Actividad # 7.1 - Seguridad en Redes: Configuración de IPS, SSH en Switches y Routers, y Seguridad en Puertos

1. Escenario del Laboratorio

Contexto

Eres un administrador de redes en una empresa y se te ha solicitado implementar medidas de seguridad en la red para evitar accesos no autorizados y ataques internos. Para ello, debes configurar un sistema de seguridad en un router y un switch, asegurando que la administración remota sea segura y que los puertos del switch estén protegidos contra accesos no deseados.

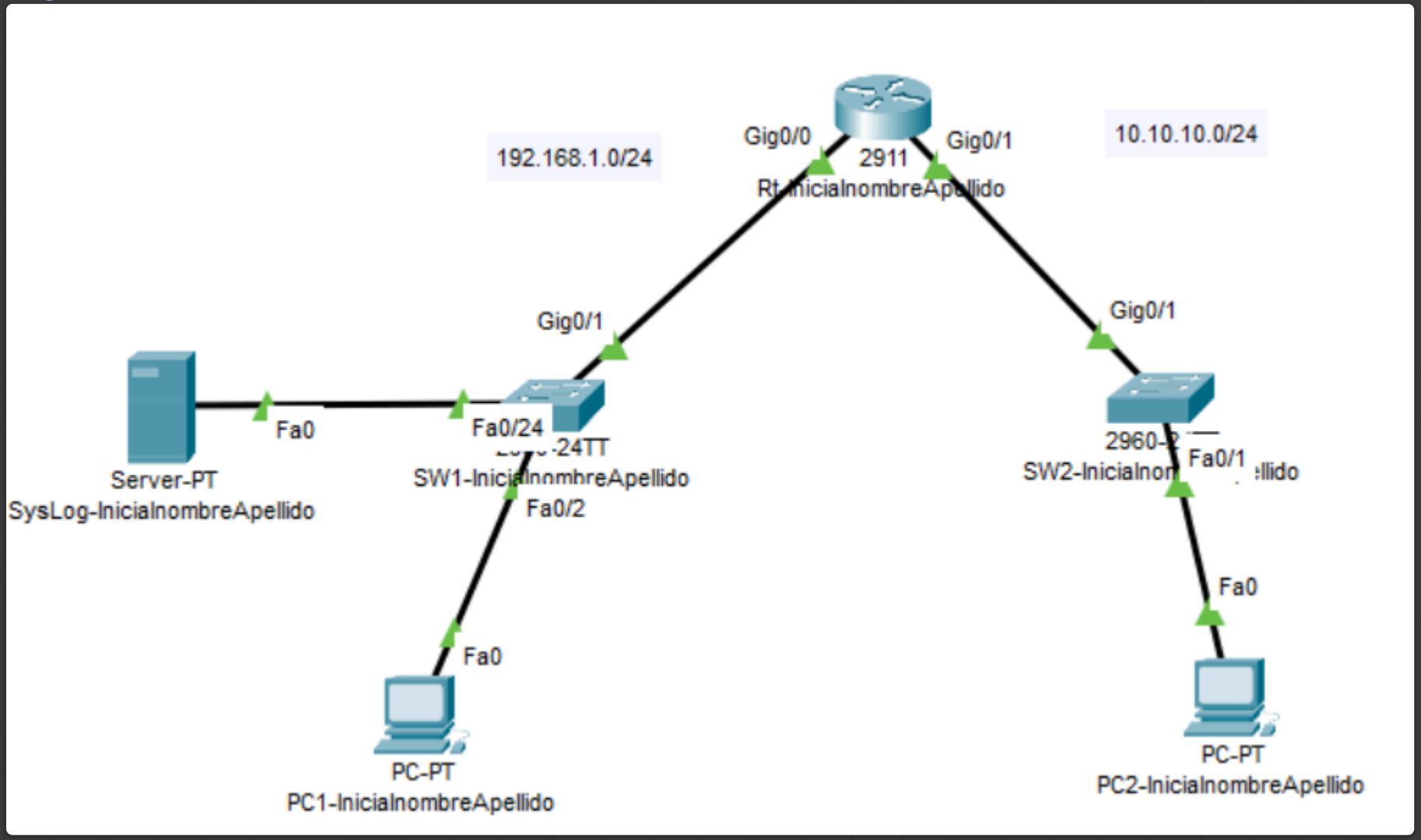
Cada estudiante debe personalizar la configuración utilizando su nombre y apellido en los nombres de dispositivos y en los usuarios de autenticación. Las contraseñas deben ser seguras y personales.

2. Requerimientos y Topología

Material Necesario

- **1 Router (R1 - Nombre: Router_InicialNombreApellido)**
- **2 Switches administrable (S1 - Nombre: Switch_InicialNombreApellido)**
- **2 PCs (PC1 y PC2) y 1 Server**

Diagrama de Red



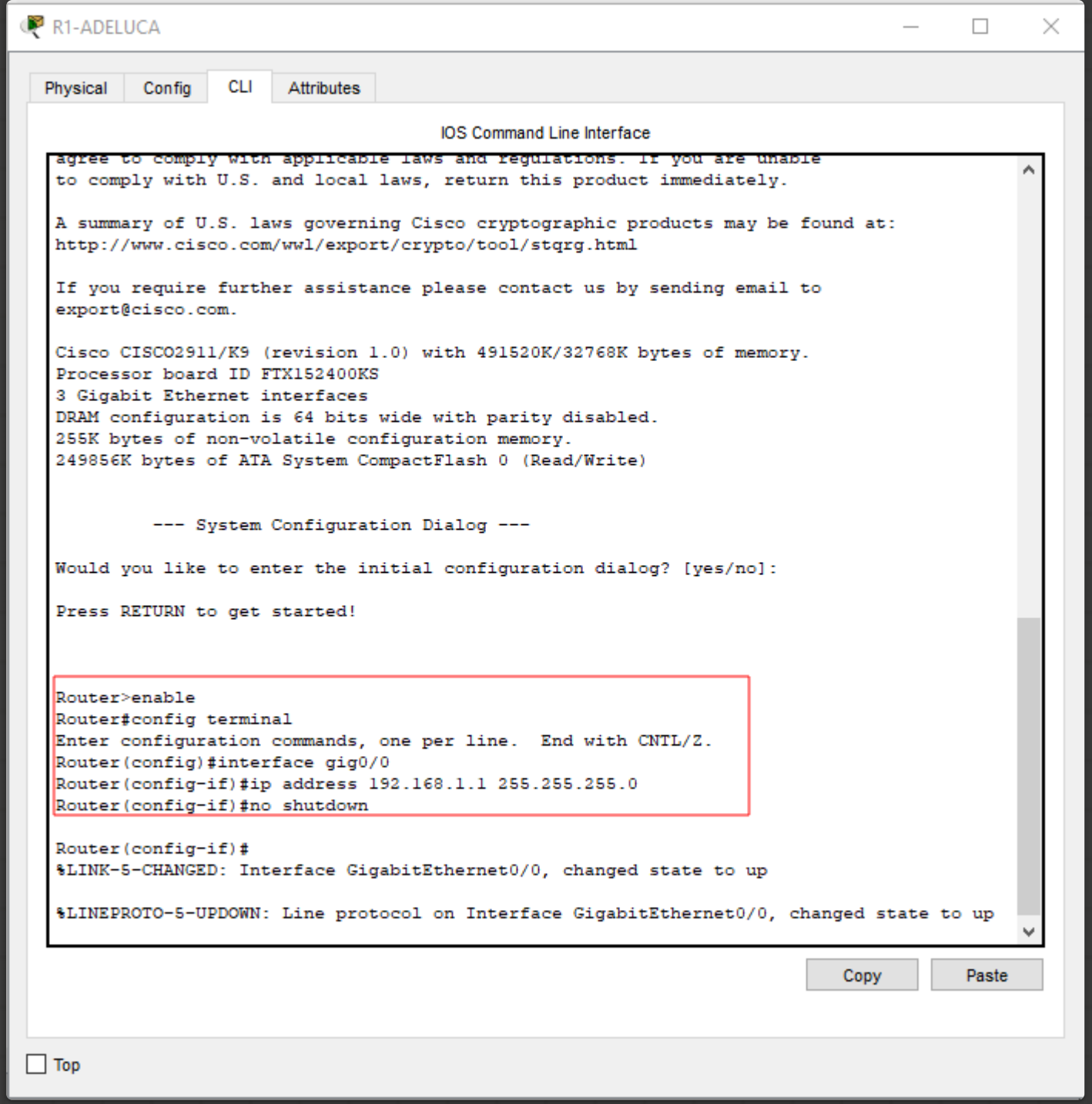
para configurar el Router1 primero es necesario ingresar a la terminal, para ello hay que usar los siguientes comandos

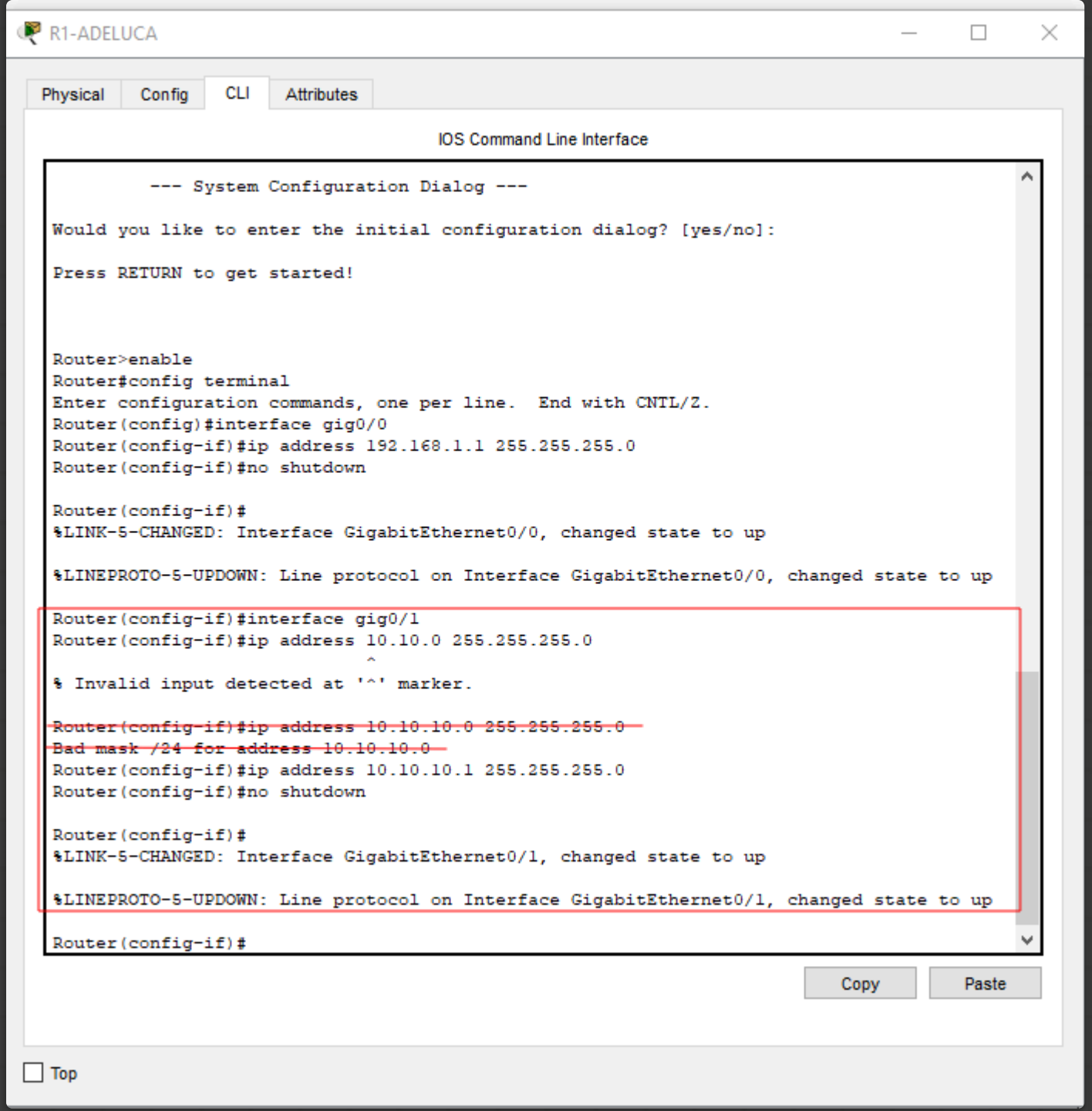
```
enable
config terminal
```

para configurar las ip's hay que seleccionar las interfaces que se quiere configurar una a la vez

```
interface gig0/0
ip address 192.168.1.1 255.255.255.0
```

