

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

CINDY MAYERLY HERNÁNDEZ GUERRERO

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

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

CINDY MAYERLY HERNÁNDEZ GUERRERO

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

BOGOTÁ, 27 de Noviembre de 2020

## **AGRADECIMIENTOS**

Agradecemos los consejos, el cariño, el afecto y ayuda de nuestro equipo, que no solo fue de trabajo, si no de amistad y solidaridad, que se mantuvo firme.

A todos nuestros tutores agradecemos por su apoyo y colaboración que nos brindaron durante estos años y que gracias a ellos estamos aquí presentes para dar a conocer nuestro proyecto a través de los conocimientos brindados por personas que nos motivaron a continuar hacia adelante con nuestro proyecto.

Al personal administrativo y de laboratorios del CEAD José Acevedo y Gómez, quienes en su momento supieron guiar mi dudas, y apoyaron mis falencias de conocimiento con su amabilidad y entrega por esta gran institución educativa y todos sus miembros.

## CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS.....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN.....	10
DESARROLLO .....	11
1. Escenario 1 .....	11
2. Escenario 2 .....	24
CONCLUSIONES .....	54
BIBLIOGRAFÍA.....	55

## LISTA DE TABLAS

Tabla 1. Configuración VLAN.....	20
Tabla 2. Configuración de interfaces VLAN.....	26

## LISTA DE FIGURAS

Figura 1. Escenario 1	12
Figura 2. Simulación de escenario 1	13
Figura 3. Aplicando traza y ping R2	16
Figura 4: Show ip route R3	19
Figura 5: verificación de rutas R1.	20
Figura 6: verificación de rutas R5.	21
Figura 7: verificación de OSPF R1.	22
Figura 8: verificación de EIGRP R5.	23
Figura 9: verificación de TRAZA Y PING R1.	24
Figura 10: Topología escenario 2.	25
Figura 11: simulación de escenario 2.	25
Figura 12: verificación servidor principal DLS1.	30
Figura 13: verificación clientes VTP ALS1.	31
Figura 14: verificación clientes VTP ALS2	32
Figura 15: verificación VLAN DLS1	33
Figura 16: verificación VLAN DLS2	35
Figura 17: verificación VLAN DLS1	38
Figura 18: verificación VLAN DLS2	39
Figura 19: verificación VLAN ALS1	40
Figura 20: verificación VLAN ALS2	41
Figura 21: verificación interfaces DLS1	42
Figura 22: verificación interfaces DLS2.	43
Figura 23: verificación interfaces ALS1.	44
Figura 24: verificación interfaces ALS2.	45
Figura 25: verificación ETHERCHANNEL en DLS1 Y ALS1.	46
Figura 26: verificación Spanning-tree en DLS2 Y ALS2.	46

## GLOSARIO

**EIGRP:** Es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP.

**VLAN:** Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

**OSPF:** Open Shortest Path First (OSPF), es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol para calcular la ruta más corta entre dos nodos. Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces.

**Conmutación:** se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido.

**Loopback:** es una interfaz de red virtual. Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas, una práctica común en los routers y son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

## RESUMEN

El presente informe documenta de forma detalla la prueba de habilidades práctica para la evaluación final del diplomado de profundización CISCO CCNP (Cisco Certified Networking Professional / Profesional en Redes certificado por Cisco), el cual está conformado por dos módulos principales (CCNP Route y CCNP Switch), y se lleva a cabo mediante el desarrollo de 2 escenarios planteados dentro de una red empresarial.

En este trabajo se evalúa la capacidad de configurar y administrar dispositivos de redes orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones a través de las redes de datos y electrónica estableciendo alternativas a problemas de interconectividad.

El módulo 1 CCNP Route comprende los temas de conceptos básicos de red y enrutamiento, implementación de EIGRP, implementación de OSPF.

El módulo 2 CCNP Switch está compuesto por los temas de revisión de los conceptos básicos de conmutación, Fundamentos de diseño de red, arquitectura de red de campus.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

This report documents in detail the practical skills test for the final evaluation of the CISCO CCNP (Cisco Certified Networking Professional / Professional in Networks certified by Cisco), which is made up of two main modules (CCNP Route and CCNP Switch), and is carried out through the development of 2 scenarios proposed within a business network.

This work evaluates the ability to configure and manage network devices oriented to the design of scalable and switching networks, through the study of the OSI model, TCP / IP architecture, and the use of resources and tools depending on the protocols and physical layer services to support communications through data and electronic networks, establishing alternatives to interconnectivity problems.

Module 1 CCNP Route covers the topics of basic network and routing concepts, EIGRP implementation, OSPF implementation.

The CCNP Switch Module 2 is comprised of the review topics of Switching Basics, Network Design Fundamentals, Campus Network Architecture.

Keywords: CISCO, CCNP, Routing, Switching, Networking, Electronics.

## INTRODUCCIÓN

El Diplomado de profundización Cisco CCNP tiene esta prueba de habilidades prácticas como herramienta para validar las competencias y conocimientos que el estudiante ha adquirido durante el curso, es esta oportunidad se proponen dos escenarios en donde se exponen casos donde se evidencian configuraciones de routing y switching, para que sean desarrollados y se evidencie su desarrollo mediante simuladores como Packet tracer.

Se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking. Donde a través de los conocimientos adquiridos desde entorno de conocimiento que proporciona el curso, como la investigación individual se pudo consolidar el producto final, esto con el fin de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia, partiendo de conocimientos previos y fundamentos de redes.

El primer escenario corresponde al módulo CCNP ROUTE, donde se aplicarán los principios básicos de red y los protocolos de IP versión 4 (IPv4), el protocolo de enrutamiento de gateway interior mejorado (EIGRP), el protocolo primer camino más corto (OSPF) y el protocolo de puerta de enlace de frontera (BGP).

El segundo escenario corresponde al módulo CCNP SWITCH, el cual permite apropiar las temáticas relacionadas con la implementación, monitoreo y administración de la conmutación en una arquitectura de red empresarial, la implementación de VLAN en redes corporativas, y la configuración y optimización para una alta disponibilidad y redundancia en los switches de capa 2 y capa 3.

## DESARROLLO

### Primer Escenario

Teniendo en cuenta la siguiente imagen:

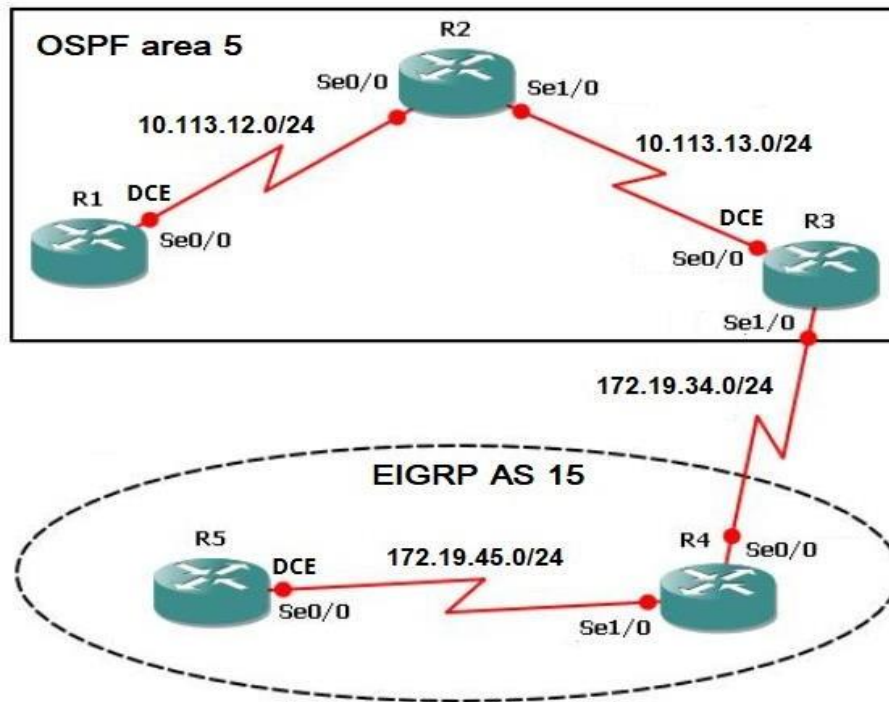


Figura 1: Topología escenario 1

## Topología realizada en Packet Tracer

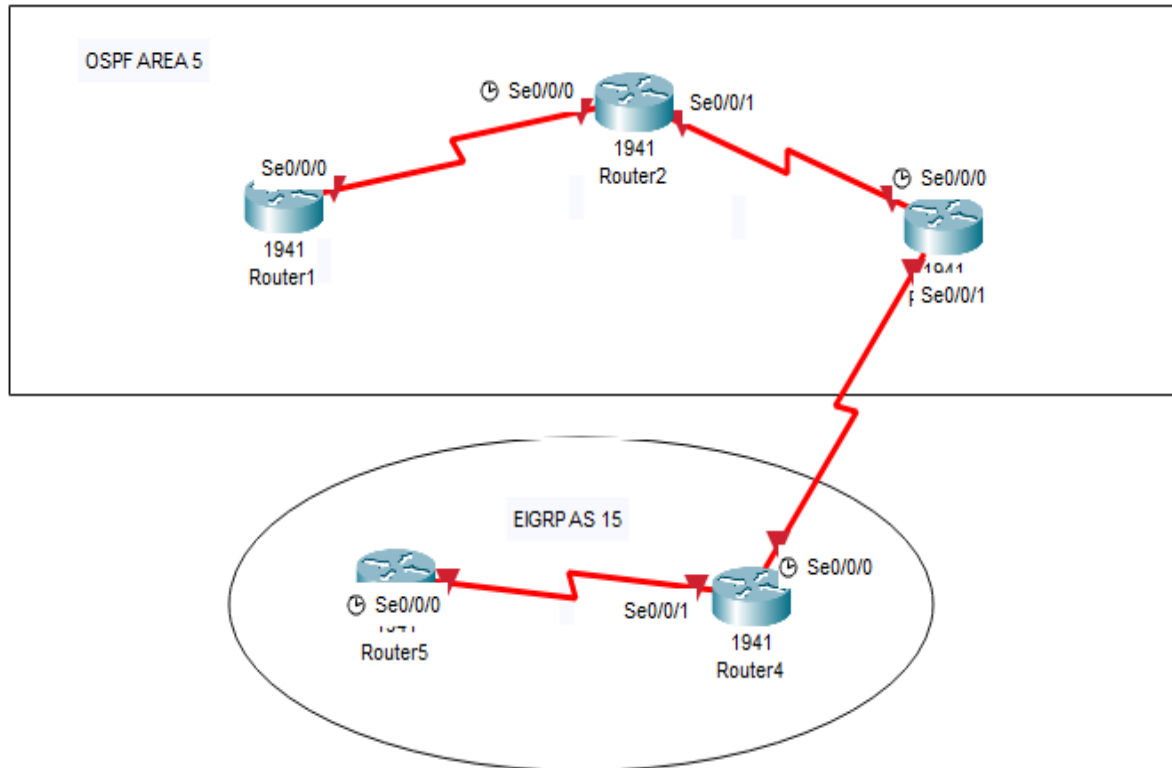


Figura 2: simulación de escenario 1.

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.

### Configuración inicial para R1 y direccionamiento de IP

```
Router#configure terminal
Router(config)#hostname R1
R1(config)# no ip domain-lookup
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-if)# interface serial 0/0/0
R1(config-if)# ip address 10.113.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)# no shutdown
```

### Configuración inicial para R2 y direccionamiento de IP

```
Router#configure terminal
Router(config)#hostname R2
```

```
R2(config)# no ip domain-lookup
R2(config)# line console 0
R2(config-line)# logging synchronous
R2(config-if)# interface serial 0/0/0
R2(config-if)# ip address 10.113.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface serial 0/0/1
R2(config-if)# ip address 10.113.13.1 255.255.255.0
R2(config-if)# no shutdown
```

Configuración inicial para R3 y direccionamiento de IP

```
Router#configure terminal
Router(config)#hostname R3
R3(config)# no ip domain-lookup
R3(config)# line console 0
R3(config-line)# logging synchronous
R3(config-if)# interface serial 0/0/0
R3(config-if)# ip address 10.113.13.2 255.255.255.0
R3(config-if)# clock rate 64000
R3(config-if)# no shutdown
R3(config-if)# interface serial 0/0/1
R3(config-if)# ip address 172.19.34.1 255.255.255.0
R3(config-if)# no shutdown
```

Configuración inicial para R4 y direccionamiento de IP

```
Router#configure terminal
Router(config)#hostname R4
R4(config)# no ip domain-lookup
R4(config)# line console 0
R4(config-line)# logging synchronous
R4(config-if)# interface serial 0/0/0
R4(config-if)# ip address 172.19.34.2 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# interface serial 0/0/1
R4(config-if)# ip address 172.19.45.1 255.255.255.0
R4(config-if)# no shutdown
```

Configuración inicial para R5 y direccionamiento de IP

```
Router#configure terminal
Router(config)#hostname R5
```

```
R5(config)# no ip domain-lookup
R5(config)# line console 0
R5(config-line)# logging synchronous
R5(config-if)# interface serial 0/0/0
R5(config-if)# ip address 172.19.45.2 255.255.255.0
R5(config-if)#clock rate 64000
R5(config-if)# no shutdown
```

#### Configuración de protocolo de enrutamiento OSPF entre R1, R2 y R3

```
R1(config)#router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)#network 10.113.12.0 0.0.0.255 area 5
```

```
R2(config)#router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)#network 10.113.12.0 0.0.0.255 area 5
R2(config-router)#network 10.113.13.0 0.0.0.255 area 5
```

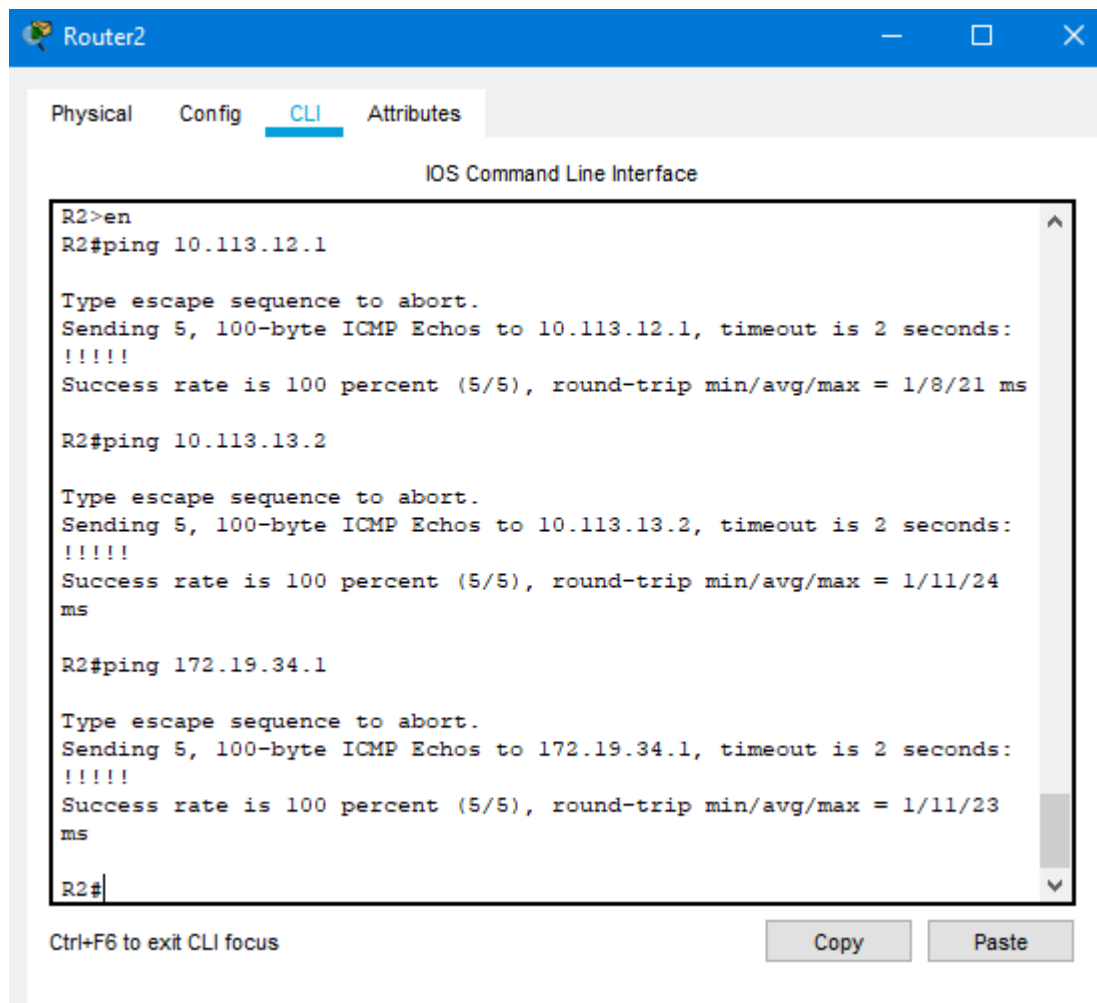
```
R3(config)#router ospf 1
R3(config-router)# router-id 3.3.3.3
R3(config-router)#network 10.113.13.0 0.0.0.255 area 5
R3(config-router)# network 172.19.34.0 0.0.0.255 area 5
R3(config)#router eigrp 15
R3(config-router)#network 172.19.34.0 0.0.0.255
R3(config-router)# no auto-summary
R3(config-router)#end
```

#### Configuración de protocolo de enrutamiento entre R5 y R4

```
R4(config)# router eigrp 15
R4(config-router)# network 172.19.34.0 0.0.0.255
R4(config-router)# network 172.19.45.0 0.0.0.255
R4(config-router)# no auto-summary
R4(config-router)#end
```

```
R5(config)# router eigrp 15
R5(config-router)#network 172.19.45.0 0.0.0.255
R5(config-router)# no auto-summary
R5(config-router)#end
```

Después de la configuración inicial se hace una comprobación para verificar la comunicación de los router ubicados en la misma área: ping desde R2 a R1 y R3.



```
R2>en
R2#ping 10.113.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.113.12.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/21 ms

R2#ping 10.113.13.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.113.13.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/24
ms

R2#ping 172.19.34.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.19.34.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/23
ms

R2#
```

Figura 3: Aplicando ping y traza R2.

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.

Creación de las interfaces Loopback en R1 y configuración de participación en area 5 OSPF

```
R1(config)# interface loopback 1
R1(config-if)# description Engineering Department
R1(config-if)# ip address 10.1.2.1 255.255.252.0

R1(config)# interface loopback 2
R1(config-if)# ip address 10.1.2.1 255.255.252.0
R1(config)# interface loopback 3
R1(config-if)# ip address 10.1.3.1 255.255.252.0
R1(config)# interface loopback 4
R1(config-if)# ip address 10.1.4.1 255.255.252.0
R1(config-if)# exit
R1(config)# router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.0.0 255.255.252.0 area 5
R1(config-router)# exit

R1(config) # interface loopback 1
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
R1(config)# interface loopback 2
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
R1(config)# interface loopback 3
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
R1(config)# interface loopback 4
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
```

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.

#### Creación de interfaces loopback en R5

```
R5(config)# interface loopback 1
R5(config-if)# description Engineering Department
R5(config-if)# ip address 172.5.10.1 255.255.252.0
R5(config-if)# exit
R5(config)# interface loopback 2
R5(config-if)# ip address 172.5.20.1 255.255.252.0
R5(config-if)# exit
R5(config)# interface loopback 3
R5(config-if)# ip address 172.5.30.1 255.255.252.0
R5(config-if)# exit
R5(config)# interface loopback 4
R5(config-if)# ip address 172.5.40.1 255.255.252.0
R5(config-if)# exit
```

#### Configuración para participar en EIGRP 15

```
R5(config)# router eigrp 15
R5(config-router)# auto-summary
R5(config-router)# network 172.5.0.0 0.0.255.255
R5(config-router)# exit
```

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***.

```
R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O       10.1.0.0/22 [110/129] via 10.113.13.1, 00:13:49, Serial0/0/0
O       10.113.12.0/24 [110/128] via 10.113.13.1, 00:23:00,
Serial0/0/0
C       10.113.13.0/24 is directly connected, Serial0/0/0
L       10.113.13.2/32 is directly connected, Serial0/0/0
D       172.5.0.0/16 [90/2809856] via 172.19.34.2, 00:07:38, Serial0/0/1
        172.19.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.19.34.0/24 is directly connected, Serial0/0/1
L       172.19.34.1/32 is directly connected, Serial0/0/1
D       172.19.45.0/24 [90/2681856] via 172.19.34.2, 00:21:35,
Serial0/0/1

R3#
```

Figura 4: Show ip route R3.

Por medio del uso del comando show ip route se logra identificar las redes accesibles o las que se han actualizado en la tabla de enrutamiento.

- 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.

Configuración de rutas EIGRP en OSPF costo 50000 y retribución de rutas OSPF en EIGRP.

```

R3(config)#router ospf 1
R3(config-router)# redistribute ospf 1 metric 50000 100 255 1 1500
R3(config-router)# exit
R3(config)# exit
R3(config)# router ospf 1
R3(config-router)# log-adjacency-changes
R3(config-router)# redistribute eigrp 15 metric 50000 subnets
R3(config-router)# exit
R3(config)# router eigrp 15
R3(config-router)# redistribute ospf 1 metric 1544000 22000 255 1 1500
R3(config-router)# exit

```

Para redistribuir las rutas EIGRP en OSPF, se incorporó el R3 al proceso EIGRP que lo comunica con R4; con ello R3 queda funcionando con los dos procesos (OSPF y EIGRP).

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

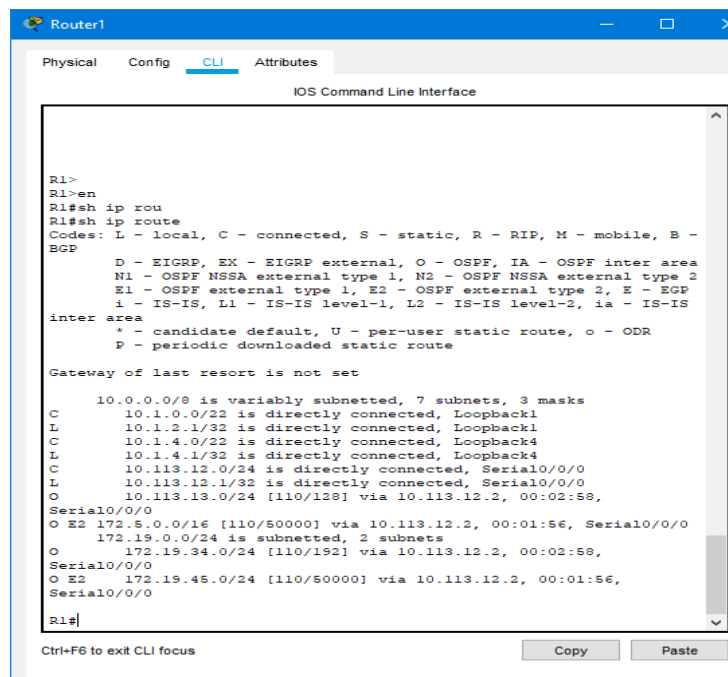


Figura 5: verificación de rutas R1.

```
R5#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX   10.1.0.0/22 [170/8313856] via 172.19.45.1, 00:02:34,
Serial0/0/0
D EX   10.113.12.0/24 [170/8313856] via 172.19.45.1, 00:02:34,
Serial0/0/0
D EX   10.113.13.0/24 [170/8313856] via 172.19.45.1, 00:02:34,
Serial0/0/0
      172.5.0.0/16 is variably subnetted, 9 subnets, 3 masks
D      172.5.0.0/16 is a summary, 00:18:33, Null0
C      172.5.8.0/22 is directly connected, Loopback1
L      172.5.10.1/32 is directly connected, Loopback1
C      172.5.20.0/22 is directly connected, Loopback2
L      172.5.20.1/32 is directly connected, Loopback2
C      172.5.28.0/22 is directly connected, Loopback3
L      172.5.30.1/32 is directly connected, Loopback3
C      172.5.40.0/22 is directly connected, Loopback4
L      172.5.40.1/32 is directly connected, Loopback4
      172.19.0.0/16 is variably subnetted, 4 subnets, 3 masks
D      172.19.0.0/16 is a summary, 00:15:42, Null0
D      172.19.34.0/24 [90/2681856] via 172.19.45.1, 00:18:42,
Serial0/0/0
C      172.19.45.0/24 is directly connected, Serial0/0/0
L      172.19.45.2/32 is directly connected, Serial0/0/0

R5#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 6: verificación de rutas R5.

Al ejecutar el comando show ip route, se puede verificar que R1 como R5 presentan las rutas del sistema autónomo opuesto anexándolas a sus respectivas tablas de enrutamiento (figura 6 y figura 7).

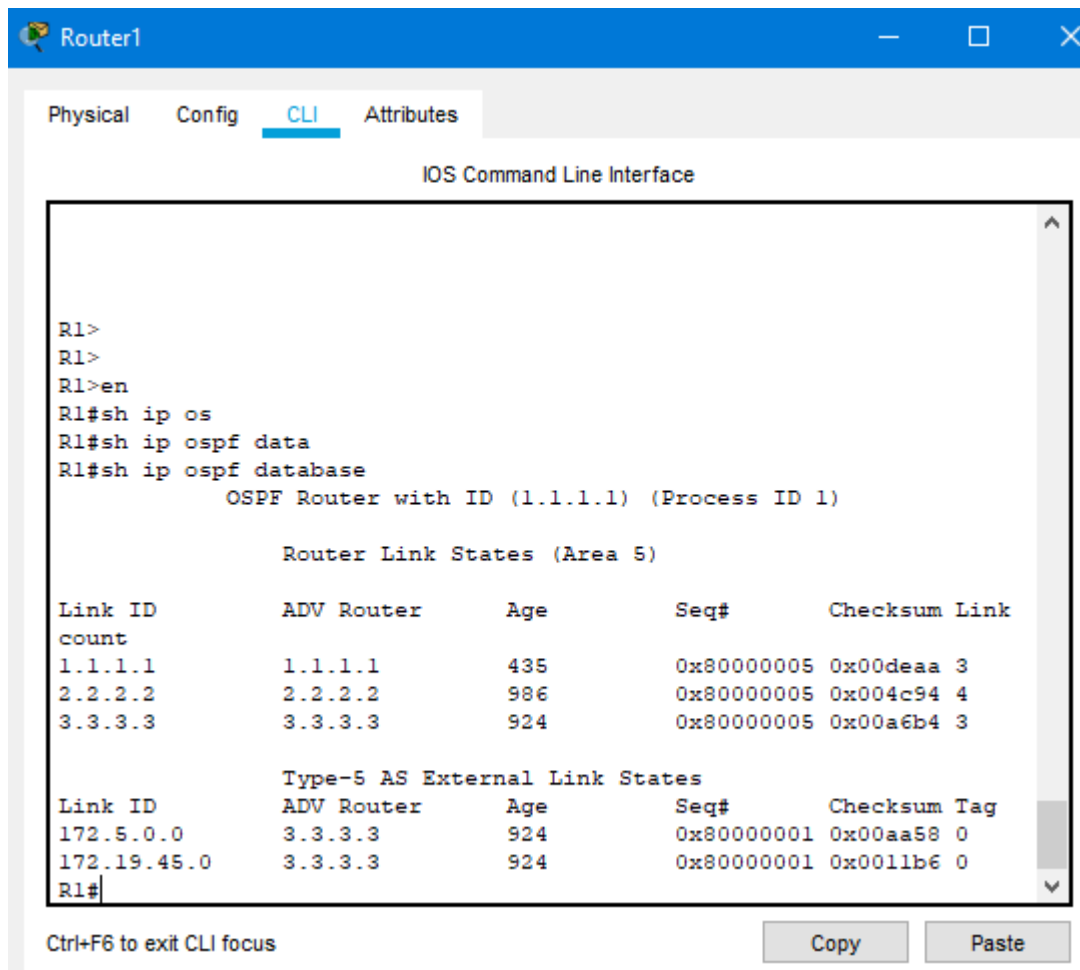
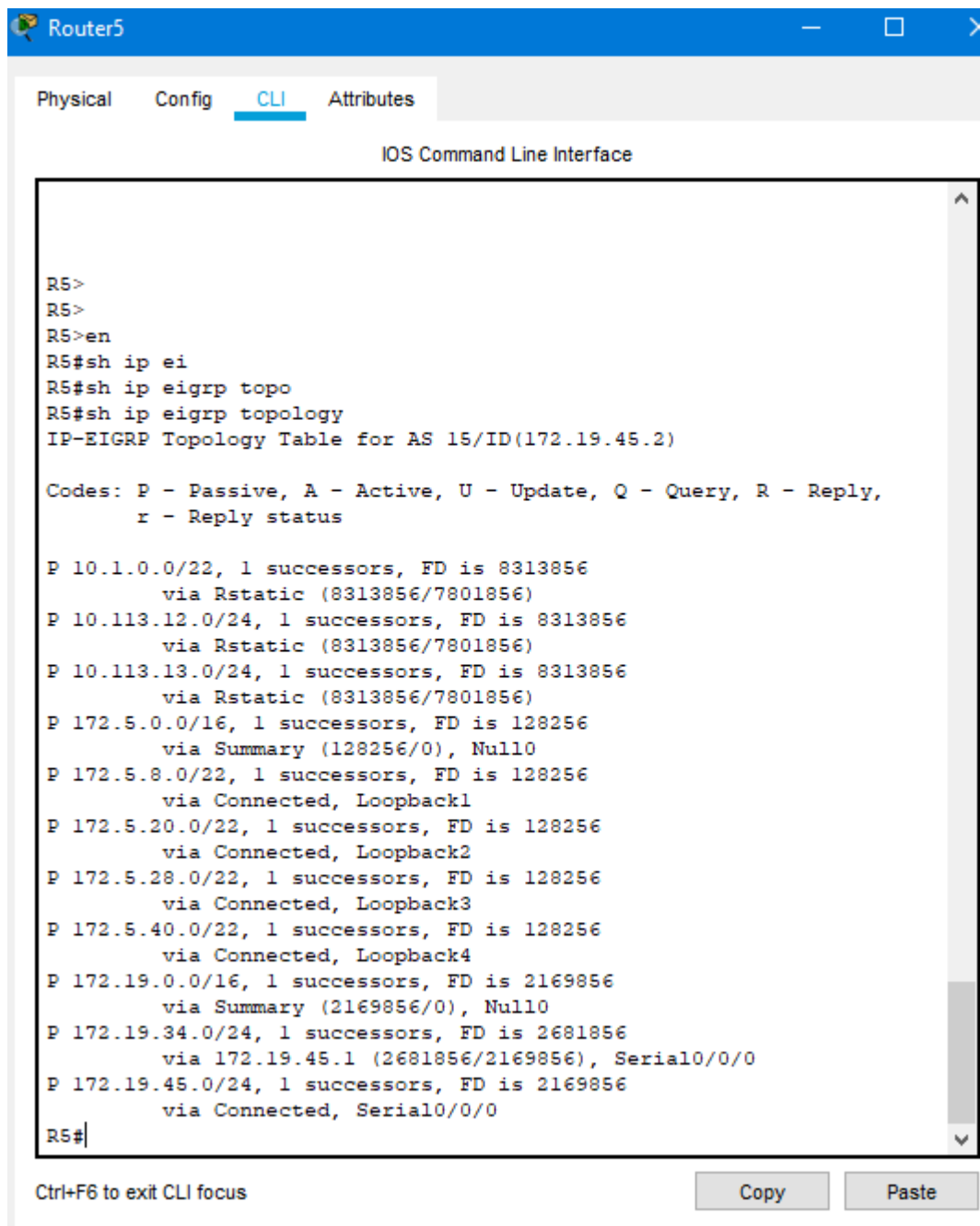


Figura 7: verificación de OSPF R1.



The screenshot shows a window titled "Router5" with a blue header bar. Below the header are four tabs: "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected and highlighted. The main content area is titled "IOS Command Line Interface" and contains a terminal window with the following text:

```
R5>
R5>
R5>en
R5#sh ip ei
R5#sh ip eigrp topo
R5#sh ip eigrp topology
IP-EIGRP Topology Table for AS 15/ID(172.19.45.2)

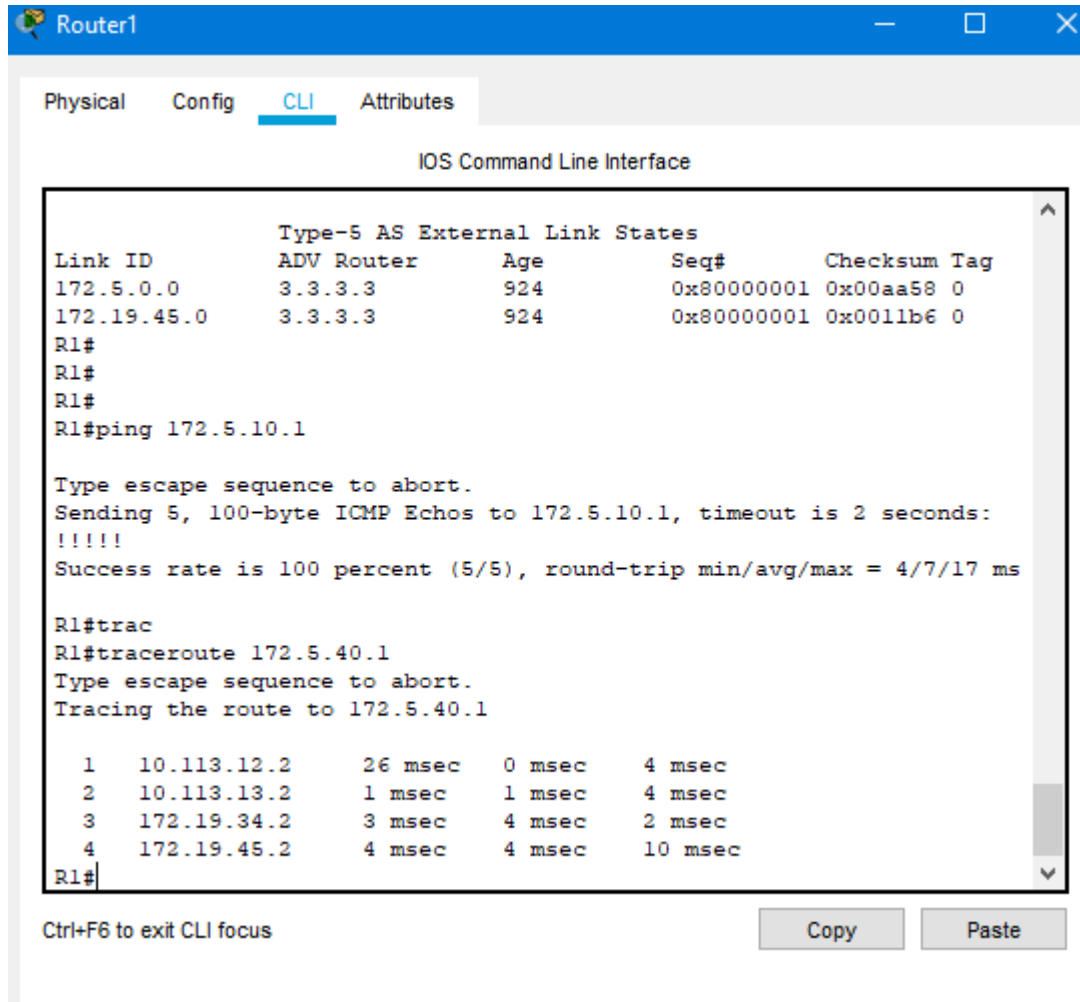
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.1.0.0/22, 1 successors, FD is 8313856
   via Rstatic (8313856/7801856)
P 10.113.12.0/24, 1 successors, FD is 8313856
   via Rstatic (8313856/7801856)
P 10.113.13.0/24, 1 successors, FD is 8313856
   via Rstatic (8313856/7801856)
P 172.5.0.0/16, 1 successors, FD is 128256
   via Summary (128256/0), Null0
P 172.5.8.0/22, 1 successors, FD is 128256
   via Connected, Loopback1
P 172.5.20.0/22, 1 successors, FD is 128256
   via Connected, Loopback2
P 172.5.28.0/22, 1 successors, FD is 128256
   via Connected, Loopback3
P 172.5.40.0/22, 1 successors, FD is 128256
   via Connected, Loopback4
P 172.19.0.0/16, 1 successors, FD is 2169856
   via Summary (2169856/0), Null0
P 172.19.34.0/24, 1 successors, FD is 2681856
   via 172.19.45.1 (2681856/2169856), Serial10/0/0
P 172.19.45.0/24, 1 successors, FD is 2169856
   via Connected, Serial10/0/0
R5#
```

Below the terminal window, there is a text label "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Figura 8: verificación de EIGRP R5.

## Pruebas de traza



The screenshot shows the CLI of Router1 with the following output:

```
IOS Command Line Interface

Type-5 AS External Link States
Link ID          ADV Router      Age             Seq#            Checksum Tag
172.5.0.0        3.3.3.3        924             0x80000001     0x00aa58 0
172.19.45.0     3.3.3.3        924             0x80000001     0x0011b6 0
R1#
R1#
R1#
R1#ping 172.5.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.5.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/17 ms

R1#trac
R1#traceroute 172.5.40.1
Type escape sequence to abort.
Tracing the route to 172.5.40.1

 1  10.113.12.2    26 msec    0 msec    4 msec
 2  10.113.13.2    1 msec     1 msec    4 msec
 3  172.19.34.2    3 msec     4 msec    2 msec
 4  172.19.45.2    4 msec     4 msec    10 msec
R1#
```

Below the CLI window, there are buttons for 'Copy' and 'Paste', and a note: 'Ctrl+F6 to exit CLI focus'.

Figura 9: verificación de TRAZA Y PING R1.

En la figura10 se logra evidenciar el ping exitoso, como también el traceroute a la Loopback de R5, con lo cual se demuestra que se tiene acceso a las demás Loopback.

## 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.

### Topología de red

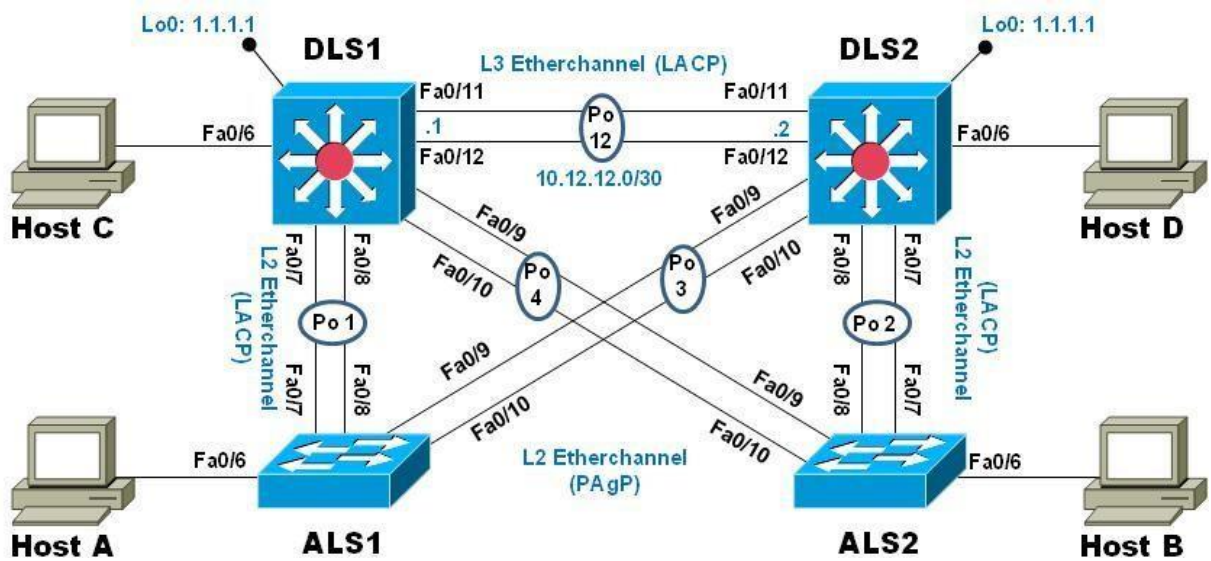


Figura 10: Topología escenario 2.

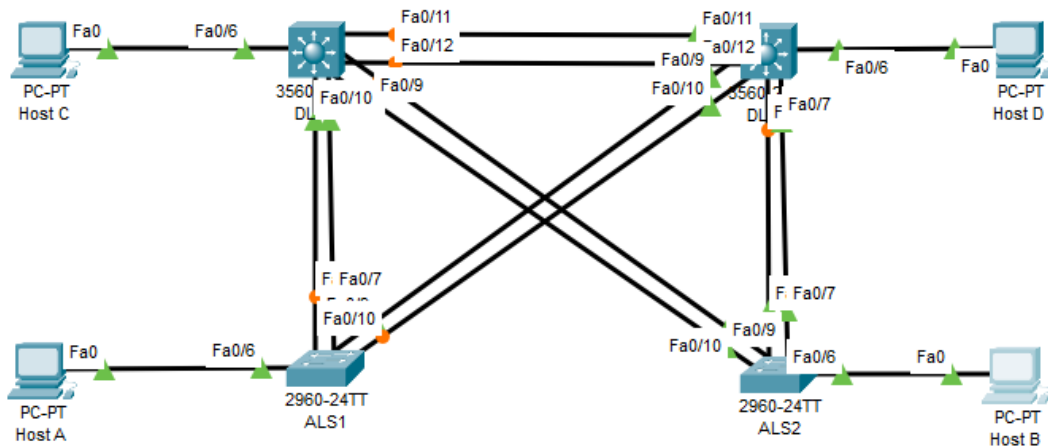


Figura 11: simulación de escenario 2.

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

- a. Apagar todas las interfaces en cada switch.

Se realiza el apagado de cada una de las interfaces de los 4 Switch por medio del comando "shutdown".

```
Switch#configure terminal
Switch(config)#interface range FastEthernet0/1-9
Switch(config-if-range)#shu
Switch(config-if-range)#shutdown
Switch(config-if-range)#ex
Switch(config)#interface range FastEthernet0/10-19
Switch(config-if-range)#shu
Switch(config-if-range)#shutdown
Switch(config-if-range)#ex
Switch(config)#interface range FastEthernet0/19-22
Switch(config-if-range)#shu
Switch(config-if-range)#shutdown
Switch(config-if-range)#
```

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

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

```
Switch #configure terminal
Switch (config)#hostname DLS2
DLS2(config)#
```

```
Switch #configure terminal
Switch(config)#hostname ALS1
ALS1(config)#
```

```
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 10.12.12.1/30 y para DLS2 utilizará 10.12.12.2/30.

```
DLS1(config)#interface port-channel 12
DLS1(config-if-range)#no switchport
DLS1(config-if)#ip address 10.12.12.1 255.255.255.252
DLS1(config-if)#exit
DLS1(config)#interface range FastEthernet0/11-12
DLS1(config-if-range)#no switchport
DLS1(config-if-range)#channel-group 12 mode active
DLS1(config-if-range)#exit
```

```
DLS2(config)#interface port-channel 12
DLS2(config-if-range)#no switchport
DLS2(config-if)#ip address 10.12.12.2 255.255.255.252
DLS2(config-if-range)#exit
DLS2(config)# interface range FastEthernet0/11-12
DLS2(config-if-range)#no switchport
DLS2(config-if-range)#channel-group 12 mode active
DLS2(config-if-range)#exit
```

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

Se configura LACP en los Port-channels en las interfaces deseadas y se asigna el mode active.

```
DLS1(config-if)#interface range FastEthernet0/7-8
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 1 mode active
DLS1(config-if-range)#no shutdown
DLS1(config-if-range)#end
```

```
ALS1(config)#interface range FastEthernet0/7-8
ALS1(config-if-range)#switchport trunk encapsulation dot1q
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 1 mode active
ALS1(config-if-range)#no shutdown
ALS1(config-if-range)#end
```

```
DLS2(config-if)#interface range FastEthernet0/7-8
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 2 mode active
DLS2(config-if-range)#no shutdown
DLS2(config-if-range)#end
```

```
ALS2(config)#interface range FastEthernet0/7-8
ALS2(config-if-range)#switchport trunk encapsulation dot1q
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#no shutdown
```

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

Se configura PAgP en los Port-channels en las interfaces deseadas y se asigna el mode deseable:

```
DLS1(config-if)#interface range FastEthernet0/9-10
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
DLS1(config-if-range)#end
```

```
ALS1(config-if)# interface range FastEthernet0/9-10
ALS1(config-if-range)#switchport trunk encapsulation dot1q
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 3 mode desirable
ALS1(config-if-range)#no shutdown
ALS1(config-if-range)#end
```

```
DLS2(config-if)# interface range FastEthernet0/9-10
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 3 mode desirable
DLS2(config-if-range)#no shutdown
```

```
DLS2(config-if-range)#end
```

```
ALS2(config-if)# interface range FastEthernet0/9-10  
ALS2(config-if-range)#switchport trunk encapsulation dot1q  
ALS2(config-if-range)#switchport mode trunk  
ALS2(config-if-range)#channel-group 4 mode desirable  
ALS2(config-if-range)#no shutdown  
ALS2(config-if-range)#end
```

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

```
DLS1#vlan database  
DLS1(vlan)# vlan 500  
DLS1(vlan)#apply  
DLS1(vlan)#exit  
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)#exit
```

```
ALS1(config)#interface Po1  
ALS1(config-if)#switchport trunk native Vlan 500  
ALS1(config-if)#exit  
ALS1(config)#interface Po3  
ALS1(config-if)#switchport trunk native Vlan 500  
ALS1(config-if)#exit
```

```
DLS2(config)#interface Po2  
DLS2(config-if)#switchport trunk native Vlan 500  
DLS2(config)#interface Po3  
DLS2(config-if)#switchport trunk native Vlan 500  
DLS2(config-if)#exit
```

```
ALS2(config)#interface Po2  
ALS2(config-if)#switchport trunk native Vlan 500  
ALS2(config-if)#exit  
ALS2(config)#interface Po4  
ALS2(config-if)#switchport trunk native Vlan 500  
ALS2(config-if)#exit
```

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

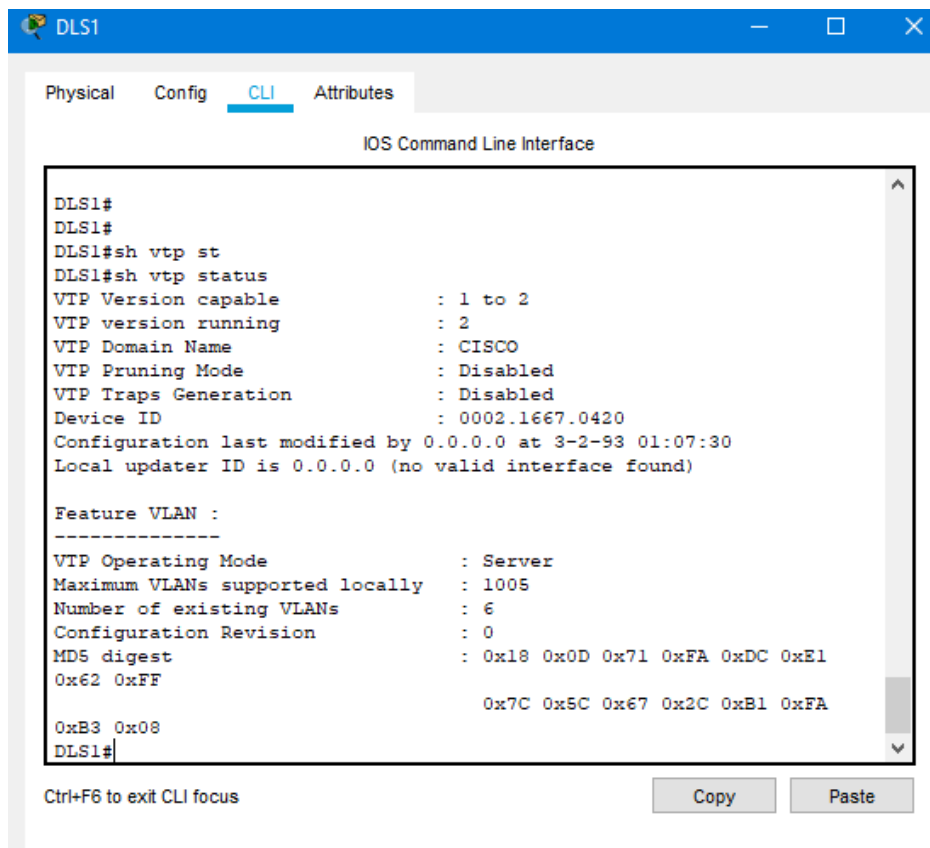
1) Utilizar el nombre de dominio CISCO con la contraseña ccnp321

```
DLS1(config)#vtp domain CISCO
DLS1(config)#vtp version 3
DLS1(config)#vtp password ccnp321
DLS1(config)#end
```

```
ALS1(config)#vtp domain CISCO
ALS1(config)#vtp version 3
ALS1(config)#vtp password ccnp321
ALS1(config)#end
```

```
ALS2(config)#vtp domain CISCO
ALS2(config)#vtp version 3
ALS2(config)#vtp password ccnp321
```

2) Configurar DLS1 como servidor principal para las VLAN.



