DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Jennifer Molina Diaz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *TELECOMUNICACIONES*
BOGOTA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Jennifer Molina Diaz

Diplomado de opción de grado presentado para optar el título de INGENIERO *TELECOMUNICACIONES*

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA *TELECOMUNICACIONES*
BOGOTA
2020

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 19 de octubre de 2020

AGRADECIMIENTOS

Quiero agradecer a mis padres y a mi hermano y familia por llegar hasta este punto de mi vida y poder decir que he finalizado otro capítulo de mi etapa de estudio, y verme graduada como ingeniera de telecomunicaciones ya que fue un largo camino hasta aquí.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO: es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

CCNP: La certificación Cisco Certified Network Professional (CCNP) enrutamiento y conmutación valida la capacidad de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia y trabajar en colaboración con especialistas en seguridad avanzada, voz, soluciones inalámbricas y de video.

REDES: Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un ejemplo es Internet, el cual es una gran red de millones de ordenadores ubicados en distintos puntos del planeta interconectados básicamente para compartir información y recursos

ROUTER: Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

RESUMEN

En el siguiente trabajo se abarcan temas tan importantes como la configuración de las redes y los métodos que más se utilizan para crear, modificar, y realizar enlaces con el uso de diferentes canales en base a la tecnología usada por Cisco junto con sus equipos de red. Teniendo en cuenta lo anterior y en la fase final del curso en CCNP y para probar las habilidades adquiridas es necesario que se desarrollen las dos simulaciones propuestas, con diferentes aspectos para lograr un networking exitoso soportado en la configuración de Vlans, administración y enrutamiento, utilización de protocolos y algo que es muy importante con la introducción de las direcciones IPV6 y cómo utilizarlas en los diferentes escenarios.

Veremos cómo paso a paso se va dando solución a el ejercicio planteado utilizando el software Packet tracer en Routers y switch.

Para conseguir que se cumpla con el objetivo de esta actividad es necesario cumplir con los estándares de calidad establecidos por la Universidad y los conocimientos obtenidos en el transcurso del curso.

Palabras Clave: CISCO, CCNP, REDES, ROUTER, SWITCH, IPV6, NETWORKING.

ABSTRACT

The following work covers topics as important as the configuration of the networks and the methods that are most used to create, modify, and make links with the use of different channels based on the technology used by Cisco together with its network equipment . Taking into account the above and in the final phase of the course in CCNP and to test the acquired skills it is necessary to develop the two simulations proposed, with different aspects to achieve a successful networking supported in the configuration of Vlans, administration and routing, use of protocols and something that is very important with the introduction of IPV6 addresses and how to use them in different scenarios.

We will see how step by step solution is being given to the exercise proposed using the Packet tracer software on routers and switches.

In order to achieve the objective of this activity, it is necessary to comply with the quality standards established by the University and the knowledge obtained during the course.

Keywords: CISCO, CCNP, REDES, ROUTER, SWITCH, IPV6, NETWORKING.

INTRODUCCIÓN

El presente trabajo de la asignatura CCNP correspondiente a la actividad final Prueba de Habilidades, se puso en práctica todas las unidades manejadas en el transcurso de la materia. Las redes de la actualidad tienen un impacto significativo en nuestras vidas, ya que cambian nuestra forma de vivir, trabajar y divertirnos. Las redes de computadoras permiten a las personas comunicarse, colaborar e interactuar de maneras totalmente. Utilizamos la red de distintas formas, entre ellas las aplicaciones web, la telefonía IP, video conferencia, los juegos interactivos, el comercio electrónico, la educación y más.

En este trabajo se desarrollan los conceptos y temáticas descritos durante el curso para ser puestos en práctica durante el diplomado de profundización cisco, para ello tenemos tres propuestas representadas en escenarios, donde se aplica el direccionamiento, protocolos de enrutamiento OSPF, EIGRP 10, interfaces, vlans, se configuran relaciones de vecinos BGP, VTP y DTP; actividades desarrolladas en packet tracer.

Se realizará verificación de conectividad mediante pruebas con el uso de los comandos ping, traceroute, show ip router, show run para verificar la configuración completa y detallada de los switch y router cisco implementado en los escenarios. Con el fin de validar el procedimiento.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

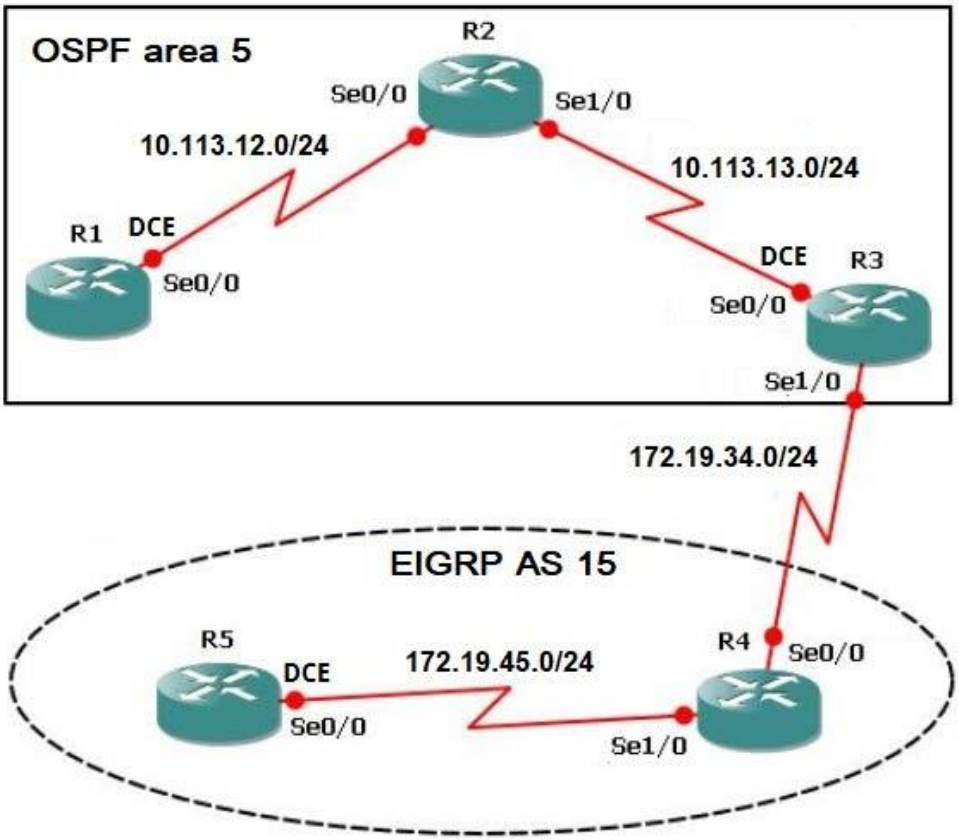
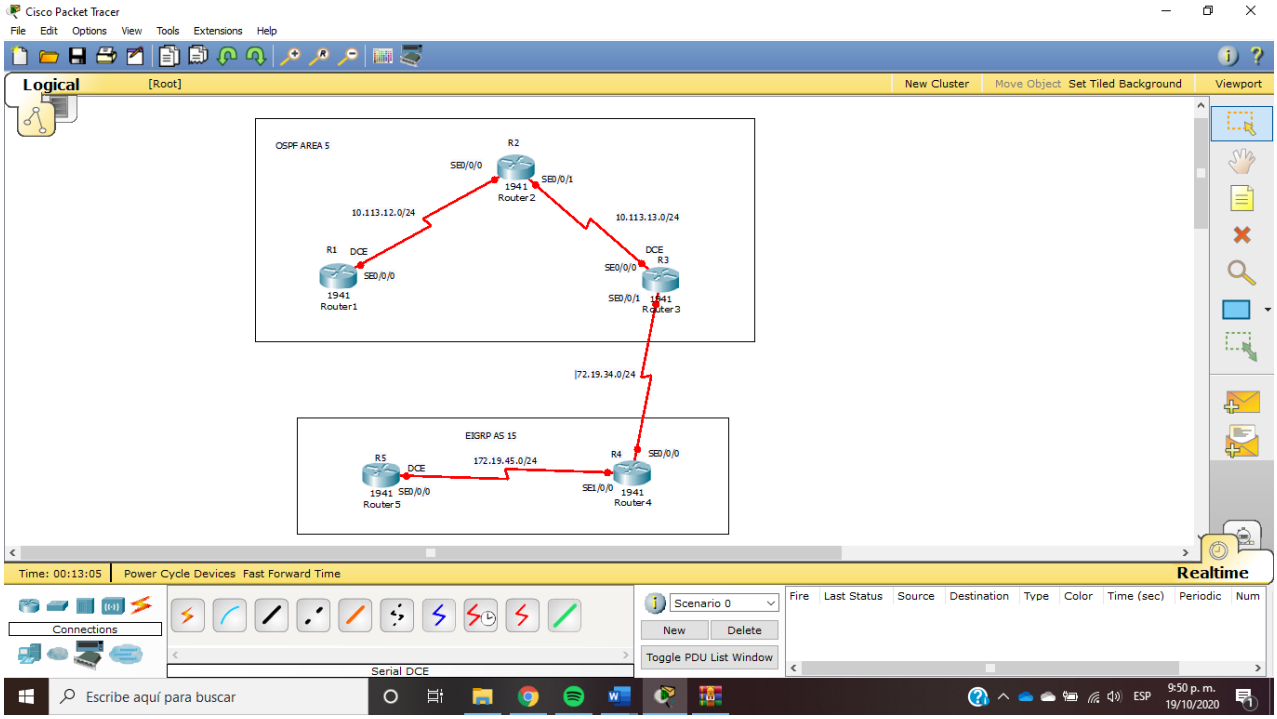


Figura 2. Simulación de escenario 1



1.1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Se procede a configurar cada uno de los enrutadores. 1, 2, 3, 4, 5
Se asignan nombre y protocolos de comunicación mediante EIGRP que fueron asignados.

Se adjunta código y pantallazos con veracidad del código.

Tabla 1. Interfaces loopback para crear R1

Router 1	interface Loopback 11
IP	ip address 10.1.0.0 255.255.255.252
IP	ip address 10.1.1.1 255.255.255.252
IP	ip address 10.103.12.1 255.255.255.248

Router R1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface lo0 11
                   ^
% Invalid input detected at '^' marker.

R1(config)#interface Lo0 11
                   ^
% Invalid input detected at '^' marker.

R1(config)#interface Loopback 11

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback11, changed state to up

R1(config-if)#ip address 10.1.0.0 255.255.255.252
Bad mask /30 for address 10.1.0.0
R1(config-if)#ip address 10.1.1.1 255.255.255.252
R1(config-if)#exit
R1(config)#interface serial0/0/0
R1(config-if)#descriptio R1
R1(config-if)#clock rate 64000
R1(config-if)#bandwith 64
                ^
% Invalid input detected at '^' marker.

R1(config-if)#bandwidth 64
R1(config-if)#ip address 10.103.12.1 255.255.255.248
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
```

Figura 3. Aplicando código R1

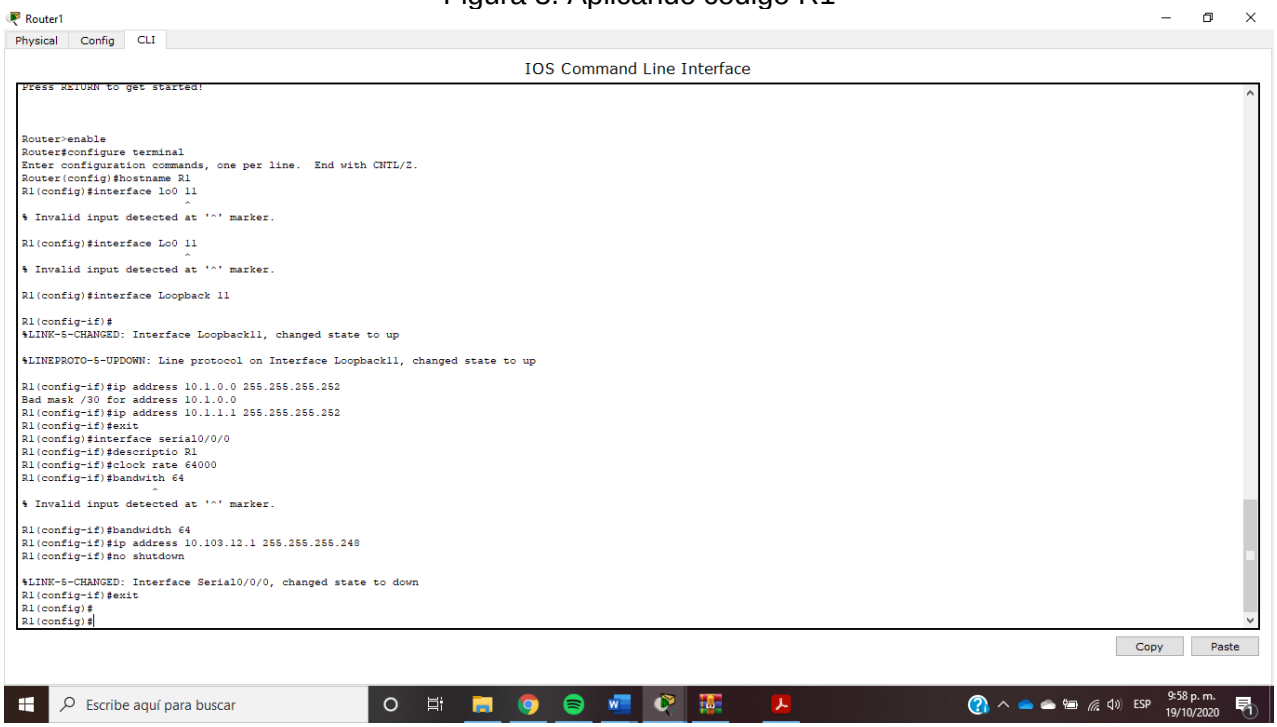


Tabla 2. Interfaces loopback para crear R2

Router 2	interface Loopback 23
IP	ip address 10.1.2.1 255.255.255.252
IP	ip address 10.103.12.2 255.255.255.248
IP	ip address 10.103.23.2 255.255.255.248

Router R2

R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2
R2(config)#interface Loopback 23

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback23, changed state to up

R2(config-if)#ip address 10.1.2.1 255.255.255.252
R2(config-if)#exit
R2(config)#interface serial0/0/0
R2(config-if)#description R2->R1
R2(config-if)#bandwidth 64

R2(config-if)#ip address 10.103.12.2 255.255.255.248
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#exit
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R2(config)#interface serial0/0/1
R2(config-if)#description R2->R3
R2(config-if)#clock rate 64000
R2(config-if)#bandwidth 64
R2(config-if)#ip address 10.103.23.2 255.255.255.248
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit

Figura 4. Aplicando código R2

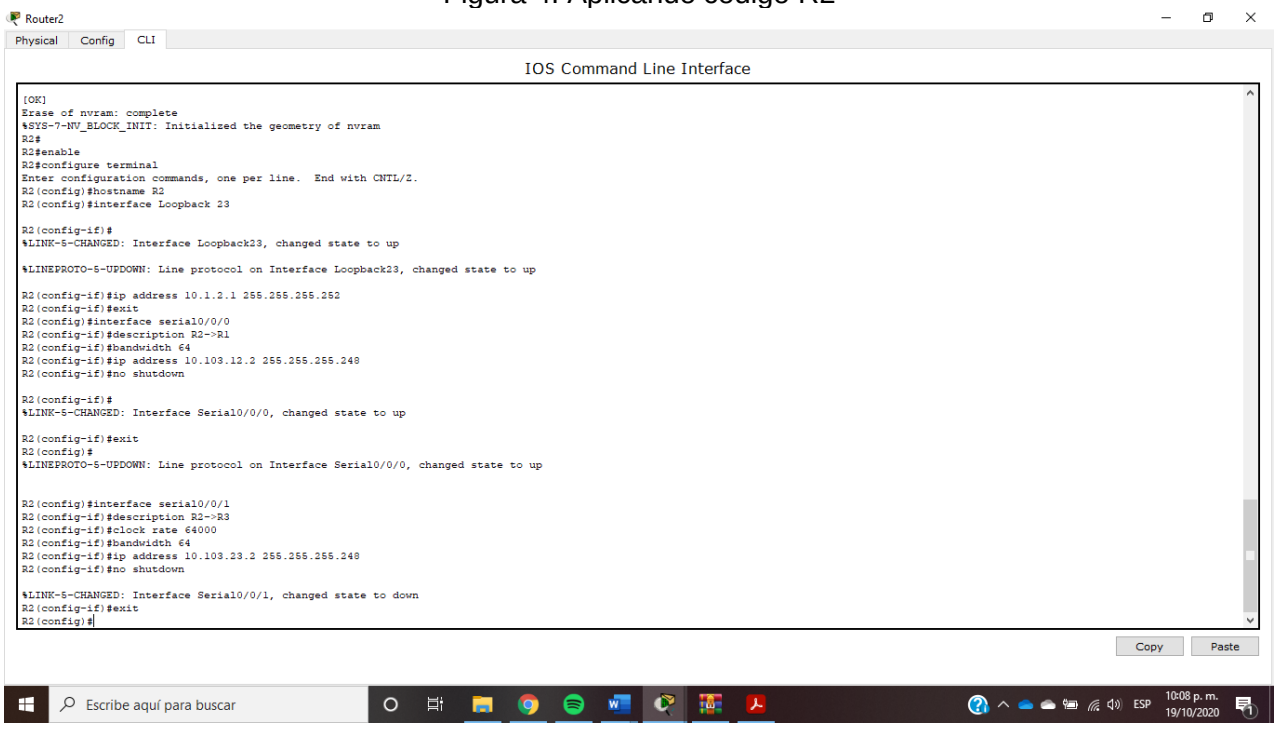


Tabla 3. Loopback para crear R3

Router 3	interface Loopback 33
IP	ip address 10.1.3.1 255.255.255.252
IP	ip address 10.103.23.3 255.255.255.248

IP	ip address 10.103.23.3 255.255.255.248

Router R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#hostname R3
R3(config)#interface Loopback 33

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback33, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback33, changed state to up

R3(config-if)#ip address 10.1.3.1 255.255.255.252
R3(config-if)#exit
R3(config)#interface serial0/0/0
R3(config-if)#description R3->R2
R3(config-if)#clock rate 64000
This command applies only to DCE interfaces
R3(config-if)#bandwidth 64
R3(config-if)#ip address 10.103.23.3 255.255.255.248
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R3(config-if)#exit
R3(config)#no shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R3(config)#interface serial0/0/1
R3(config-if)#description R3->R4
R3(config-if)#bandwidth 64
R3(config-if)#ip address 172.29.34.4 255.255.255.248
R3(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#exit
```

Figura 5. Aplicando código R3

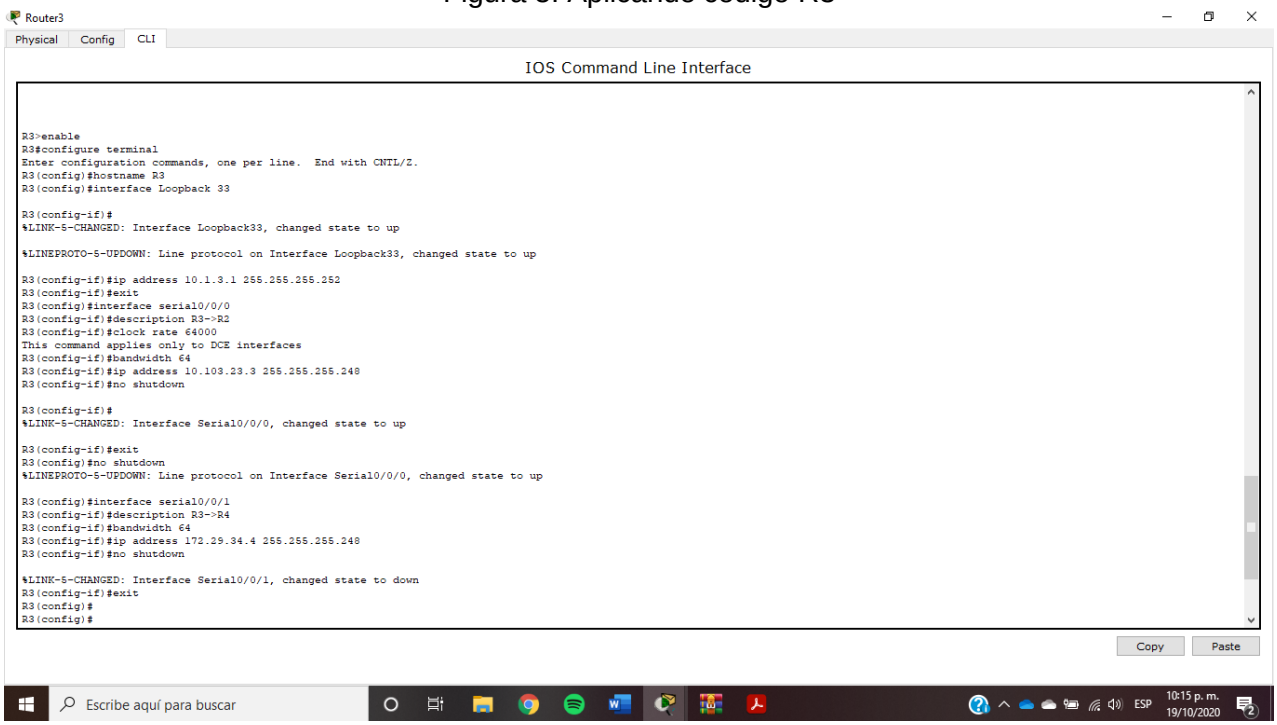


Tabla 4. Loopback para crear R4

Router 4	interface Loopback 43
IP	ip address 10.1.4.1 255.255.255.252
IP	ip address 172.29.34.4 255.255.255.248
IP	ip address 172.29.45.5 255.255.255.248

Router R4

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#interface Loopback 43

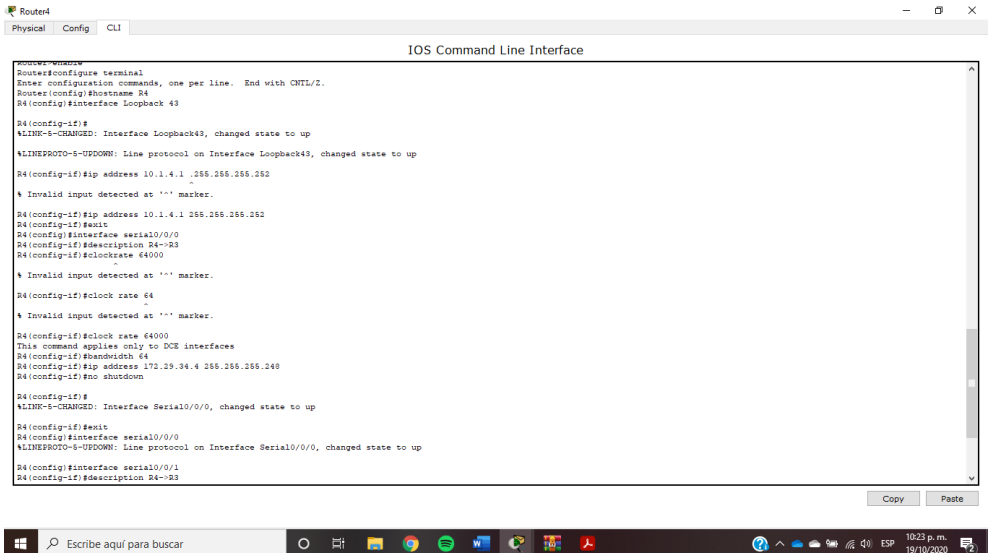
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback43, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback43, changed state to up

R4(config-if)#ip address 10.1.4.1 .255.255.255.252
                                  ^
% Invalid input detected at '^' marker.

```
R4(config-if)#ip address 10.1.4.1 255.255.255.252
R4(config-if)#exit
R4(config)#interface serial0/0/0
R4(config-if)#description R4->R3
R4(config-if)#clockrate 64000
               ^
% Invalid input detected at '^' marker.

R4(config-if)#clock rate 64
                    ^
% Invalid input detected at '^' marker.

R4(config-if)#clock rate 64000
This command applies only to DCE interfaces
R4(config-if)#bandwidth 64
R4(config-if)#ip address 172.29.34.4 255.255.255.248
R4(config-if)#no shutdown

R4(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R4(config-if)#exit
R4(config)#interface serial0/0/0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R4(config)#interface serial0/0/1
R4(config-if)#description R4->R3
R4(config-if)#bandwidth 64
R4(config-if)#ip address 172.29.45.5 255.255.255.248
R4(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R4(config-if)#exit
R4(config)#router eigrp 10
R4(config-router)#network 10.0.0.0
R4(config-router)#exit
R4(config)#exit
R4#
```

Figura 6. Aplicando código R4



Router R5

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R5
R5(config)#interface Loopback 53

R5(config-if)#
%LINK-5-CHANGED: Interface Loopback53, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback53, changed state to up

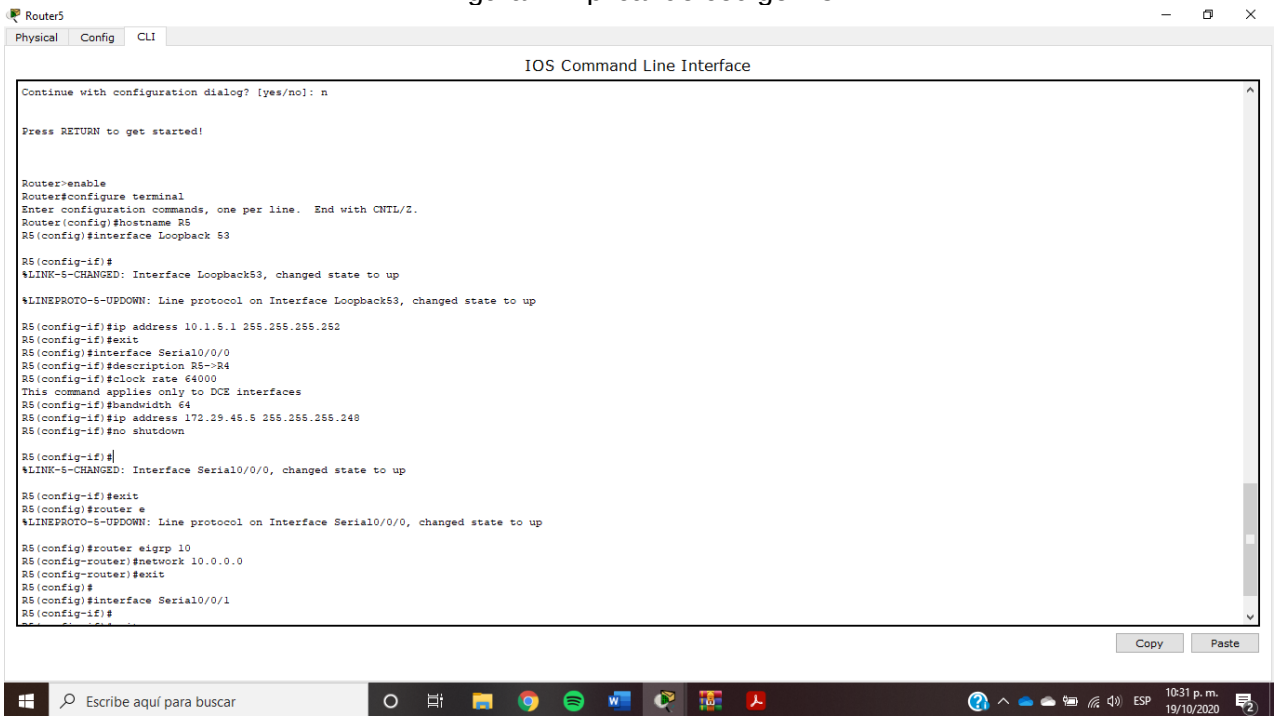
R5(config-if)#ip address 10.1.5.1 255.255.255.252
R5(config-if)#exit
R5(config)#interface Serial0/0/0
R5(config-if)#description R5->R4
R5(config-if)#clock rate 64000
This command applies only to DCE interfaces
R5(config-if)#bandwidth 64
R5(config-if)#ip address 172.29.45.5 255.255.255.248
R5(config-if)#no shutdown

R5(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R5(config-if)#exit
R5(config)#router e
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
R5(config)#router eigrp 10

```
R5(config-router)#network 10.0.0.0
R5(config-router)#exit
```

Figura 7. Aplicando código R5



1.2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 5 de OSPF.

```
R1>enable
R1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Loopback 20

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback20, changed state to up

R1(config-if)#ip address 10.1.1.3 255.255.255.252
Bad mask /30 for address 10.1.1.3
R1(config-if)#
R1(config-if)#ip address 10.1.1.4 255.255.255.252
Bad mask /30 for address 10.1.1.4
R1(config-if)#ip address 10.1.1.5 255.255.255.252
R1(config-if)#exit
R1(config)#interface Loopback 30
```

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback30, changed state to up

R1(config-if)#ip address 10.1.1.9 255.255.255.252
R1(config-if)#exit
R1(config)#interface Loopback 40

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback40, changed state to up

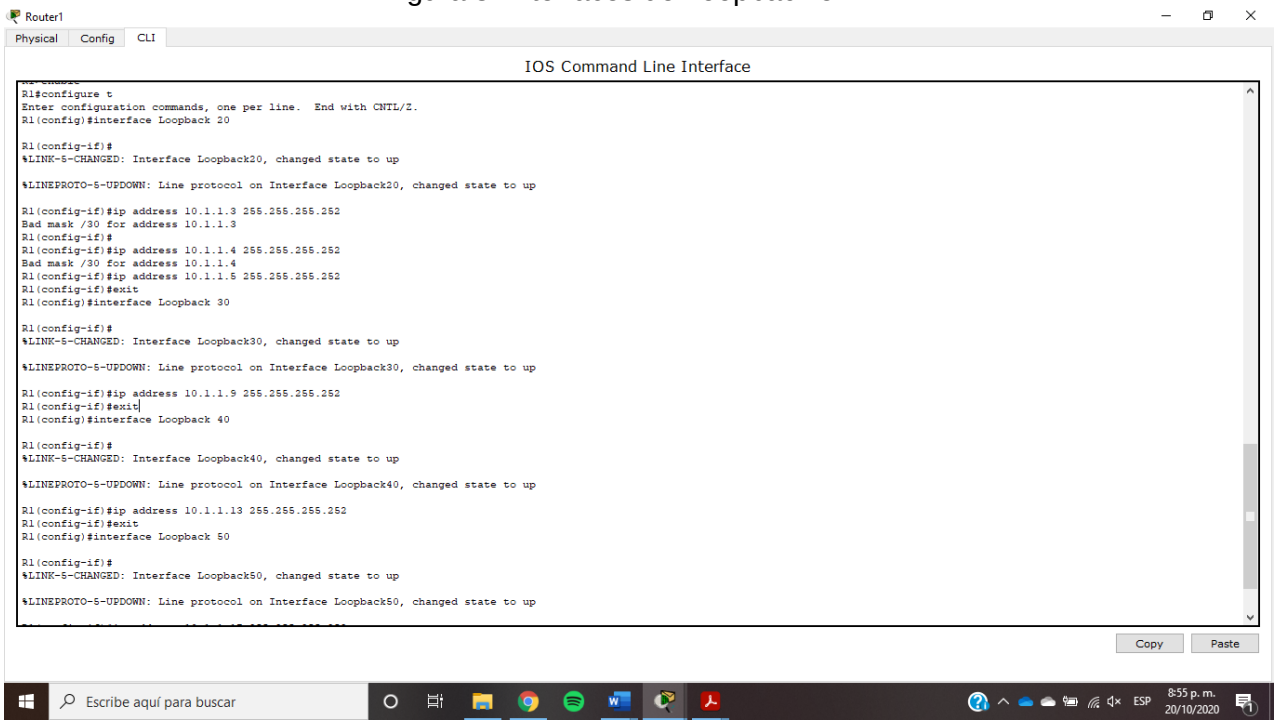
R1(config-if)#ip address 10.1.1.13 255.255.255.252
R1(config-if)#exit
R1(config)#interface Loopback 50