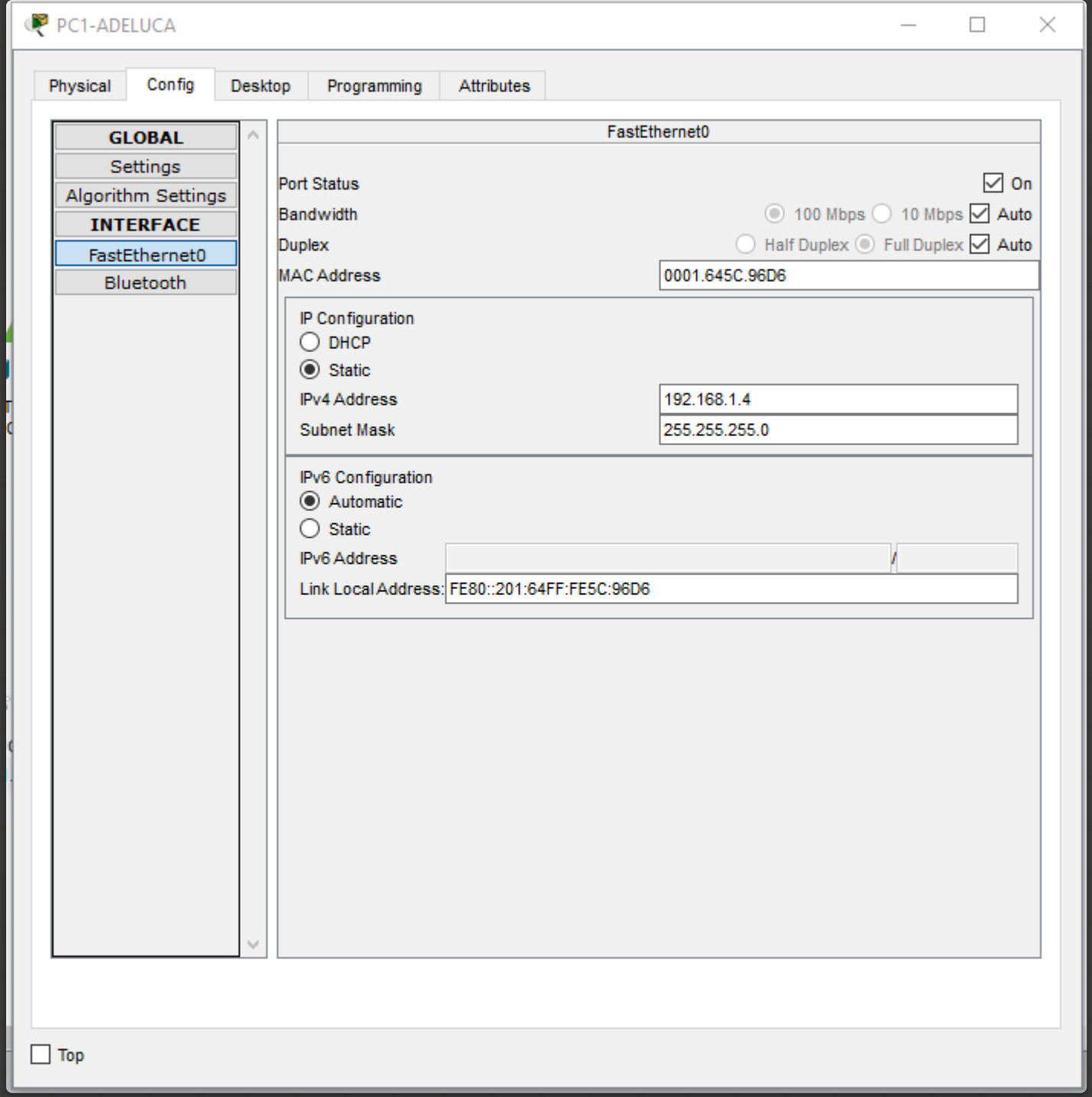
```
no shutdown
```

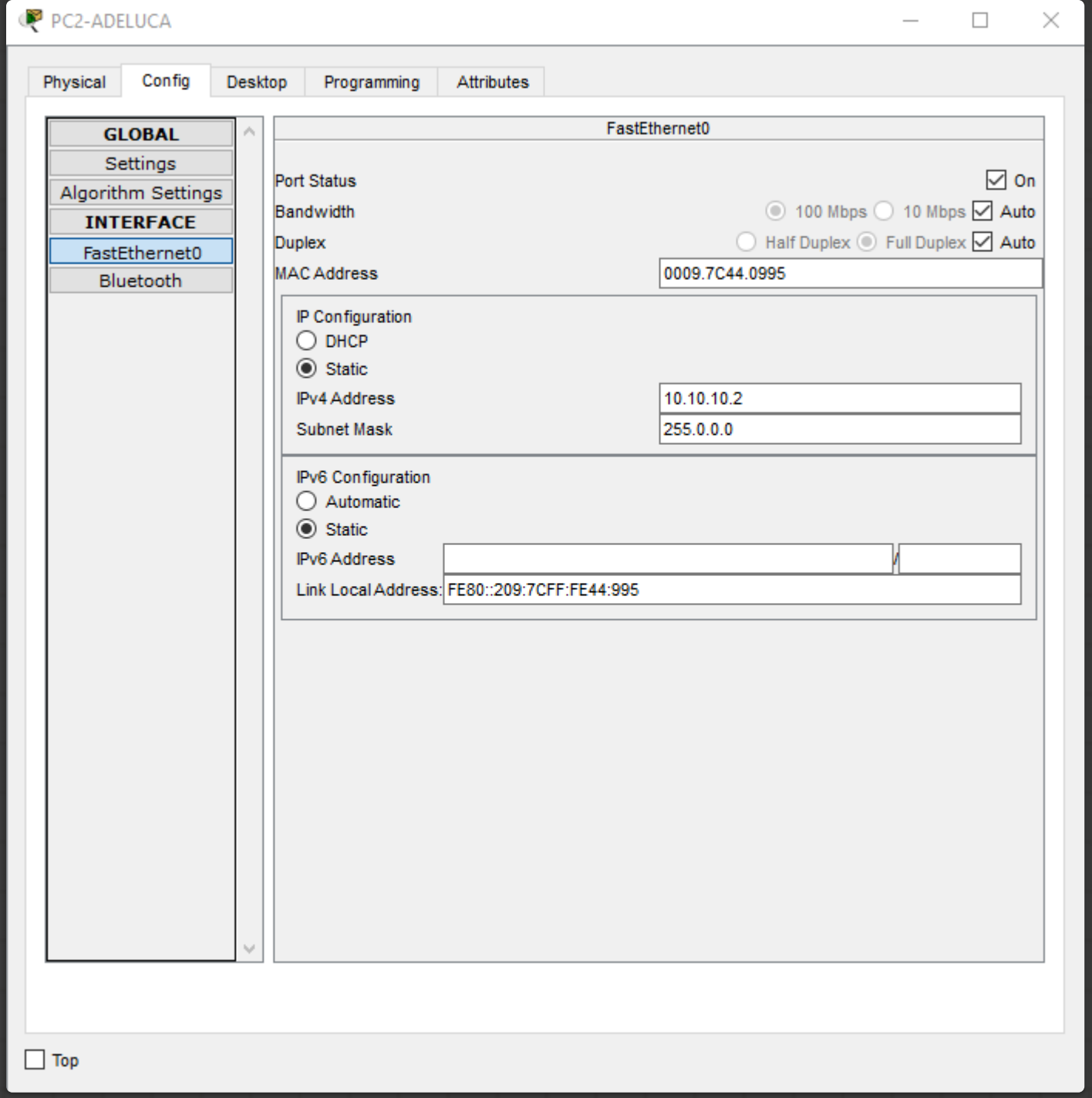

R1-ADELUCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 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)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
Press RETURN to get started!
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
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
Copy
Paste
Top

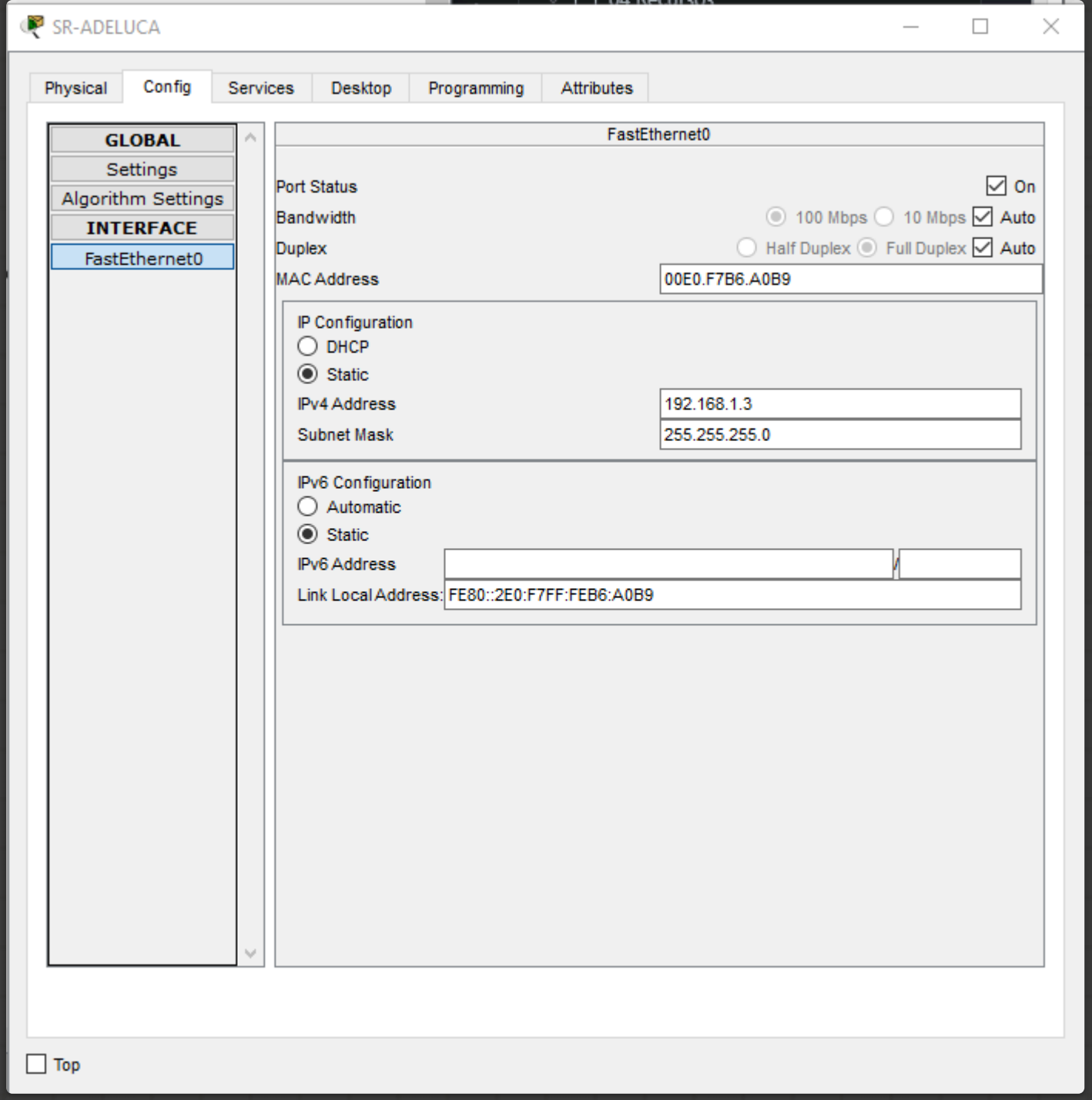

R1-ADELUCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
Press RETURN to get started!
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
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
Router(config-if)#interface gig0/1
Router(config-if)#ip address 10.10.0 255.255.255.0
^
% Invalid input detected at '^' marker.
Router(config-if)#ip address 10.10.10.0 255.255.255.0
Bad mask /24 for address 10.10.10.0
Router(config-if)#ip address 10.10.10.1 255.255.255.0
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
Router(config-if)#
Copy
Paste
Top

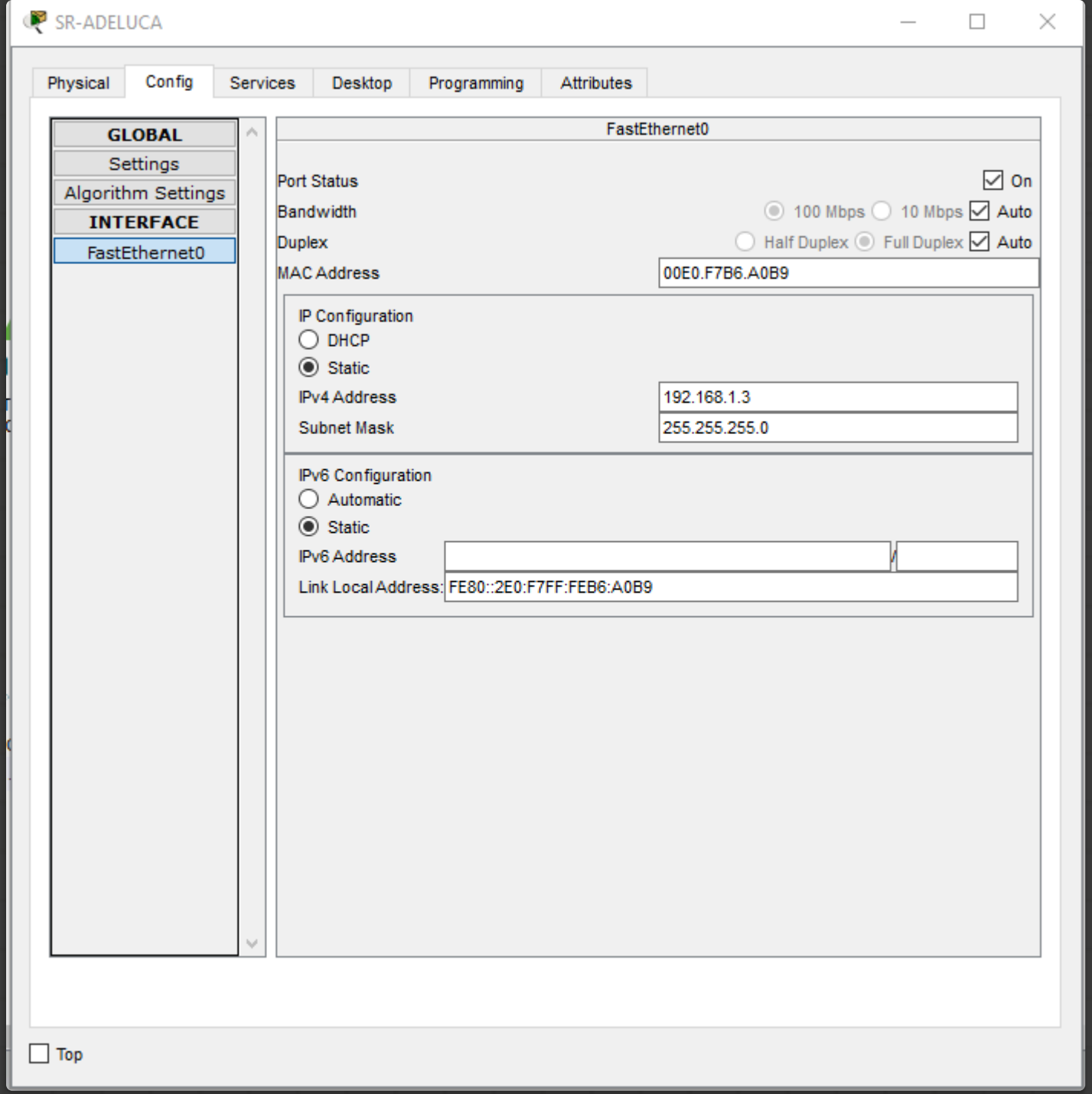
importante recordar que la dirección de Red Cuando todos los bits de la porción de host son cero, está reservada para identificar la red en sí misma.

una vez realizada la asignación de IP's del Router continuaremos con los dispositivos finales

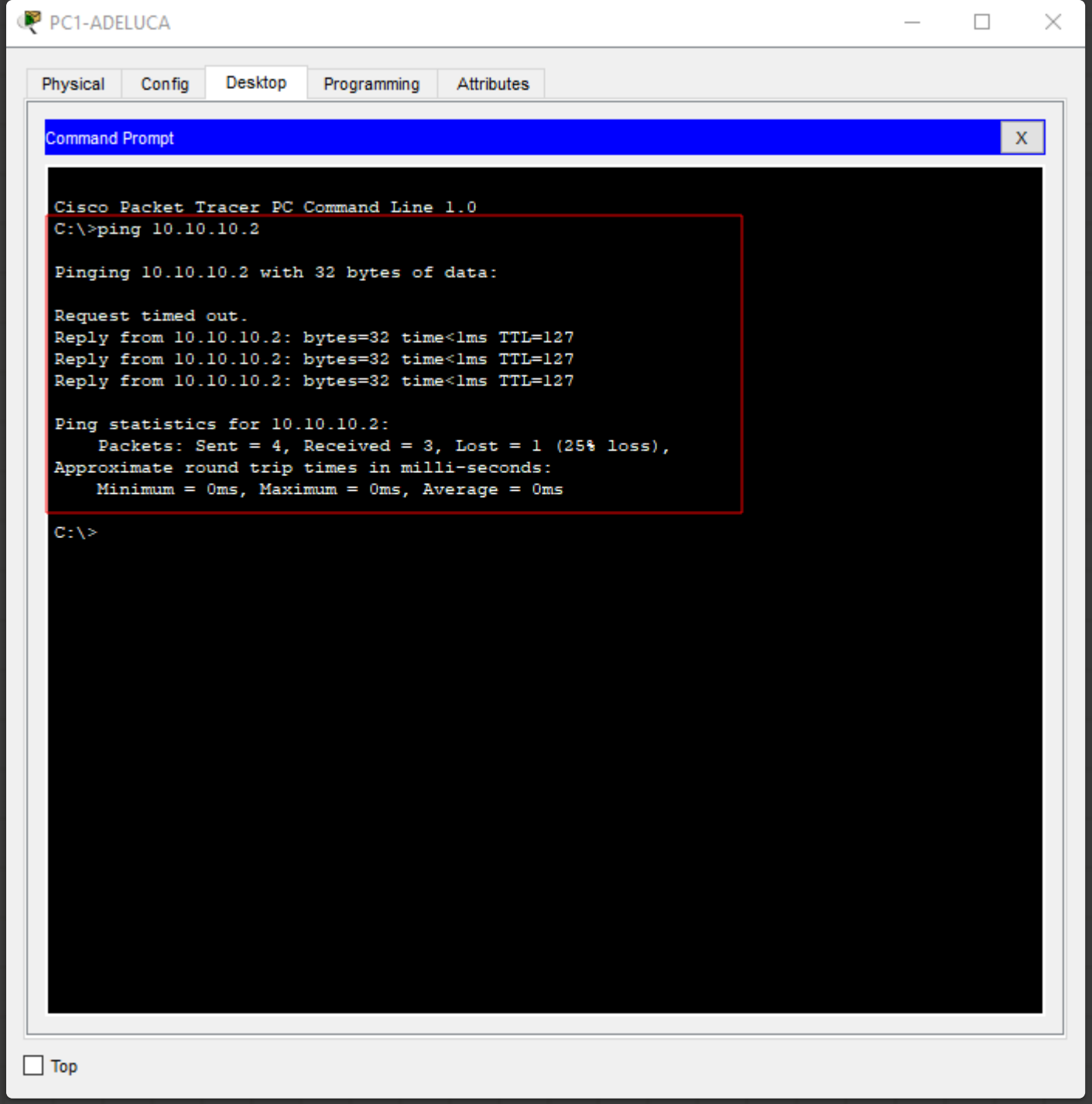

PC1-ADELUCA
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.645C.96D6
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::201:64FF:FE5C:96D6
Top


PC2-ADELUCA
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0009.7C44.0995
IP Configuration
DHCP
Static
IPv4 Address
10.10.10.2
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::209:7CFF:FE44:995
Top


SR-ADELUCA
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F7B6.A0B9
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::2E0:F7FF:FEB6:A0B9
Top



Realizamos el test haciendo ping de pc1 a pc2

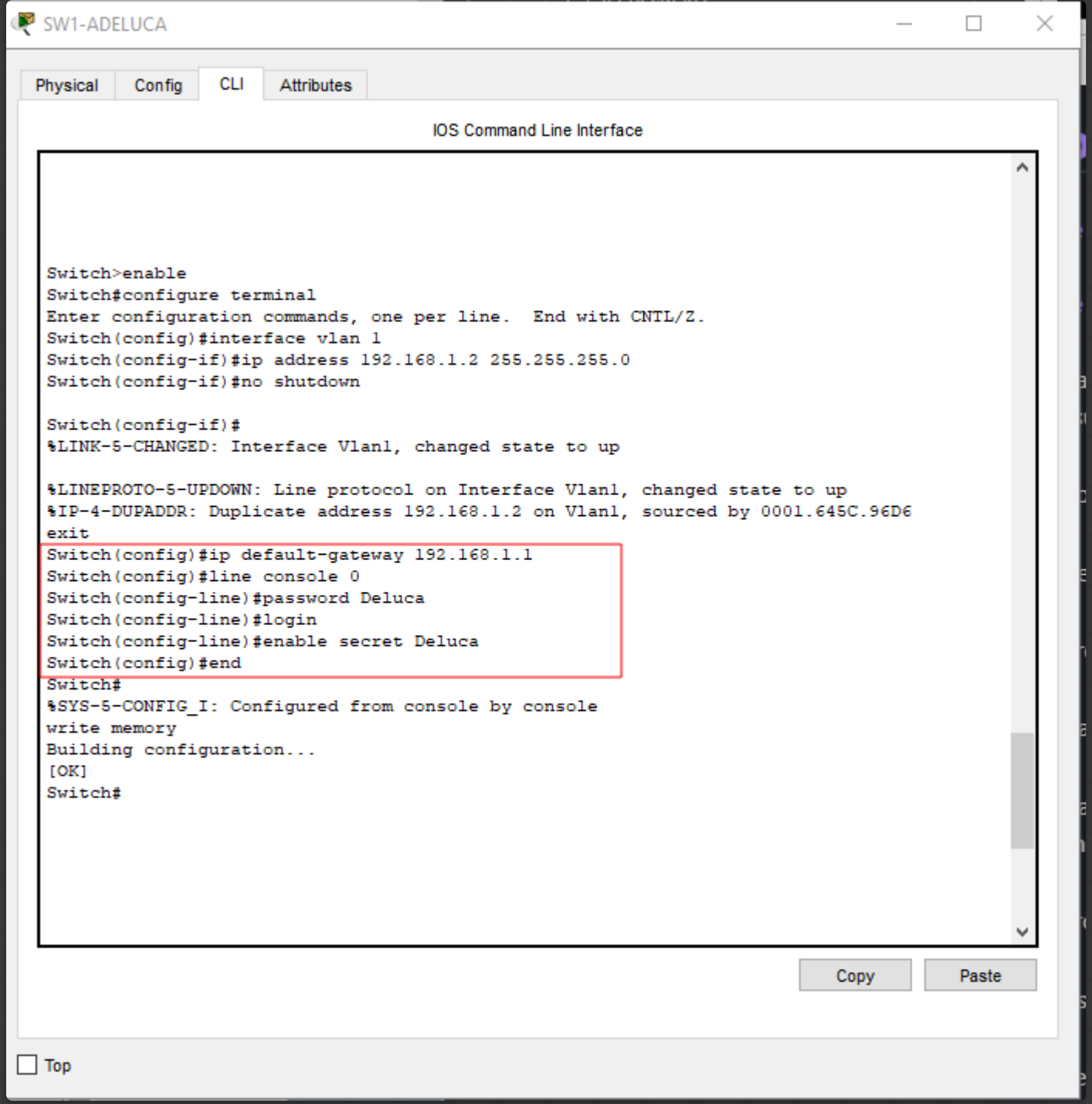


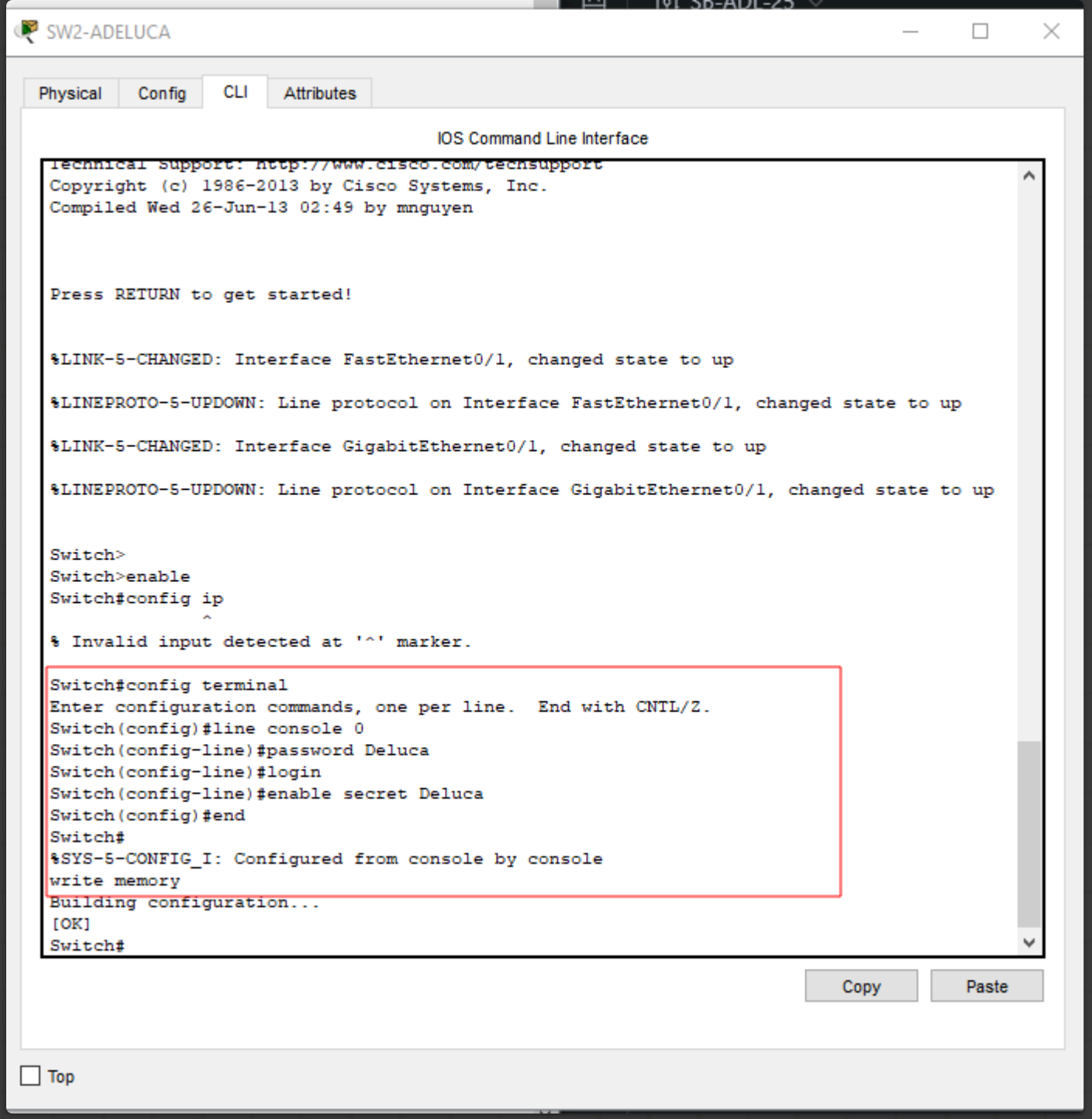
3. Desarrollo del Laboratorio

Parte 1: Configuración de Direcciones IP

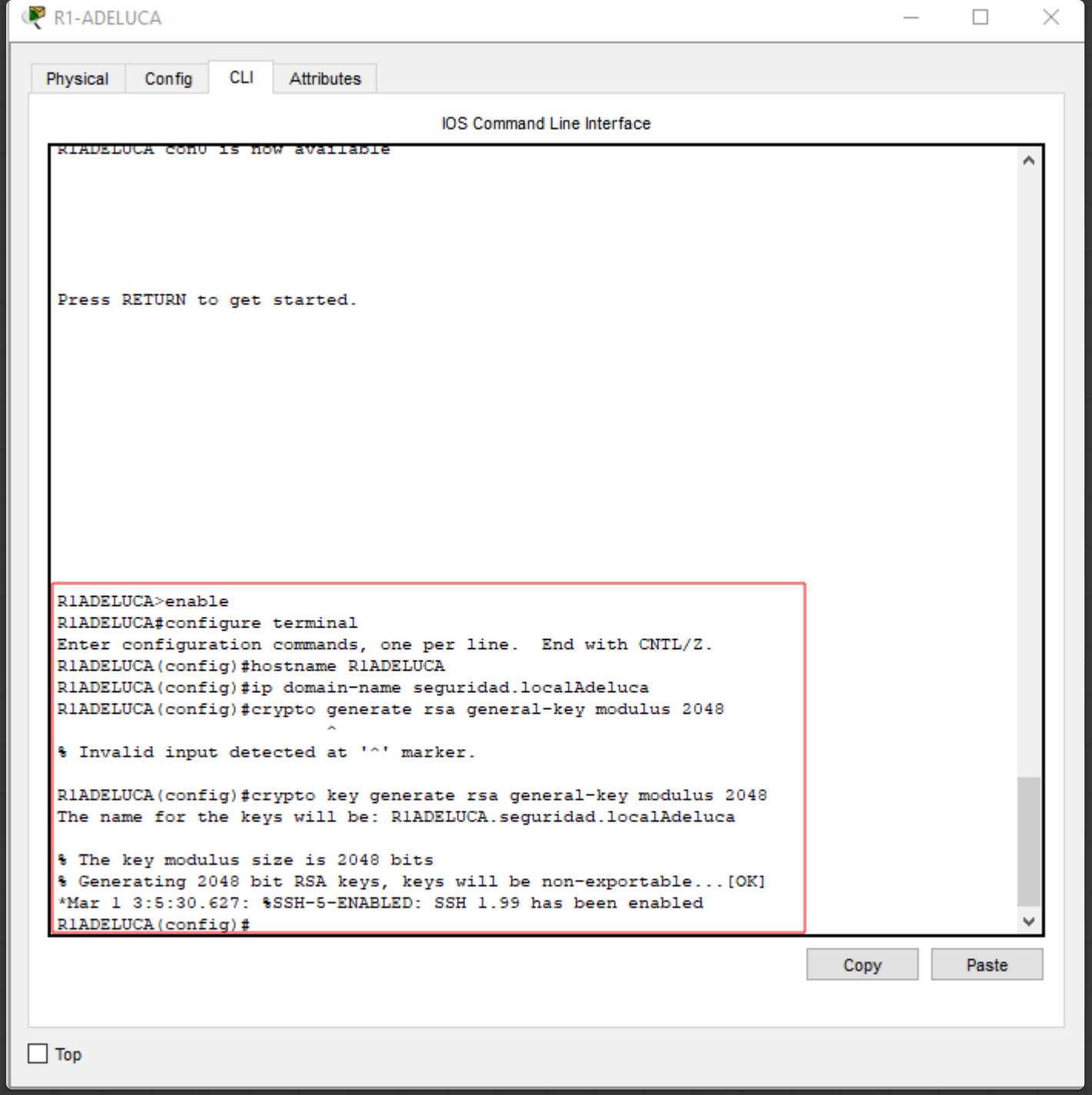
Parte 2: Configuración de SSH en Switch y Router

- **Cada estudiante debe usar sus datos personales para configurar usuarios y contraseñas necesarias y anotarlas en la topología**
- **Configurar un dominio seguridad.local.**
- **Generar claves RSA (1024 o 2048 bits).**
- **Crear un usuario con su nombre y una contraseña segura.**
- **Habilitar acceso SSH en las líneas VTY.**
- **Habilitar la encriptación de passwords (todos los passwords deben estar encriptados)**
- **Probar el acceso SSH desde una PC:**
- **Usar el comando ssh -l usuario 192.168.1.2 para acceder al switch.**
- **Verificar que solo SSH esté permitido y que el acceso por Telnet esté bloqueado.**

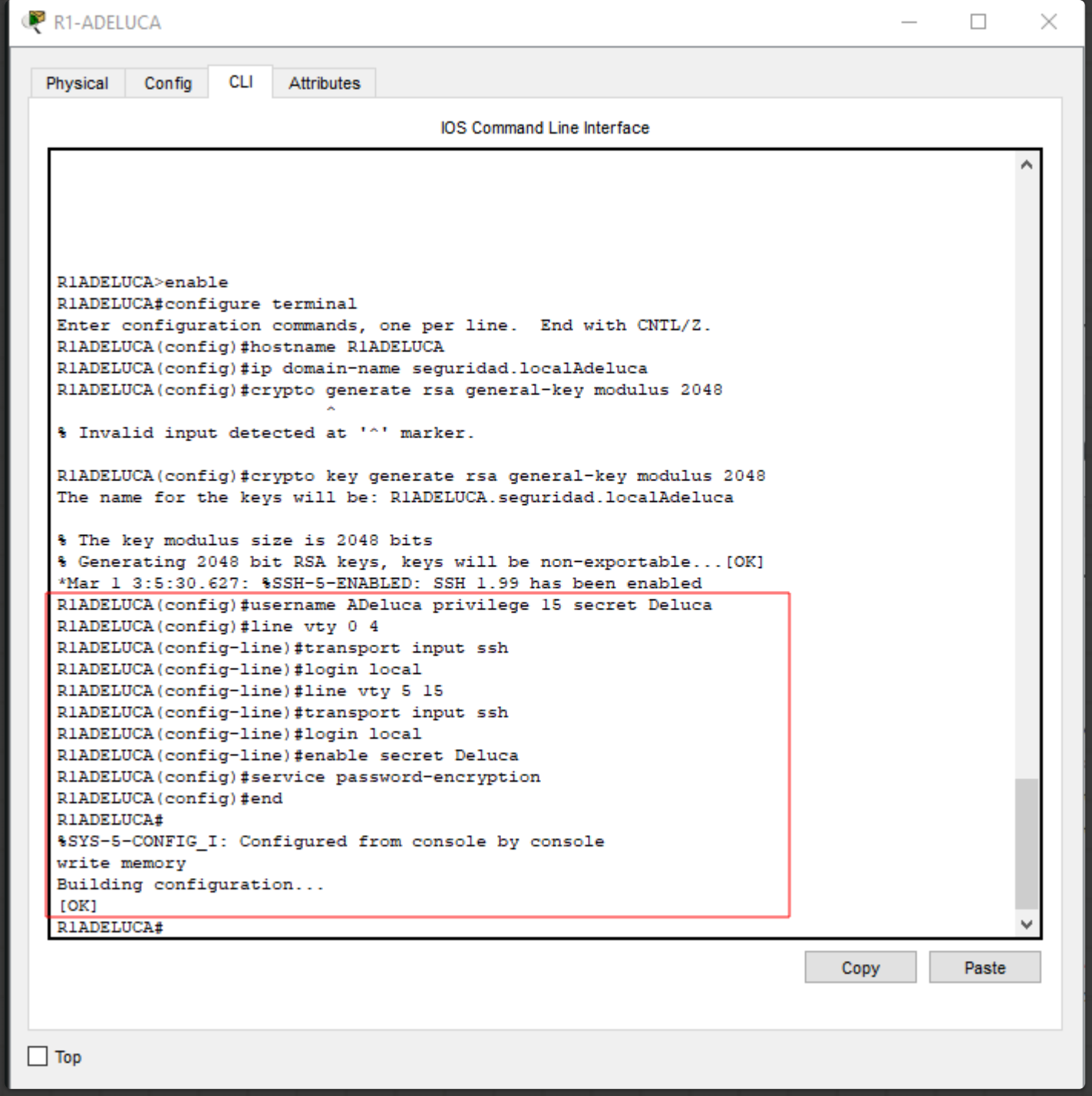

SW1-ADELUCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%IP-4-DUPADDR: Duplicate address 192.168.1.2 on Vlan1, sourced by 0001.645C.96D6
exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#line console 0
Switch(config-line)#password Deluca
Switch(config-line)#login
Switch(config-line)#enable secret Deluca
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Switch#
Copy
Paste
Top

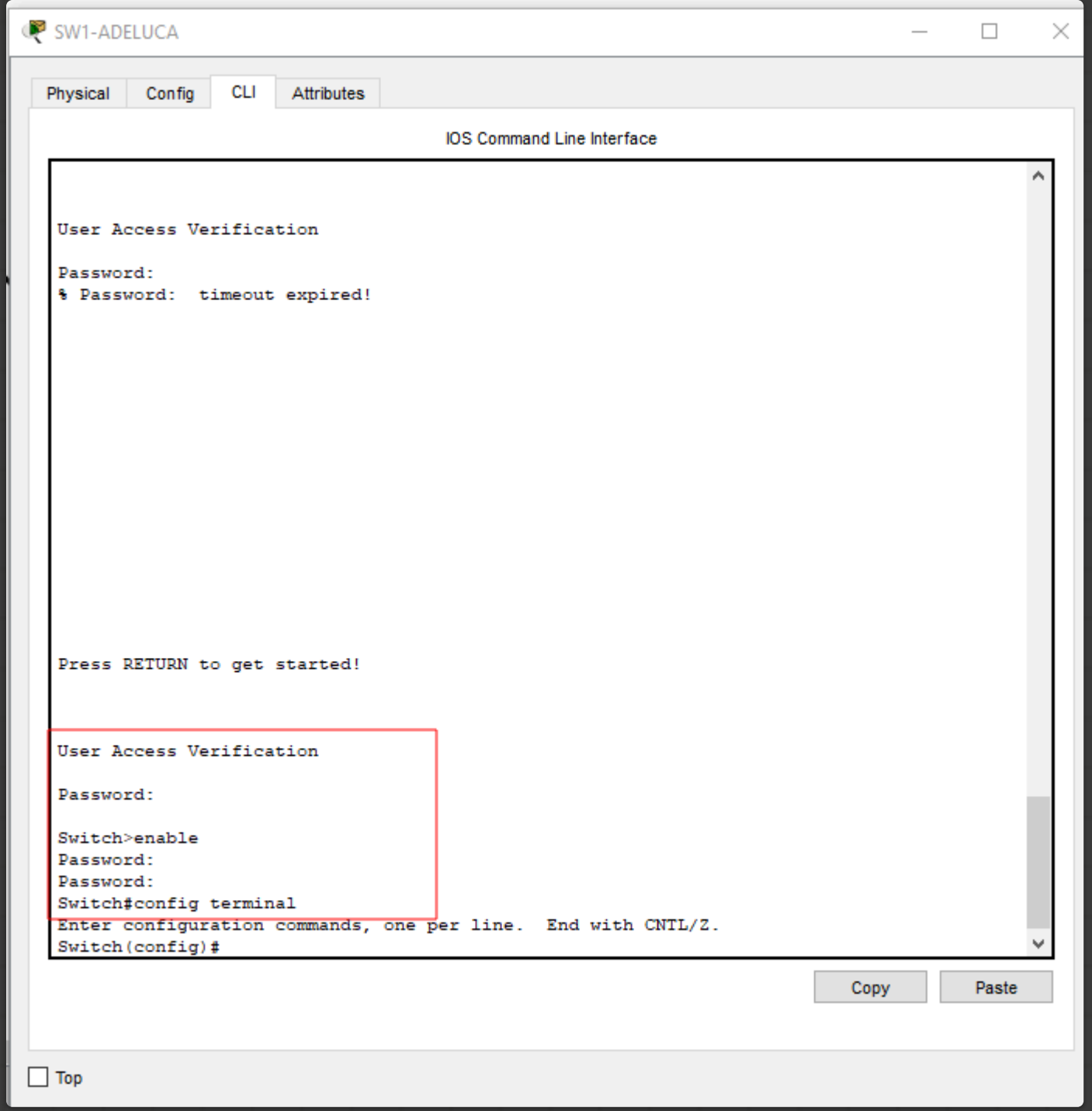


Configuramos el dominio y generamos las claves RSA

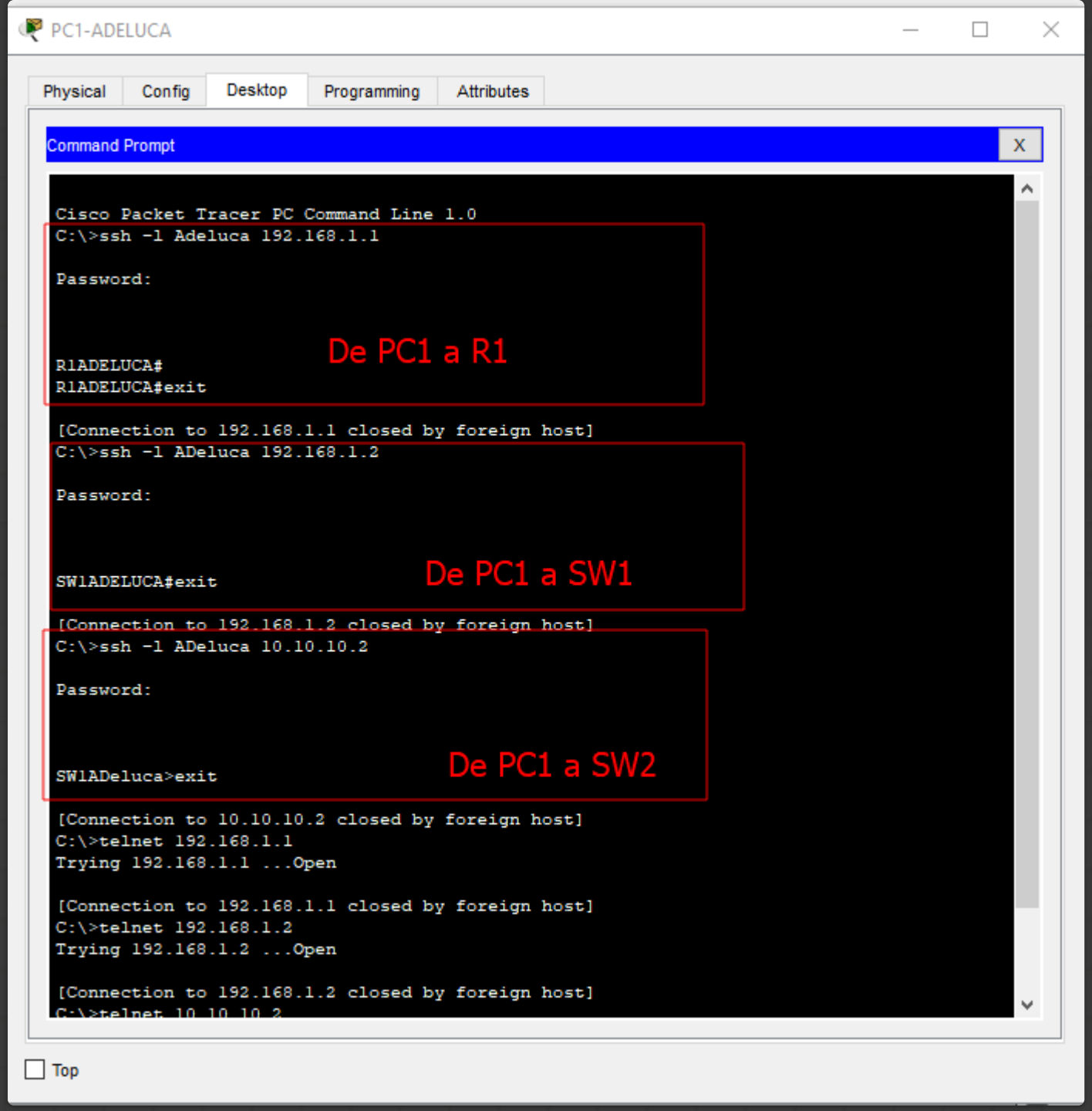


Crear usuario, contraseña y encriptar


R1-ADELUCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
R1ADELUCA>enable
R1ADELUCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1ADELUCA(config)#hostname R1ADELUCA
R1ADELUCA(config)#ip domain-name seguridad.localAdeluca
R1ADELUCA(config)#crypto generate rsa general-key modulus 2048
                  ^
% Invalid input detected at '^' marker.
R1ADELUCA(config)#crypto key generate rsa general-key modulus 2048
The name for the keys will be: R1ADELUCA.seguridad.localAdeluca
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 3:5:30.627: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1ADELUCA(config)#username ADeluca privilege 15 secret Deluca
R1ADELUCA(config)#line vty 0 4
R1ADELUCA(config-line)#transport input ssh
R1ADELUCA(config-line)#login local
R1ADELUCA(config-line)#line vty 5 15
R1ADELUCA(config-line)#transport input ssh
R1ADELUCA(config-line)#login local
R1ADELUCA(config-line)#enable secret Deluca
R1ADELUCA(config)#service password-encryption
R1ADELUCA(config)#end
R1ADELUCA#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R1ADELUCA#
Copy
Paste
Top



Ya solicita la contraseña



Se solicitará la contraseña `Deluca`. Una vez dentro, escribe `enable` y proporciona `Deluca` para acceder al modo privilegiado.

Parte 3: Seguridad en Puertos del Switch

- **Configurar seguridad en los puertos de usuario (Fa0/1 y Fa0/2):**
- **Establecer el modo de puerto en access.**
- **Habilitar port-security.**
- **Configurar un máximo de 2 direcciones MAC por puerto.**
- **Activar sticky MAC para que las direcciones aprendidas se almacenen de manera automática.**
- **Configurar la acción restrict para registrar y bloquear direcciones MAC no autorizadas.**
- **Verificar configuraciones con los comandos adecuados.**
- **show port-security interface Fa0/1**
- **show mac address-table**

SW2-ADELUCA

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
User Access Verification

Password:

Switch>enable
Password:
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.10.10.2 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%IP-4-DUPADDR: Duplicate address 10.10.10.2 on Vlan1, sourced by 0009.7C44.0995
ip default-gateway 10.10.10.1
Switch(config)#line console 0
Switch(config-line)#logging synchronous
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write memory
Building configuration...
[OK]
Switch#
```

Copy | Paste

Top

SW1-ADELUCA

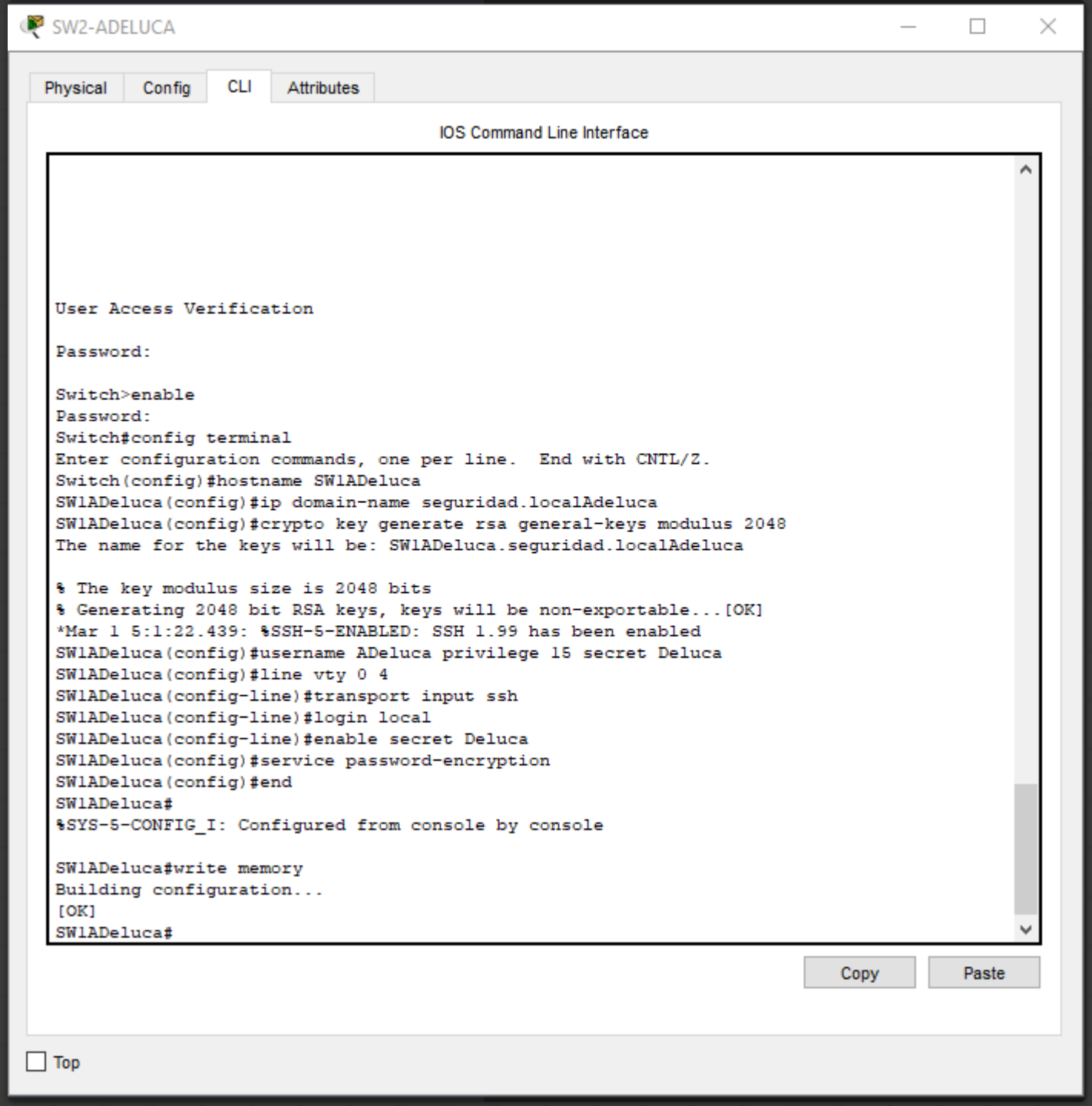
Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Switch#
Switch#enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW1ADELUCA
SW1ADELUCA(config)#ip domain-name seguridad.localAdeluca
SW1ADELUCA(config)# crypto key generate rsa general-keys modulus 2048 ! Or 1024
                                                                       ^
% Invalid input detected at '^' marker.

SW1ADELUCA(config)# crypto key generate rsa general-keys modulus 2048
The name for the keys will be: SW1ADELUCA.seguridad.localAdeluca

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 4:49:46.178: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1ADELUCA(config)#username ADeluca priovilege 15 secret Deluca
                                   ^
% Invalid input detected at '^' marker.

SW1ADELUCA(config)#username ADeluca privilege 15 secret Deluca
SW1ADELUCA(config)#line vty 0 4
SW1ADELUCA(config-line)#transport input ssh
SW1ADELUCA(config-line)#login local
SW1ADELUCA(config-line)#line vty 5 15
SW1ADELUCA(config-line)#transport input ssh
SW1ADELUCA(config-line)#login local
SW1ADELUCA(config-line)#enable secret Deluca
SW1ADELUCA(config)#service password-encryption
SW1ADELUCA(config)#end
SW1ADELUCA#
%SYS-5-CONFIG_I: Configured from console by console

SW1ADELUCA#write memory
Building configuration...
[OK]
SW1ADELUCA#
```

Copy | Paste

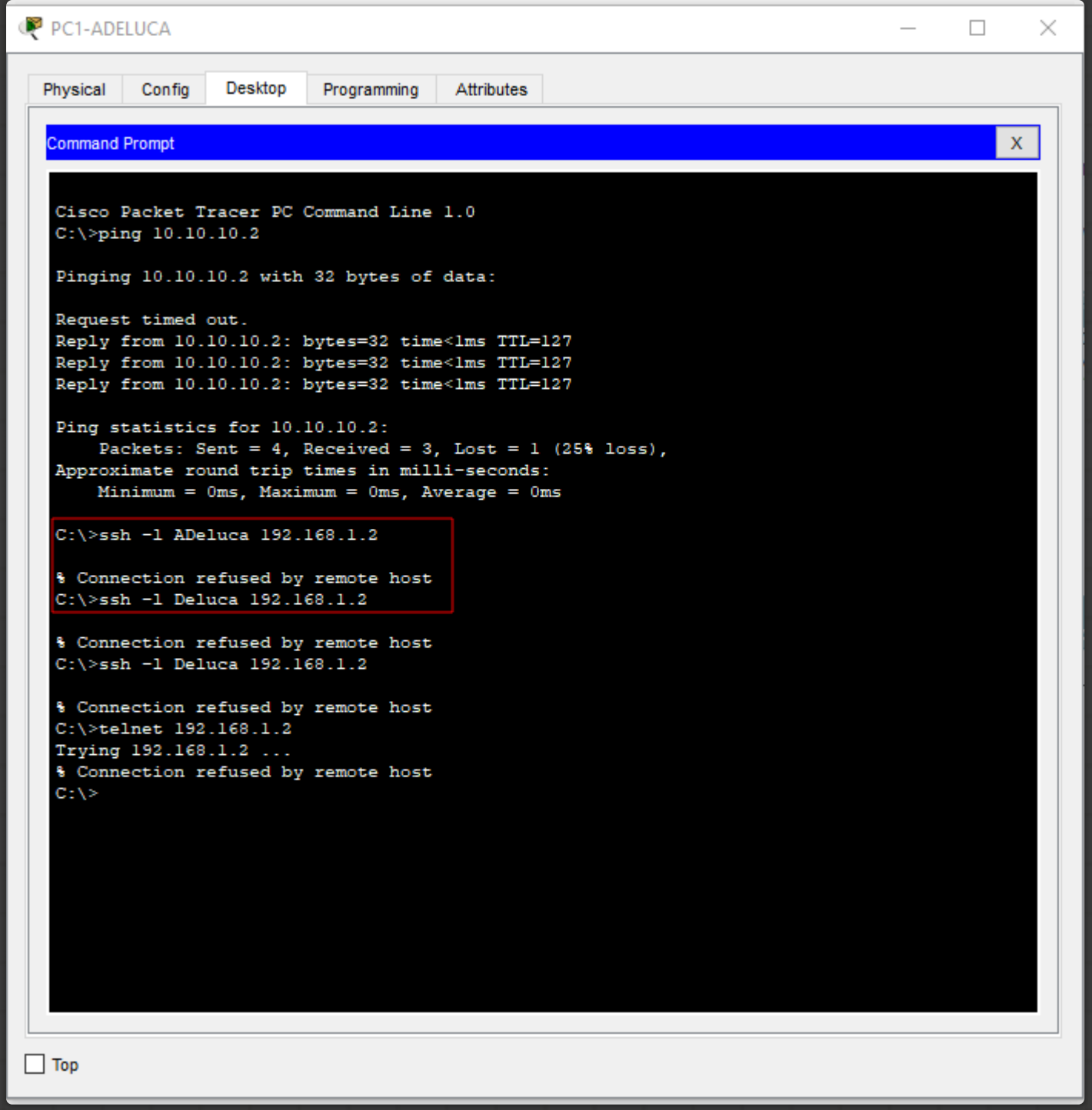
Top



hostname: Establece el nombre de host del dispositivo. ip domain-name seguridad.local: Configura el nombre de dominio. crypto key generate rsa general-keys modulus 2048: Genera claves RSA para SSH (utilizando un módulo de 2048 bits para mayor seguridad). username

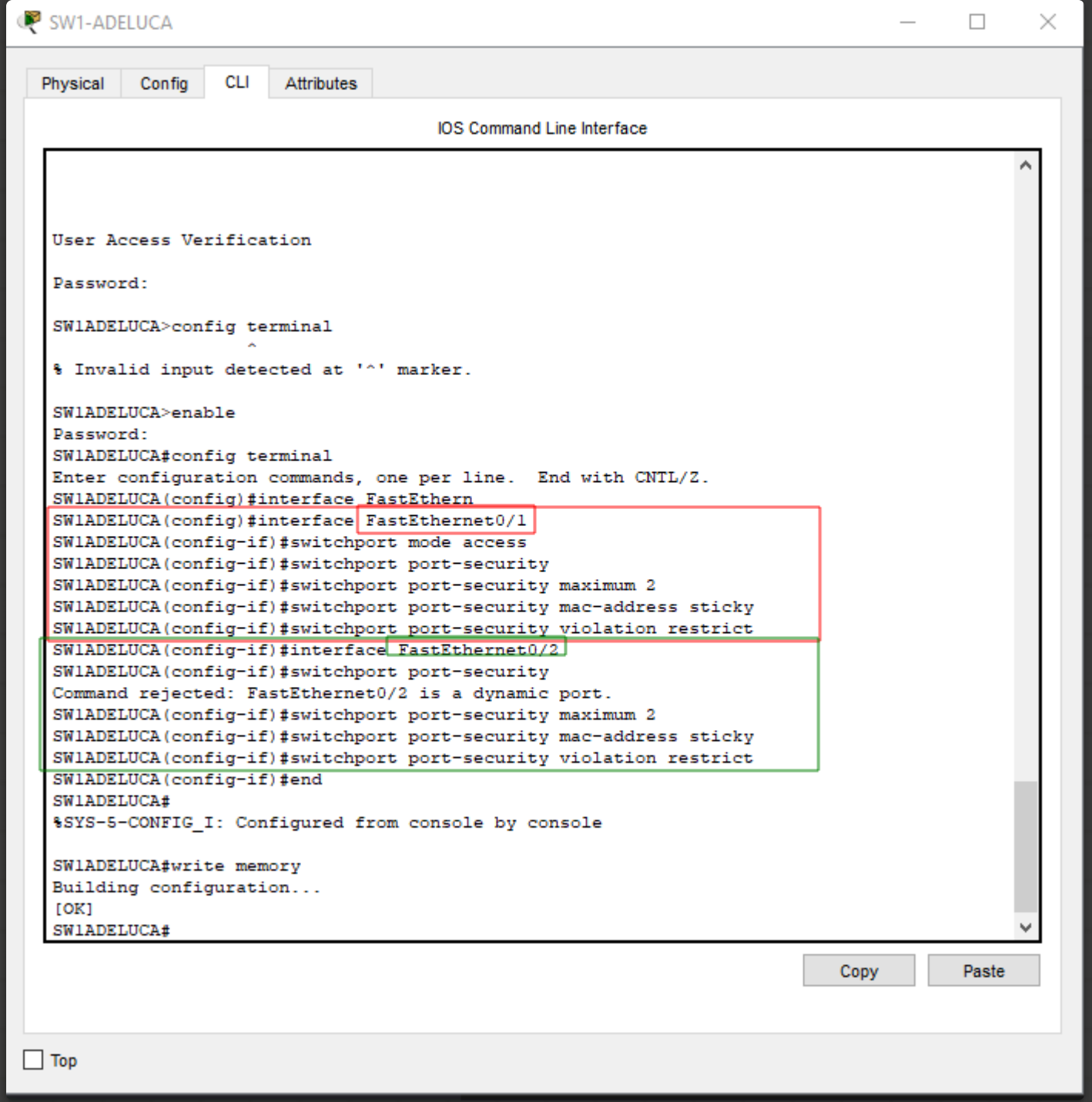
INombreApellido privilege 15 secret securePasswordINombreApellido: Crea un usuario privilegiado con una contraseña segura. Reemplace securePasswordINombreApellido con la contraseña elegida. line vty 0 4 and line vty 5 15: Configura las líneas de terminal virtual (para acceso remoto). transport input ssh: Restringe la entrada en las líneas VTY solo a SSH. login local: Especifica que la autenticación debe realizarse utilizando la base de datos de nombres de usuario local. enable secret secureEnablePasswordINombreApellido: Establece una contraseña cifrada segura para el comando enable. Reemplace secureEnablePasswordINombreApellido con la contraseña de habilitación elegida. service password-encryption: Cifra todas las contraseñas almacenadas en el archivo de configuración.

Se le solicitará la contraseña configurada para el usuario en el Switch 1. También puede intentar conectarse por SSH a la dirección IP del router (192.168.1.1) y a la dirección IP del Switch 2 (10.10.10.2). Verificación de bloqueo de Telnet: Intente conectarse por Telnet a las direcciones IP del router y los switches desde la PC1: telnet 192.168.1.2 La conexión debería ser rechazada o agotar el tiempo de espera, lo que indica que Telnet no está habilitado en las líneas VTY.

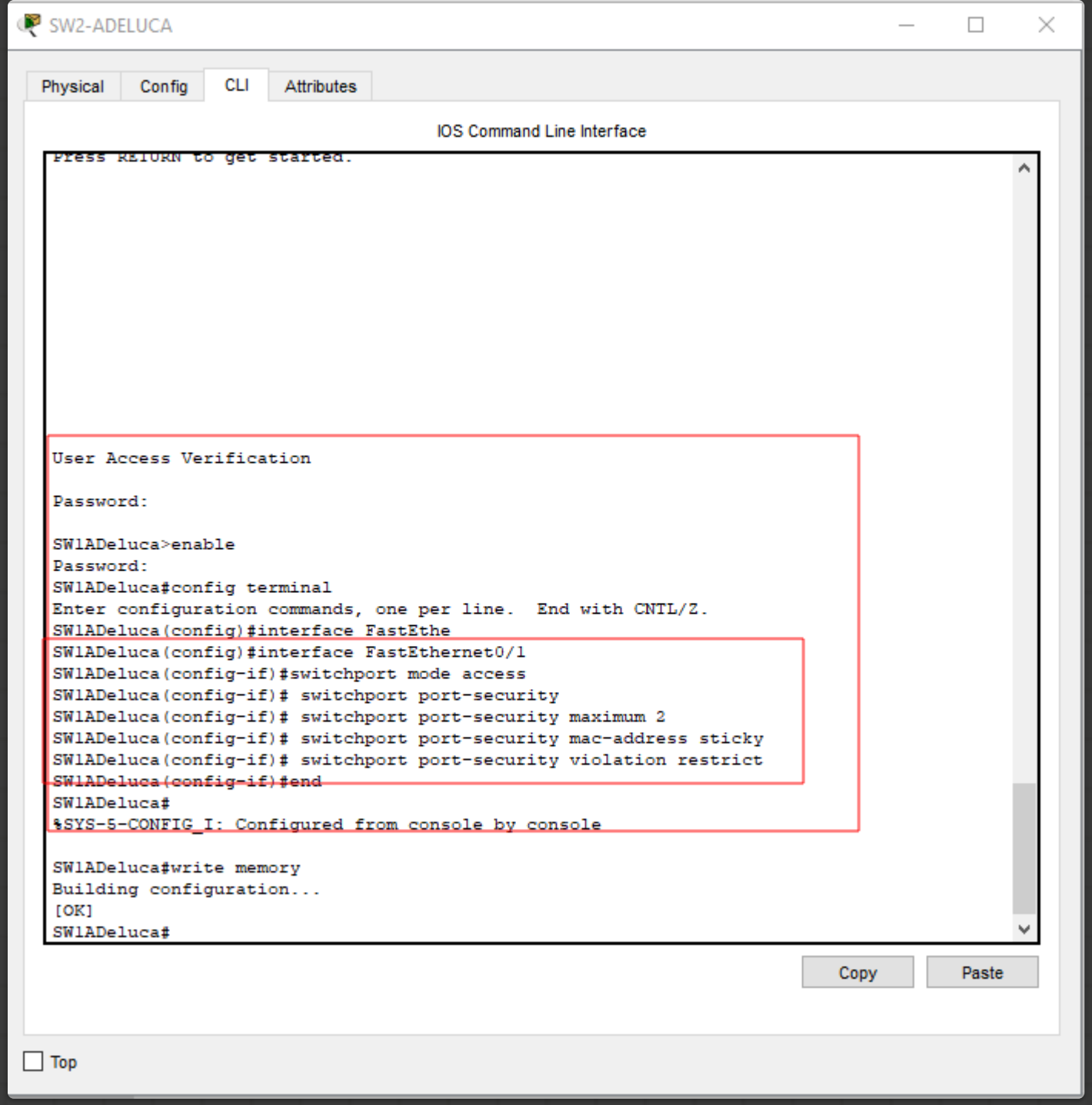


Interfaz FastEthernet0/1 e interfaz FastEthernet0/2: Selecciona las interfaces que se configurarán.
switchport mode access: Establece el puerto en modo de acceso (para conectar dispositivos finales).

switchport port-security: Habilita la seguridad del puerto en la interfaz.
switchport port-security maximum 2: Permite el aprendizaje de un máximo de dos direcciones MAC en el puerto.
switchport port-security mac-address sticky: Habilita las direcciones MAC persistentes, lo que significa que el switch aprenderá automáticamente las direcciones MAC de los dispositivos conectados y las almacenará en la configuración en ejecución.
switchport port-security breach restrict: Configura la acción que se tomará cuando se produzca una violación de seguridad. Restrict descartará paquetes de direcciones MAC no autorizadas y registrará la violación, pero el puerto permanecerá activo.

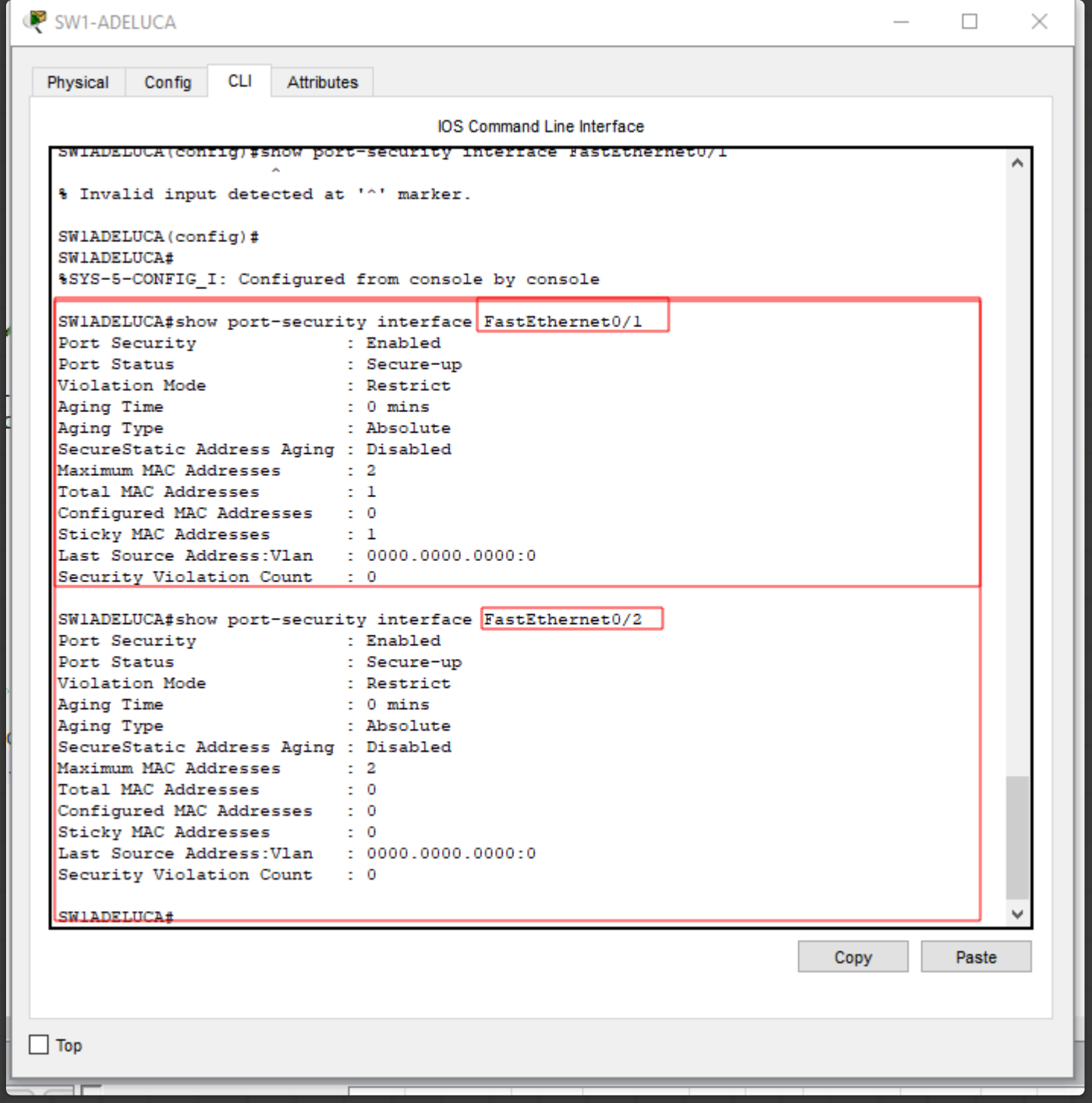


repetir lo mismo con SW2

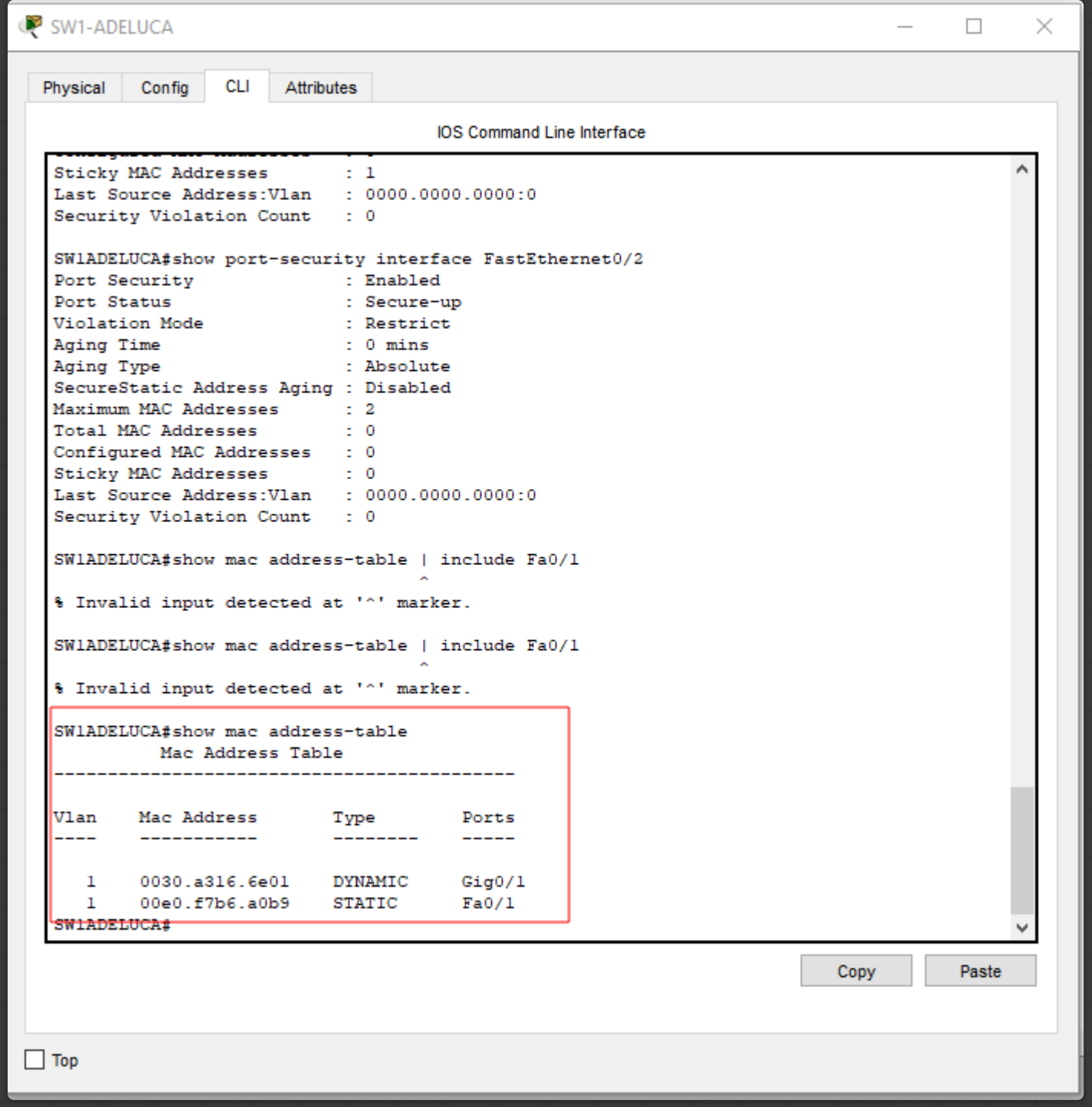


Verificamos la configuracion de SW1

```
show port-security interface FastEthernet0/1
show port-security interface FastEthernet0/2
```




```
show mac address-table
```

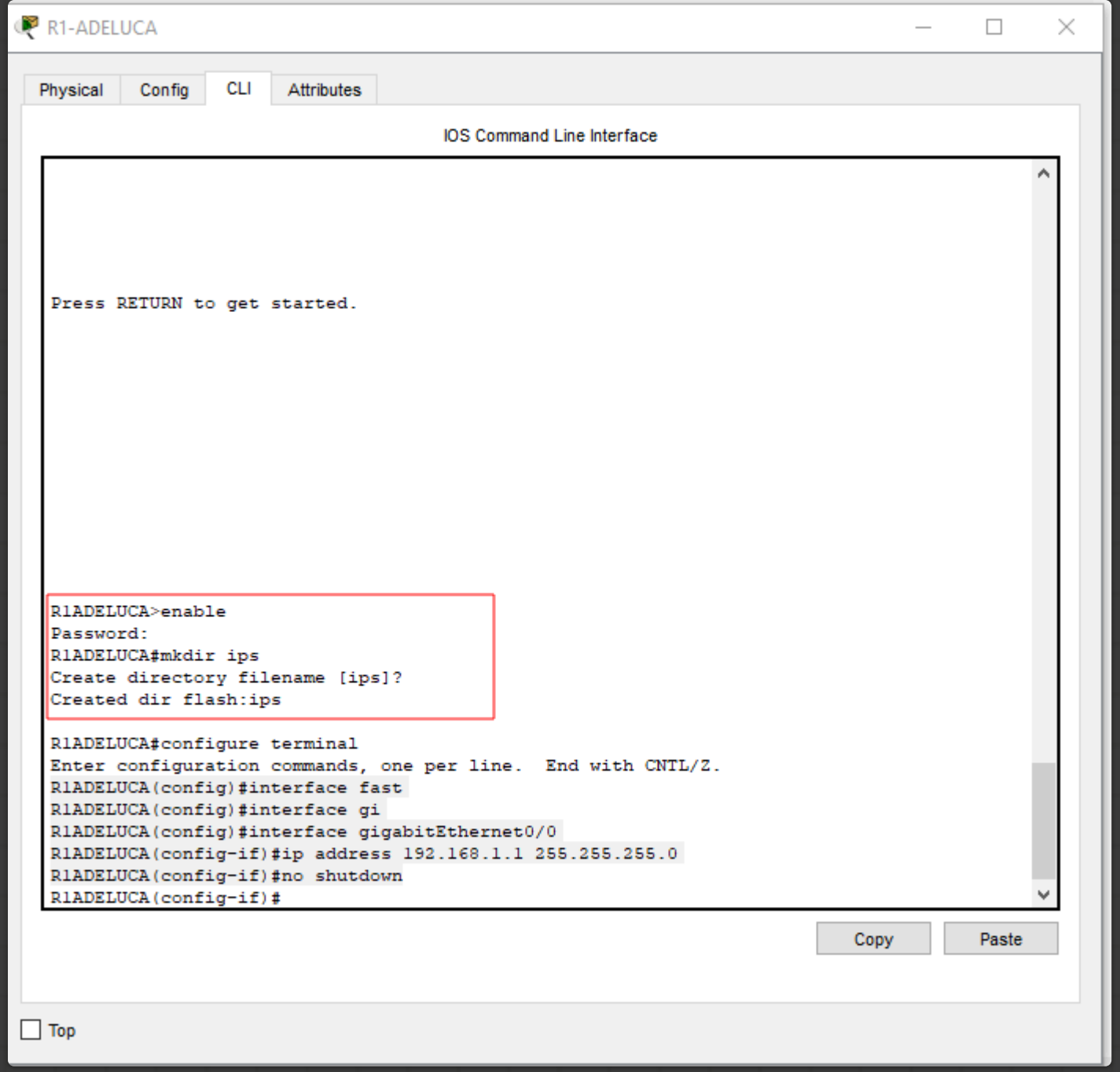


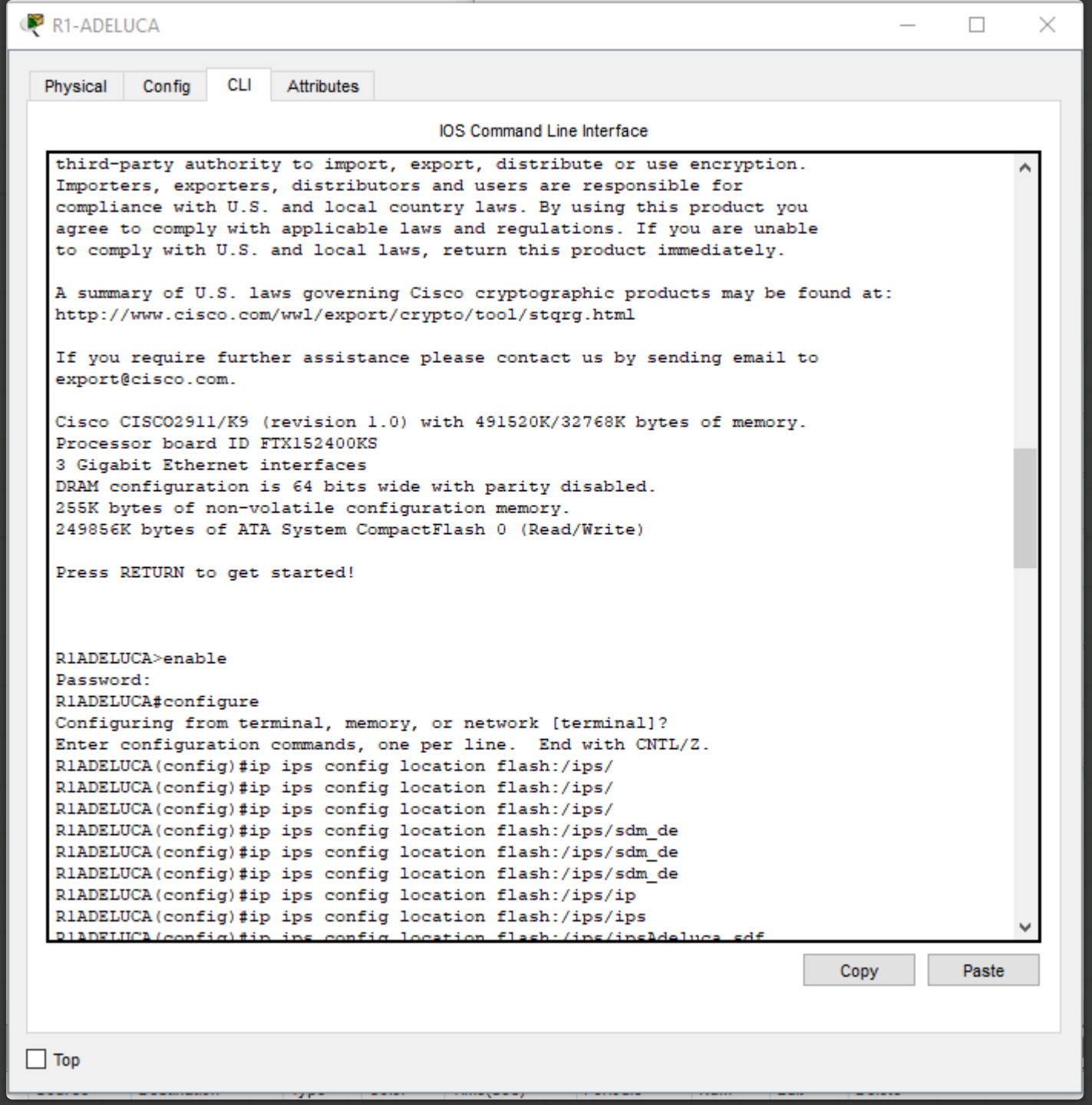
Parte 4: Configuración de IPS en el Router

- **Habilitar un sistema de prevención de intrusos (IPS) básico.**

- **Crear una política IPS con el nombre IPS_NombreApellido.**
- **Aplicar IPS en la interfaz que conecta al switch (GigabitEthernet0/0).**
- **Realizar pruebas de IPS.**
- **Simular intentos de acceso no autorizado y verificar el syslog en el servidor.**

En el Router1 creamos la carpeta “ips” para almacenar firmas y configuraciones de IPS. También se realizaron configuraciones de conectividad básica.


R1-ADELUCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
R1ADELUCA>enable
Password:
R1ADELUCA#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
R1ADELUCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1ADELUCA(config)#interface fast
R1ADELUCA(config)#interface gi
R1ADELUCA(config)#interface gigabitEthernet0/0
R1ADELUCA(config-if)#ip address 192.168.1.1 255.255.255.0
R1ADELUCA(config-if)#no shutdown
R1ADELUCA(config-if)#
Copy
Paste
Top


R1-ADELUCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
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 CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 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!
R1ADELUCA>enable
Password:
R1ADELUCA#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1ADELUCA(config)#ip ips config location flash:/ips/
R1ADELUCA(config)#ip ips config location flash:/ips/
R1ADELUCA(config)#ip ips config location flash:/ips/
R1ADELUCA(config)#ip ips config location flash:/ips/sdm_de
R1ADELUCA(config)#ip ips config location flash:/ips/sdm_de
R1ADELUCA(config)#ip ips config location flash:/ips/sdm_de
R1ADELUCA(config)#ip ips config location flash:/ips/ip
R1ADELUCA(config)#ip ips config location flash:/ips/ips
Copy
Paste
Top

R1-ADELUCA

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
%IPS-3-IPS_FILE_OPEN_ERROR: flash:/ips/Adeluca.sdf/sigdef-delta.xml - Directory doesn't
exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash:/ips/Adeluca.sdf/sigdef-category.xml - Directory
doesn't exist
R1ADELUCA(config)#ip ips config location flash
%IPS-3-IPS_FILE_OPEN_ERROR: flash/sigdef-default.xml - Directory doesn't exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash/sigdef-delta.xml - Directory doesn't exist
%IPS-3-IPS_FILE_OPEN_ERROR: flash/sigdef-category.xml - Directory doesn't exist
R1ADELUCA(config)#ip ips config location flash:
R1ADELUCA(config)#ip ips signature-category
R1ADELUCA(config-ips-category)#category all
R1ADELUCA(config-ips-category-action)#retired true
R1ADELUCA(config-ips-category-action)#exit
R1ADELUCA(config-ips-category)#category ios_ips basic
R1ADELUCA(config-ips-category-action)#retired false
R1ADELUCA(config-ips-category-action)#exit
R1ADELUCA(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

R1ADELUCA(config)#ip ips config location
%IPS: Could not configure empty directory name
R1ADELUCA(config)#ip ips config location flash:/
R1ADELUCA(config)#ip ips notify log
R1ADELUCA(config)#ip ips name IPS_ADeluca
R1ADELUCA(config)#end
R1ADELUCA#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1ADELUCA#
```

Copy | Paste

Top

R1-ADELUCA

Physical | Config | CLI | Attributes

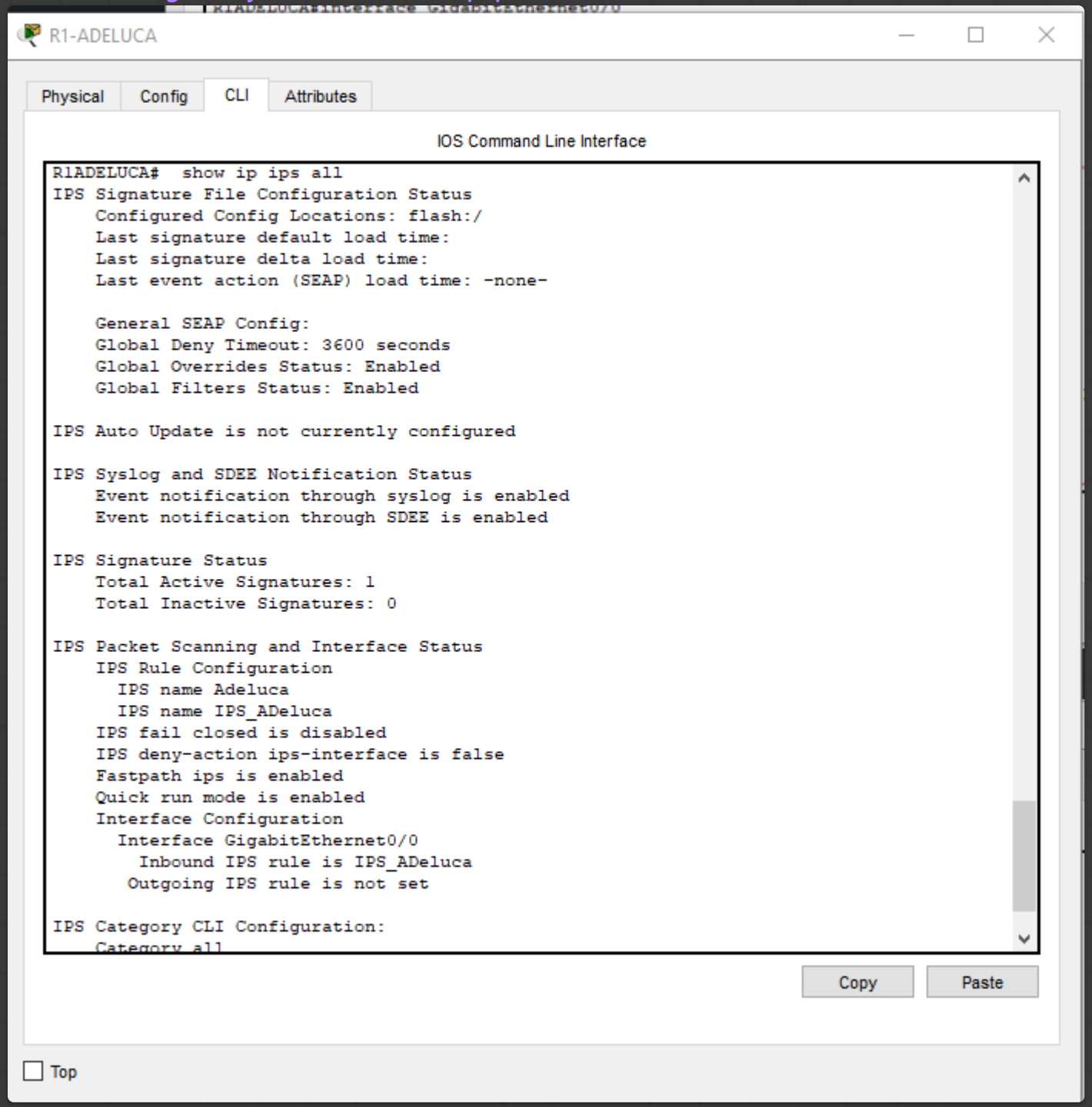
IOS Command Line Interface

```
scanned

R1ADELUCA(config)#ip ips config location
%IPS: Could not configure empty directory name
R1ADELUCA(config)#ip ips config location flash:/
R1ADELUCA(config)#ip ips notify log
R1ADELUCA(config)#ip ips name IPS_ADeluca
R1ADELUCA(config)#end
R1ADELUCA#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1ADELUCA#interface GigabitEthernet0/0
                   ^
% Invalid input detected at '^' marker.

R1ADELUCA# ip ips IPS_InicialNombreApellido in
           ^
% Invalid input detected at '^' marker.

R1ADELUCA#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1ADELUCA(config)#interface GigabitEthernet0/0
R1ADELUCA(config-if)# ip ips IPS_ADeluca in
R1ADELUCA(config-if)#
 %IPS-6-ENGINE_BUILDS_STARTED:  00:25:25 UTC mar. 01 1993

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be
scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

Copy | Paste

Top

- Verificar los registros y alertas con show ip ips statistics.



R1-ADELUCA

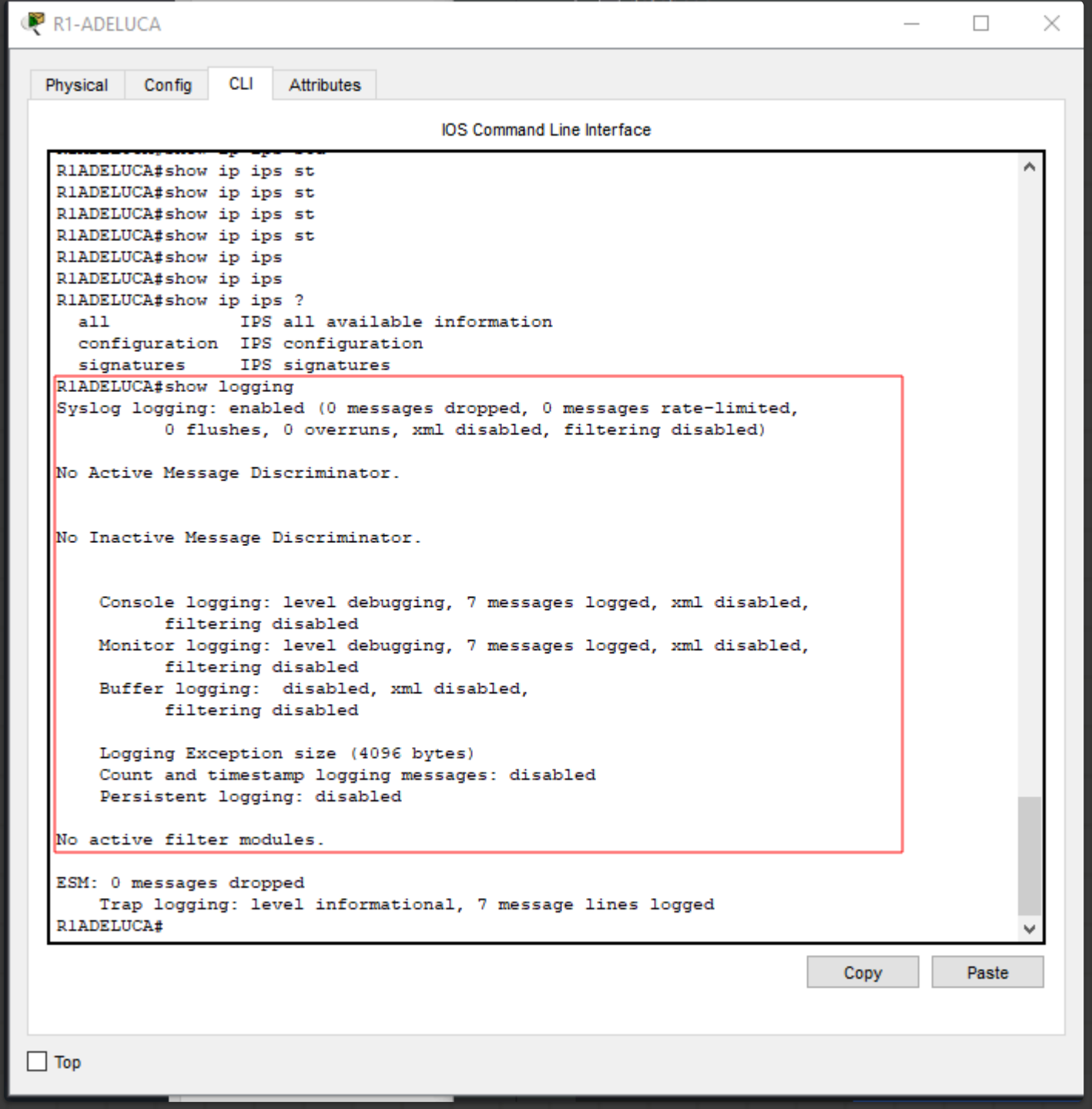
Physical | Config | CLI | Attributes

IOS Command Line Interface

```
R1ADELUCA#show ip ips configuration
IPS Signature File Configuration Status
    Configured Config Locations: flash:/
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name Adeluca
      IPS name IPS_ADeluca
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/0
        Inbound IPS rule is IPS_ADeluca
       Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all
```

Copy | Paste

Top

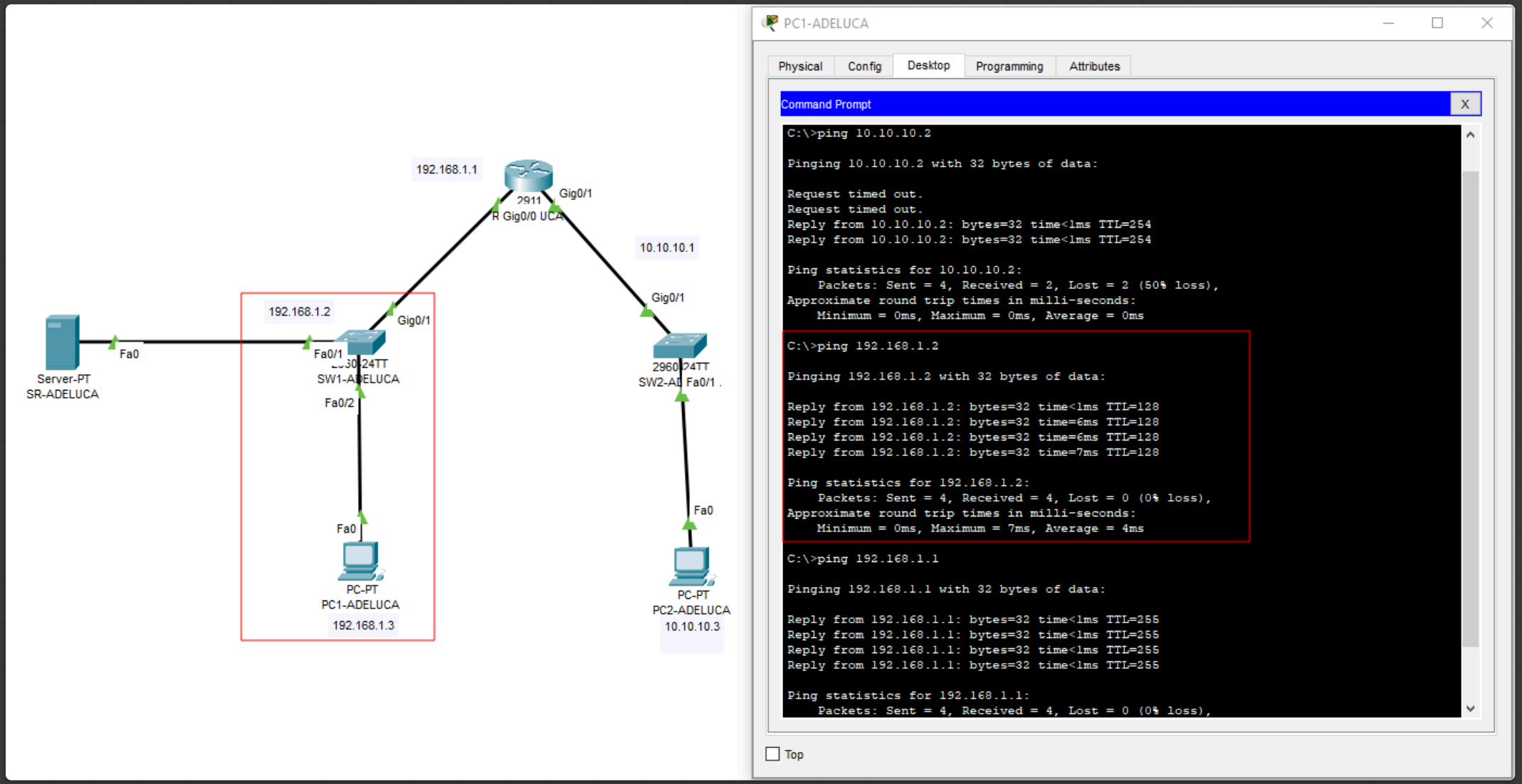


4. Pruebas y Verificación

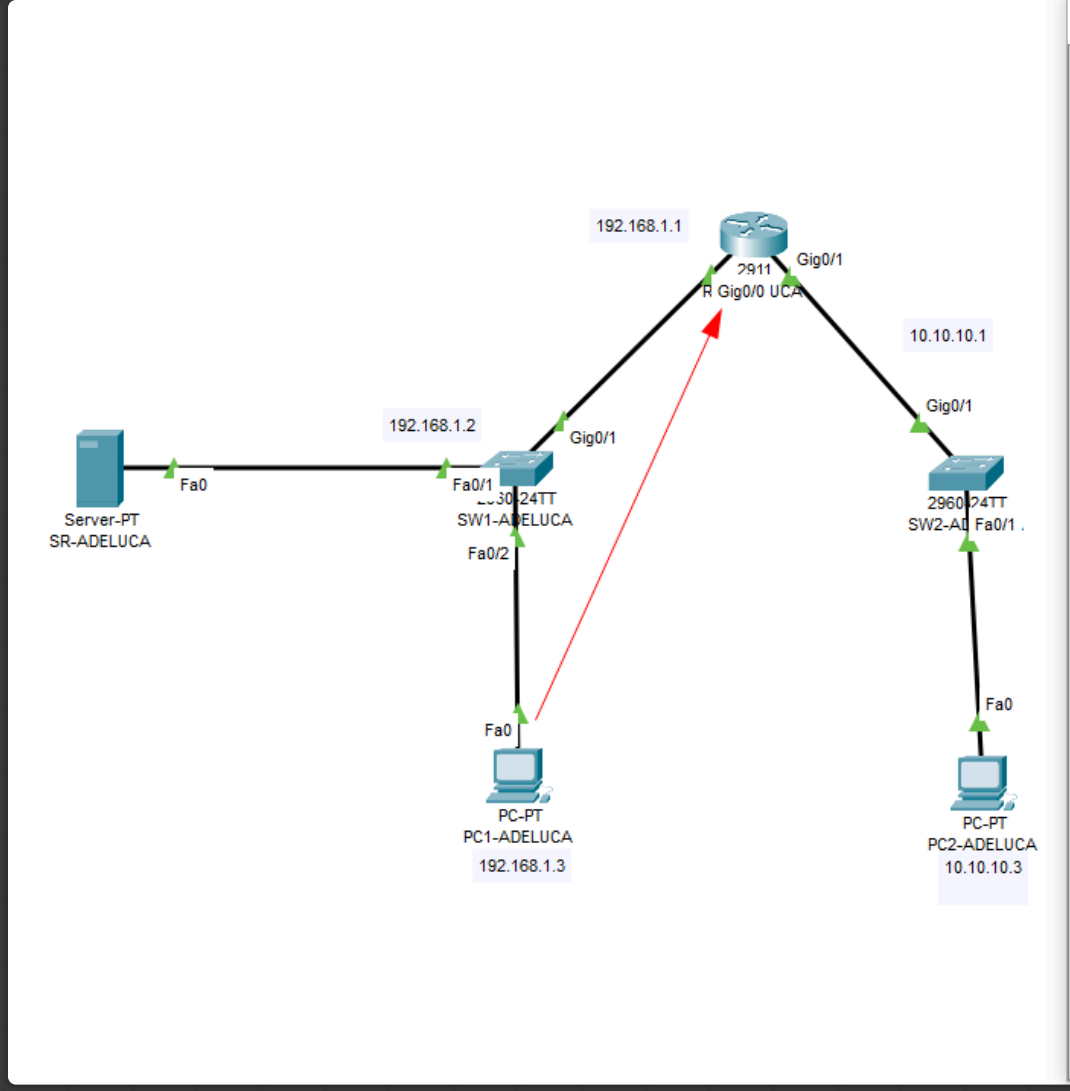
Verificar conectividad:

- **Realizar ping desde cada PC hacia el router y el switch.**

PC1 a SW1



PC1 a R1



PC1-ADELUCA

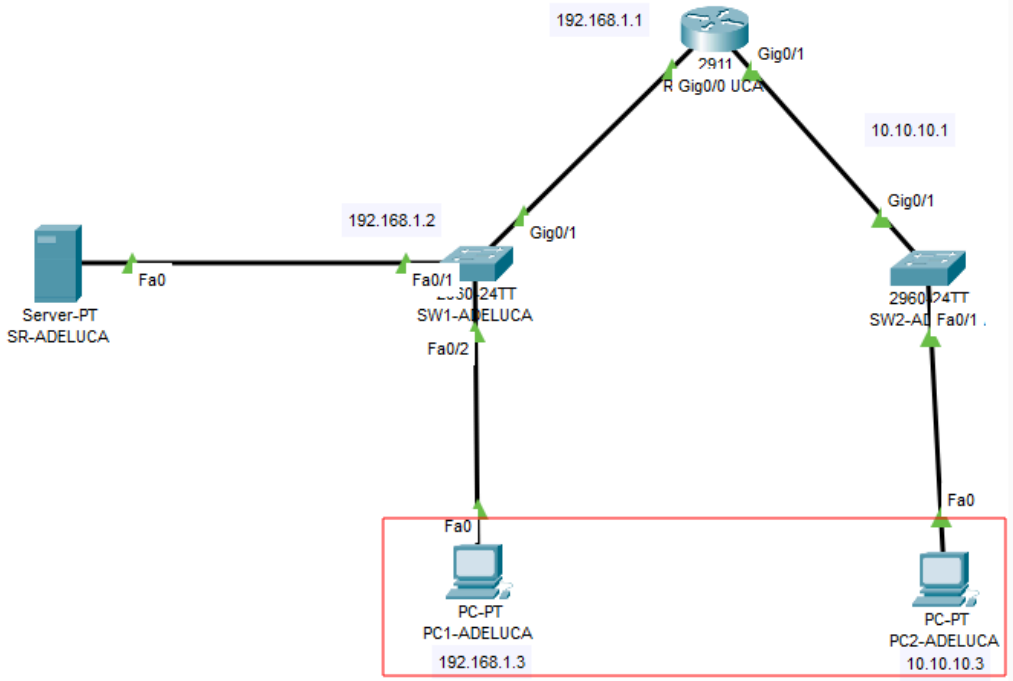
Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.10.10.2: bytes=32 time<1ms TTL=254
Reply from 10.10.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 4ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Top

PC1 a PC2



PC1-ADELUCA

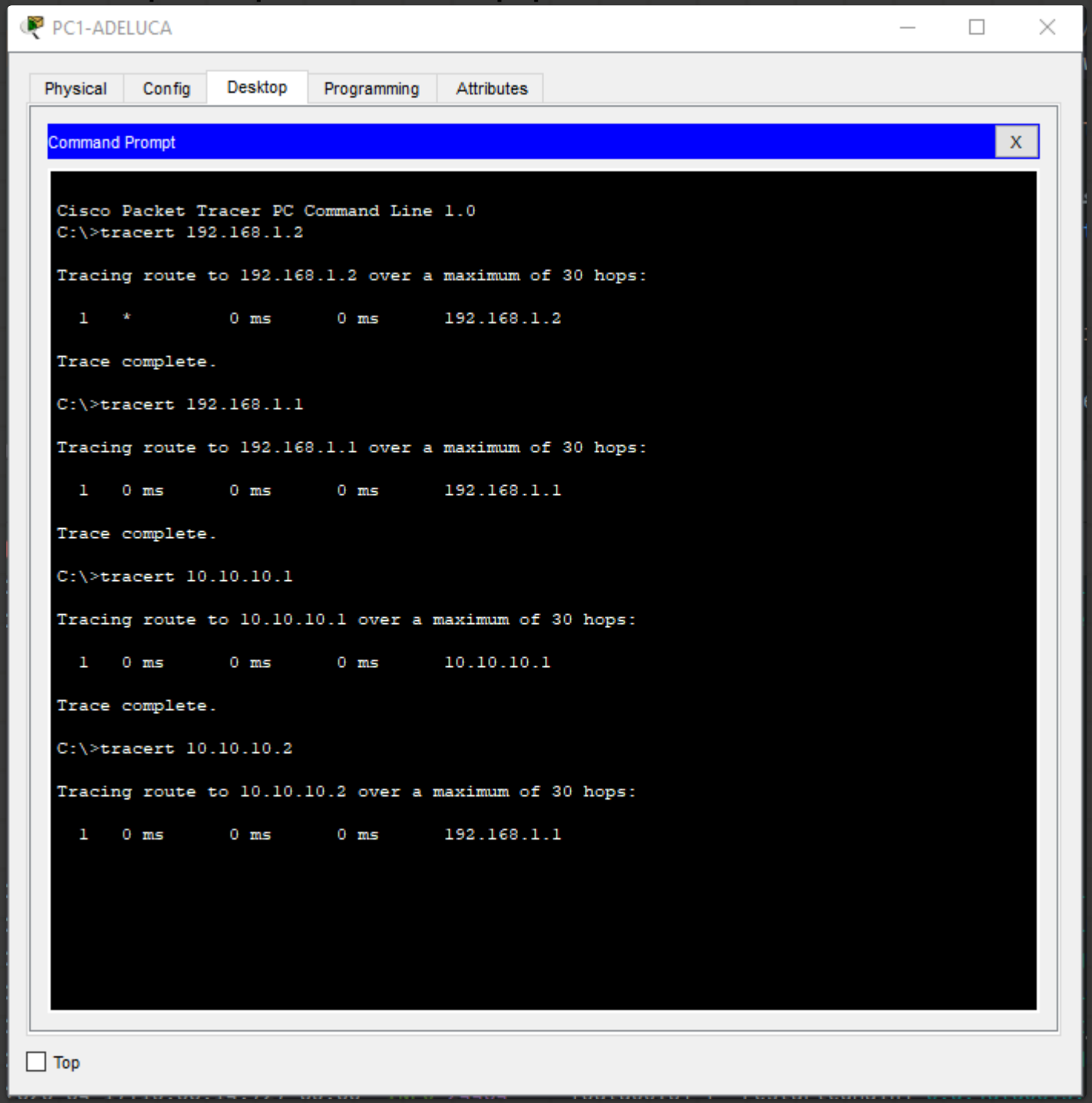
Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 4ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Request timed out.
Reply from 10.10.10.3: bytes=32 time=11ms TTL=127
Reply from 10.10.10.3: bytes=32 time<1ms TTL=127
Reply from 10.10.10.3: bytes=32 time=1ms TTL=127

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 4ms

C:\>
```

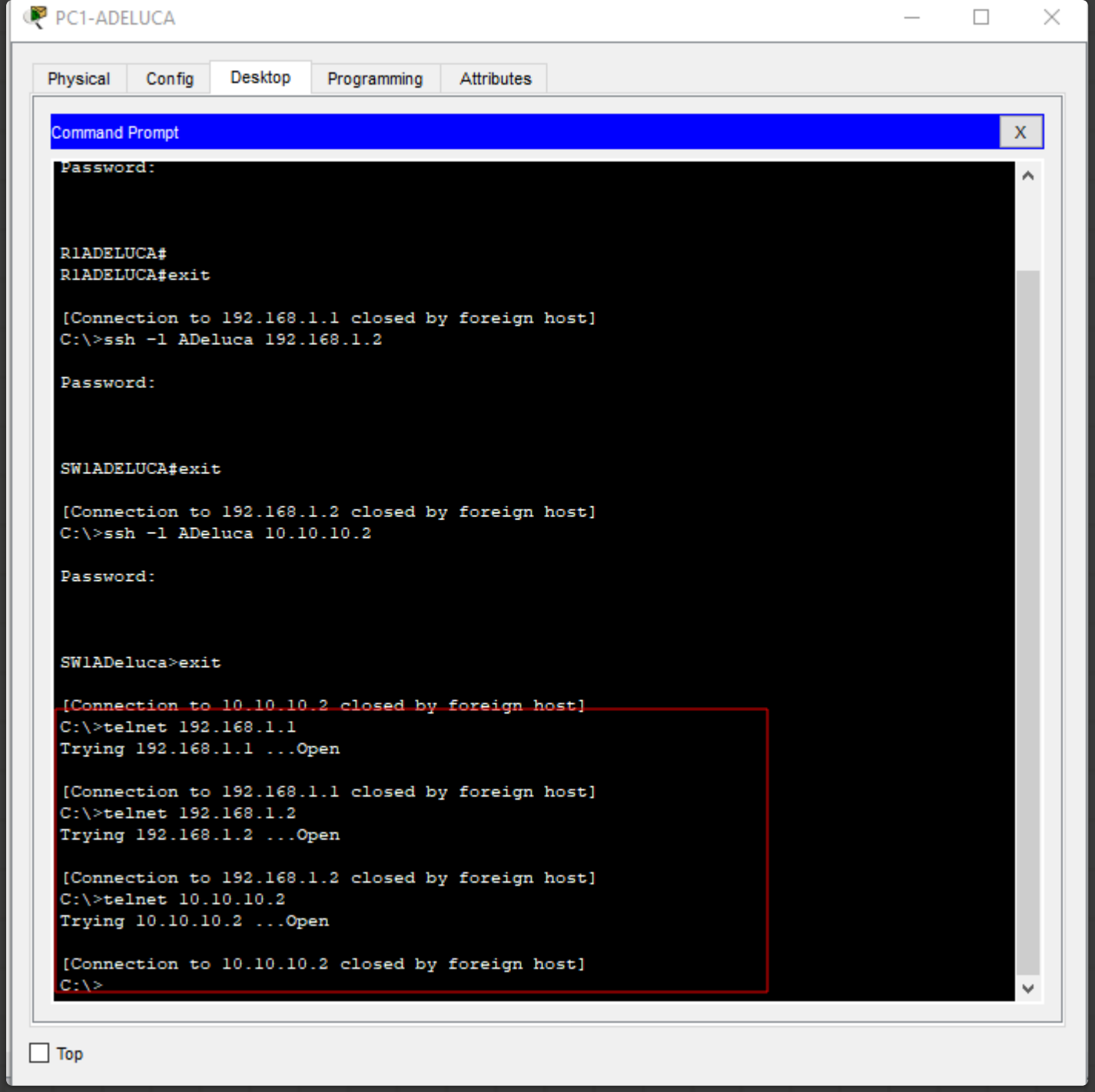
Top

- **Usar tracert para comprobar la ruta de los paquetes.**



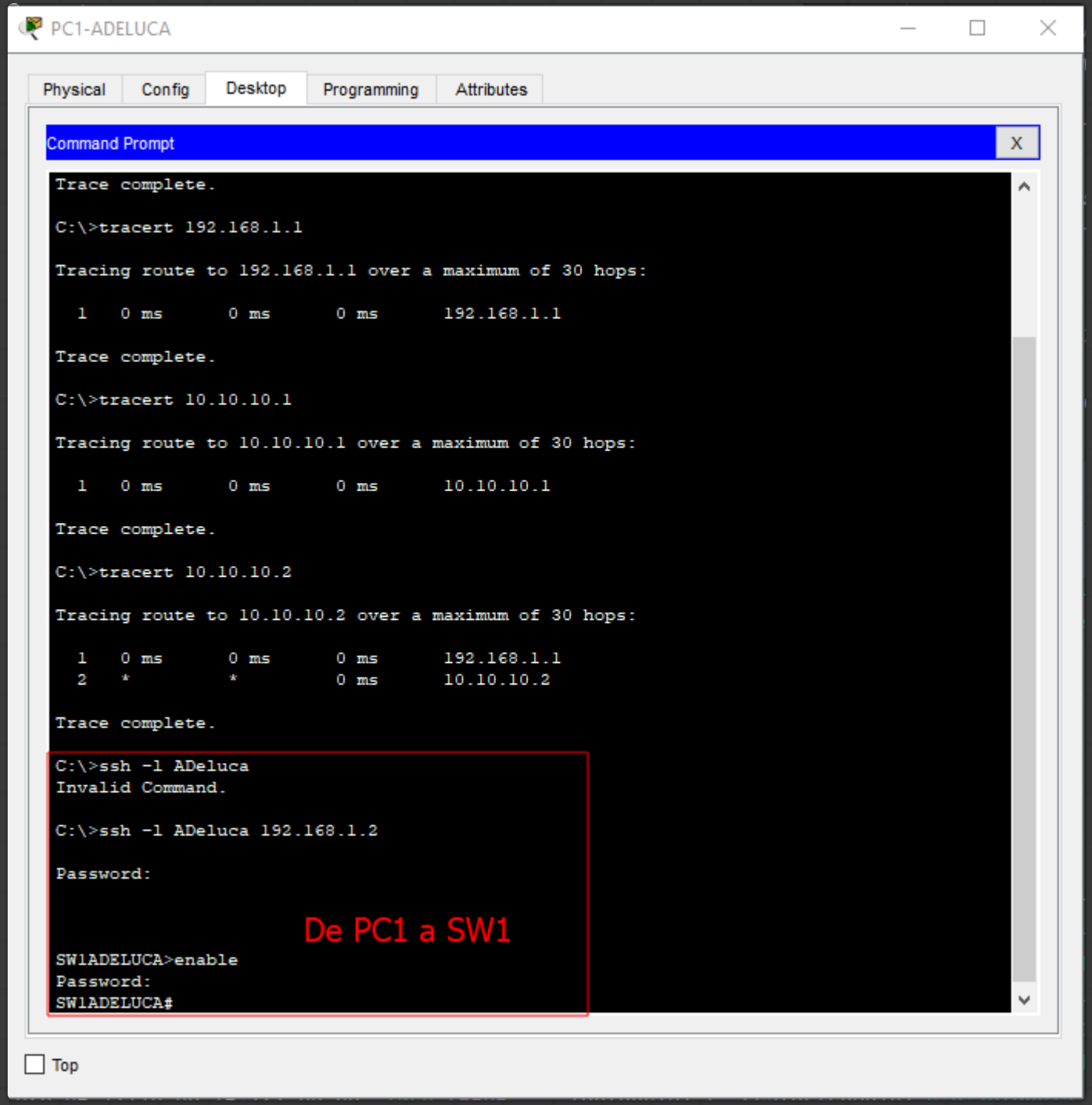
Probar seguridad de acceso:

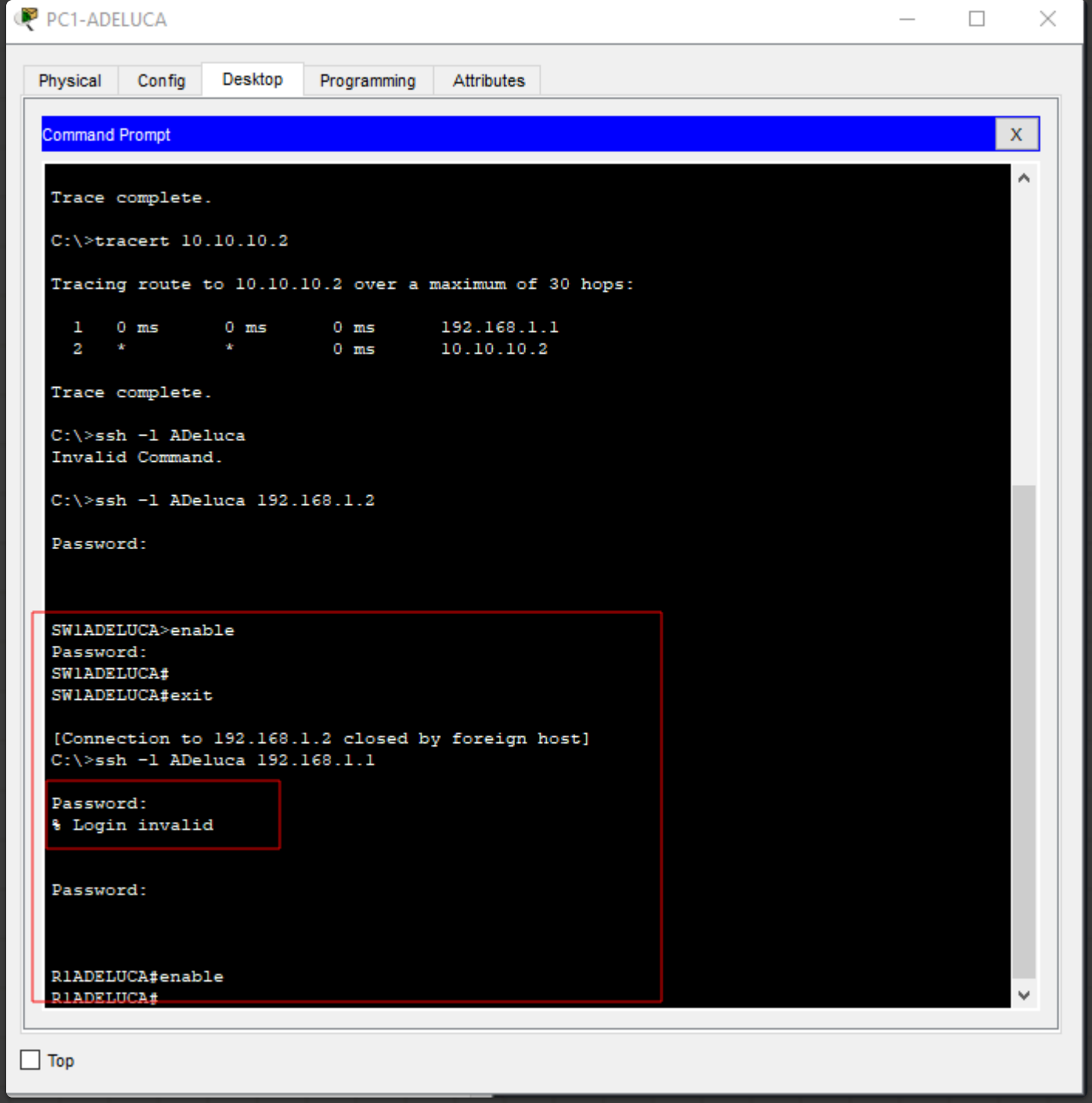
- **Intentar acceso SSH con credenciales correctas e incorrectas.**
- **Comprobar que Telnet esté bloqueado.**



La conexión debería ser rechazada o expirar.

- **Comprobar seguridad en puertos:**





- **Conectar un dispositivo no autorizado y verificar si el puerto lo bloquea.**

Monitorear IPS:

- **Usar show ip ips interfaces para ver el estado del IPS.**
- **Revisar los eventos de seguridad generados.**

Conclusión y Preguntas de Reflexión

Preguntas de Reflexión:

1. ¿Cuáles son los beneficios de utilizar SSH en administración de redes?
   SSH cifra toda la sesión de administración, previniendo que la información sea leída por alguien que capture el tráfico. Tambien asegura que los datos transmitidos no sean modificados en tránsito. Nos proporciona mecanismos de autenticación más fuertes (contraseñas, claves públicas/privadas) para verificar la identidad tanto del usuario como del servidor (dispositivo de red), protegiendo contra suplantación.
2. ¿Cómo puede un atacante explotar puertos abiertos en un switch y cómo lo mitigamos con port-security?
   Conectando su propio dispositivo (laptop) a un puerto de switch activo y no asegurado en un área física accesible (sala de reuniones, punto de red en pared) para obtener acceso a la red local. Inundando el switch con tramas Ethernet que contienen direcciones MAC de origen falsas. Si la tabla CAM (MAC Address Table) del switch se llena, este puede empezar a comportarse como un hub, reenviando todo el tráfico por todos los puertos, permitiendo al atacante capturar tráfico de otros usuarios (sniffing). Otra de las opciones es conectándose a un puerto abierto, un atacante puede ejecutar un servidor DHCP falso para asignar IPs mal configuradas (ej., con un gateway o DNS malicioso) o agotar las direcciones IP del servidor DHCP legítimo.
3. ¿Qué impacto tiene un IPS en la seguridad de la red y cuáles son sus limitaciones?
   - Positivo:
     Un IPS puede identificar patrones de tráfico asociados con ataques conocidos (virus, gusanos, exploits, escaneos) basados en firmas y, si está configurado para prevenir, puede bloquear activamente ese tráfico antes de que alcance su objetivo. A su vez proporciona información sobre los tipos de ataques que intentan ingresar a la red. Mientras que los firewalls suelen operar basados en puertos, protocolos e IPs, un IPS inspecciona el contenido del tráfico (inspección profunda de paquetes - DPI) buscando amenazas dentro de tráfico permitido por el firewall.
   - Limitaciones:
     Principalmente efectivo contra amenazas conocidas para las cuales existe una firma. Los ataques nuevos o desconocidos (Zero-Day) pueden pasar desapercibidos hasta que se cree y distribuya una nueva firma. Tampoco puede inspeccionar el contenido del tráfico cifrado (HTTPS, SSH, VPNs) a menos que se implementen soluciones de descifrado (como SSL Decryption/Inspection), lo cual añade complejidad y sobrecarga. Una inspección profunda de paquetes consume recursos significativos (CPU, memoria), puede impactar el rendimiento del dispositivo donde se ejecuta (router, firewall) y potencialmente convertirse en un cuello de botella. El IPS puede no

detectar un ataque real, ya sea por falta de firma, evasión por parte del atacante, o configuración inadecuada. Para finalizar requiere actualizaciones constantes de las firmas y del software para mantenerse efectivo.