CONFIGURE A SITE TO SITE VPN USING CISCO IOS (DIGITAL ASSIGNMENT - 4)

submitted by

ABHISHEK SHARMA (19BCE0653)

For

INFORMATION SECURITY MANAGEMENT (CSE3502)

LAB COMPONENT(L19+L20)

submitted to

Prof. Lavanya K

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

APRIL 2022

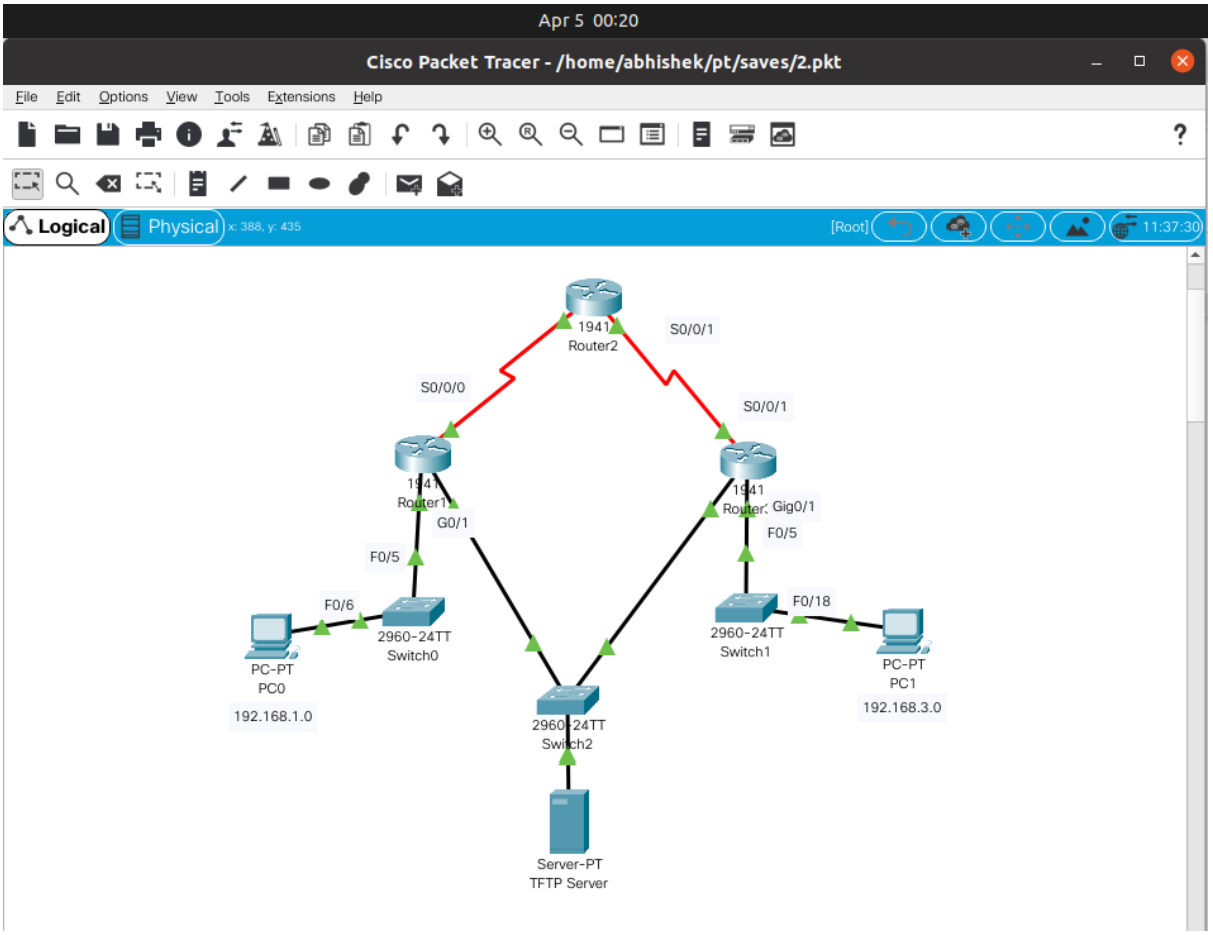
Introduction to VPN:

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. VPN connections can help reduce the costs associated with leased lines. Site-to-Site VPNs typically provide a secure (IPsec or other) tunnel between a branch office and a central office. Another common implementation of VPN technology is remote access to a corporate office from a telecommuter location, such as a small office or home office.

Components of the Network:

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Screenshot of Final Network Topology:



Commands executed:

Device	Command Executed
Router1	*router ospf 101*
	network 192.168.1.0 0.0.0.255 area 0
	network 10.1.1.0 0.0.0.3 area 0
	crypto isakmp enable
	crypto isakmp policy 10
	crypto isakmp policy 10
	hash sha
	authentication pre-share
	group 5
	lifetime 3600
	encryption aes 256
	end
	crypto isakmp key cisco123 address 10.2.2.1
	crypto ipsec transform-set 50 ?
	crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
	exit
	ip ips signature-definition
	signature 2004 0
	status
	exit
	crypto ipsec security-association lifetime seconds 1800
	access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
	crypto map CMAP 10 ipsec-isakmp
	match address 101

	set ?
	set peer 10.2.2.1
	set pfs group5
	set transform-set 50
	set security-association lifetime seconds 900
	exit
	interface S0/0/0
	crypto map CMAP
	end
	show crypto ipsec transform-set
	show crypto map
	debug ip ospf hello
	ping
Router3	*router ospf 101*
	network 192.168.3.0 0.0.0.255 area 0
	network 10.2.2.0 0.0.0.3 area 0
	crypto isakmp enable
	crypto isakmp policy 10
	crypto isakmp policy 10
	hash sha
	authentication pre-share
	group 5
	lifetime 3600
	encryption aes 256
	end
	crypto isakmp key cisco123 address 10.1.1.1
	crypto ipsec transform-set 50 ?

	crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
	exit
	ip ips signature-definition
	signature 2004 0
	status
	exit
	crypto ipsec security-association lifetime seconds 1800
	access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
	crypto map CMAP 10 ipsec-isakmp
	set ?
	set peer 10.2.2.1
	set pfs group5
	set transform-set 50
	set security-association lifetime seconds 900
	exit
	interface S0/0/0
	crypto map CMAP
	end
	show crypto ipsec transform-set
	show crypto map
	debug ip ospf hello
	ping
Router2	*router ospf 101*
	network 10.1.1.0 0.0.0.3 area 0
	network 10.2.2.0 0.0.0.3 area 0

Screenshots of the Procedure:

Part1: Configure Basic Device Settings

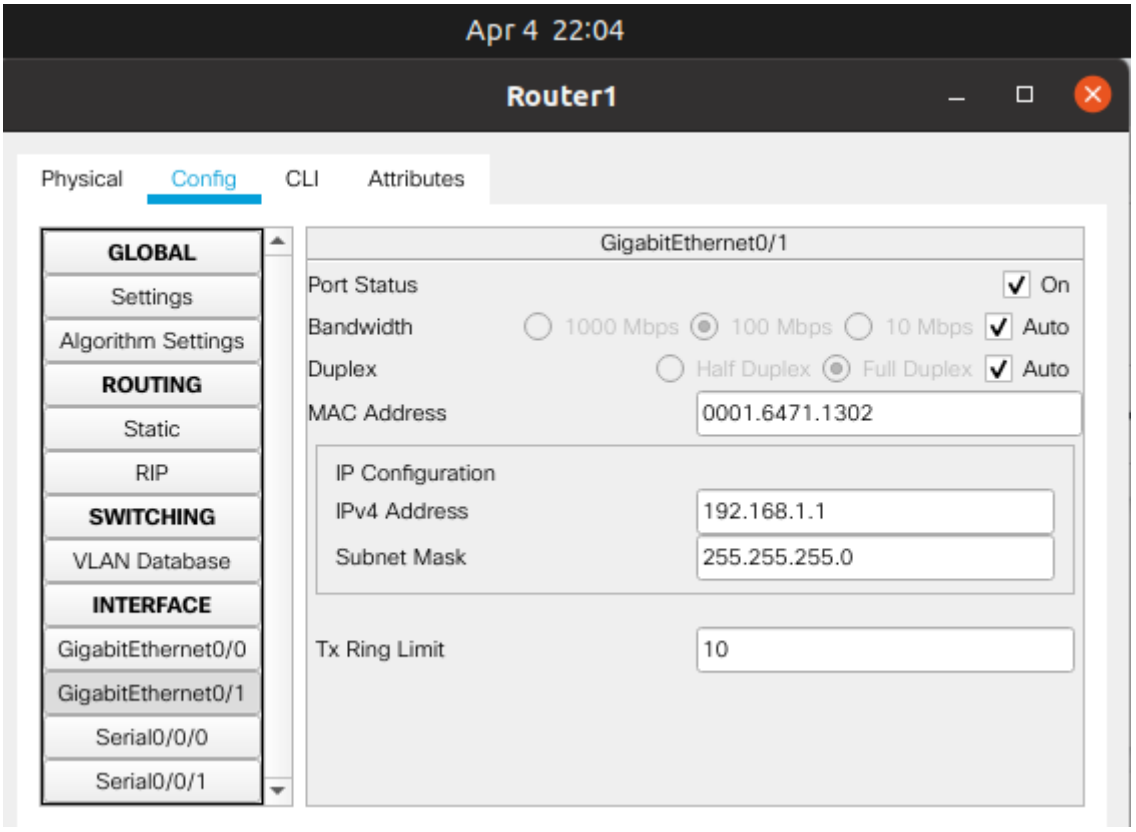


Fig.1:Router1 GigabitEthernet0/1

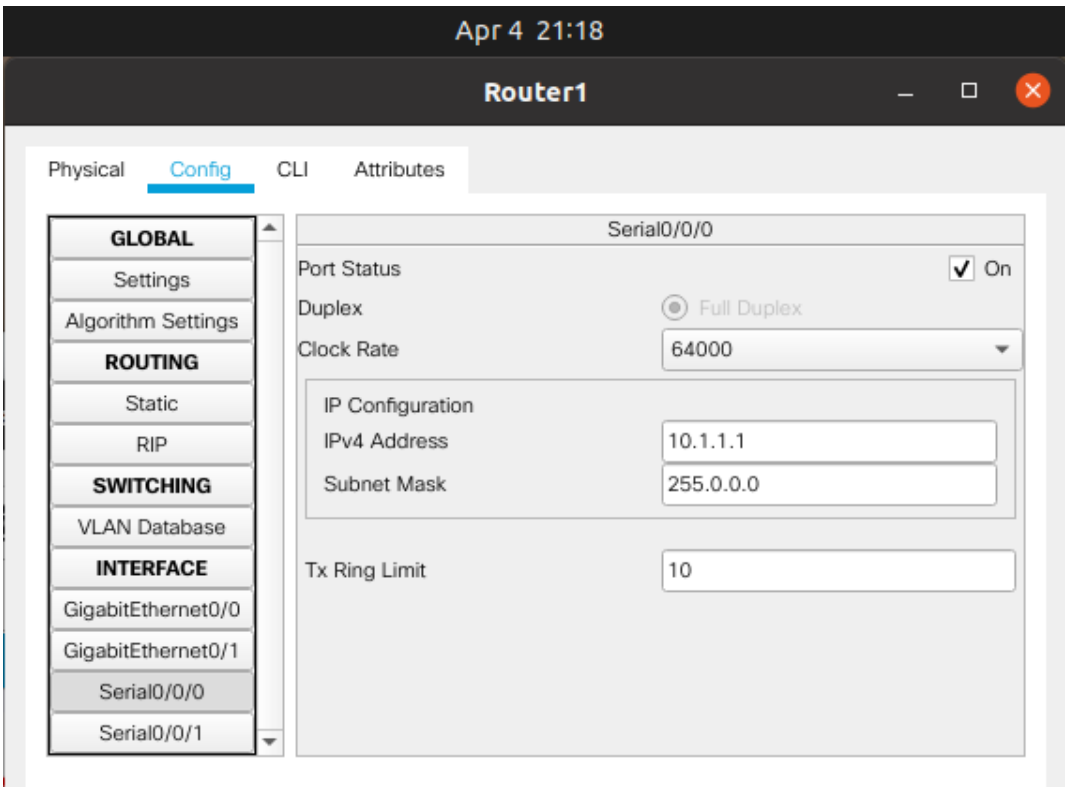


Fig.2: Router1 Serial0/0/0

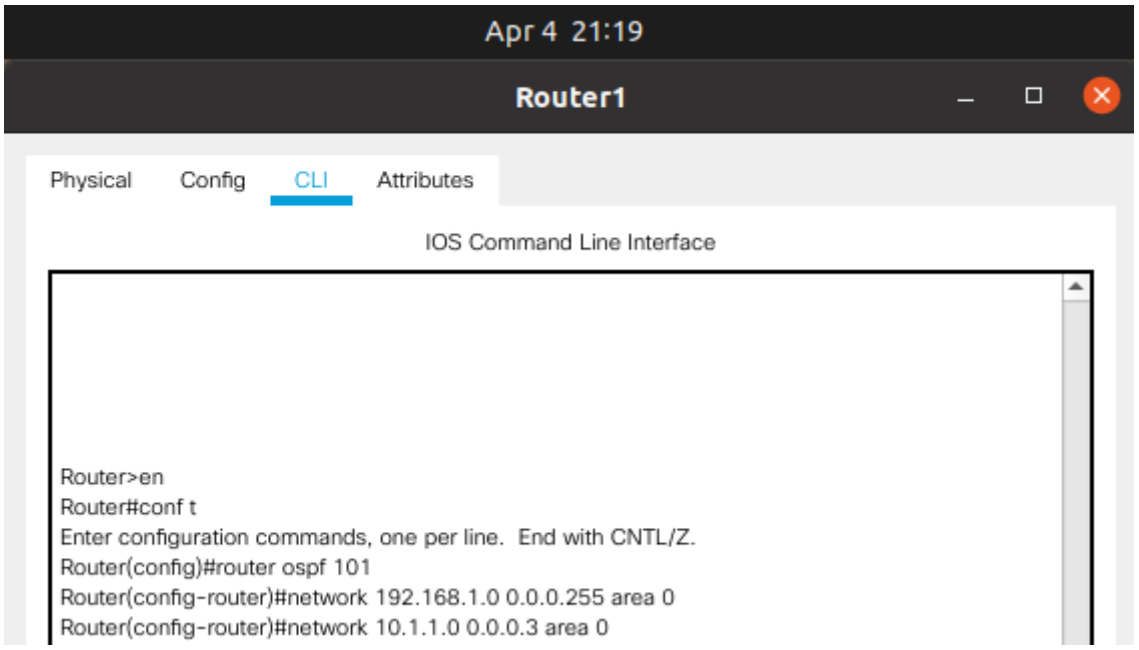


Fig.3: OSPF Routing in Router1

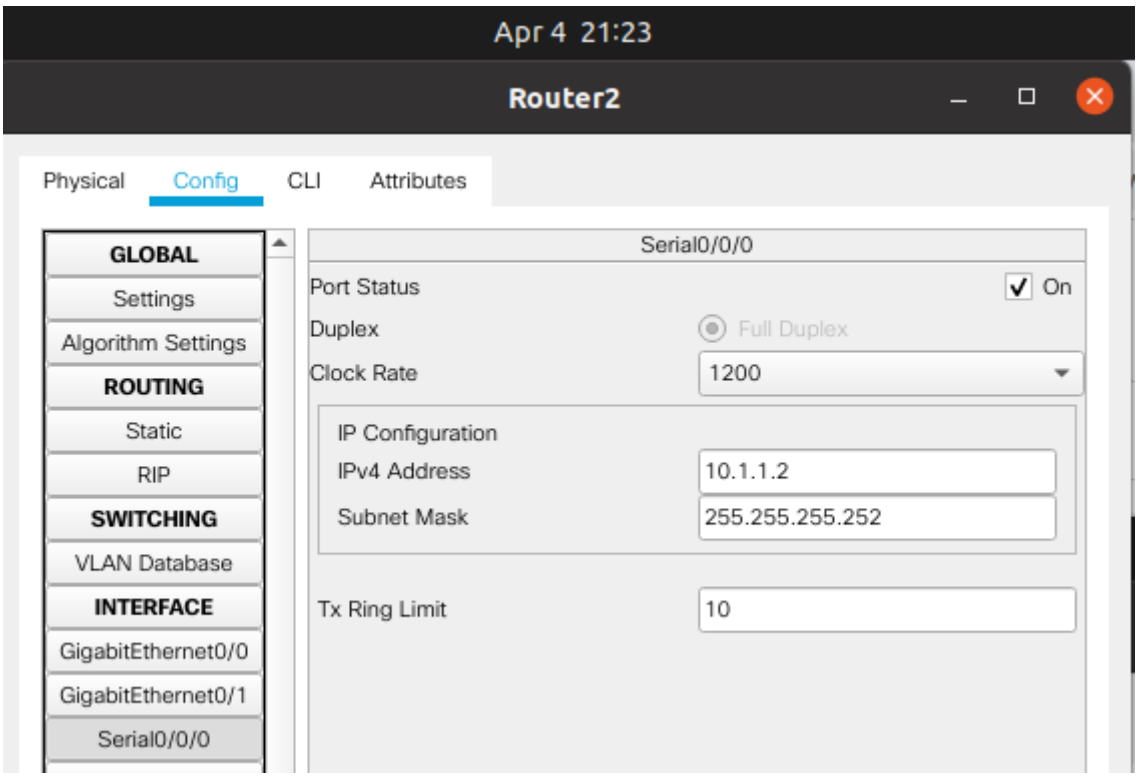


Fig.4: Router2 Serial0/0/0

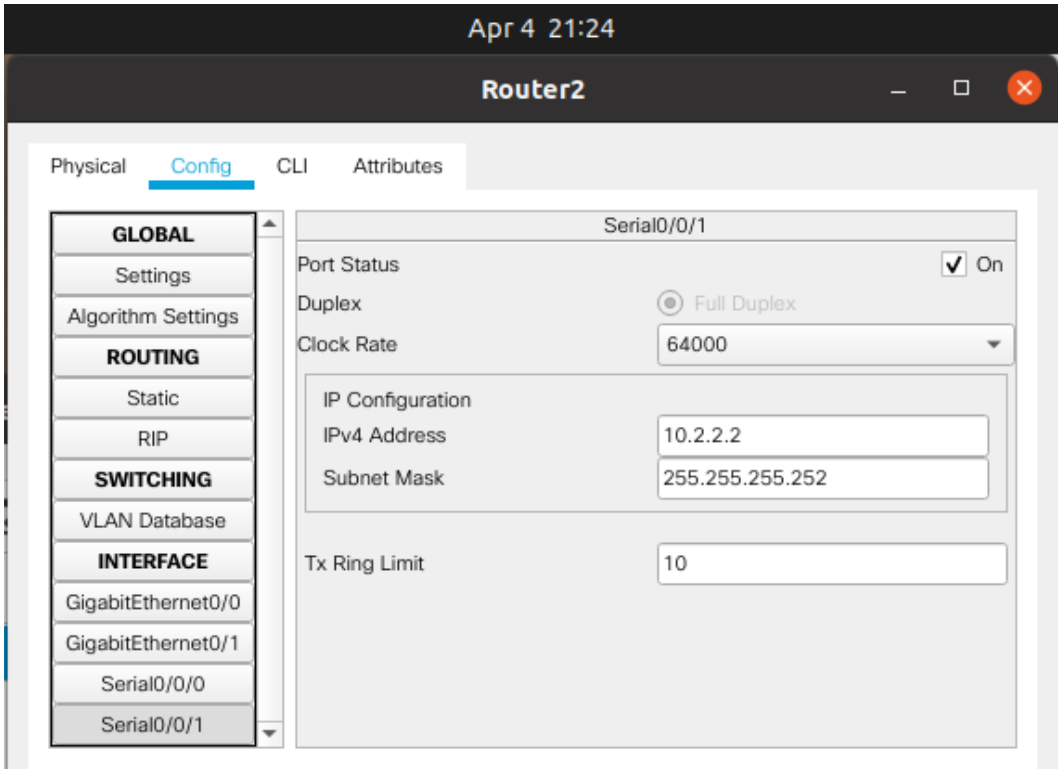


Fig.5: Router2 Serial0/0/1