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback50, changed state to up

R1(config-if)#ip address 10.1.1.17 255.255.255.252
R1(config-if)#exit

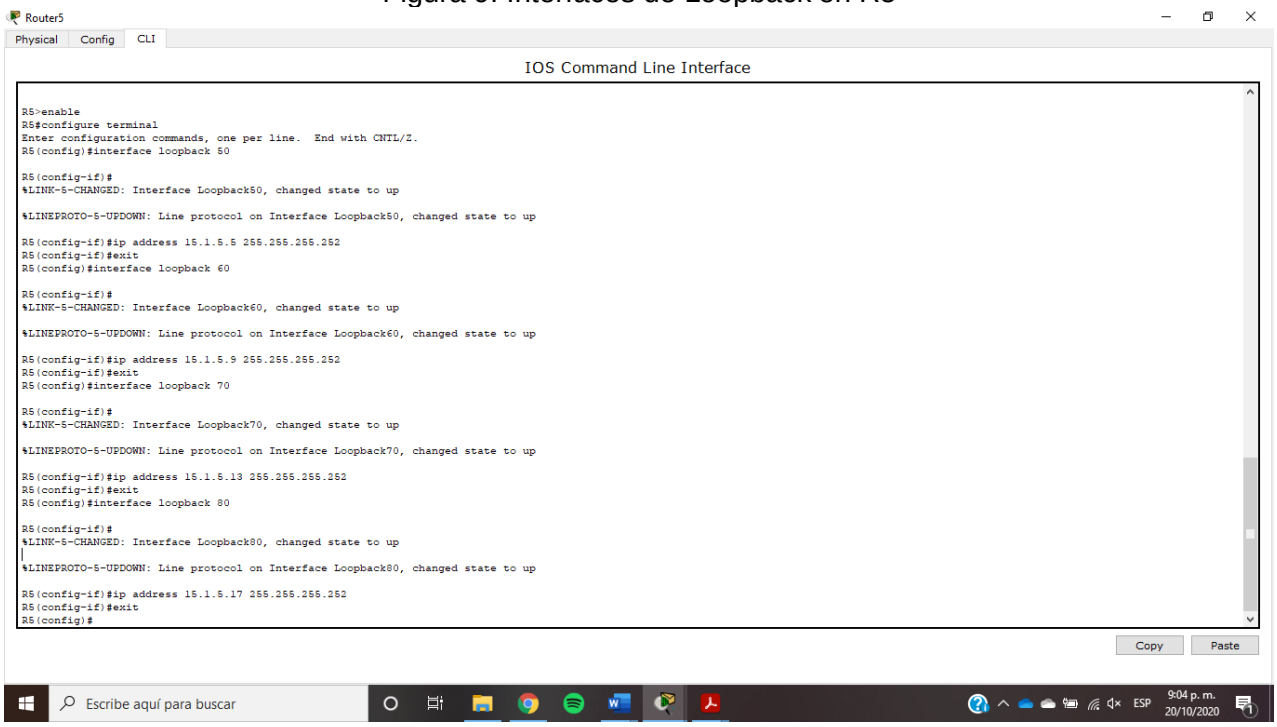
Figura 8. Interfaces de Loopback en R1



1.3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 15.

```
R5>enable
R5#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#interface loopback 50

R5(config-if)#
%LINK-5-CHANGED: Interface Loopback50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback50, changed state to up

R5(config-if)#ip address 15.1.5.5 255.255.255.252
R5(config-if)#exit
R5(config)#interface loopback 60

R5(config-if)#
%LINK-5-CHANGED: Interface Loopback60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback60, changed state to up

R5(config-if)#ip address 15.1.5.9 255.255.255.252
R5(config-if)#exit
R5(config)#interface loopback 70

R5(config-if)#
%LINK-5-CHANGED: Interface Loopback70, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback70, changed state to up

R5(config-if)#ip address 15.1.5.13 255.255.255.252
R5(config-if)#exit
R5(config)#interface loopback 80

R5(config-if)#
%LINK-5-CHANGED: Interface Loopback80, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback80, changed state to up

R5(config-if)#ip address 15.1.5.17 255.255.255.252
R5(config-if)#exit
R5(config)#
```

Figura 9. Interfaces de Loopback en R5

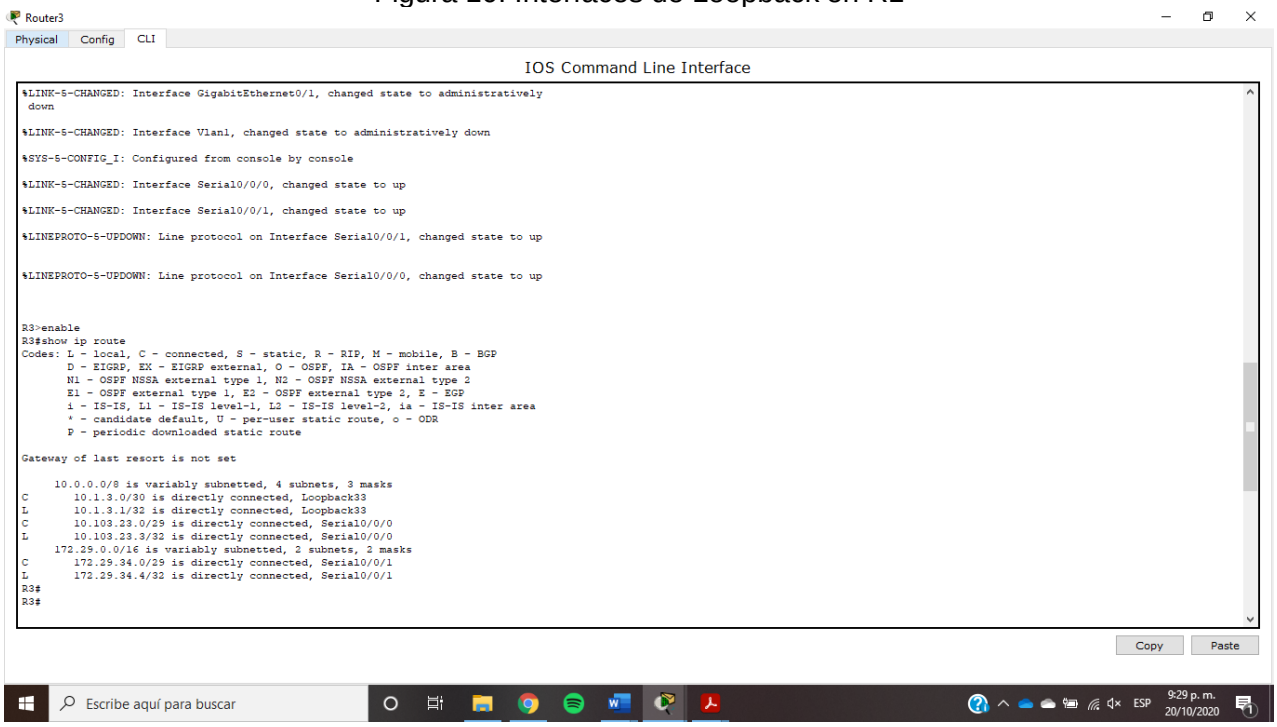


1.4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando show ip route.

Tabla 5. Configuración direcciones IP

ROUTER	INTERFAZ	IP
R3	Loopback 31	**LO11: 10.1.3.1/30**
R3	Loopback 35	**LO15: 10.1.3.5/30**
R3	Loopback 39	**LO19: 10.1.3.9/30**
R3	Loopback 13	**LO19: 10.1.3.13/30**
R3	Loopback 17	**LO19: 10.1.3.17/30**

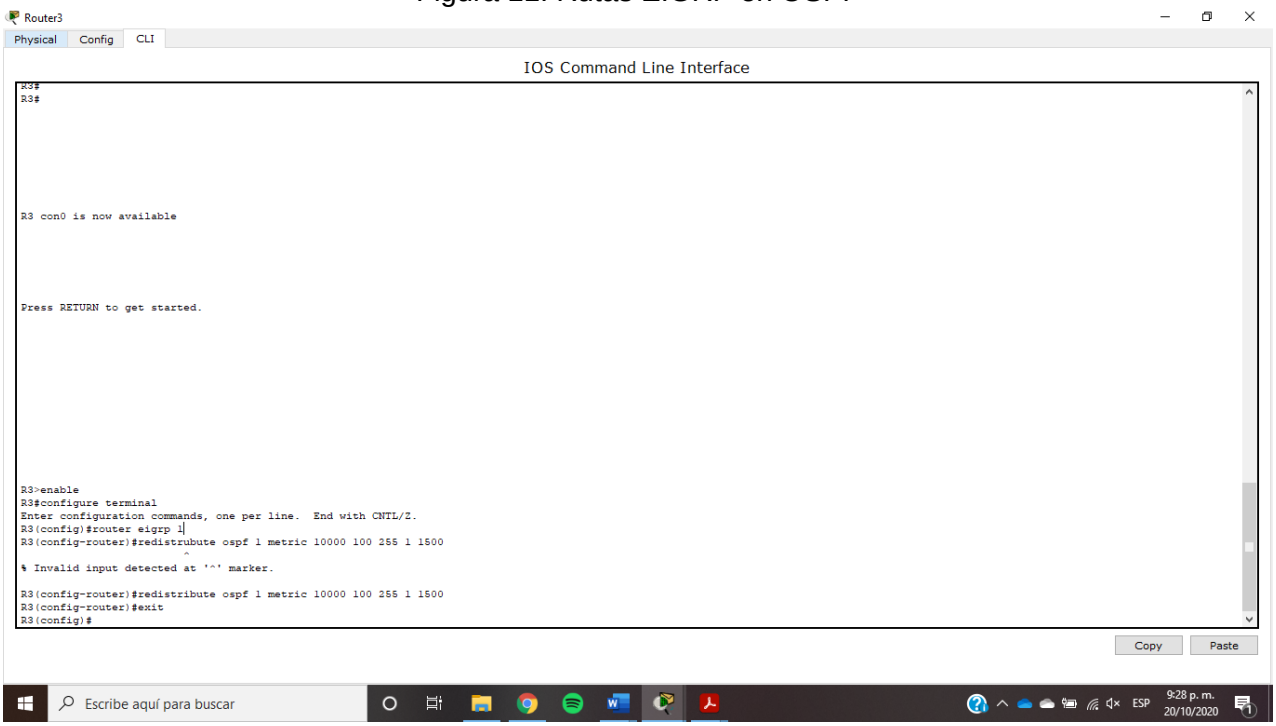
Figura 10. Interfaces de Loopback en R1



1.5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router eigrp 1
R3(config-router)#redistrubute ospf 1 metric 10000 100 255 1 1500
                  ^
% Invalid input detected at '^' marker.

