918, data-base: 0x24729040', and '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'.

Router1

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 0001.C9E9.7902

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

170 West Tasman Drive
San Jose, California 95134-1706

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) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

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

Top

Router1

Physical Config CLI Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

GigabitEthernet0/0

Port Status ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ On

Bandwidth ☒ 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 ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ On

Bandwidth ☒ 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

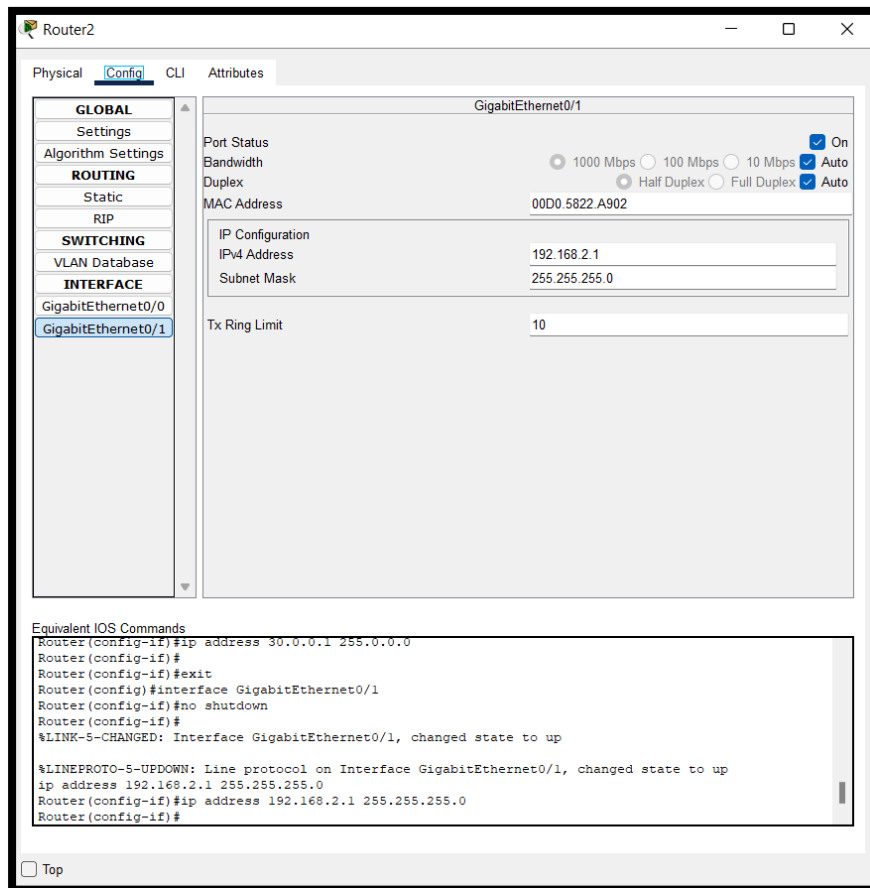
Tx Ring Limit 10

Equivalent IOS Commands

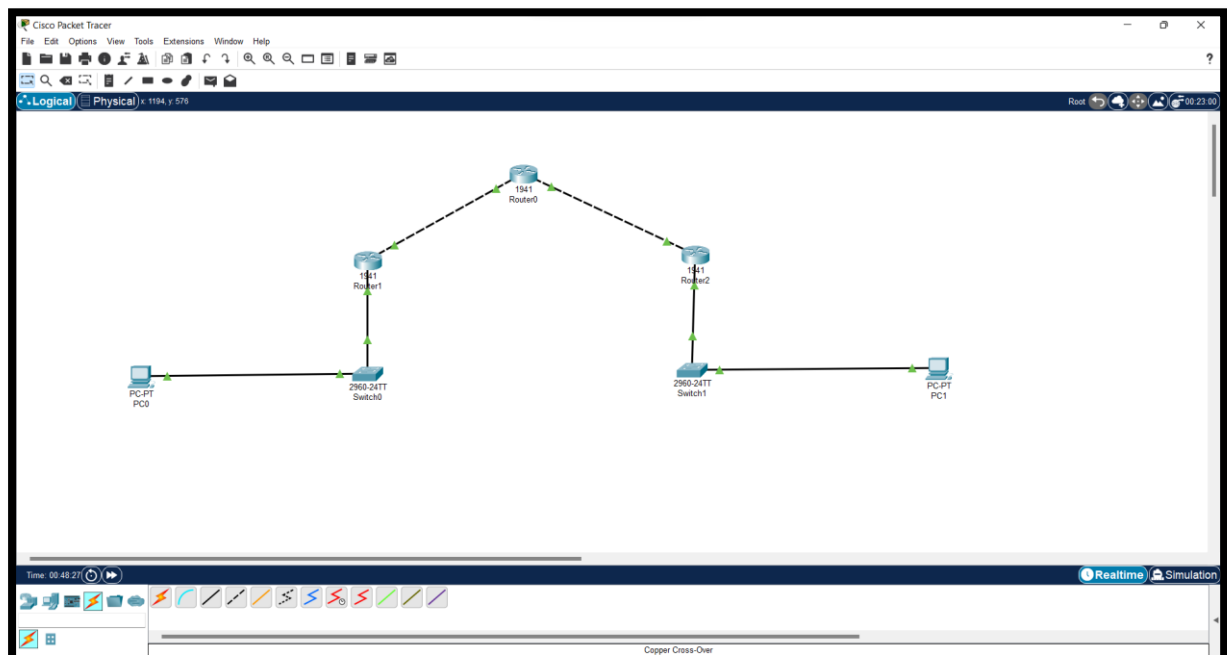
```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%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

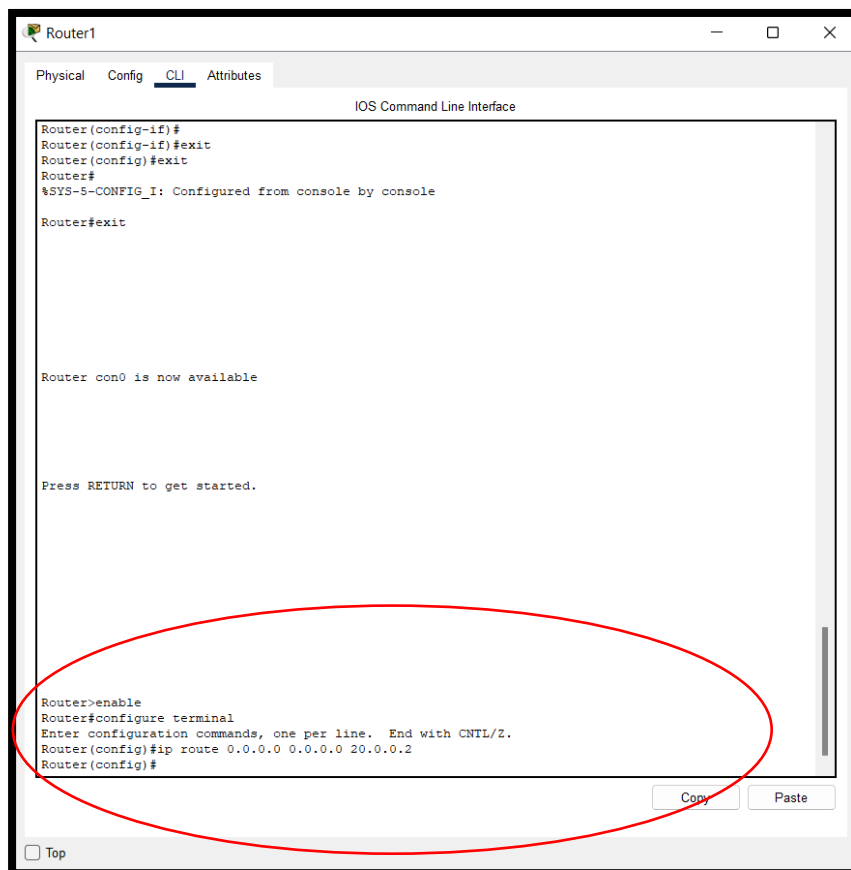


- Now we can see all the connections are properly configured as given below (Green Arrow).

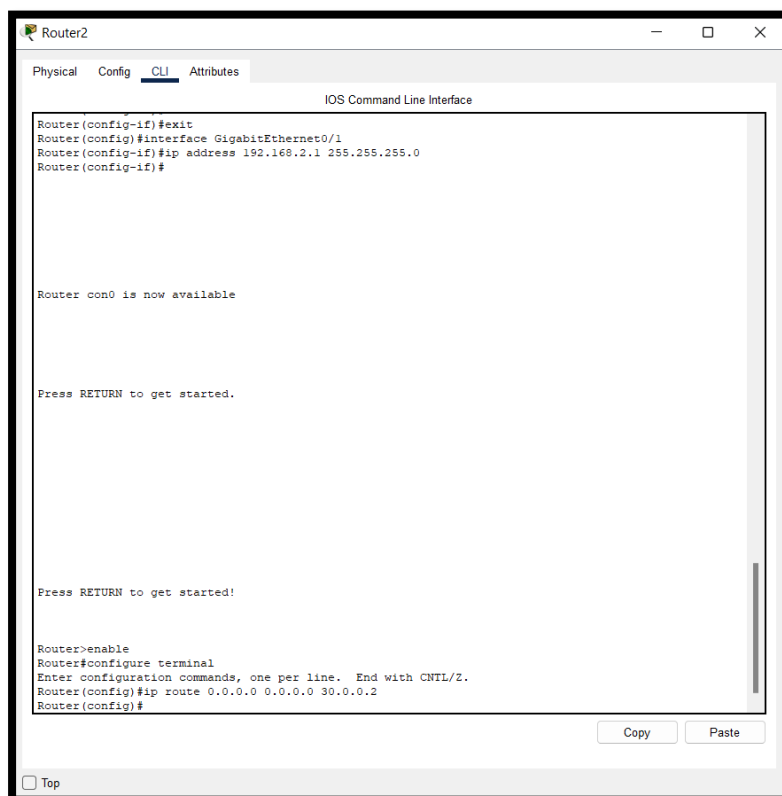


- We have to set the path from Router 0 - 20.0.0.2 to Router 1 and Router 0 – 30.0.0.2 to Router 2 as shown below.

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

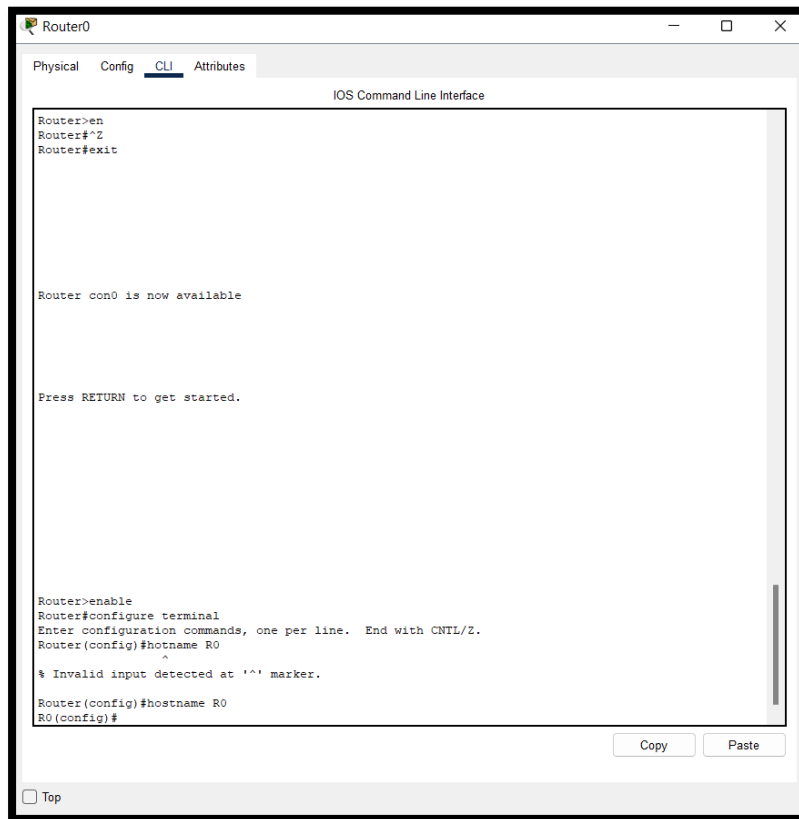


