DIPLOMADO DE PROFUNDIZACION CISCO CCNP
SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

Diana María Garzón Henao

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

PROGRAMA DE INGENIERIA DE TELECOMUNICACIONES

DIPLOMADO DE PROFUNDIZACION CISCO CCNP

MEDELLÍN

2021

DIPLOMADO DE PROFUNDIZACION CISCO CCNP
SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

Diana María Garzón Henao

Tutor

John Harold Pérez Calderón

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

PROGRAMA DE INGENIERIA DE TELECOMUNICACIONES

DIPLOMADO DE PROFUNDIZACION CISCO CCNP

MEDELLÍN

2021

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

MEDELLIN, 18 de Julio de 2021

TABLA DE CONTENIDO

LISTA DE TABLAS

TABLA DE FIGURAS

GLOSARIO

BGP: Border Gateway Protocol: Protocolo usado para intercambiar información entre sistemas autónomos y no autónomos.

EIGRP: Enhached Interior Gateway Routing Protocol: es un protocolo de encaminamiento de vector distancia, es considerado como protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

OSPF: Open Shortest Path First: el OSPF es un protocolo de puerta de enlace interior (IGP) y es normalmente utilizado en grandes redes empresariales. Es un protocolo de enrutamiento de estado de enlace que proporciona convergencia rápida y una escalabilidad excelente.

VLAN: Protocolo para crear redes lógicas, todas independientes dentro de una misma red.

VTP: VLAN Trunking Protocol: Es un protocolo de nivel 2 usado en VLANs para equipos de la marca CISCO y permite administrar las VLANs de todos los equipos desde uno solo.

RESUMEN

En este documento, se busca evidenciar el aprendizaje en clave de las competencias y habilidades adquiridas en el proceso del diplomado de profundización CCNP(Cisco Certified Networking Professional) mediante dos escenarios que se enfocaron en el diseño de la red que en cada escenario ocaso ésta variará, la conmutación y la escalabilidad; Estas se simularon con el apoyo del softwar packet tracer; que es un software de propiedad de CISCO, que posibilita vivenciar una experiencia cercana a la realidad a la hora de realizar una implementación de red y sus: componentes, configuraciones, prerrequisitos, topología diseño. Cabe aclarar que los casos utilizados para este proceso de aprendizaje son suposiciones que perfectamente se pueden vivenciar en la cotidianidad de nuestro que hacer como ingenieros; estos casos los nombraremos todo el tiempo como escenarios.

El primer escenario se realizaron configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5; se realizaron configuraciones de enrutamiento con los protocolos OSPF y EIGRP

El segundo escenario se debe configurar e interconectar cada uno de los dispositivos acorde con los lineamientos establecidos para el direccionamiento IP, etherchannels, VLANs y demás aspectos; este diseño tiene una redundancia para gargarizar que caso de una falla electrónica o desconexión física realice la conmutación a otro switch.

Palabras claves: CISCO, CCNP, conmutación, enrutamiento, redes, electrónica

ABSTRAC

This document seeks to demonstrate the key learning of the competencies and skills acquired in the process of the deepening diploma CCNP (Cisco Certified Networking Professional) through two scenarios that focused on the design of the network that in each scenario or case will vary , switching and scalability; These were simulated with the support of the war packet tracer software; which is a software owned by CISCO, which makes it possible to have an experience close to reality when carrying out a network implementation and its: components, configurations, prerequisites, design topology. It should be clarified that the cases used for this learning process are assumptions that can perfectly be experienced in our daily life as engineers; these cases we will name them all the time as scenarios.

The first scenario was made initial configurations and routing protocols for routers R1, R2, R3, R4, and R5; routing configurations are made with OSPF and EIGRP protocols

The second scenario must be configured and interconnected each of the devices according to the guidelines established for IP addressing, etherchannels, VLANs and other aspects; This design has redundancy to ensure that in the event of an electronic failure or physical disconnection, make the switch to another switch.

Keywords: CISCO, CCNP, switching, routing, networks, electronics

INTRODUCCION

En este proceso de aprendizaje donde me enriqueció en clave de habilidades y competencias en Networking; las cuales evidenciare en los siguientes dos escenario; donde se ponen a prueba los conocimientos y habilidades Networking en cisco como enrutamiento, OSPF, EIGRP, VLAN, VTP, Conectividad, Conmutación, Troubleshooting, entre otros. Cada escenario estará acompañado de los respectivos procesos y documentación correspondientes de la configuración de cada uno de los dispositivos, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, trace route, show ip route.

Para el primer escenario propuesto, debemos de conocer y aplicar los conceptos de OSPF, EIGRP y el código de programación de configuración de cada router de acuerdo con la funcionalidad de cada uno de ellos.

En ese escenario se plantea el desarrollo de la solución de los posibles problemas que se presentan en el networking, en los protocolos de enrutamiento de la configuración de sistemas avanzados en VLANs y en las medidas de seguridad que se dan en ellas; Esto se soluciona aplicando las siguientes configuraciones LACP y PAgP como modelo de agrupación; además, de los enlaces EthernetChannel y demás configuraciones que aseguren el correcto funcionamiento de la red a configurar.

A continuación, iniciare a evidenciar el proceso en el primer escenario:

Primer Escenario

Teniendo como referencia la siguiente imagen que nos indica una topología de red:

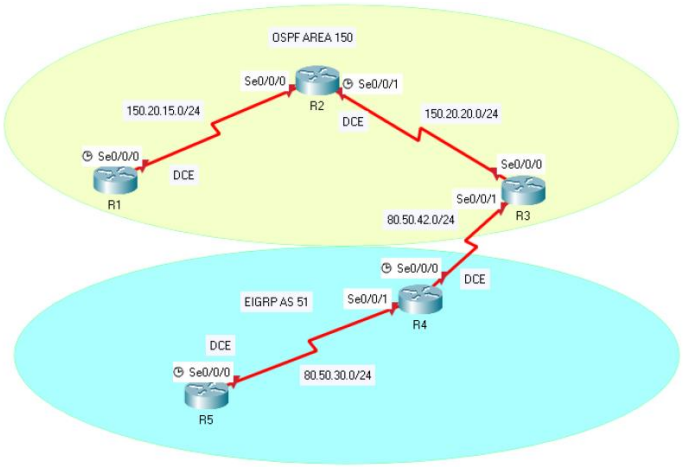

FIGURA 1. Topología de la red

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.
   Iniciamos la construcción de la interfaz usando el router 1941

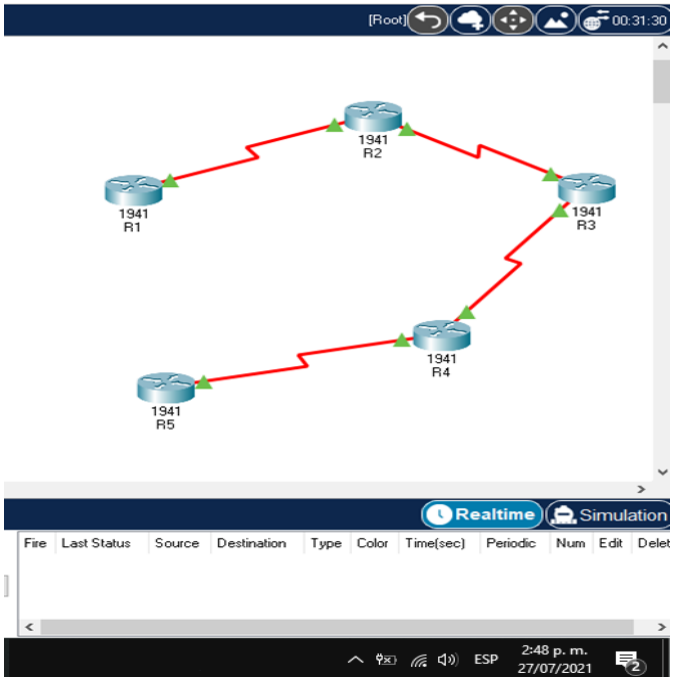

FIGURA 2.Topologia Packet Tracer

Y luego procedemos a configurar cada router:

Para R1:

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#interface s0/0/0
R1(config-if)#bandwidth 12800
R1(config-if)#ip address 150.20.15.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#network 150.20.15.0 0.0.0.255
R1(config-router)#end
R1#
```

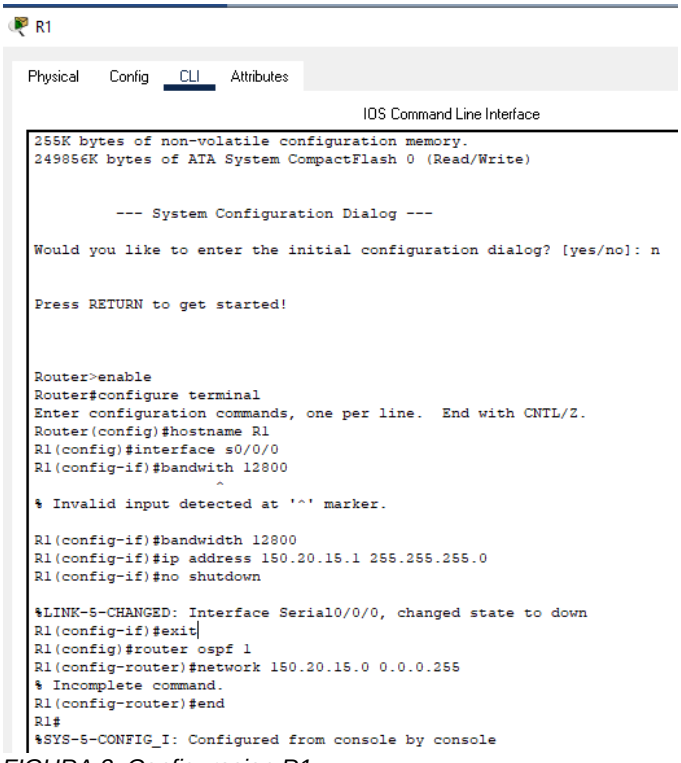

FIGURA 3. Configuracion R1

Para R2:

```
Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#interface s0/0/0
R2(config-if)#ip address 150.20.15.2 255.255.255.0
R2(config-if)#no shutdown
```

R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ip address 150.20.20.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#network 150.20.15.0 0.0.0.255 area 150
R2(config-router)#network 150.20.20.0 0.0.0.255 area 150
R2(config-router)#end

FIGURA 4. Configuración R2

Para R3:

Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#interface s0/0/0
R3(config-if)#ip address 150.20.20.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/0/1
R3(config-if)#ip address 80.50.42.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router ospf 1
R3(config-router)#network 150.20.15.0 0.0.0.255 area 150

R3(config-router)#exit
R3(config)#router eigrp 51
R3(config-router)#network 80.50.30.0 0.0.0.255
R3(config-router)#end
R3#

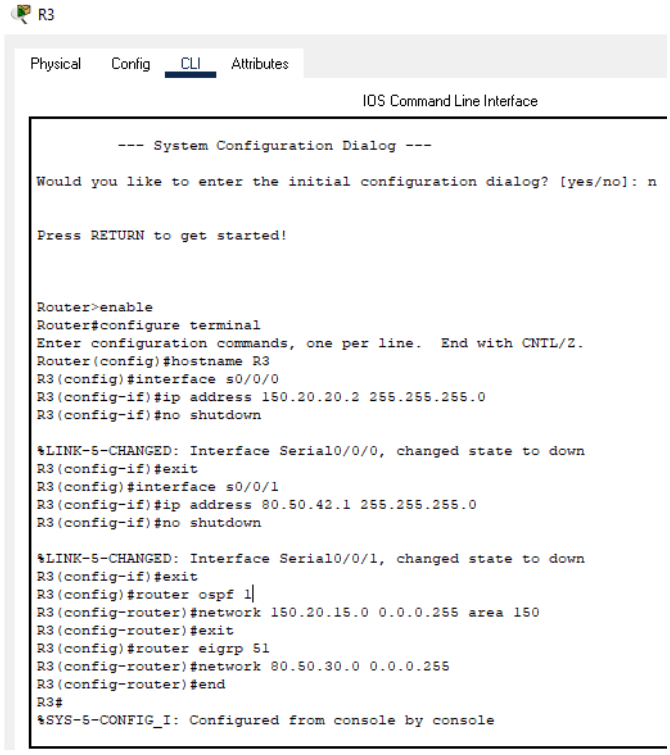

FIGURA 5. Configuración R3

Para R4:

Router>enable
Router#configure terminal
Router(config)#hostname R4
R4(config)#interface s0/0/0
R4(config-if)#ip address 80.50.42.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#interface s0/0/1
R4(config-if)#ip address 80.50.30.1 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router eigrp 51
R4(config-router)#network 80.50.30.0 0.0.0.255
R4(config-router)#network 80.50.42.0 0.0.0.255
R4(config-router)#end
R4#

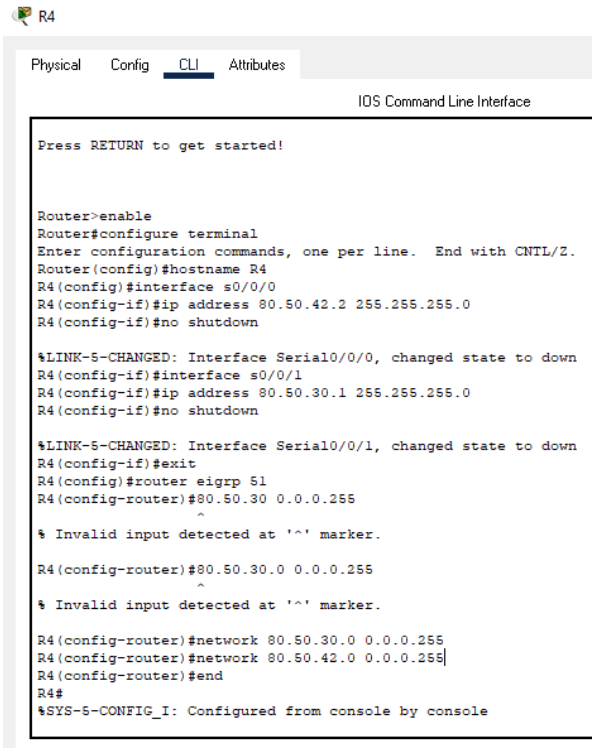

FIGURA 6. Configuración R4

Para R5:

Router>enable
Router#configure terminal
Router(config)#hostname R5
R5(config)#interface s0/0/0
R5(config-if)#bandwidth 12800
R5(config-if)#ip address 80.50.30.2 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#router eigrp 51
R5(config-router)#network 80.50.30.0 0.0.0.255
R5(config-router)#end
R5#

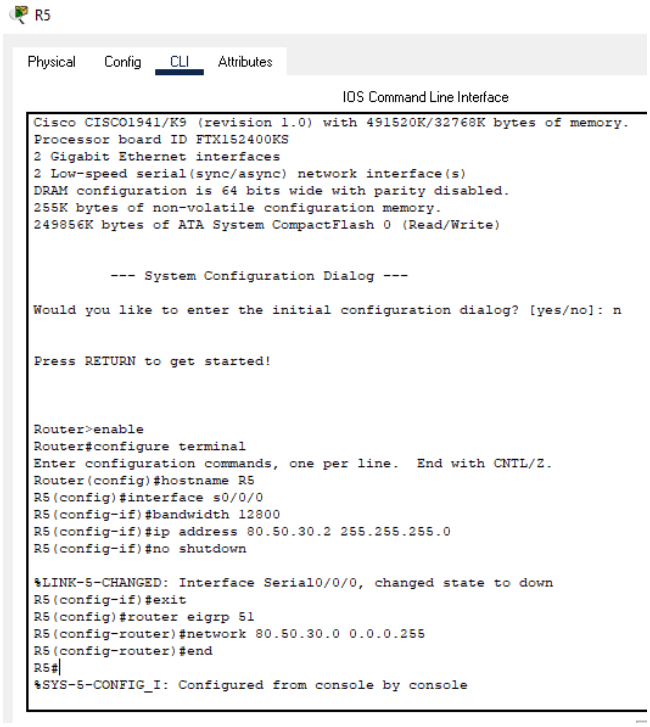

FIGURA 7 Configuración R5

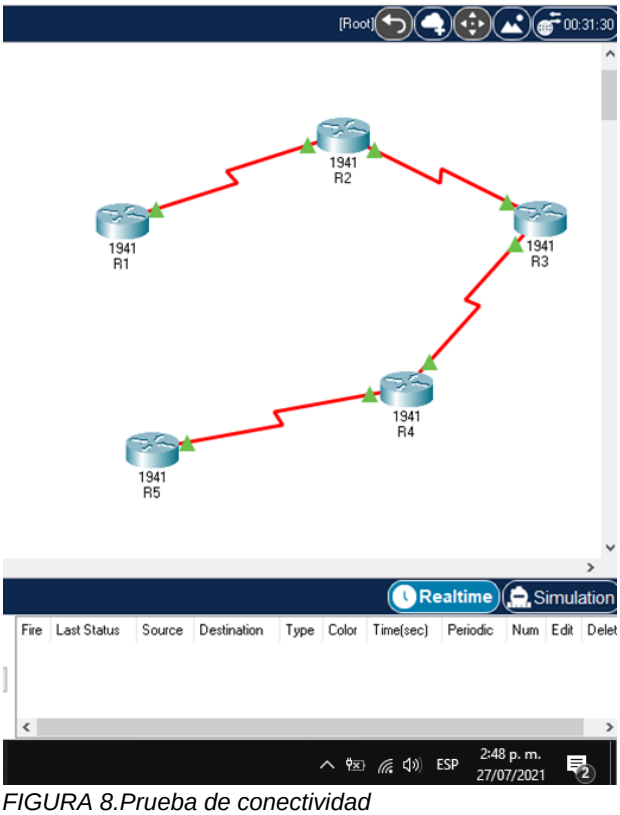

FIGURA 8.Prueba de conectividad

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 20.1.0.0/22 y configure esas interfaces para participar en el área 5 de OSPF.