R3(config-router)#redistribute ospf 1 metric 10000 100 255 1 1500
R3(config-router)#exit
```

Figura 11. Rutas EIGRP en OSPF



1.6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando show ip route.

Figura 12. Comando show ip route

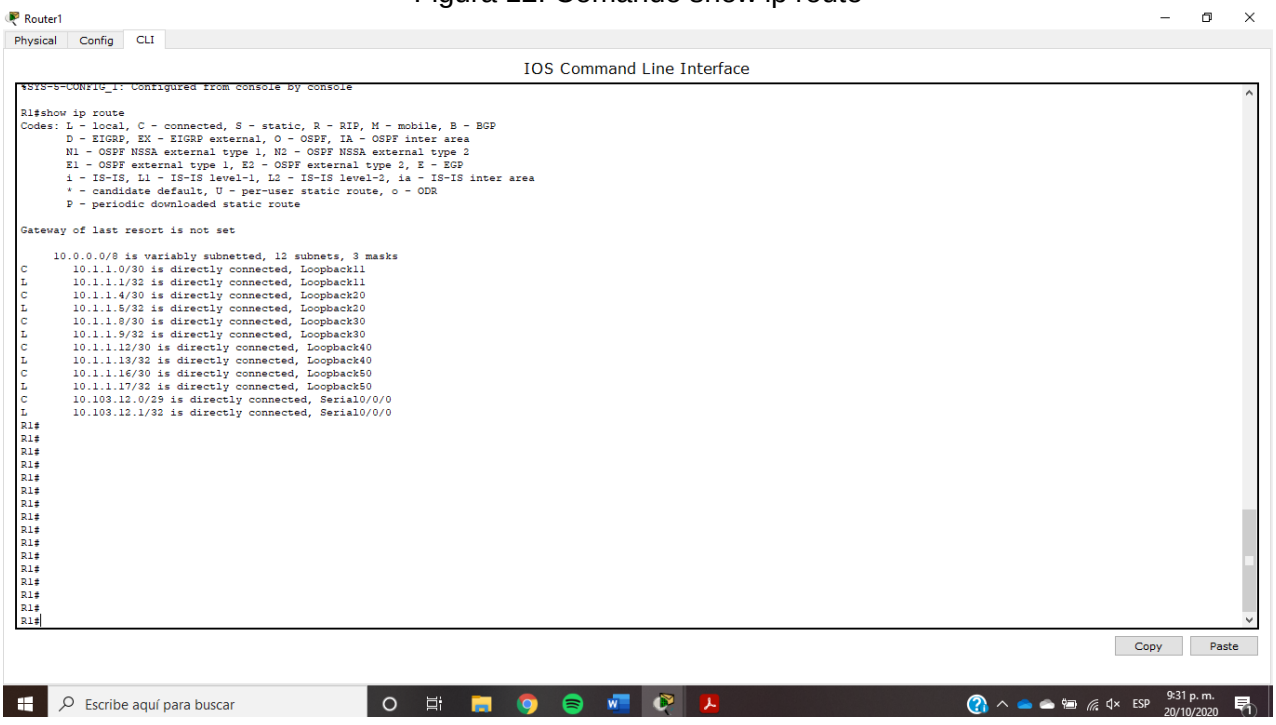


Figura 13. Comando show ip route

Segundo Escenario

Una empresa de comunicaciones presenta una estructura Core acorde a la topología de red, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, etherchannels, VLANs y demás aspectos que forman parte del escenario propuesto.

Figura 14. Escenario 2

Topología de red

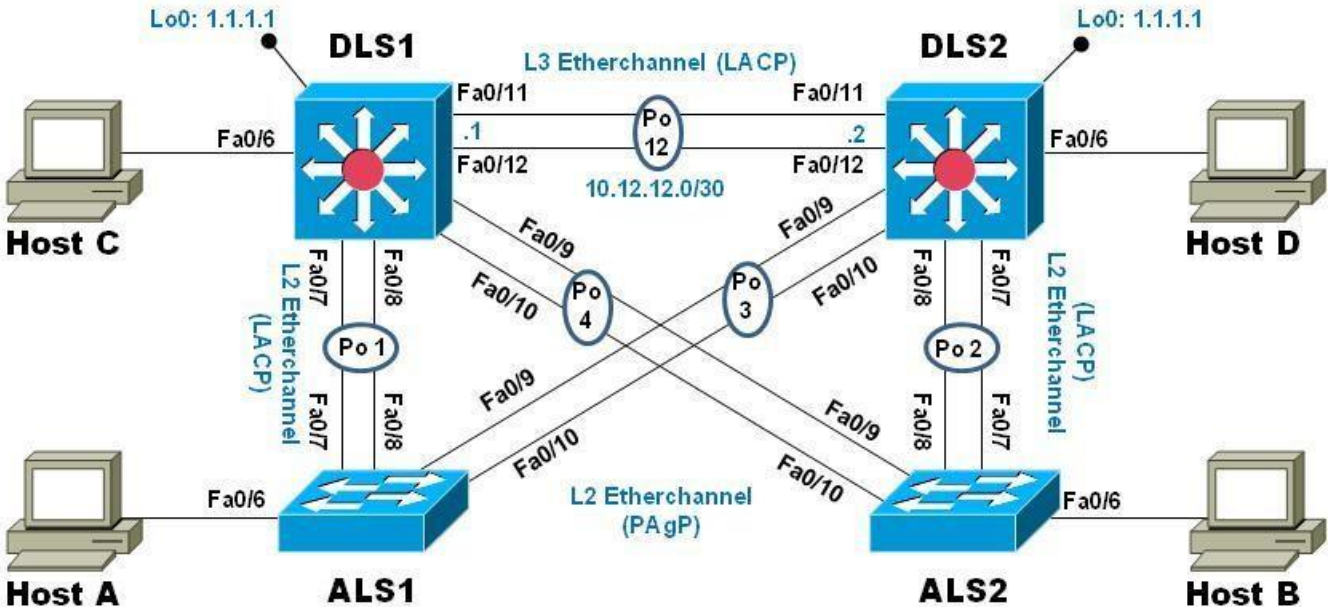
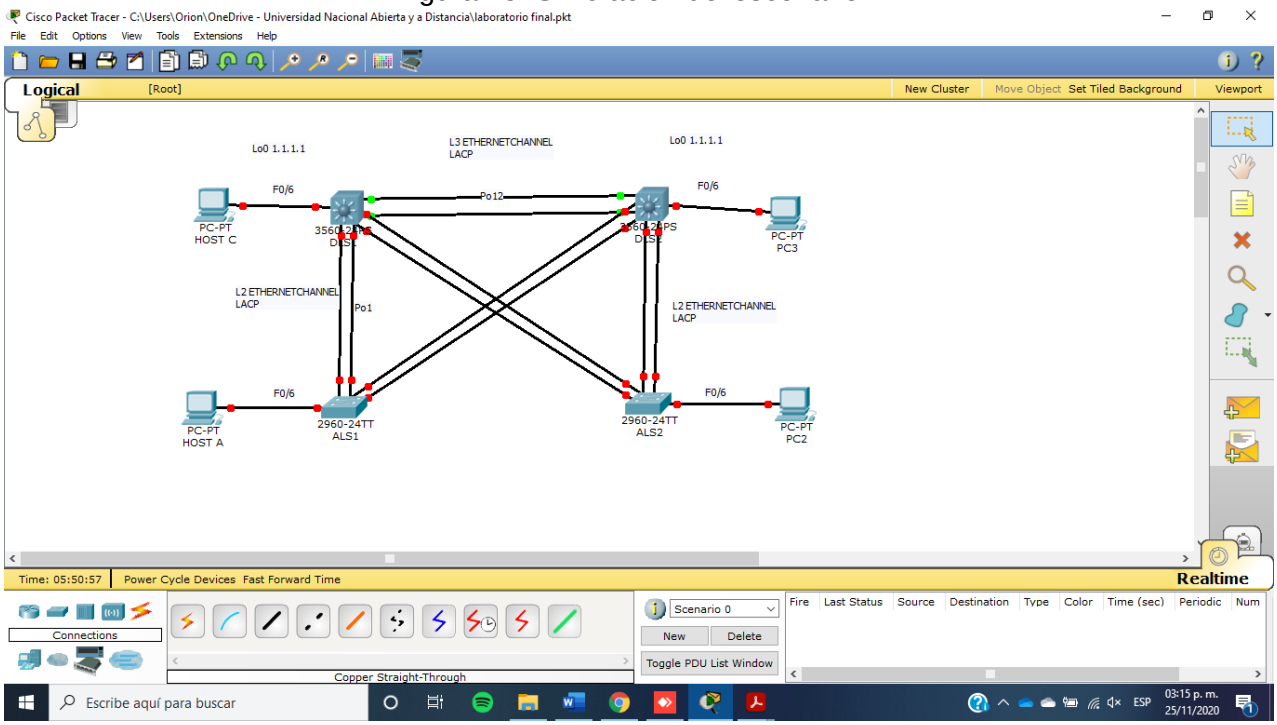


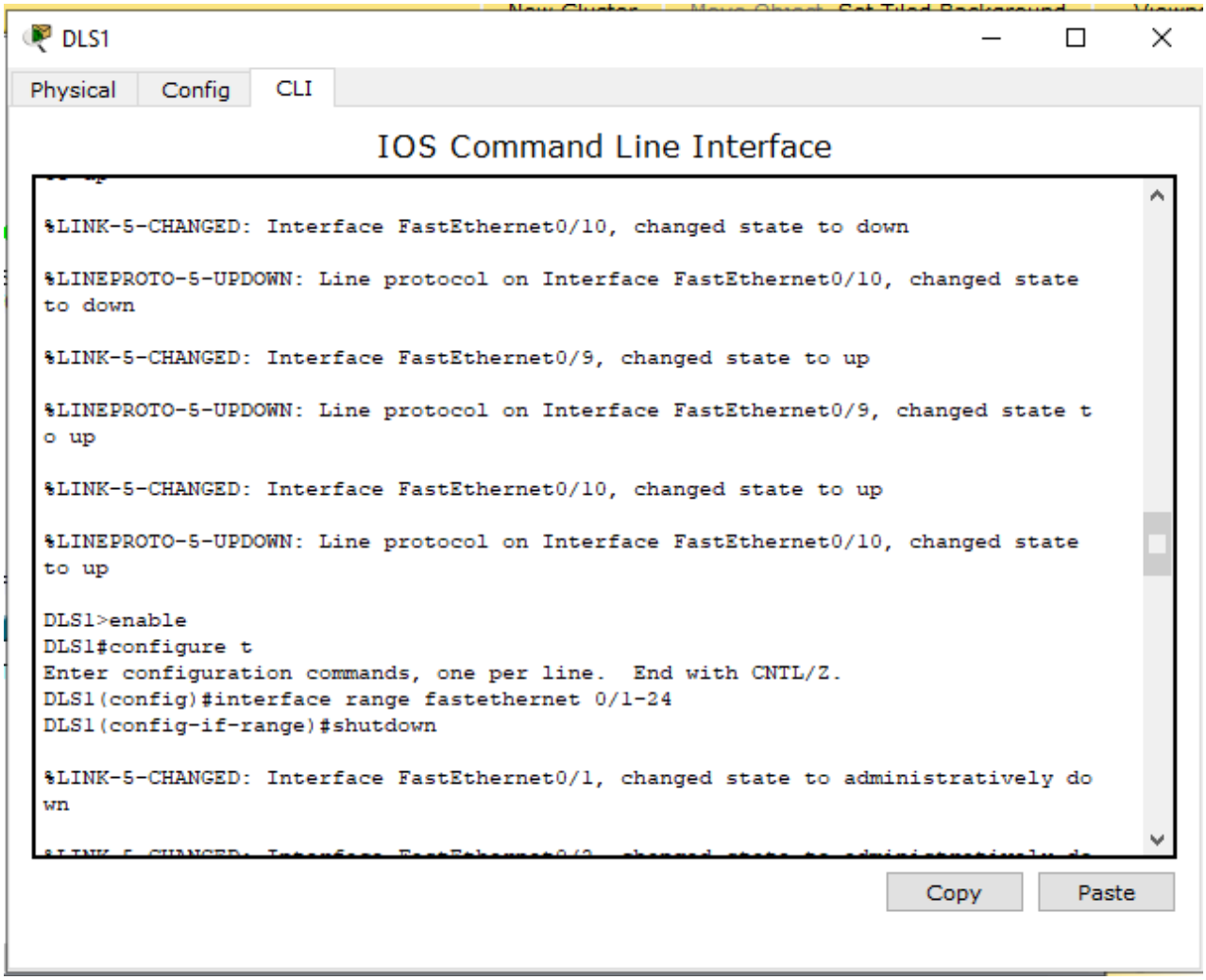
Figura 15. Simulación del escenario 2



Parte 1: Configurar la red de acuerdo con las especificaciones.

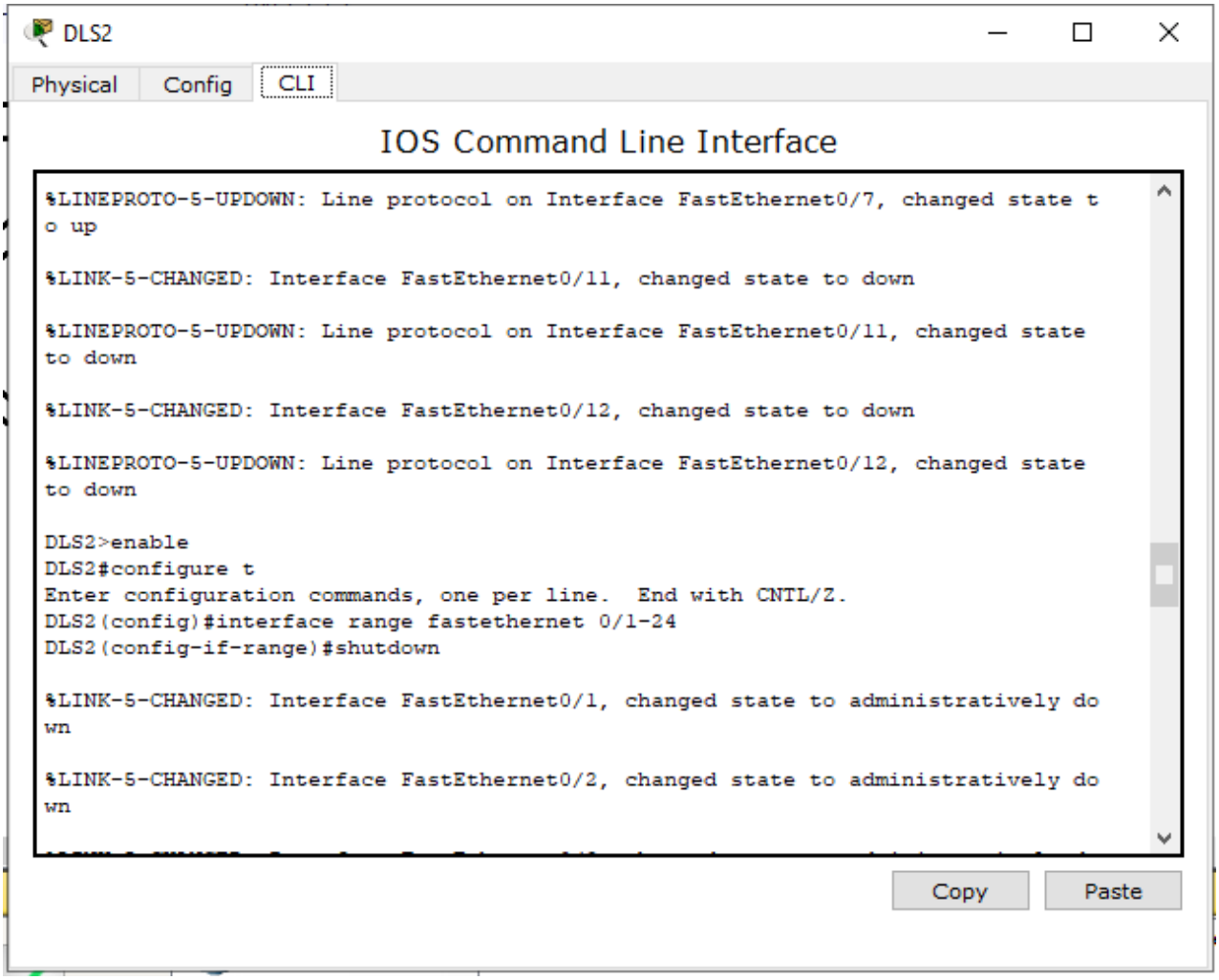
a. Apagar todas las interfaces en cada switch.

Figura 16. Se aplica código DLS1



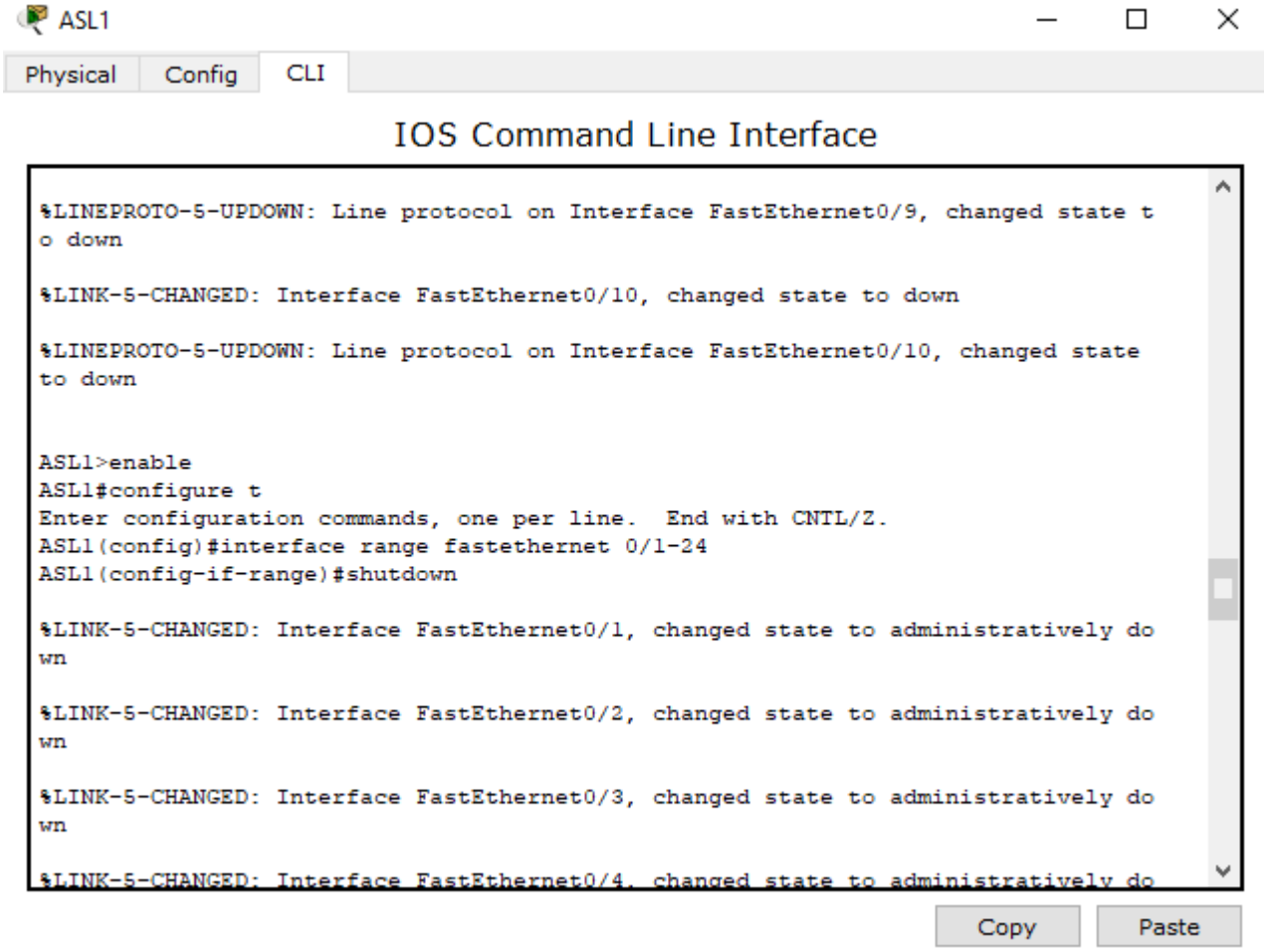
Se apaga las interfaces del swtich DLS1.

Figura 17. Se aplica código DLS2



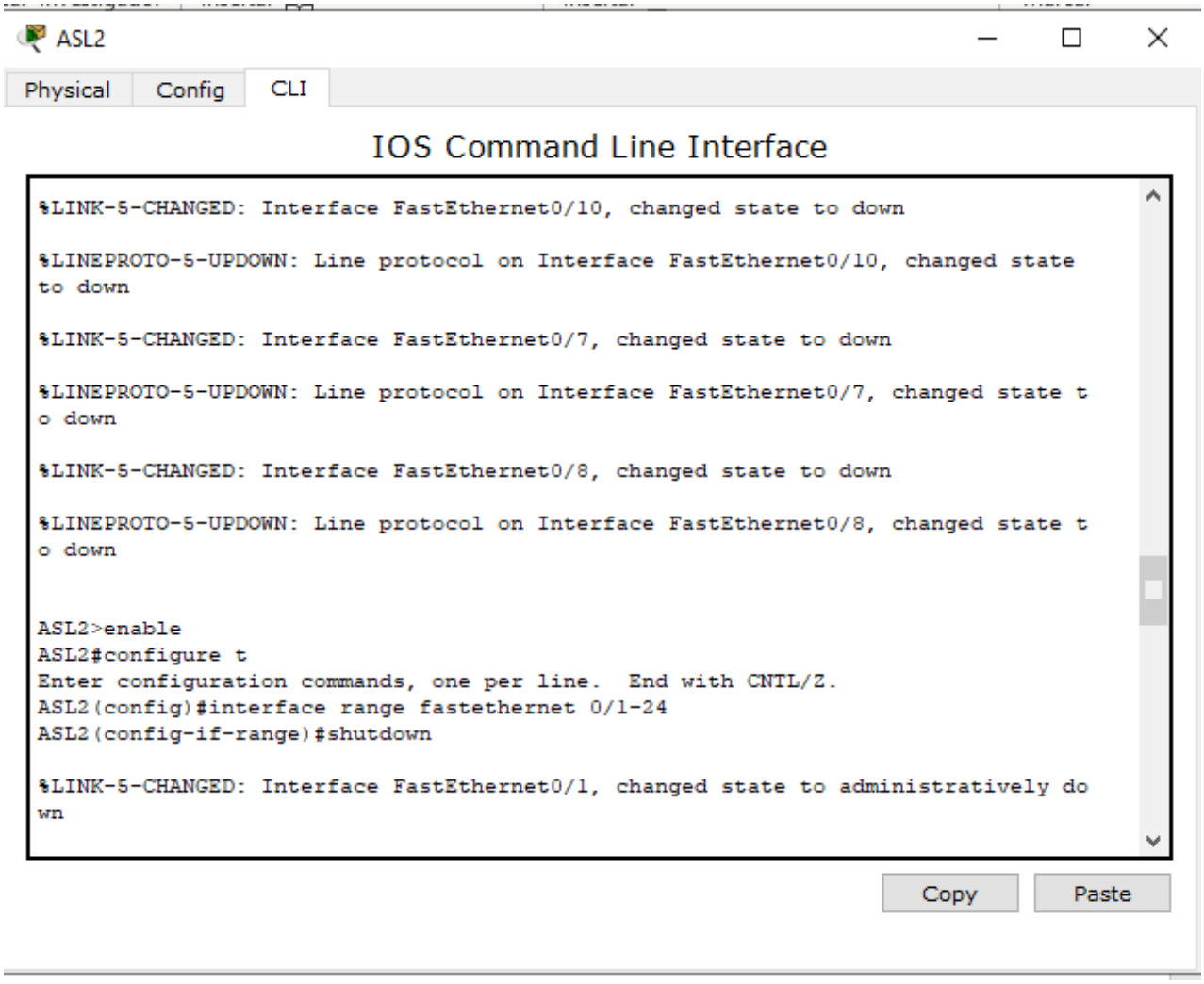
Se apaga las interfaces del swtich DLS2

Figura 18. Se aplica código ASL1



Se apaga las interfaces del swtich ASL1

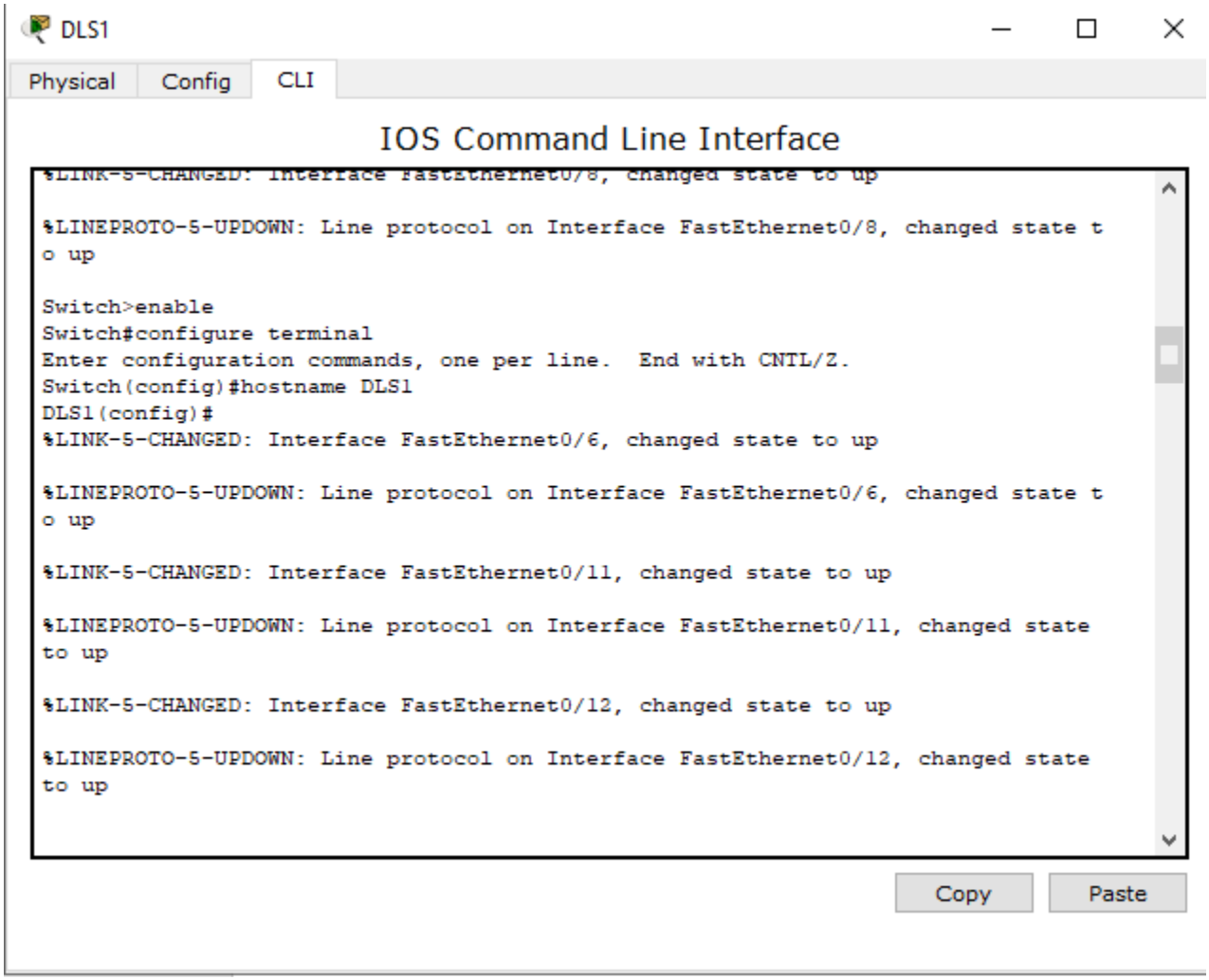
Figura 19. Se aplica código ASL2



Se apaga las interfaces del swtich ASL2

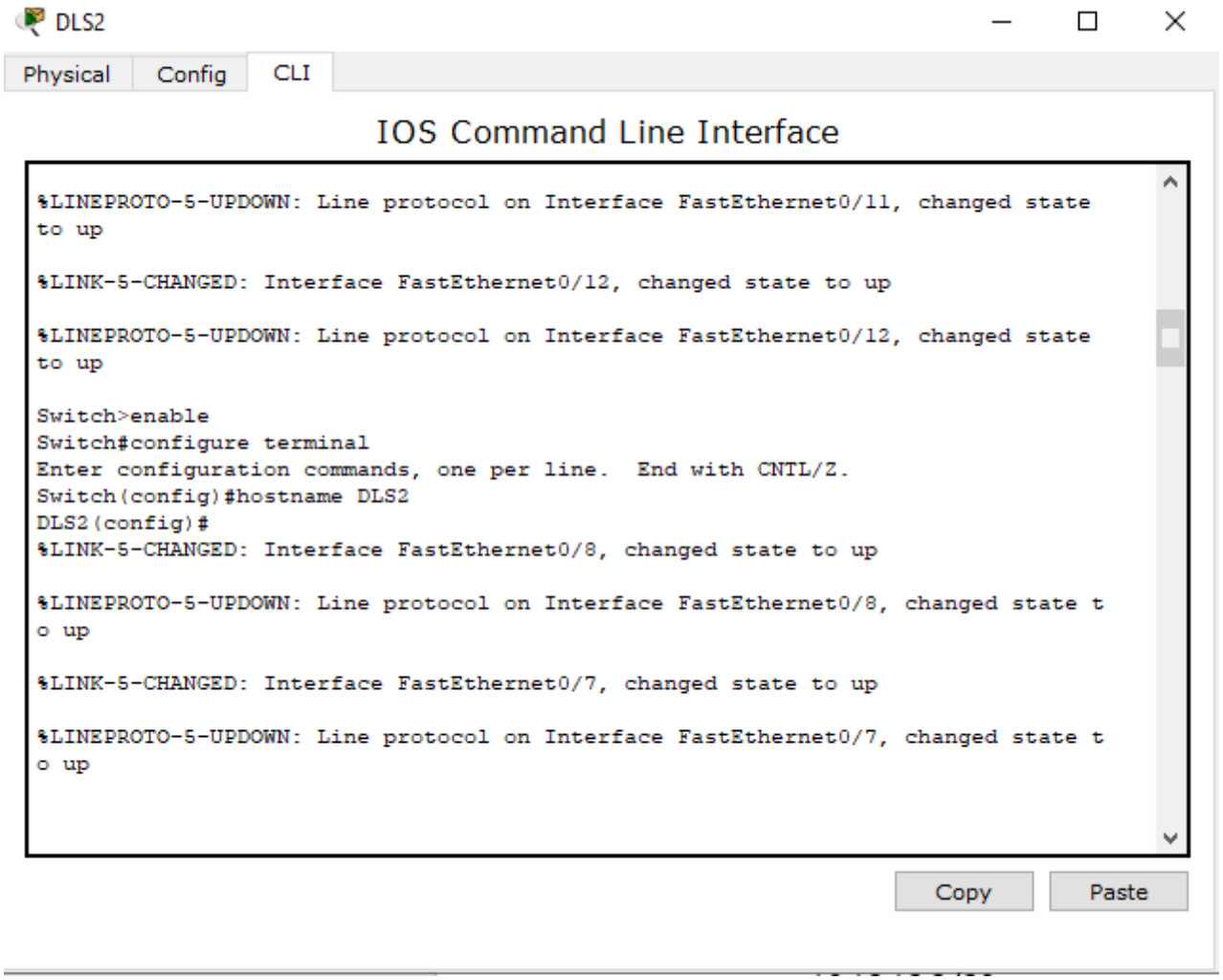
b. Asignar un nombre a cada switch acorde con el escenario establecido.

Figura 20. Correcta configuración de DLS1



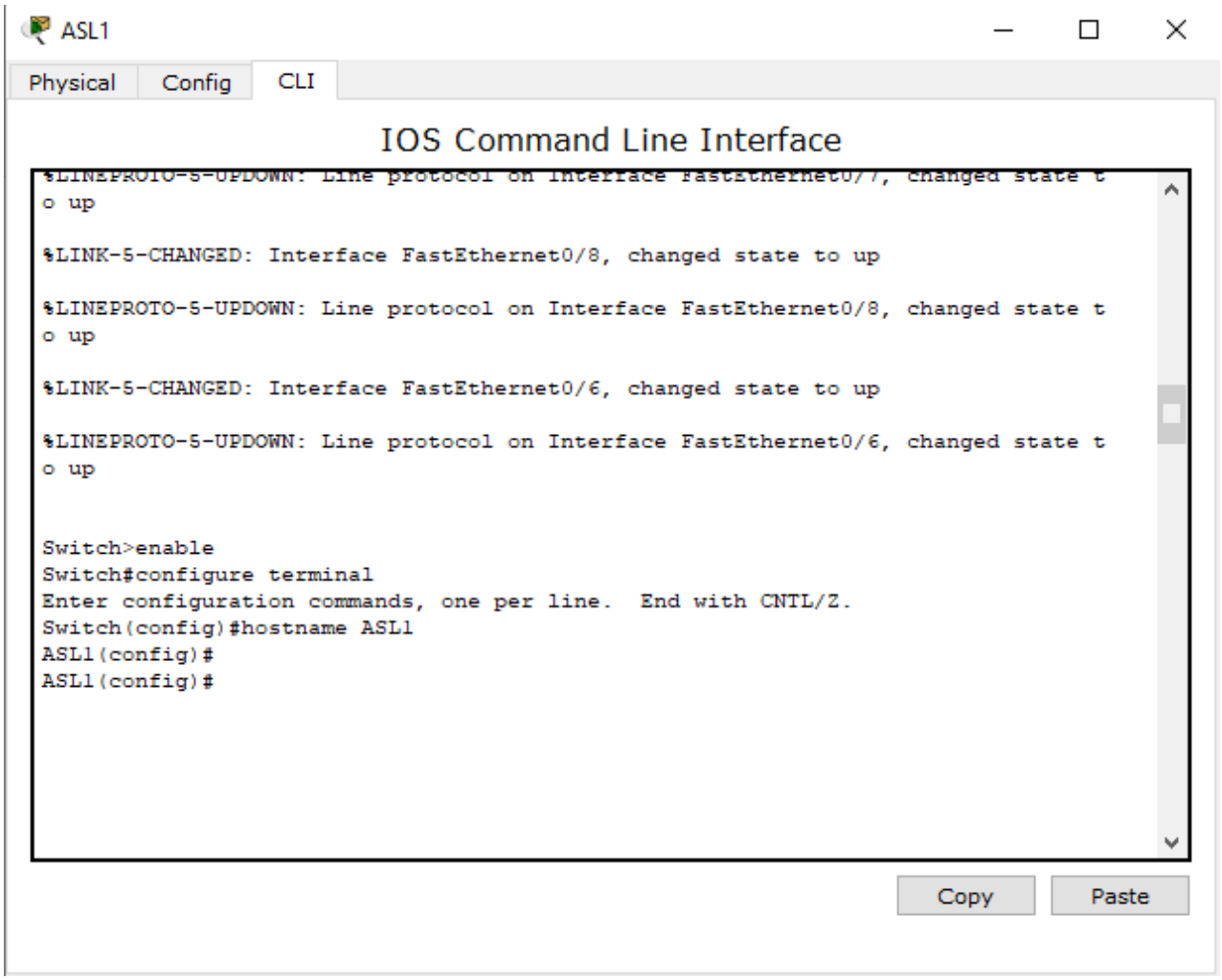
Cambio de nombre del switch DLS1.

Figura 21. Correcta configuración de DLS2



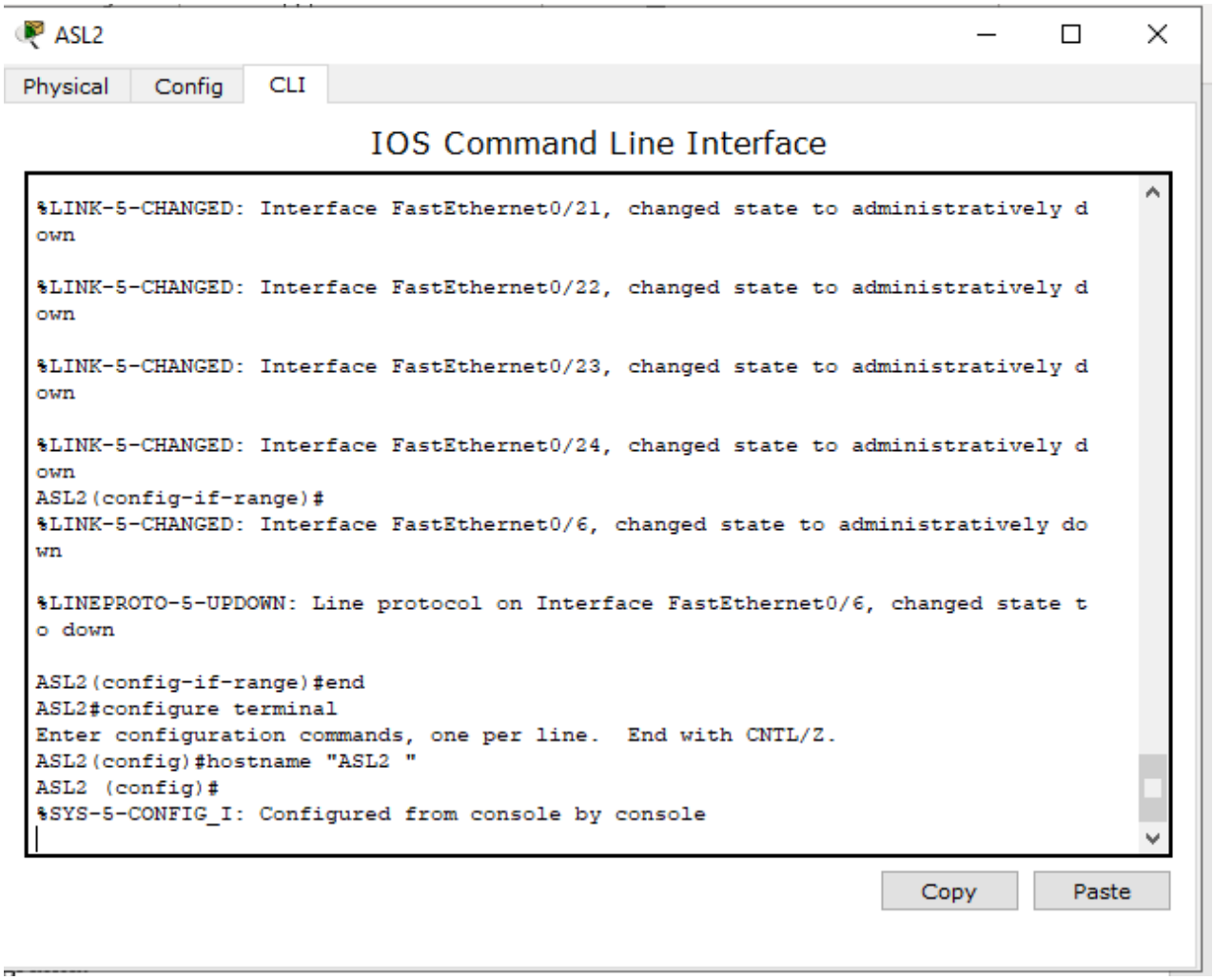
Cambio de nombre del switch DLS2

Figura 22. Correcta configuración de ASL1



Cambio de nombre del switch ASL1

Figura 23. Correcta configuración de ASL2



Cambio de nombre del switch ASL2 se dejó la misma imagen ya que se realizó el proceso de configuración con los 4 switch esta primera parte.

c. Configurar los puertos troncales y Port-channels tal como se muestra en el diagrama.

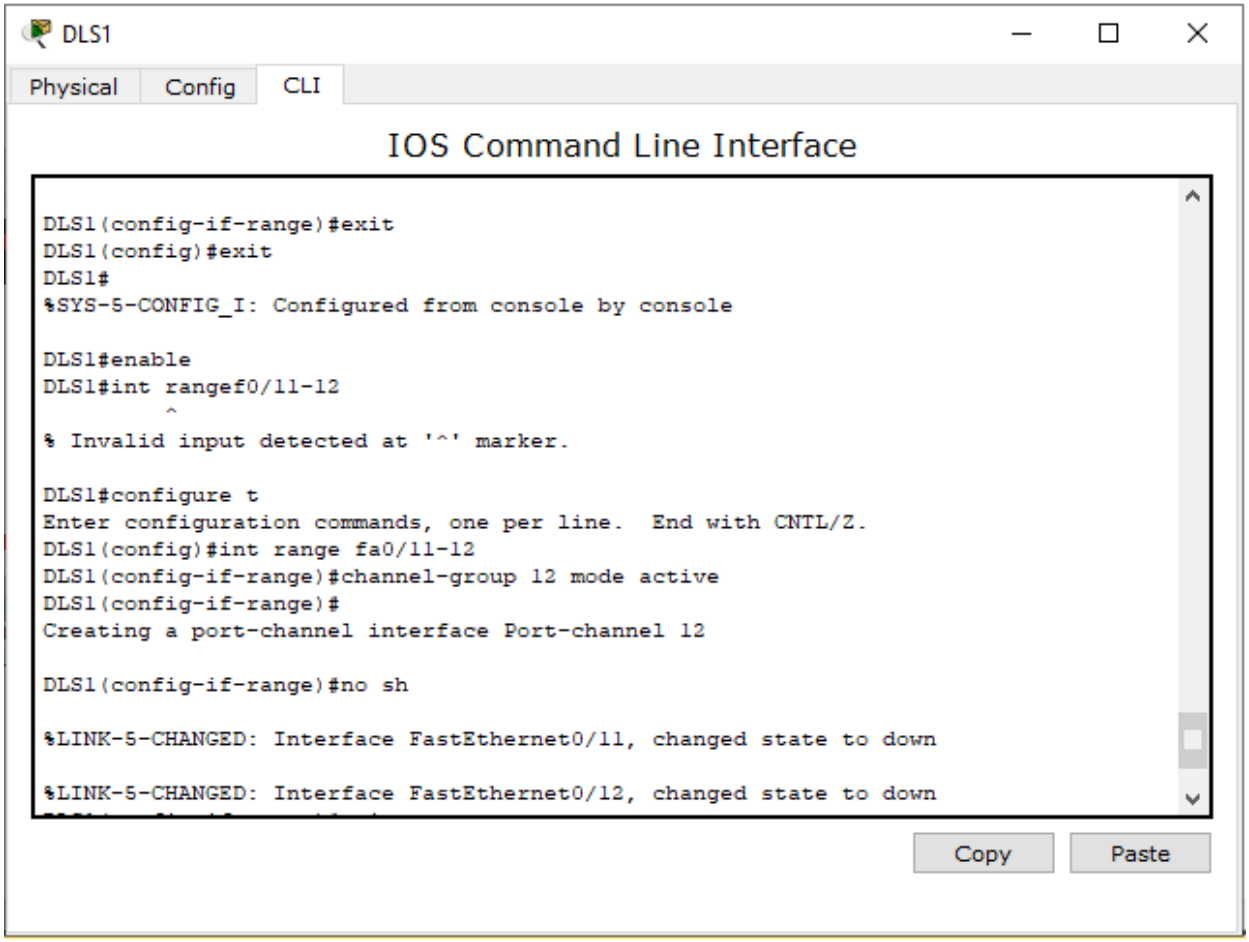
   1) La conexión entre DLS1 y DLS2 será un EtherChannel capa-3 utilizando LACP. Para DLS1 se utilizará la dirección IP 10.12.12.1/30 y para DLS2 utilizará 10.12.12.2/30.

Se ejecuta comando cada sw:

DLS1>en