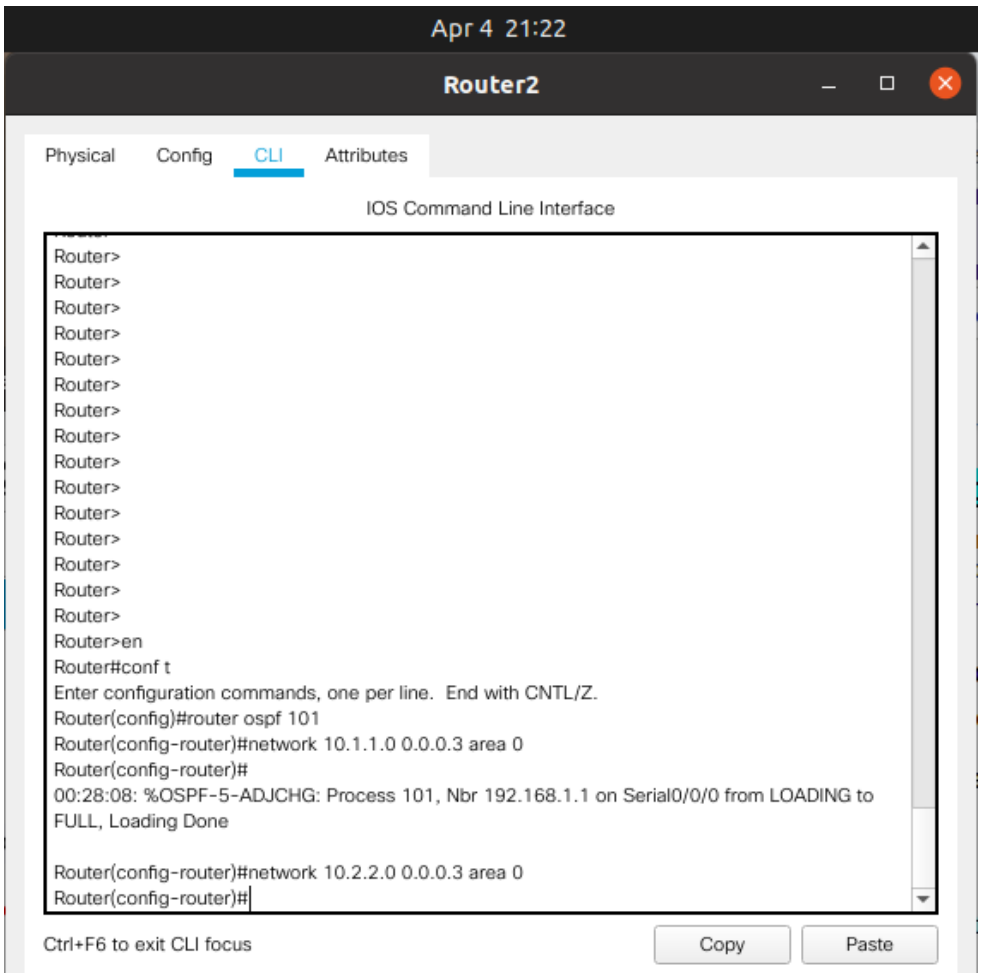


Fig.6: Router2 OSPF Routing

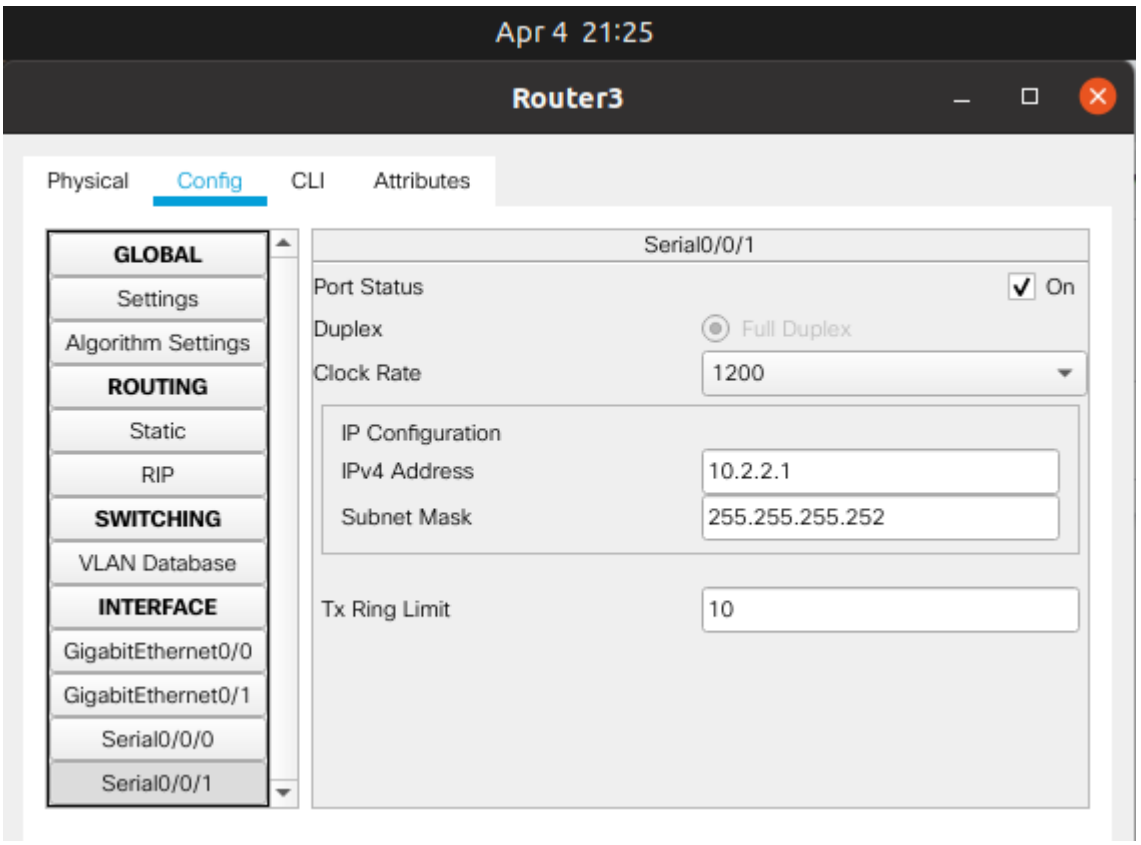


Fig.7: Router3 Serial0/0/1

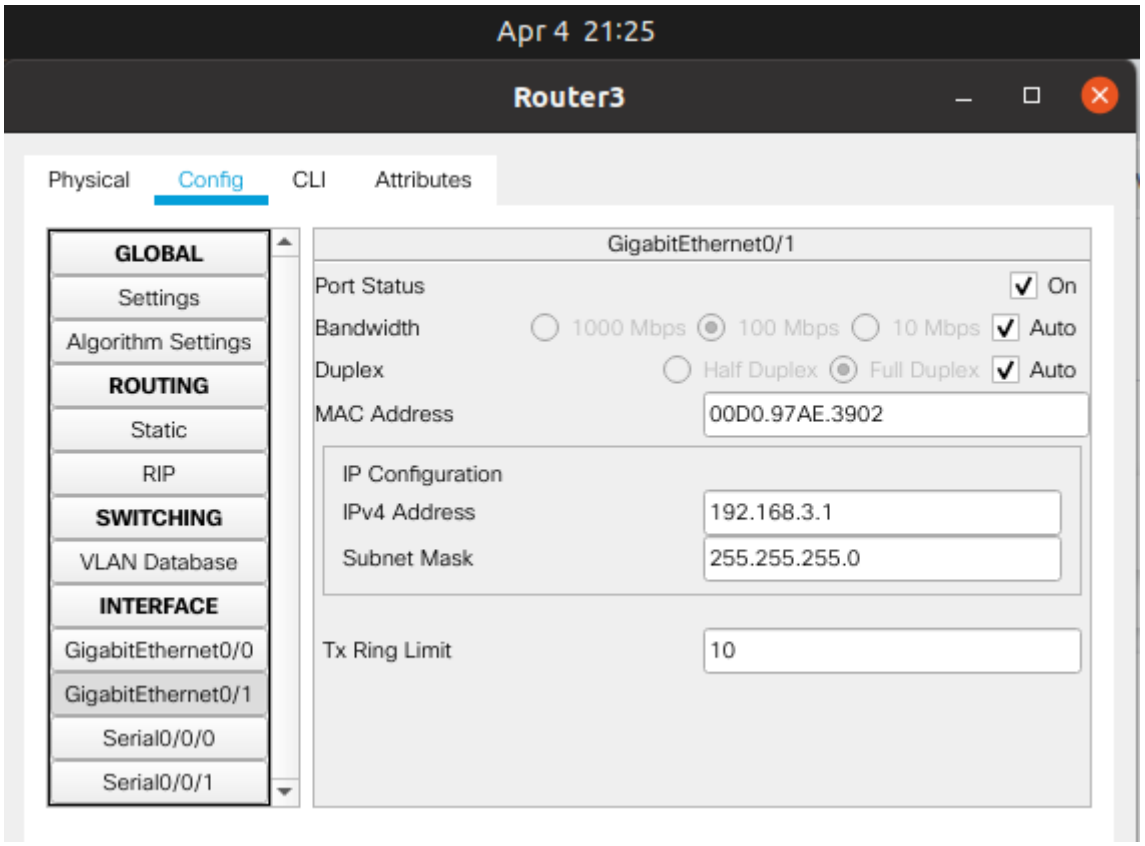


Fig.8: Router3 GigabitEthernet0/1

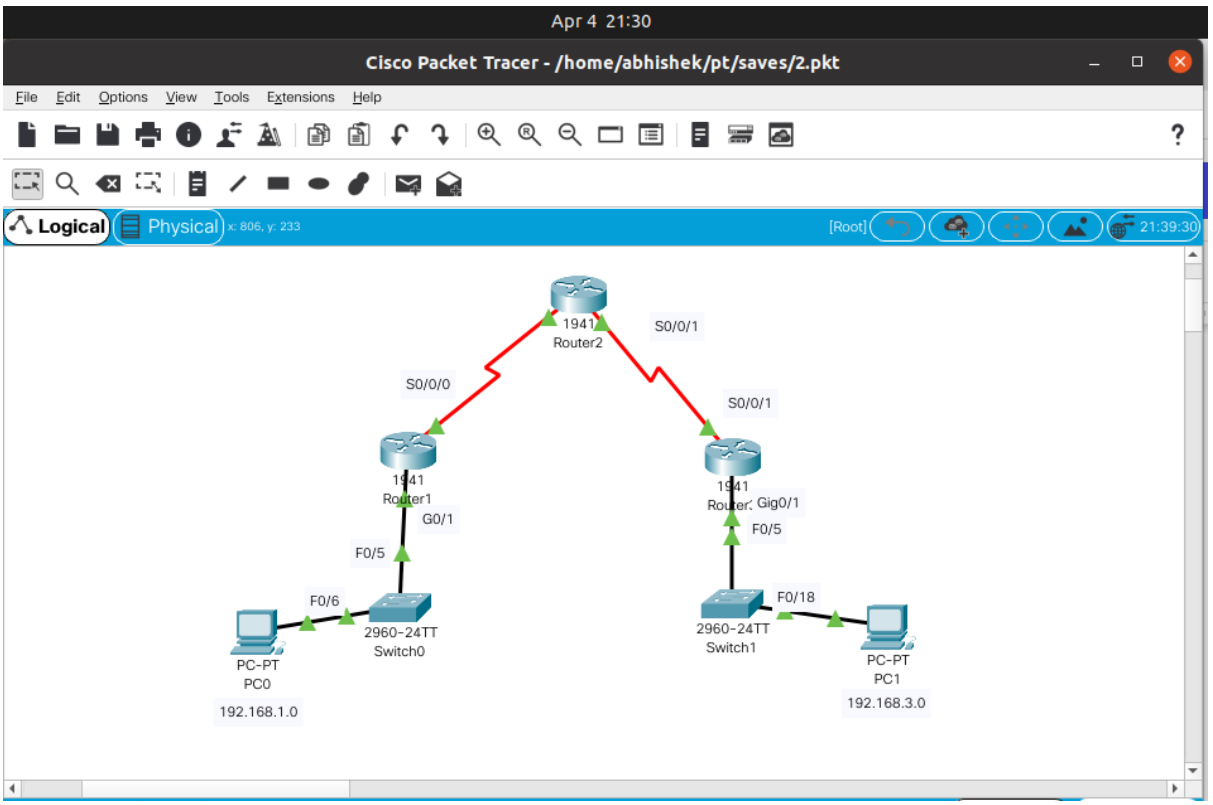


Fig.9: Connected Network topology

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	IC...		0.000	N	0	(e...	(delete)
	Successful	PC1	PC0	IC...		0.000	N	1	(e...	(delete)