```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#exit
Router#exit
Router con0 is now available
Press RETURN to get started.
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
Router(config)#
```



```
Router2
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#
Router con0 is now available
Press RETURN to get started.
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.2
Router(config)#
```

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).



The screenshot shows the CLI interface of Router0. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The main area displays the following text:

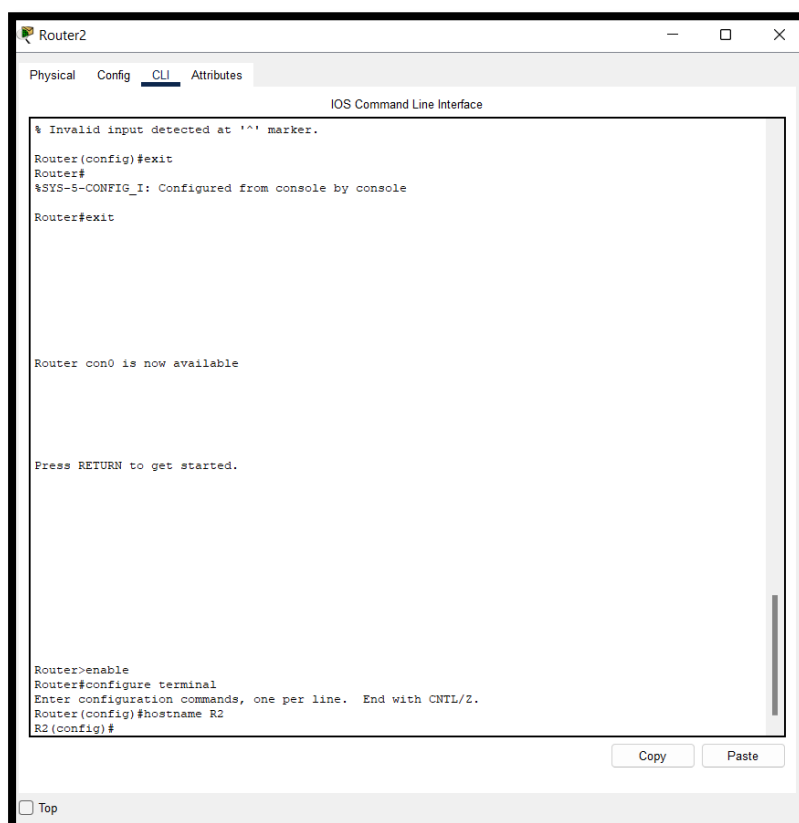
```
Router0>en
Router0#^Z
Router0#exit

Router con0 is now available

Press RETURN to get started.

Router0>enable
Router0#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router0(config)#hostname R0
^
% Invalid input detected at '^' marker.
Router0(config)#hostname R0
R0(config)#
```

At the bottom right, there are 'Copy' and 'Paste' buttons. At the bottom left, there is a 'Top' button.



The screenshot shows the CLI interface of Router2. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The main area displays the following text:

```
% Invalid input detected at '^' marker.
Router2(config)#exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console
Router2#exit

Router2 con0 is now available

Press RETURN to get started.