```
DLS1#conf ter
DLS1(config)#interface port-channel 12
DLS1(config-if)#no switchport
DLS1(config-if)#ip address 10.12.12.1 255.255.255.252
DLS1(config-if)#exit
DLS1(config)#interface range fa0/11-12
DLS1(config-if-range)#no switchport
DLS1(config-if-range)#channel-group 12 mode active
DLS1(config-if-range)#exit
```

Figura 24. Aplicando código DLS1 Port-channels



DLS2>en

DLS2#conf ter

DLS2(config)#interface port-channel 12

DLS2(config-if)#no switchport

DLS2(config-if)#ip address 10.12.12.2 255.255.255.252

DLS2(config-if)#exit

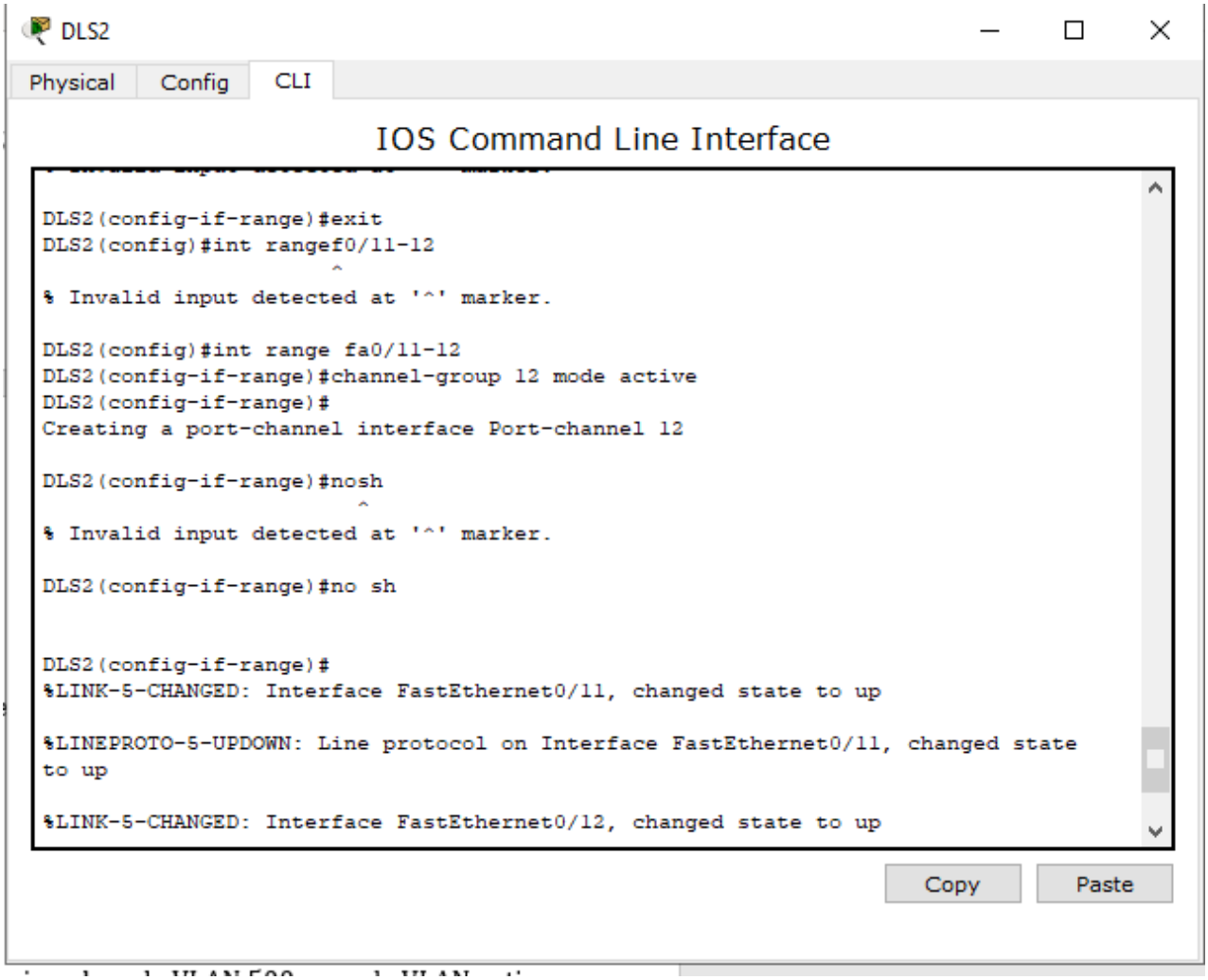
DLS2(config)#interface range fa0/11-12

DLS2(config-if-range)#no switchport

DLS2(config-if-range)#channel-group 12 mode active

DLS2(config-if-range)#exit

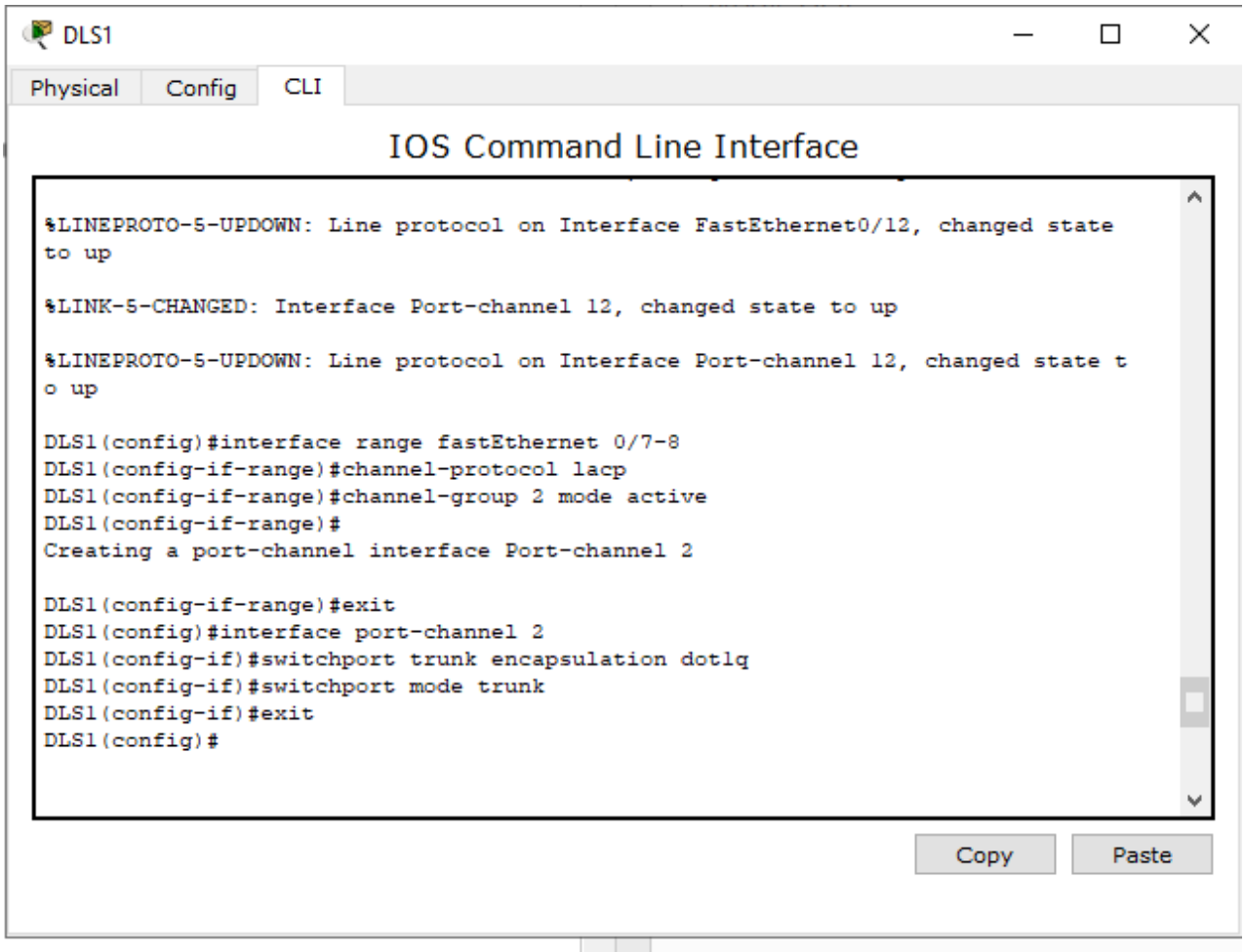
Figura 25. Aplicando código DLS2 Port-channels



2) Los Port-channels en las interfaces Fa0/7 y Fa0/8 utilizarán LACP.

DLS1

Figura 26. Aplicando código DLS1 LACP



DLS1(config)#interface range fastEthernet 0/7-8

DLS1(config-if-range)#channel-protocol lacp

DLS1(config-if-range)#channel-group 2 mode active

DLS1(config-if-range)#

Creating a port-channel interface Port-channel 2

DLS1(config-if-range)#exit

DLS1(config)#interface port-channel 2

DLS1(config-if)#switchport trunk encapsulation dot1q

DLS1(config-if)#switchport mode trunk

DLS1(config-if)#exit

DLS1(config)#

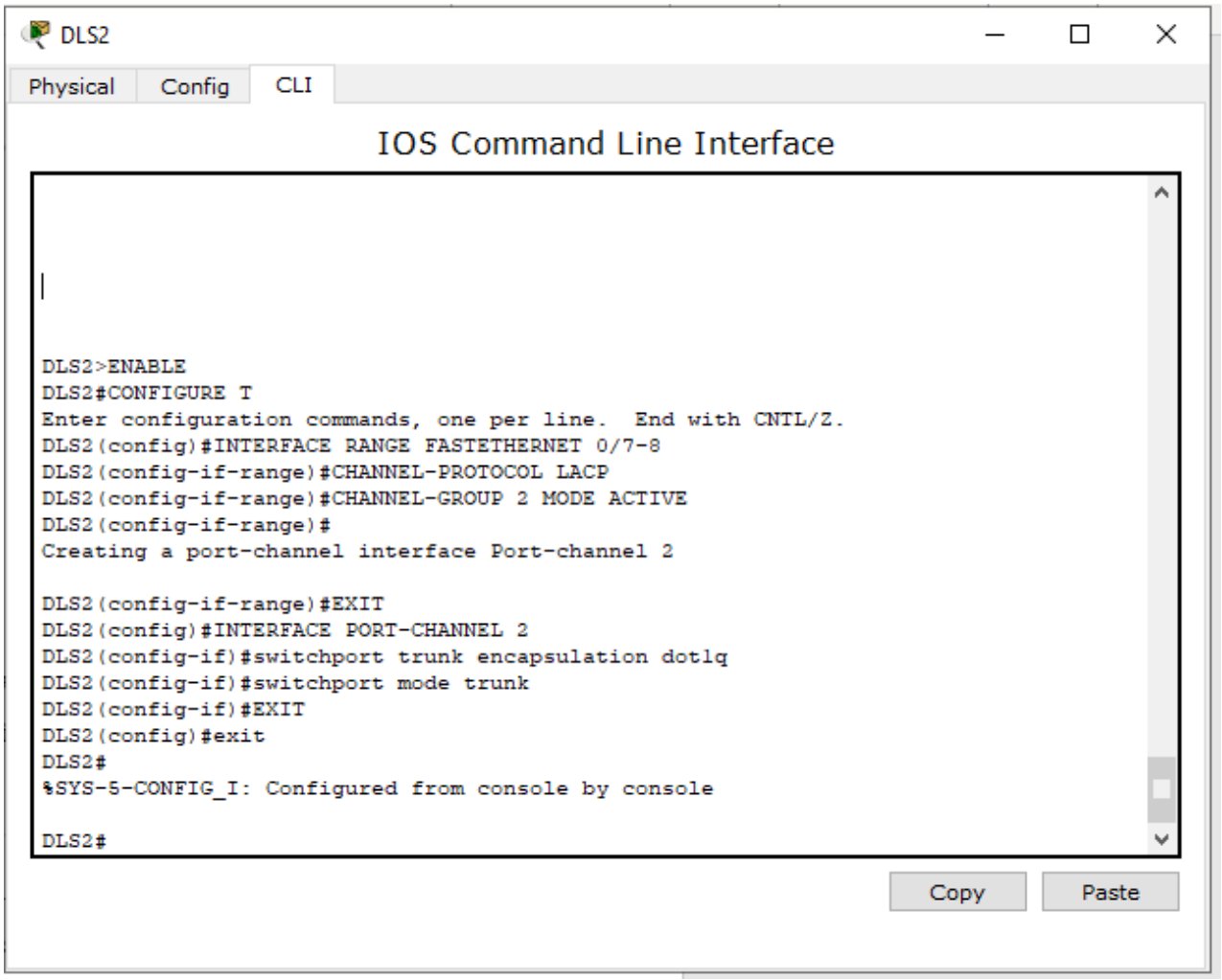
DLS2

DLS2>ENABLE
DLS2#CONFIGURE T
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#INTERFACE RANGE FASTETHERNET 0/7-8
DLS2(config-if-range)#CHANNEL-PROTOCOL LACP
DLS2(config-if-range)#CHANNEL-GROUP 2 MODE ACTIVE
DLS2(config-if-range)#
Creating a port-channel interface Port-channel 2

DLS2(config-if-range)#EXIT
DLS2(config)#INTERFACE PORT-CHANNEL 2
DLS2(config-if)#switchport trunk encapsulation dot1q
DLS2(config-if)#switchport mode trunk
DLS2(config-if)#EXIT
DLS2(config)#exit
DLS2#
%SYS-5-CONFIG_I: Configured from console by console

DLS2#

Figura 27. Aplicando código DLS2 LACP



ALS1

ALS1>enable

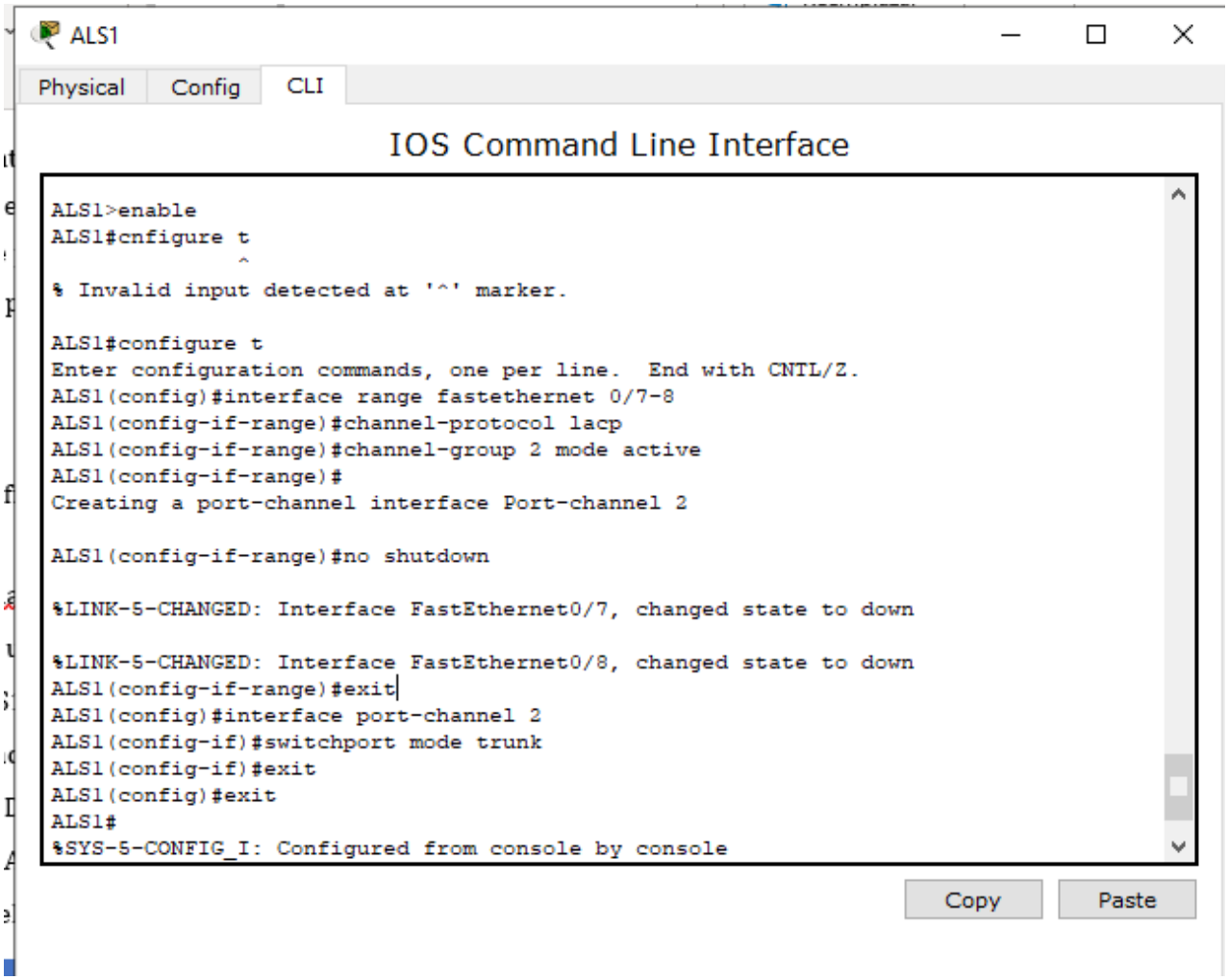
ALS1#cnfigure t

^

% Invalid input detected at '^' marker.

```
ALS1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
ALS1(config)#interface range fastethernet 0/7-8
ALS1(config-if-range)#channel-protocol lacp
ALS1(config-if-range)#channel-group 2 mode active
ALS1(config-if-range)#
Creating a port-channel interface Port-channel 2

ALS1(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to down
ALS1(config-if-range)#exit
ALS1(config)#interface port-channel 2
ALS1(config-if)#switchport mode trunk
ALS1(config-if)#exit
ALS1(config)#exit
ALS1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 28. Aplicando código ALS1 LACP



ALS2

ALS2>enable

ALS2#configure t

Enter configuration commands, one per line. End with CNTL/Z.