```
R1>enable
R1#configure terminal
R1(config)#interface lo0
R1(config-if)#ip address 20.1.0.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface lo1
R1(config-if)#ip address 20.1.4.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface lo2
R1(config-if)#ip address 20.1.8.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface lo3
R1(config-if)#ip address 20.1.12.1 255.255.255.0
R1(config-if)#exit
R1(config)#router ospf 1
R1(config-router)#network 150.20.15.0 0.0.0.255 area 5
R1(config-router)#network 150.20.20.0 0.0.0.255 area 5
R1(config-router)#end
R1#
```

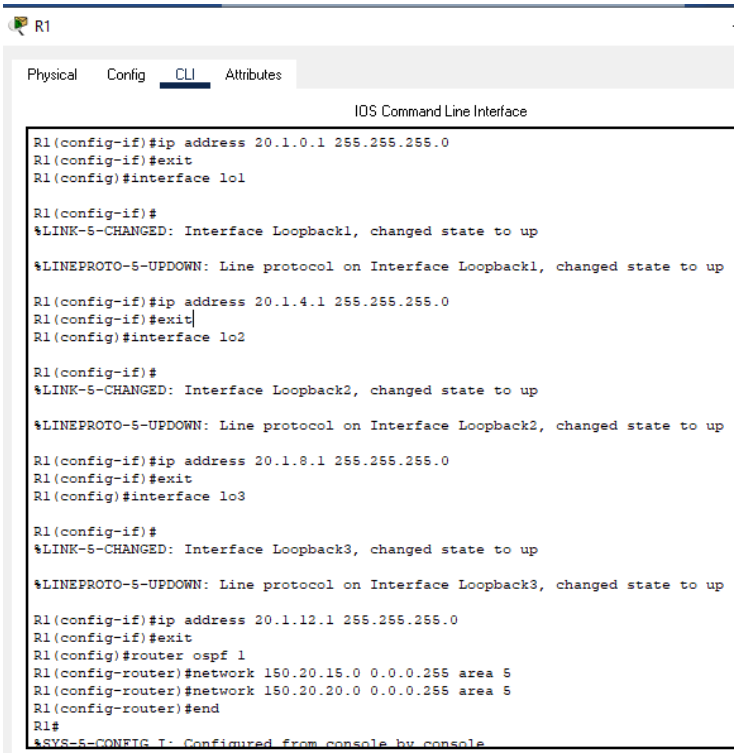

FIGURA 9. Loopback en R1

TABLA 1.Loopback IP address

# Loopback	IP address
Loopback 0	20.1.0.1
Loopback 1	20..1.4.1
Loopback 2	20.1.8.1
Loopback 3	20.1.12.1

3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 180.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 51.

```
R5>enable
R5#configure terminal
R5(config)#in lo0
R5(config-if)#ip address 180.5.0.1 255.255.252.0
R5(config-if)#exit
R5(config)#in lo1
R5(config-if)#ip address 180.5.4.1 255.255.252.0
R5(config-if)#exit
R5(config)#in lo2
R5(config-if)#ip address 180.5.8.1 255.255.252.0
R5(config-if)#exit
R5(config)#in lo3
R5(config-if)#ip address 180.5.12.1 255.255.252.0
R5(config-if)#exit
R5(config)#router eigrp 51
R5(config-router)#auto-summary
R5(config-router)#network 180.5.0.0 0.0.3.255
R5(config-router)#network 80.50.30.0 0.0.0.255
R5(config-router)#end
R5#
```

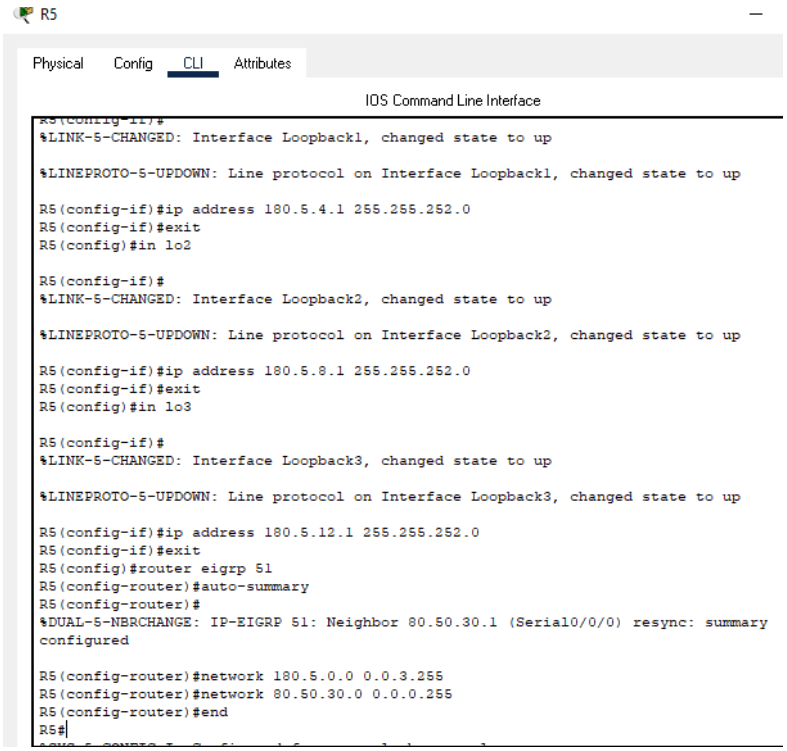

FIGURA 10. Loopback en R5

TABLA 2. Loopback IP address

# Loopback	IP address
Loopback 0	180.5.0.1
Loopback 1	180.5.4.1
Loopback 2	180.5.8.1
Loopback 3	180.5.12.1

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.

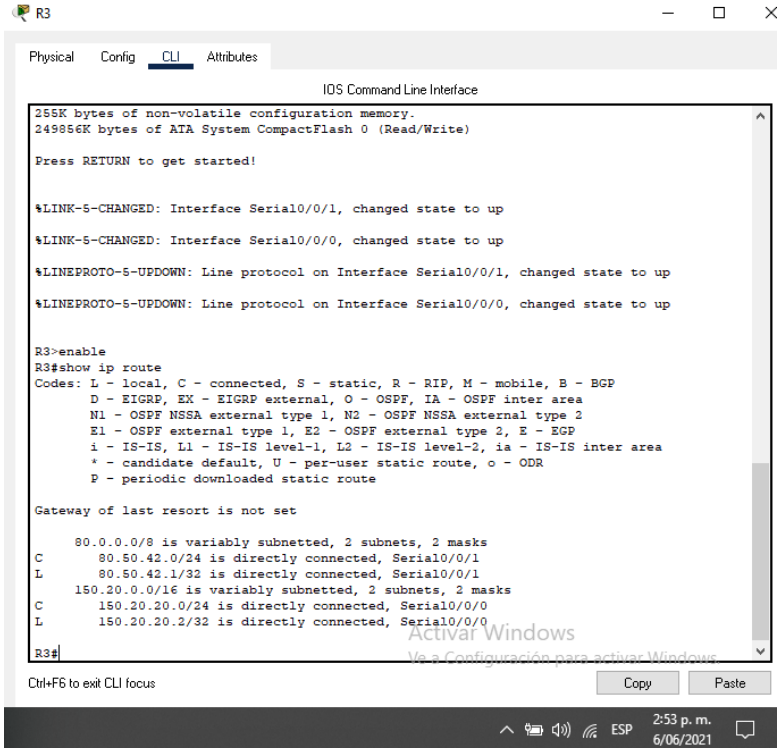

FIGURA 11. Enrutamiento de R3

Podemos observar que efectivamente R3 aprendió las interfaces loobpack

5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 80000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 50,000 microsegundos de retardo.

```
R3>enable
R3#configure terminal
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 51 metric 80000 subnets
R3(config-router)#exit
R3(config)#router eigrp 51
R3(config-router)#redistribute ospf 1 metric 1544 50000 255 1 1500
R3(config-router)#exit
R3(config)#end
R3#
```

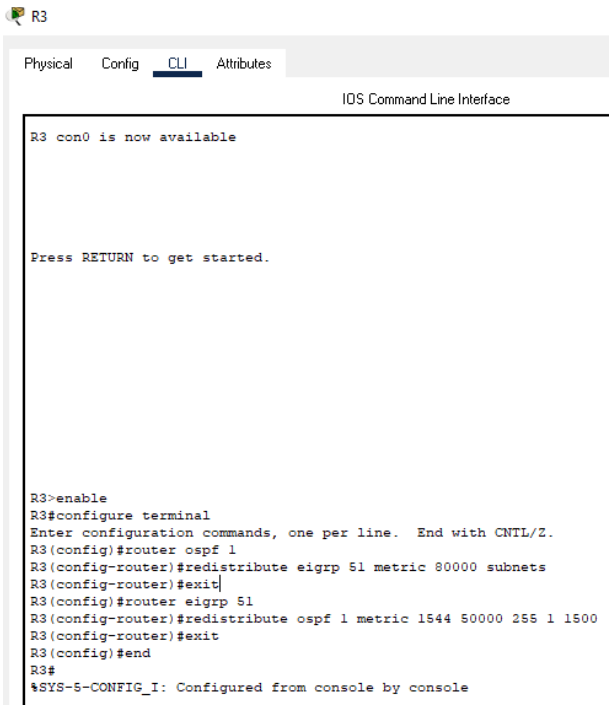

FIGURA 12. Rutas EIGRP en OSPF R3

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***.

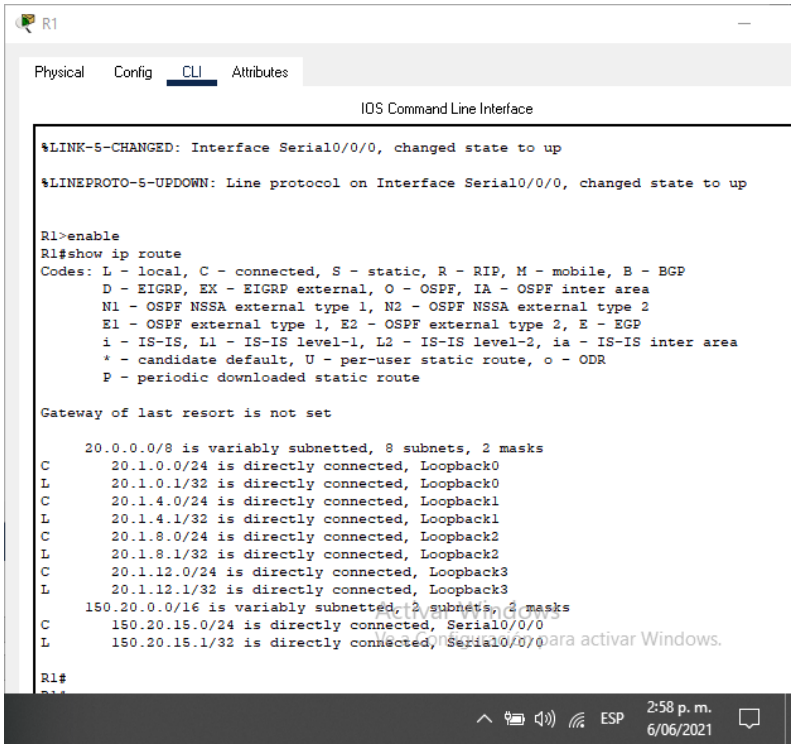

FIGURA 13. Rutas del sistema autónomo R1

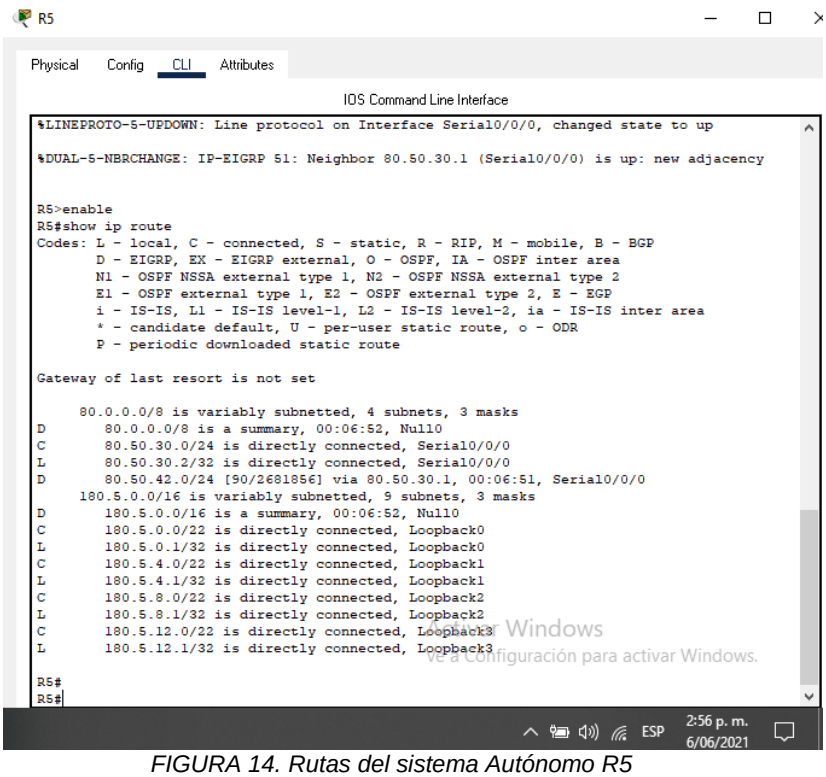

FIGURA 14. Rutas del sistema Autónomo R5

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.

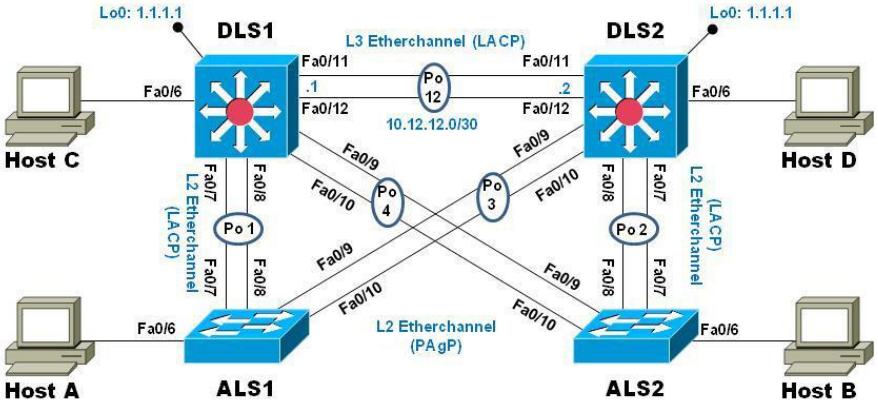

FIGURA 15. Topología de la red

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

a. Apagar todas las interfaces en cada switch

Replicamos el siguiente código en DLS1, DLS2, ALS1 y ALS2