Router2>enable
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#hostname R2
R2(config)#
```

At the bottom right, there are 'Copy' and 'Paste' buttons. At the bottom left, there is a 'Top' button.

- 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.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#exit
R1#
$SYS-S-CONFIG_I: Configured from console by console

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 1 hours, 24 minutes, 46 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

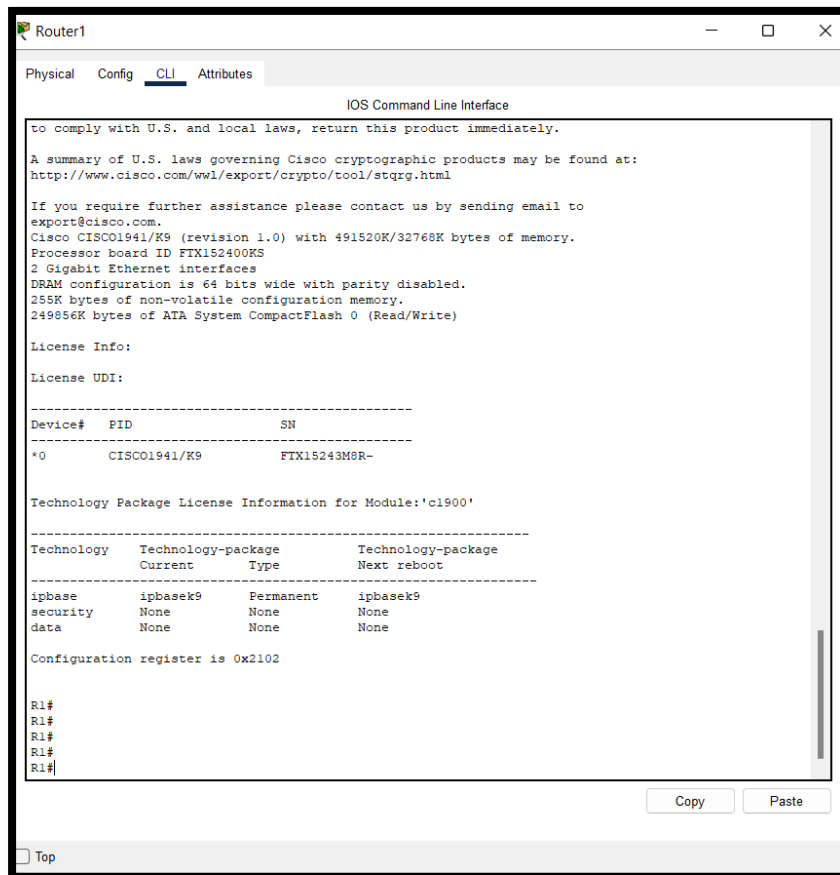
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors 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.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/ww1/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco C1900/K9 (revision 1.0) with 491520K/32768K bytes of memory.
```

Copy Paste

Top



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

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/wll/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISC01941/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)

License Info:

License UDI:

Device#	PID	SN
*0	CISC01941/K9	FTX15243M8R-

Technology Package License Information for Module:'c1900'

Technology	Technology-package Current	Type	Technology-package Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	None	None	None
data	None	None	None

Configuration register is 0x2102

R1#
R1#
R1#
R1#
R1#

Copy Paste

Top

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



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

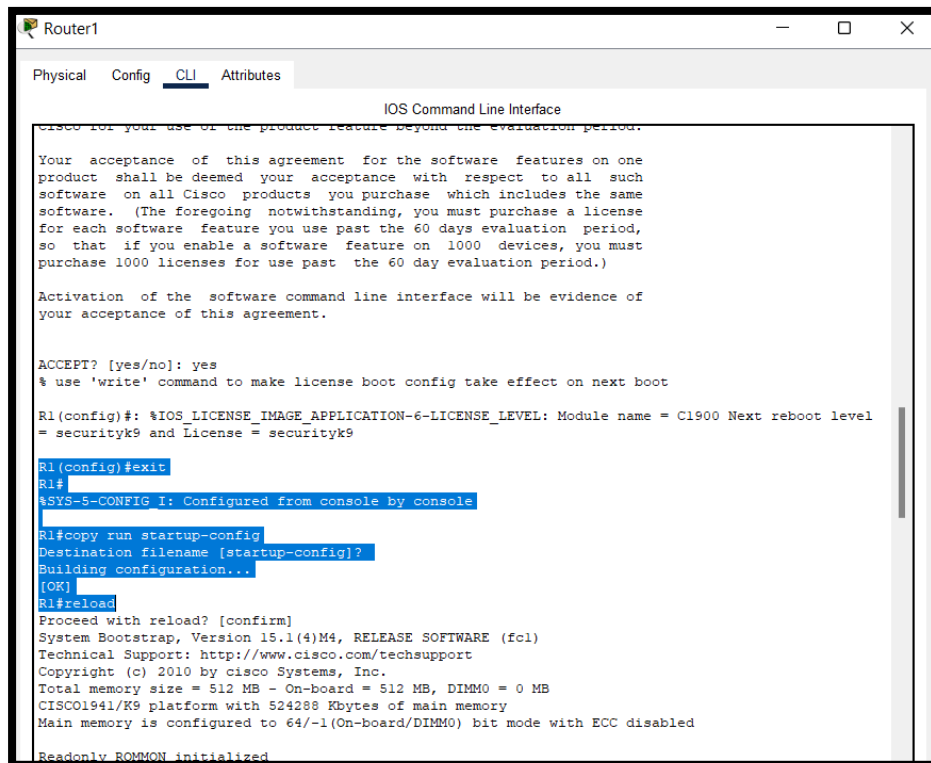
R1#license boot module c1900 technology-package securityk9
^
% Invalid input detected at '^' marker.

R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#

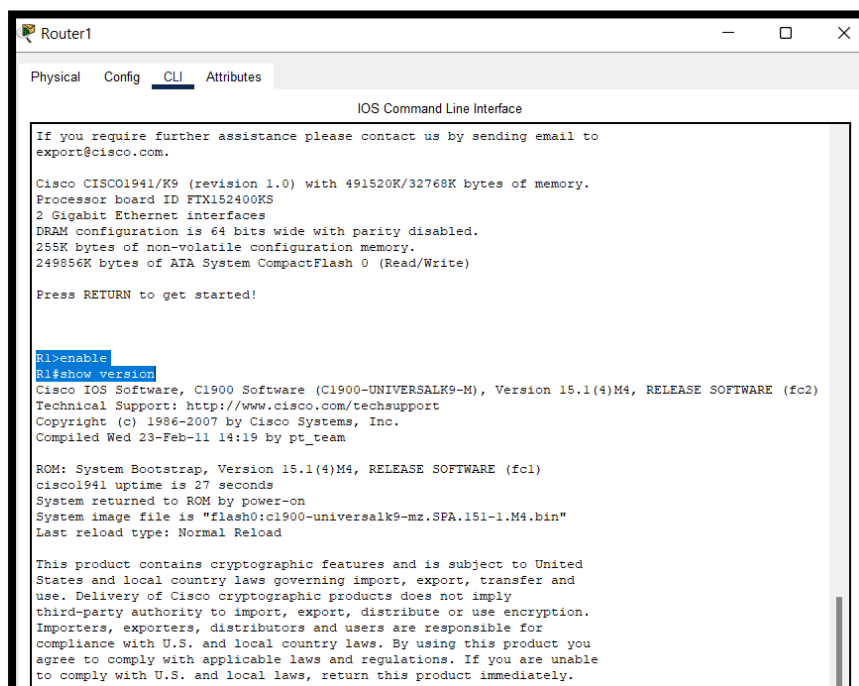
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

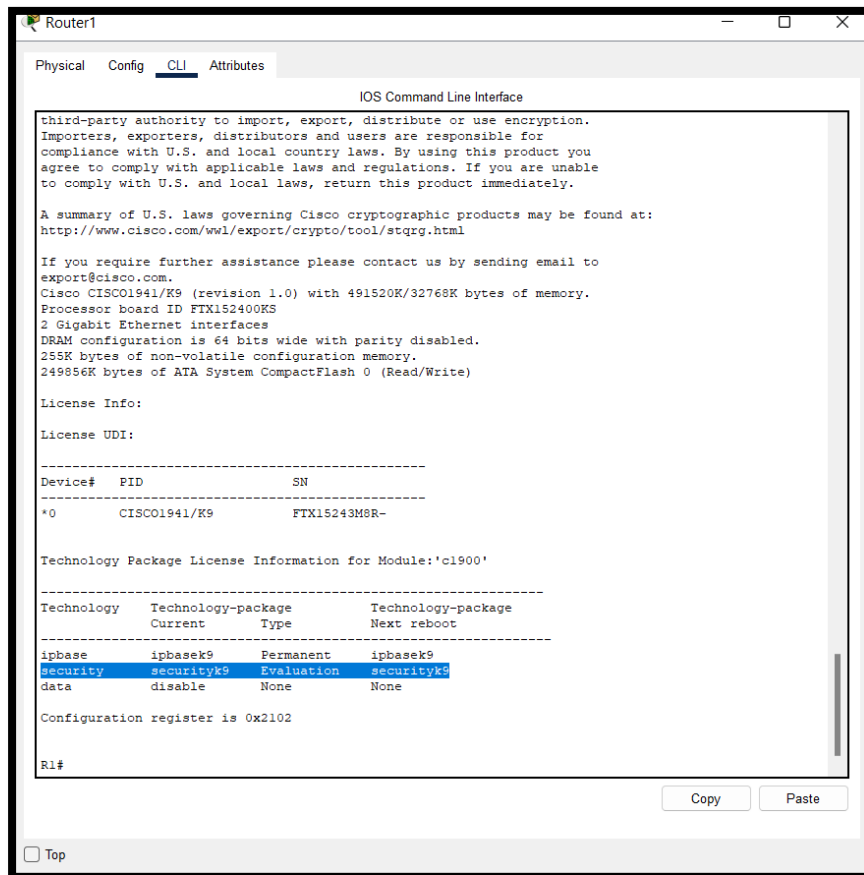
Use of this product feature requires an additional license from Cisco,
together with an additional payment. You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the product, including during the 60 day evaluation period, is



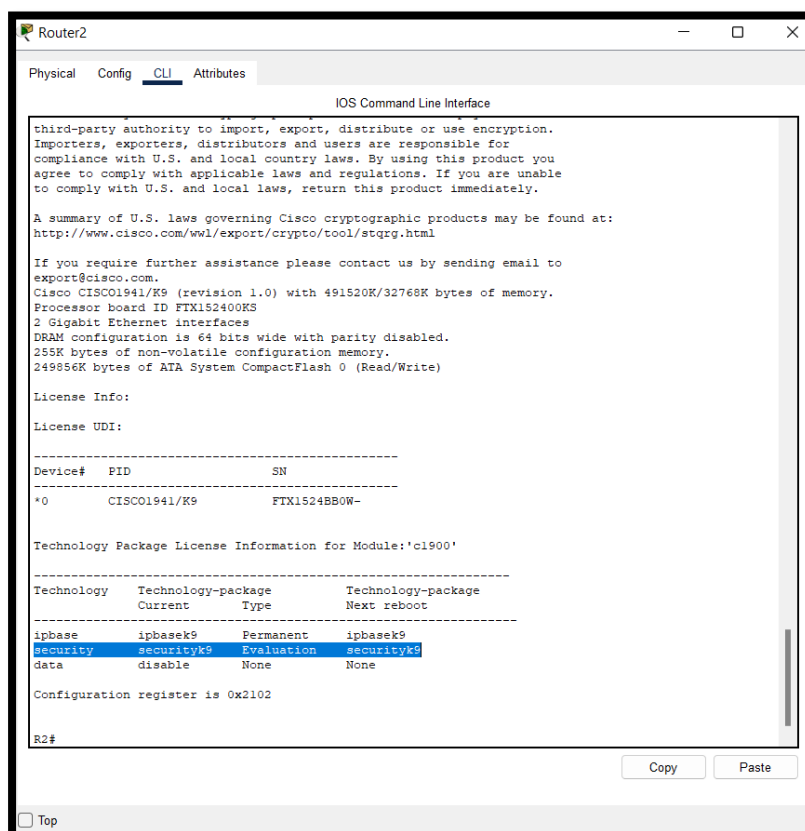
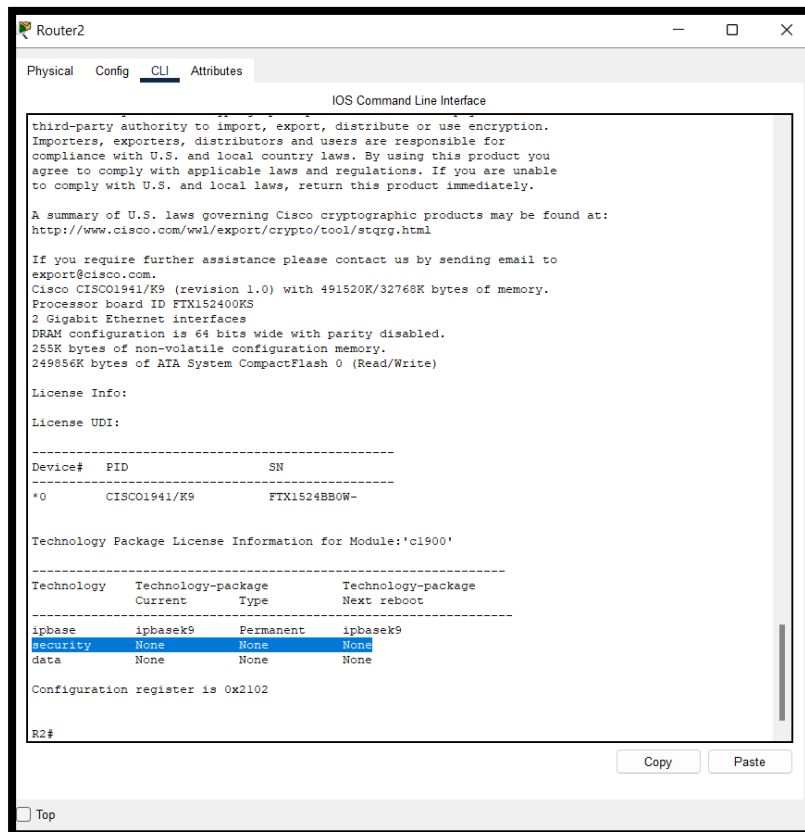
```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
cisco for your use of the product feature beyond the evaluation period.
Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products 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
```



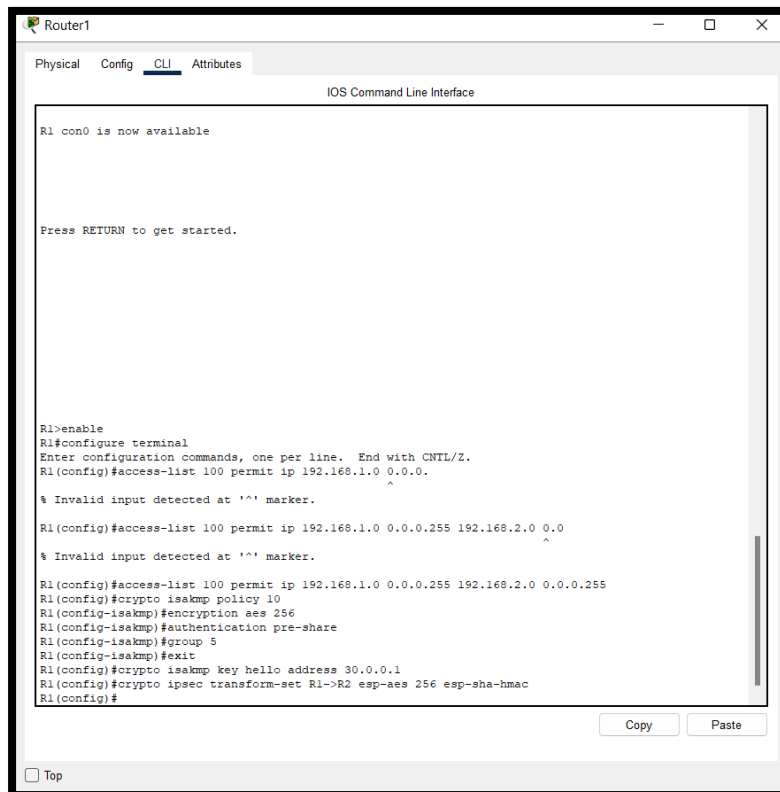
```
Router1
Physical Config CLI Attributes
IOS Command Line Interface
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration 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.



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

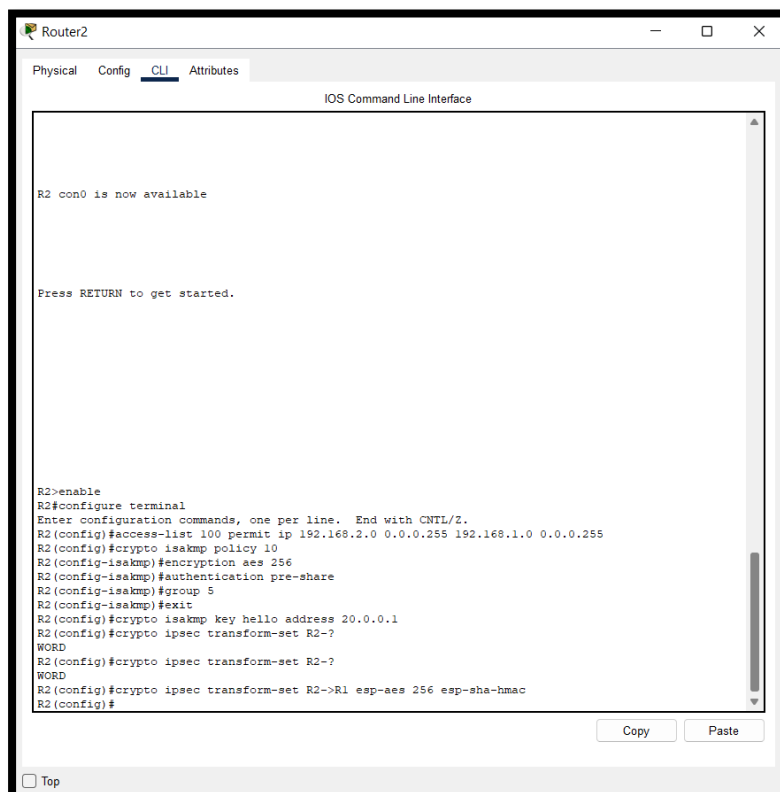
R1 con0 is now available

Press RETURN to get started.

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.
^
% Invalid input detected at '^' marker.

R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0
^
% Invalid input detected at '^' marker.

R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key hello address 30.0.0.1
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac
R1(config)#
```



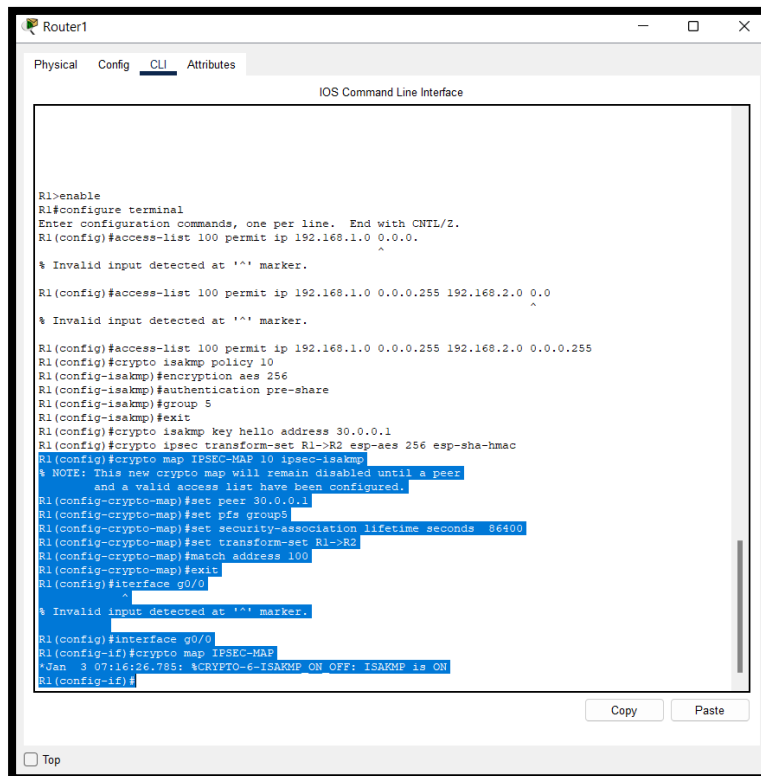
```
Router2
Physical Config CLI Attributes
IOS Command Line Interface

R2 con0 is now available

Press RETURN to get started.

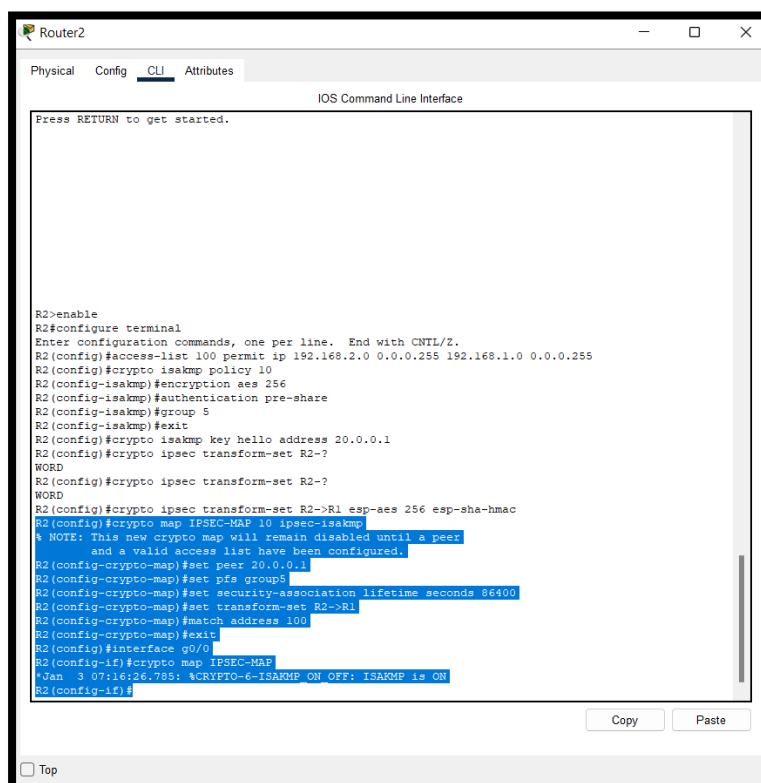
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key hello address 20.0.0.1
R2(config)#crypto ipsec transform-set R2-?
WORD
R2(config)#crypto ipsec transform-set R2-?
WORD
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#
```

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



The screenshot shows the CLI of Router1 with the following configuration commands entered:

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.0
% Invalid input detected at '^' marker.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
% Invalid input detected at '^' marker.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key hello address 30.0.0.1
R1(config)#crypto ipsec transform-set R1->R2 esp-aes 256 esp-sha-hmac
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)#set peer 30.0.0.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set transform-set R1->R2
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#interface g0/0
% Invalid input detected at '^' marker.
R1(config)#interface g0/0
R1(config-if)#crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP ON OFF: ISAKMP is ON
R1(config-if)#
```



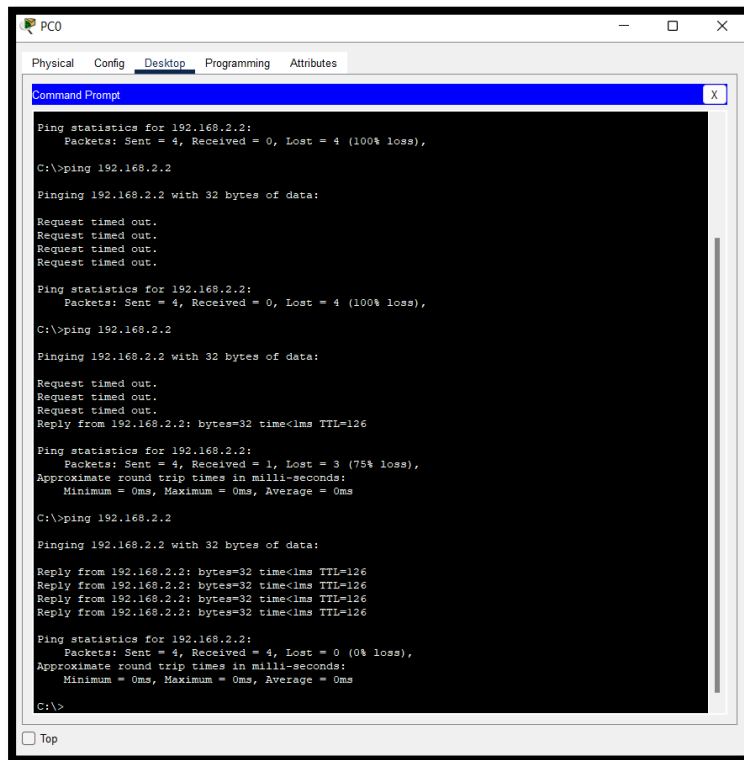
The screenshot shows the CLI of Router2 with the following configuration commands entered:

```
Press RETURN to get started.

R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key hello address 20.0.0.1
R2(config)#crypto ipsec transform-set R2-?
WORD
R2(config)#crypto ipsec transform-set R2-?
WORD
R2(config)#crypto ipsec transform-set R2->R1 esp-aes 256 esp-sha-hmac
R2(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R2(config-crypto-map)#set peer 20.0.0.1
R2(config-crypto-map)#set pfs group5
R2(config-crypto-map)#set security-association lifetime seconds 86400
R2(config-crypto-map)#set transform-set R2->R1
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
R2(config)#interface g0/0
R2(config-if)#crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP ON OFF: ISAKMP is ON
R2(config-if)#
```

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.



The screenshot shows a window titled 'PC0' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the following output:

```
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

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

Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

At the bottom left of the Command Prompt window, there is a checkbox labeled 'Top' which is currently unchecked.