ALS2(config)#interface range fastEthernet 0/7-8

ALS2(config-if-range)#channel-protocol lacp

ALS2(config-if-range)#channel-group 2 mode active

ALS2(config-if-range)#

Creating a port-channel interface Port-channel 2

ALS2(config-if-range)#interface port-channel 2

ALS2(config-if)#switchport mode trunk

ALS2(config-if)#exit

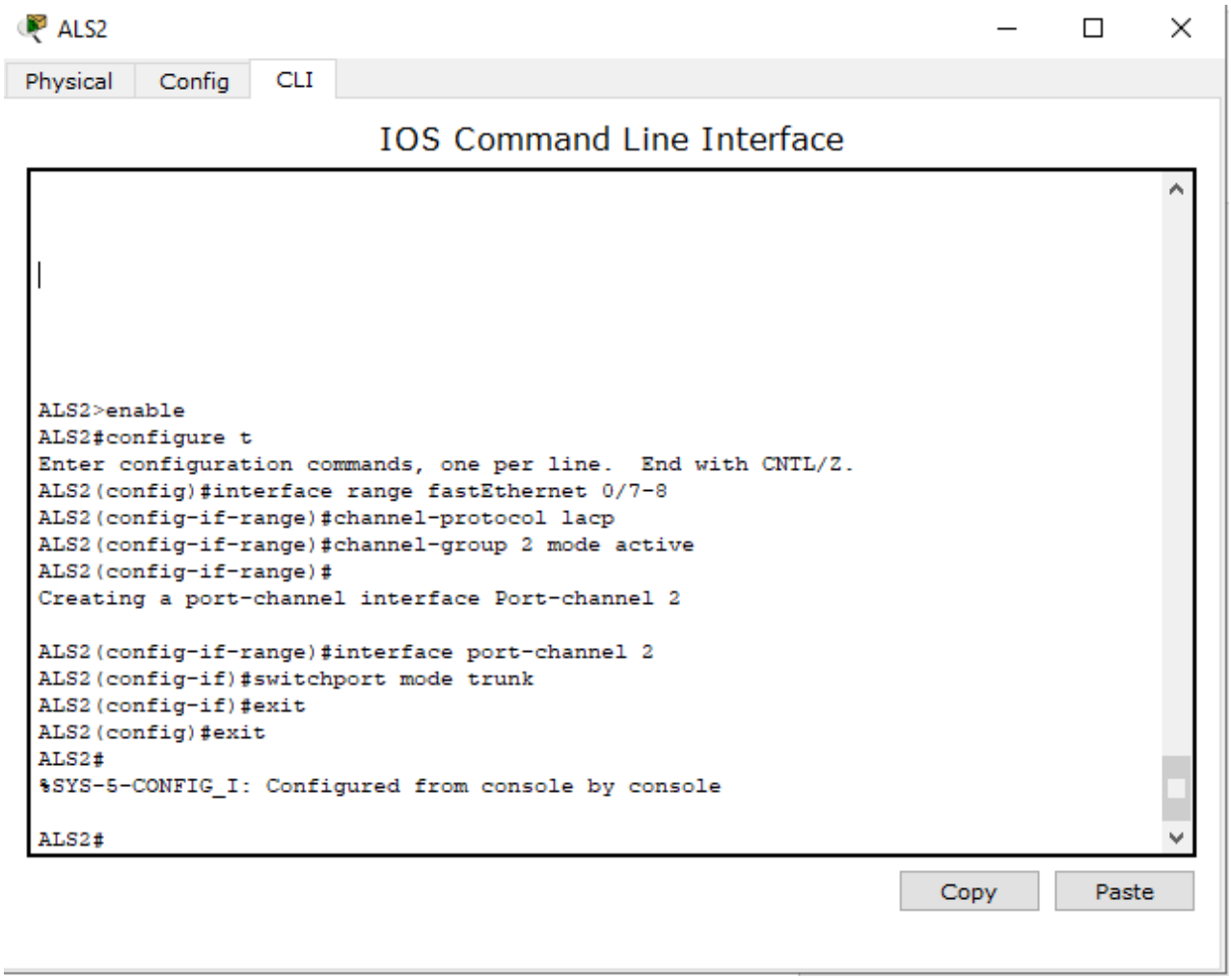
ALS2(config)#exit

ALS2#

%SYS-5-CONFIG_I: Configured from console by console

ALS2#

Figura 29. Aplicando código ASL2 LACP



3) Los Port-channels en las interfaces F0/9 y fa0/10 utilizará PAgP.

```
DLS1>enable
DLS1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
DLS1(config)#int range fa0/9-10
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 4 mode desirable
DLS1(config-if-range)#
Creating a port-channel interface Port-channel 4

DLS1(config-if-range)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down
DLS1(config-if-range)#exit
DLS1(config)#
DLS1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 30. Aplicando código DLS1 PAgP

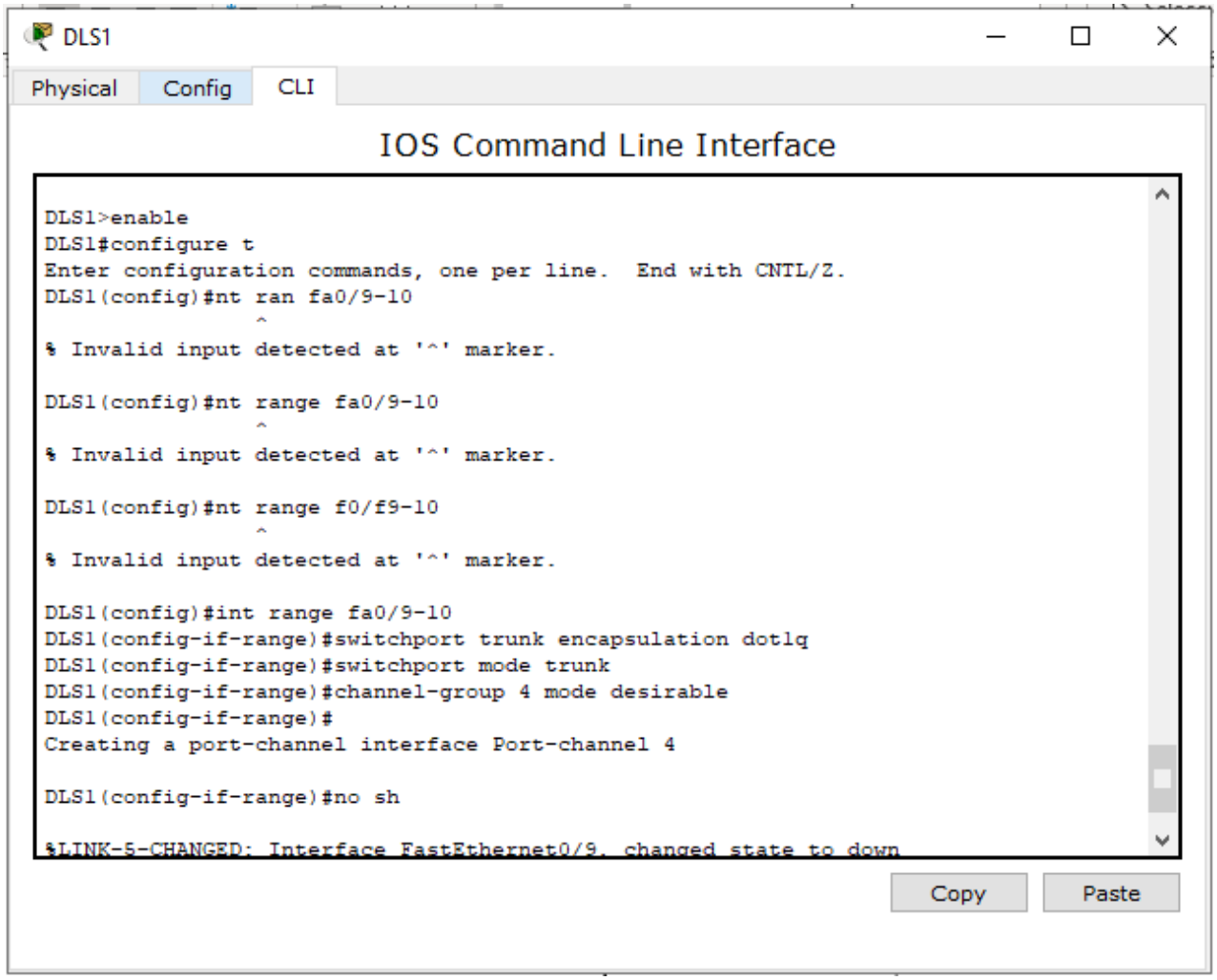


Figura 31. Aplicando código DLS2 PAgP

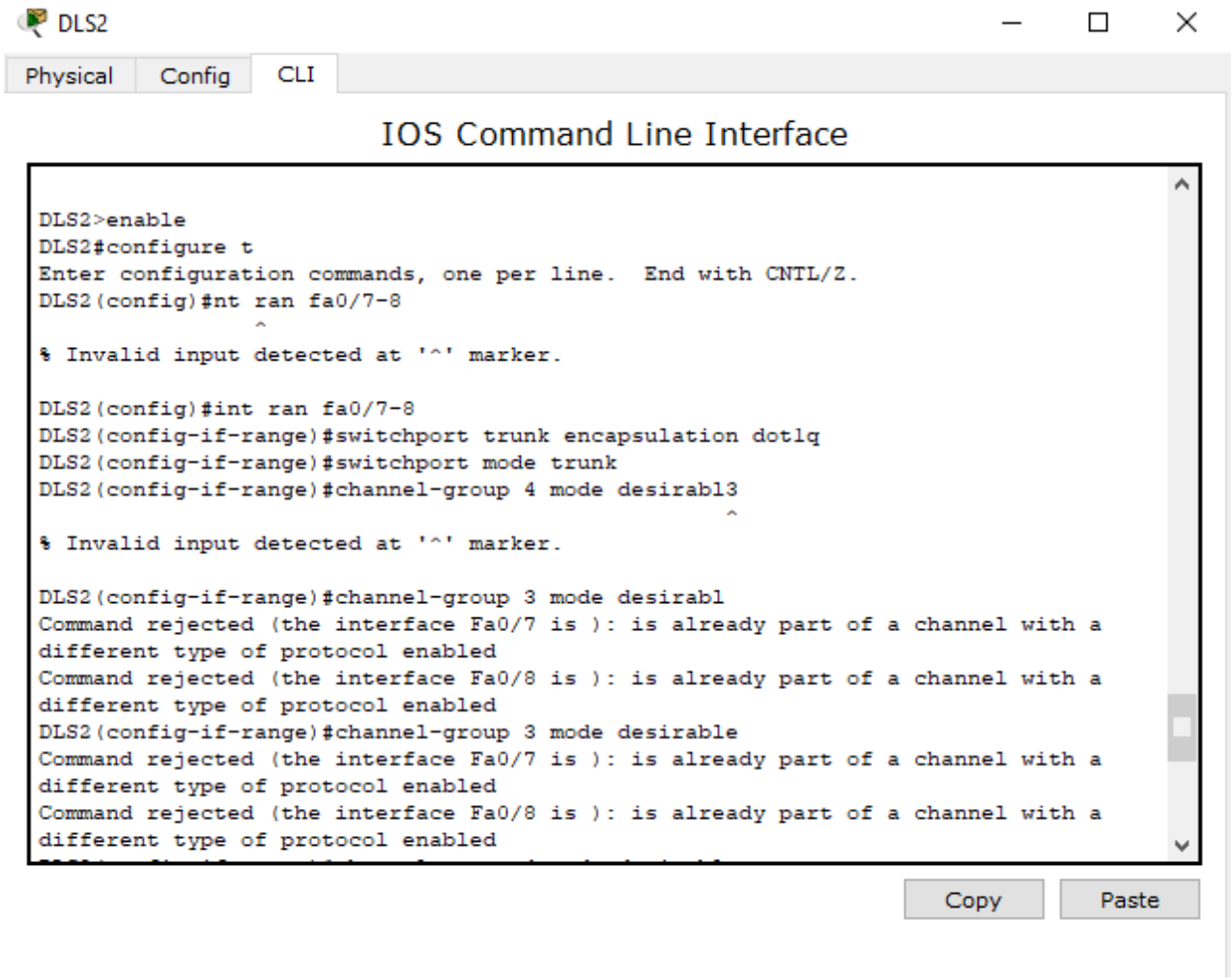


Figura 32. Aplicando código ASL1 PAgP

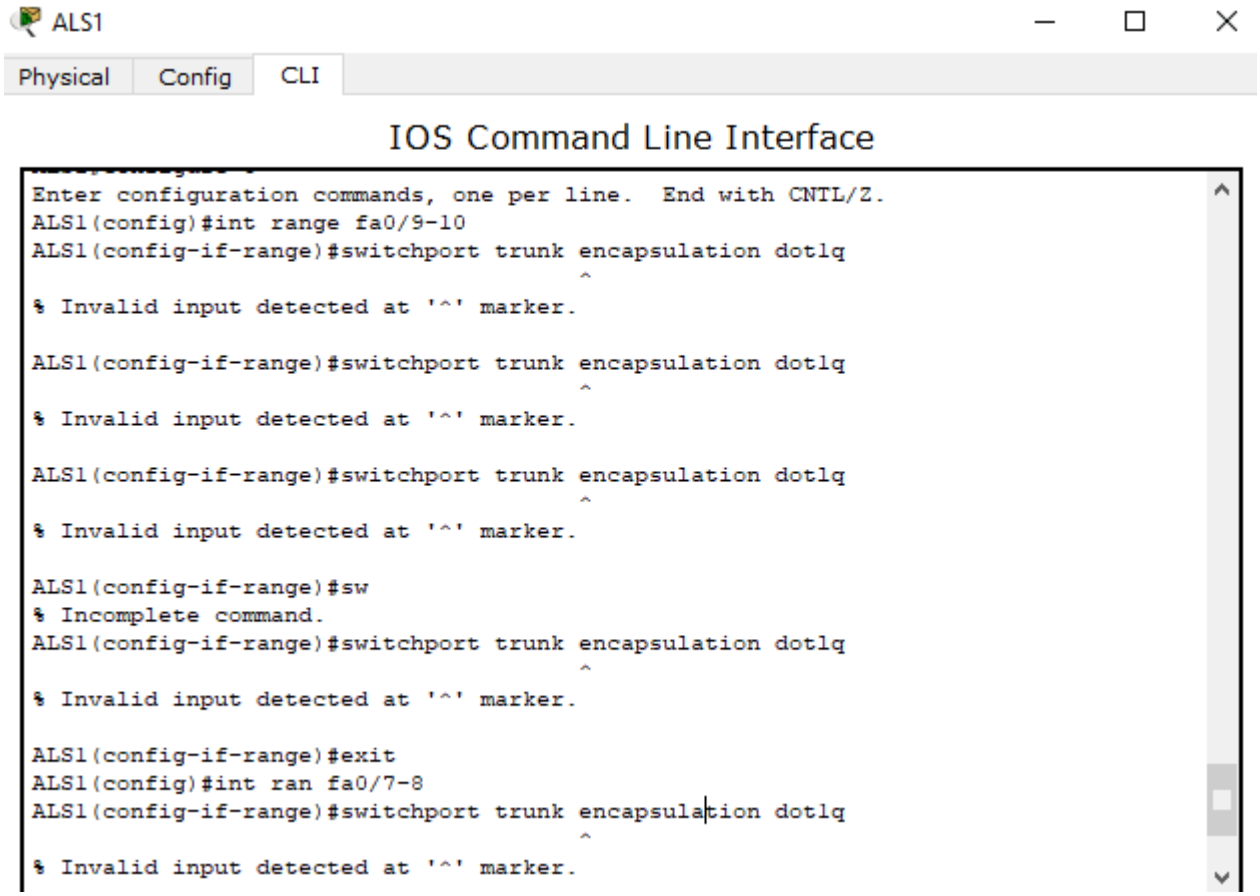
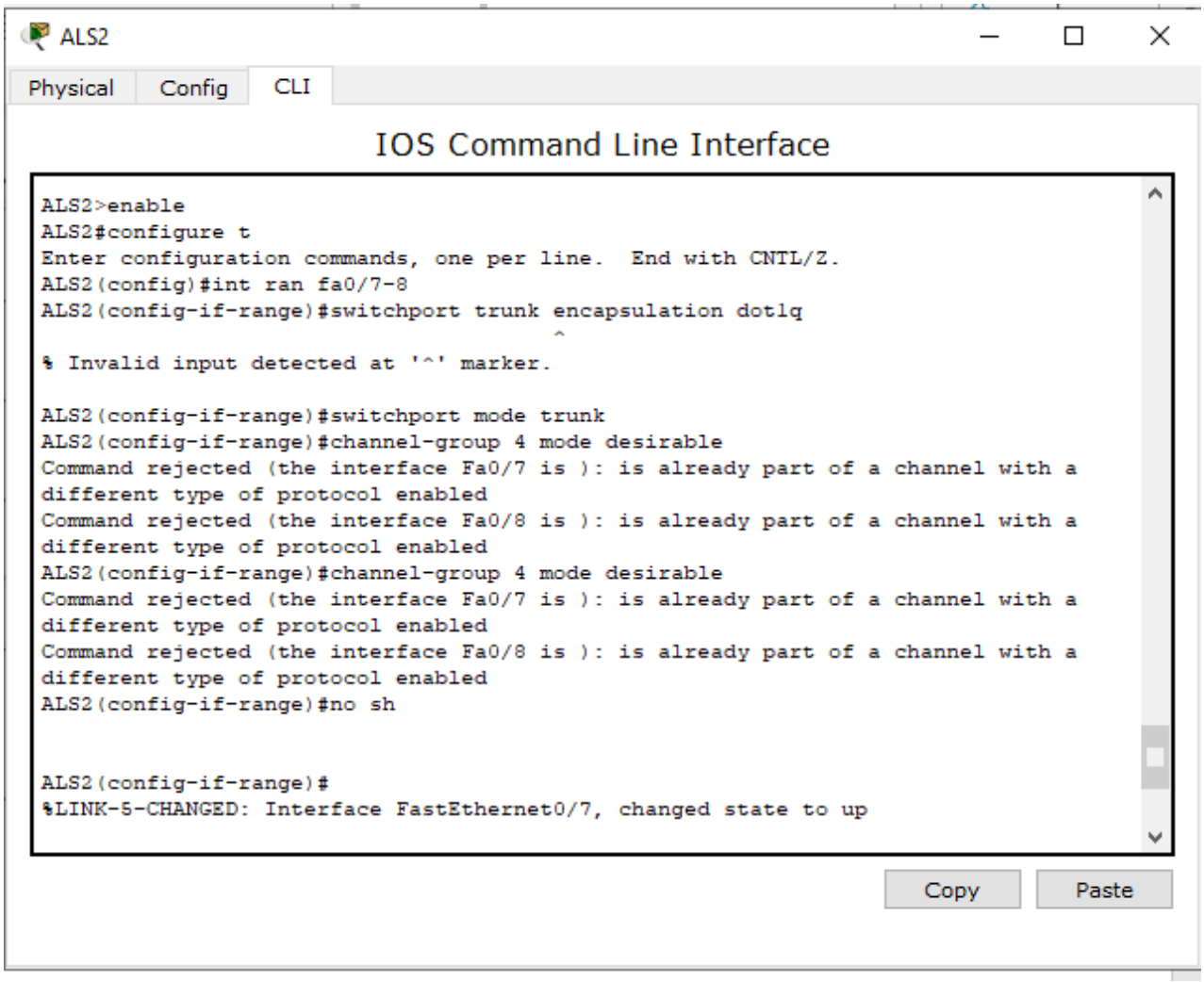


Figura 33. Aplicando código ASL2 PAgP



4) Todos los puertos troncales serán asignados a la VLAN 500 como la VLAN nativa.

Figura 34. Aplicando código DLS1 VLAN 500

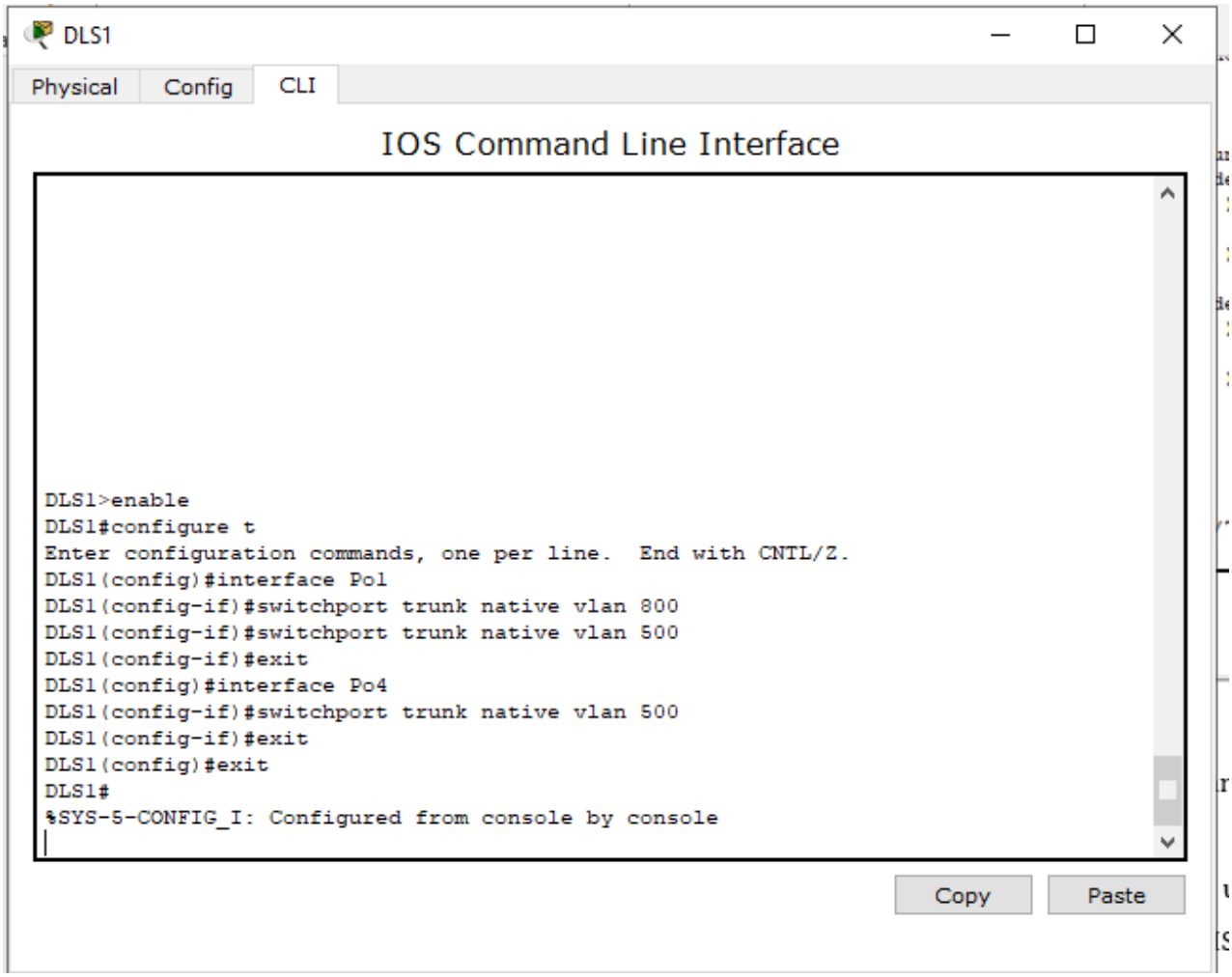


Figura 35. Aplicando código DLS2 VLAN 500

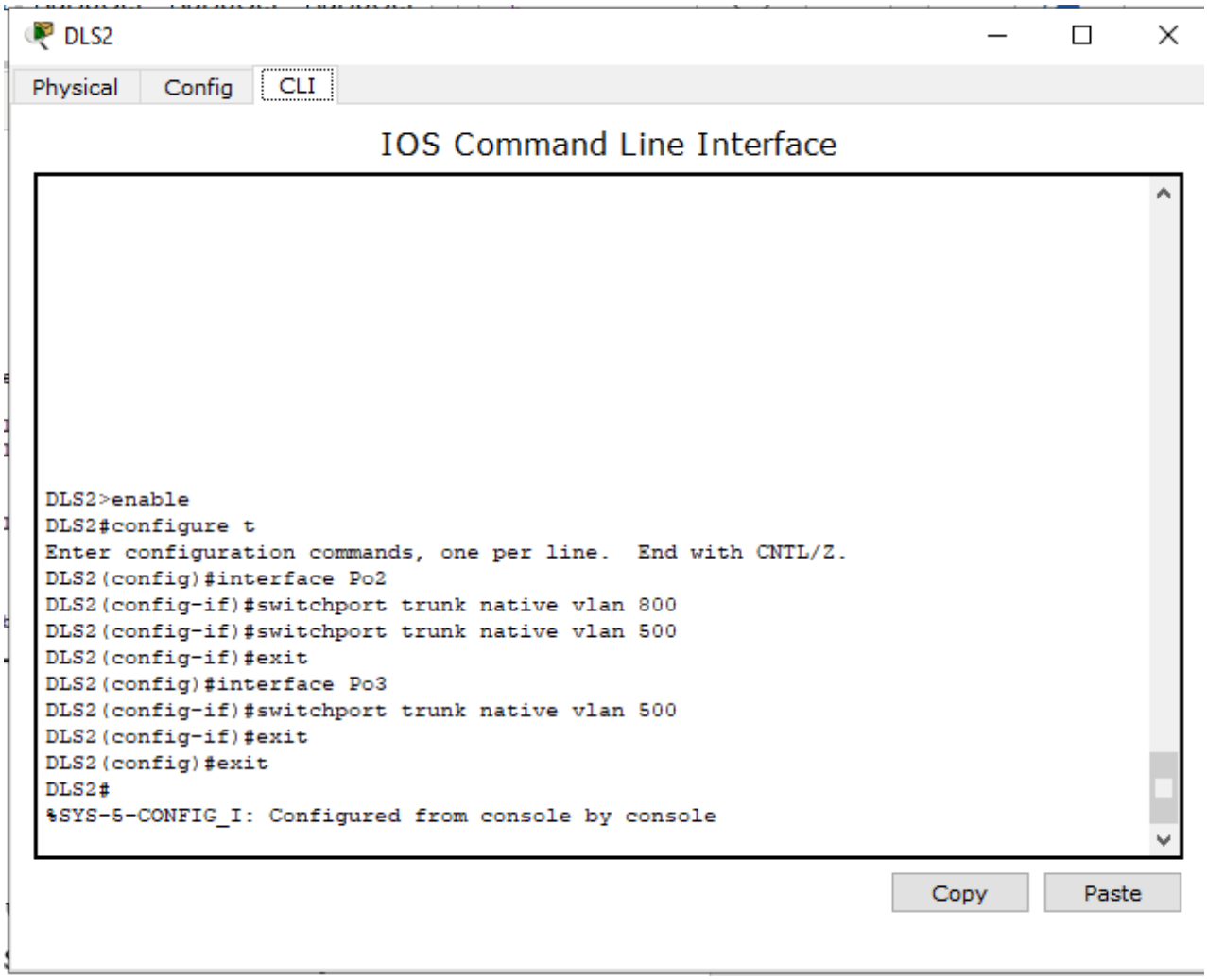


Figura 36. Aplicando código ASL1 VLAN 500

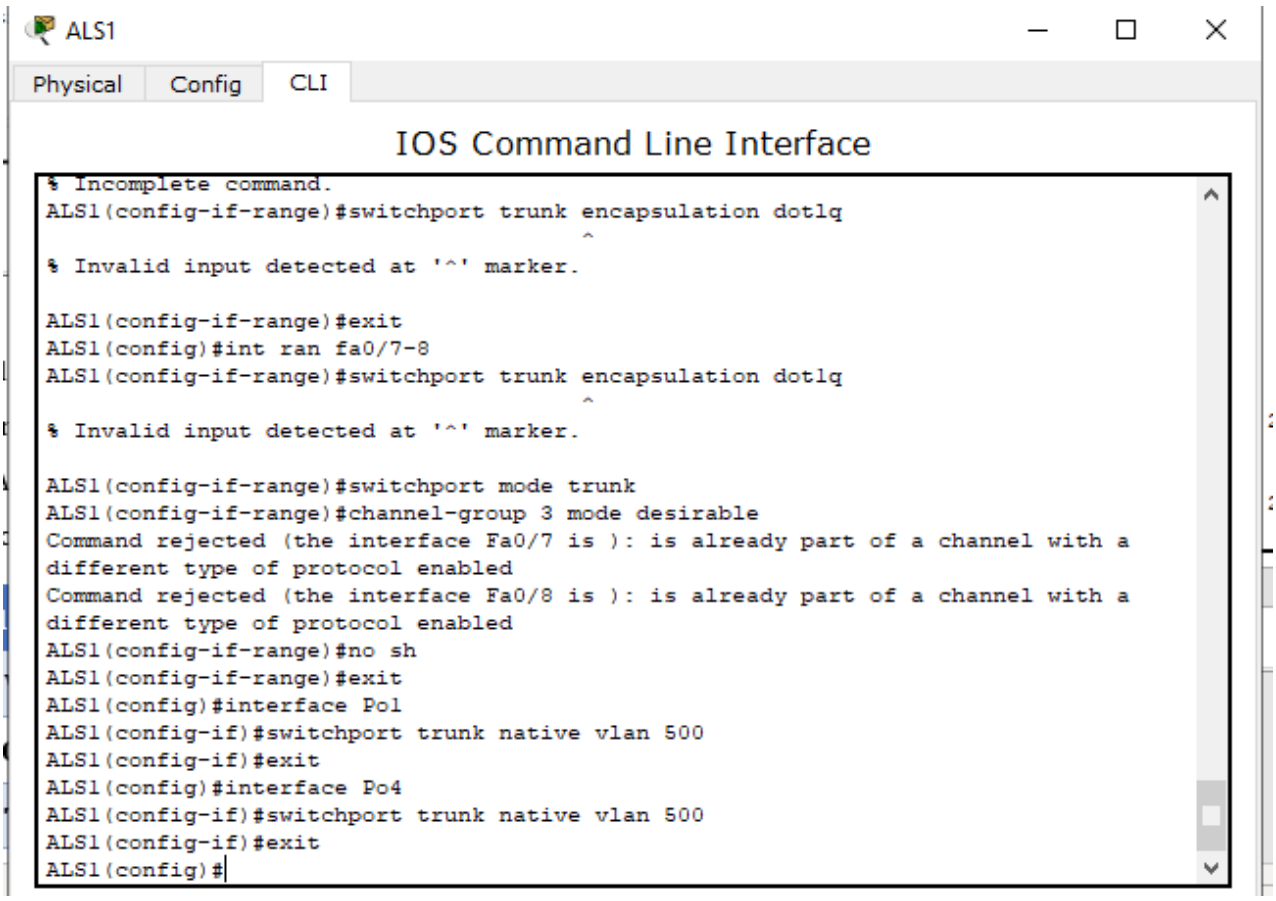
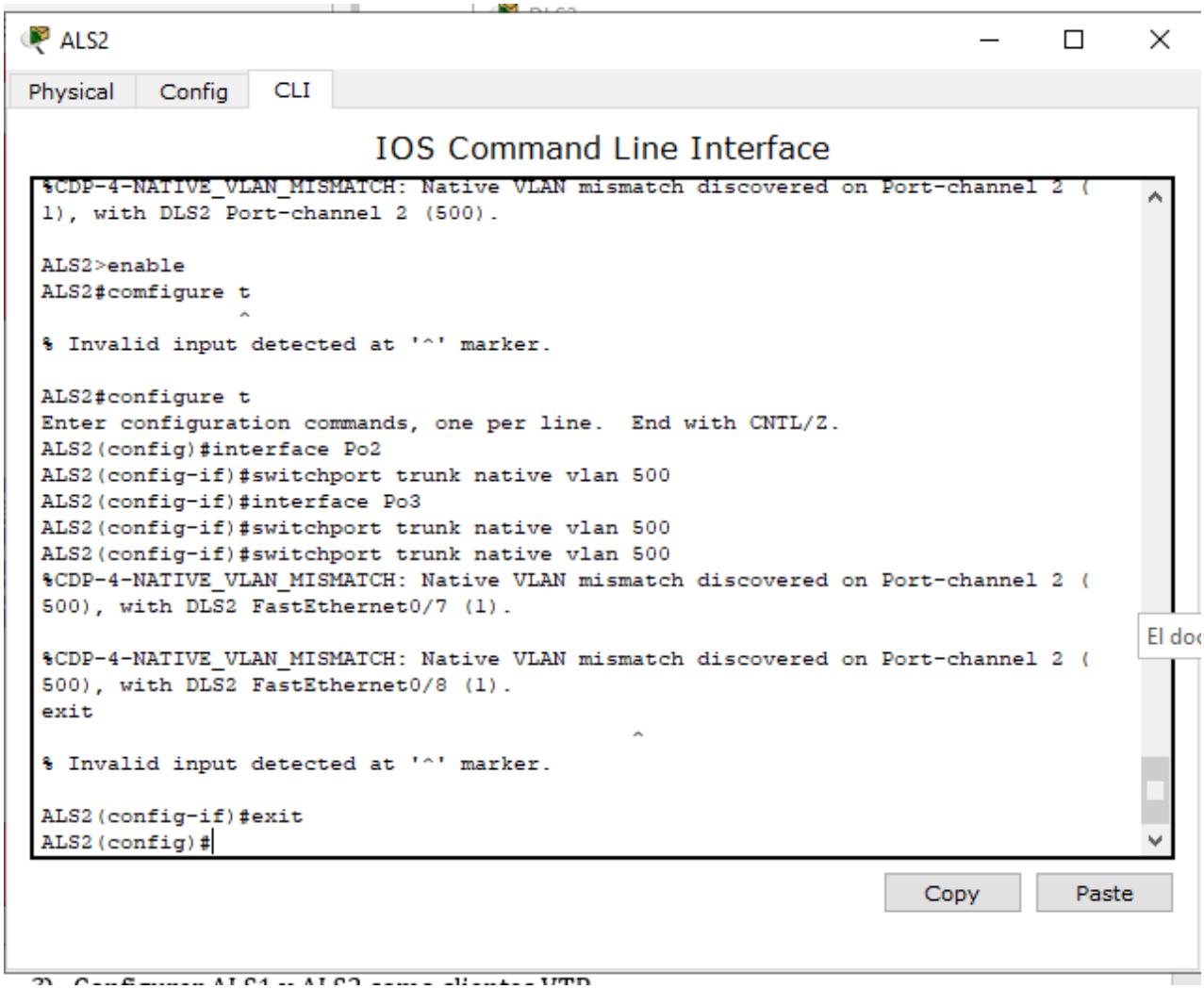


Figura 37. Aplicando código ASL2 VLAN 500



d. Configurar DLS1, ALS1, y ALS2 para utilizar VTP versión 3

1) Utilizar el nombre de dominio CISCO con la contraseña ccnp321

Figura 38. Aplicando código DLS1 VTP versión 3

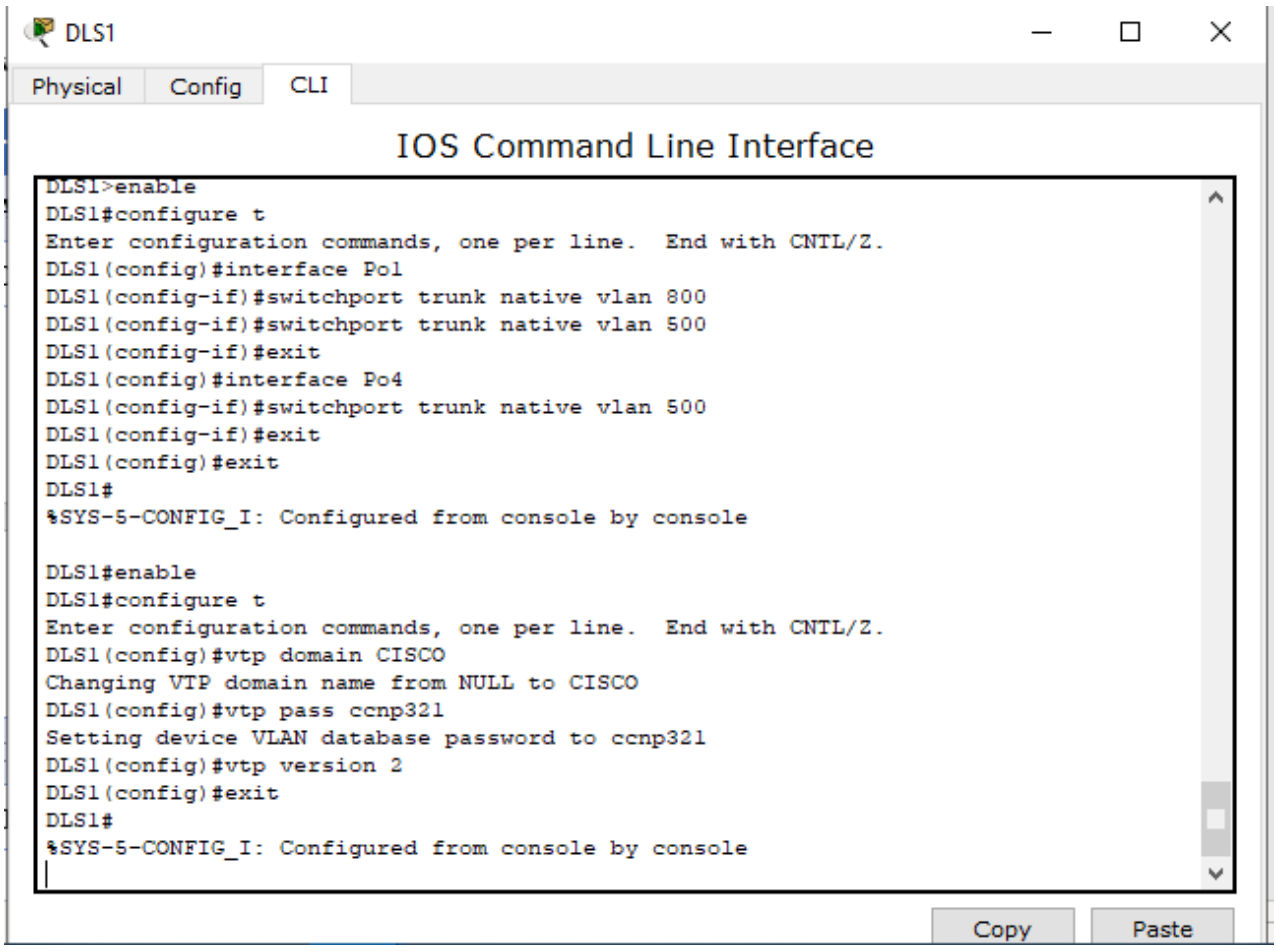
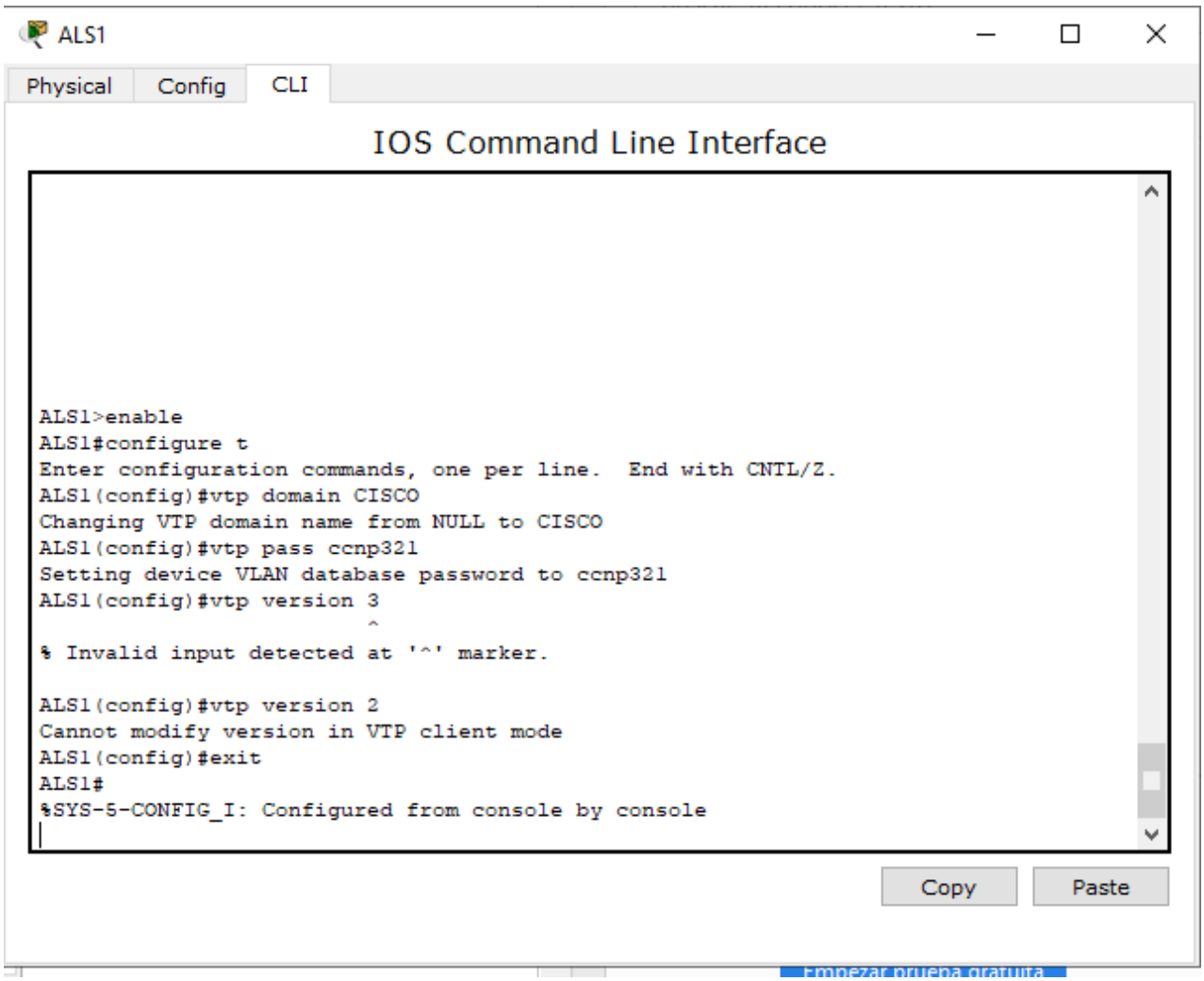
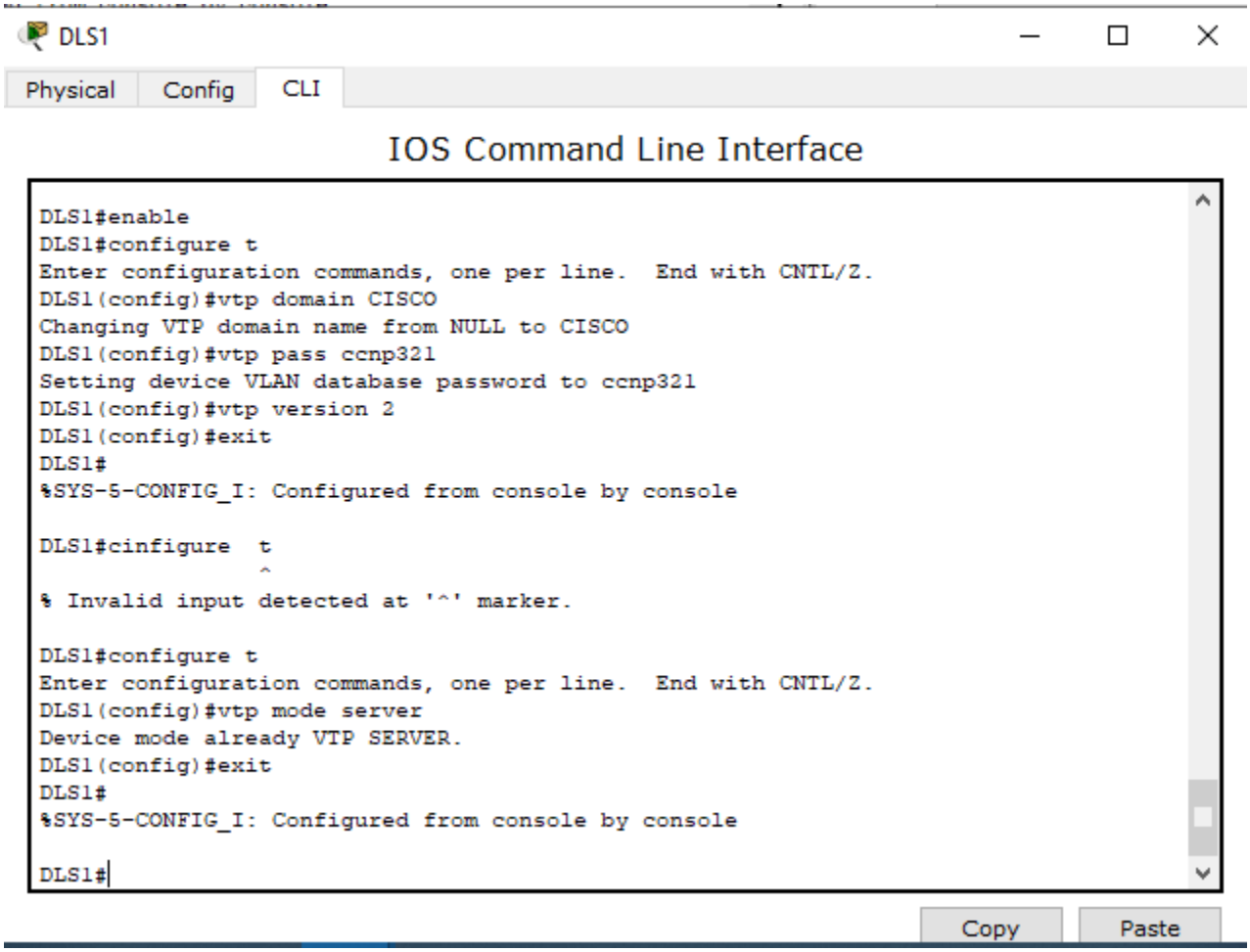


Figura 39. Aplicando código ASL1 VTP versión 3



2) Configurar DLS1 como servidor principal para las VLAN.

Figura 40. Aplicando código DLS1 VLAN principal



3) Configurar ALS1 y ALS2 como clientes VTP.

Figura 41. Aplicando código ASL1 clientes VTP

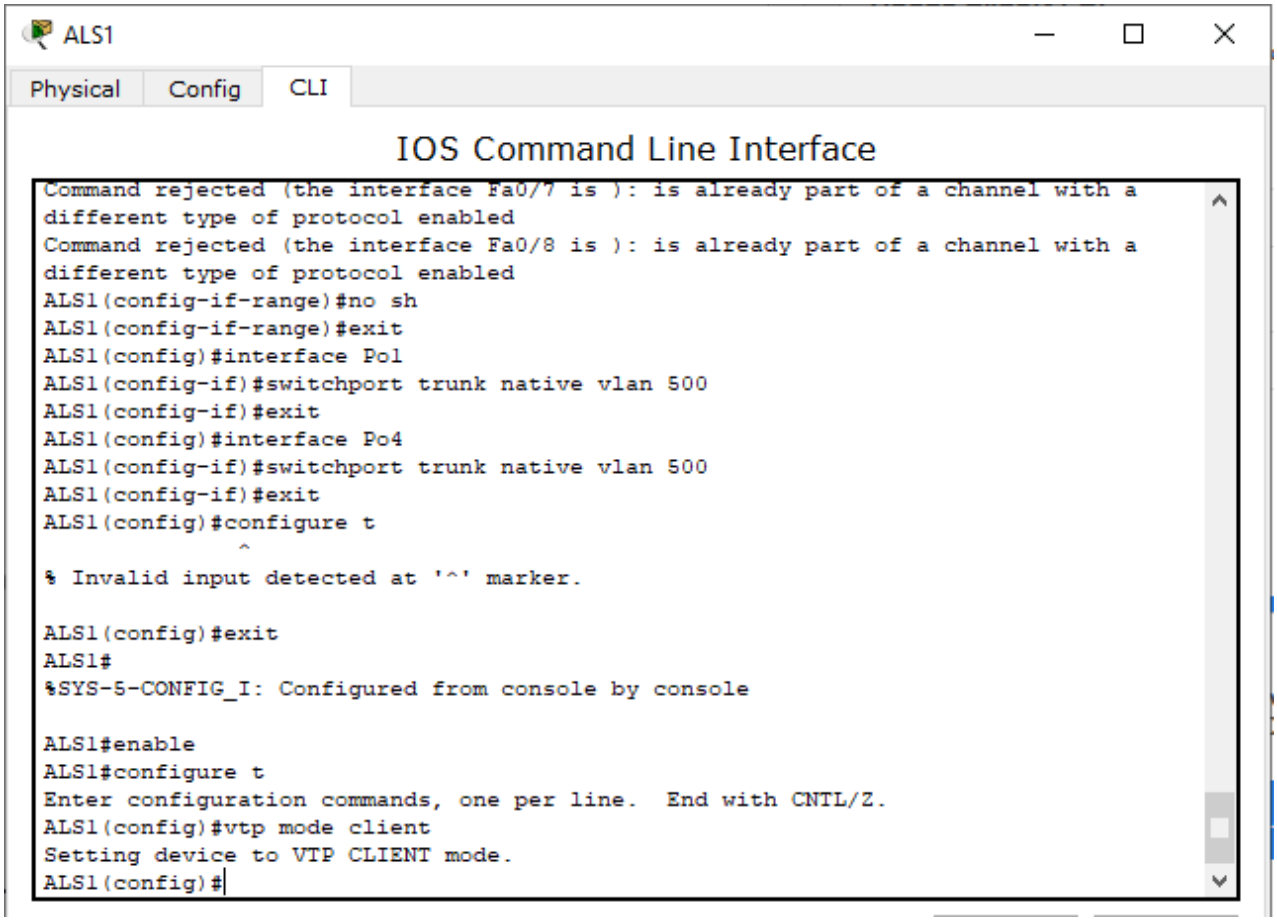