```
Switch>enable
Switch#configure terminal
Switch(config)#int ran f0/1-24, g0/1-2
Switch(config-if-range)#shutdown
```

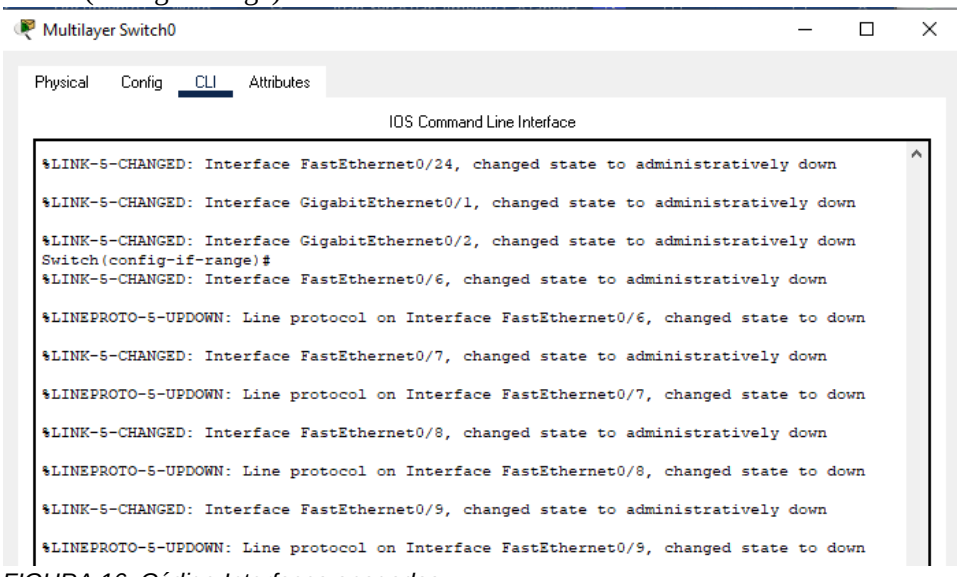

FIGURA 16. Código Interfaces apagadas

Verificamos que todas las interfaces estén apagadas

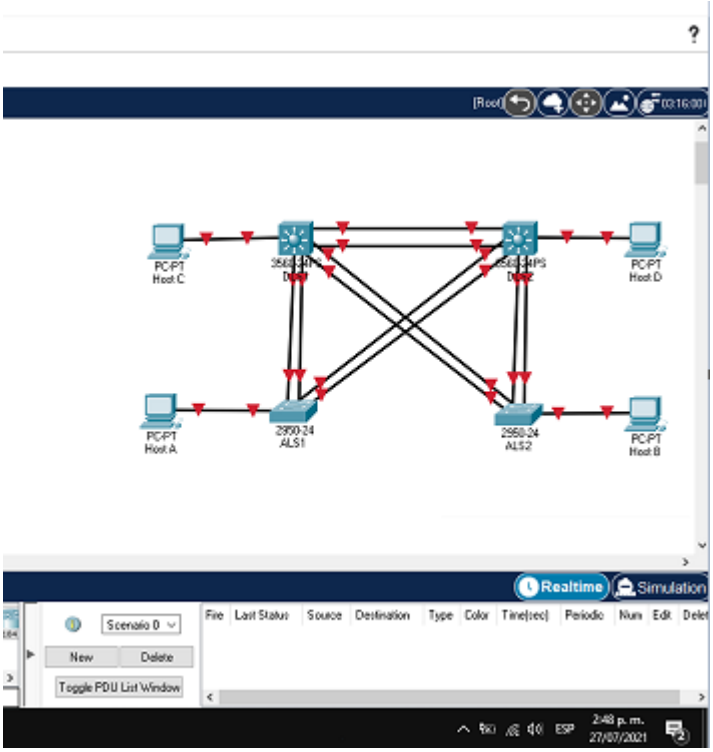

FIGURA 17. Interfaces apagadas

b. Asignar un nombre a cada switch acorde con el escenario establecido.
Para DLS1

Switch#enable
Switch#configure terminal
Switch(config)#hostname DLS1
DLS1(config)#

Para DLS2
Switch#enable
Switch#configure terminal
Switch(config)#hostname DLS2
DLS2(config)#

Para ALS1
Switch#enable
Switch#configure terminal
Switch(config)#hostname ALS1
ALS1(config)#

Para ALS2
Switch#enable

Switch#configure terminal
Switch(config)#hostname ALS2
ALS2(config)#

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 10.20.20.1/30 y para DLS2 utilizará 10.20.20.2/30.

Para DLS1
DLS1>enable
DLS1#configure terminal
DLS1(config)#interface port-channel 12
DLS1(config-if)#no switchport
DLS1(config-if)#ip address 10.20.20.1 255.255.255.252
DLS1(config-if)#exit
DLS1(config)#interface ran fa0/11-12
DLS1(config-if-range)#no switchport
DLS1(config-if-range)#channel-group 12 mode active
DLS1(config-if-range)#no shutdown
DLS1(config-if-range)#exit

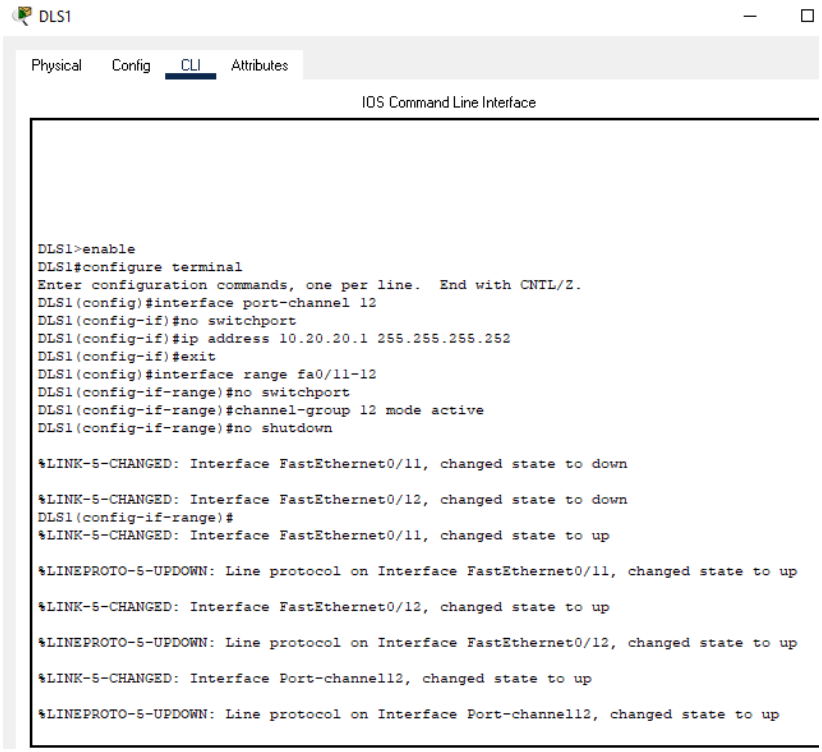

FIGURA 18. conexión entre DLS1 y DLS2 usando LACP en DLS1

Para DLS2

DLS2>enable
DLS2#configure terminal
DLS2(config)#interface port-channel 12
DLS2(config-if)#no switchport
DLS2(config-if)#ip address 10.20.20.1 255.255.255.252
DLS2(config-if)#exit
DLS2(config)#interface ran fa0/11-12
DLS2(config-if-range)#no switchport
DLS2(config-if-range)#channel-group 12 mode active
DLS2(config-if-range)#no shutdown
DLS2(config-if-range)#exit

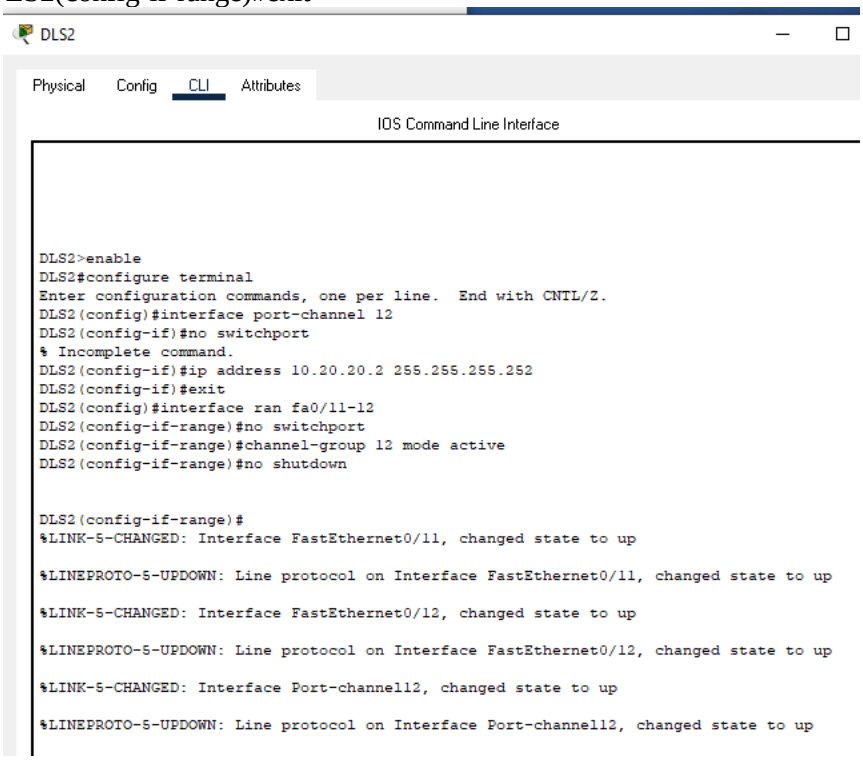

FIGURA 19. conexión entre DLS1 y DLS2 usando LACP en DLS2

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

Para DLS1

DLS1>enable
DLS1#configure terminal
DLS1(config)#interface ran fastethernet 0/7-8
DLS1(config-if-range)#channel-protocol lacp
DLS1(config-if-range)#channel-group 2 mode active
DLS1(config-if-range)#
DLS1(config-if-range)#no shutdown
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

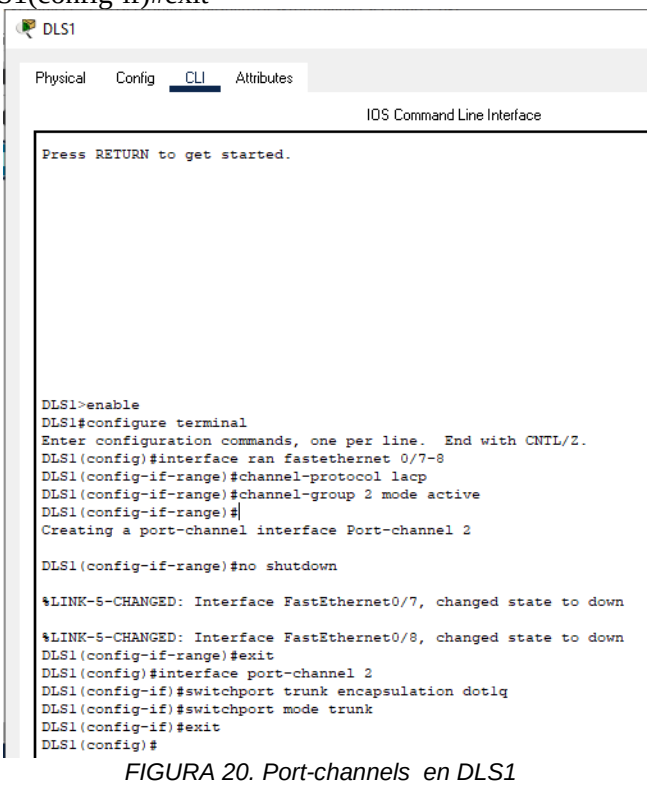

FIGURA 20. Port-channels en DLS1

Para DLS2

DLS2>enable
DLS2#configure terminal
DLS2(config)#interface ran fastethernet 0/7-8
DLS2(config-if-range)#channel-protocol lacp
DLS2(config-if-range)#channel-group 2 mode active
DLS2(config-if-range)#
DLS2(config-if-range)#no shutdown
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

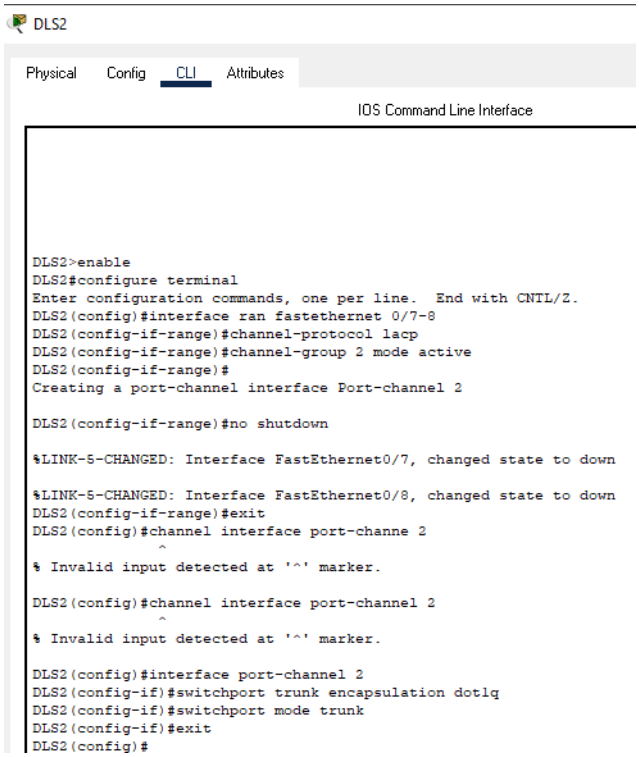

FIGURA 21. Port-channels en DLS2

Para ALS1

ALS1>enable
ALS1#configure terminal
ALS1(config)#interface ran fastethernet 0/7-8
ALS1(config-if-range)#channel-protocol lacp
ALS1(config-if-range)#channel-group 2 mode active
ALS1(config-if-range)#no shutdown
ALS1(config-if-range)#exit
ALS1(config)#interface port-channel 2
ALS1(config-if)#switchport mode trunk
ALS1(config-if)#exit

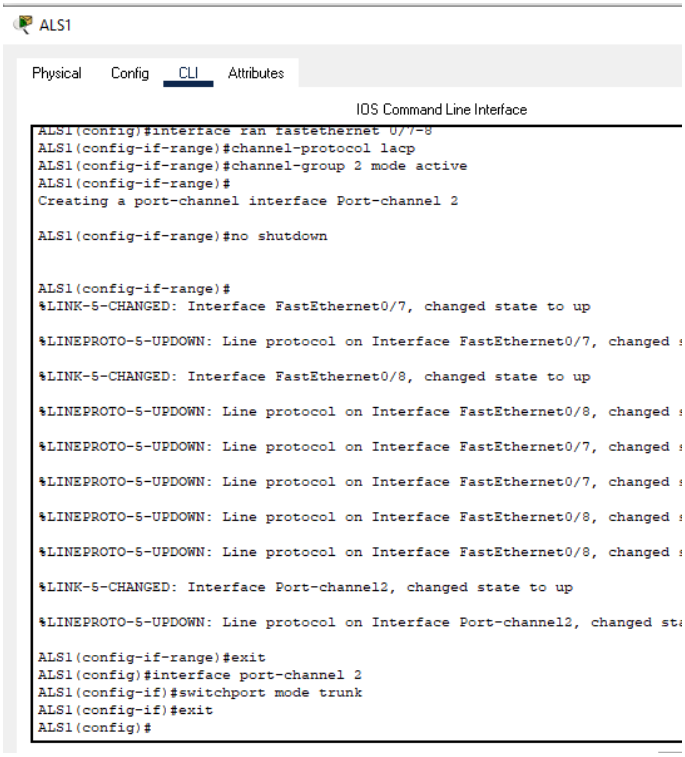

FIGURA 22. Port-channels en ALS1

Para ALS2

ALS2>enable
ALS2#configure terminal
ALS2(config)#interface ran fastethernet 0/7-8
ALS2(config-if-range)#channel-protocol lacp
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#no shutdown
ALS2(config-if-range)#exit
ALS2(config)#interface port-channel 2
ALS2(config-if)#switchport mode trunk
ALS2(config-if)#exit

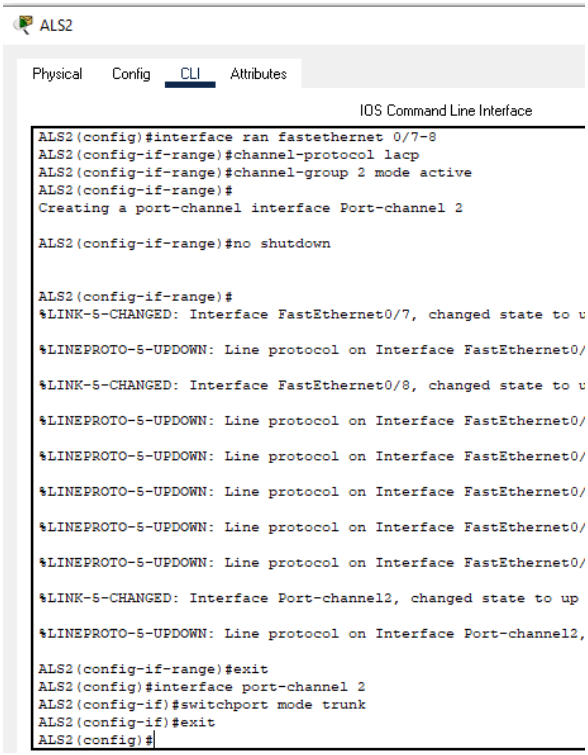

FIGURA 23. Port-channels en ALS2

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

Para DLS1

DLS1>enable
DLS1#configure terminal
DLS1(config)#int ran 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)#no shutdown

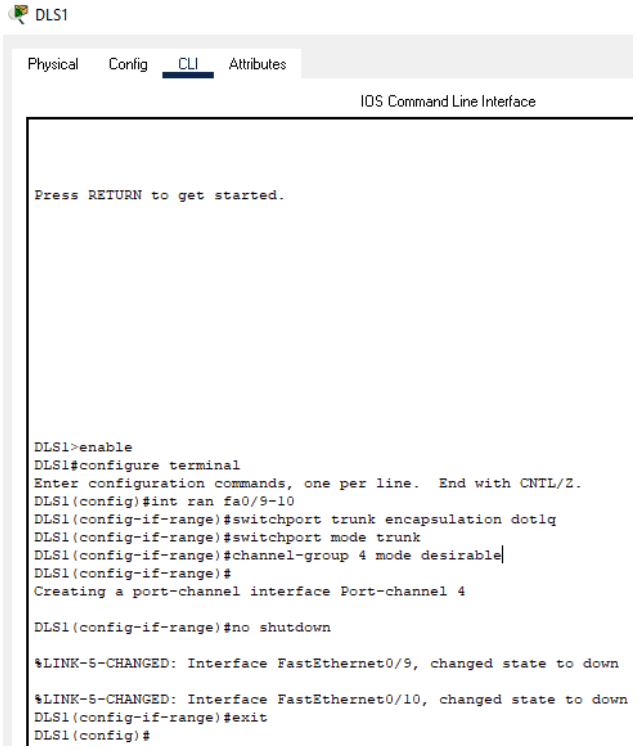

FIGURA 24. PAgP en DSL1

Para DLS2

DLS2>enable
DLS2#configure terminal
DLS2(config)#int ran fa0/9-10
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 4 mode desirable
DLS2(config-if-range)#no shutdown

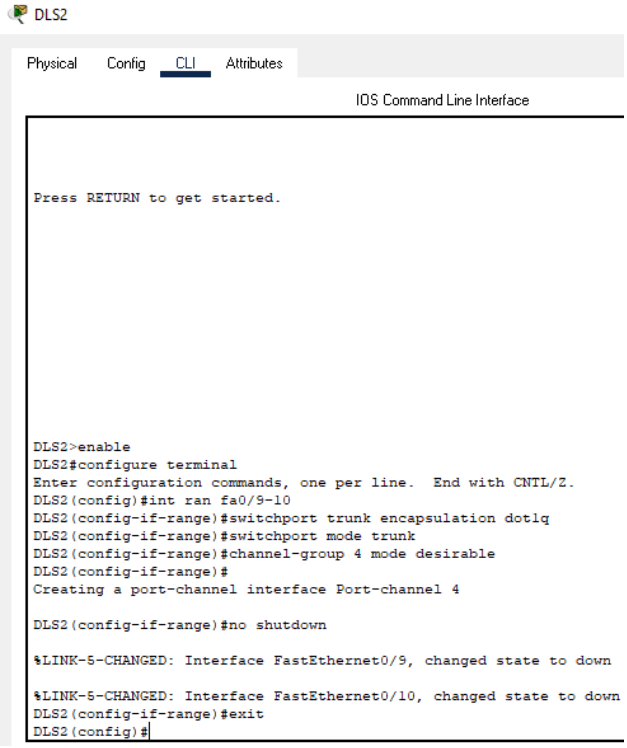

FIGURA 25. PAgP en DSL2

Para ALS1

ALS1>enable
ALS1#configure terminal
ALS1(config)#int ran fa0/9-10
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 4 mode desirable
ALS1(config-if-range)#no shutdown

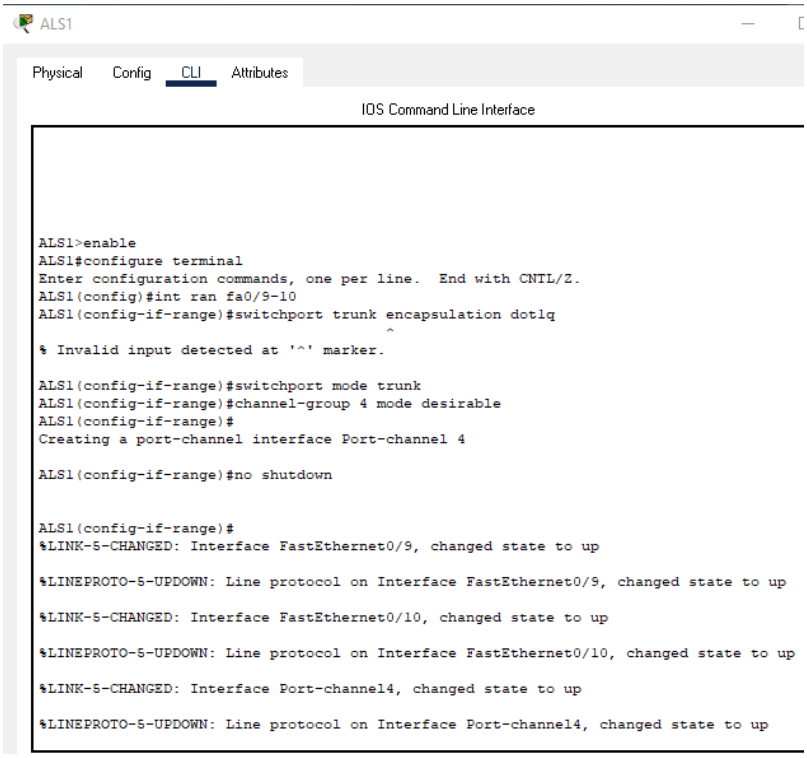

FIGURA 26. PAgP en ASL1

Para ALS2

ALS2>enable
ALS2#configure terminal
ALS2(config)#int ran fa0/9-10
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#no shutdown

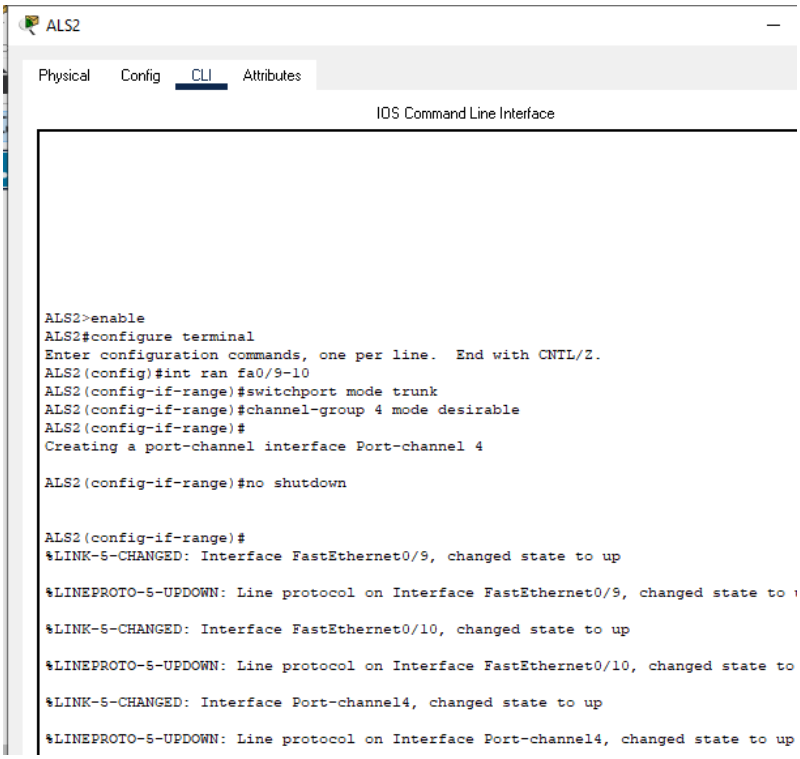

FIGURA 27. PAgP en ASL2

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

```
DLS1>enable
DLS1#configure terminal
DLS1(config)#interface Po1
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#exit
DLS1(config)#interface Po4
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#
```

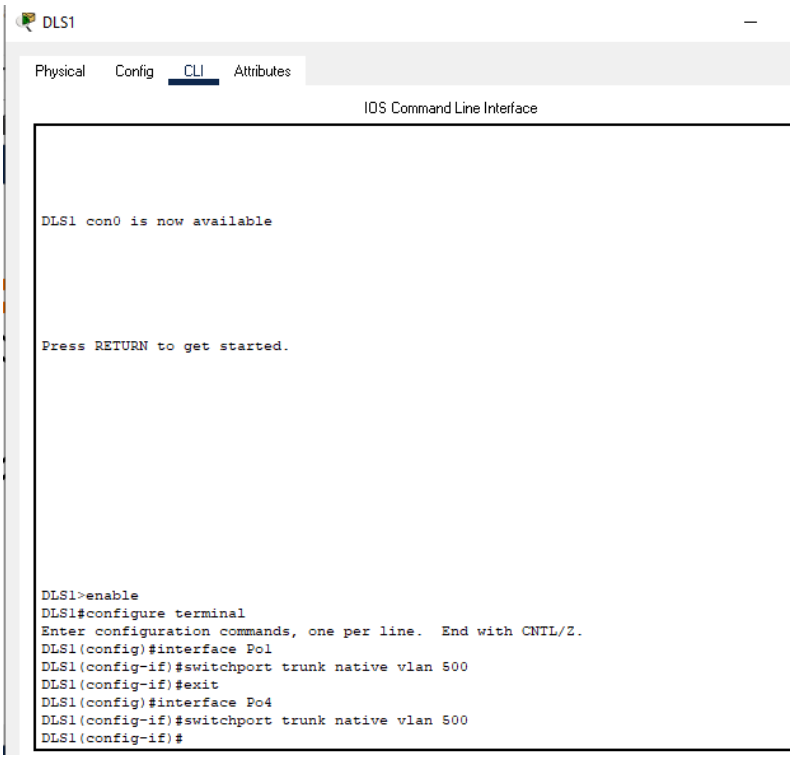

FIGURA 28. Puertos troncales VLAN 500 en DLS1

Para DLS2

DLS2>enable
DLS2#configure terminal
DLS2(config)#interface Po2
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#exit
DLS2(config)#interface Po3
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#

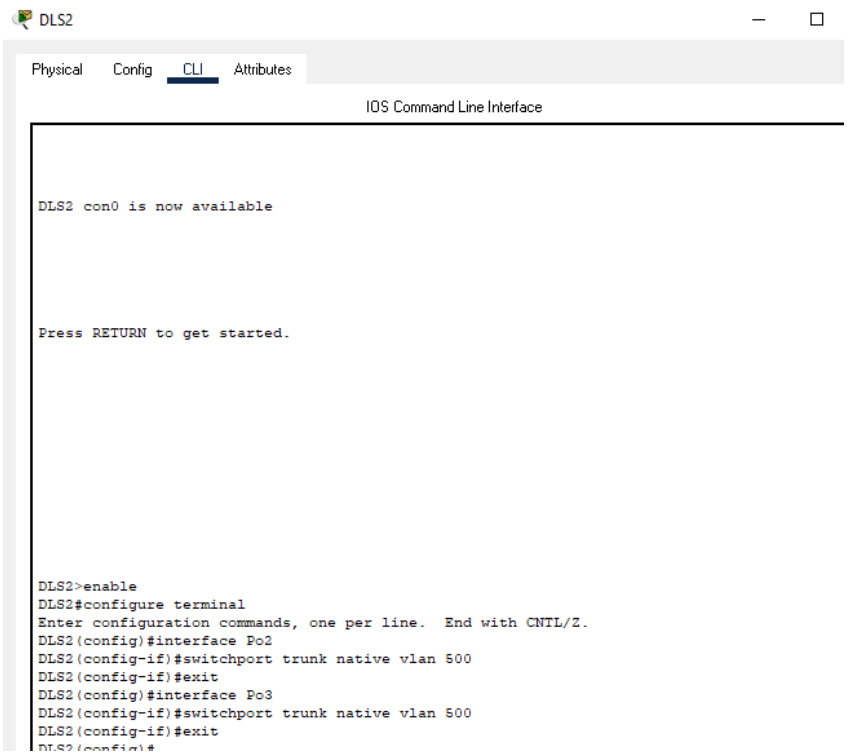

FIGURA 29. Puertos troncales VLAN 500 en DLS2

Para ALS1

ALS1>enable
ALS1#configure terminal
ALS1(config)#interface Po1
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#exit
ALS1(config)#interface Po4
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#

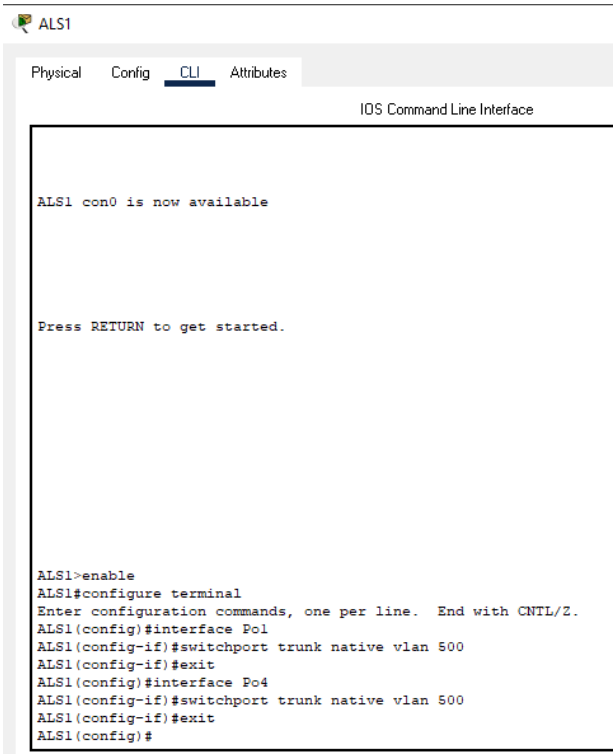

FIGURA 30. Puertos troncales VLAN 500 en ALS1

Para ALS2

ALS2>enable
ALS2#configure terminal
ALS2(config)#interface Po2
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#exit
ALS2(config)#interface Po3
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#

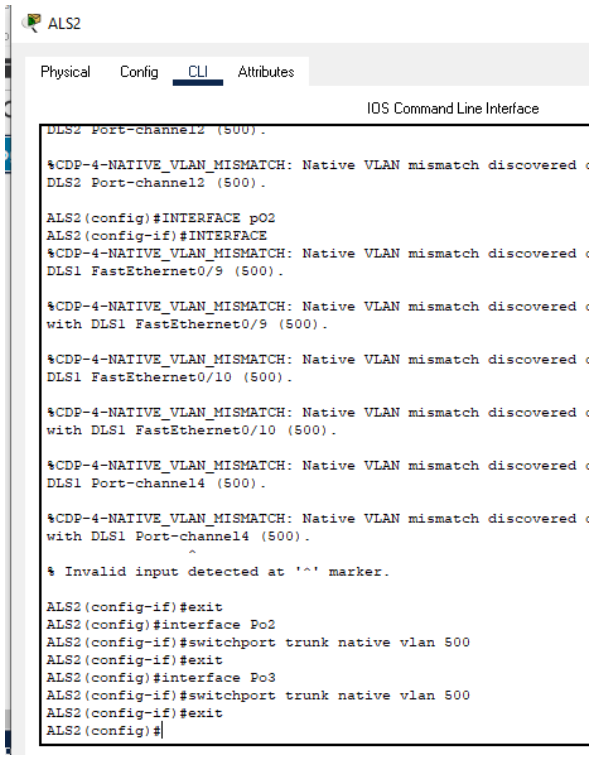

FIGURA 31. Puertos troncales VLAN 500 en ALS2

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

Nota:
Esta configuración que se pide realizar en el programa Packet tracer, no es posible ya que no soporta la versión 3; mediante el comando “show vtp status” se evidencia que es compatible con la versión 2 de VTP por lo que se ejecuta en la versión 2.

1. Utilizar el nombre de dominio *CISCO* con la contraseña *ccnp321*

```
DLS1>enable
DLS1#configure terminal
DLS1(config)#vtp domain CISCO
DLS1(config)#vtp pass ccnp321
DLS1(config)#vtp version 2
```

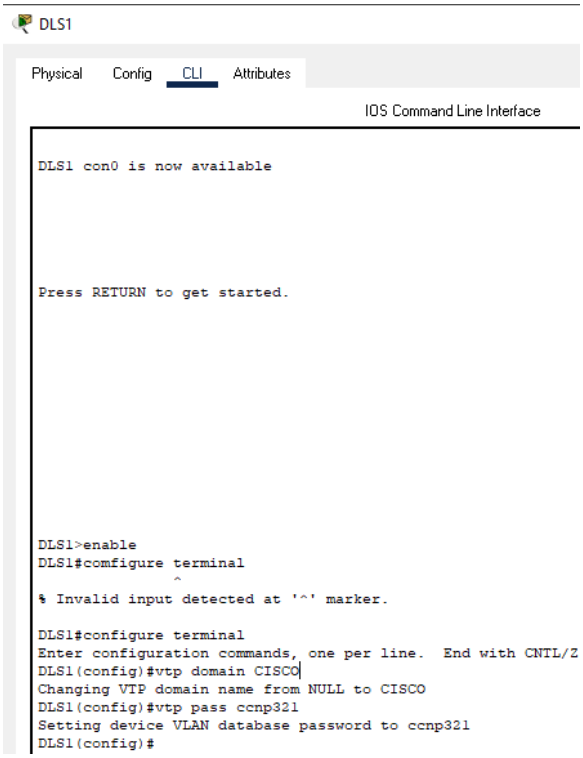

FIGURA 32. Configuración dominio CISCO y contraseña

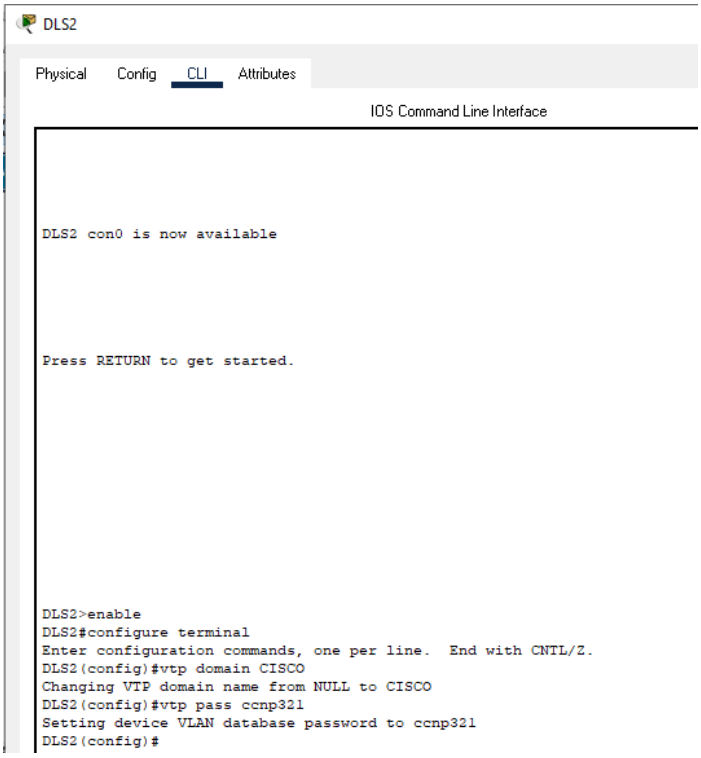

FIGURA 33. DLS1 como servidor principal

2. Configurar DLS1 como servidor principal para las VLAN.

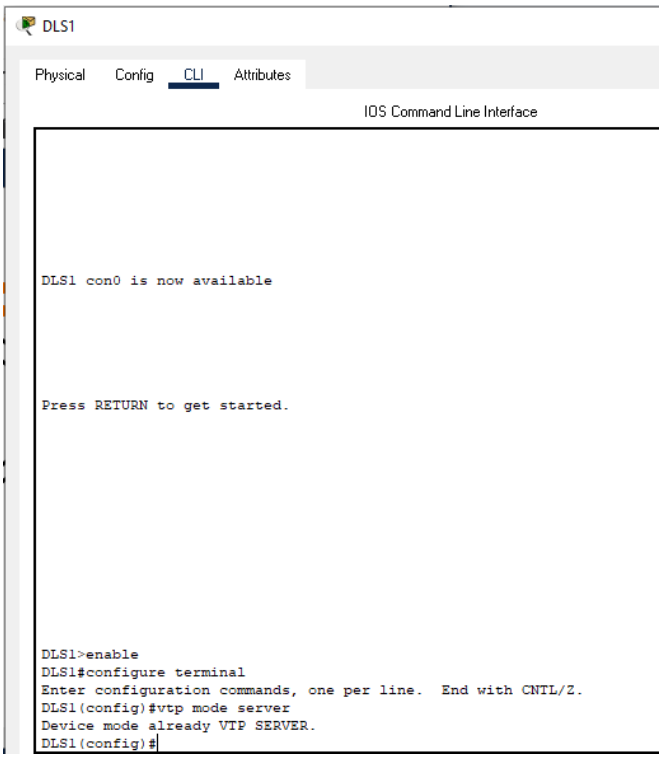

FIGURA 34. DLS1 como servidor principal

3. Configurar ALS1 y ALS2 como clientes VTP.

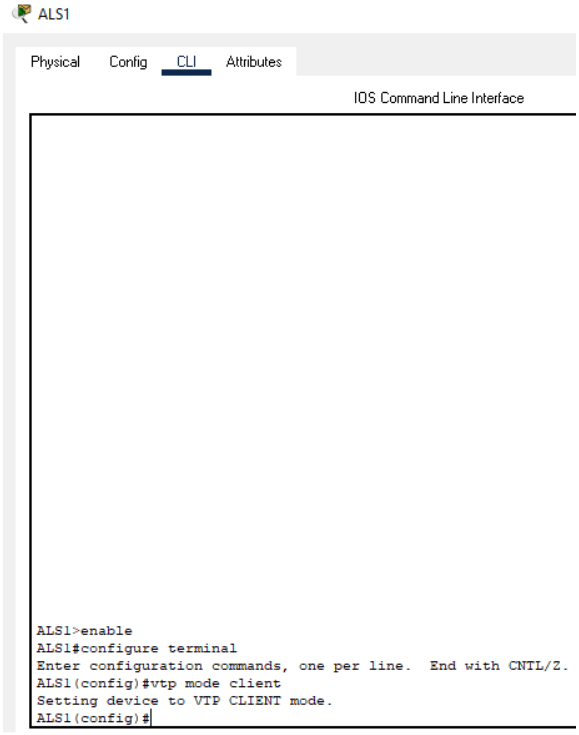

FIGURA 35. ALS1 como cliente VTP

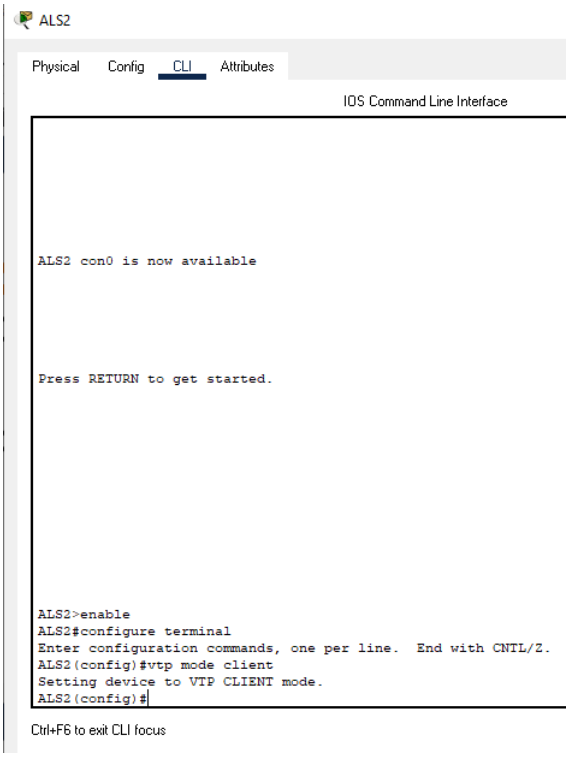

FIGURA 36. ALS2 como cliente VTP

e. Configurar en el servidor principal las siguientes VLAN:

Tabla 3. VLAN

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
600	NATIVA	420	PROVEEDORES
15	ADMON	100	SEGUROS
240	CLIENTES	105	VENTAS
111	MULTIMEDIA	355	PERSONAL

Aplicamos el código en DSL 1

```
DLS1(config)#VLAN 600
DLS1(config-vlan)#NAME NATIVA
DLS1(config-vlan)#VLAN 15
DLS1(config-vlan)#NAME ADMON
DLS1(config-vlan)#VLAN 240
DLS1(config-vlan)#NAME CLIENTES
DLS1(config-vlan)#VLAN 420
DLS1(config-vlan)#NAME PROVEEDORES
DLS1(config)#VLAN 600
DLS1(config-vlan)#NAME NATIVA
DLS1(config-vlan)#VLAN 15
DLS1(config-vlan)#NAME ADMON
DLS1(config-vlan)#VLAN 240
DLS1(config-vlan)#NAME CLIENTES
DLS1(config-vlan)#VLAN 420
DLS1(config-vlan)#NAME PROVEEDORES
```

Nota:

El switch elegido (3560), en las VLAN se identifican con un ID entre 1 y 1005, para las VLAN entre 1006 y 4094, las cuales son de rango extendido que se usan para redes Token Ring; por lo cual ajustamos las VLAN para que sean de rango ordinario, por lo tanto; MULTIMEDIA VLAN 111, VENTAS VLAN 105, PERSONAL VLAN 355

f. En DLS1, suspender la VLAN 420.

Usamos el siguiente código en DSL1

```
DLS1(config)#vlan 420
DLS1(config-vlan)#no vlan 420
DLS1(config)#
```

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

Usamos el código

```
DLS2(config)#vtp mode transparent
DLS2(config)#VLAN 600
DLS2(config-vlan)#NAME NATIVA
DLS2(config-vlan)#VLAN 15
DLS2(config-vlan)#NAME ADMON
DLS2(config-vlan)#VLAN 240
DLS2(config-vlan)#NAME CLIENTES
DLS2(config-vlan)#VLAN 111
DLS2(config-vlan)#NAME MULTIMEDIA
DLS2(config-vlan)#VLAN 420
DLS2(config-vlan)#NAME PROVEEDORES
DLS2(config-vlan)#VLAN 100
DLS2(config-vlan)#NAME SEGUROS
DLS2(config-vlan)#VLAN 105
DLS2(config-vlan)#NAME VENTAS
DLS2(config-vlan)#VLAN 355
DLS2(config-vlan)#NAME PERSONAL
```

h. Suspender VLAN 420 en DLS2.

Usamos el siguiente código en DSL2

```
DLS1(config)#vlan 420
DLS2(config-vlan)#no vlan 420
DLS2(config)#
```

i. 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.

```
DLS2>enable
DLS2#configure terminal
DLS2(config)#interface port-channel 2
DLS2(config-if)#switchport trunk allowed vlan except 567
DLS2(config-if)#exit
DLS2(config)#int port-channel 3
DLS2(config-if)#switchport trunk allowed vlan except 567
DLS2(config-if)#exit
DLS2(config)#vlan 567
DLS2(config-vlan)#NAME PRODUCCION
DLS2(config-vlan)#EXIT
DLS2(config)#
```

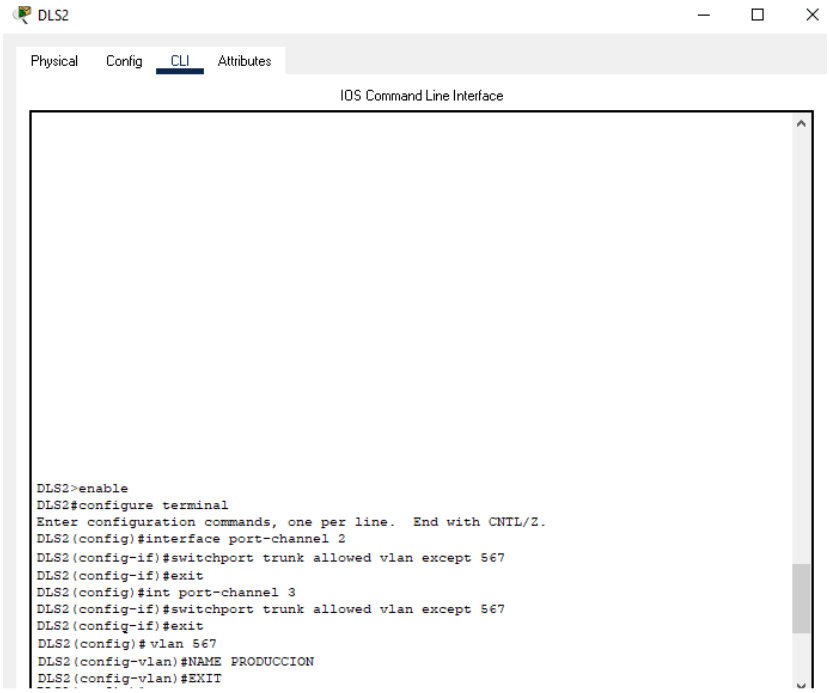

FIGURA 37. Creación VLAN 567

j. Configurar DLS1 como Spanning tree root para las VLANs 1, 12, 420, 600, 1050, 1112 y 3550 y como raíz secundaria para las VLAN 100 y 240.

Usamos el siguiente código

DLS1>enable
DLS1#configure terminal
DLS1(config)#spanning-tree vlan 1,12,420,600,105,111,355 root primary
DLS1(config)#spanning-tree vlan 100,240 root secondary

FIGURA 38. DLS1 como Spanning tree root

k. Configurar DLS2 como Spanning tree root para las VLAN 100 y 240 y como una raíz secundaria para las VLAN 15, 420, 600, 1050, 11112 y 3550.

Aplicamos el siguiente código

DLS2#configure terminal
DLS2(config)#spanning-tree vlan 100,240 root primary
DLS2(config)#spanning-tree vlan 1,12,420,600,105,111,355 root secondary
DLS2(config)#

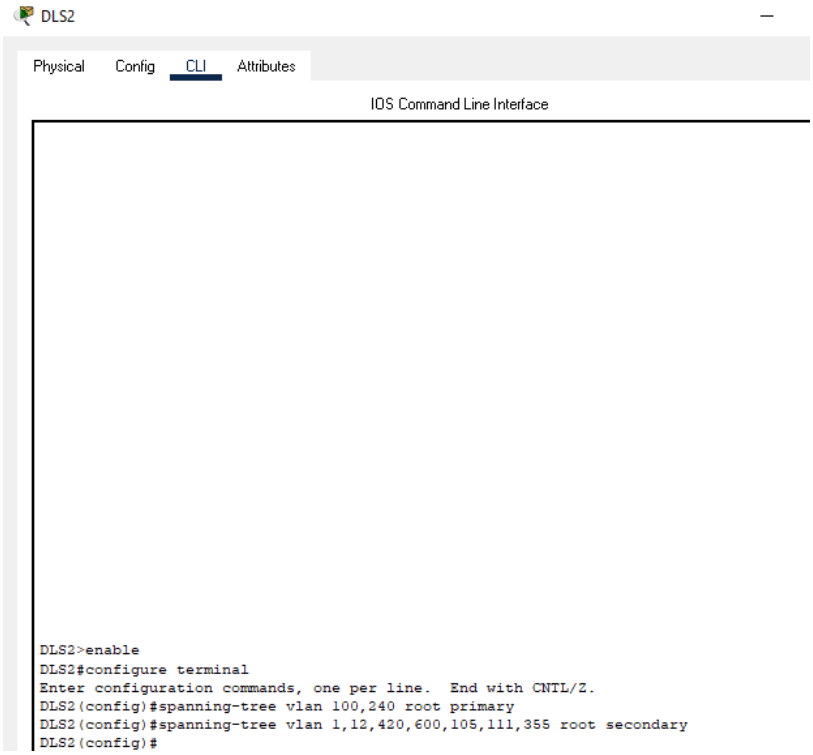

FIGURA 39. DLS2 como Spanning tree root

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

Aplicamos el siguiente código

```
DLS1>enable
DLS1#configure terminal
DLS1(config)#interface port-channel 1
DLS1(config-if)#switchport trunk allowed vlan 1,12,420,600,105,111,355
DLS1(config-if)#exit
DLS1(config)#interface port-channel 4
DLS1(config-if)#switchport trunk allowed vlan 1,12,420,600,105,111,355
DLS1(config-if)#exit
```

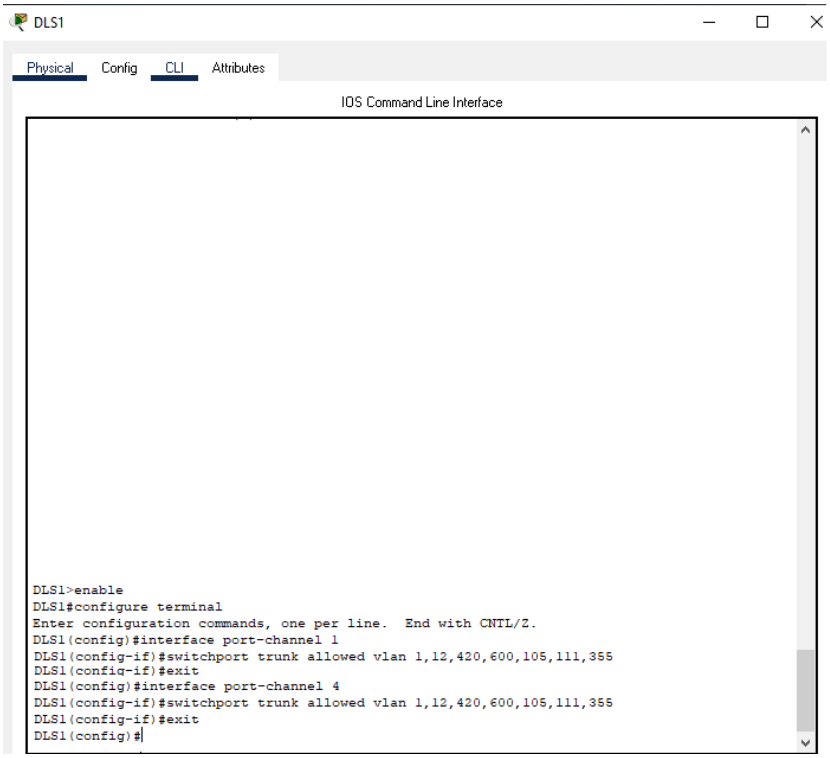

FIGURA 40. configuración de puertos troncales DLS1

Para DLS2

DLS2>enable
DLS2#configure terminal
DLS2(config)#interface port-channel 1
DLS2(config-if)#switchport trunk allowed vlan 1,12,420,600,105,111,355
DLS2(config-if)#exit
DLS2(config)#interface port-channel 4
DLS2(config-if)#switchport trunk allowed vlan 1,12,420,600,105,111,355
DLS2(config-if)#exit

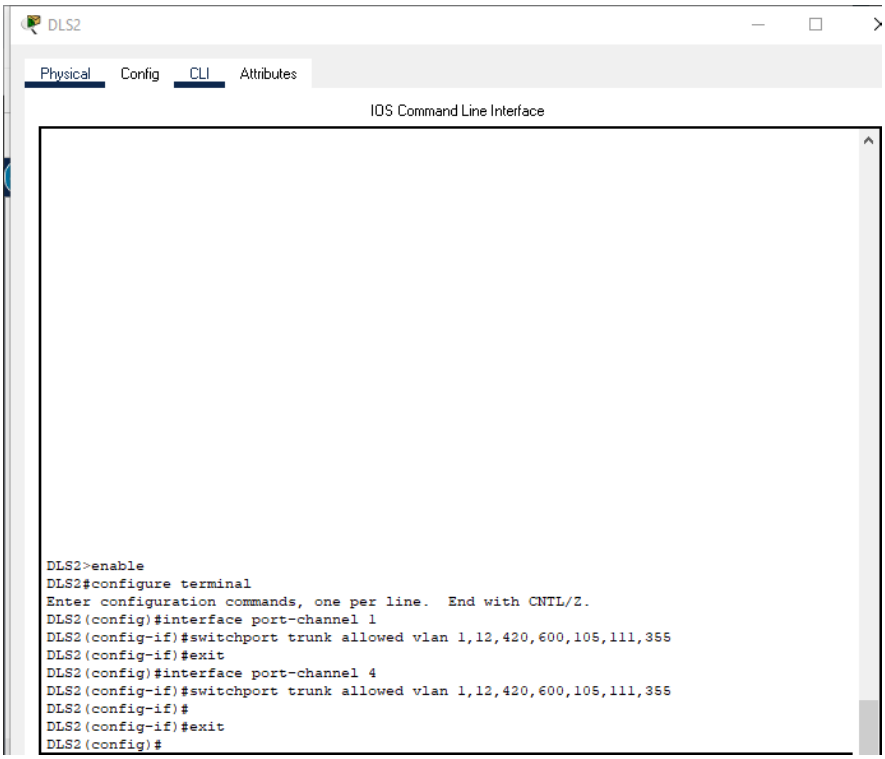

FIGURA 41. configuración de puertos troncales DLS2

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

Tabla 4. Puertos de accesos.

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3550	15, 1050	100, 1050	240
Interfaz Fa0/15	1112	1112	1112	1112
Interfaces F0 /16-18		567		

Aplicamos el siguiente código para DLS1

DLS1>enable
DLS1#configure terminal
DLS1(config)#interface f0/6
DLS1(config-if)#switchport mode acces
DLS1(config-if)#switchport Access vlan 355
DLS1(config-if)#no shutdown
DLS1(config-if)#interface f0/15

DLS1(config-if)#switchport mode Access
DLS1(config-if)#switchport Access vlan 111
DLS1(config-if)#no shutdown

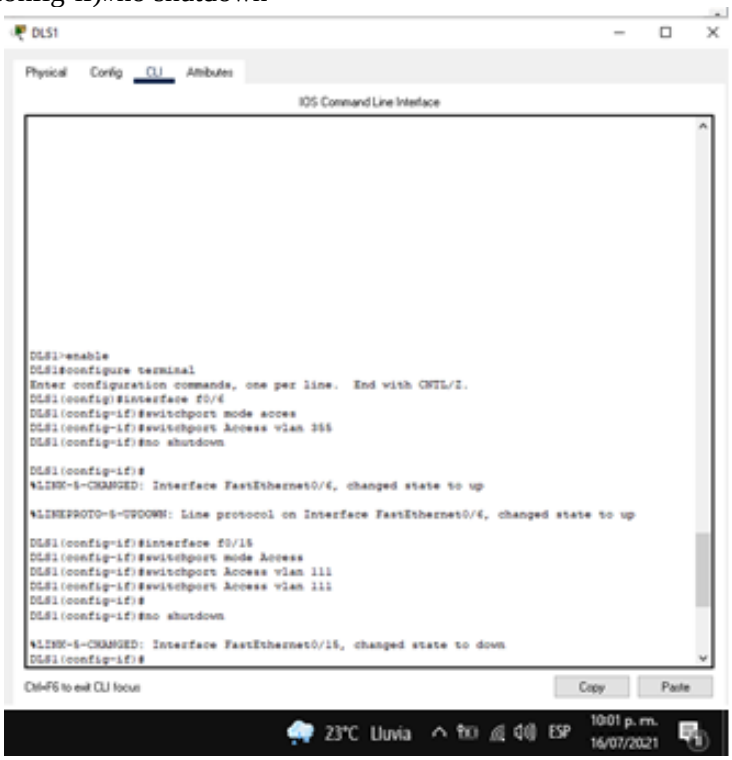

FIGURA 42. configuración de interfaces para DLS1

Aplicamos el siguiente codigo para DLS2

DLS2>enable
DLS2#configure terminal
DLS2(config)#interface f0/6
DLS2(config-if)#switchport mode acces
DLS2(config-if)#switchport Access vlan 15
DLS2(config-if)#no shutdown
DLS2(config-if)#switchport Access vlan 105
DLS2(config-if)#no shutdown
DLS2(config-if)#interface f0/15
DLS2(config-if)#switchport mode Access
DLS2(config-if)#switchport Access vlan 111
DLS2(config-if)#no shutdown
DLS2(config-if)#switchport mode Access
DLS2(config-if)#interface ran f0/16-18
DLS2(config-if)#switchport Access vlan 567
DLS2(config-if)#no shutdown

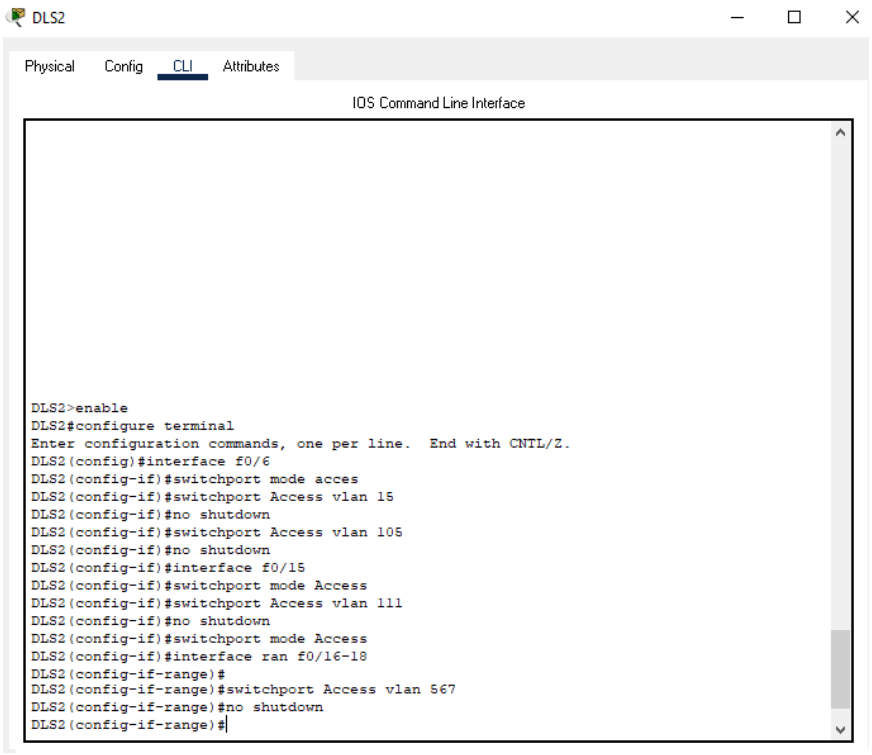

FIGURA 43. configuración de interfaces para DLS2

Aplicamos el siguiente código para ALS1

ALS1>enable
ALS1#configure terminal
ALS1(config)#interface f0/6
ALS1(config-if)#switchport mode acces
ALS1(config-if)#switchport Access vlan 100
ALS1(config-if)#no shutdown
ALS1(config-if)#switchport Access vlan 105
ALS1(config-if)#no shutdown
ALS1(config-if)#interface f0/15
ALS1(config-if)#switchport mode Access
ALS1(config-if)#switchport Access vlan 111
ALS1(config-if)#no shutdown

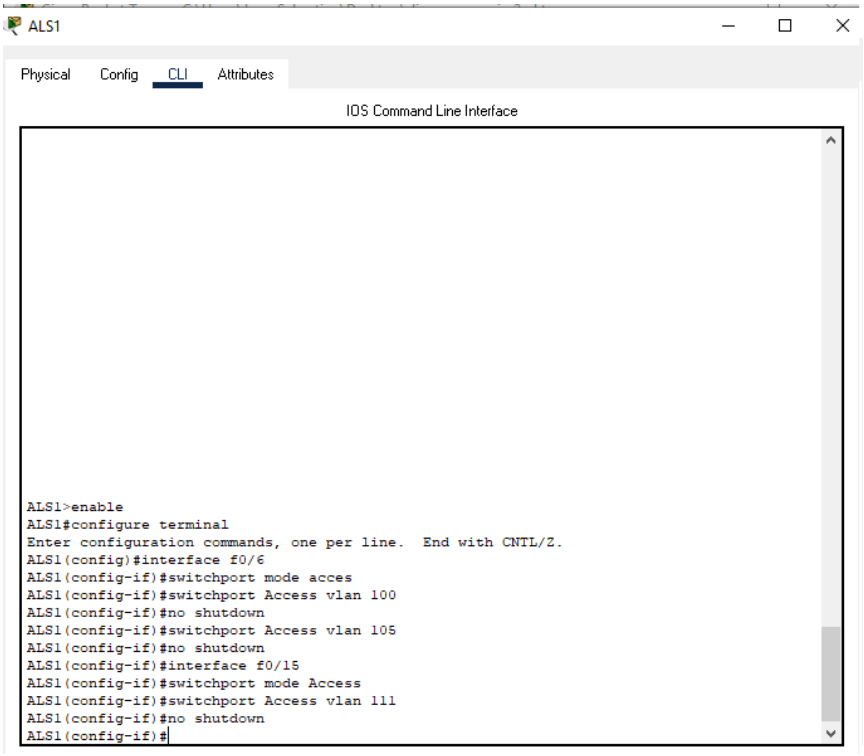

FIGURA 44. configuración de interfaces para ALS1

Para ALS2

ALS2>enable
ALS2#configure terminal
ALS2(config)#interface f0/6
ALS2(config-if)#switchport mode acces
ALS2(config-if)#switchport Access vlan 240
ALS2(config-if)#no shutdown
ALS2(config-if)#interface f0/15
ALS2(config-if)#switchport mode Access
ALS2(config-if)#switchport Access vlan 111
ALS2(config-if)#no shutdown

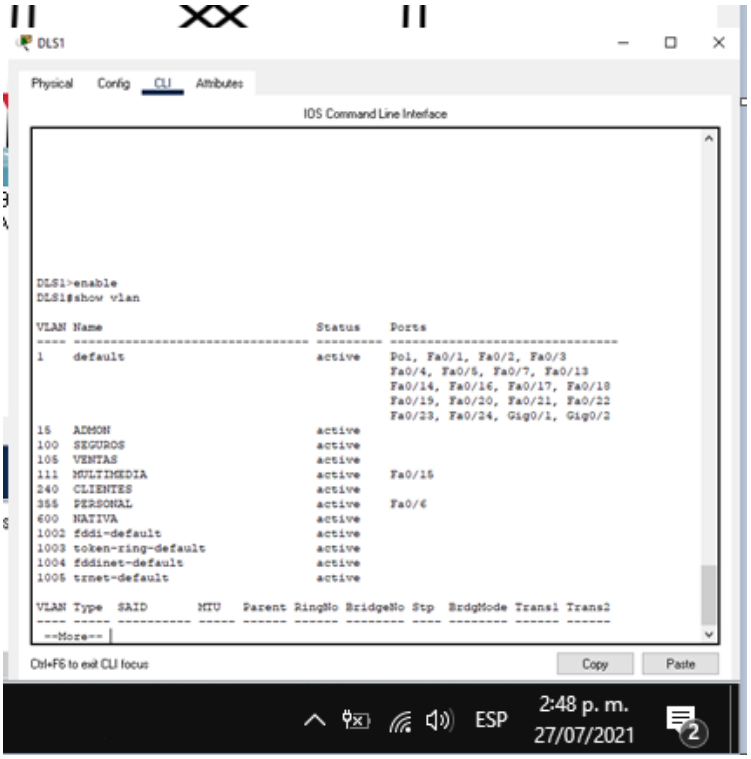

FIGURA 45. configuración de interfaces para ALS2

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

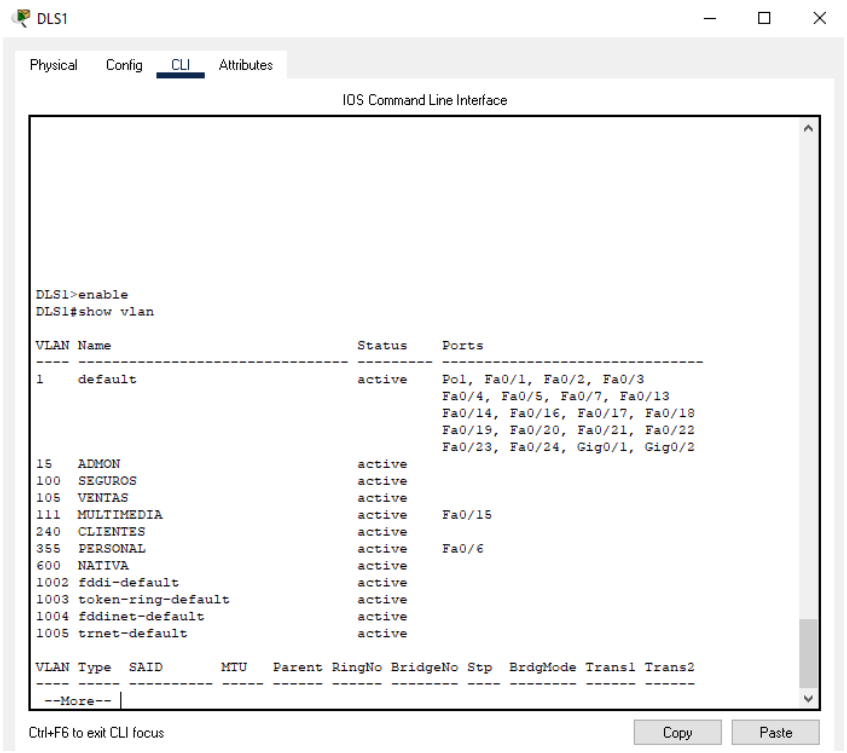

FIGURA 46. Verificación de VLAN para DLS1

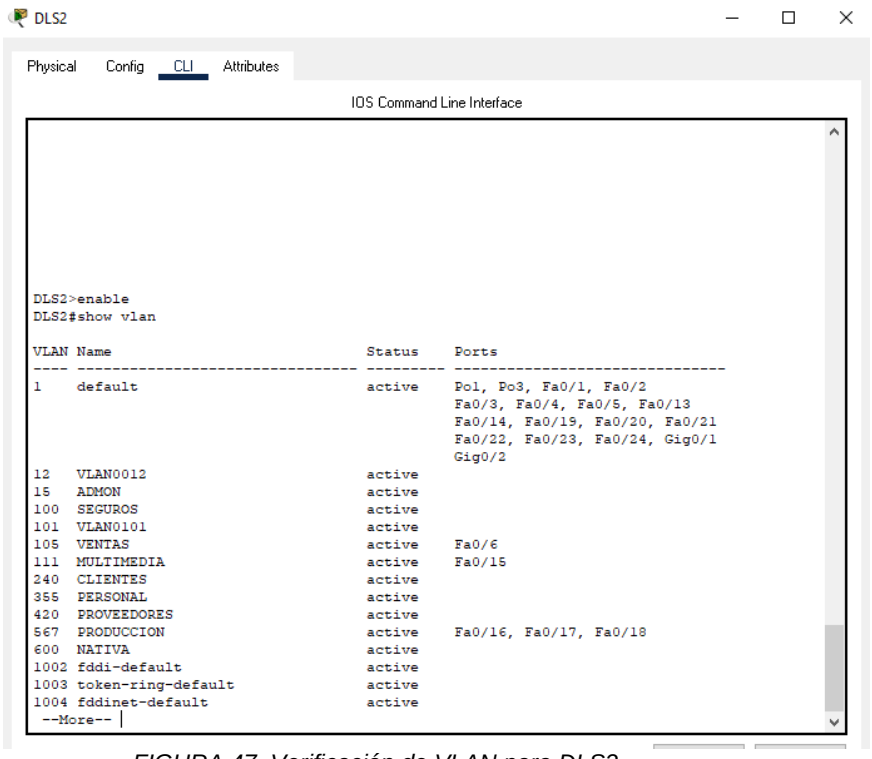

FIGURA 47. Verificación de VLAN para DLS2

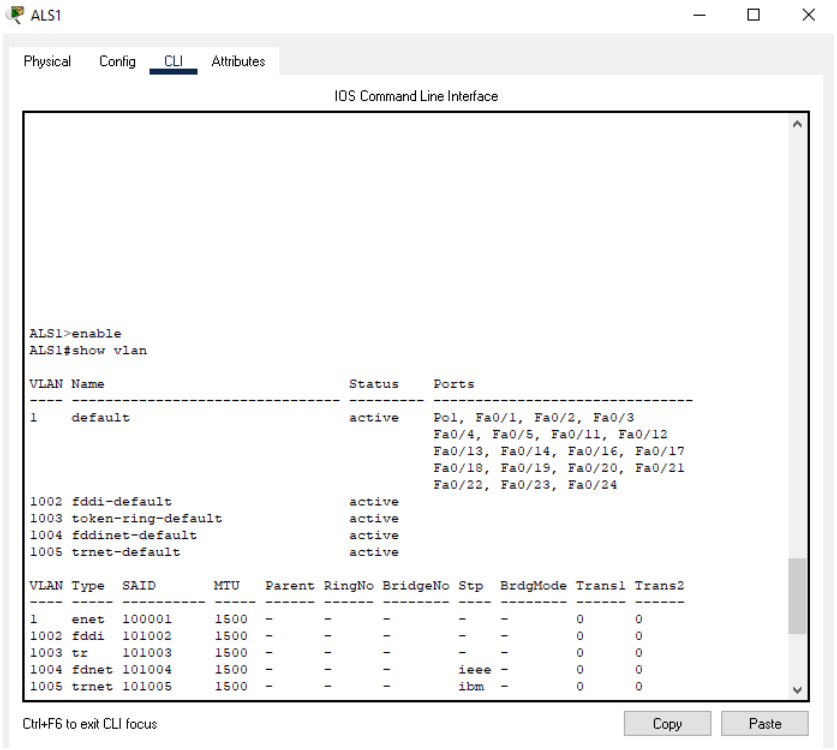

FIGURA 48. Verificación de VLAN para ALS1

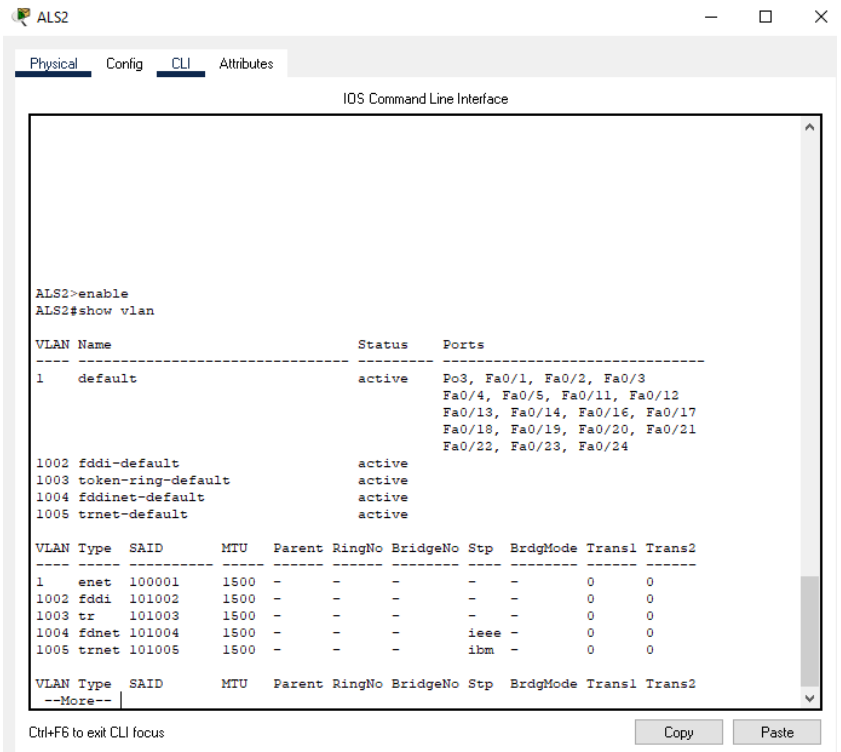

FIGURA 49. Verificación de VLAN para ALS2

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

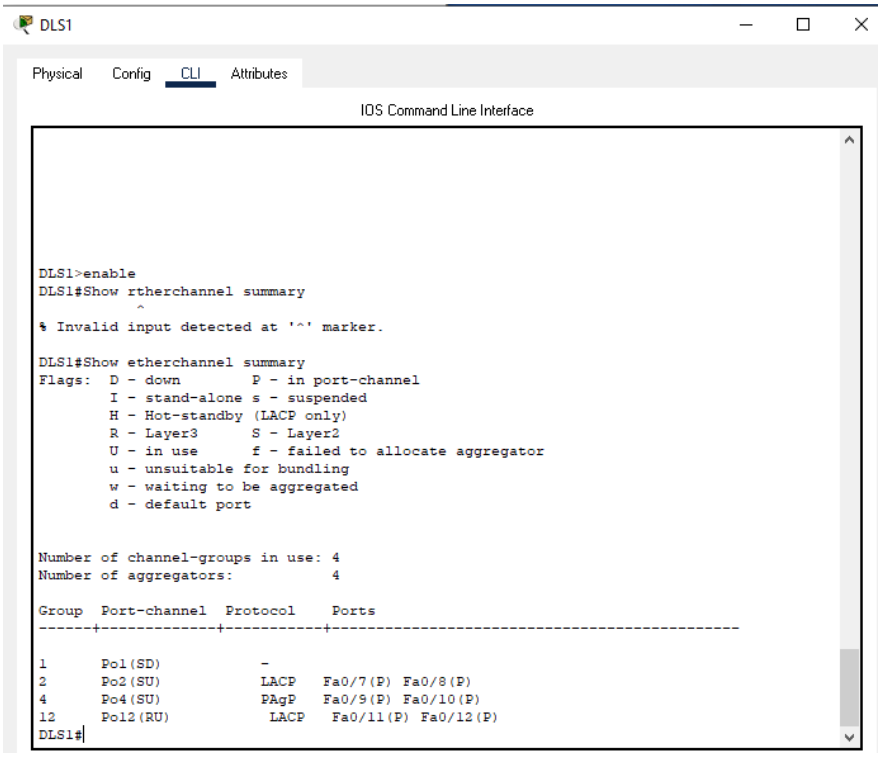

FIGURA 50. EtherChannel en DLS1

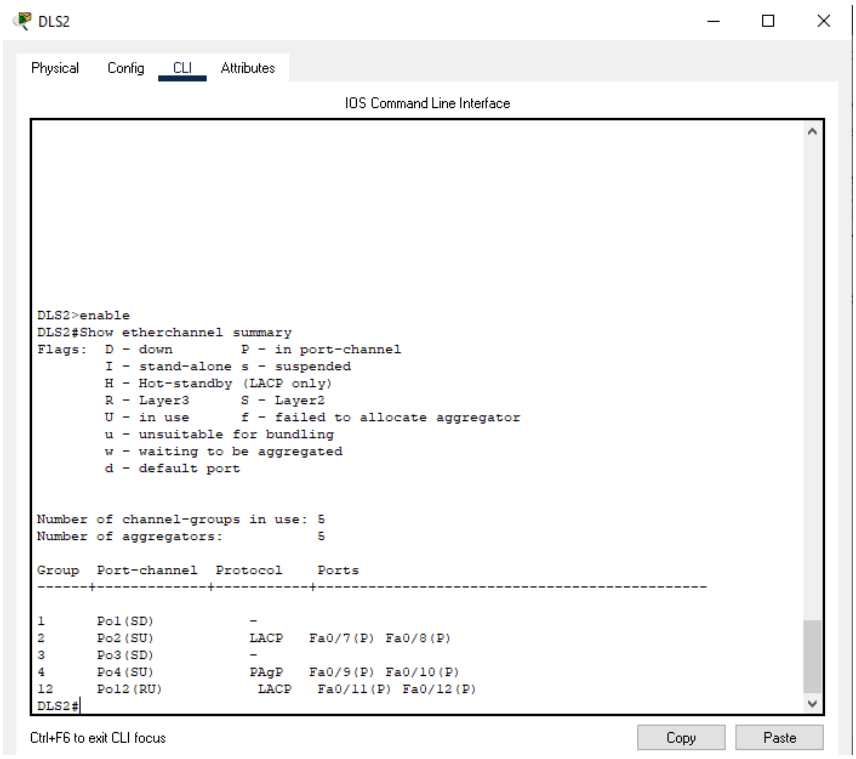

FIGURA 51. EtherChannel en DLS2

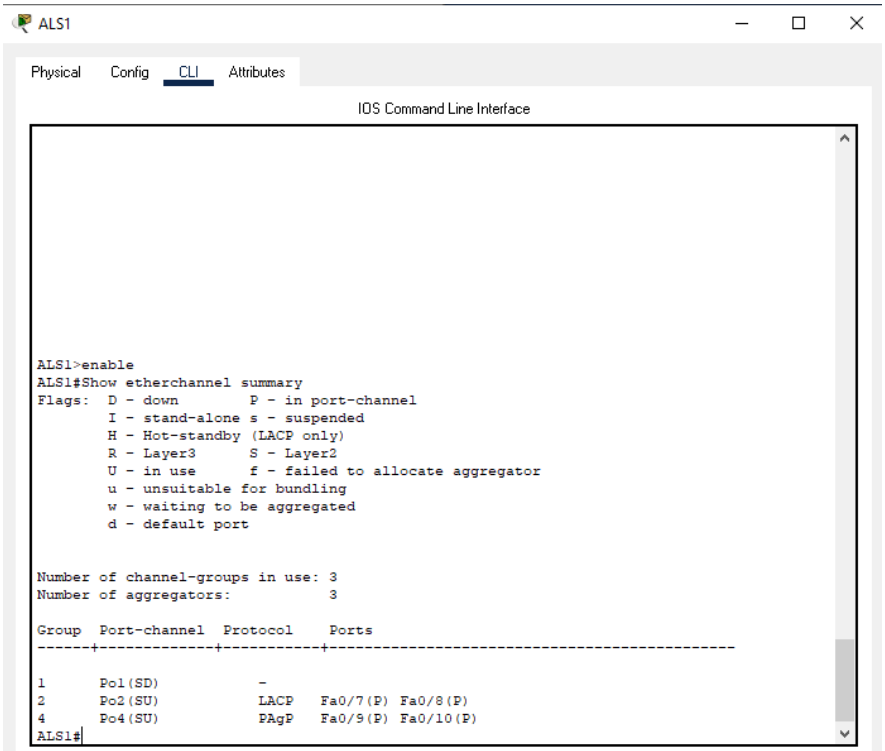

FIGURA 52. EtherChannel en ALS1

FIGURA 53. EtherChannel en ALS2

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

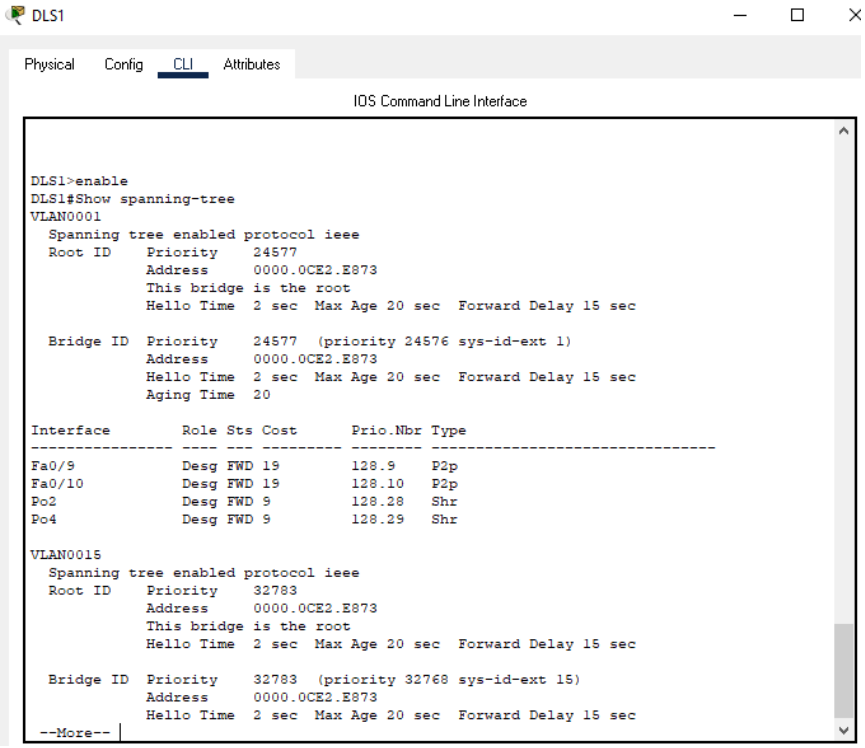

FIGURA 54. configuración de Spanning tree en DLS1

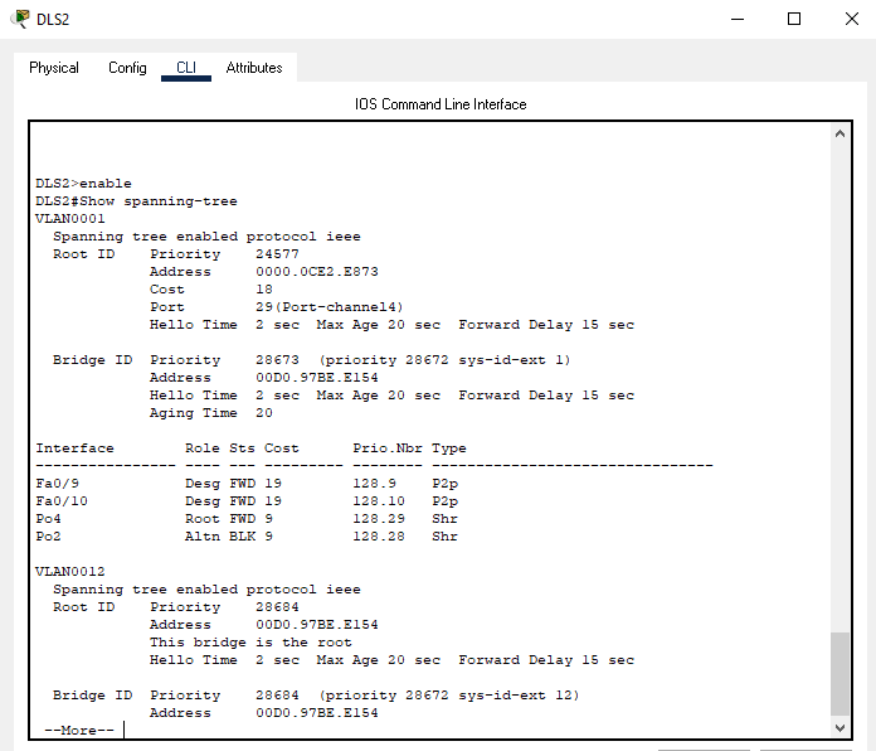

FIGURA 55. configuración de Spanning tree en DLS2

CONCLUSIONES

En este proceso que evidencie para dar cuenta de las habilidades y competencias adquiridas en Diplomado CCNP; mi intención fue reflejar como durante el primer escenario o momento de aprendizaje; logre reforzar conocimientos adquiridos durante la realización de los laboratorios de cada una de las unidades; Cabe aclarar que estas unidades fueron además evaluadas en la plataforma netacad, proceso evaluativo que cumplir a cabalidad.

En este diplomado se nos permitió comprobar de manera práctica el protocolo OSPF (Open Shortest Path First) que permiten que los paquetes de comunicación busquen siempre la ruta más eficiente, para la transmisión de información; lo cual permite que las redes sean redundantes y más estables; aprendizaje que resalto pues eran una de mis falencias al momento inicial del proceso del diplomado y que hoy ya interiorice para mi que hacer laboral.

Un aspecto importante y que se reforzo constantemente dentro del diplomado, fue sobre la redistribución de un protocolo a través del otro. Un ejemplo es que para redistribuir las rutas EIGRP (Enhanced Interior Gateway Routing Protocol) en OSPF (Open Shortest Path First); se realizó la asignación de un costo de 80000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo, también se realizó la configuración inicial de los dispositivos, la asignación del direccionamiento en las interfaces seriales según con el escenario propuesto.

En esta línea en el segundo escenario; los conocimientos previos son sumamente importantes a la hora de ejecutar el código de configuración, de lo contrario puede presentarse muchos errores, situación que se materializa en repetir el código varias veces.

Se logró interiorizar los usos que pueden llegar a tener el código de configuración y los protocolos para las VTP; luego se pudo aprovechar para actualizar las VLAN a las VLAN solicitadas y así crear configuraciones especiales para cada cliente, estableciendo VLANs a cada uno de ellos, situación que va mejorando la administración, la seguridad y la estabilidad de los procesos.

BIBLIOGRAFIA

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

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

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