UNIVERSIDAD POLITECNICA
DE SAN LUIS POTOSI

ACTIVIDAD 06
IPSec VPN

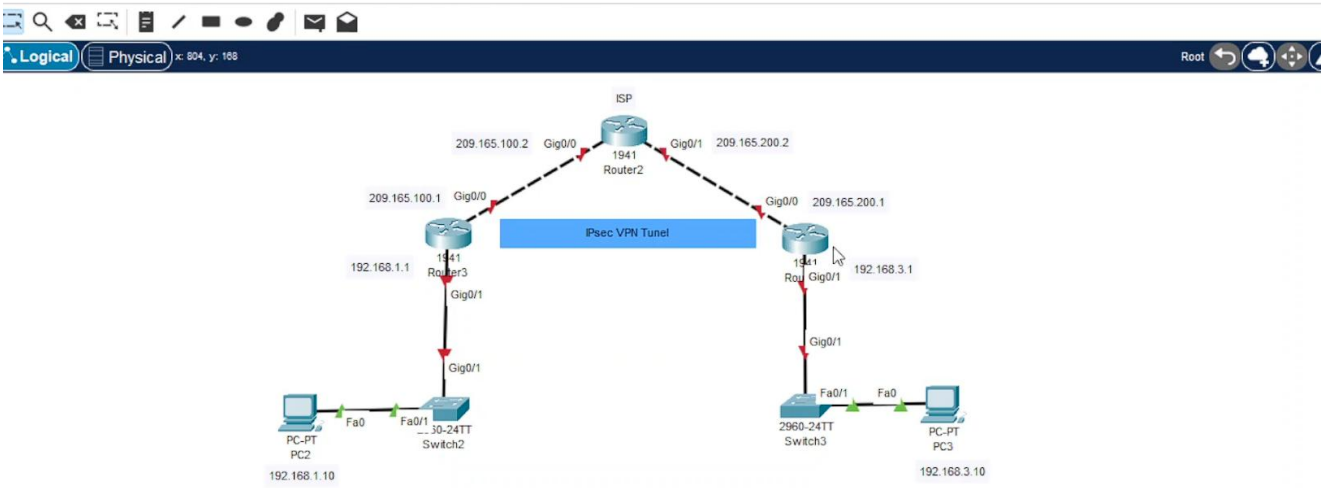
Contenido

Introducción

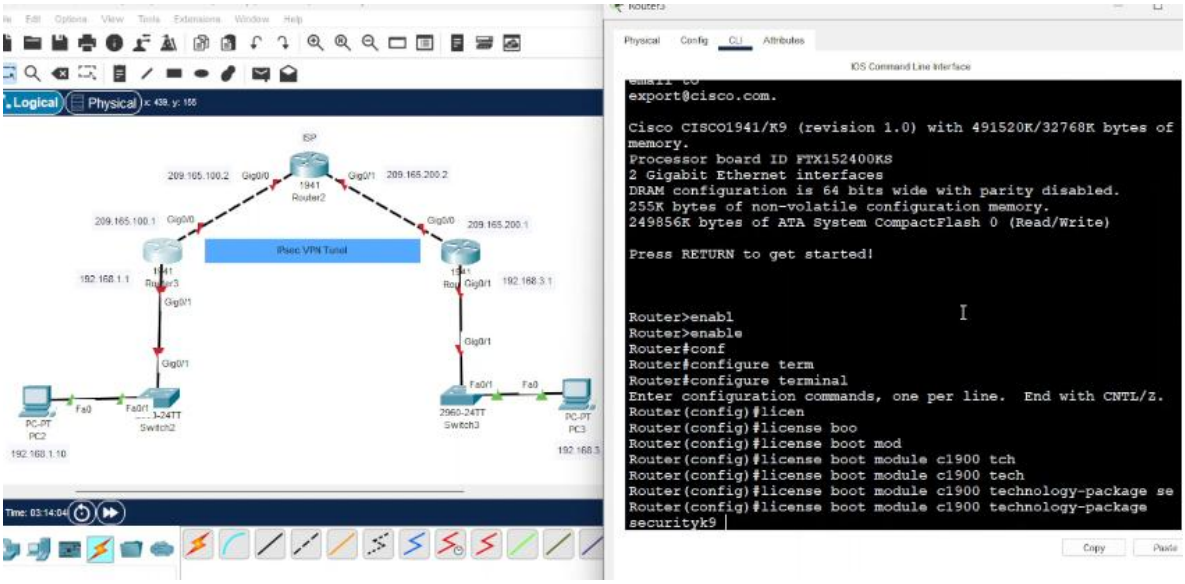
En esta actividad se demostrarán las habilidades adquiridas del alumno para montar una implementación IPSec VPN en un entorno cerrado haciendo uso de la herramienta de redes conocida como Cisco Packet Tracer.