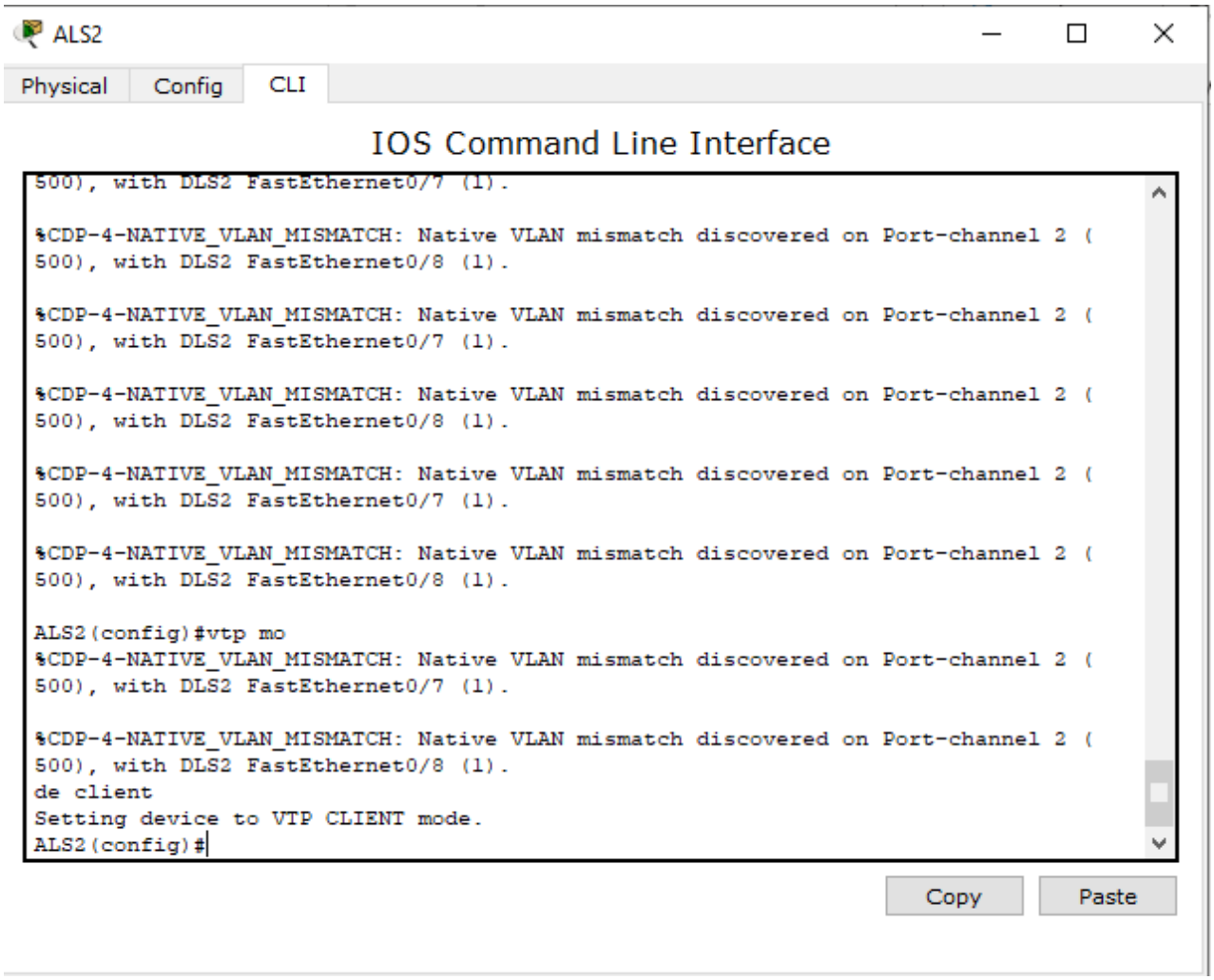


Figura 42. Aplicando código ASL2 clientes VTP



e. Configurar en el servidor principal las siguientes VLAN:

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
500	**NATIVA**	434	**PROVEEDORES**
12	**ADMON**	123	**SEGUROS**
234	**CLIENTES**	1010	**VENTAS**
1111	**MULTIMEDIA**	3456	**PERSONAL**

Figura 43. Aplicando código DLS1 VLAN

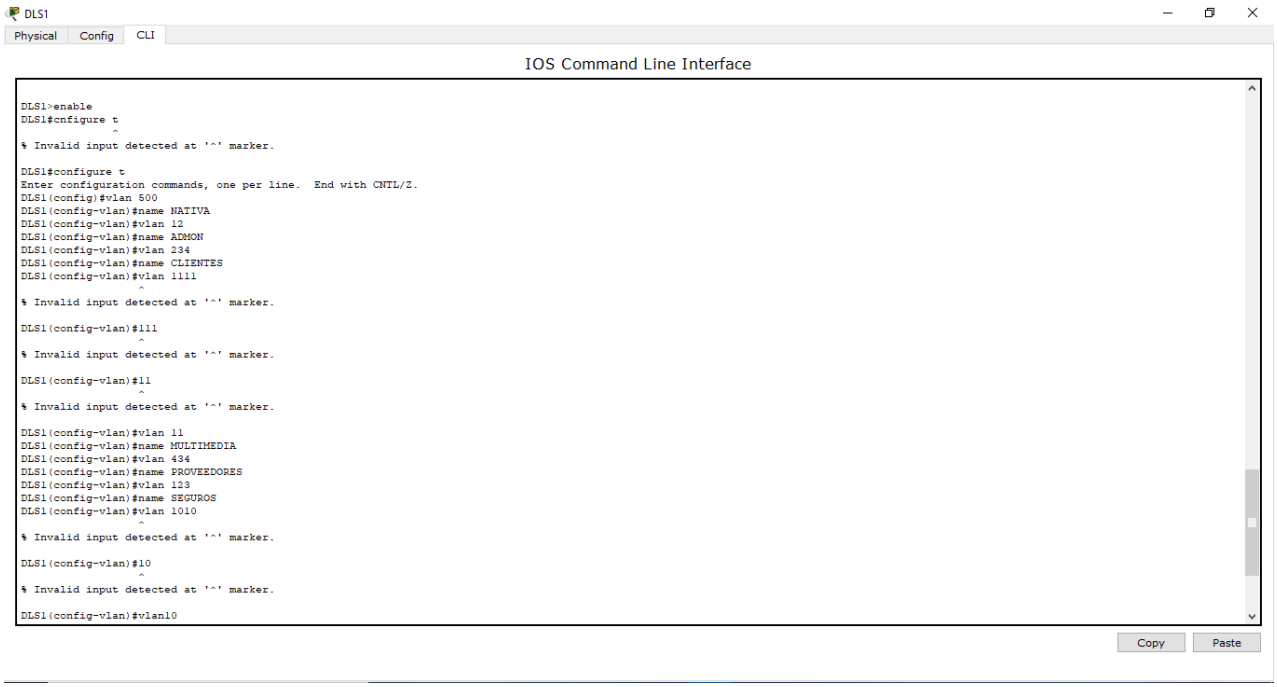
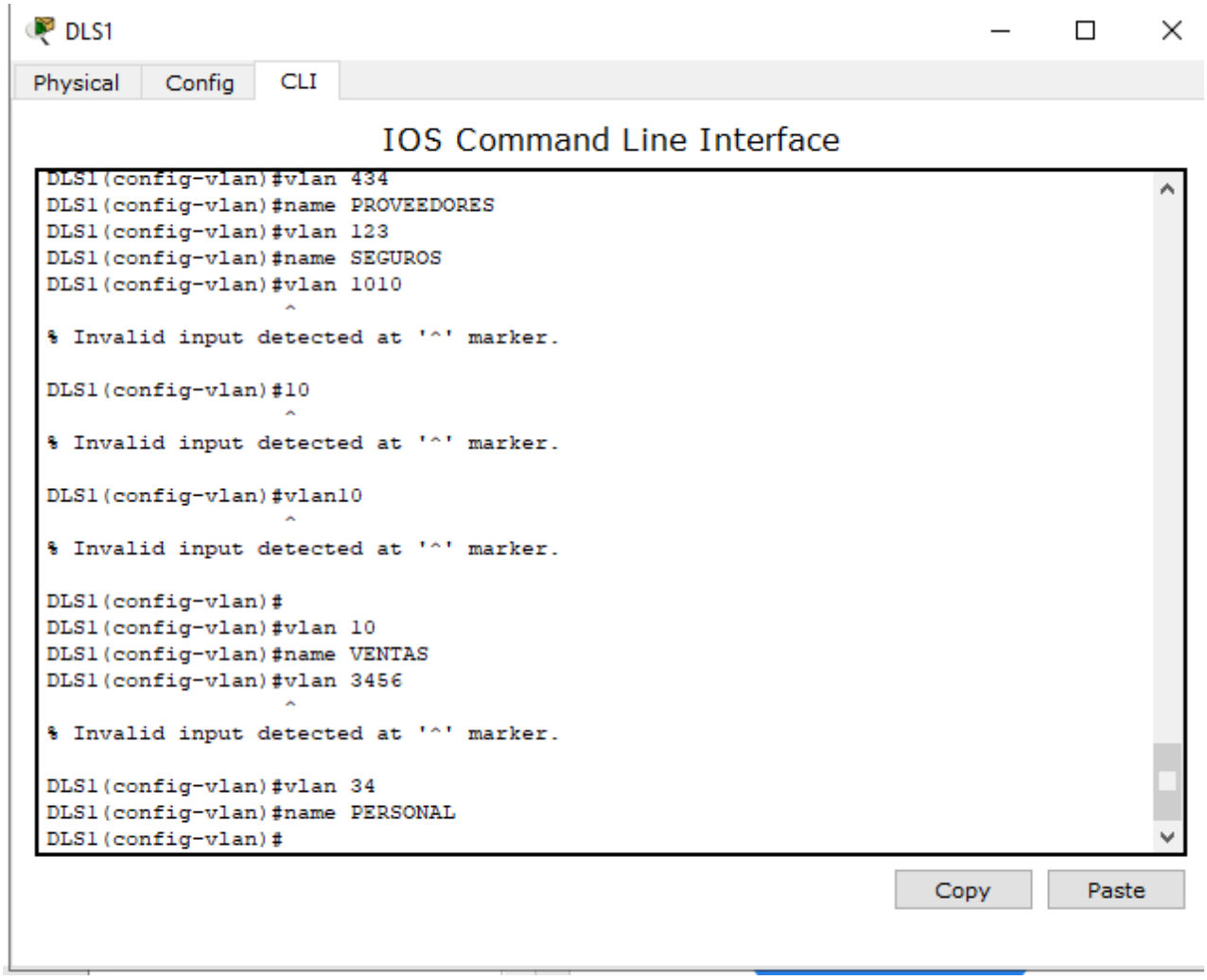
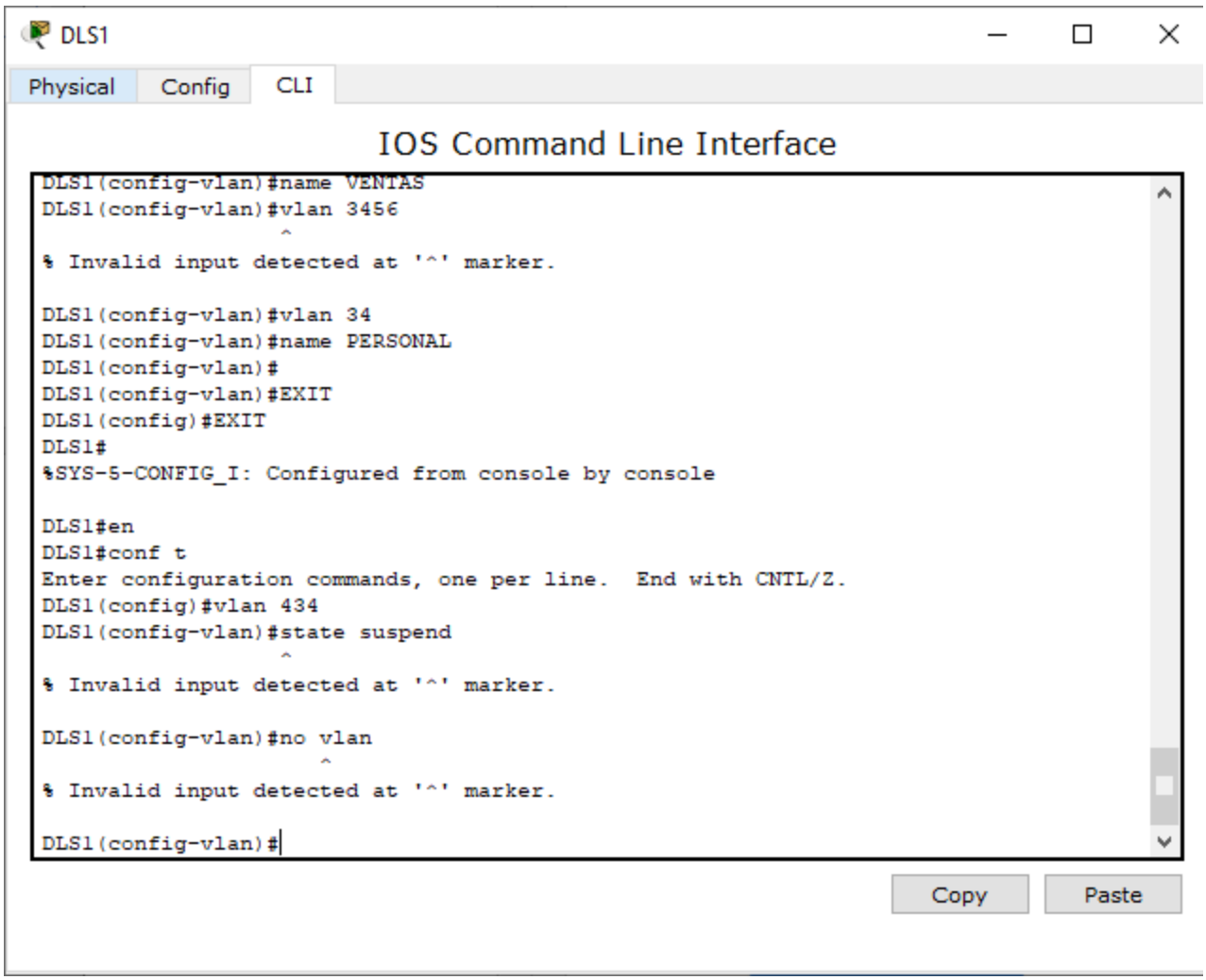


Figura 44. Aplicando código DLS1 VLAN



a. En DLS1, suspender la VLAN 434.

Figura 43. Aplicando código DLS1 434



Packet tracer no soporta el comando para suspender la Vlan.

b. Configurar DLS2 en modo VTP transparente VTP utilizando VTP versión 2, y configurar en DLS2 las mismas VLAN que en DLS1.

Figura 44. Aplicando código DLS2 VTP transparente

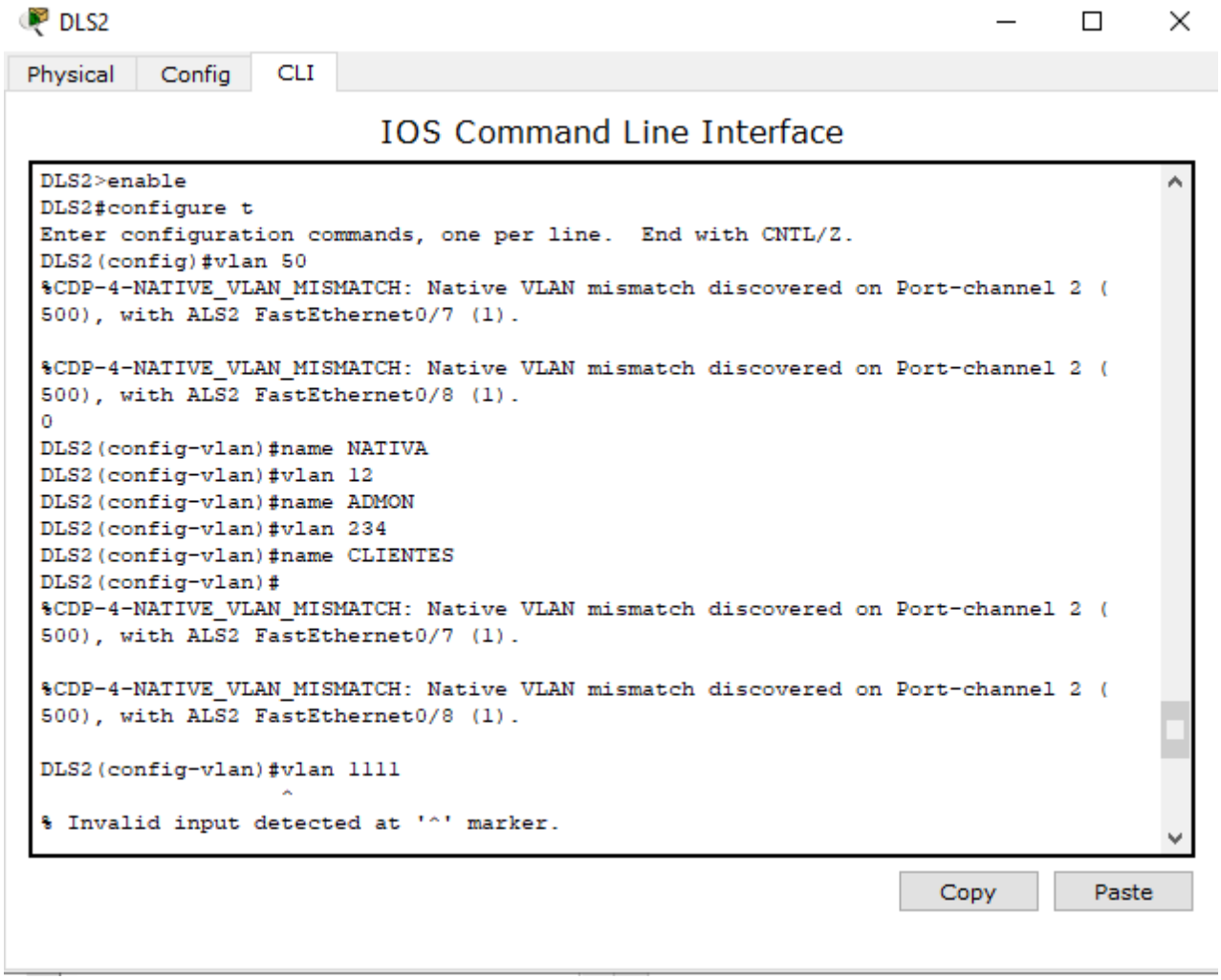
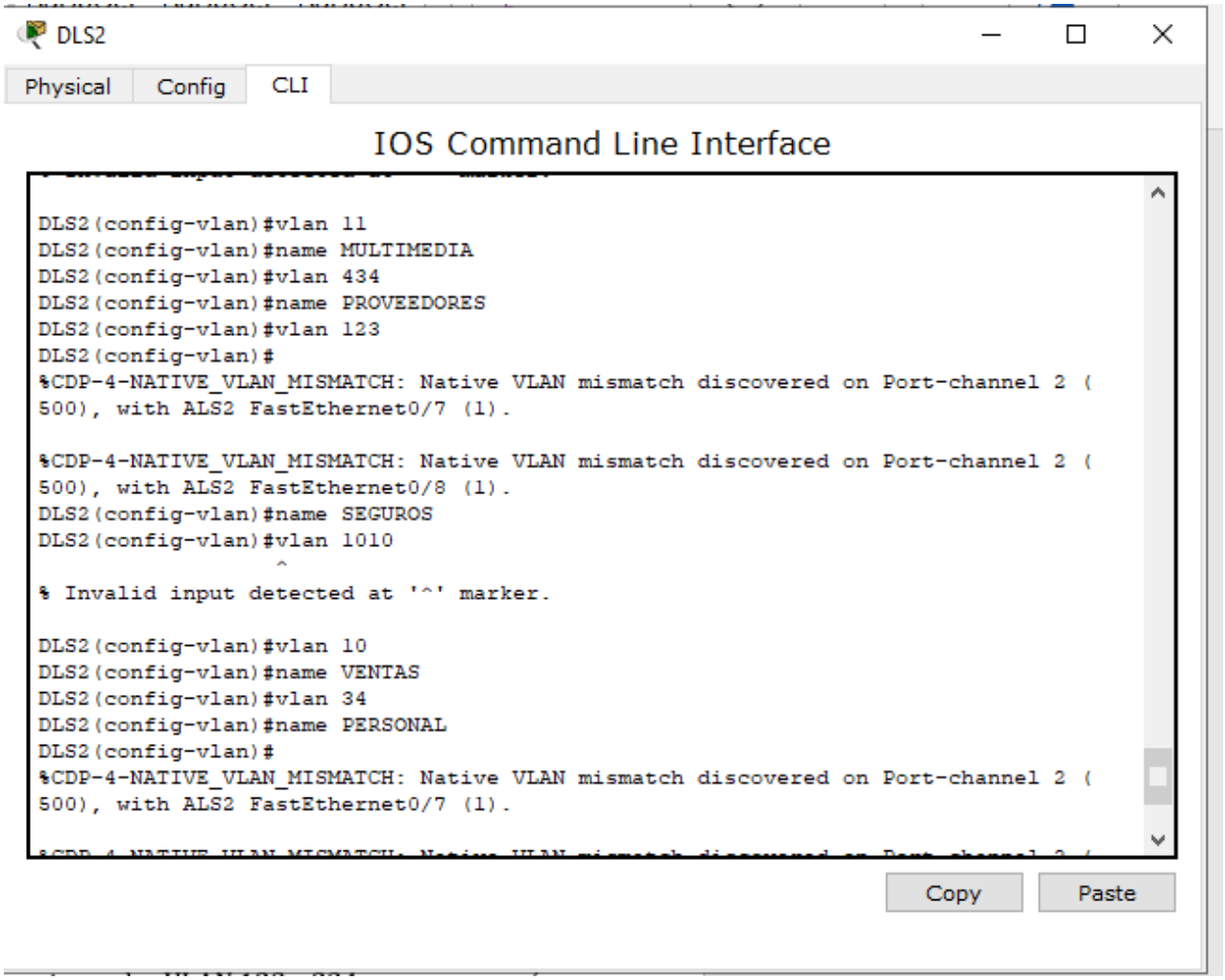
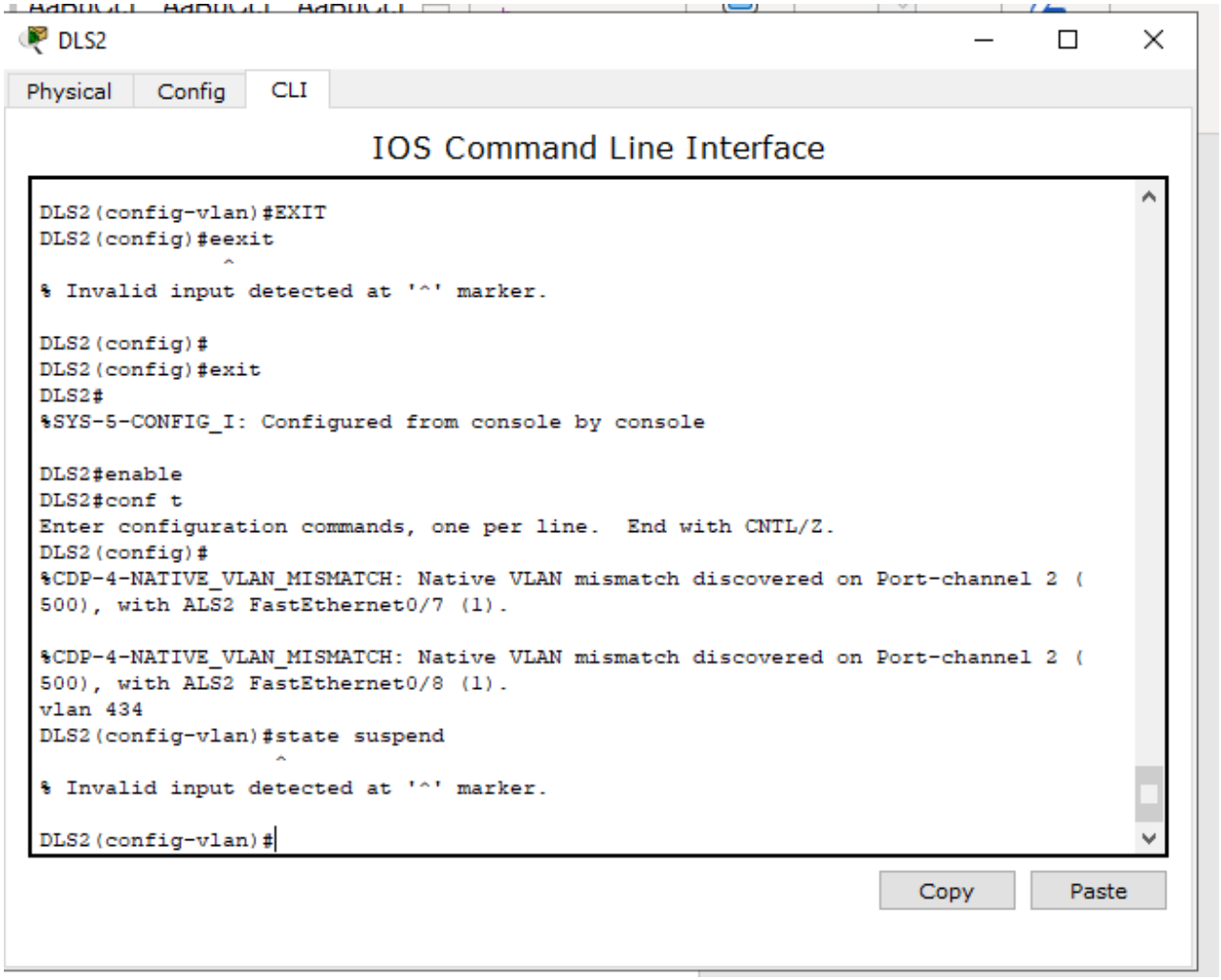


Figura 45. Aplicando código DLS2 VTP transparente



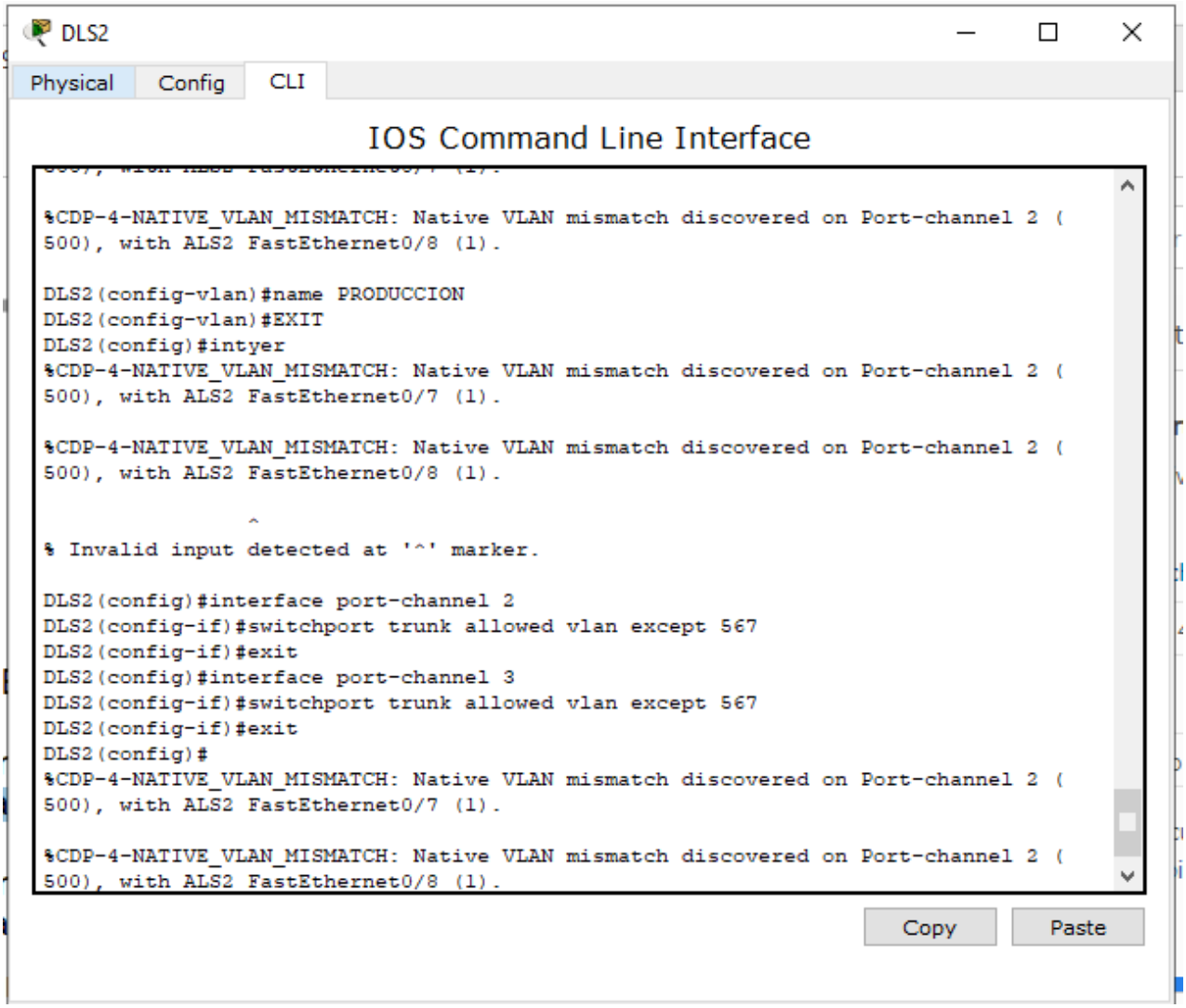
c. Suspender VLAN 434 en DLS2.

Figura 46. Aplicando código DLS2 suspender VLAN 434



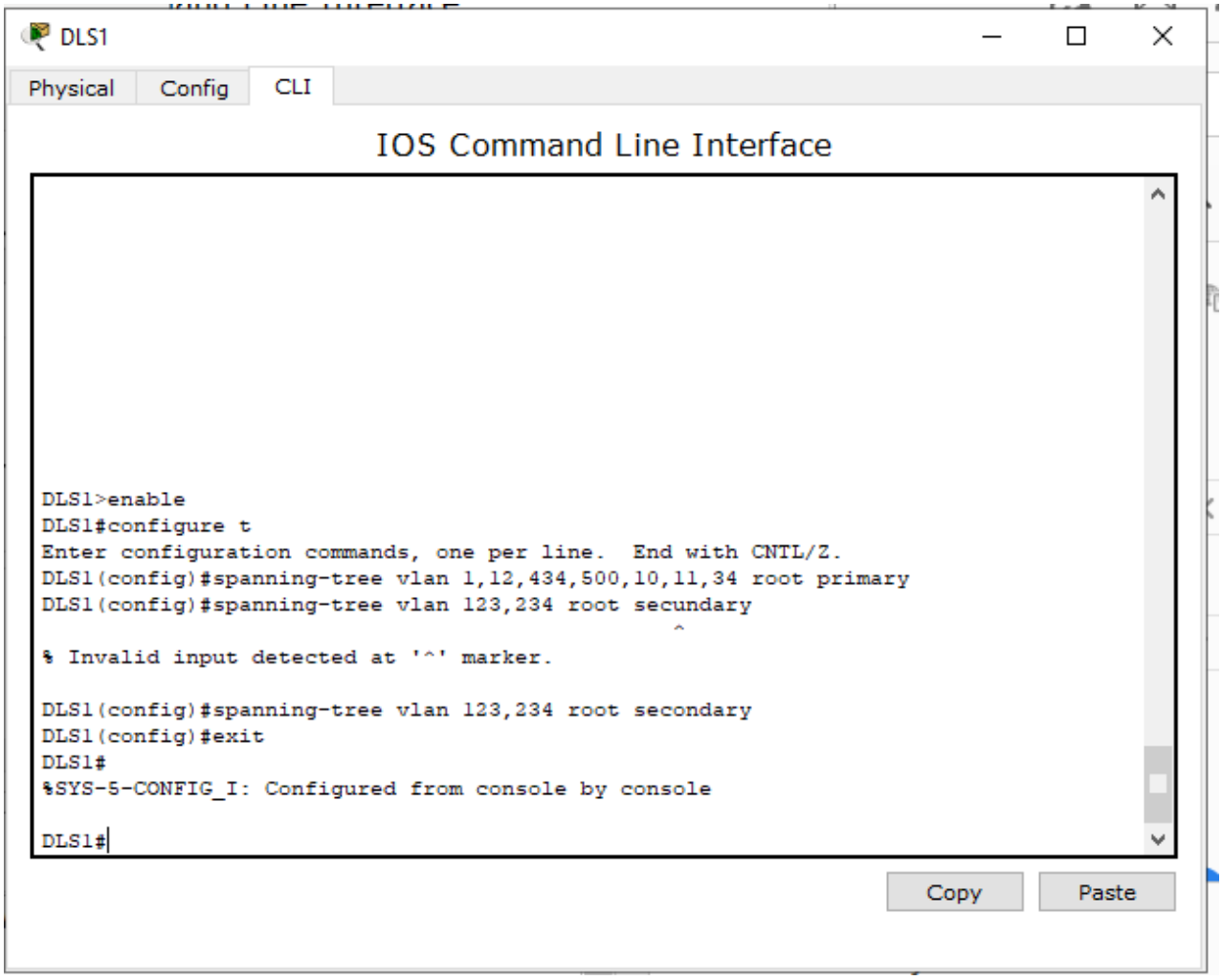
d. En DLS2, crear VLAN 567 con el nombre de PRODUCCION. La VLAN de PRODUCCION no podrá estar disponible en cualquier otro Switch de la red.

Figura 47. Aplicando código DLS2 VLAN 567



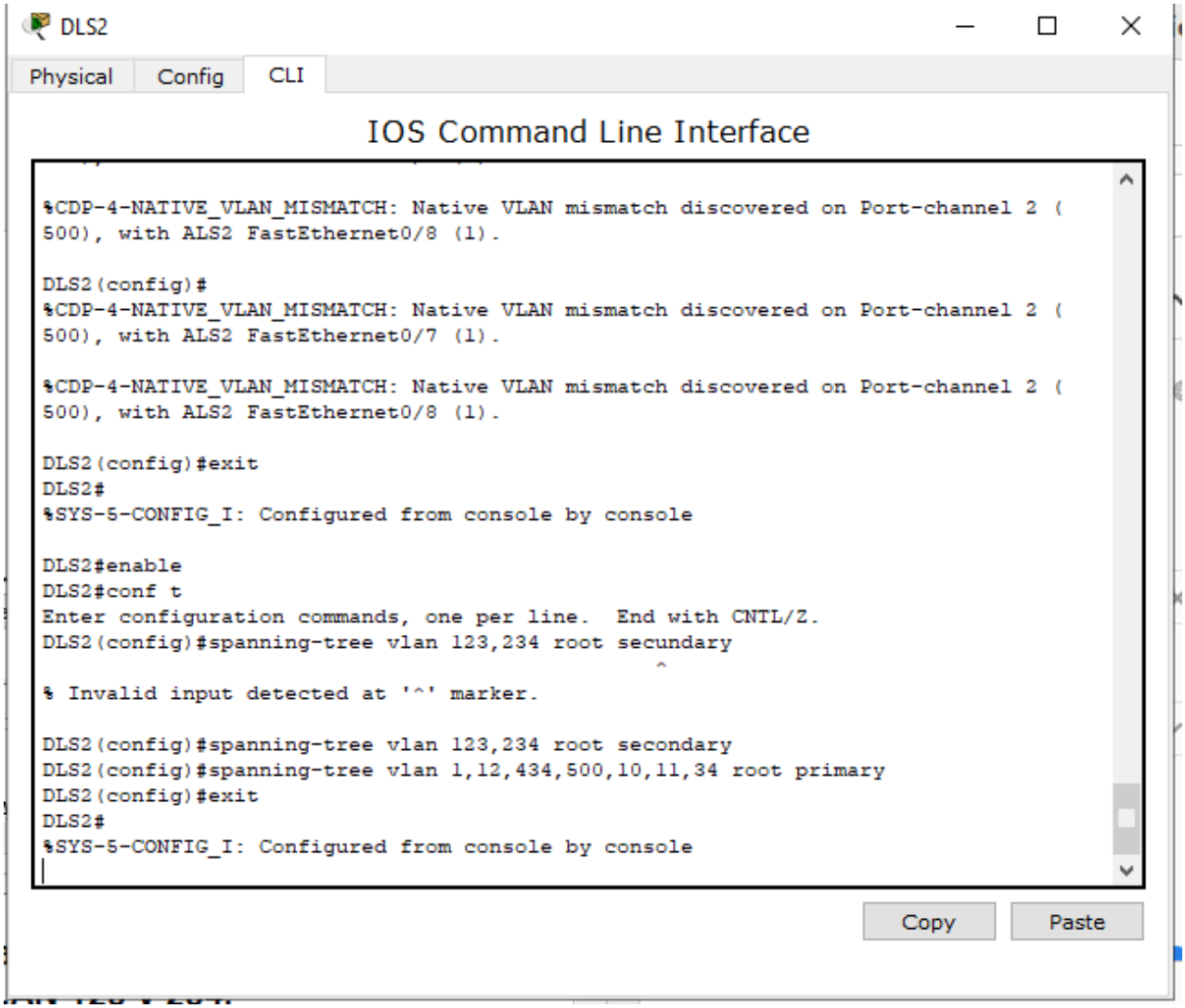
e. Configurar DLS1 como Spanning tree root para las VLAN 1, 12, 434, 500, 1010, 1111 y 3456 y como raíz secundaria para las VLAN 123 y 234.

Figura 48. Aplicando código DLS1 Spanning tree root



f. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 500, 1010, 1111 y 3456.

Figura 49. Aplicando código DLS2 Spanning tree root



g. Configurar todos los puertos como troncales de tal forma que solamente las VLAN que se han creado se les permitirá circular a través de éstos puertos.

Figura 50. Aplicando código DLS1 puertos como troncales

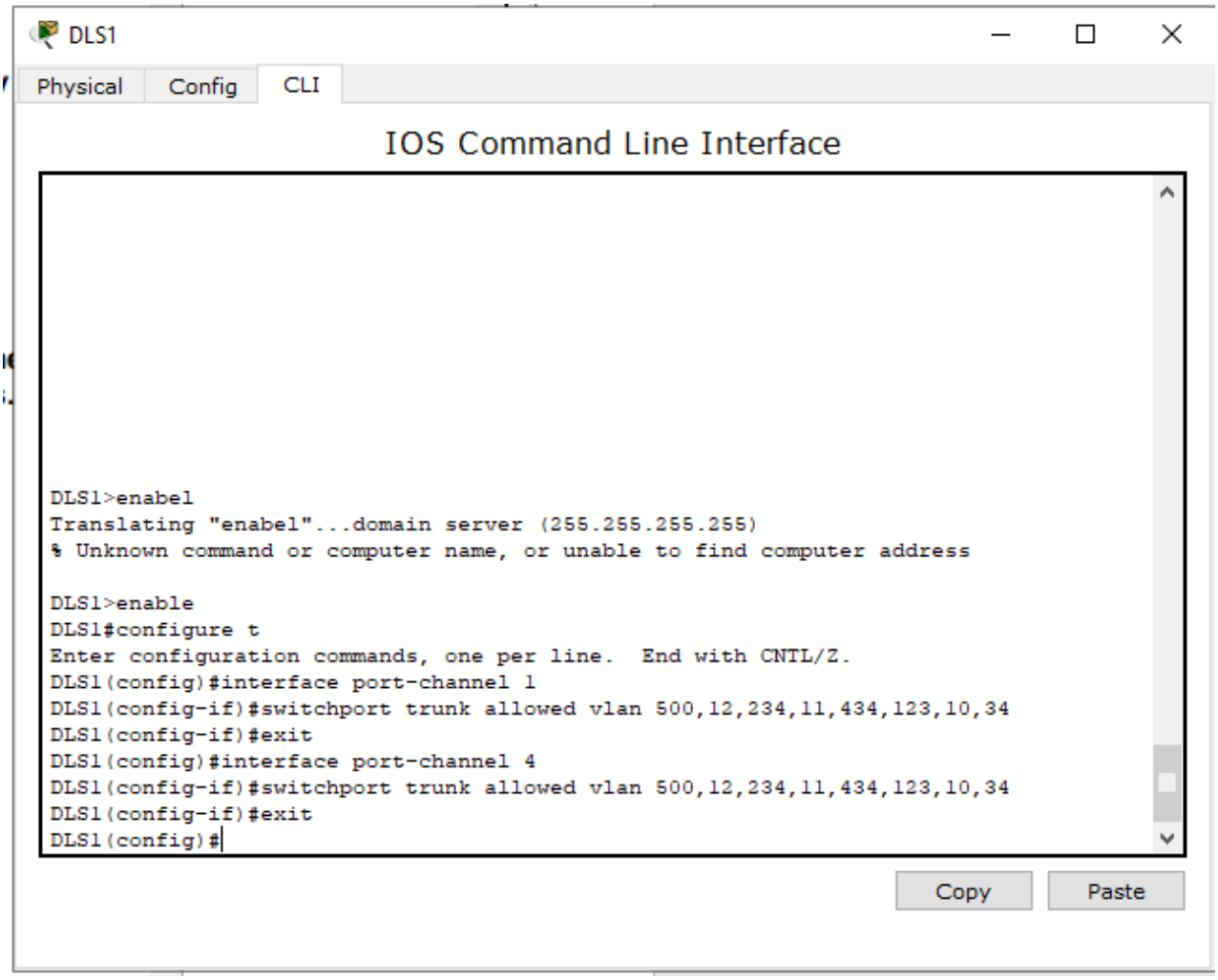
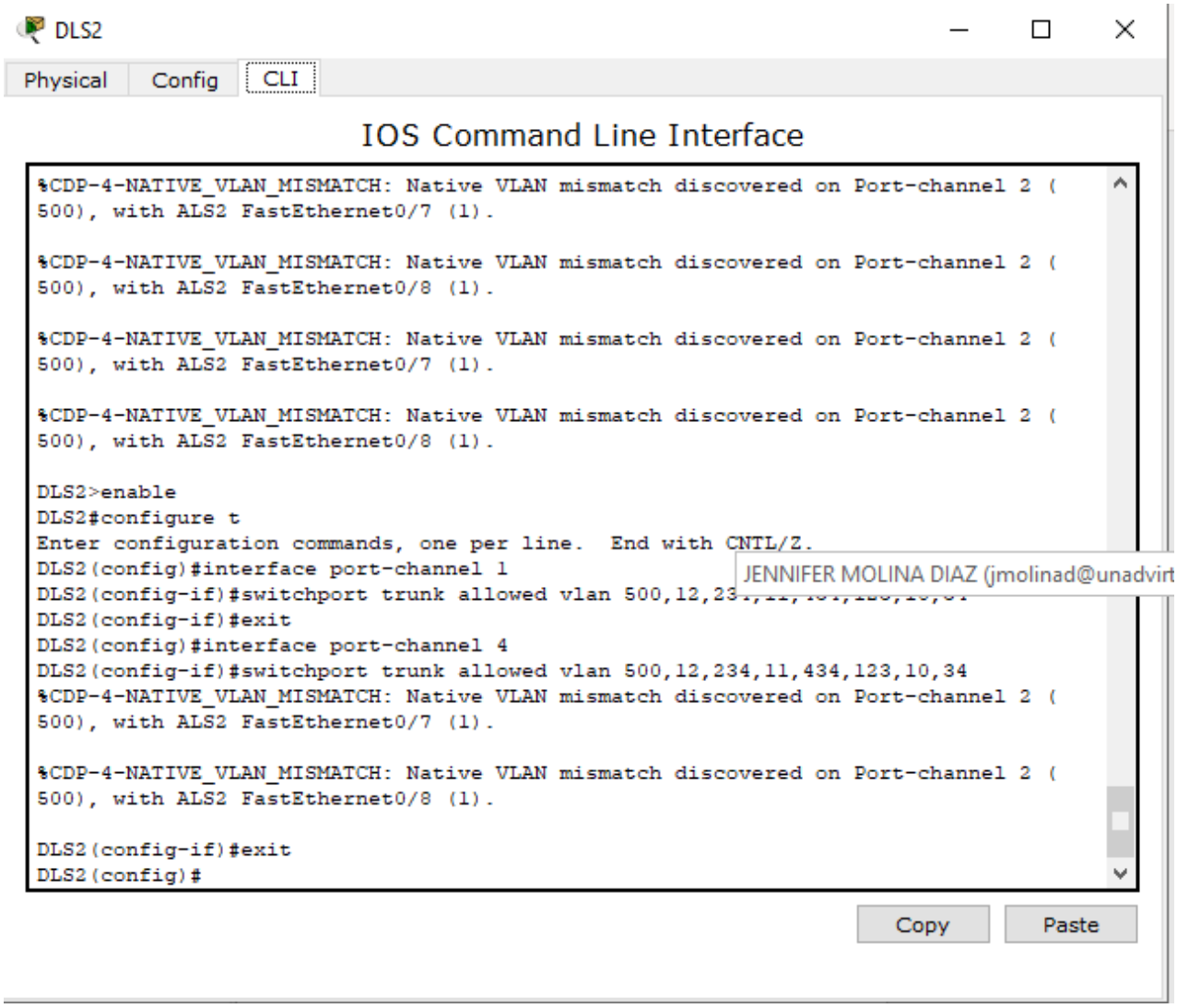


Figura 51. Aplicando código DLS2 puertos como troncales



Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3456	12 , 1010	123, 1010	234

Interfaz Fa0/15	1111	1111	1111	1111
Interfaces F0 /16-18		567		