Fig.10: Successful Pings from PC0 to PC1 and vice versa

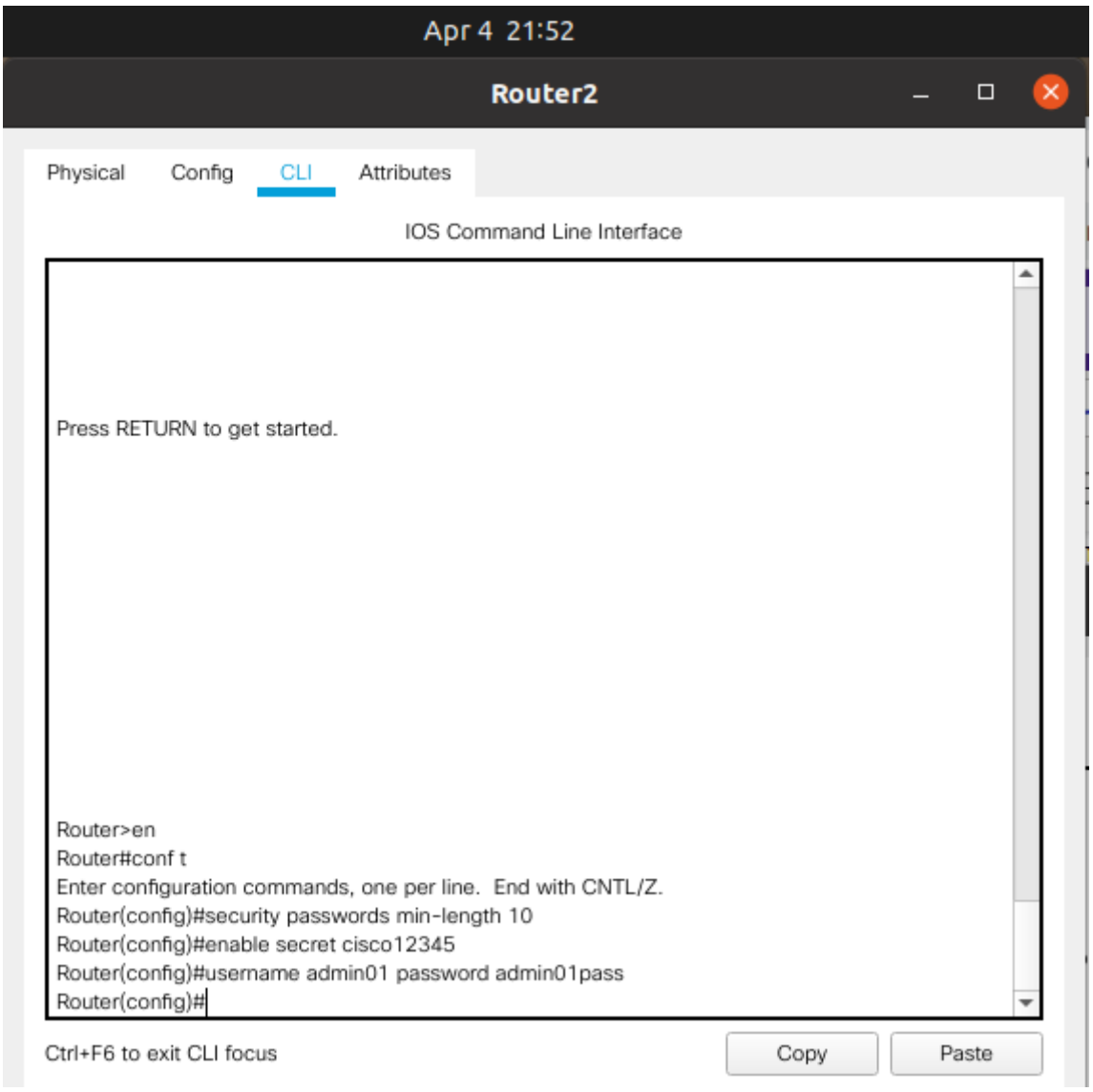


Fig.11: Configure passwords Router2

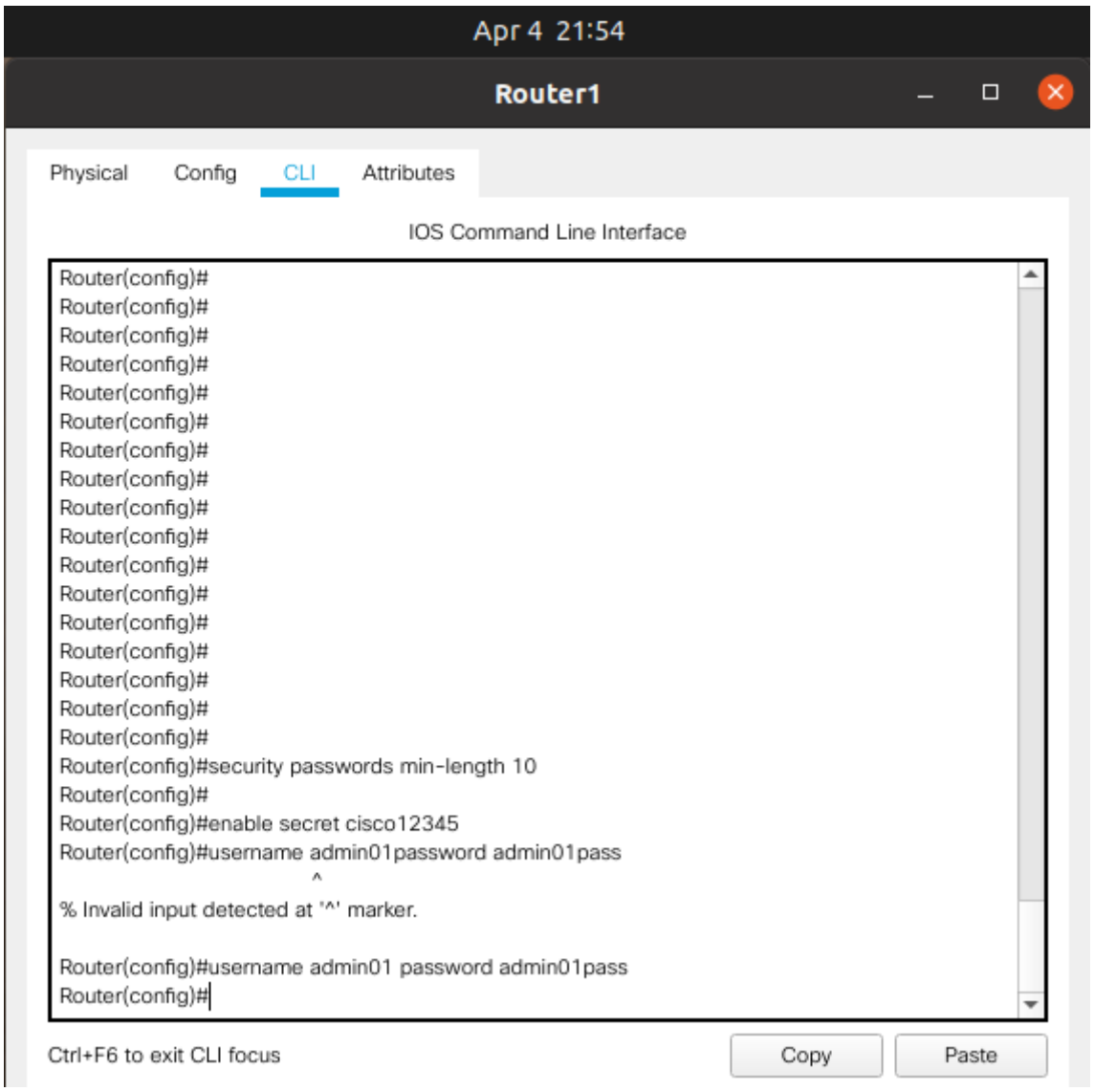


Fig.12: Configure passwords for Router1

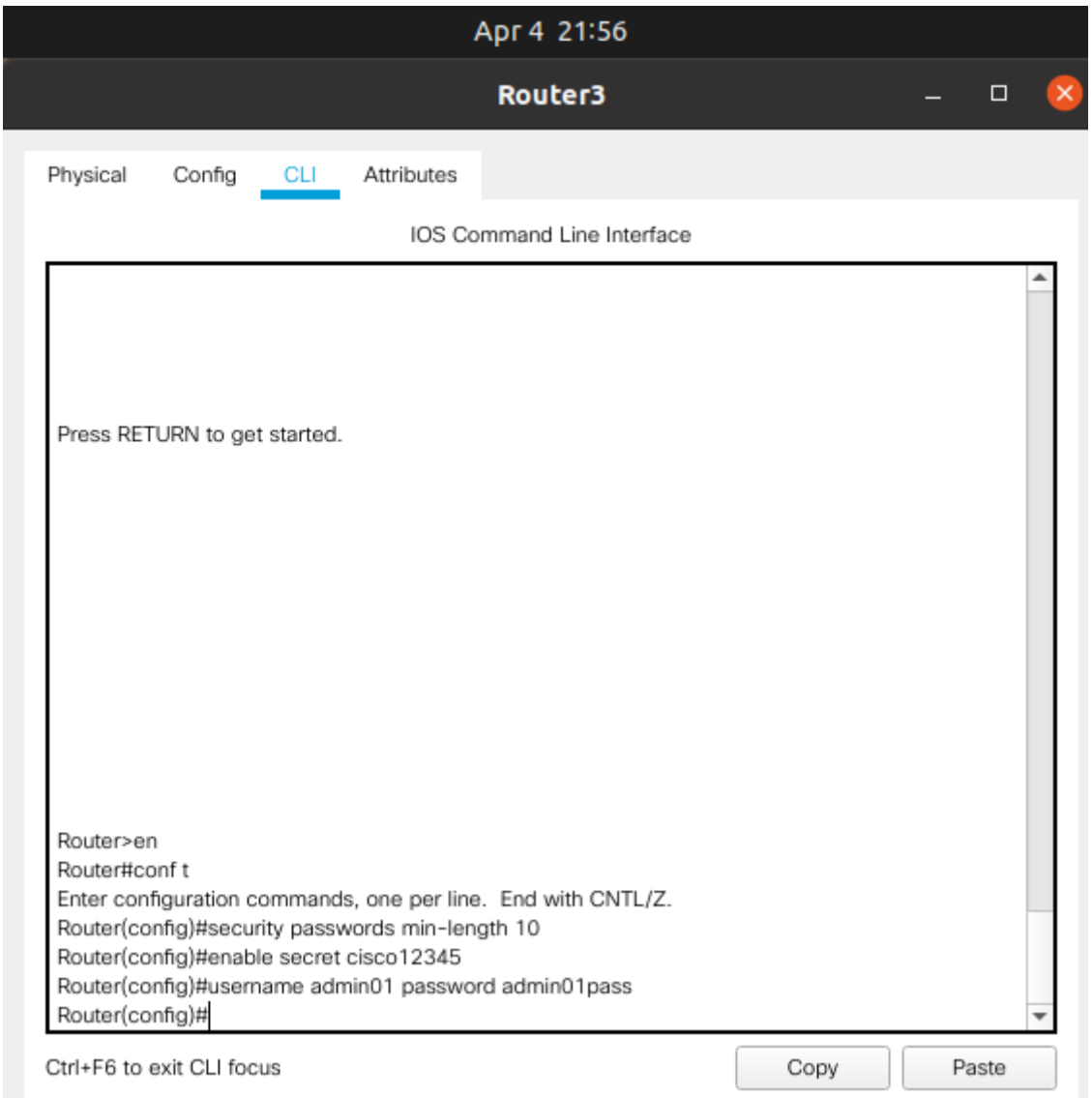


Fig.13: Configure passwords for Router3

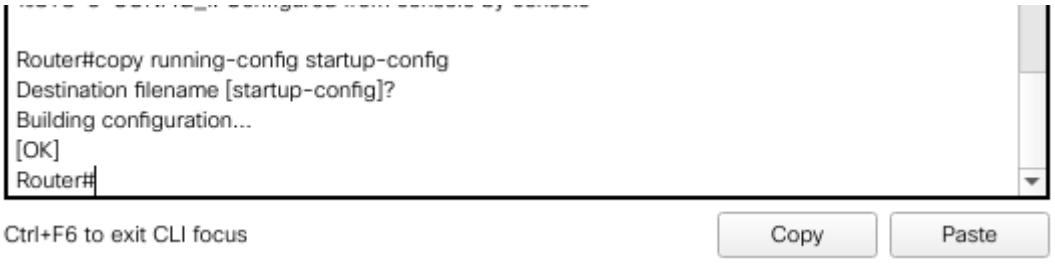


Fig.14: Saving running config for all routers

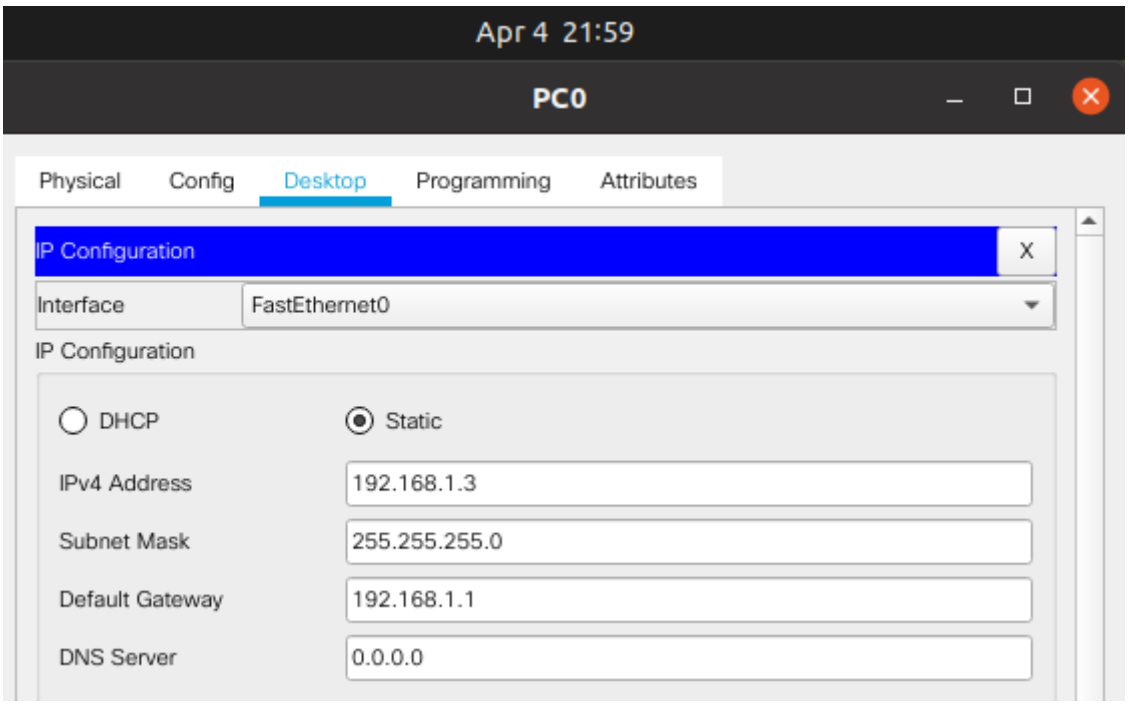


Fig.15: PC0 IP Configuration

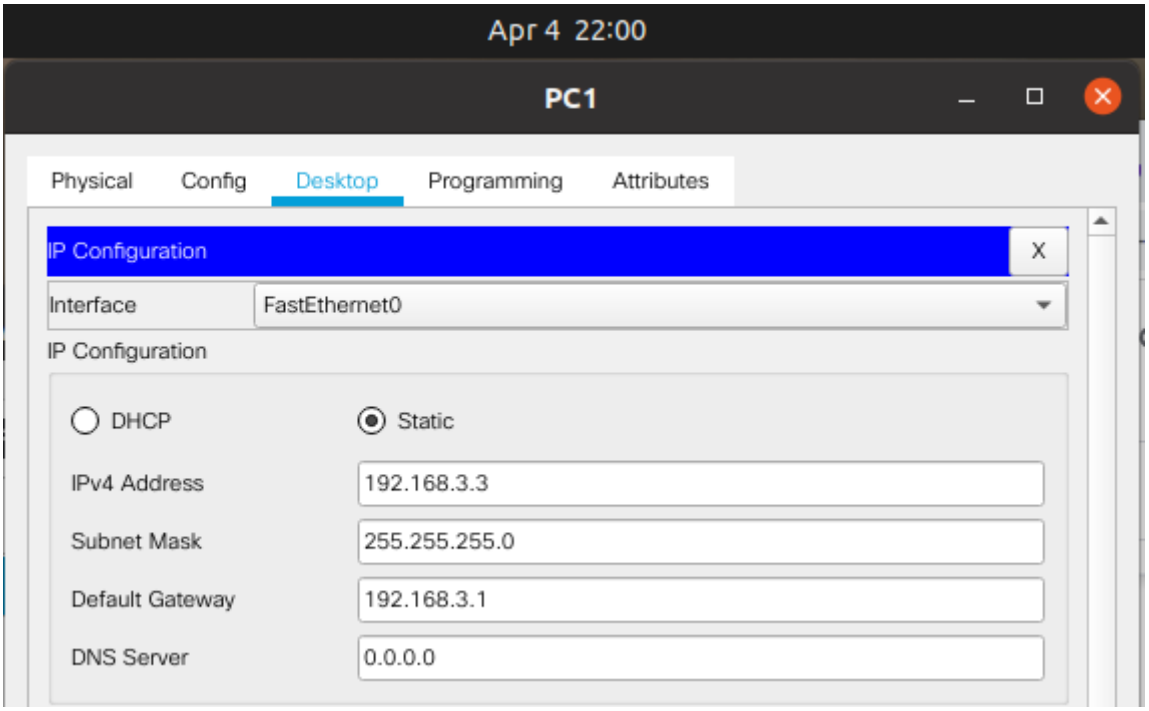


Fig.16: PC1 IP Configuration

Part2: Configure a Site-to-Site VPN with Cisco IOS

Task1: Configure IPsec VPN Settings on R1 and R3

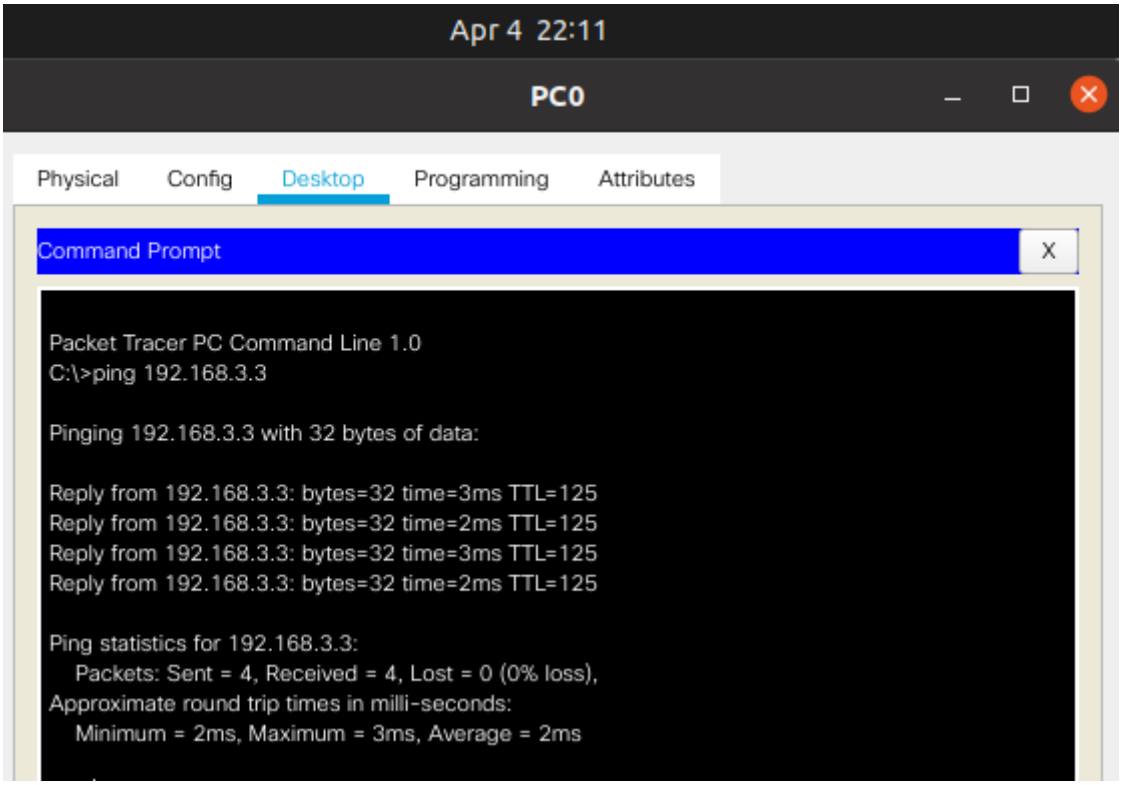


Fig.17: Verify connectivity from the R1 LAN to the R3 LAN.

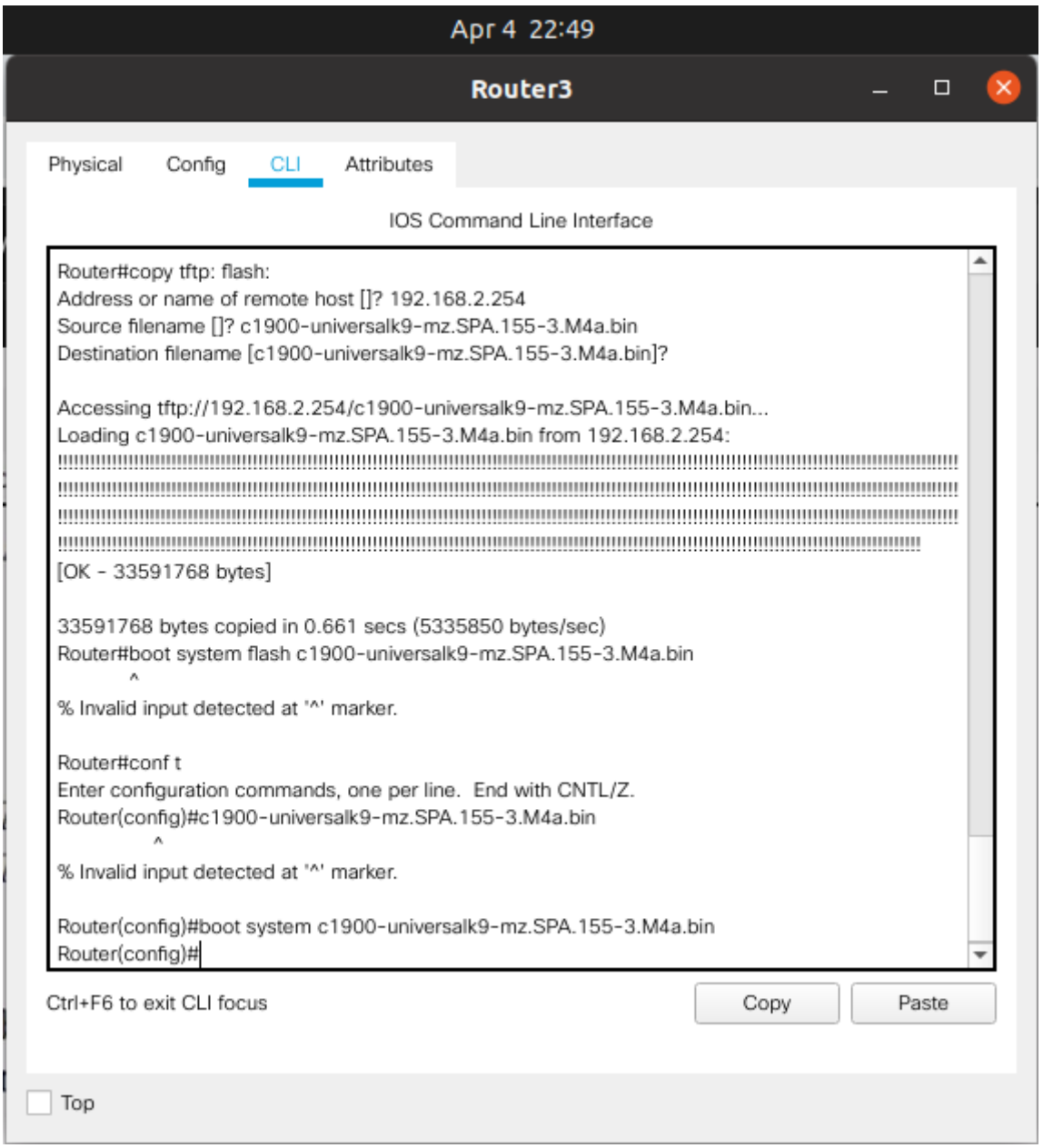


Fig.18:Update IOS Image using TFTP server

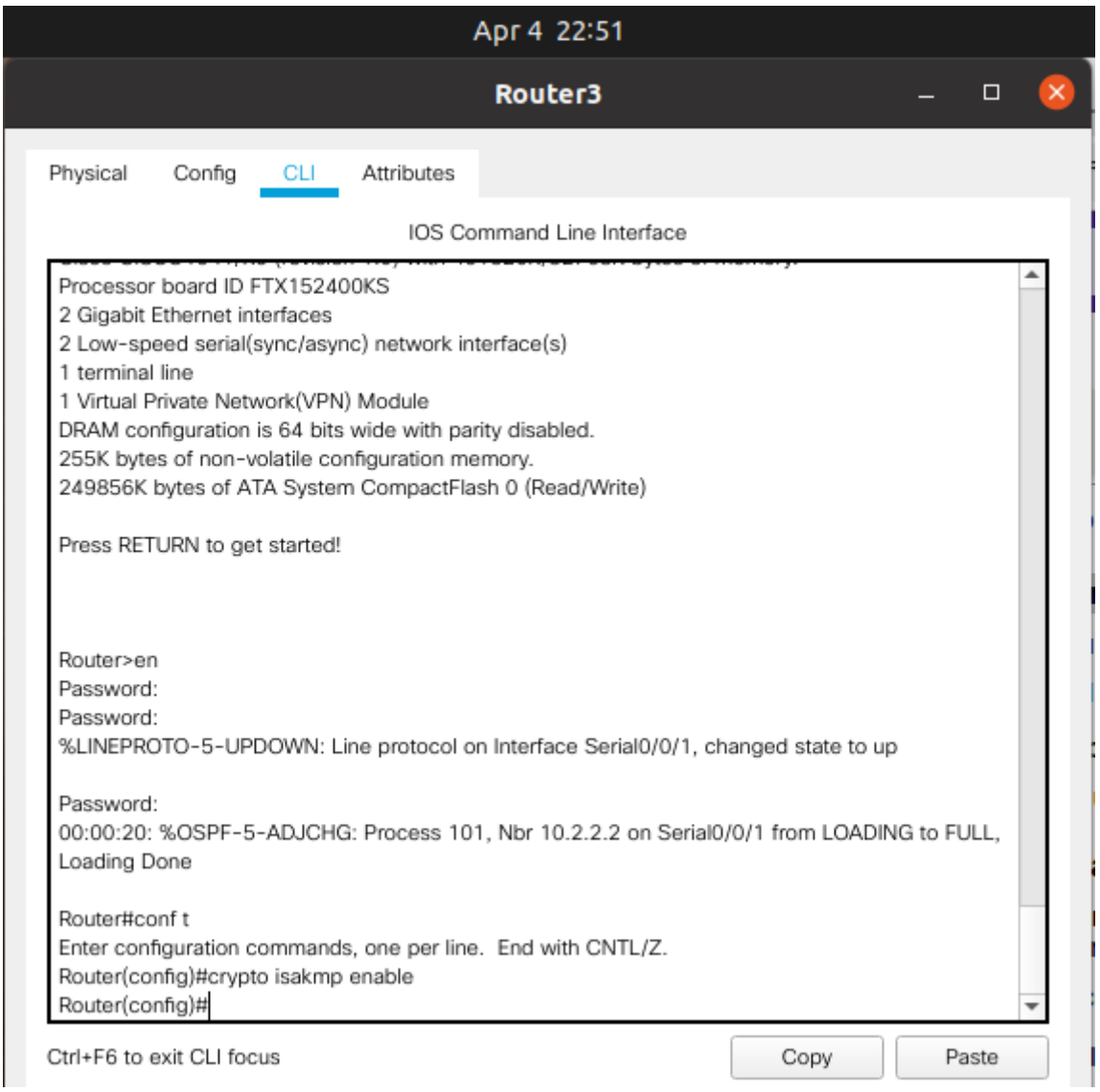


Fig.19: Check if crypto isakmp enable in Router3

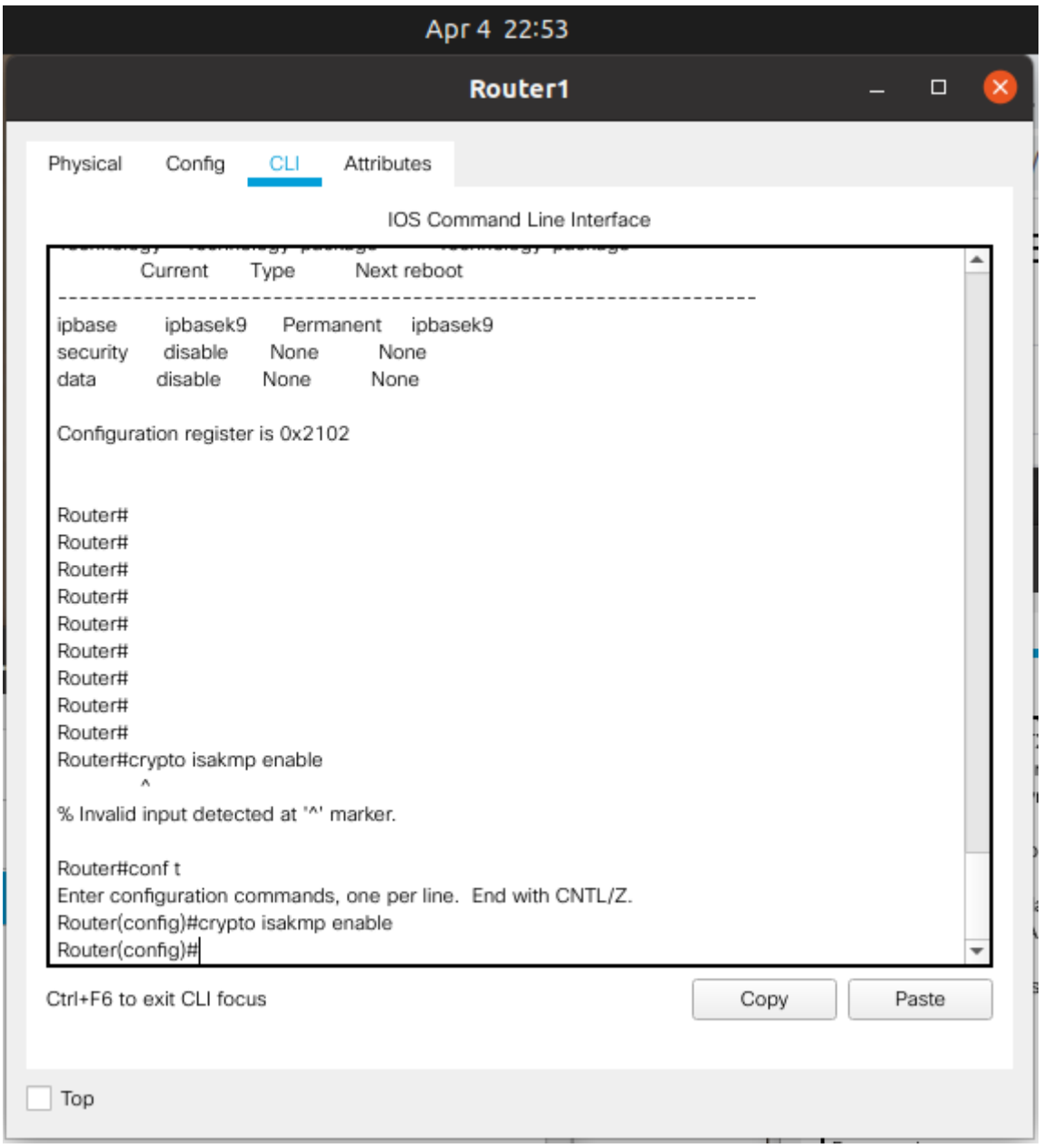


Fig.20: Check if crypto isakmp Router1

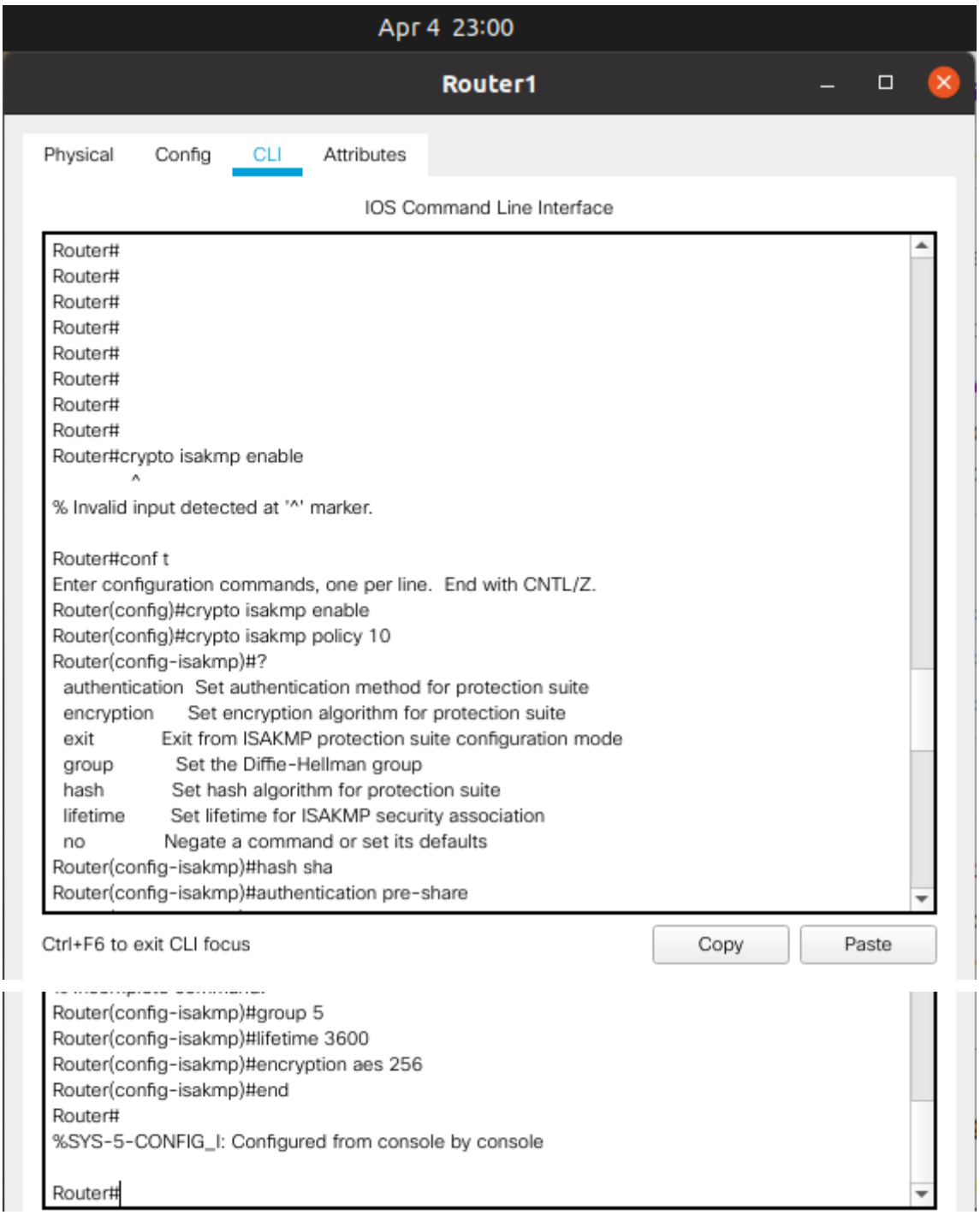


Fig.21: Configure the IKE Phase 1 ISAKMP policy on R1.

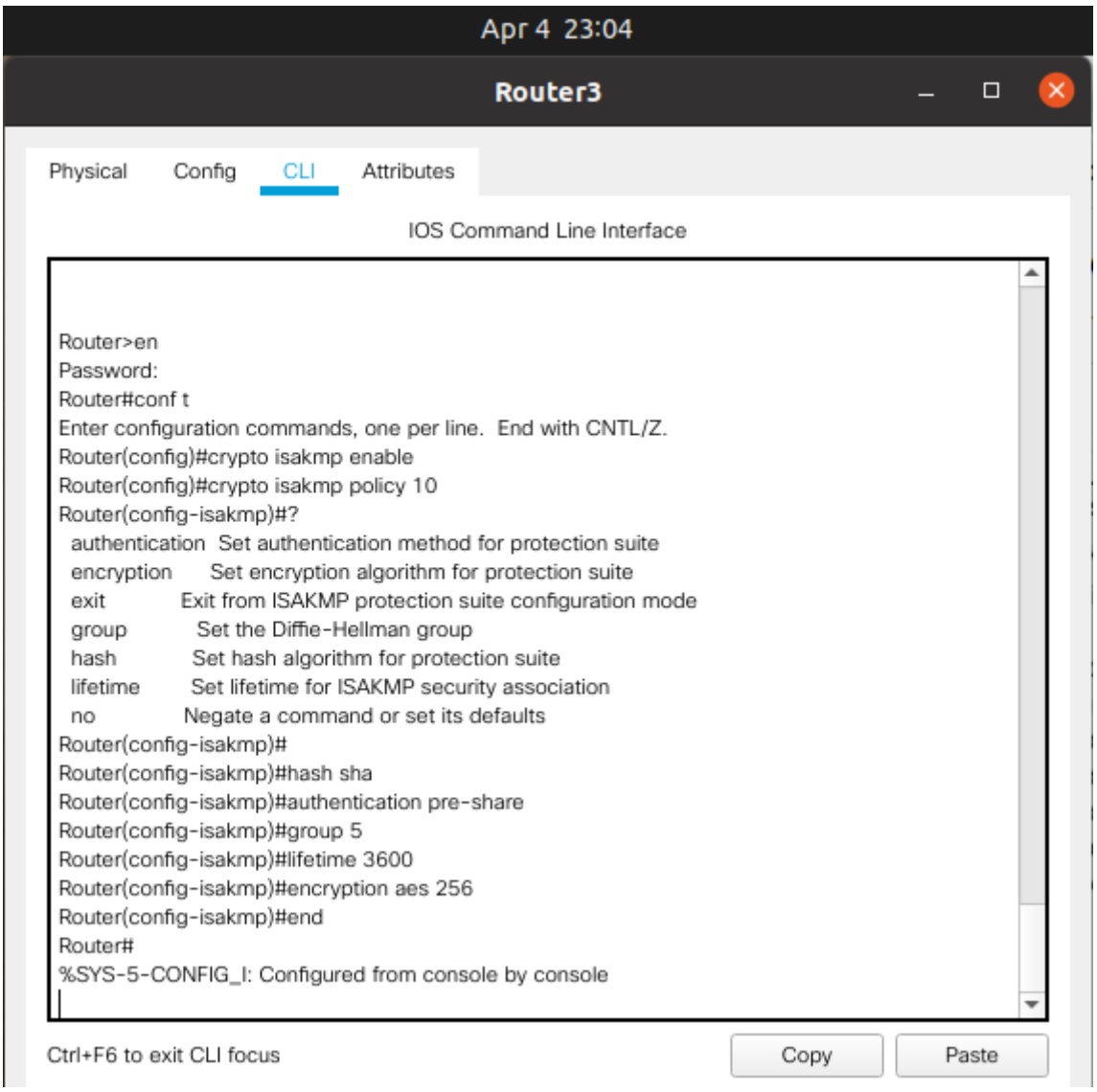


Fig.22: Configure the IKE Phase 1 ISAKMP policy on R3.

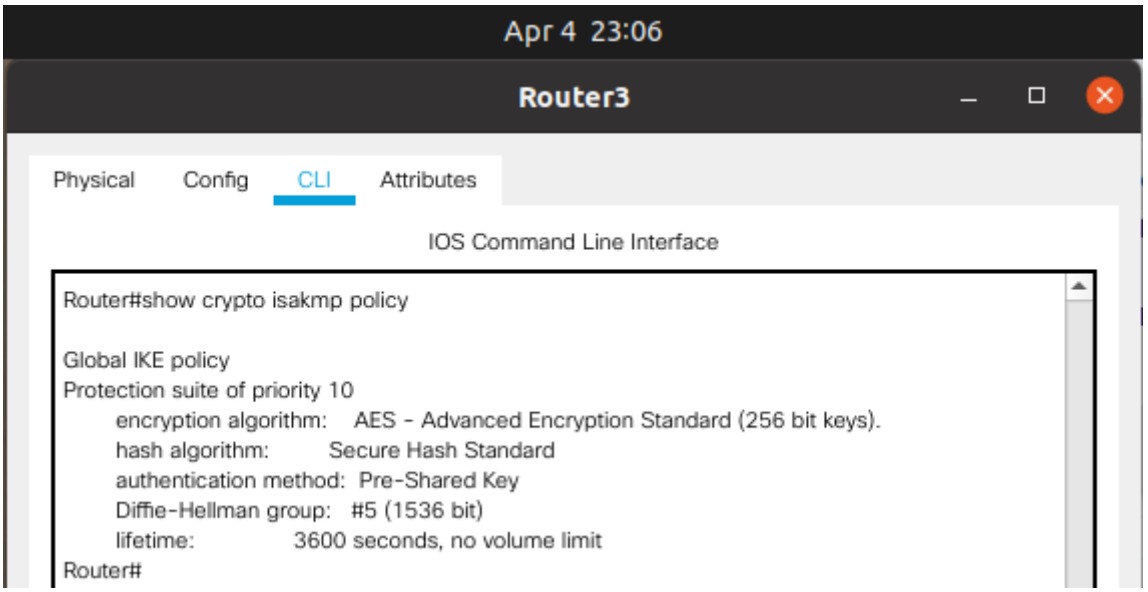


Fig.23: crypto isakmp policy in Router3

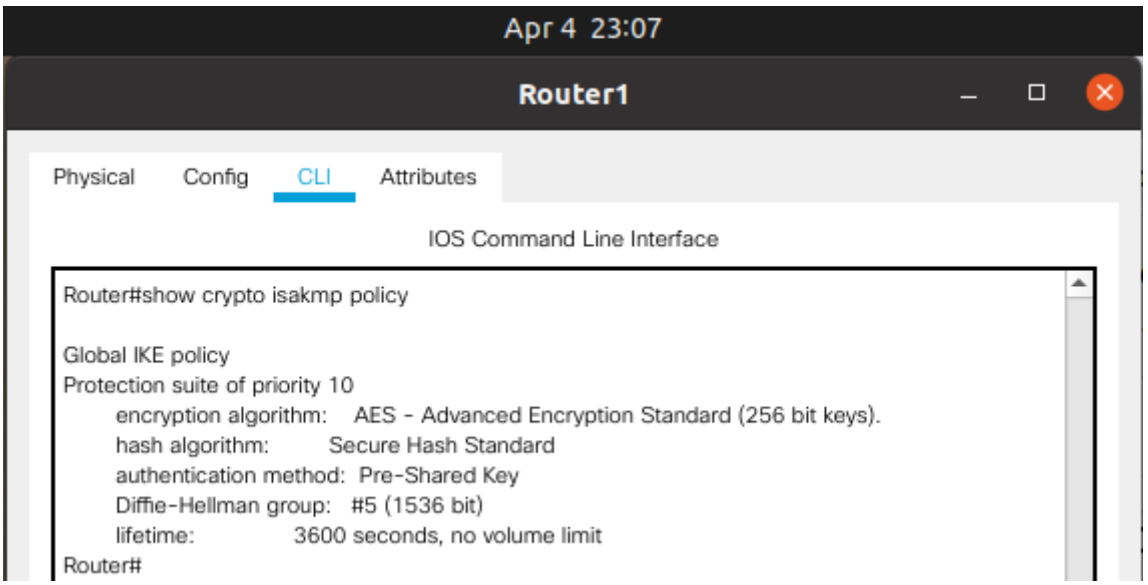


Fig.24: crypto isakmp policy in Router1

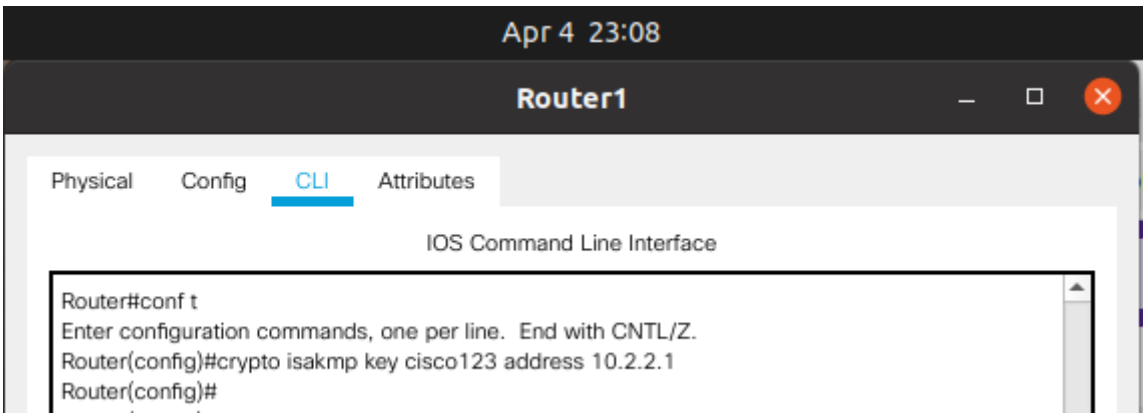


Fig.25: Configuring pre-shared keys on Router1

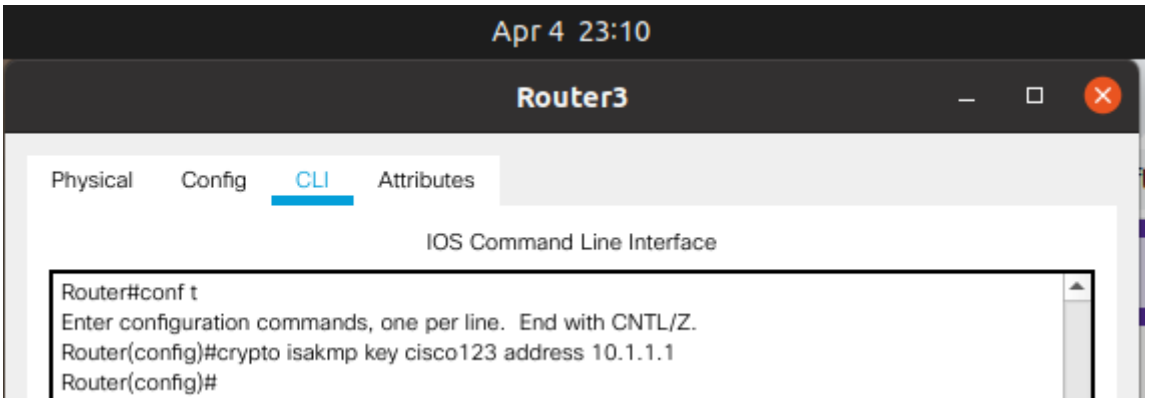


Fig.26: Configuring pre-shared keys on Router3

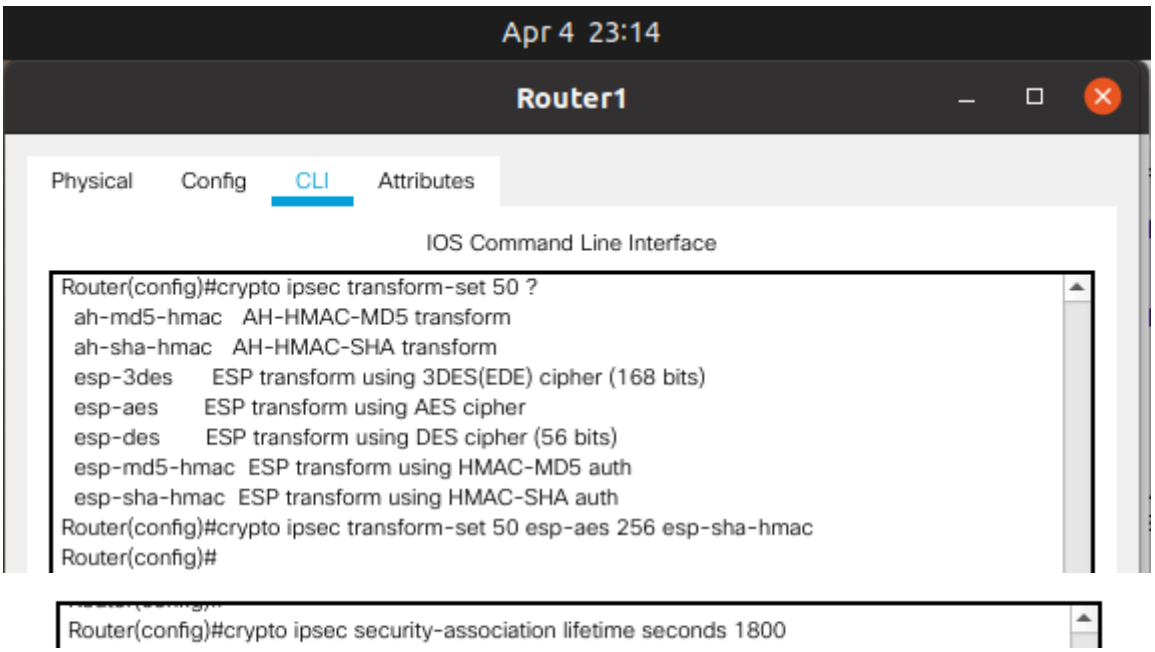


Fig.27: Configuring the IPsec transform set and lifetime in Router1

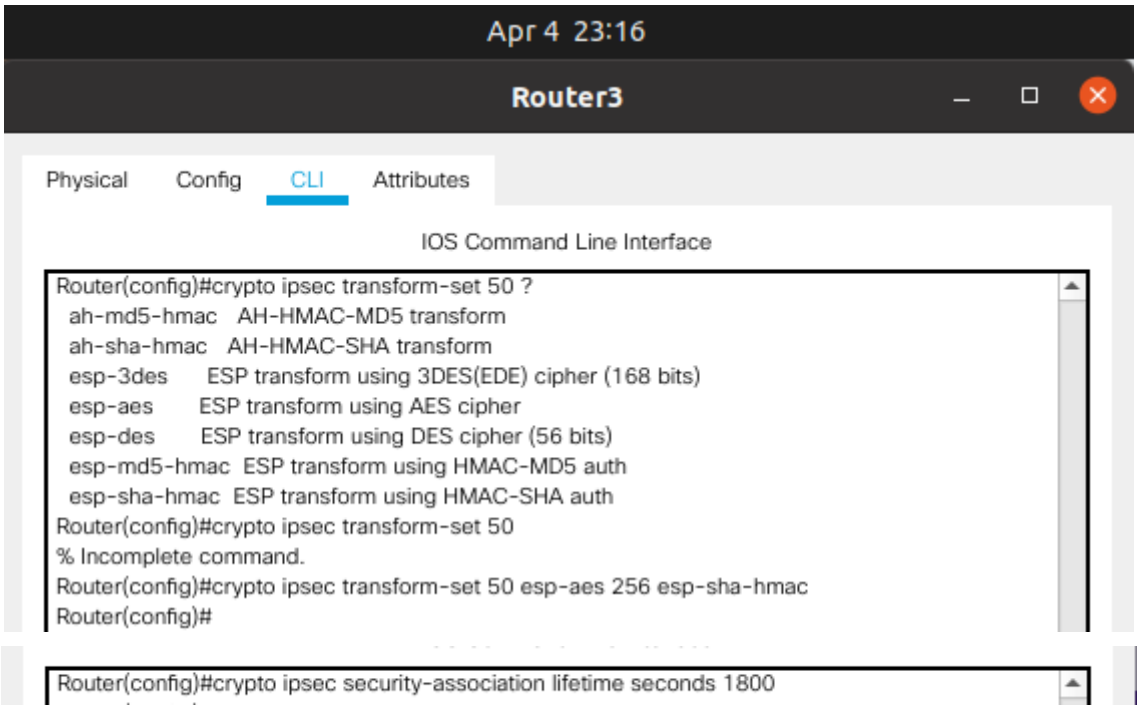


Fig.28: Configuring the IPsec transform set and lifetime in Router3

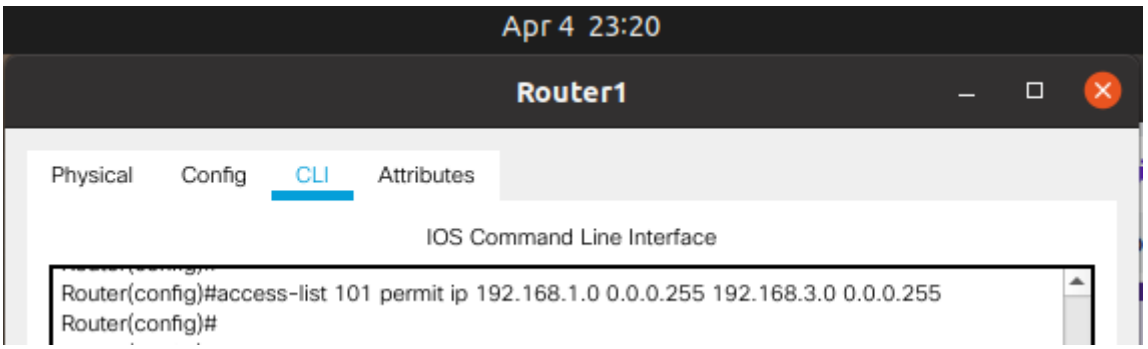


Fig.29: Configure the IPsec VPN interesting traffic ACL on Router1.

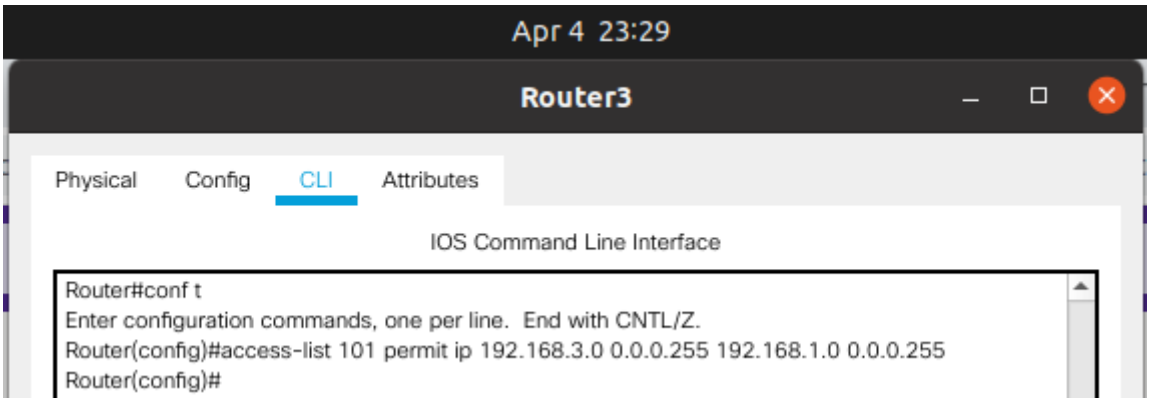


Fig.30: Configure the IPsec VPN interesting traffic ACL on Router3.

Apr 4 23:35

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set ?
  peer               Allowed Encryption/Decryption peer.
  pfs                Specify pfs settings
  security-association  Security association parameters
  transform-set      Specify list of transform sets in priority order
Router(config-crypto-map)#set peer 10.2.2.1
Router(config-crypto-map)#set pfs ?
  group1  D-H Group1 (768-bit modp)
  group2  D-H Group2 (1024-bit modp)
  group5  D-H Group5 (1536-bit modp)
  <cr>
Router(config-crypto-map)#set pfs
Router(config-crypto-map)#set pfs group5
Router(config-crypto-map)#set transform-set 50
Router(config-crypto-map)#set security-association lifetime seconds 900
Router(config-crypto-map)#exit
Router(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

Apr 4 23:42

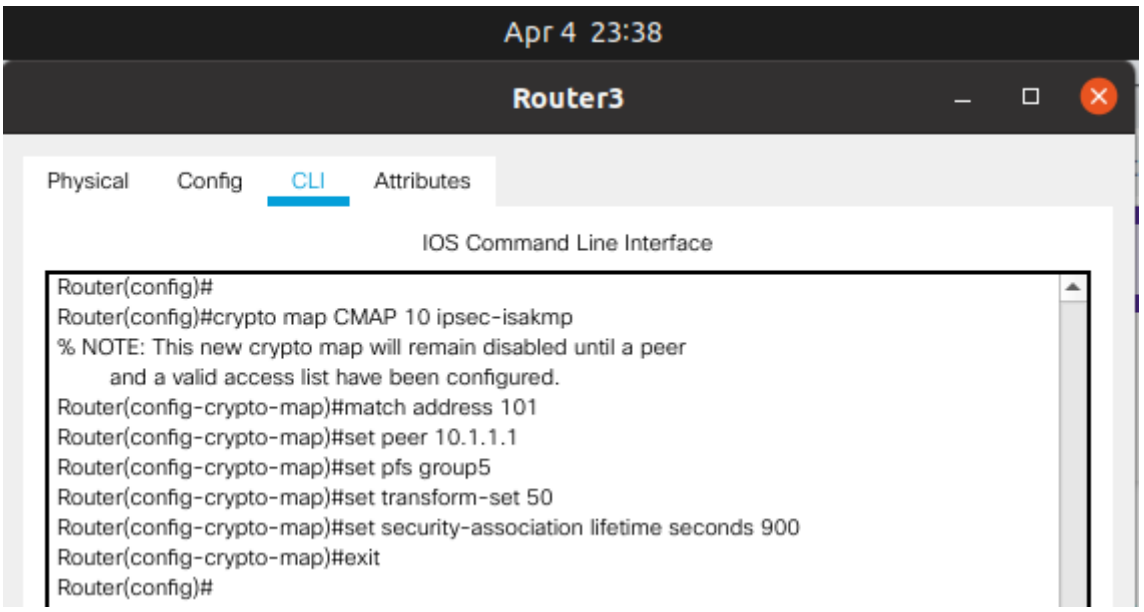
Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#interface S0/0/0
Router(config-if)#crypto map CMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Fig.31: Creating and applying a crypto map to Router1



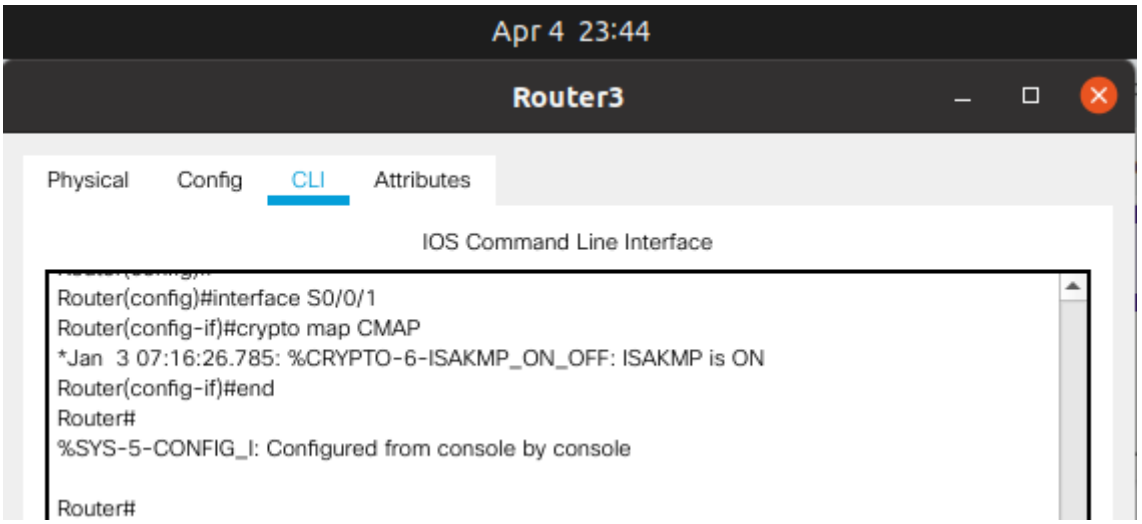


Fig.32: Creating and applying a crypto map to Router3

Task2: Verify the Site-to-Site IPsec VPN Configuration.

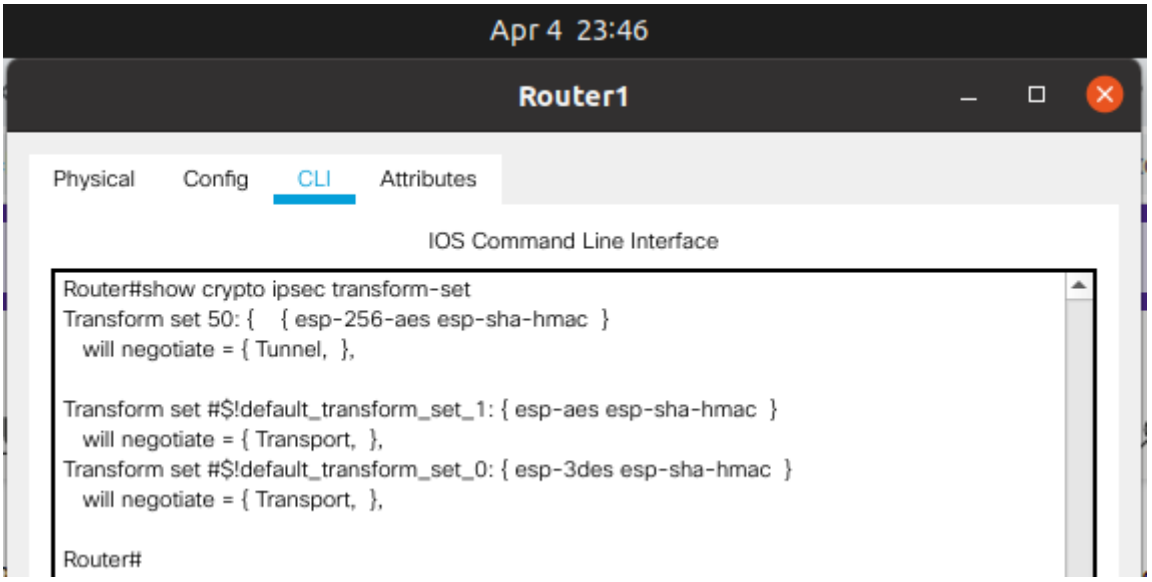


Fig.33: show crypto ipsec transform-set in Router1

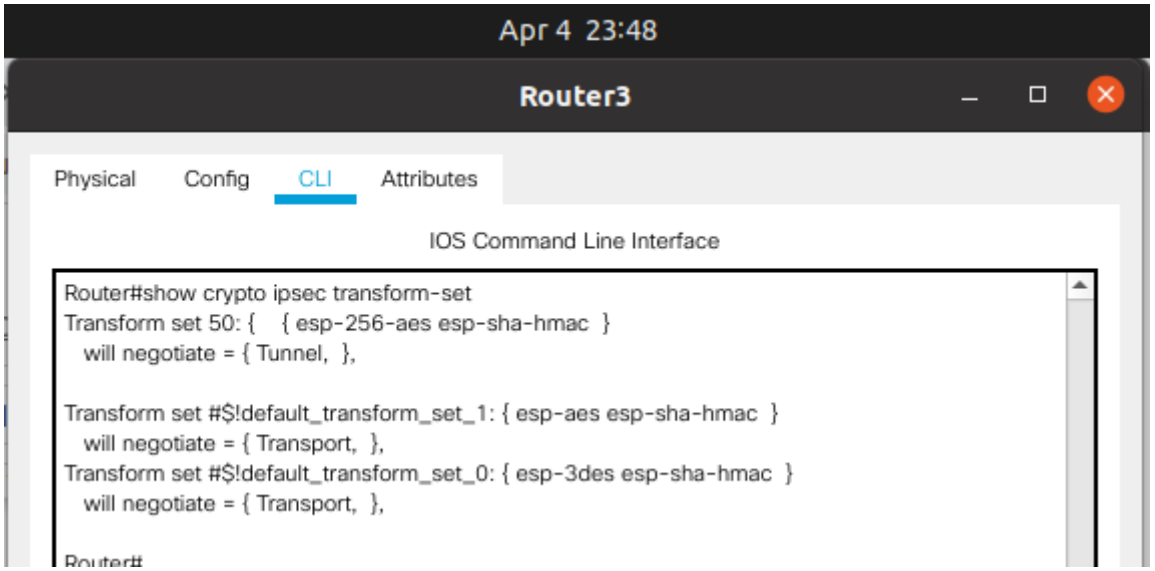


Fig.34: show crypto ipsec transform-set in Router3

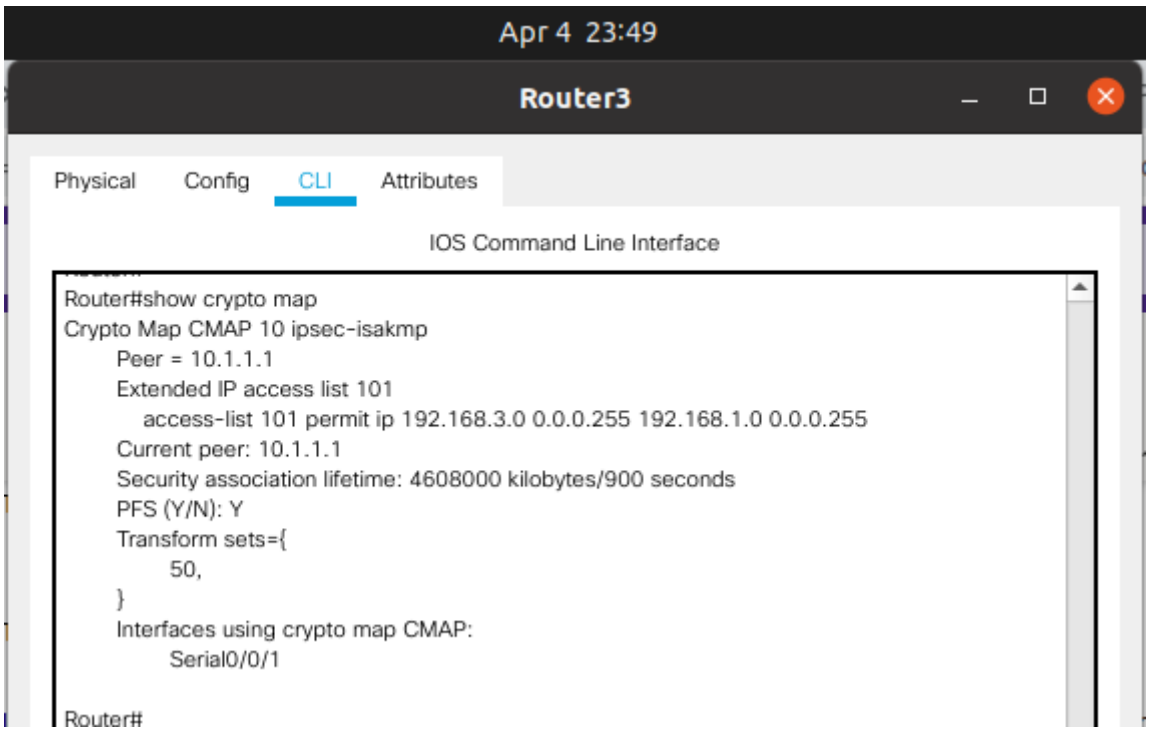


Fig.35: show crypto map command in Router3

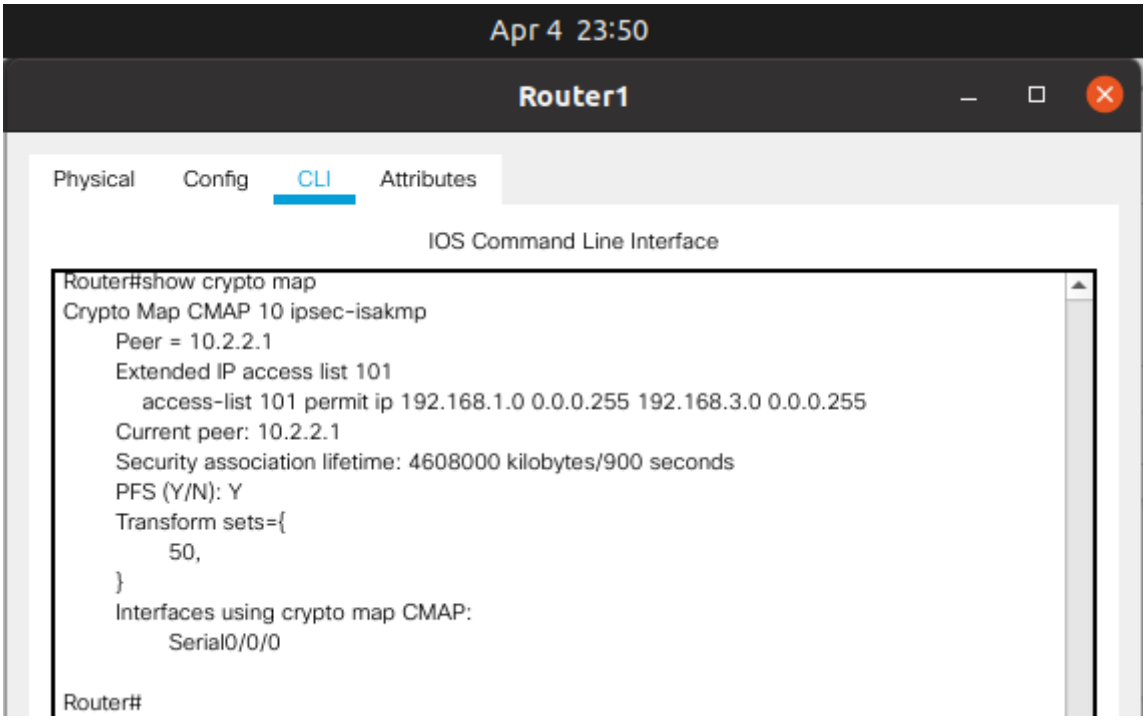


Fig.36: show crypto map command in Router1

Task3: Verify the IPsec VPN Operation.

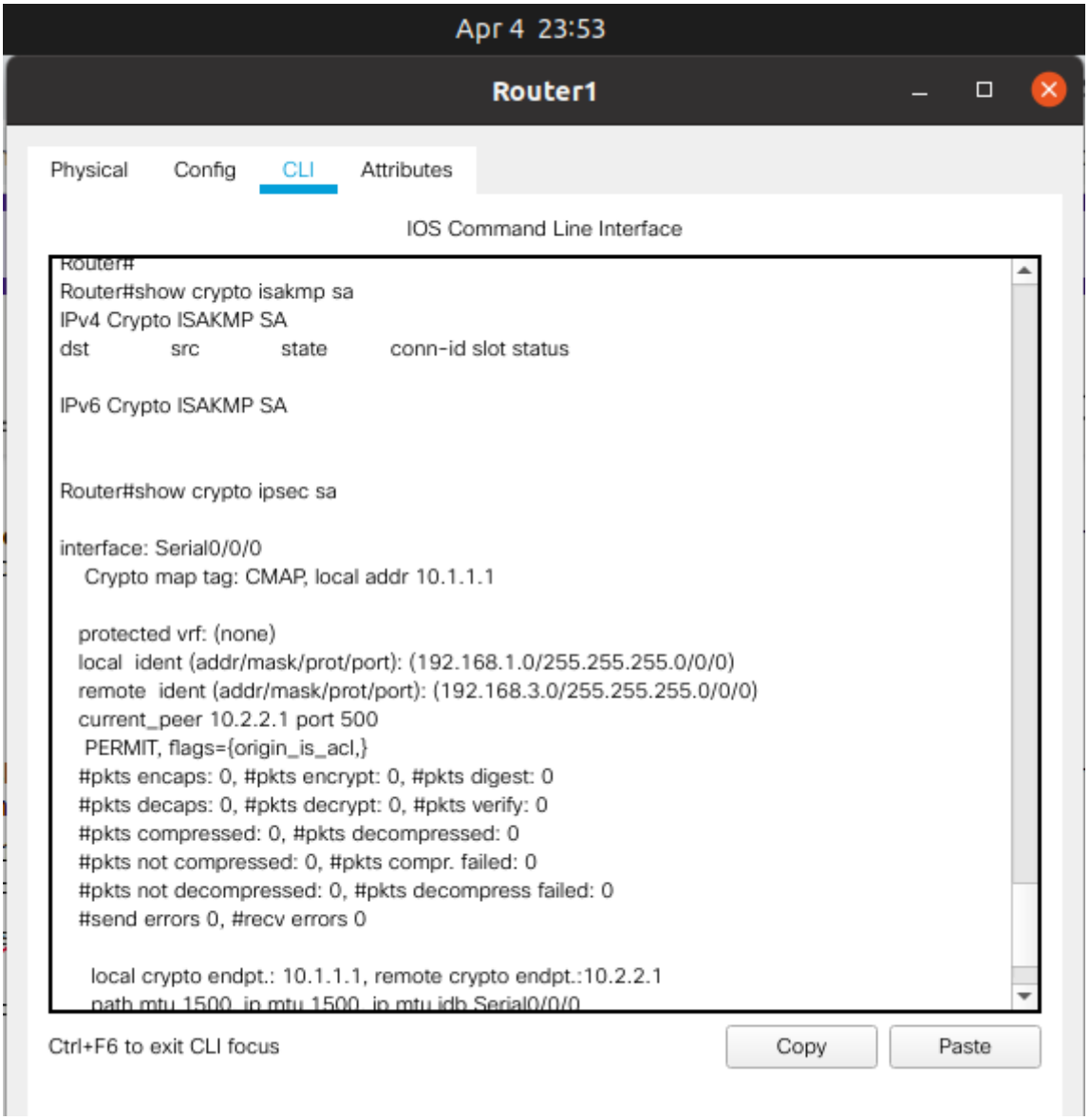
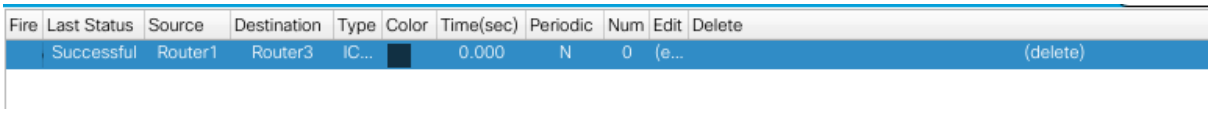
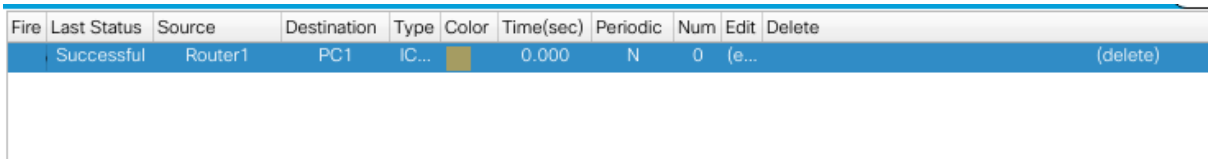


Fig.37: Display ISAKMP and IPsec security associations for Router1



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router1	Router3	IC...		0.000	N	0	(e...	(delete)

Fig.38: Ping from R1 to the R3 S0/0/1 interface IP address 10.2.2.1. These pings are successful.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router1	PC1	IC...		0.000	N	0	(e...	(delete)

Fig.39: Ping from R1 to the R3 G0/1 interface IP address 192.168.3.1. These pings are successful.

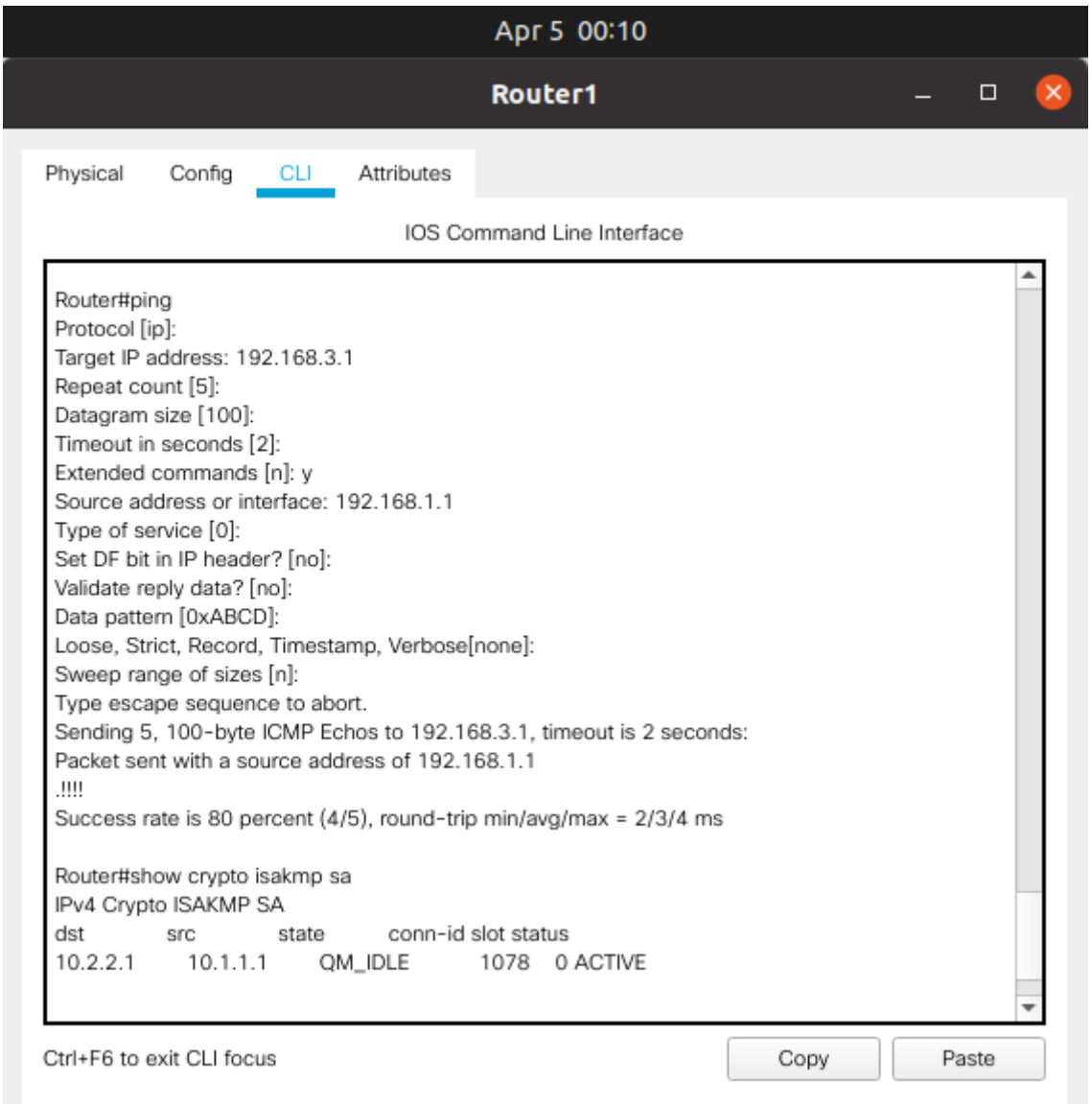


Fig.40: Generate some interesting test traffic and observe the results.

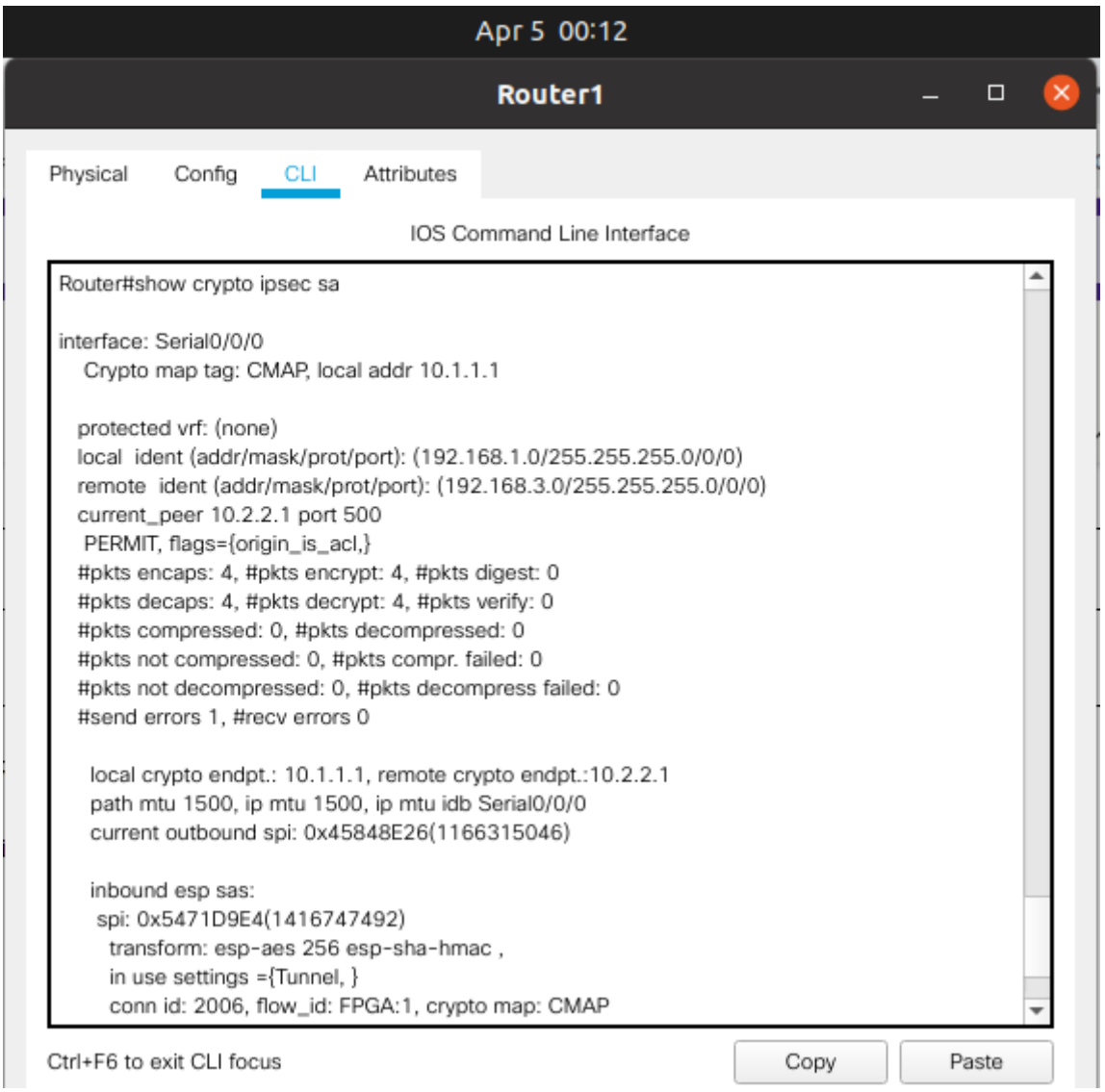


Fig.41: show crypto ipsec sa from Router1