The screenshot shows a terminal window titled 'DLS1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following commands and their results:

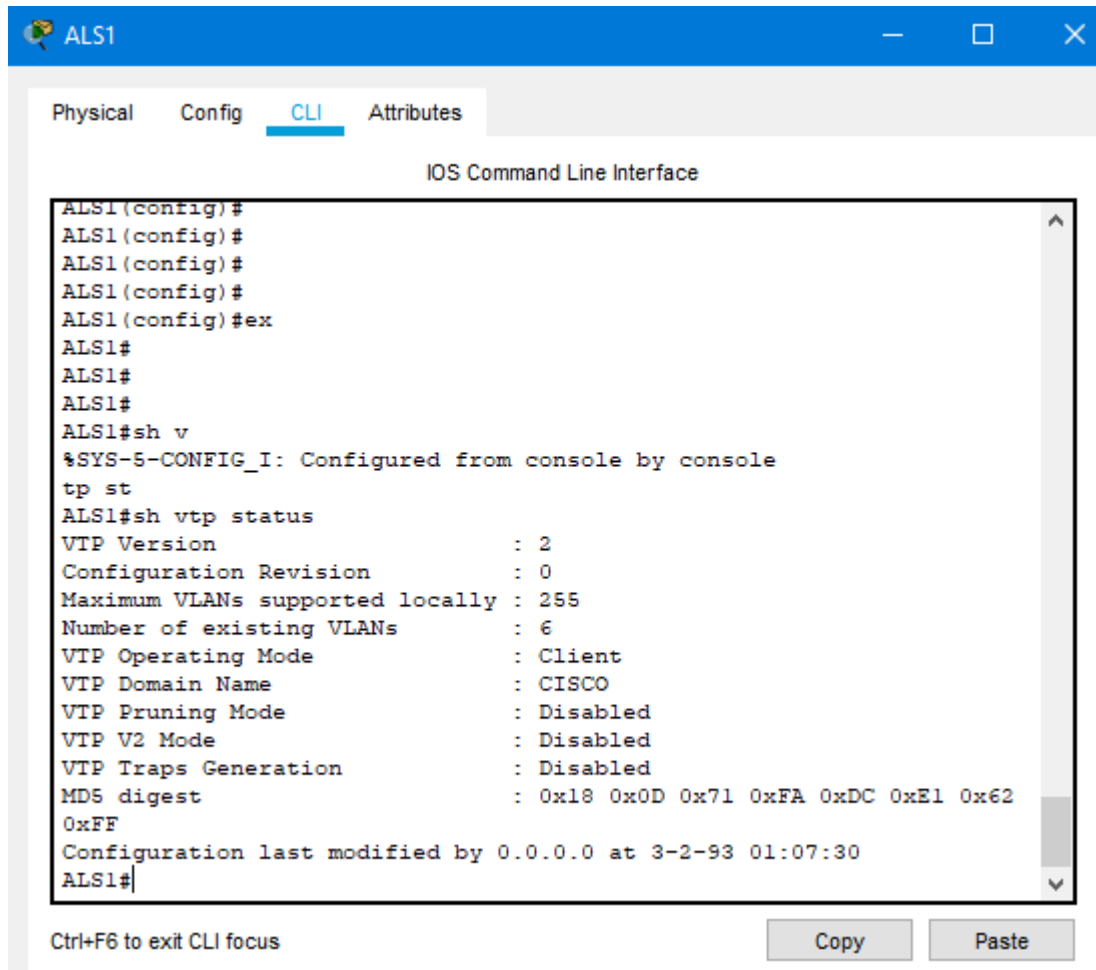
```
DLS1#
DLS1#
DLS1#sh vtp st
DLS1#sh vtp status
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : CISCO
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0002.1667.0420
Configuration last modified by 0.0.0.0 at 3-2-93 01:07:30
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
-----
VTP Operating Mode      : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 6
Configuration Revision  : 0
MD5 digest              : 0x18 0x0D 0x71 0xFA 0xDC 0xE1
                        0x62 0xFF
                        0x7C 0x5C 0x67 0x2C 0xB1 0xFA
                        0xB3 0x08
DLS1#
```

At the bottom of the terminal window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons labeled 'Copy' and 'Paste'.

Figura 12: verificación servidor principal DLS1.

### 3) Configurar ALS1 y ALS2 como clientes VTP.



The screenshot shows a window titled 'ALS1' with a blue header bar. Below the header are four tabs: 'Physical', 'Config', 'CLI' (which is selected and highlighted in blue), and 'Attributes'. The main content area is titled 'IOS Command Line Interface' and contains a text-based terminal window. The terminal shows the following sequence of commands and outputs:

```
ALS1(config)#
ALS1(config)#
ALS1(config)#
ALS1(config)#
ALS1(config)#ex
ALS1#
ALS1#
ALS1#
ALS1#sh v
%SYS-5-CONFIG_I: Configured from console by console
tp st
ALS1#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 6
VTP Operating Mode         : Client
VTP Domain Name            : CISCO
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x18 0x0D 0x71 0xFA 0xDC 0xE1 0x62
0xFF
Configuration last modified by 0.0.0.0 at 3-2-93 01:07:30
ALS1#
```

At the bottom of the window, there is a status bar that reads 'Ctrl+F6 to exit CLI focus' on the left and two buttons, 'Copy' and 'Paste', on the right.

Figura 13: verificación clientes VTP ALS1.

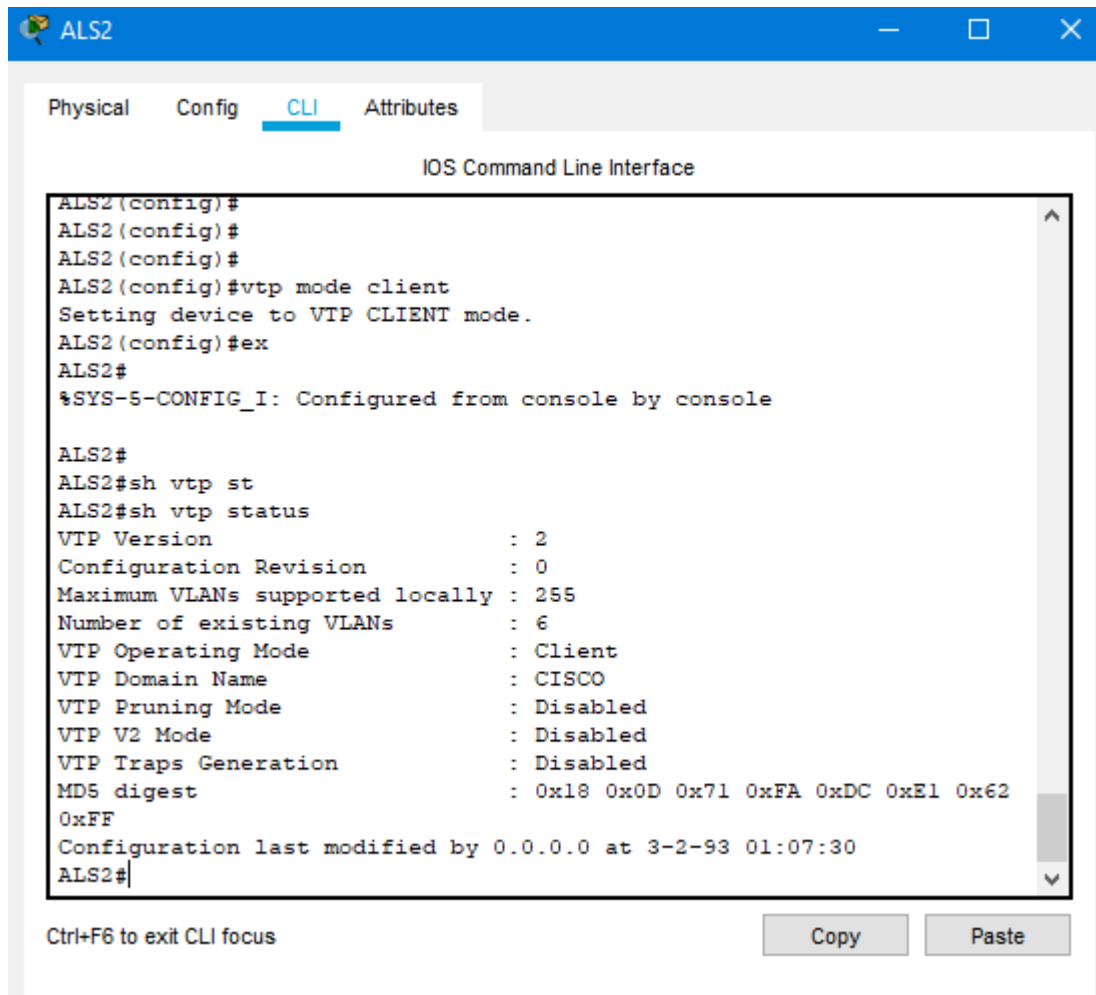


Figura 14: verificación clientes VTP ALS2

Se asigna el nombre de dominio y la contraseña establecida a los switches DLS1, ALS1 y ALS2.

- e. Configurar en el servidor principal las siguientes VLAN:

Tabla 1. Configuración 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

Se realiza la respectiva configuración de las VLAN en el servidor principal.

```
DLS1(config)#vlan 500
DLS1(config-vlan)#name NATIVA
DLS1(config-vlan)#vlan 434
DLS1(config-vlan)#name PROVEEDORES
DLS1(config-vlan)#vlan 12
DLS1(config-vlan)#name ADMON
DLS1(config-vlan)#vlan 123
DLS1(config-vlan)#name SEGUROS
DLS1(config-vlan)#vlan 234
DLS1(config-vlan)#name CLIENTES
DLS1(config-vlan)#vlan 1010
DLS1(config-vlan)#name VENTAS
DLS1(config-vlan)#vlan 1111
DLS1(config-vlan)#name MULTIMEDIA
DLS1(config-vlan)#vlan 3456
DLS1(config-vlan)#name PERSONAL
DLS1(config-vlan)#exit
```

f. En DLS1, suspender la VLAN 434.

Se procede a suspender la VLAN 434 con el comando “state suspend”

```
DLS1(config)#vlan 434
DLS1(config-vlan)#state suspend
```

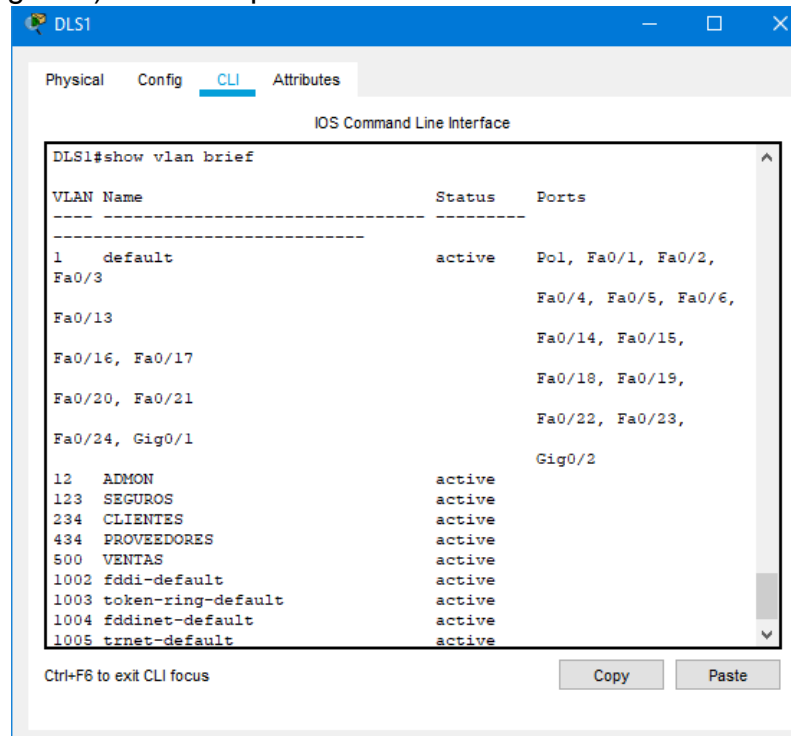


Figura 15: verificación VLAN DLS1

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

Por medio de los comandos “vtp version 2” “vtp mode transparent” se configuran en

DLS2 cada una de las VLANs estipuladas.

```
DLS2(config)#vtp version 2
DLS2(config)#vtp mode transparent
DLS2(config)#vlan 500
DLS2(config-vlan)#name NATIVA
DLS2(config-vlan)#vlan 434
DLS2(config-vlan)#name PROVEEDORES
DLS2(config-vlan)#vlan 12
DLS2(config-vlan)#name ADMON
DLS2(config-vlan)#vlan 123
DLS2(config-vlan)#name SEGUROS
DLS2(config-vlan)#vlan 234
DLS2(config-vlan)# name CLIENTES
DLS2(config-vlan)#vlan 1010
DLS2(config-vlan)#name VENTAS
DLS2(config-vlan)#vlan 1111
DLS2(config-vlan)#name MULTIMEDIA
DLS2(config-vlan)#vlan 3456
DLS2(config-vlan)#name PERSONAL
DLS2(config-vlan)#exit
```

- h. Suspender VLAN 434 en DLS2.

Se procede a suspender la VLAN 434 con el comando “state suspend”

```
DLS2(config)#vlan 434
DLS2(config-vlan)#state suspend
DLS2(config-vlan)#exit
```

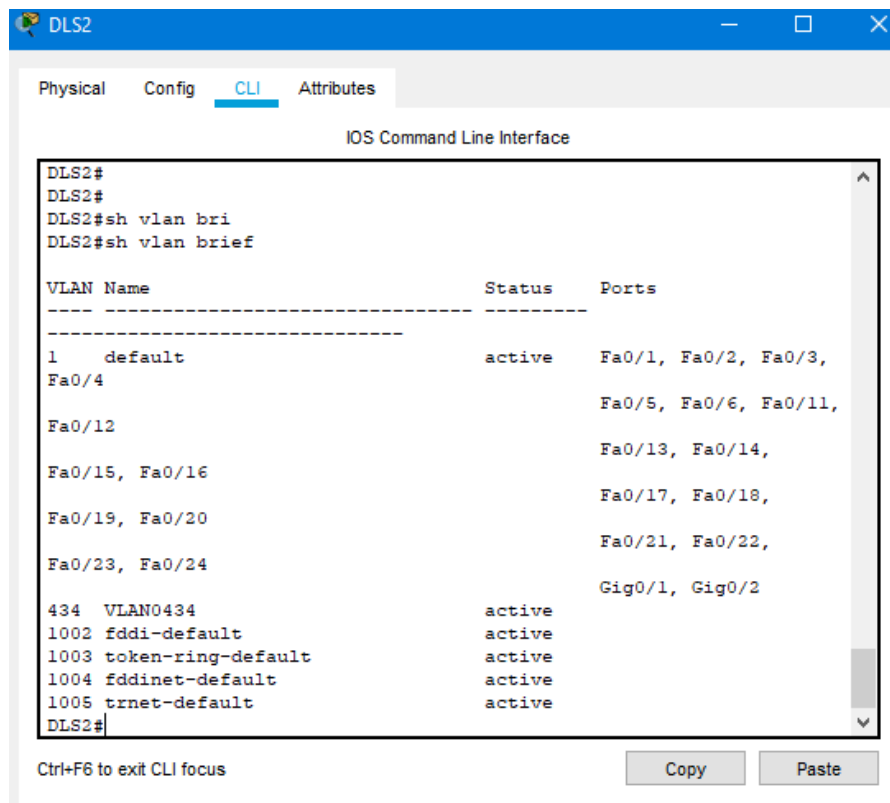


Figura 16: verificación VLAN DLS2

- 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.

Se crea la VLAN 567 en DLS2 y se configura tal forma que ésta no sea reconocida por los demás switches de la red.

```
DLS2(config)#vlan 567
DLS2(config-vlan)#name PRODUCCION
DLS2(config-vlan)#exit
DLS2(config)#interface port-channel 2
DLS2(config)#switchport trunk allowed vlan except 567
DLS2(config)#interface port-channel 3
DLS2(config)#switchport trunk allowed vlan except 567
```

- j. 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.
 

```
DLS1(config)#spanning-tree vlan 1,12,434,500,1010,1111,3456 root primary
DLS1(config)#spanning-tree vlan 123,234 root secondary
```

- k. 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.

```
DLS2(config)#spanning-tree vlan 123,234 root primary
DLS2(config)#spanning-tree vlan 1,12,434,500,1010,1111,3456 root secondary
```

- 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 éstos puertos.

```
DLS1(config)#interface range FastEthernet0/7-10
DLS1(config-if-range)#switchport trunk allowed vlan 12,123,234,500,1010,1111,3456
```

```
DLS2(config)#interface range FastEthernet0/7-10
DLS2(config-if-range)# switchport trunk allowed vlan 12,123,234,500,1010,1111,3456
```

```
ALS1(config)#interface range FastEthernet0/7-10
ALS1(config-if-range)#switchport trunk allowed vlan 12,123,234,500,1010,1111,3456
```

```
ALS2(config)#interface range FastEthernet0/7-10
ALS2(config-if-range)#switchport trunk allowed vlan 12,123,234,800,1010,1111,3456
```

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

Tabla 2. Configuración de interfaces VLAN

Interfaz	DLS1	DLS2	ALS1	ALS2
<b>Interfaz Fa0/6</b>	3456	12 , 1010	123, 1010	234
<b>Interfaz Fa0/15</b>	1111	1111	1111	1111
<b>Interfaces F0 /16-18</b>		567		

```
DLS1(config)#interface Fa0/6
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport host
DLS1(config-if)#switchport access vlan 3456
DLS1(config-if)#no shutdown
DLS1(config-if)#interface Fa0/15
DLS1(config-if)#switchport host
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 1111
DLS1(config-if)#no shutdown
```

```
DLS2(config)#interface Fa0/6
DLS2(config-if)#switchport host
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 12
DLS2(config-if)#switchport access vlan 1010
DLS2(config-if)#no shutdown
DLS2(config-if)#interface Fa0/15
DLS2(config-if)#switchport host
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 1111
DLS2(config-if)#no shut
DLS2(config-if)#interface range F0 /16-18
DLS2(config-if-range)#switchport host 39
DLS2(config-if-range)#switchport mode access
DLS2(config-if-range)#switchport access vlan 567
DLS2(config-if-range)#no shut
```

```
ALS1(config)#interface F0/6
ALS1(config-if)#switchport host
ALS1(config-if)#switchport mode access
ALS1(config-if)#switchport access vlan 123
ALS1(config-if)#switchport access vlan 1010
ALS1(config-if)#no shutdown
ALS1(config-if)#interface F0/15
ALS1(config-if)#switchport host
ALS1(config-if)#switchport mode access
ALS1(config-if)#switchport access vlan 1111
ALS1(config-if)#no shutdown
```

```
ALS2(config)#interface F0/6
ALS2(config-if)#switchport host
ALS2(config-if)#switchport mode access
ALS2(config-if)#switchport access vlan 234
ALS2(config-if)#no shutdown
```

```

ALS2(config-if)#interface F0/15
ALS2(config-if)#switchport host
ALS2(config-if)#switchport mode access
ALS2(config-if)#switchport access vlan 1111
ALS2(config-if)#no shutdown

```

**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

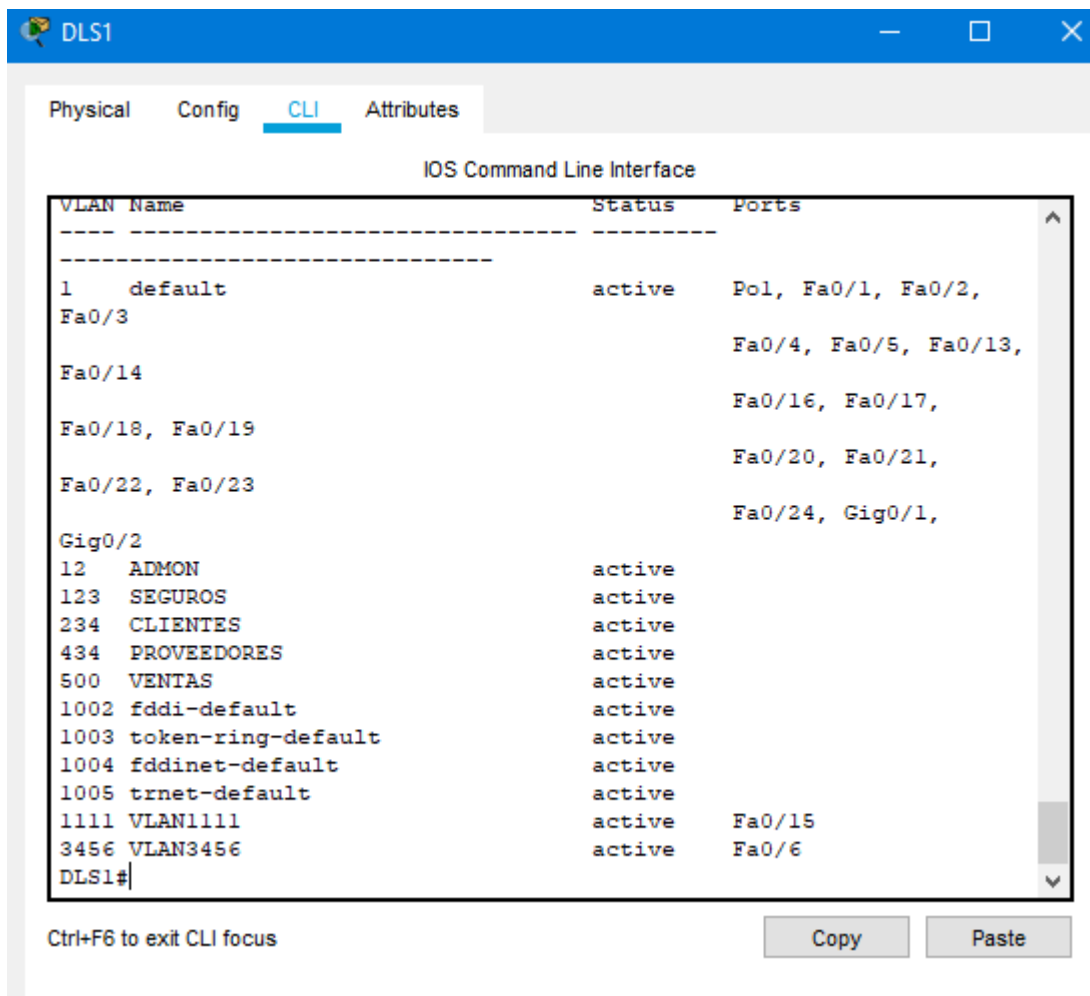


Figura 17: verificación VLAN DLS1

Por medio del comando “show vlan brief” se puede evidenciar la existencia de las VLAN estipuladas en cada uno de los conmutadores; también se puede observar que la VLAN 434 PROVEEDORES se encuentra “activa”.

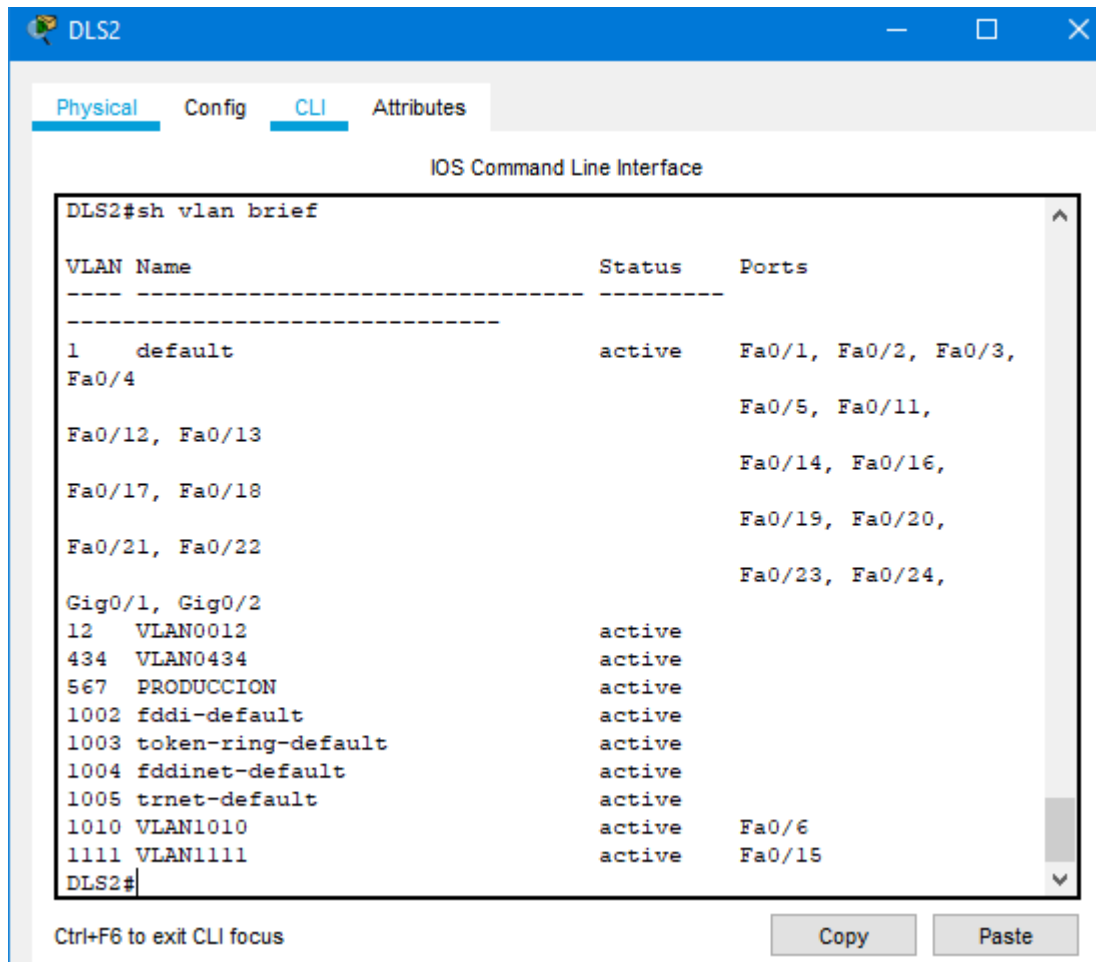


Figura 18: verificación VLAN DLS2

En la siguiente figura se puede evidenciar que sólo en DLS2 se encuentra disponible la VLAN 567 PRODUCCION

ALSI1

Physical **Config** CLI Attributes

IOS Command Line Interface

```

ALSI#sh vlan br
ALSI#sh vlan brief

```

VLAN Name	Status	Ports
1 default	active	Pol, Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/16, Fa0/17, Fa0/20, Fa0/21, Fa0/24, Gig0/1, Gig0/2
12 ADMON	active	
123 SEGUROS	active	
234 CLIENTES	active	
434 PROVEEDORES	active	
500 VENTAS	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	
1111 VLAN1111	active	Fa0/15
3456 VLAN3456	active	

ALSI#

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 19: verificación VLAN ALS1

```

ALS2#
ALS2#sh vlan bri
ALS2#sh vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4                    Fa0/5, Fa0/11,
Fa0/12, Fa0/13          Fa0/14, Fa0/16,
Fa0/17, Fa0/18          Fa0/19, Fa0/20,
Fa0/21, Fa0/22          Fa0/23, Fa0/24,
Gig0/1, Gig0/2
12    ADMON                  active
123   SEGUROS                 active
234   CLIENTES                active    Fa0/6
434   PROVEEDORES             active
500   VENTAS                  active
1002  fddi-default            active
1003  token-ring-default      active
1004  fddinet-default         active
1005  trnet-default           active
1111  VLAN1111                active    Fa0/15
3456  VLAN3456                 active
ALS2#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 20: verificación VLAN ALS2

A continuación se hace la verificación de la asignación de los puertos troncales a las VLAN; por medio del comando “show interfaces trunk” podemos observar todos los puertos que funcionan como trunk.

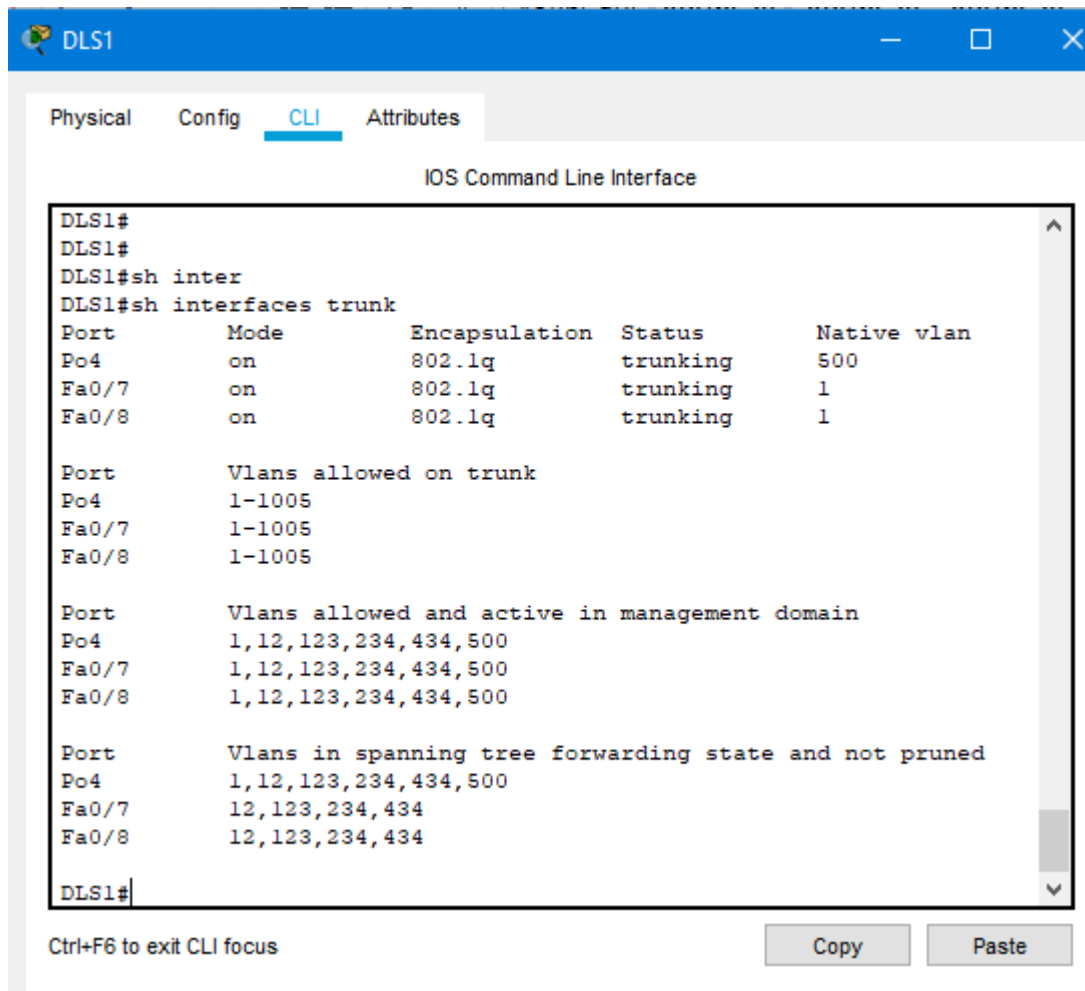


Figura 21: verificación interfaces DLS1

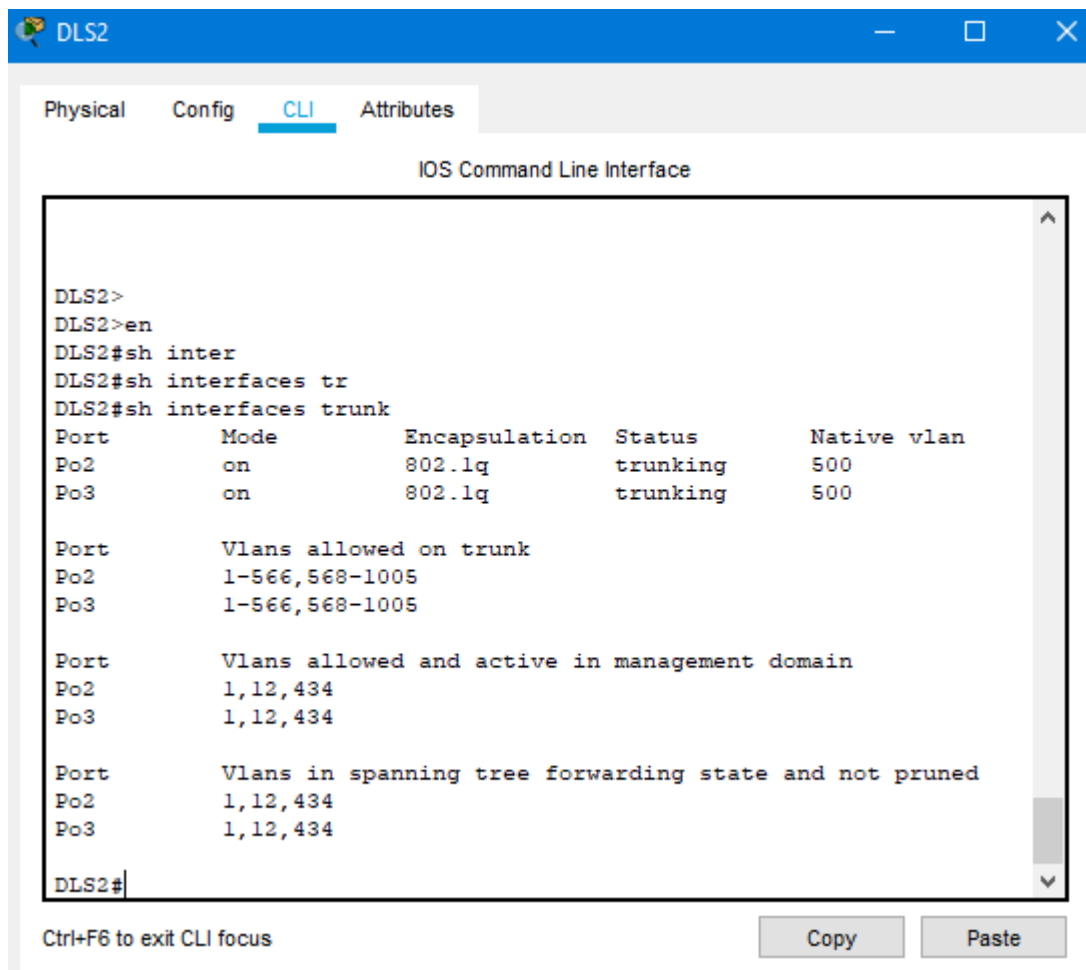


Figura 22: verificación interfaces DLS2.

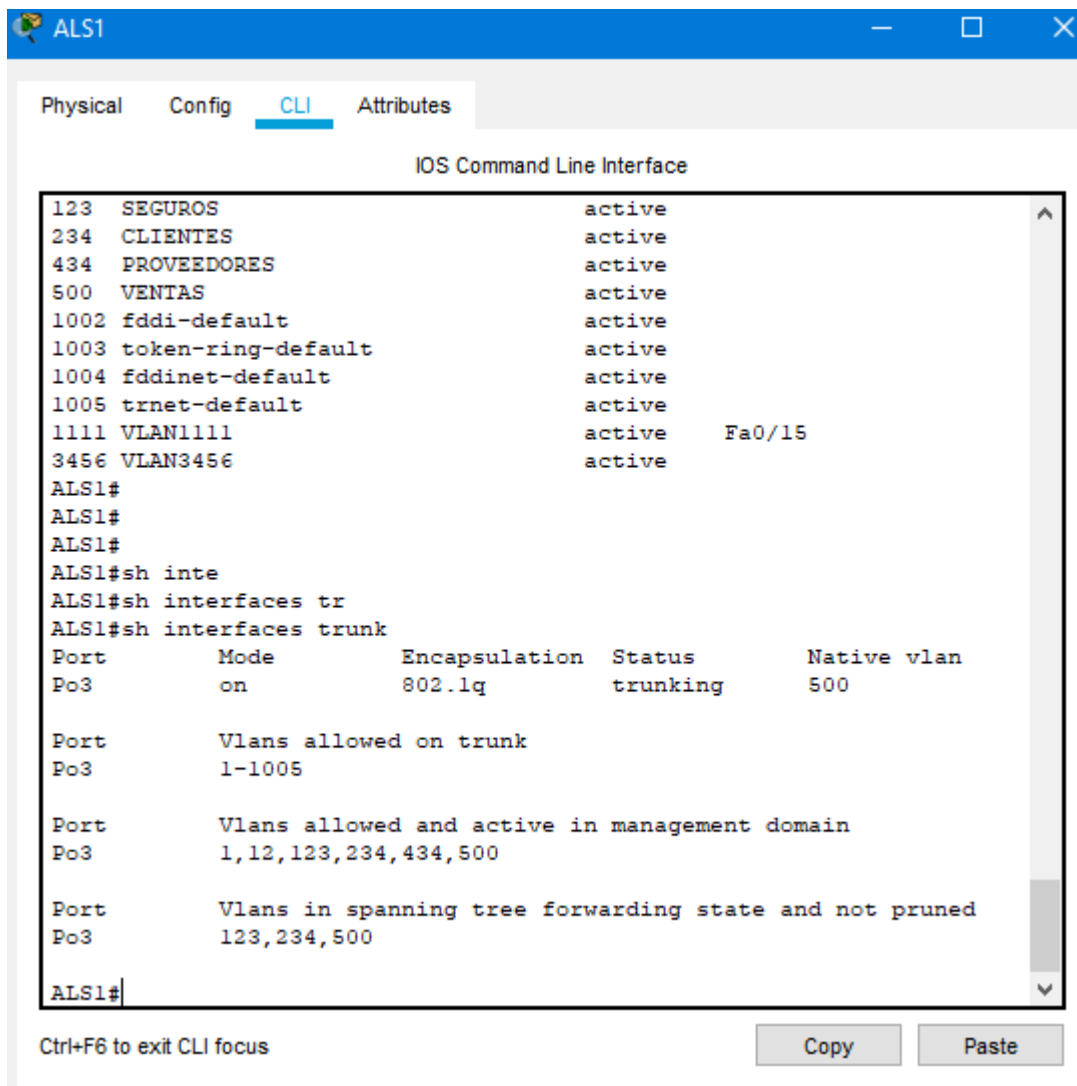


Figura 23: verificación interfaces ALS1.

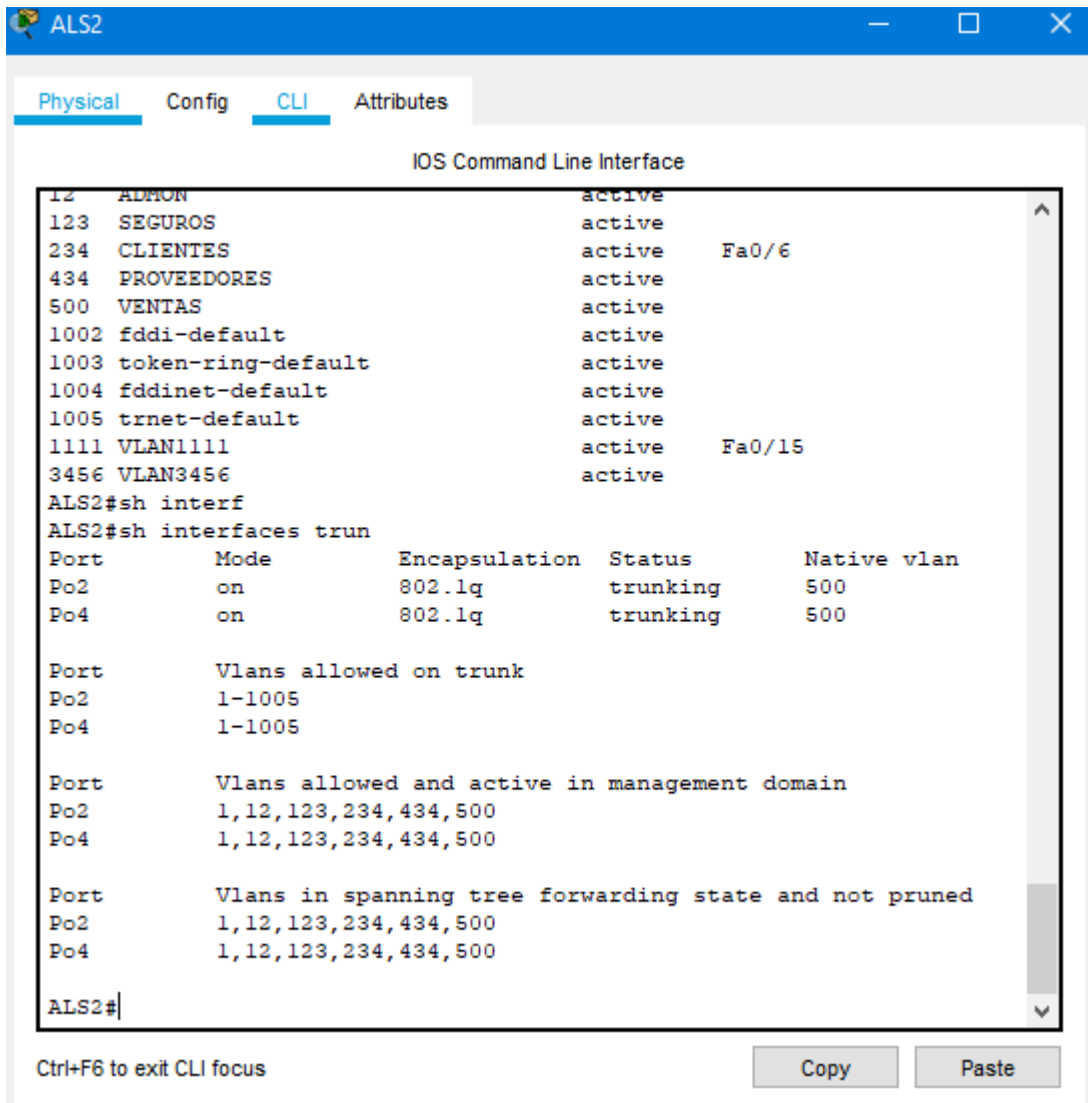


Figura 24: verificación interfaces ALS2.

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

Al ejecutar el comando “show etherchannel summary ” se logra evidenciar la correcta configuración del EtherChannel entre DLS1 y ALS1

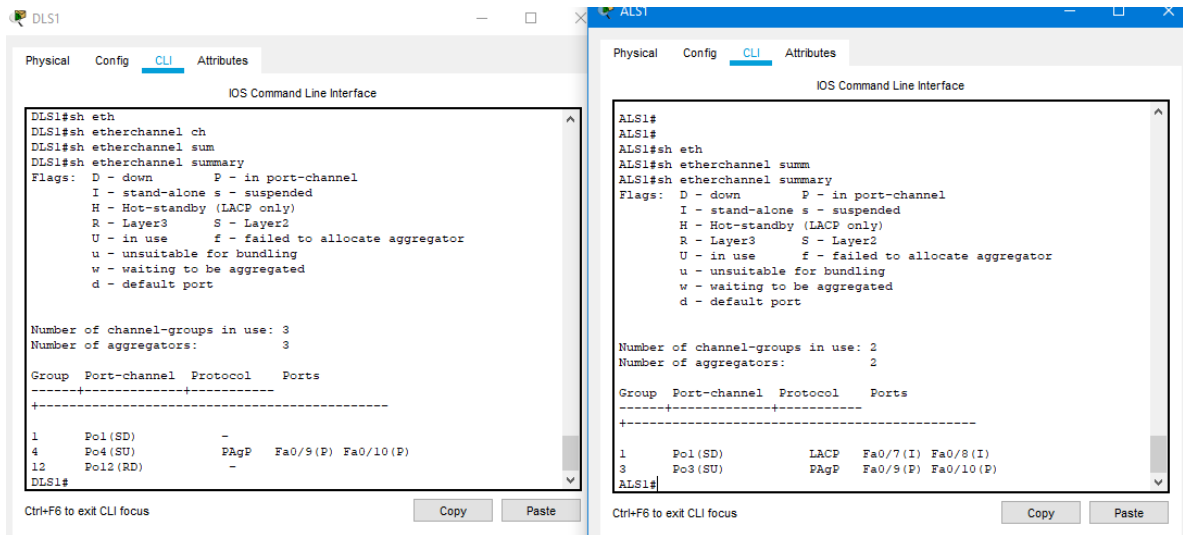


Figura 25: verificación ETHERCHANNEL en DLS1 Y ALS1.

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

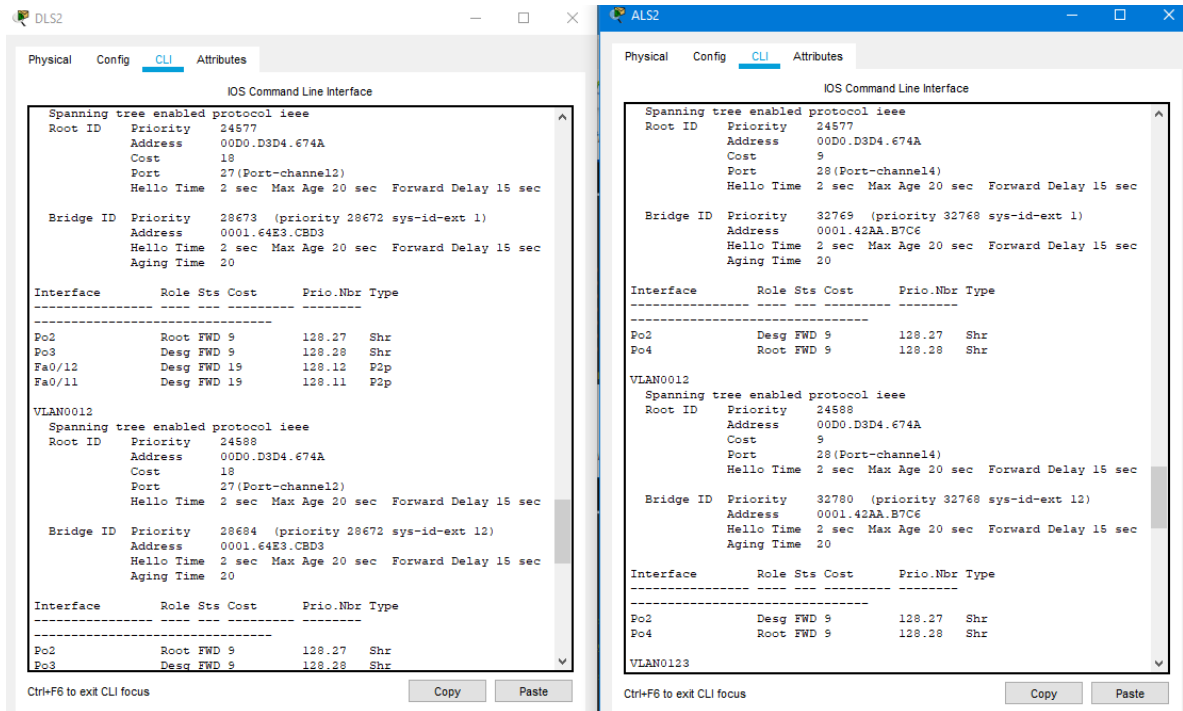


Figura 26: verificación Spanning-tree en DLS2 Y ALS2.

## CONCLUSIONES

Por medio del diplomado de profundización se adquieren conocimientos más concretos y enfáticos sobre el Routing and Switching en la tecnología de redes CISCO, por medio de la profundización se interactúa con plataformas simuladoras en implementación de redes, donde se realizan las pruebas y laboratorios requeridos en el diplomado.

Mediante el uso de balanceo de carga EIGRP se permite que un router utilice varias trayectorias a un destino al reenviar paquetes, con EIGRP es posible configurar el tráfico sobre enlaces con coste distinto utilizando el comando variance. Este mismo permite al administrador identificar el ámbito de la métrica incluyendo caminos adicionales con el uso del parámetro multiplicador.

Se puso en práctica las temáticas abordadas a lo largo del curso correspondiente a protocolos de Enrutamiento Avanzado, Implementación de soluciones soportadas en enrutamiento avanzado, configuración de sistemas de red soportados en VLANs y Administración, Seguridad y Escalabilidad en redes conmutadas.

Finalmente, se sustentó el desarrollo de cada escenario con los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de los comandos requeridos para cada caso, empleando la herramienta de simulación Packet Tracer.

## BIBLIOGRAFÍA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Inter VLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

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-NT1InMfy2rhPZHwEoWx>

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-NT1InMfy2rhPZHwEoWx>

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-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Routers and Routing Protocol Hardening. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>