h. Configurar las siguientes interfaces como puertos de acceso, asignados a las VLAN de la siguiente manera:

TABLA 6. Asignación de interfaces vlan

Figura 52. Aplicando código DLS1 interfaces

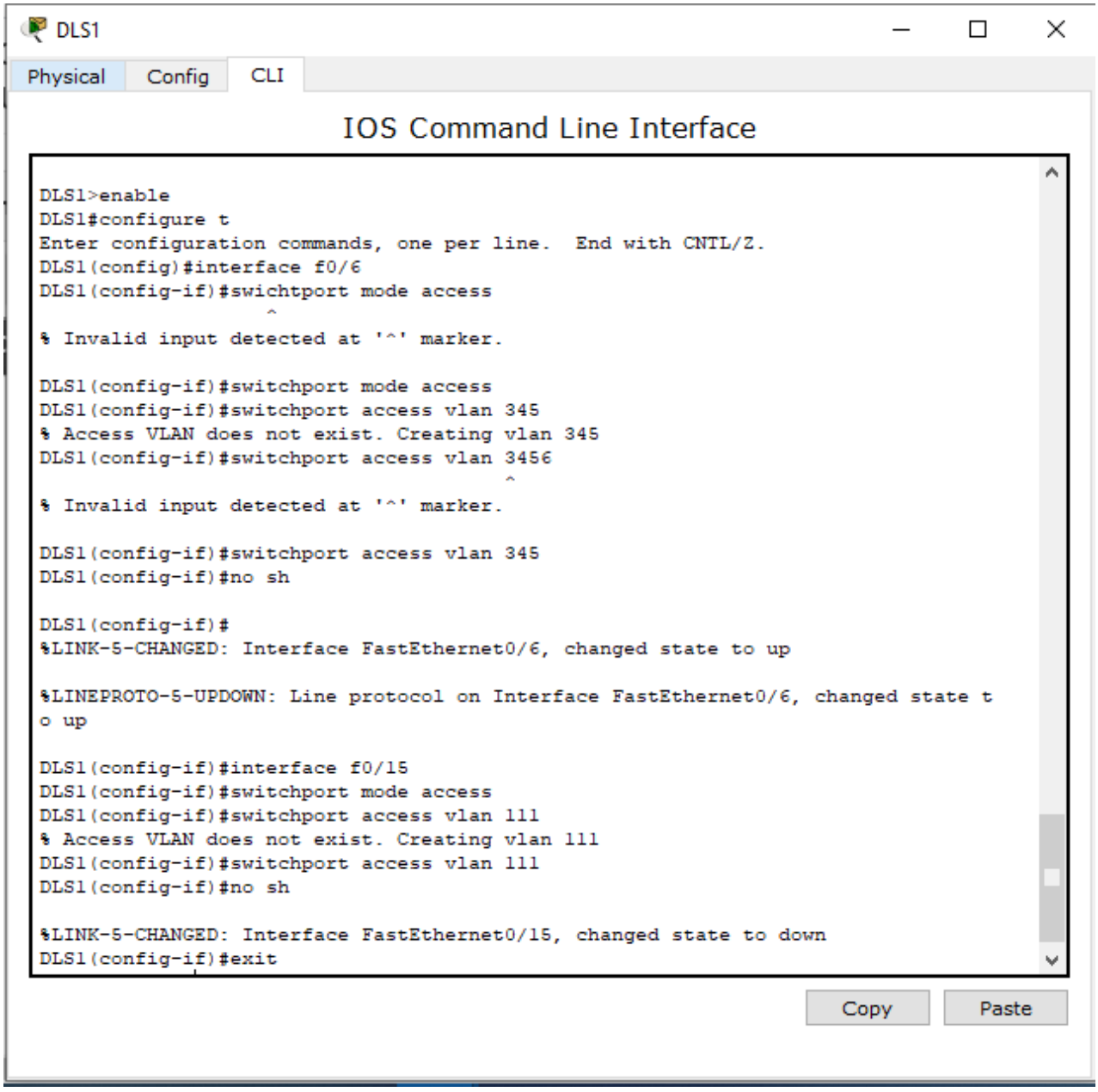


Figura 53. Aplicando código DLS2 interfaces

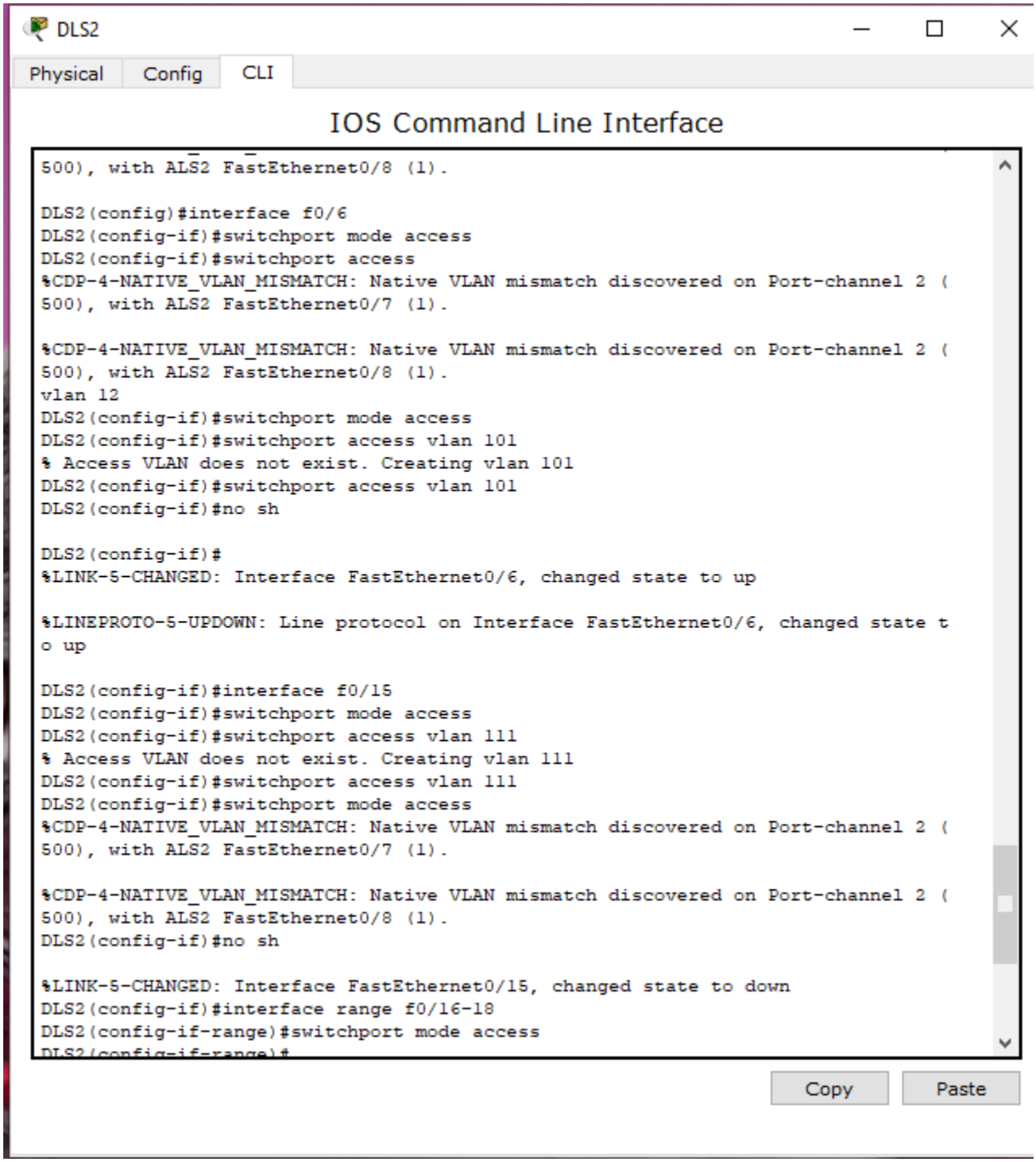


Figura 54. Aplicando código ASL1 interfaces

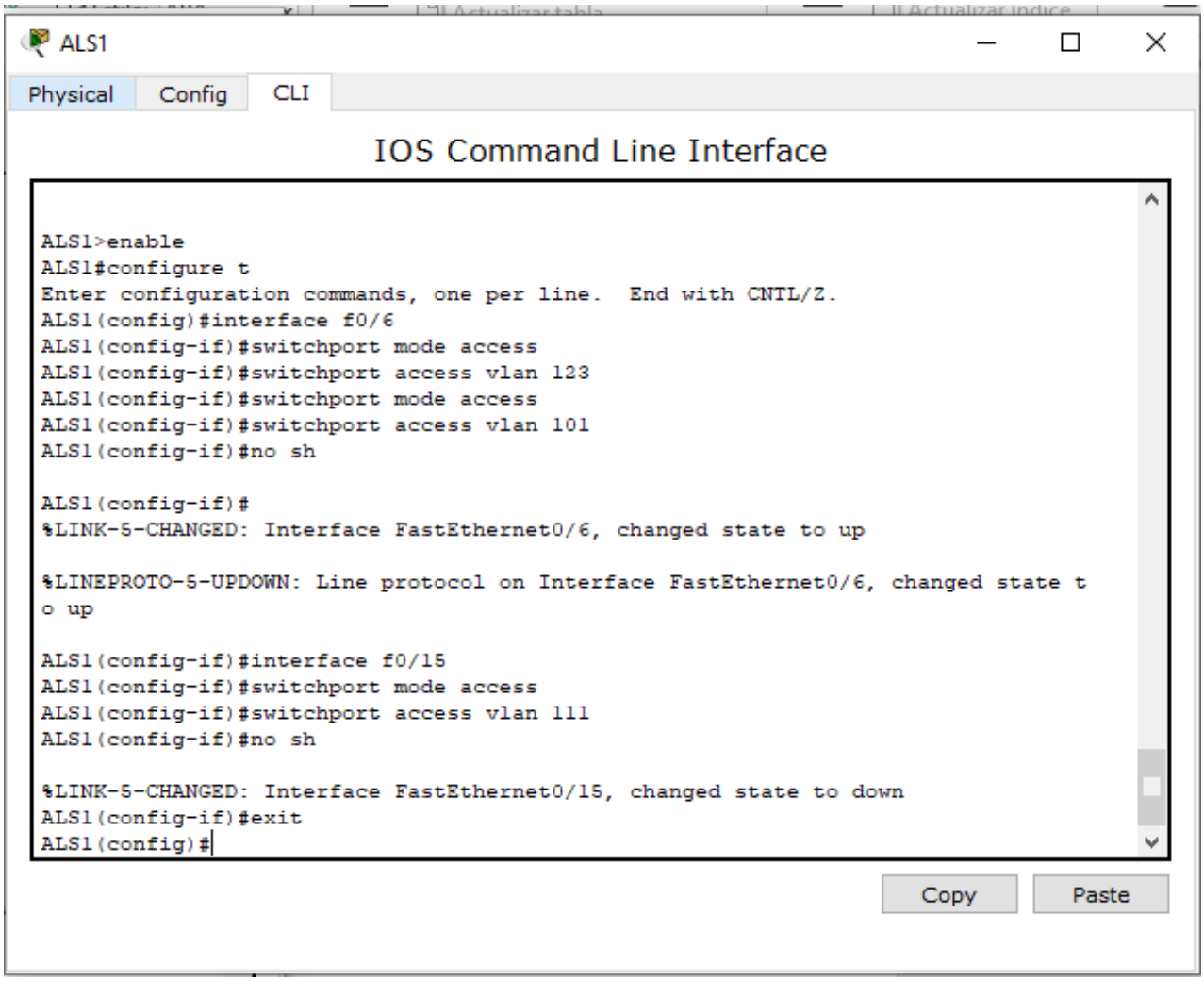
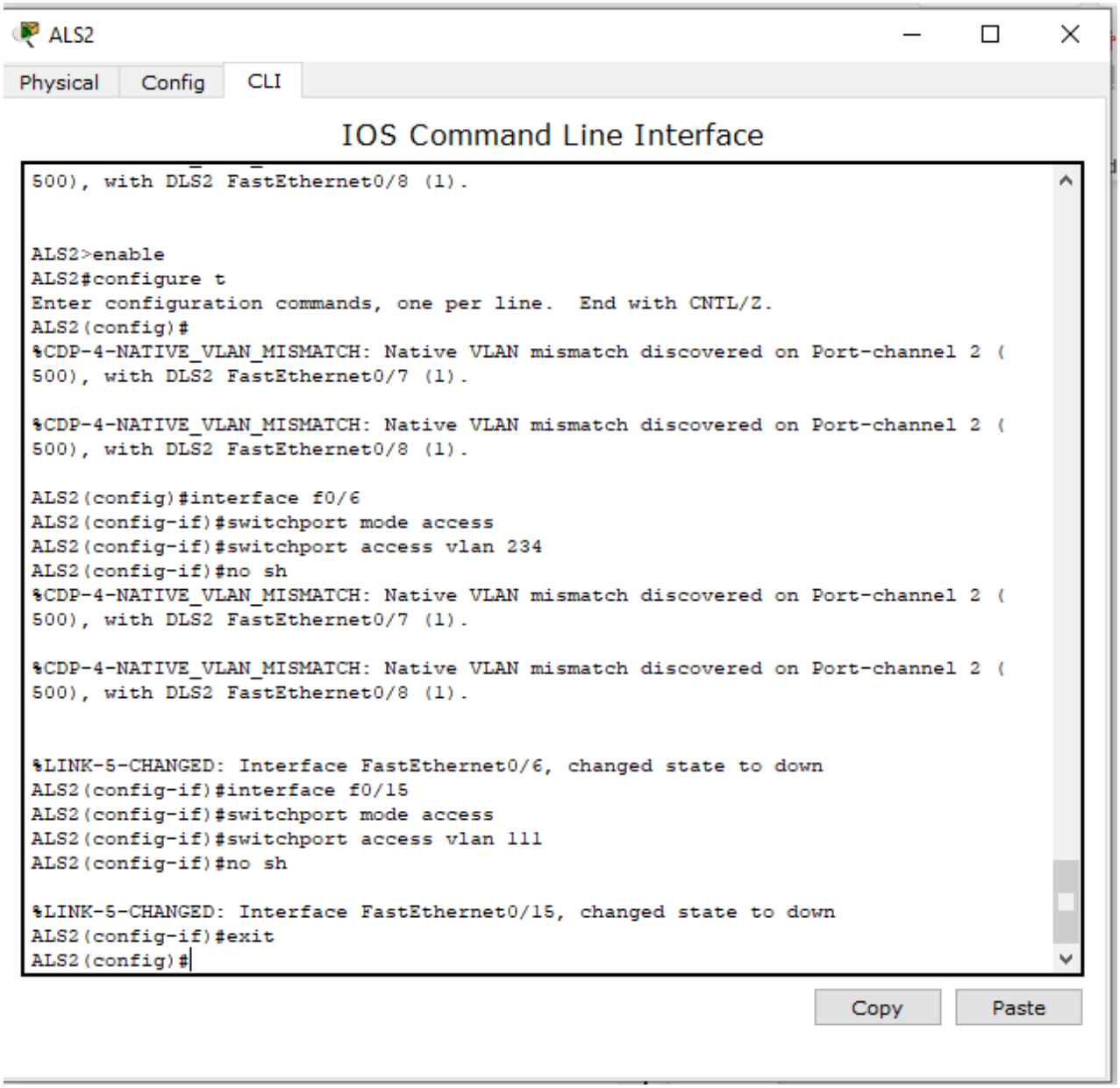


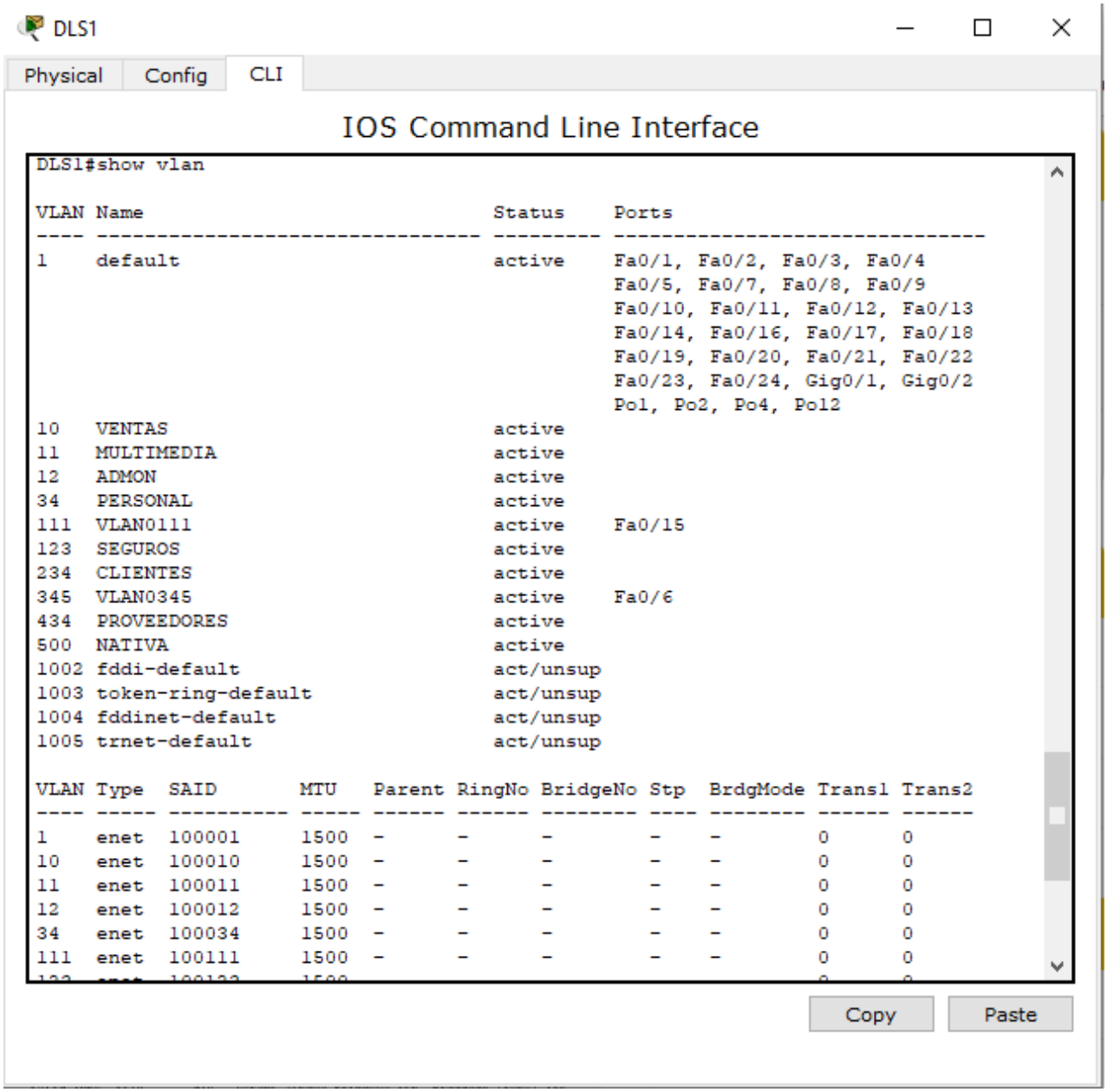
Figura 55. Aplicando código ASL2 interfaces



Parte 2: conectividad de red de prueba y las opciones configuradas.

a. Verificar la existencia de las VLAN correctas en todos los switches y la asignación de puertos troncales y de acceso

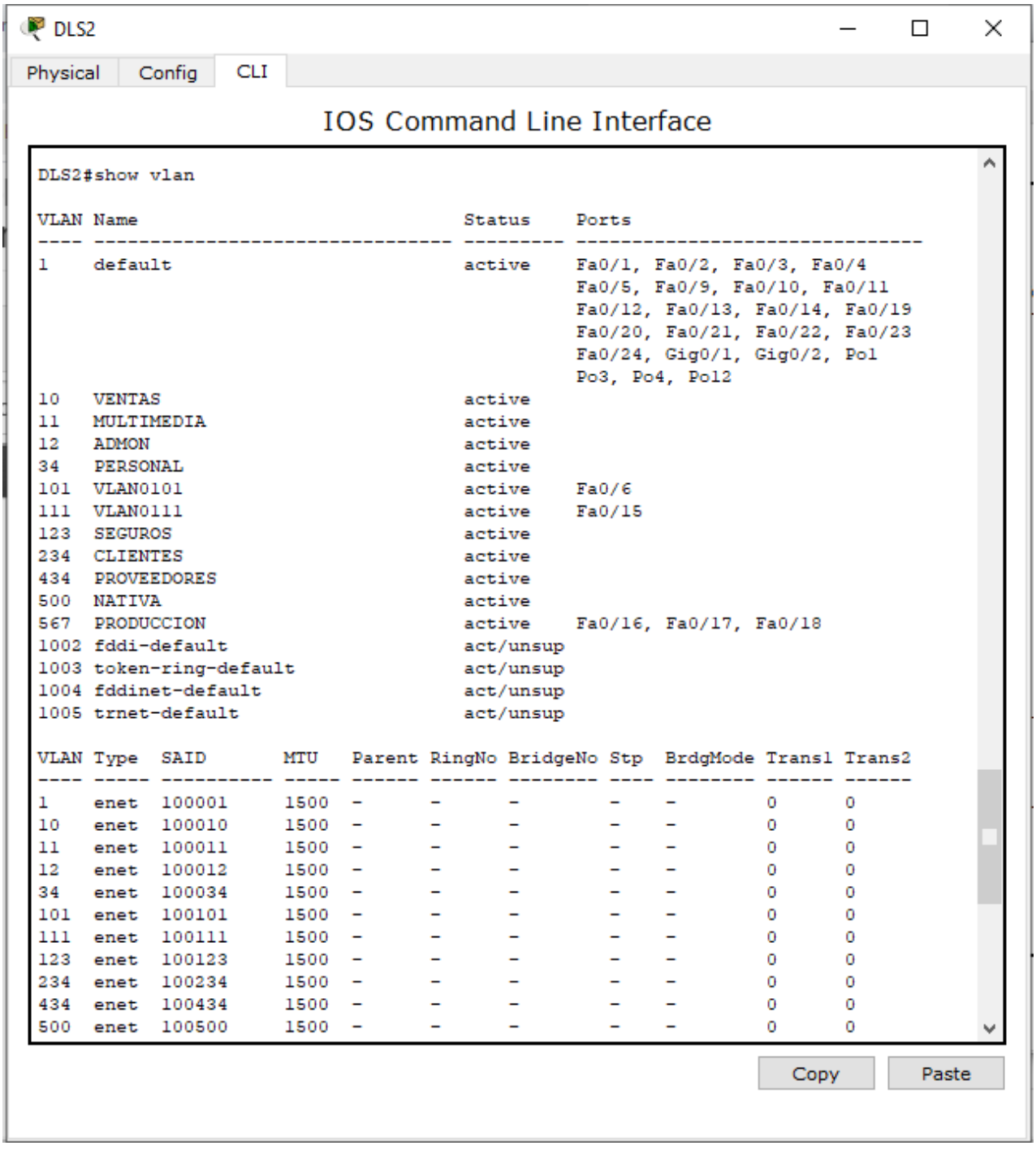
Figura 56. Aplicando código DLS1 existencia de las VLAN



Se verifica las vlan del código DSL1 se ejecuta el comando show vlan en cada swicht

DLS1# show vlan se ejecuta el comando show vlan para validar las vlan configuradas

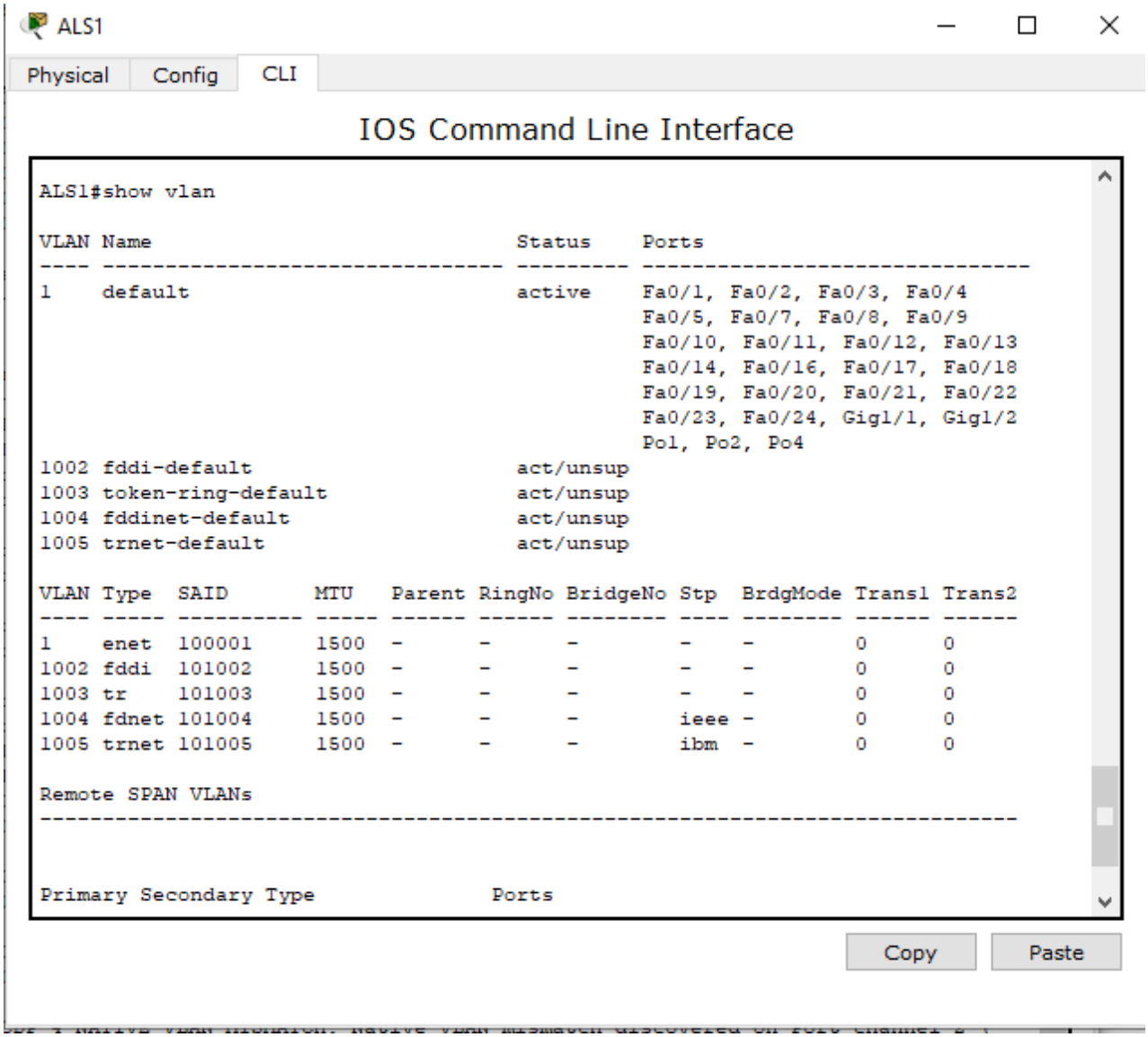
Figura 57. Aplicando código DLS2 existencia de las VLAN



Se verifica las vlan del código DSL2 se ejecuta el comando show vlan en cada swicht

DLS2# show vlan

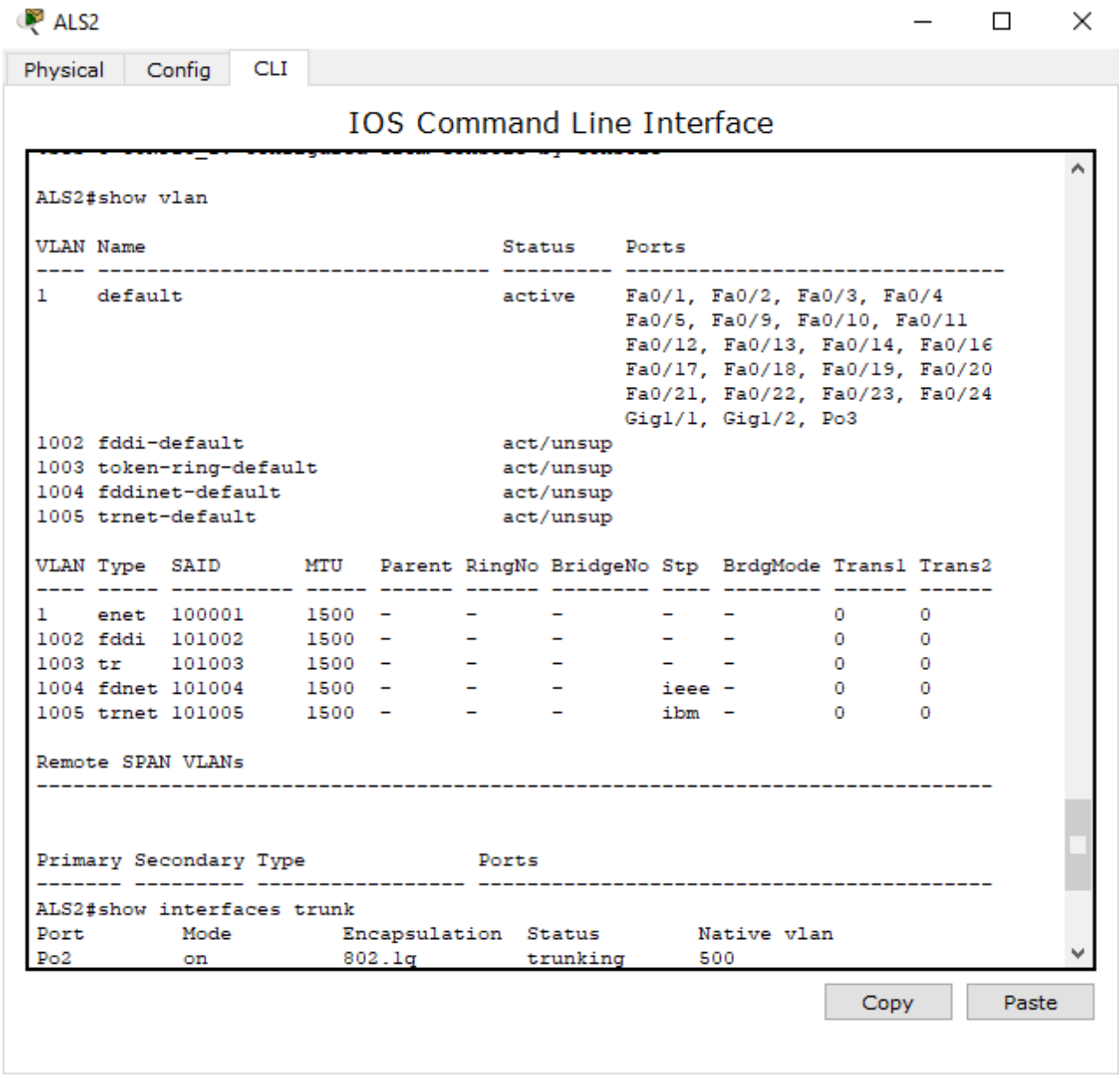
Figura 58. Aplicando código ASL1 existencia de las VLAN



Se verifica las vlan del código ASL1 se ejecuta el comando show vlan en cada swicht

ASL1# show vlan

Figura 59. Aplicando código DLS2 existencia de las VLAN



Se verifica las vlan del código ASL2 se ejecuta el comando show vlan en cada swicht

ASL2# show vlan

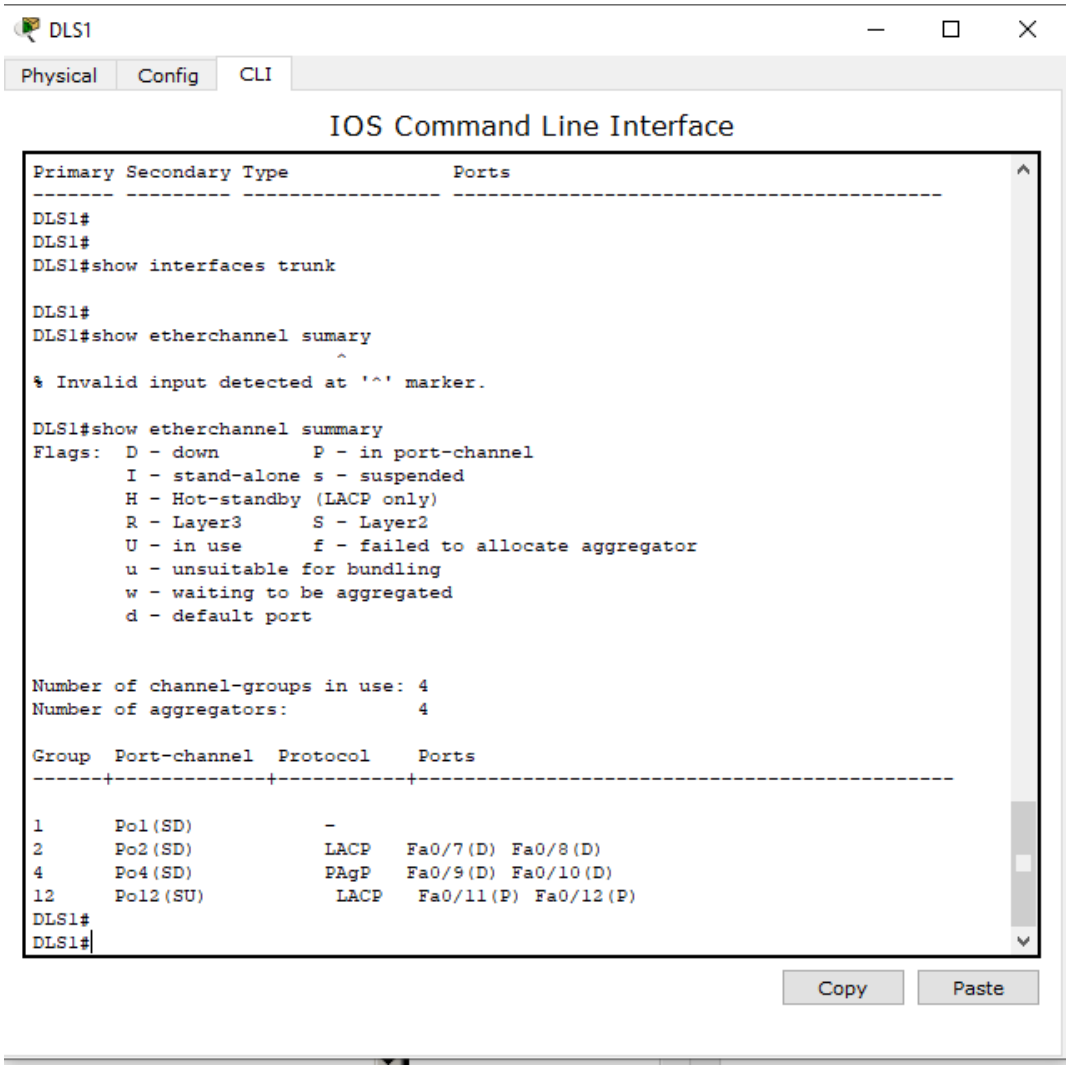
Este commando no indica las vlans configuradas en cada switch del escenario 2

b. Verificar que el EtherChannel entre DLS1 y ALS1 está configurado correctamente

Se ejecuta comando show ethertchannel sumary en cada swicht para validar su configuracion correcta

DLS1# show ethertchannel summary

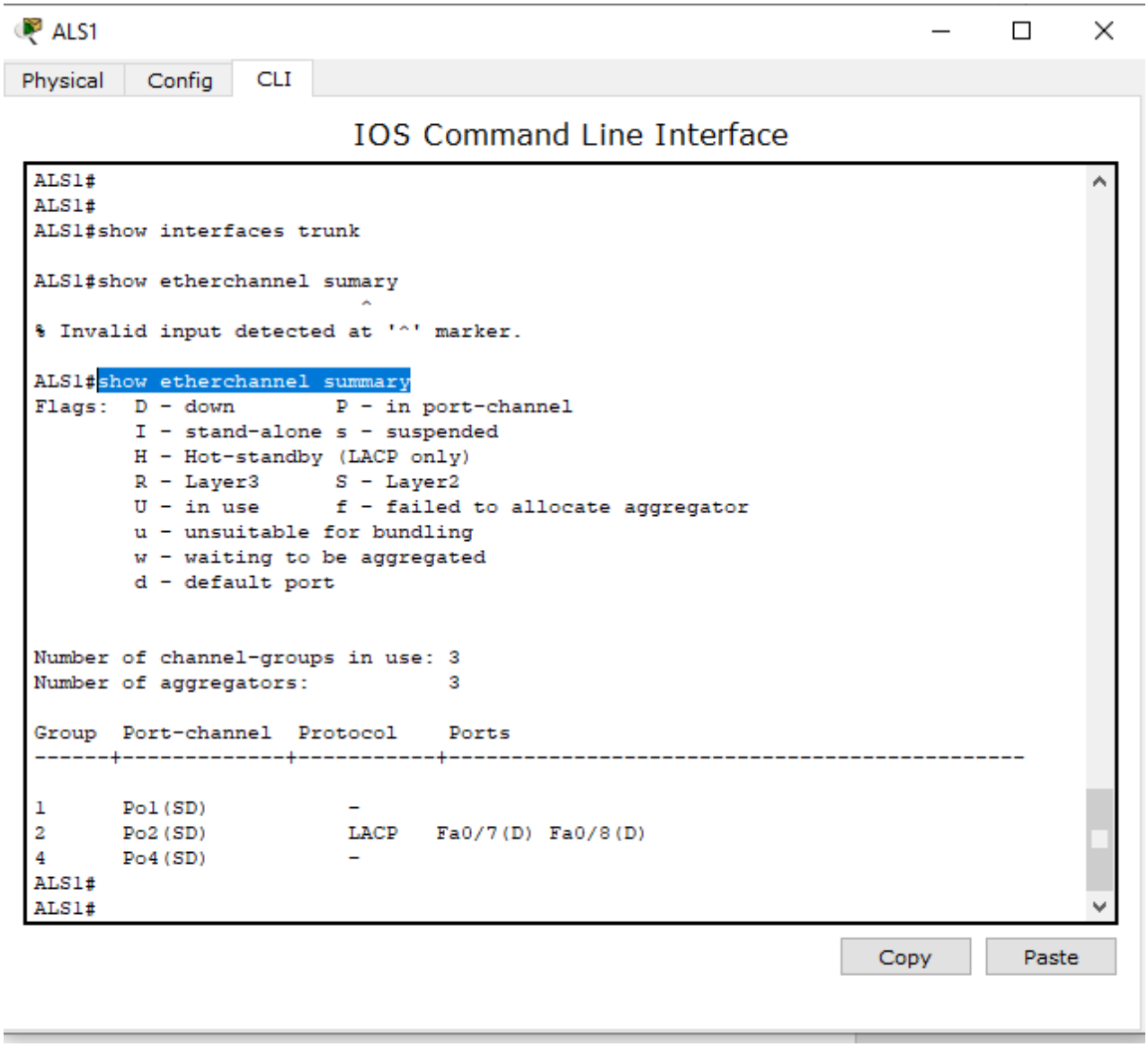
Figura 60. Aplicando código DLS1 EtherChannel



Se ejecuta comando show ethertchannel sumary en cada swicht para validar su configuracion correcta

ASL1# show ethertchannel summary

Figura 61. Aplicando código ASL1 EtherChannel



c. Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN.

Se ejecuta comando show Spanning tree en cada swicht solicitado para validar su configuracion correcta

ASL1# show Spanning-tree