Construcción de la topología

En packet tracer se realiza la siguiente topología y la asignación de Ip’s



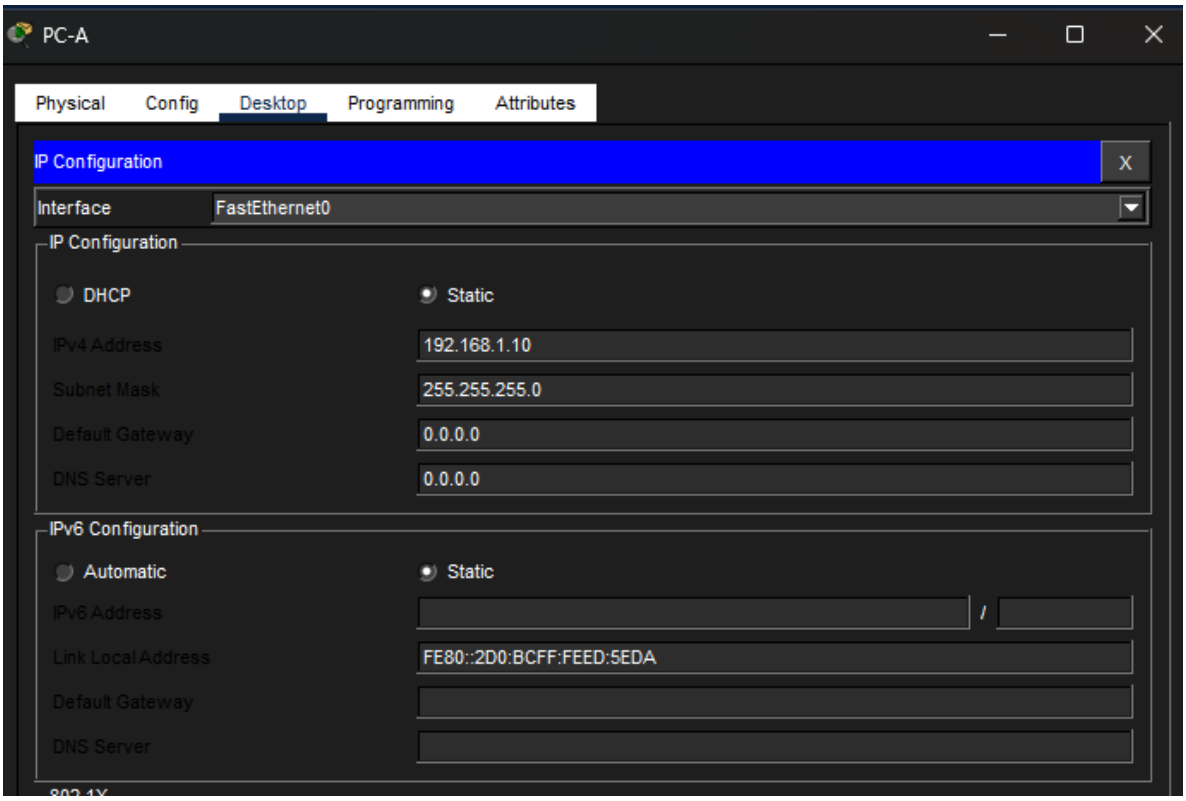
Habilitar Paquete de seguridad

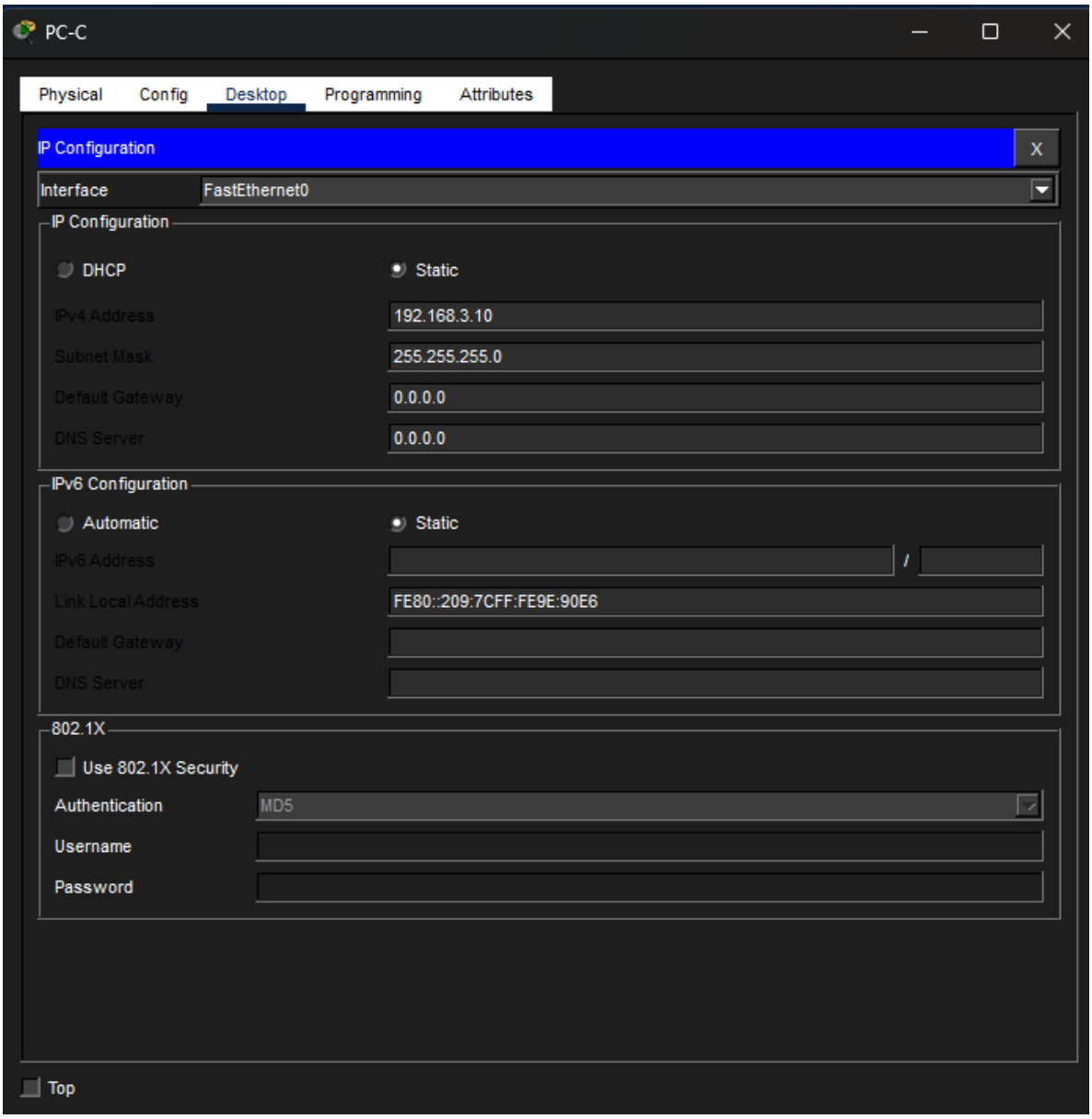


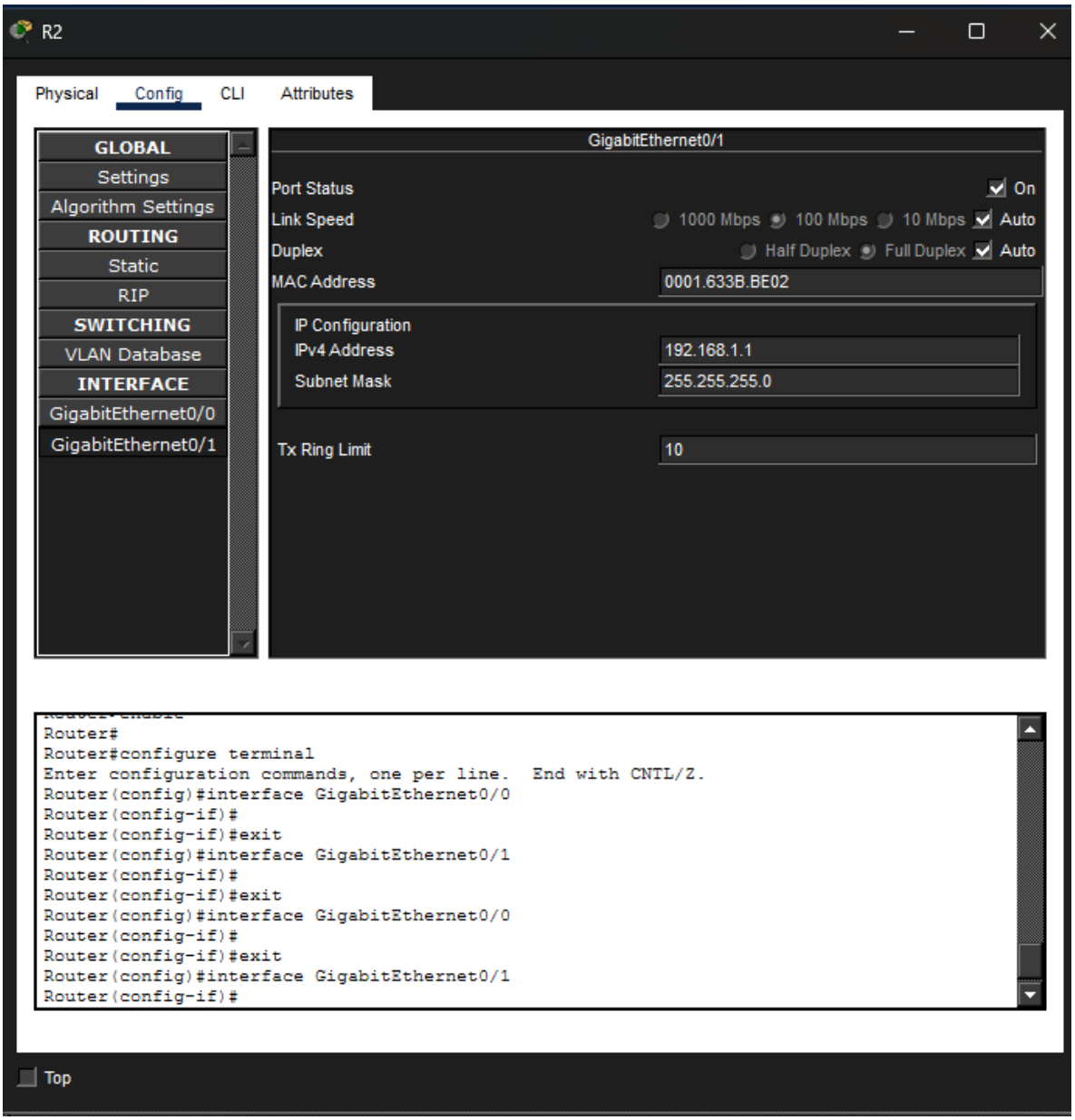
Habilitar los paquetes de seguridad son importantes para usar los comandos relacionados al IPSec VPN, este proceso se repite en ambos routers R1 Y R3

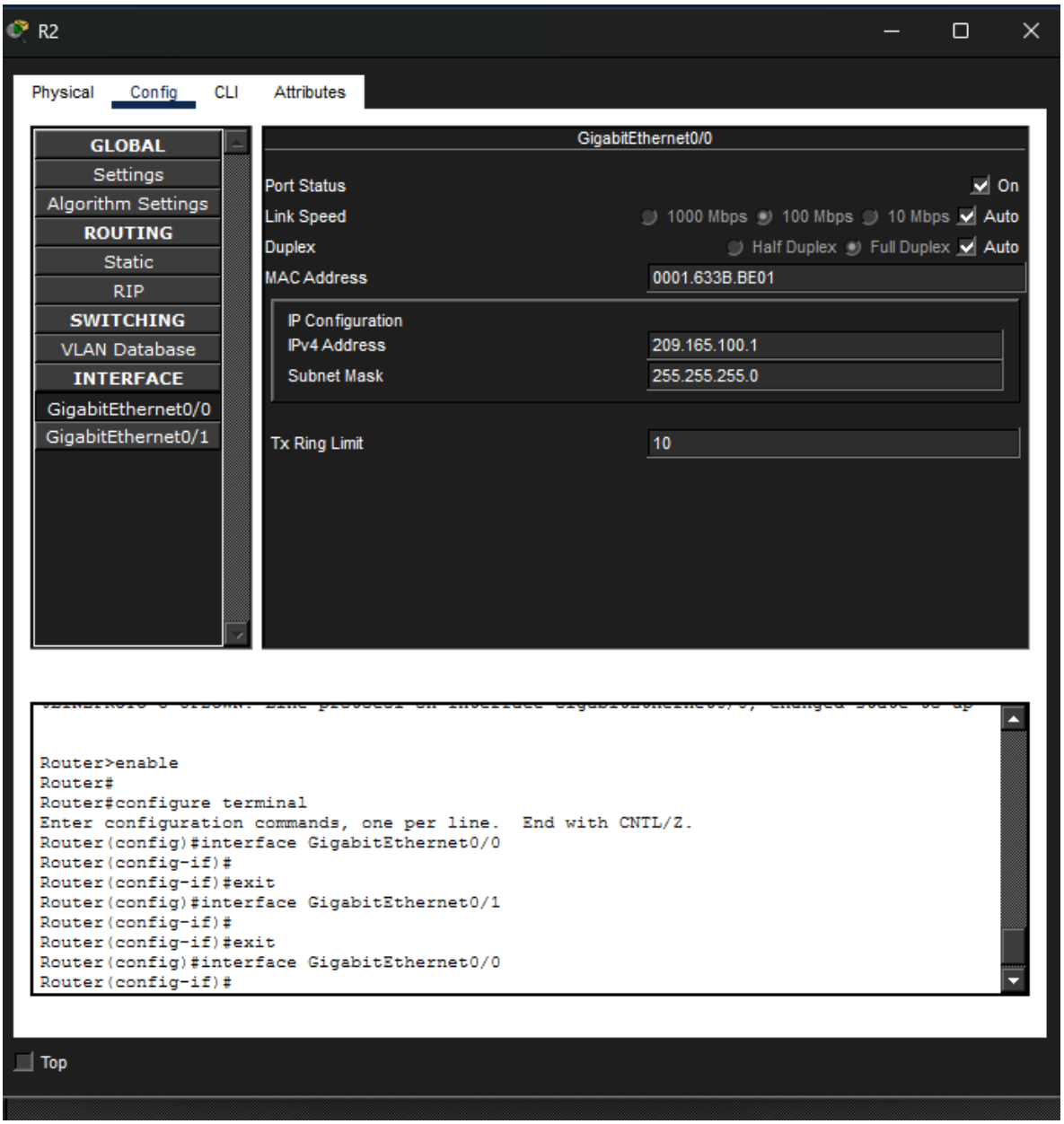
Configuración de Interfaces

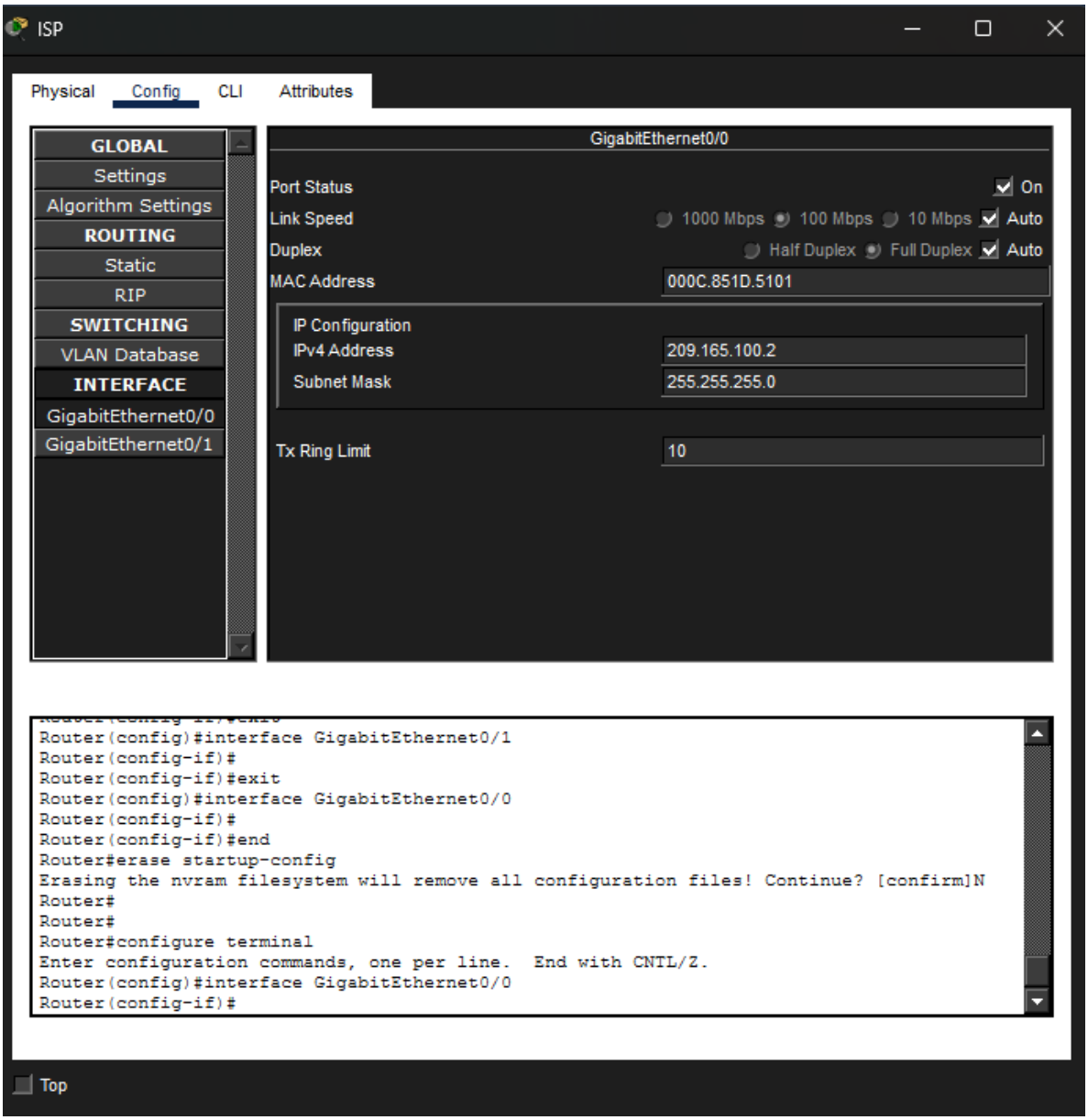
Asignación de IP'S públicas y privadas para routers y equipos personales

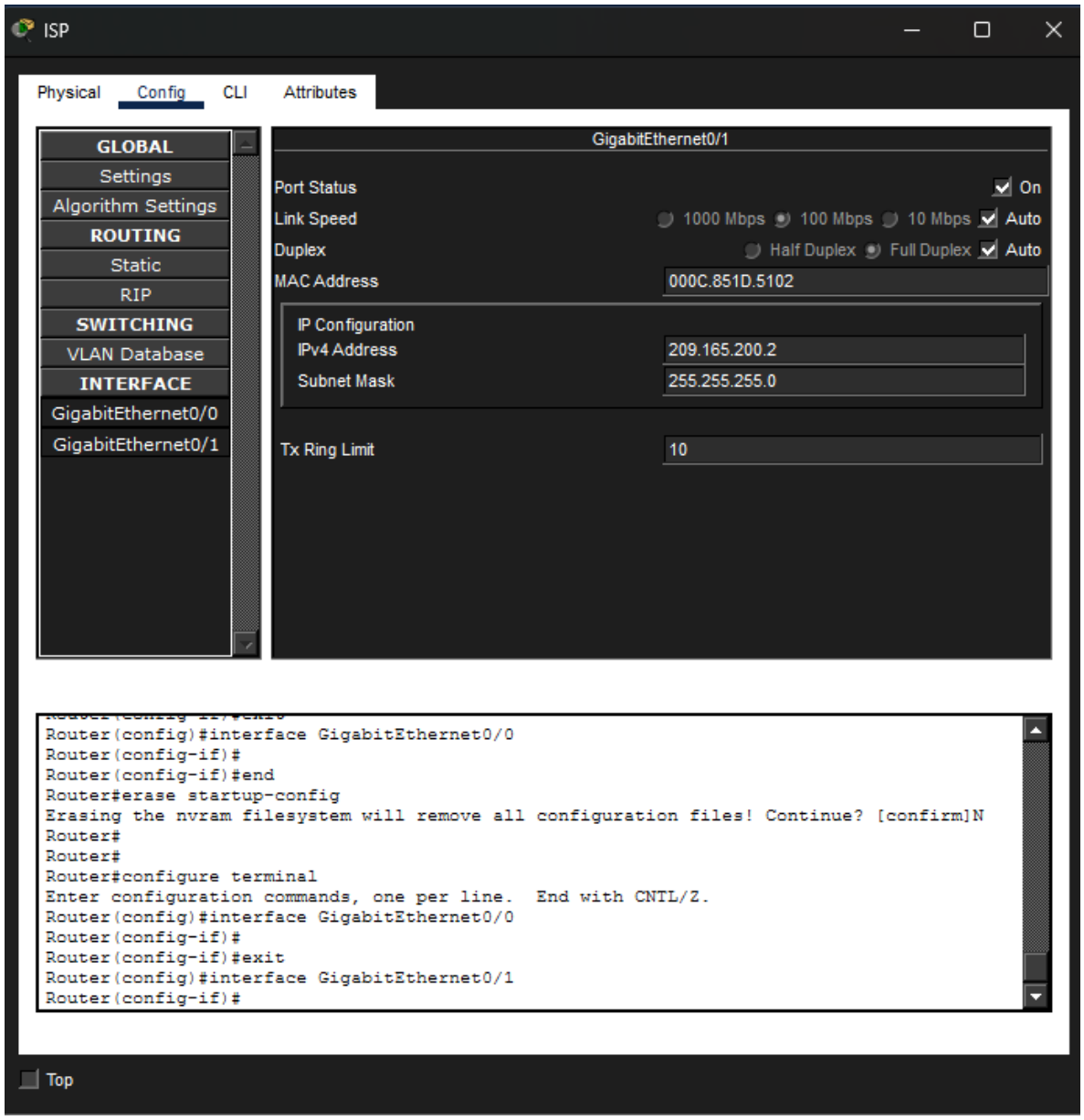


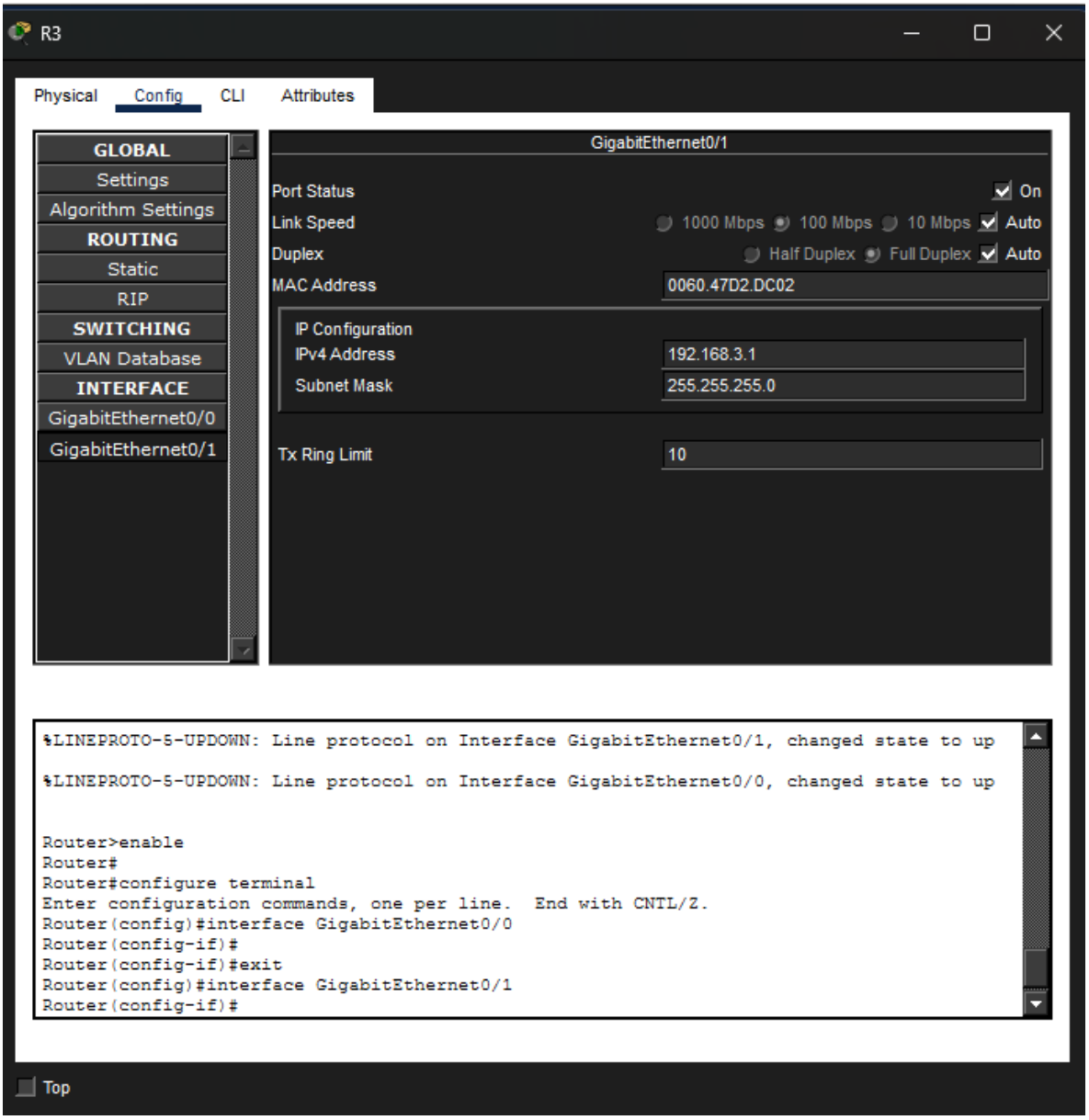

PC-C
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.10
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::209:7CFF:FE9E:90E6
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

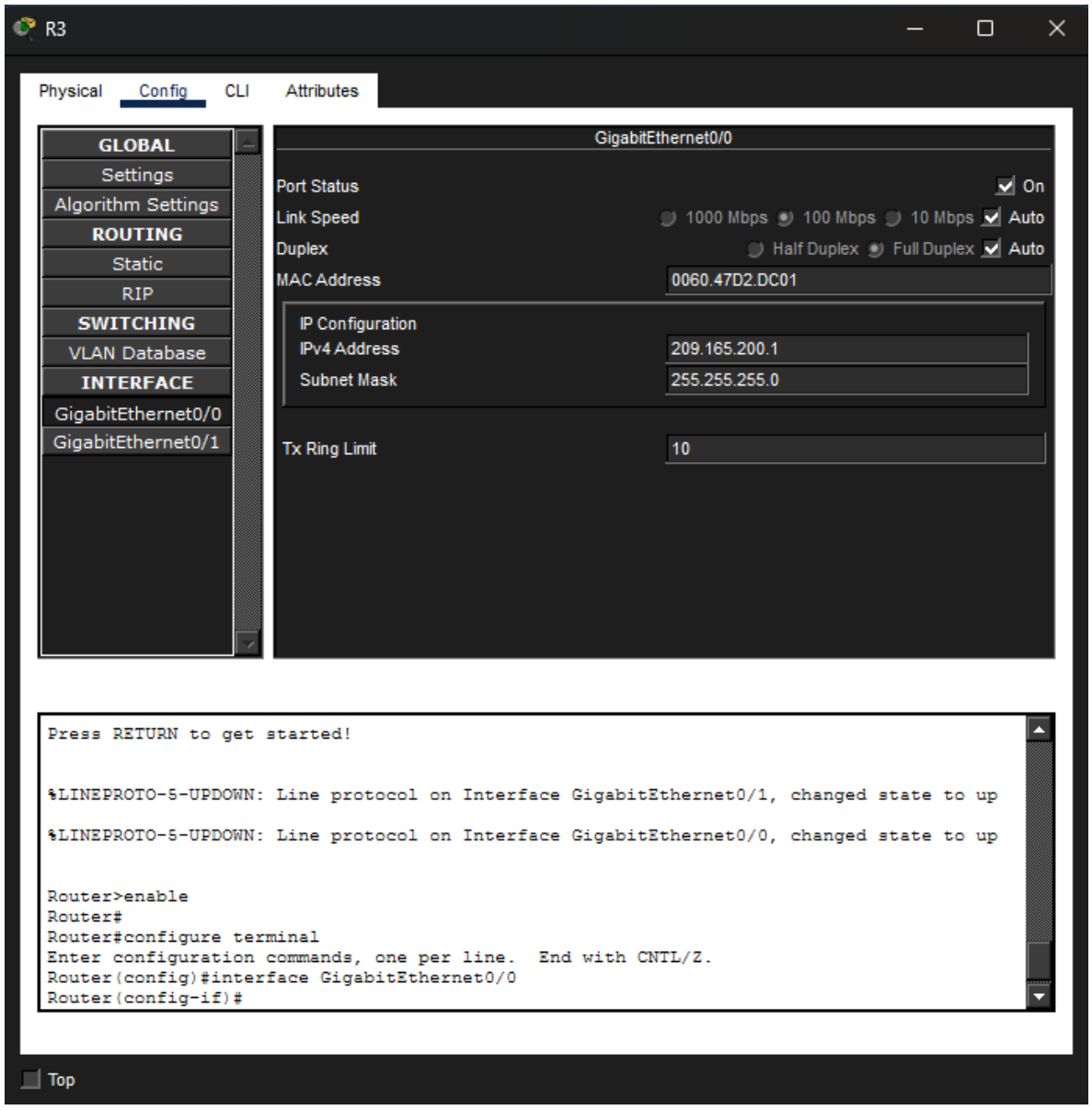

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Link Speed
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.633B.BE02
IP Configuration
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top


R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Link Speed
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.633B.BE01
IP Configuration
IPv4 Address
209.165.100.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top


ISP
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Link Speed
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.851D.5101
IP Configuration
IPv4 Address
209.165.100.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#end
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]N
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top

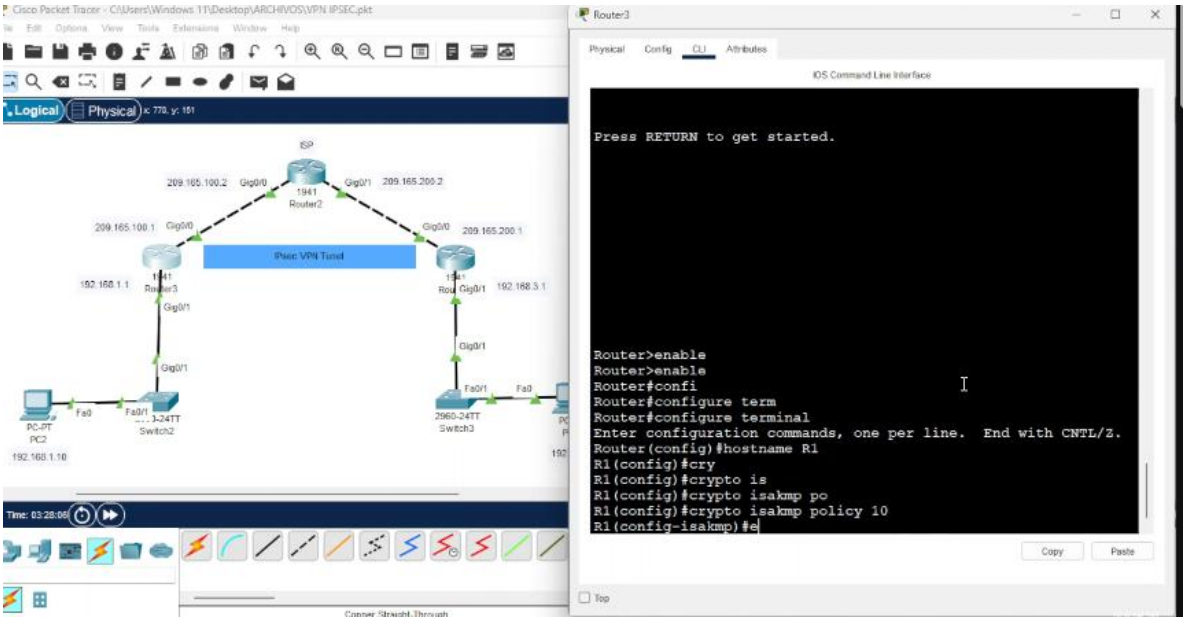

ISP
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Link Speed
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.851D.5102
IP Configuration
IPv4 Address
209.165.200.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#end
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]N
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top


R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Link Speed
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.47D2.DC02
IP Configuration
IPv4 Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top


R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Link Speed
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.47D2.DC01
IP Configuration
IPv4 Address
209.165.200.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Press RETURN to get started!
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top

Configuración del VPN

Establecer isakmp con prioridad de 10 en ambos routers (R1 y R3)




```
R1(config-isakmp)#en
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#au
R1(config-isakmp)#authentication pre
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#gr
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#cry
R1(config)#crypto is
R1(config)#crypto isakmp key secretkey ad
R1(config)#crypto isakmp key secretkey address 209.165.200.1
R1(config)#cry
R1(config)#crypto ip
R1(config)#crypto ipsec tra
R1(config)#crypto ipsec transform-set R1-R3 esp-ae
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 es
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-
sha-hmac
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-
sha-hmac
```

```
R1(config)#crypto map IPS
R1(config)#crypto map IPSEC-MAP 10 ips
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
R1(config-crypto-map)#set pe
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set
R1(config-crypto-map)#set pf
R1(config-crypto-map)#set pfs gr
R1(config-crypto-map)#set pfs grou
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set sec
R1(config-crypto-map)#set security-association life
R1(config-crypto-map)#set security-association lifetime seco
R1(config-crypto-map)#set security-association lifetime
seconds 86400
```

```
R1(config-crypto-map)#set
R1(config-crypto-map)#set tr
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#ma
R1(config-crypto-map)#match ad
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#inte
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#cryp
R1(config-if)#crypto ma
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
R1(config)#ac
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

Copy Paste

```
R3(config)#cry
R3(config)#crypto is
R3(config)#crypto isakmp po
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#en
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#aut
R3(config-isakmp)#authentication pr
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#gro
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#cry
R3(config)#crypto isa
R3(config)#crypto isakmp key secretkey ad
R3(config)#crypto isakmp key secretkey address 209.165.100.1
R3(config)#cry
R3(config)#crypto ip
R3(config)#crypto ipsec tr
R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-
sha-hmac
R3(config)#cry
R3(config)#crypto map IPSEC-MAP 10 ipse
R3(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.
```

```
R3(config-crypto-map)#set
R3(config-crypto-map)#set pe
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set sec
R3(config-crypto-map)#set security-association lifetime seco
R3(config-crypto-map)#set security-association lifetime
seconds 86400
R3(config-crypto-map)#set
R3(config-crypto-map)#set tr
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#mat
R3(config-crypto-map)#match ad
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#inter
R3(config)#interface gi
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#cry
R3(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

```
R3(config-if)#exit
R3(config)#ac
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
R3(config)#
```

Pruebas de Ping PC