Figura 62. Aplicando código DLS1 Spanning tree

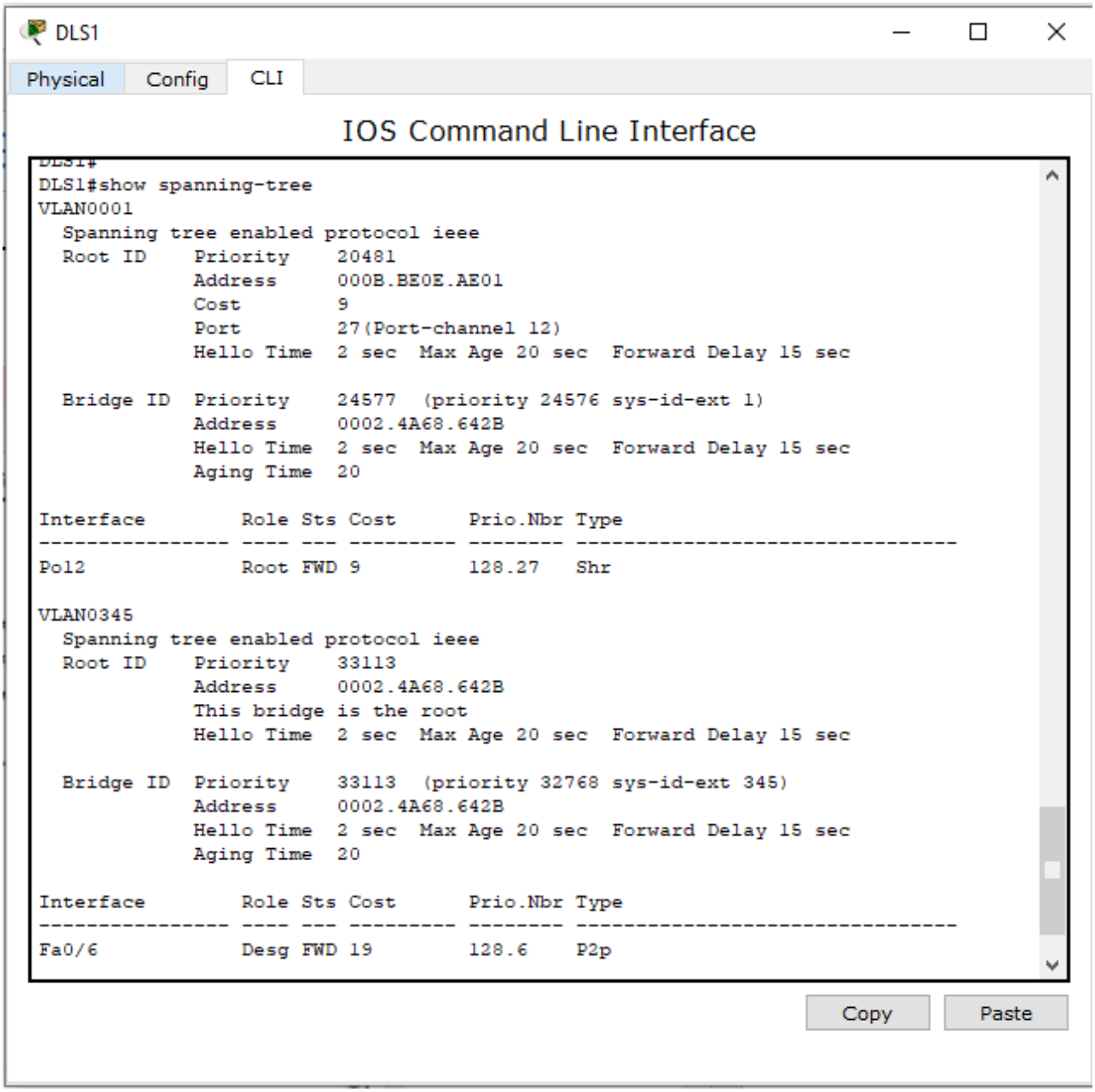
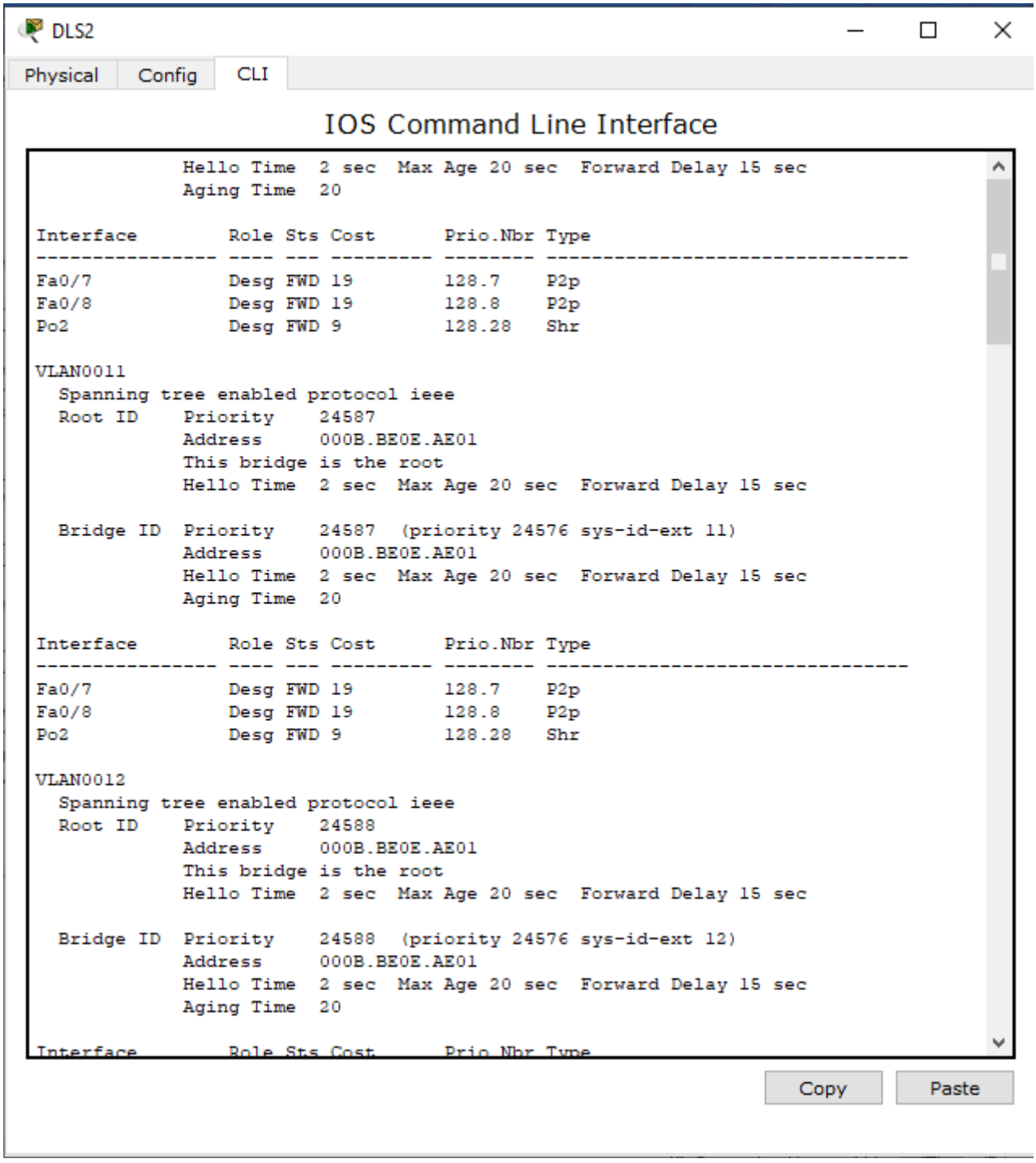


Figura 63. Aplicando código DLS2 Spanning tree



Se ejecuta comando show Spanning tree en cada swicht solicitado para validar su configuracion correcta

ASL1# show Spanning-tree

CONCLUSIONES

Por medio de este trabajo se permite comprender como se puede implementar y configurar una red que este soportada por Vlans con el uso de los protocolos VTP y STP, donde se pueda diseñar las plantillas de configuración para su uso en múltiples dispositivos, configurar troncales y vlans usando el protocolo VTP, los EtherChannel Link en red de switch interconectados, entro otros usos. El desarrollo de este trabajo permite reforzar los demás conocimientos adquiridos a través de la realización de los laboratorios durante el transcurso activo del curso y la solución de las lecciones evaluativas en el entorno de cisco (Netacad).

Para el escenario 1 Y 2 se aplicaron las configuraciones básicas y los protocolos de enrutamiento indicados, se crean interfaces loopback con asignación de direcciones, se implementan anchos de banda con tiempo de retardo de microsegundos, se verifican los resultados obtenidos por medio de los comandos show ip router.

Una red de grandes proporciones o también llamada WAN es muy propensa a redundancias entre conexiones de equipos también llamados bucles, lo que haría que la información rebote entre los equipos y nunca llegue a su destino, es por ello que el uso del protocolo STP Spanning Tree Protocol o Árbol de Expansión , protocolo que permite usar las conexiones e la difusión de mensajes a través de troncales por VLAN es una de las herramientas más efectivas para hacer llegar la información de manera segura.

El agilizar la respuesta entre redes y el tráfico en los equipos de la misma sobre una WAN es primordial para la eficacia de la red, por lo tanto protocolos como el OSPF y el EIGRP son necesarios para la identificación de cada router , así cada rotuer que comprende la red conocerá sus vecinos , las direcciones IP que tienen y la distancia de cada uno de estos , mejorando así la respuesta y comunicación entre los dispositivos de la red configurada.

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD z(2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm