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

Jhon Jairo Gomez Ramírez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA EN TELECOMUNICACIONES DE CALI 2021

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

Jhon Jairo Gomez Ramírez

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

DIRECTOR

JOHN HAROLD PEREZ CALDERON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA EN TELECOMUNICACIONES DE CALI 2021

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Jurado

_____
Firma del Jurado

Cali, 18 de Julio de 2021

AGRADECIMIENTOS

Mis agradecimientos inicialmente a Dios, que permitió durante este ciclo de mi vida dar continuidad con el proceso de aprendizaje en mi carrera profesional, Igualmente un agradecimiento a la institución Universidad Nacional y a Distancia UNAD que complemento mi formación con las temáticas vistas, para dar como cumplimiento uno de mis sueños como profesional, un agradecimiento notable a todos los compañeros que a lo largo de la formación se dispusieron para aclarar y compartir de manera virtual cada aprendizaje, y por otro lado a cada tutor que ante su profesionalismo dedicaron de su tiempo para aclarar las inquietudes de sus alumnos.

Por ultimo agradezco a toda mi familia por el apoyo en este proceso, que incito de manera alentadora, para no desfallecer a lo largo de la formación académica, a fin de dar por culminado mi carrera universitaria.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Escenario Parte 1:

LISTA DE FIGURAS

Escenario Parte 2:

GLOSARIO

EIGRP: Protocolo de enrutamiento dinámico para redes IP basado en el vector distancia obteniendo información de los vecinos conectados directamente.

EtherChannel: (Port-channels) Protocolo que hace posible agregar o unificar enlaces físicos en un solo medio lógico, permitiendo sumar la velocidad de cada enlaces físico en uno solo.

OSPF: Protocolo de enrutamiento dinámico para redes IP basado en algoritmos que facilitan la entrega de paquetes por el camino más corta.

Spanning tree: Protocolo que funciona en capa 2, su objetivo es controlar los enlaces redundantes a fin de evitar loop en la red.

VLAN: Red de área local virtual, su función principal es dividir de manera lógica una red física en varios grupos de redes usando el mismo medio físico de distribución.

VTP: Protocolo de mensajes usado para centralizar la administración de VLAN, permitiendo desde un dominio central de VLAN distribuir las VLAN en los demás nodos sin necesidad de ingresa a cada nodo a modificar las cada VLAN.

RESUMEN

En el presente documento contextualiza el desarrollo final del diplomado de profundización en CISCO CCNP, guiado por la universidad Nacional Abierta y a Distancia UNAD. Este trabajo se divide en dos fases de implementación, la cual permite abarcar de manera general todos los temas visto a lo largo del diplomado.

Con la utilización de dos herramientas prácticas como (Cisco Packet Tracer y GNS3) facilitaron el desarrollo de los esquemas de red propuestos por diplomado, de esta manera aplicar conocimiento adquirido de routing y switch.

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

ABSTRACT

In this document he contextualizes the final development of the in-depth diploma at CISCO CCNP, guided by the National Open and Distance University UNAD. This work is divided into two implementation phases, which allows us to cover in a general way all the topics seen throughout the course.

With the use of two practical tools such as (Cisco Packet Tracer and GNS3) they facilitated the development of the network schemes proposed by the graduate, in this way applying knowledge acquired from routing and switch.

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

INTRODUCCION

En el presente trabajo se desarrolló con el fin de evaluar de manera práctica y conceptual los temas vistos durante el proceso de formación del diplomado de profundización de CISCO CCNP. Permitiendo aplicar las habilidades obtenidas en los dos escenarios propuestos, como una primera fase orientada a ambientes de capa 3 y la segunda fase a ambientes de capa 2, con una única finalidad de contextualizar todo lo aprendido de cara a entornos totalmente reales.

En el entorno de capa 3 logramos aplicar protocolos de enrutamiento dinámico permitiendo comunicar un sistema autónomo EIGRP con un área de OSPF aplicando las buenas practicas obtenidas de manera conceptual.

Para el entorno de capa 2 observamos en gran profundidad la aplicación de protocolos como Etherchannel, troncalizacion de puertos, Spanning tree e implantación de un servidor VTP, esto facilita ampliar anchos de banda, distribución de redes y administración centralizada de VLAN, además de garantizar la disponibilidad de los enlaces.

DESARROLLO DE LOS DOS ESCENARIOS

ESCENARIO PRELIMINAR

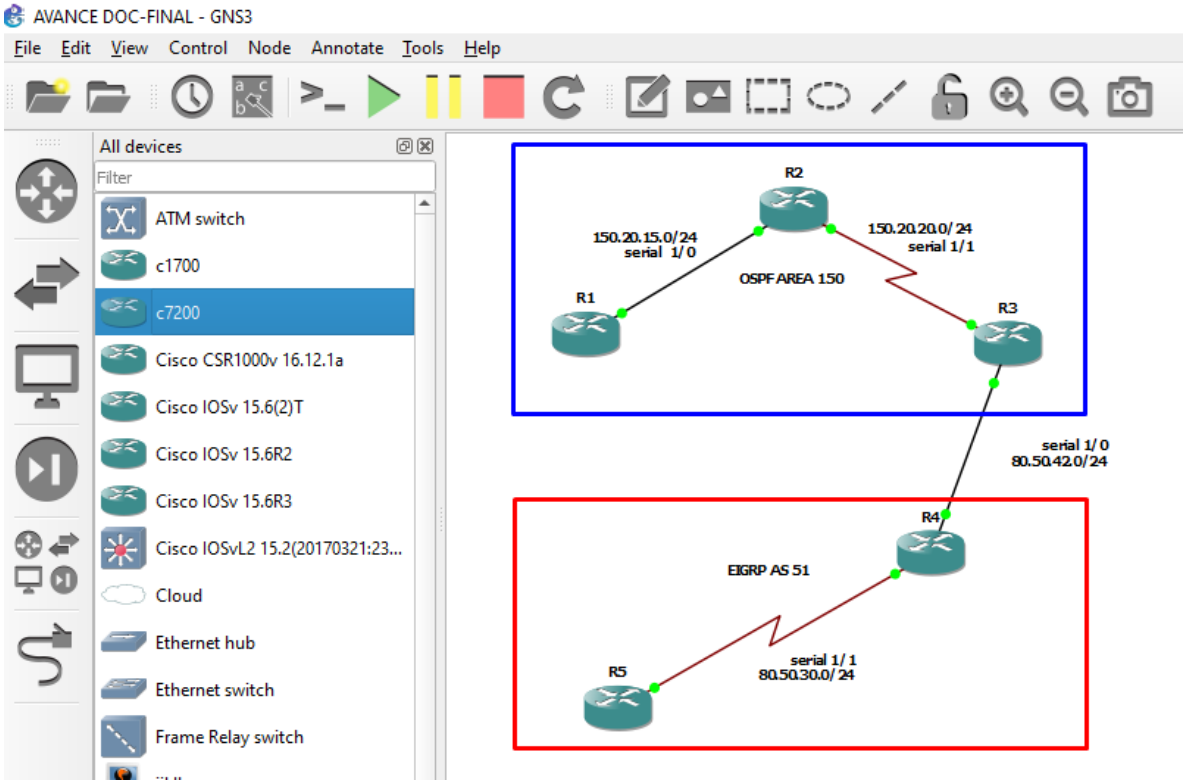

Figura 1. Escenario preliminar

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 Hostname

   Se realizó configuración del Hostname se R1 de esta manera para el resto de dispositivos.

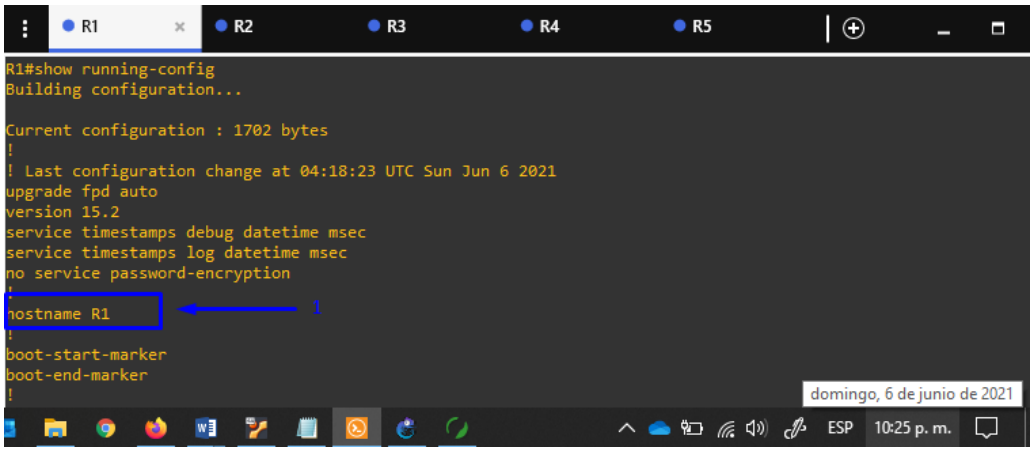

Figura 2. Configuración Hostname R1

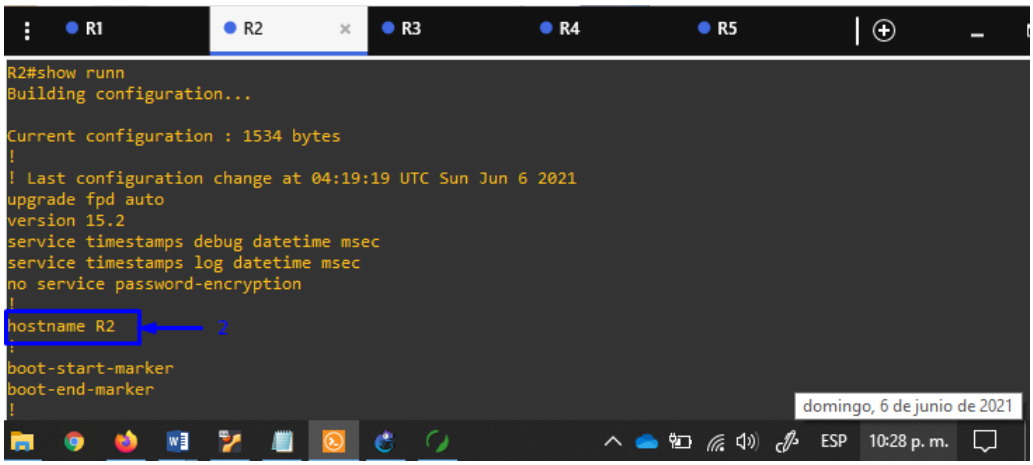

Figura 3. Configuración Hostname R2

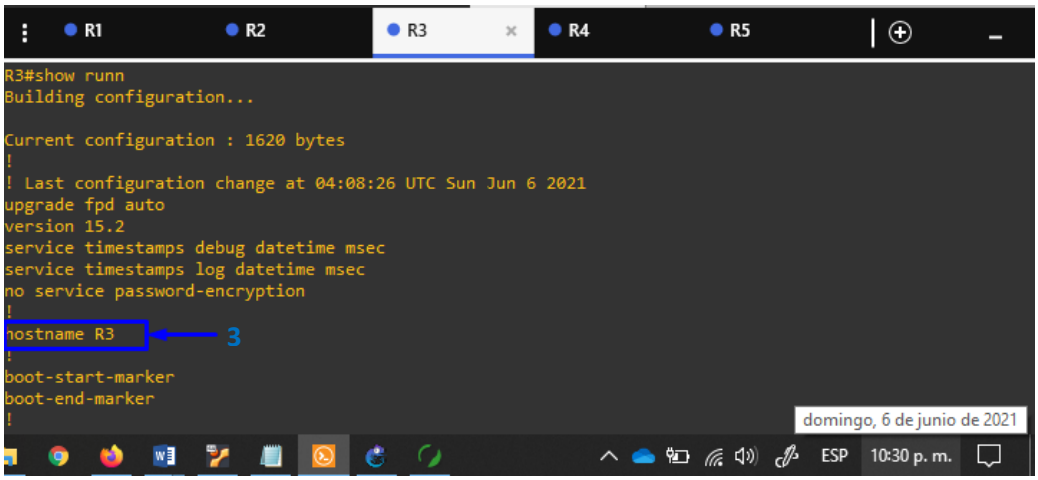

Figura 4. Configuración Hostname R3

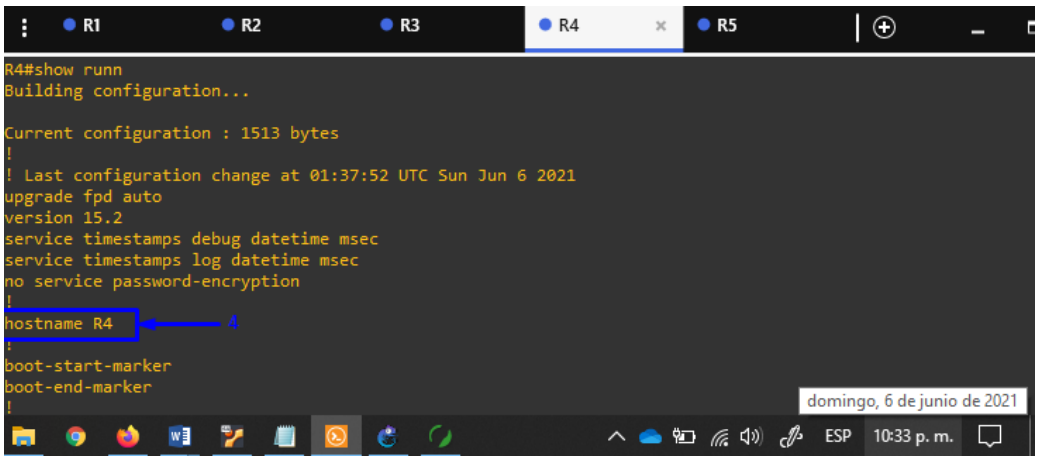

Figura 5. Configuración Hostname R4

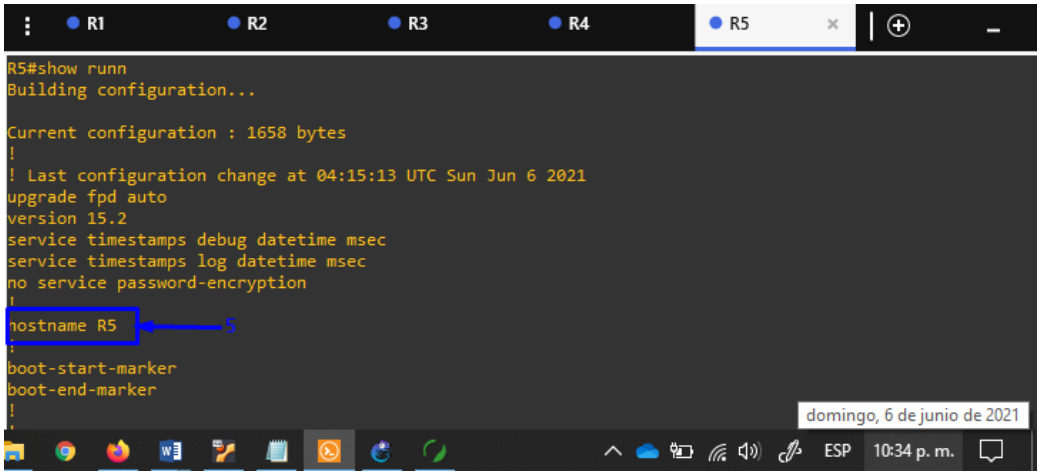

Figura 6. Configuración Hostname R5

Configuración Interfaces

Se realiza asignación de Ip y habilitación de cada una con el comando no shutdown.

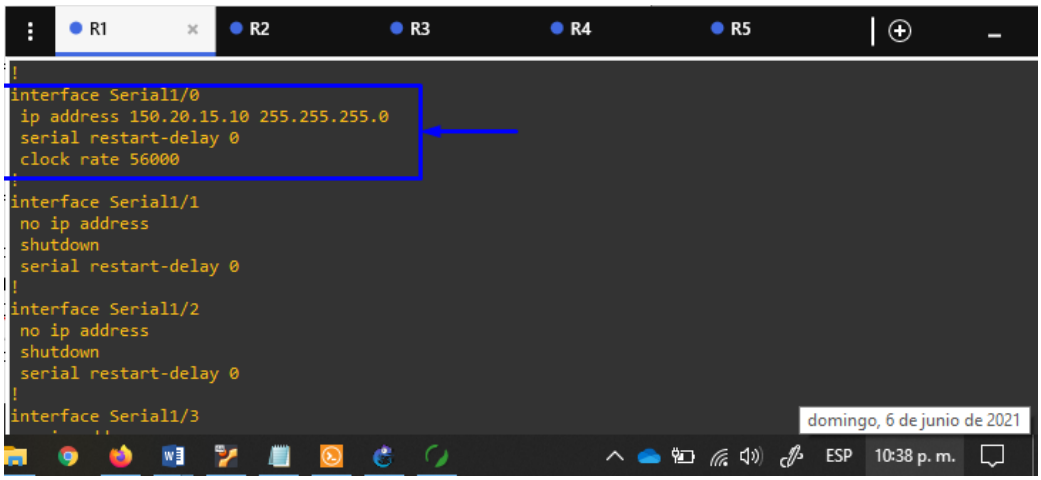

Figura 7. Configuración Interface R1

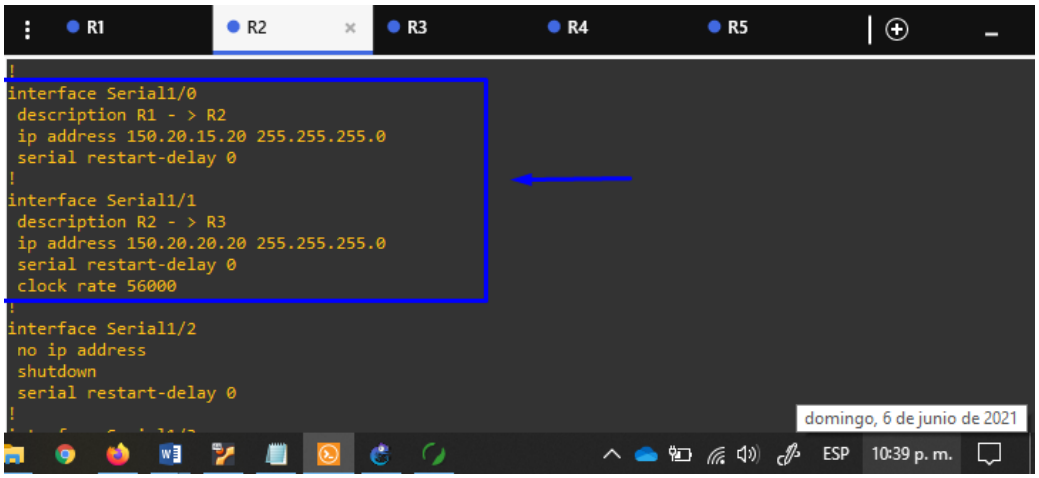

Figura 8. Configuración Interface R2

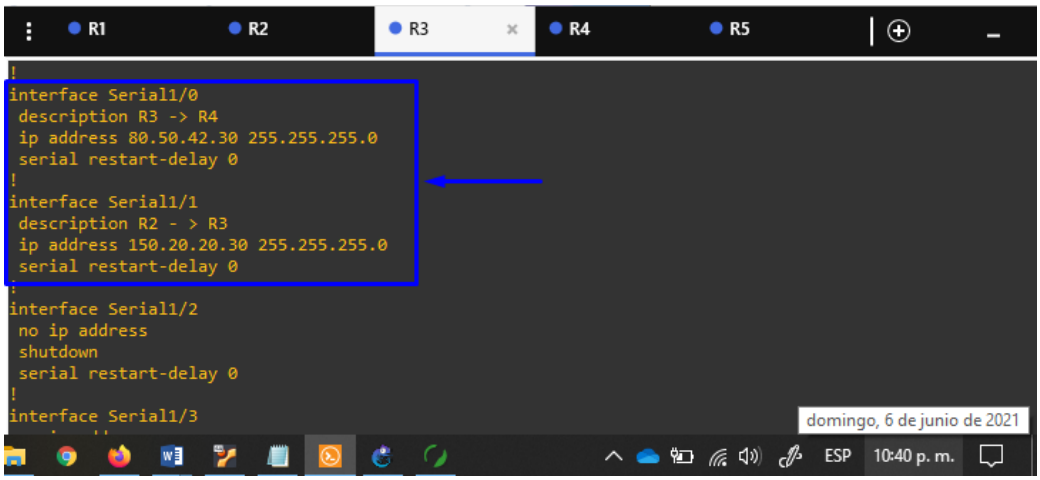

Figura 9. Configuración Interface R3

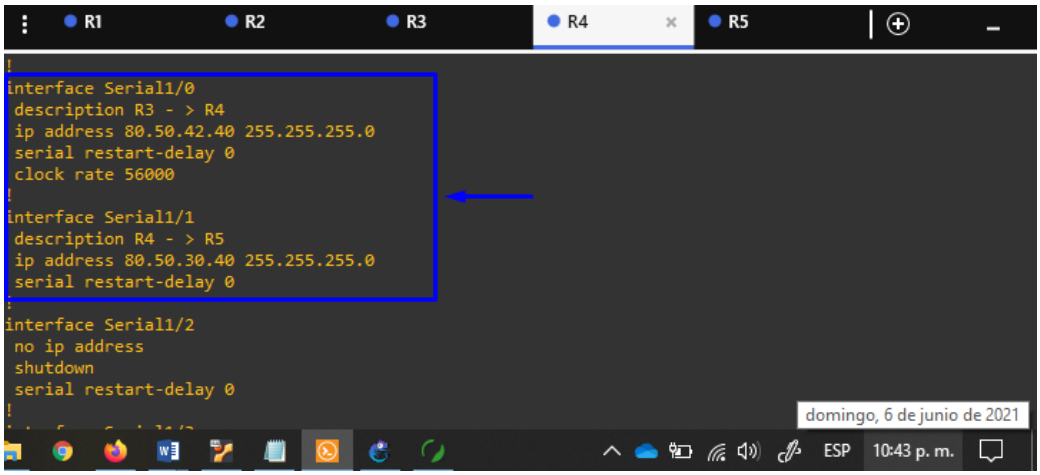

Figura 10. Configuración Interface R4

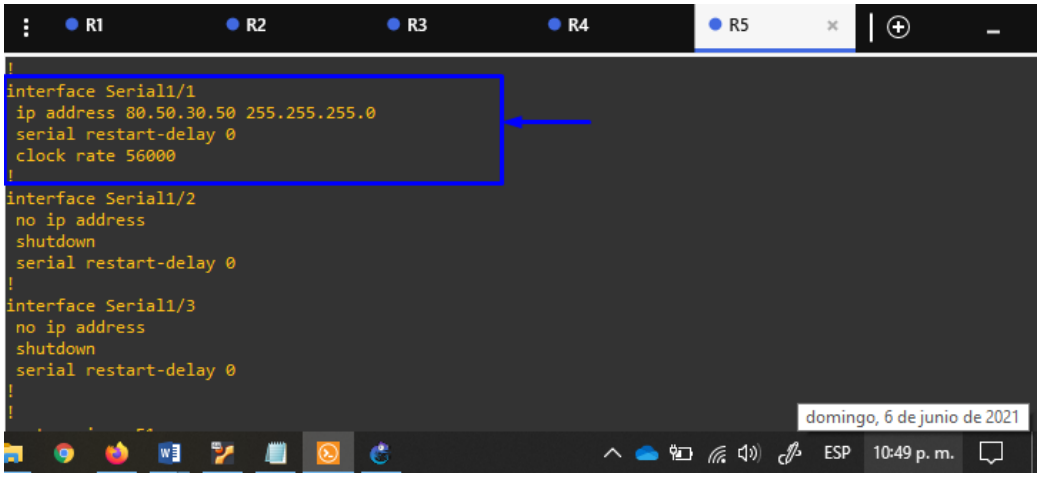

Figura 11. Configuración Interface R5

Configuración Protocolo OSPF

Se configura el protocolo de enrutamiento dinámico para habilitarlo con el comando router(config)# router ospf <id_proceso>.

Definiremos las redes que se enviaran los mensajes de actualización de las rutas con el comando router(config-router)# network <dirección_red> <máscara_wildcard> area<id_área>.

Luego definimos la área que será el que determinaría el Límite de mi Router Backend de exposición a la actualización de estados de los link.

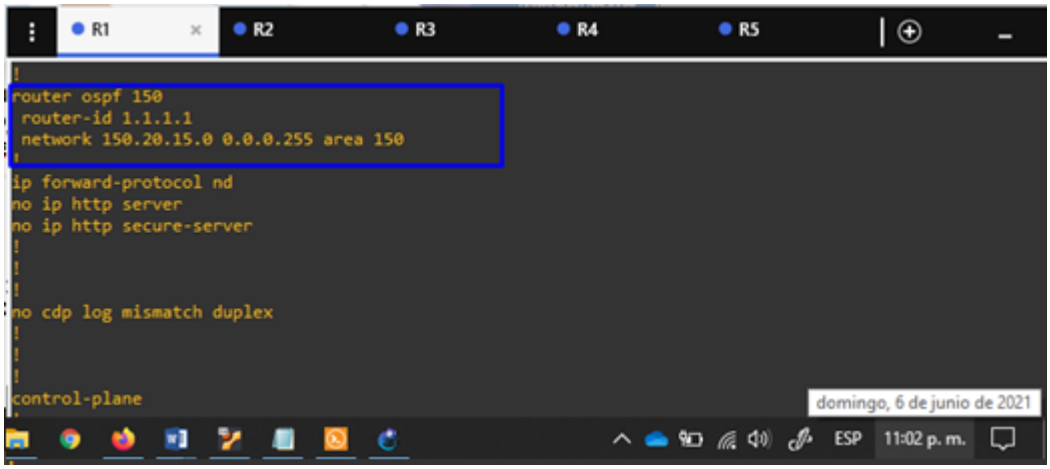

Figura 12. Configuración Protocolo OSPF R1

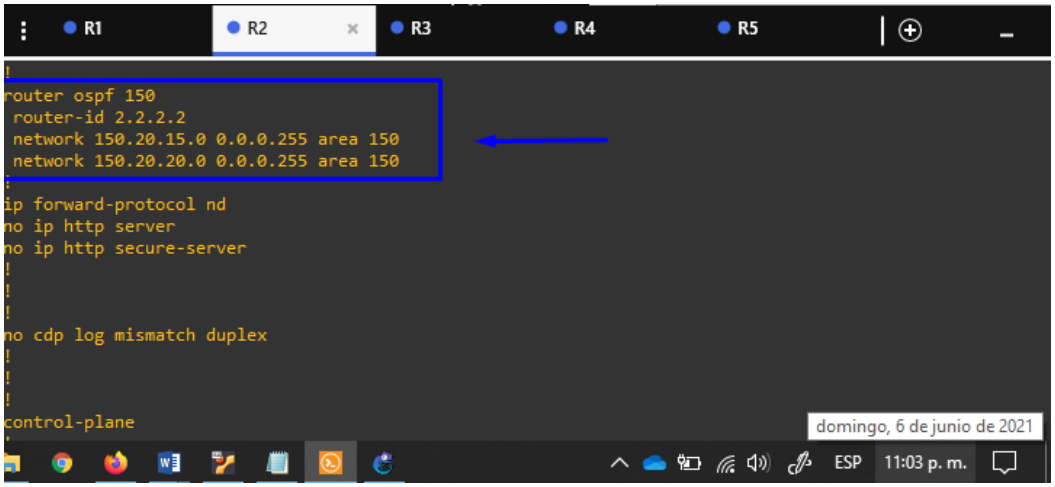

Figura 13. Configuración Protocolo OSPF R2

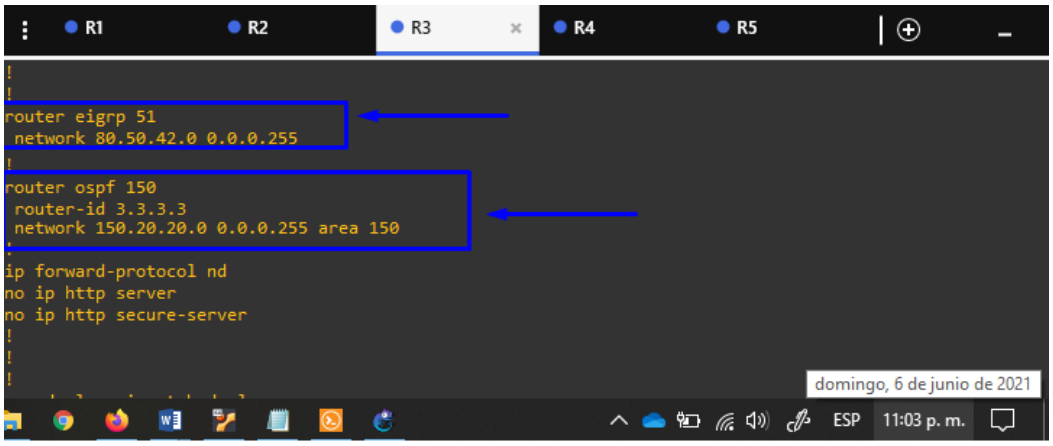

Figura 14. Configuración Protocolo OSPF R3

Configuración Protocolo EIGRP

Se configura el protocolo de enrutamiento dinámico para habilitarlo con el comando en mención y que define el sistema autónomo (config)# router eigrp <id_AS>.
Definiremos las redes que se enviaran los mensajes de actualización de las rutas con el comando router(config-router)# network <dirección_red> <máscara_wildcard>

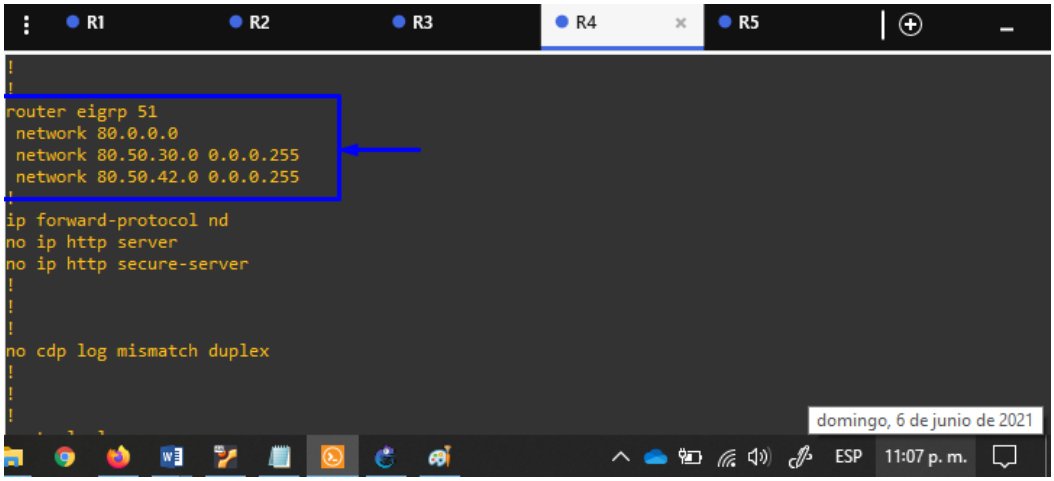

Figura 15. Configuración Protocolo EIGRP R4

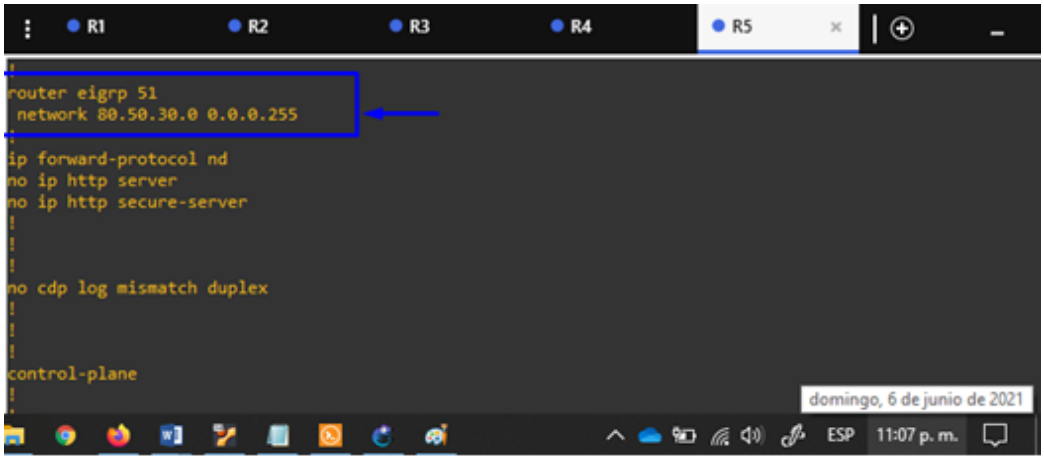

Figura 16. Configuración Protocolo EIGRP R5

Pruebas de conectividad

Router R1 ping Router R5

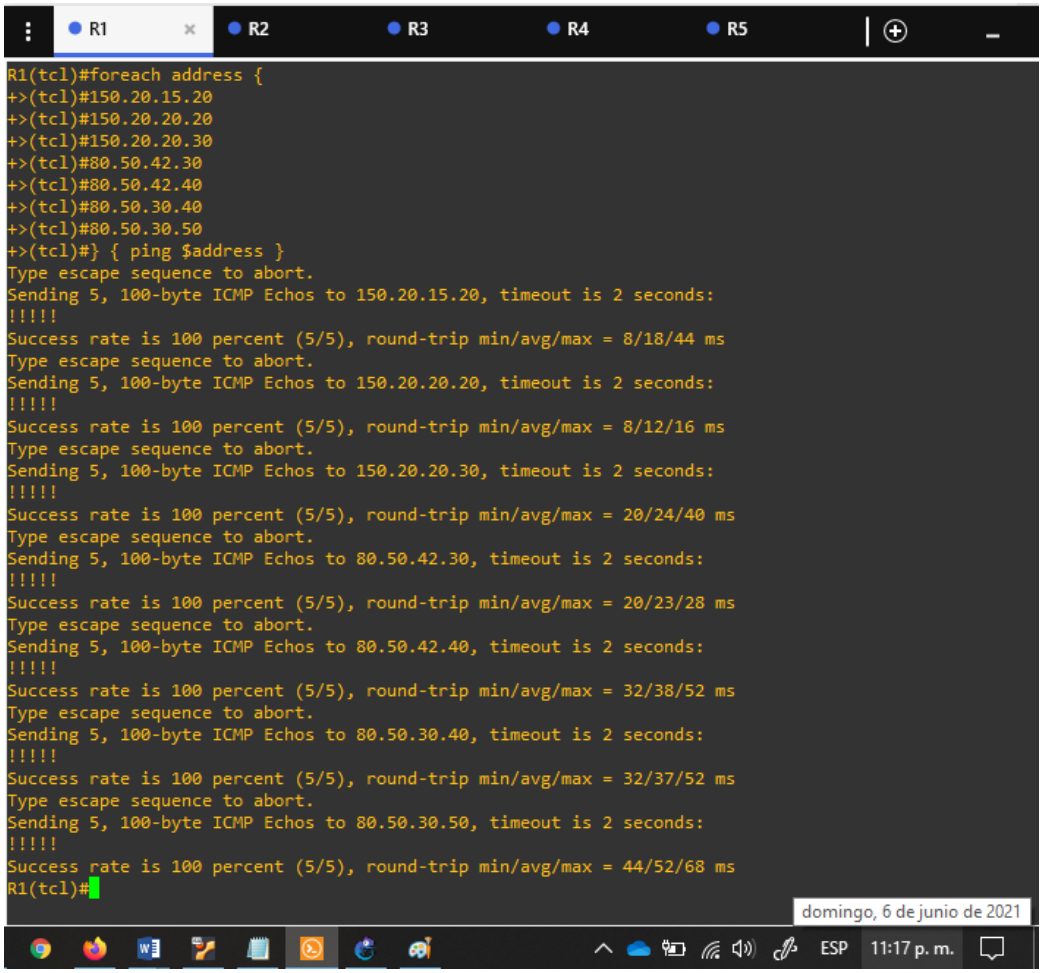

Figura 17. Pruebas de conexión R1 a R5

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 150de OSPF.

   Configuración Interfaces Loopback

   Se realiza asignación de Ip y habilitación de cada una con el comando no shutdown.

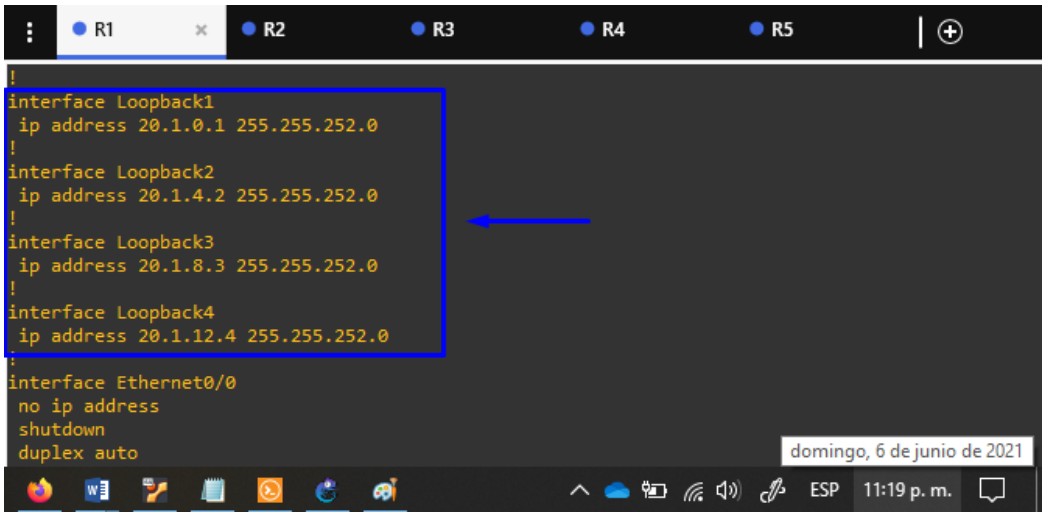

Figura 18. Configuración Interfaces Loopback R1

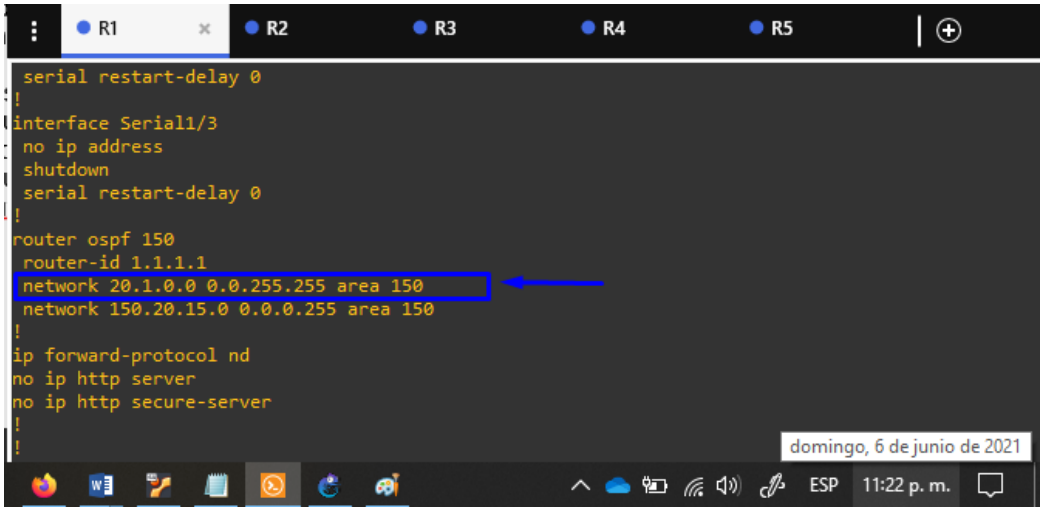

Figura 19. Configuración redes directamente conectadas R1 ospf

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.

   Configuración Interfaces Loopback
   Se realiza asignación de Ip y habilitación de cada una con el comando no shutdown.

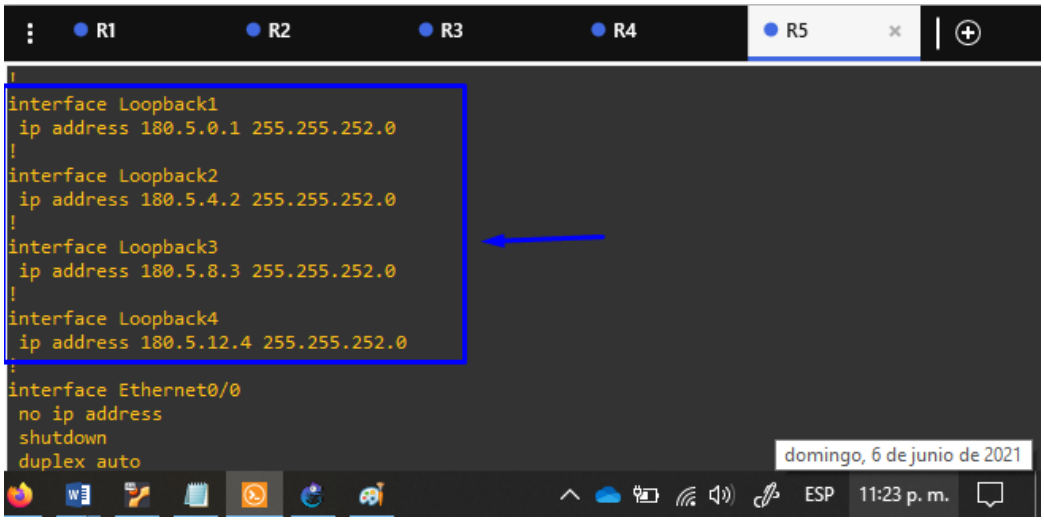

Figura 20. Configuración Interfaces Loopback R5

Figura 21. Configuración redes directamente conectadas R5 ospf

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.

   Pruebas de Validación de rutas
   Se identifica las rutas que son aprendidas por el Router 3 por los protocolos OSPF y EIGRP al ver la tabla de enrutamiento actualizada.

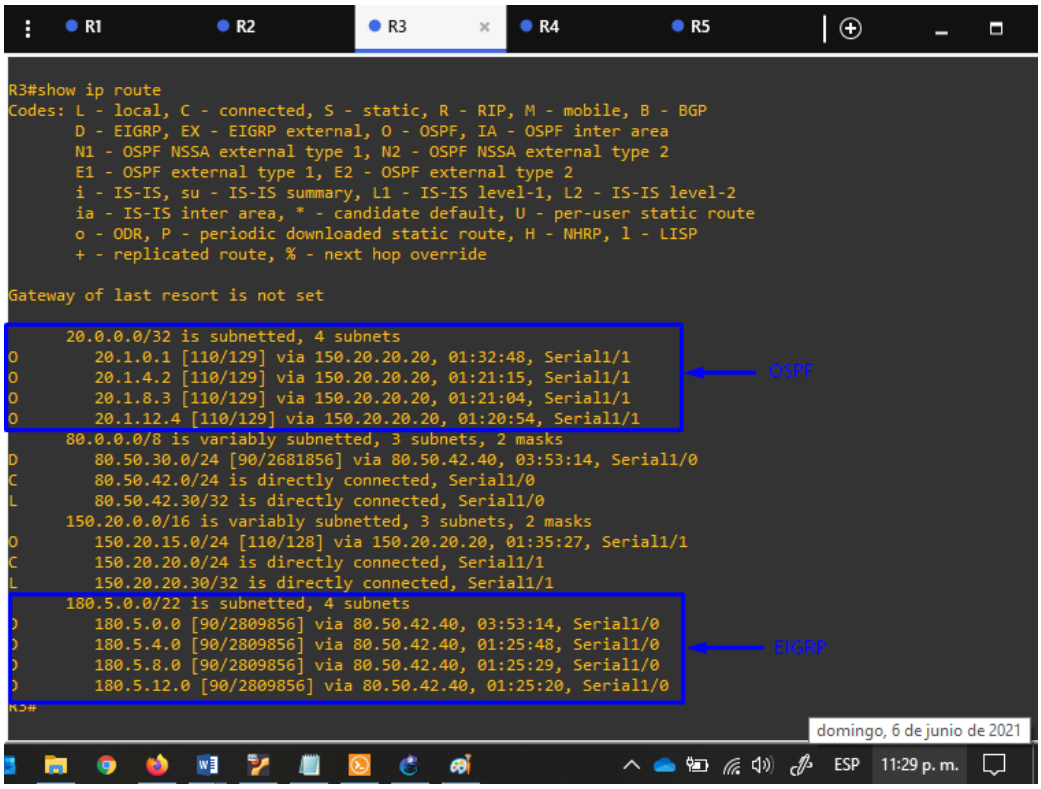

Figura 22. Pruebas de Validación de rutas R3

5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 80000y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

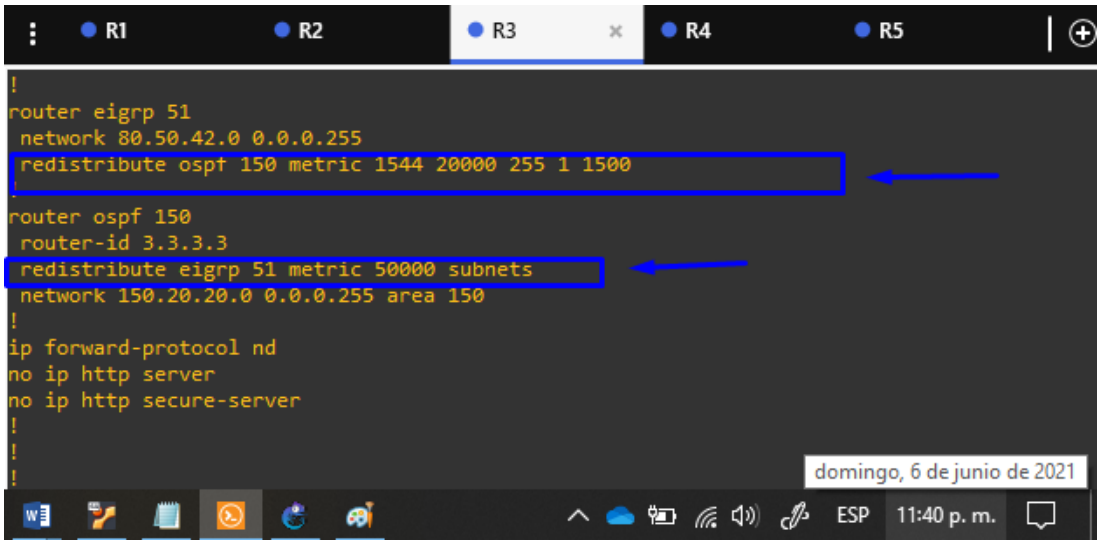

Figura 23. Configuración redistribución de rutas EIGRP en OSPF R3

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

Pruebas de Validación de rutas
Se identifica las rutas que son aprendidas por el Router R1 y R5 por los protocolos OSPF y EIGRP existen en el opuesto de cada routes con el sistema autónomo.

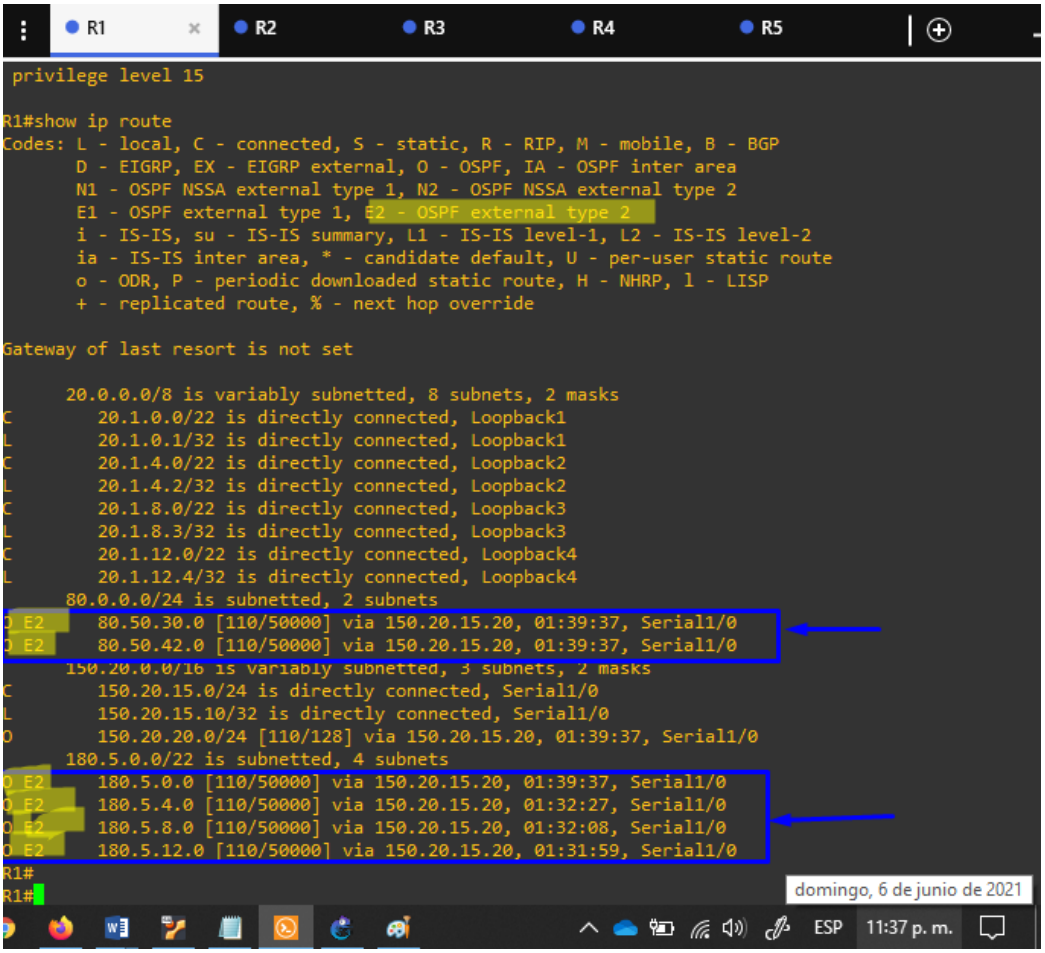

Figura 24. Validación de rutas aprendidas OSPF R1.

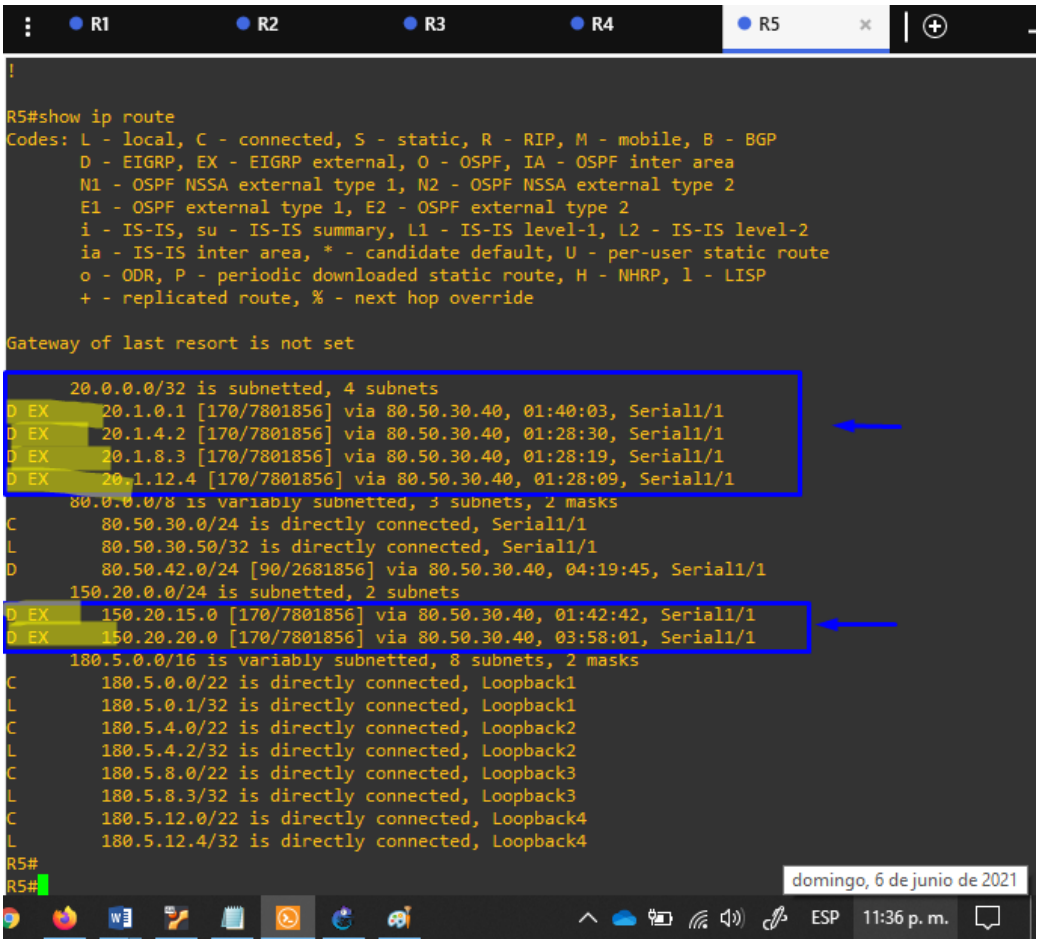

Figura 25. Validación de rutas aprendidas EIGRP R5.

SEGUNDO ESCENARIO

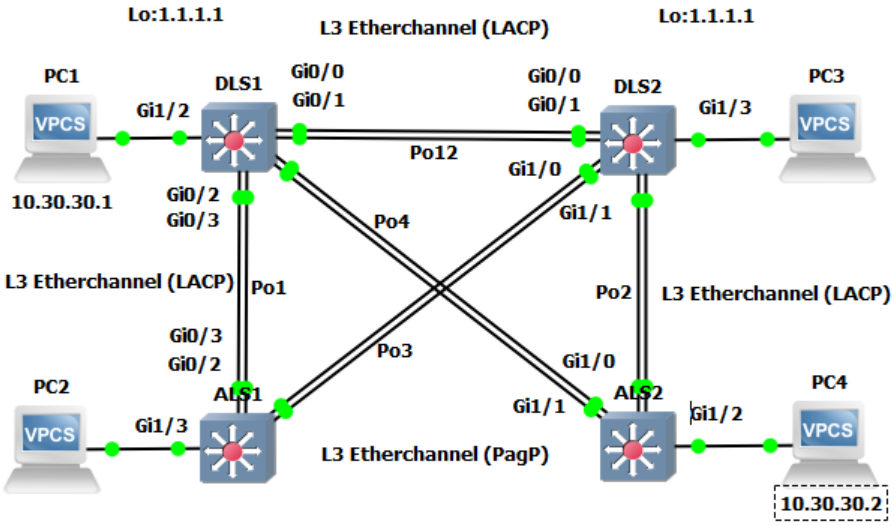

Figura 26. Segundo Escenario

Parte 1: Se Configuro la red de acuerdo a las especificaciones del esquemas de la figura 26.

a. A continuación Desactivaremos todas las interfaces en cada switch.

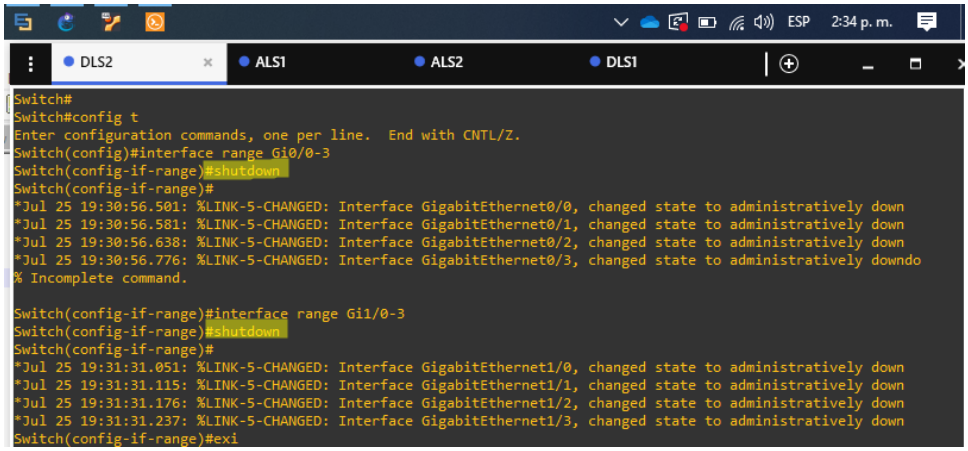

Figura 27. Validación de Interfaces deshabilitadas DSL2

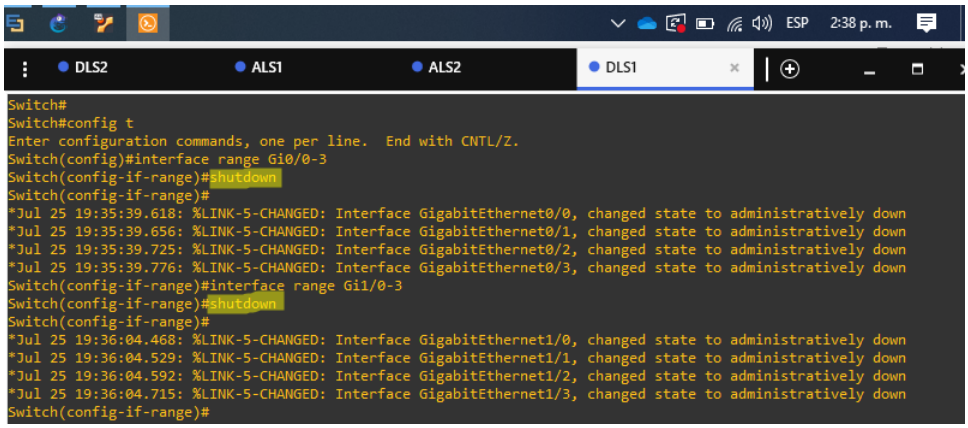

Figura 28. Validación de Interfaces deshabilitadas DSL1

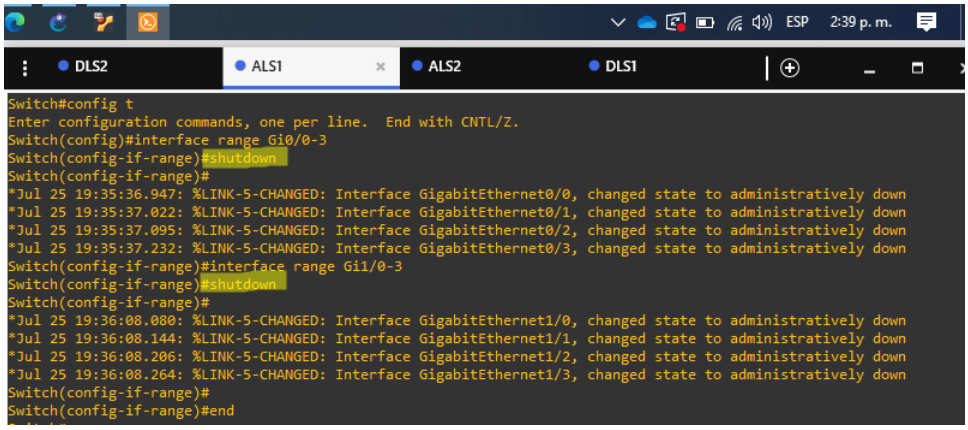

Figura 29. Validación de Interfaces deshabilitadas ASL1

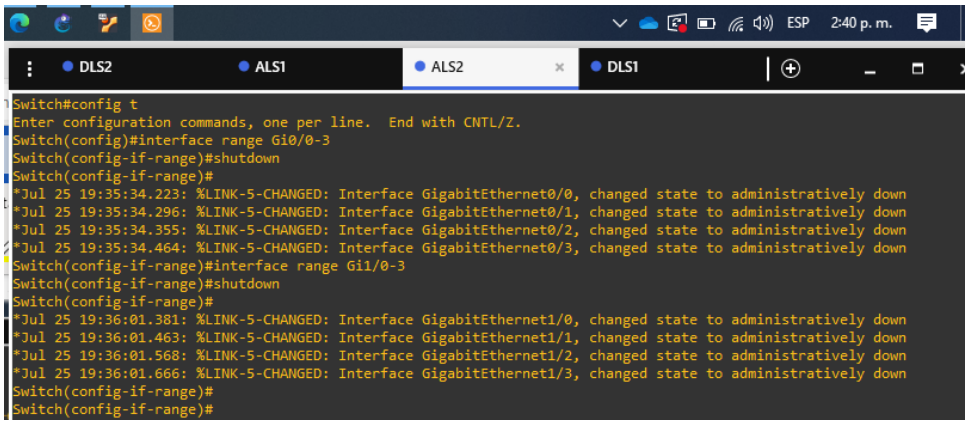

Figura 30. Validación de Interfaces deshabilitadas ASL2

b. Asignar un nombre a cada switch acorde con la figura 26 establecida.

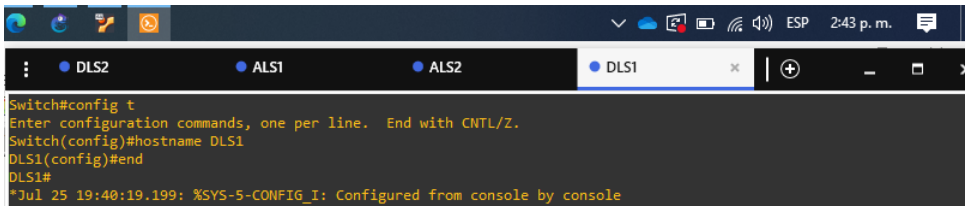

Figura 31. Configuración hostname DLS1

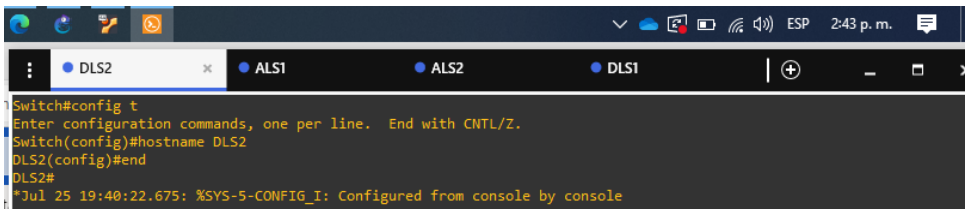

Figura 32. Configuración hostname DLS2

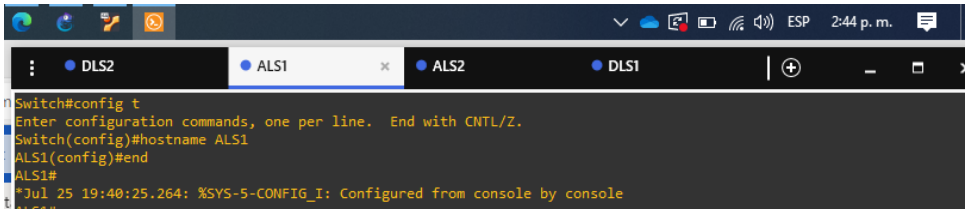

Figura 33. Configuración hostname ALS1

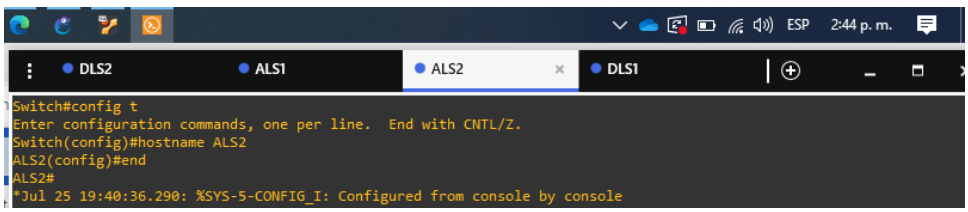

Figura 34. Configuración hostname ALS2

c. Se configura los puertos troncales y Port-channels tal como se muestra en la figura 26.

1. La conexión entre DLS1 y DLS2 será aplicada en 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.

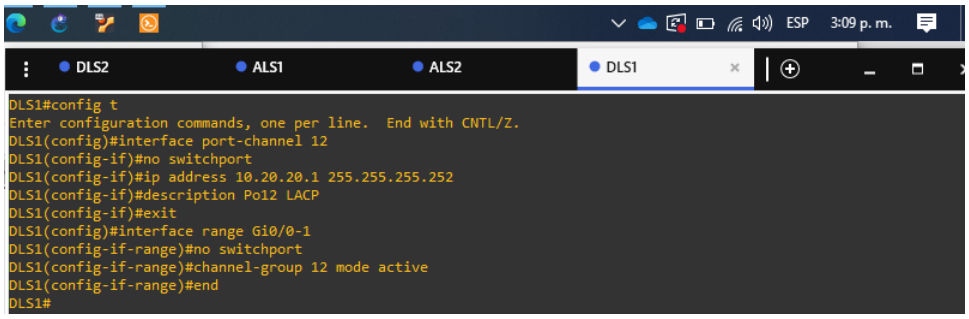

Figura 35. Configuración de Port-channels Gi0/0-1 en L3 DLS1 usando LACP

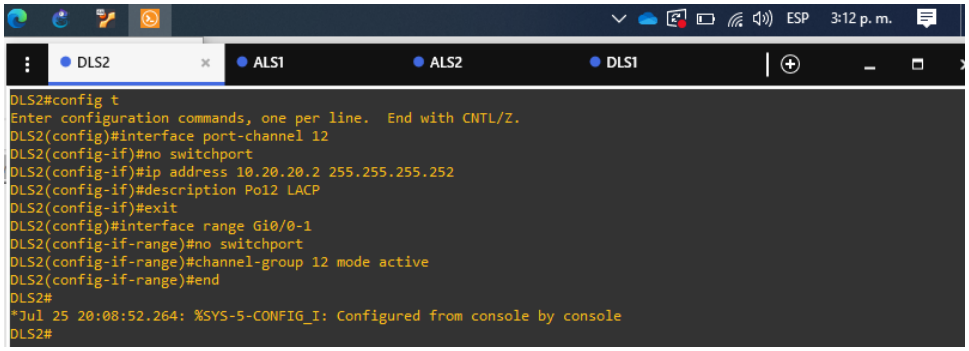

Figura 36. Configuración de Port-channels Gi0/0-1 en L3 DLS2 usando LACP

2. Los Port-channels en las interfaces Gi0/2 y Gi0/3 utilizarán LACP.

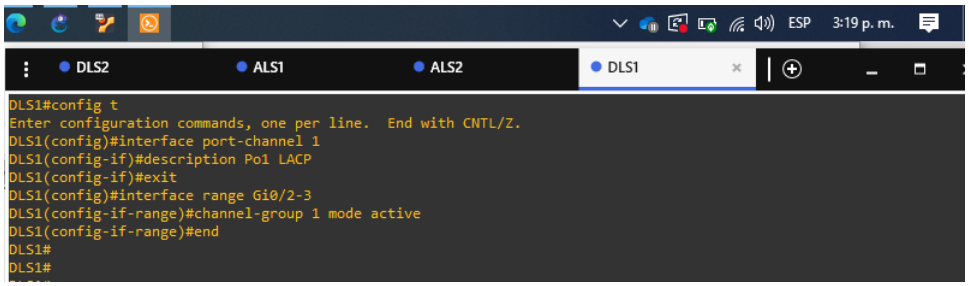

Figura 37. Configuración de Port-channels Gi0/2-3 DLS1 usando LACP

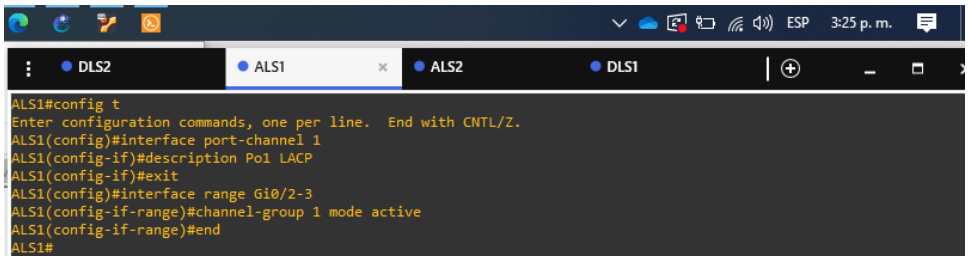

Figura 38. Configuración de Port-channels Gi0/2-3 ALS1 usando LACP

Figura 39. Configuración de Port-channels Gi0/2-3 DLS2 usando LACP

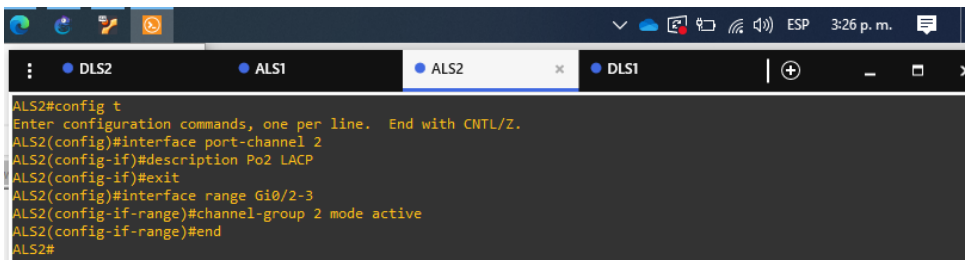

Figura 40. Configuración de Port-channels Gi0/2-3 ALS2 usando LACP

3. Los Port-channels en las interfaces Gi1/0 y Gi1/1 utilizará PAgP.

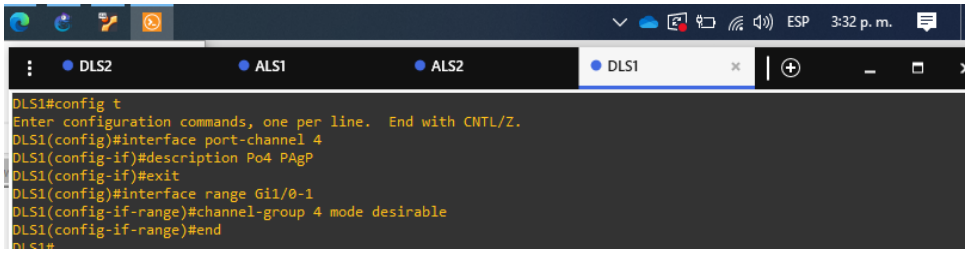

Figura 41. Configuración de Port-channels Gi1/0-1 DLS1 usando PAgP

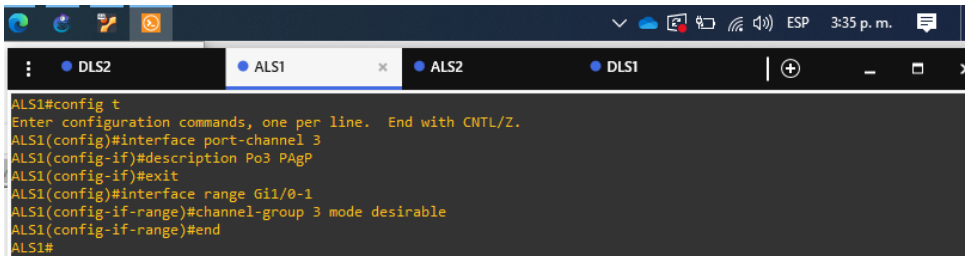

Figura 42. Configuración de Port-channels Gi1/0-1 ALS1 usando PAgP

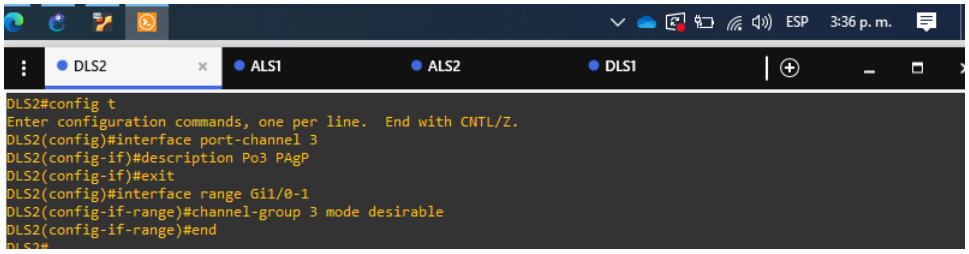

Figura 43. Configuración de Port-channels Gi1/0-1 DLS2 usando PAgP

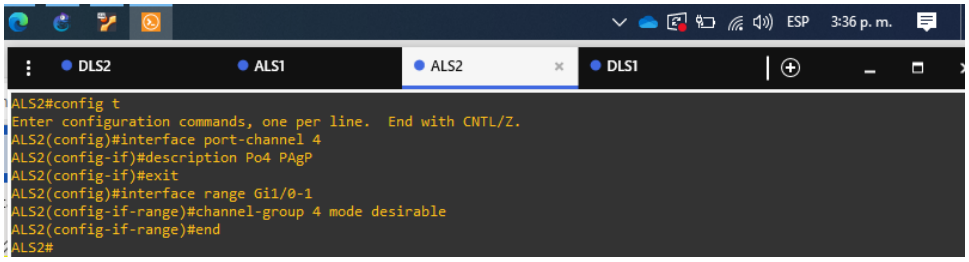

Figura 44. Configuración de Port-channels Gi1/0-1 ALS2 usando PAgP

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

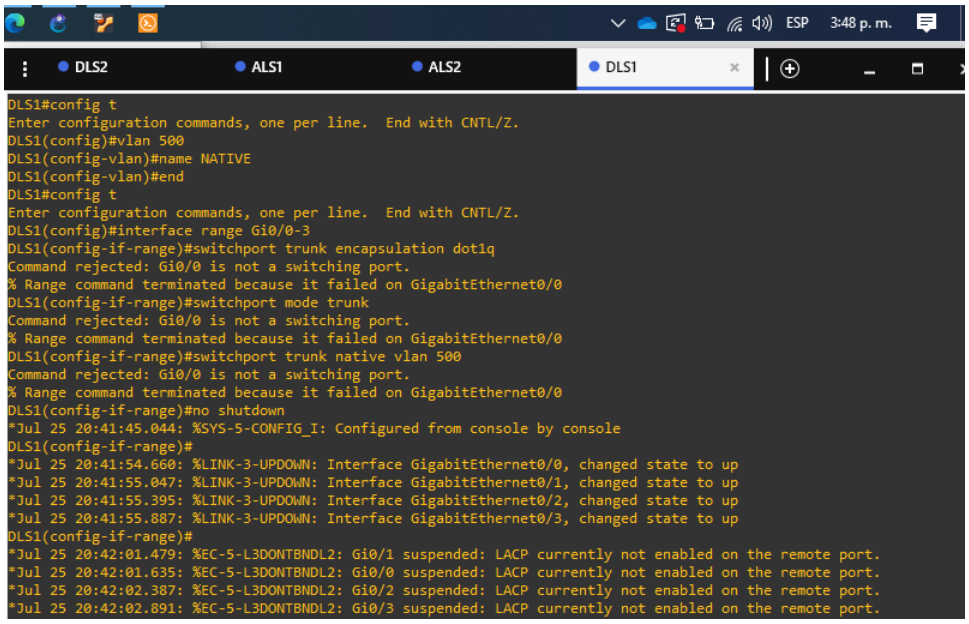

Figura 45.Configuración VLAN nativa 500 en los puerto trunk Gi0/0-3 DLS1

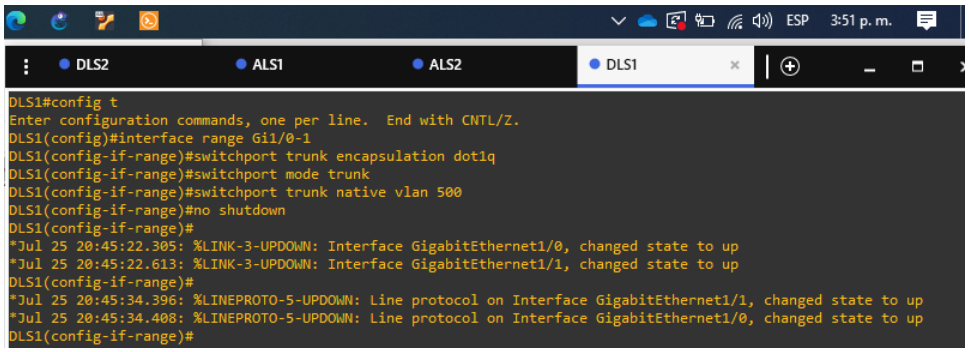

Figura 46.Configuración VLAN nativa 500 en los puerto trunk Gi1/0-1 DLS1

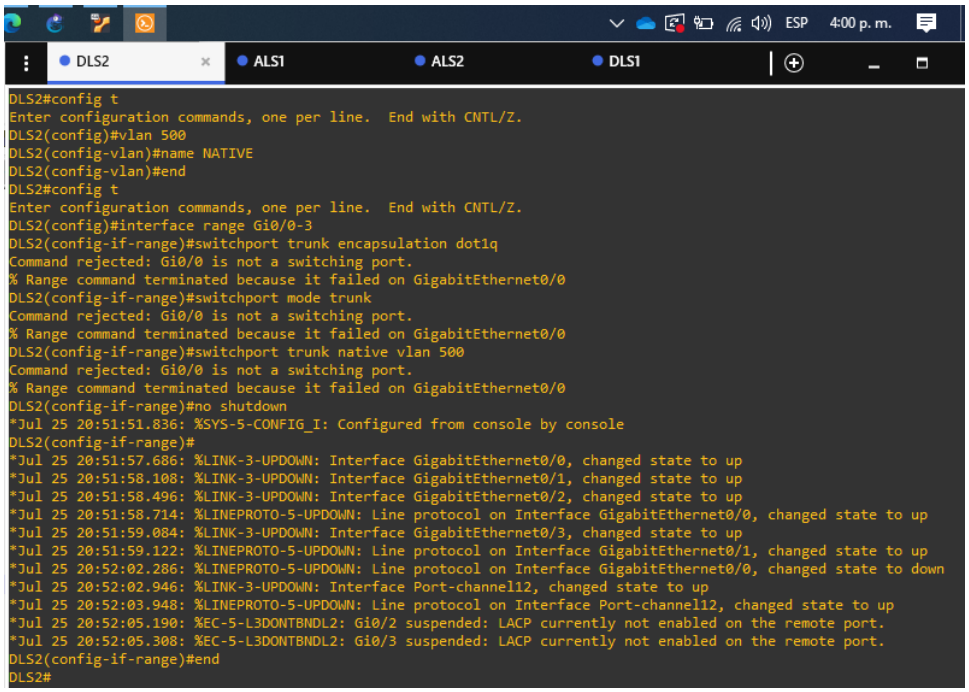

Figura 47.Configuración VLAN nativa 500 en los puerto trunk Gi0/0-3 DLS2

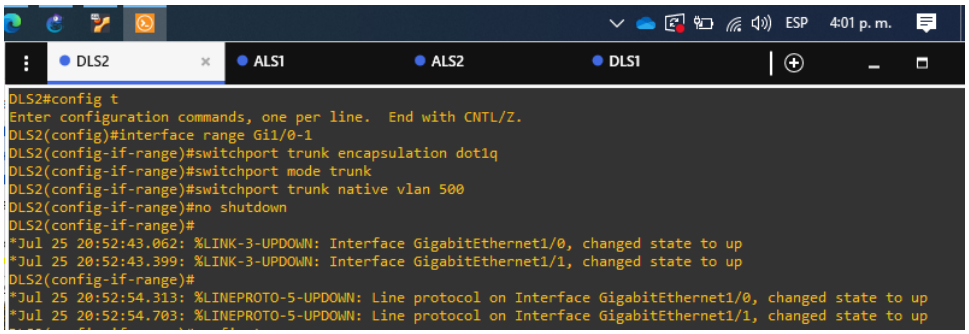

Figura 48.Configuración VLAN nativa 500 en los puerto trunk Gi1/0-1 DLS2

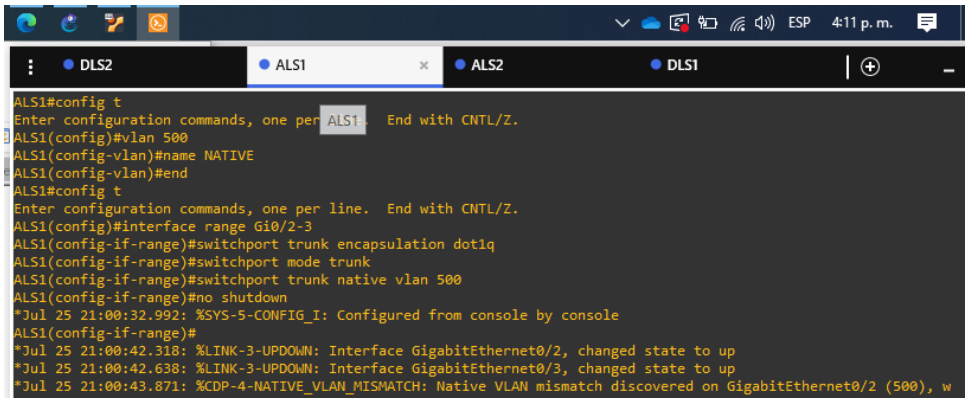

Figura 49.Configuración VLAN nativa 500 en los puerto trunk Gi0/2-3 ALS1

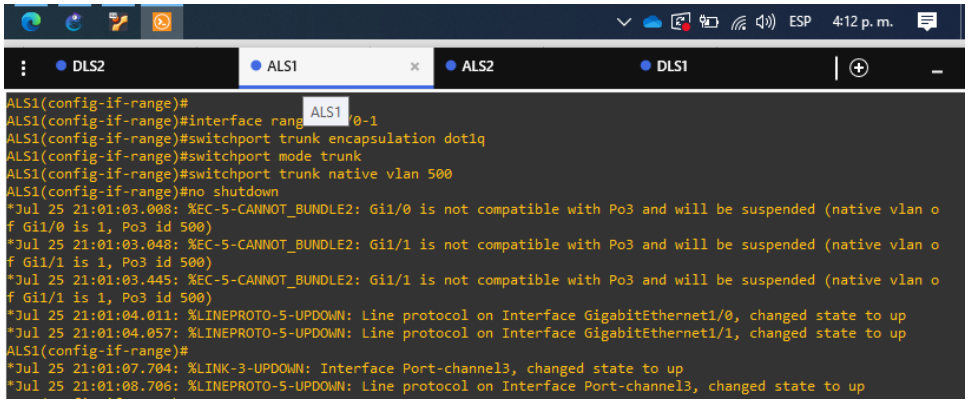

Figura 50.Configuración VLAN nativa 500 en el puerto trunk Gi1/0-1 ALS1

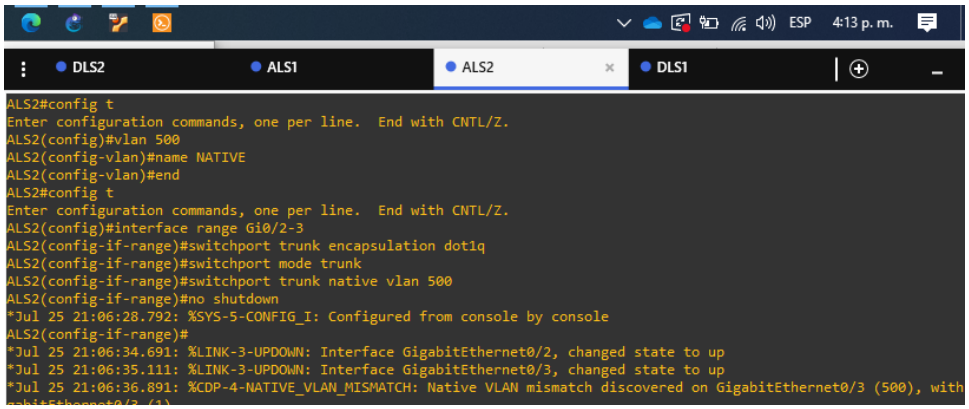

Figura 51.Configuración VLAN nativa 500 en los puerto trunk Gi0/2-3 ALS2

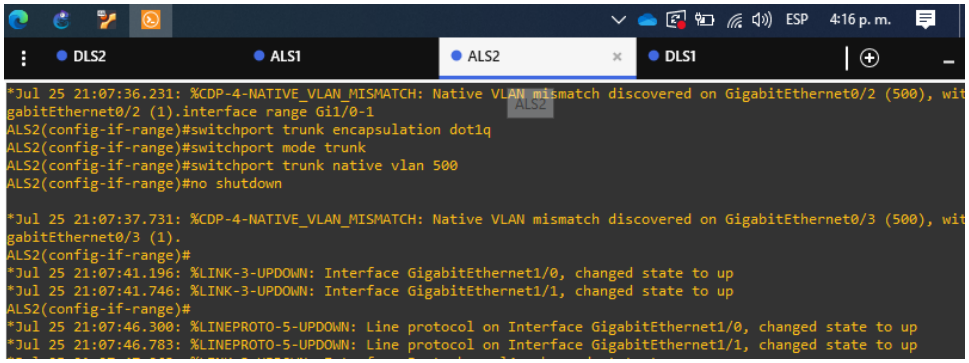

Figura 52. Configuración VLAN nativa 500 en los puerto trunk Gi1/0-1 ALS2

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

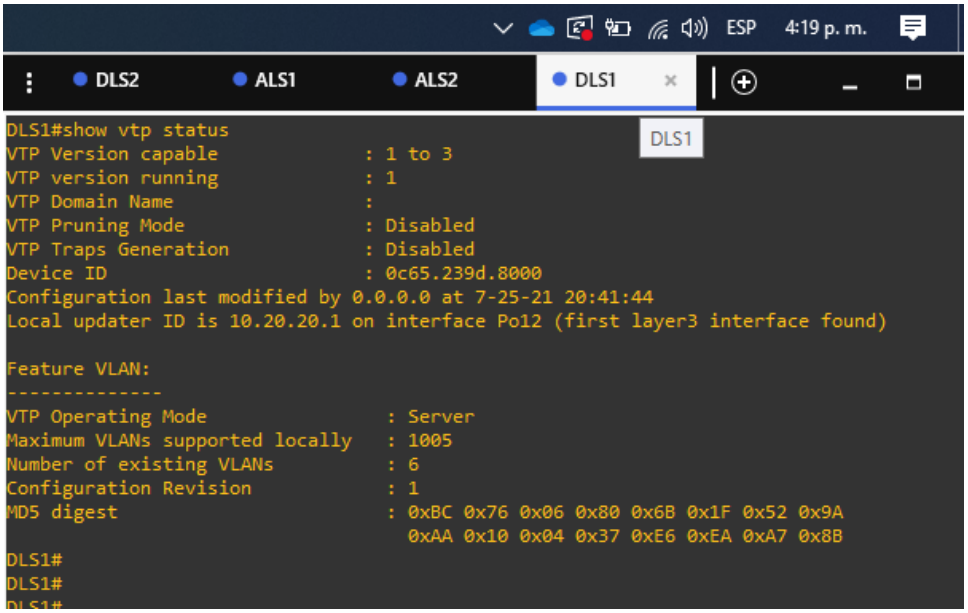

Figura 53. Validación versión VTP soportado por DLS1

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

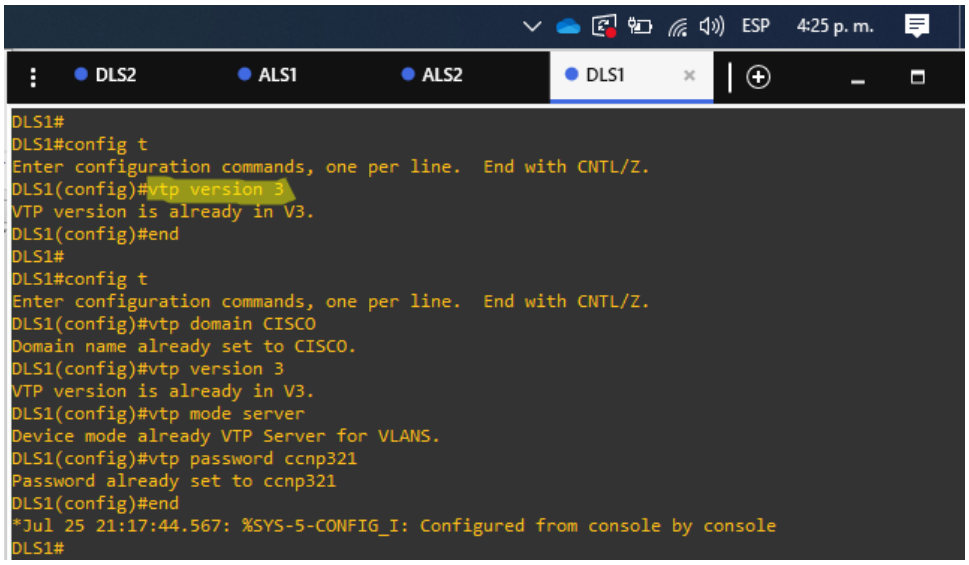

Figura 54. Configuración del Dominio VTP DLS1

2. Configurar DLS1 como servidor principal para las VLAN.

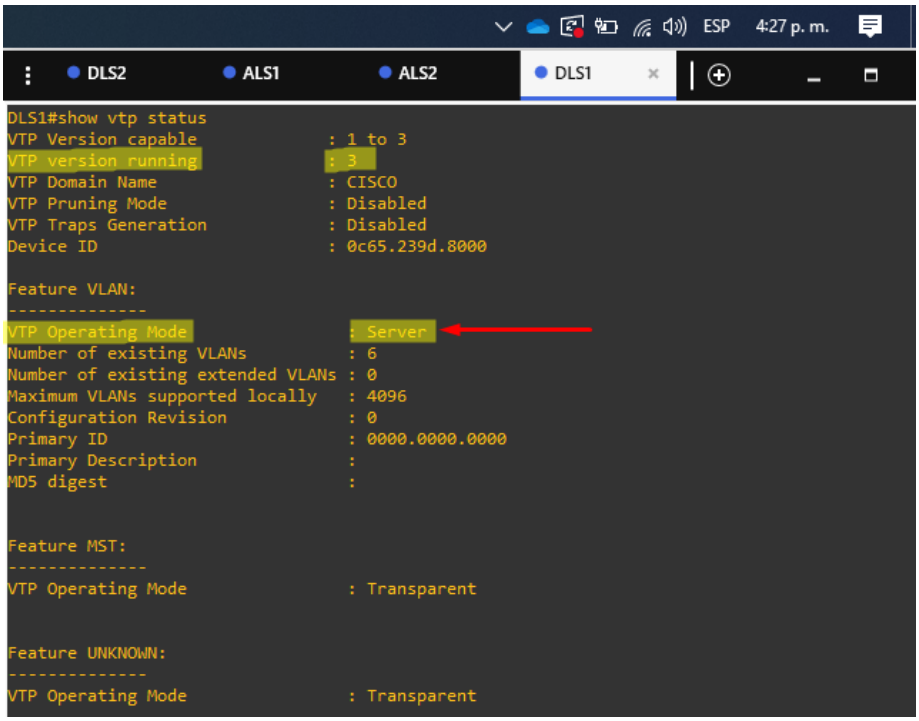

Figura 55. Configuración DLS1 como servidor VTP

3. Configurar ALS1 y ALS2 como clientes VTP.

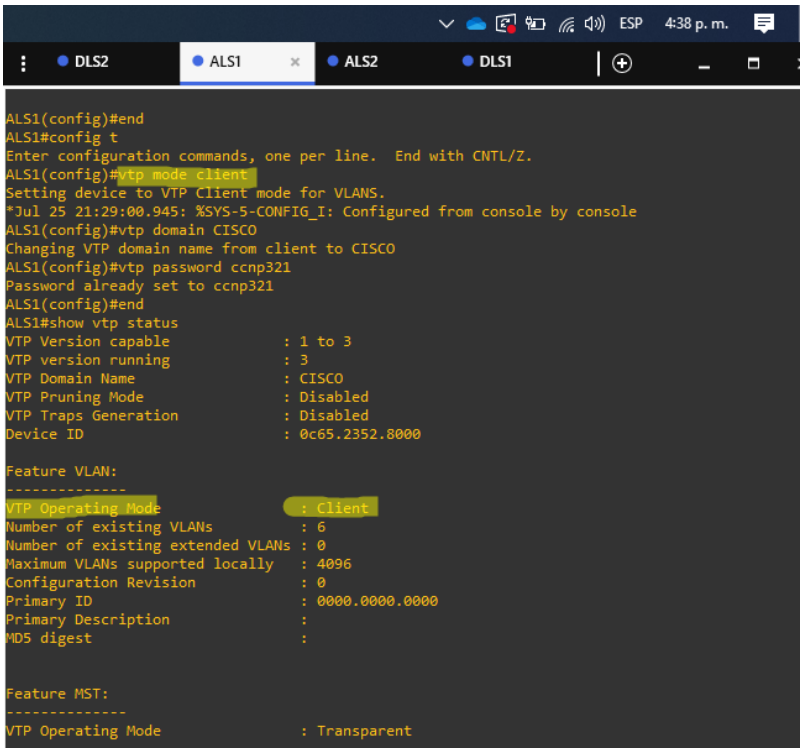

Figura 56. Configuración ALS1 como clientes VTP

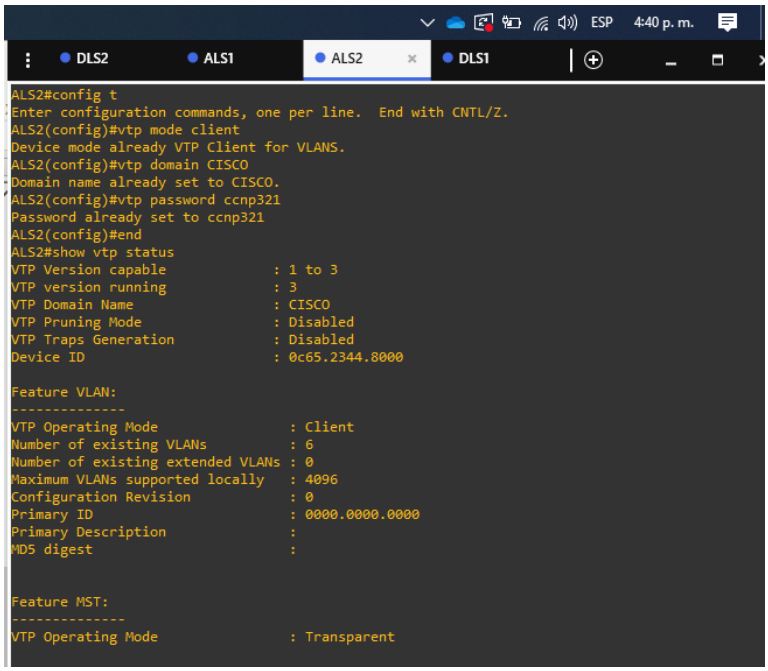

Figura 57. Configuración ALS2 como clientes VTP

e. Se Configura en el servidor DLS1 las siguientes VLAN:

Número de VLAN	Número de VLAN	Número de VLAN	Número de VLAN
500	NATIVA	420	PROVEEDORES
15	ADMON	100	SEGUROS
240	CLIENTES	150	VENTAS
112	MULTIMEDIA	350	PERSONAL

Tabla 1. VLAN Servidor VTP

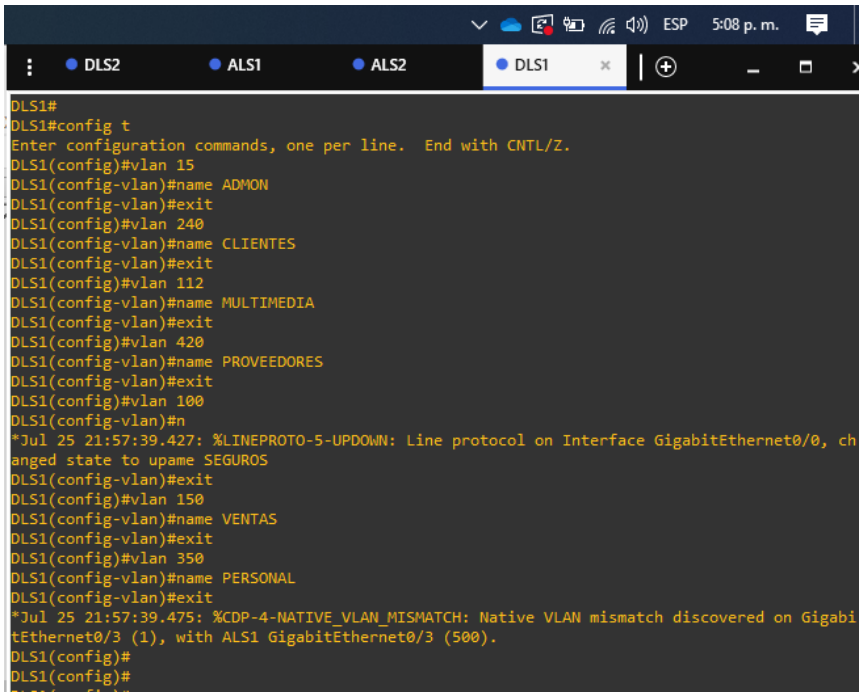

Figura 58. Configuración de VLAN en el servidor VTP DLS1

f. En DLS1, suspender la VLAN 420.

Figura 59. Suspender de VLAN “comando no soportado” DLS1

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

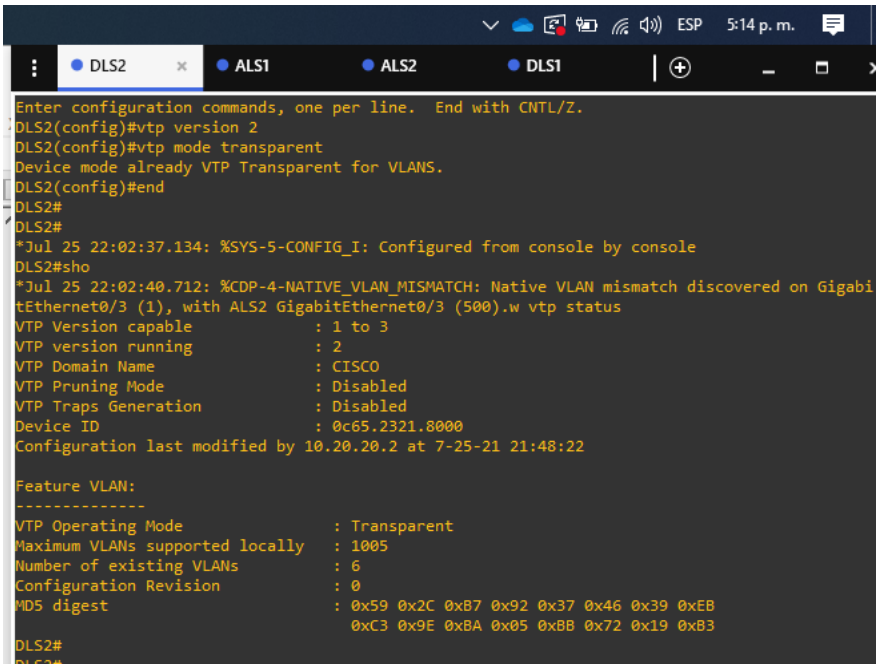

Figura 60. Configurar DLS2 en modo VTP transparente

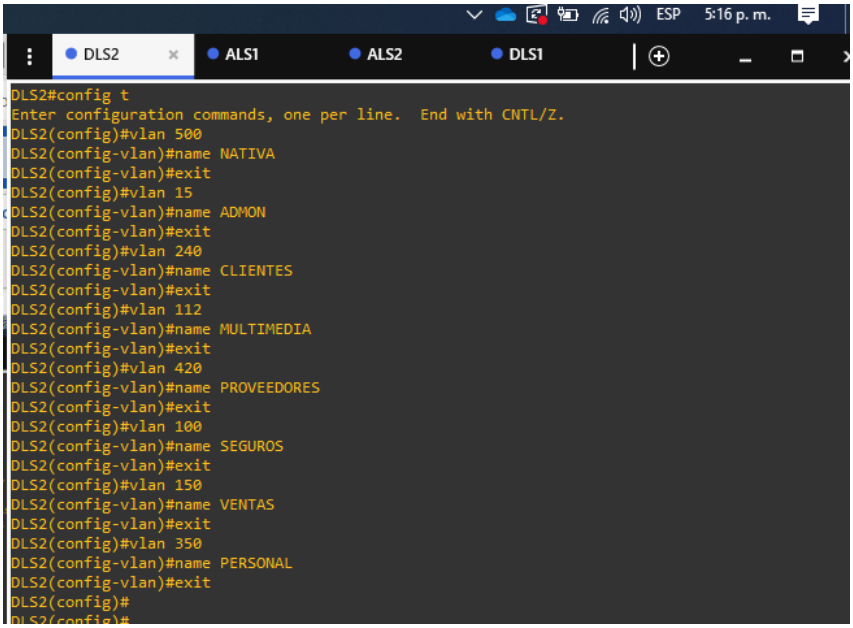

Figura 61. Configurar de VLAN en DLS2

h. Suspender VLAN 420 en DLS2.

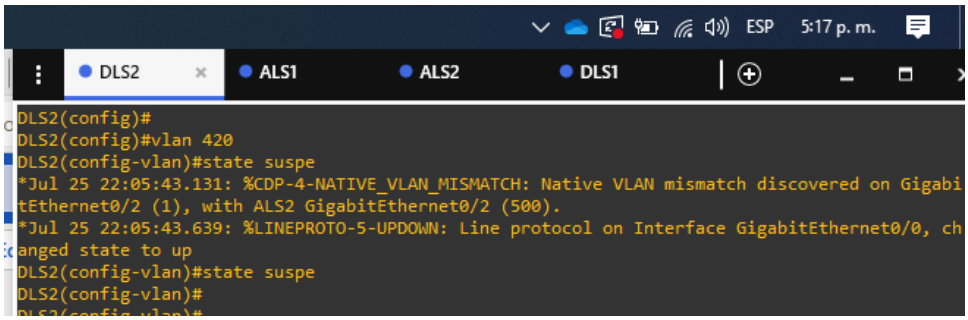

Figura 62. Suspender de VLAN “comando no soportado” DLS2

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.

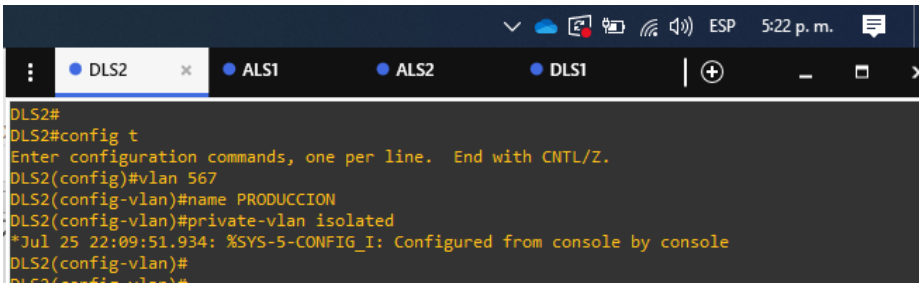

Figura 63. Creación de VLAN privada DLS2 “comando no soportado”

j. Configurar DLS1 como Spanning tree root para las VLANs 1, 15, 420, 500, 150, 112 y 350 y como raíz secundaria para las VLAN 100 y 240.

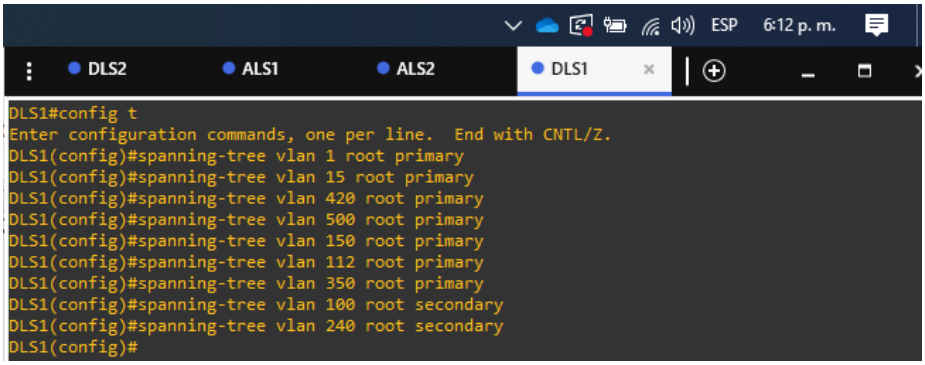

Figura 64. Configurar DLS1 como Spanning tree root

k. Configurar DLS2 como Spanning tree root para las VLAN 100 y 240 y como una raíz secundaria para las VLAN 15, 420, 500, 150, 112 y 350.

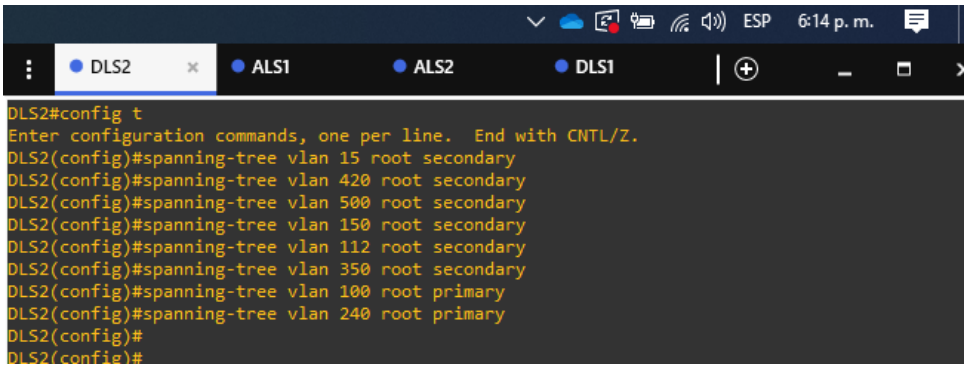

Figura 65. Configurar DLS2 como Spanning tree root

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 éstos puertos.

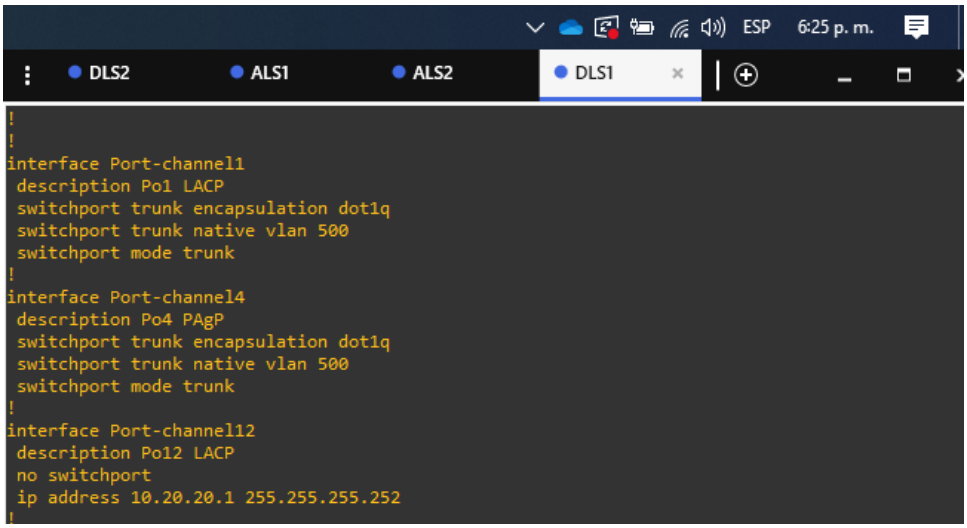

Figura 66. Configurar todos los puertos como troncales DLS1

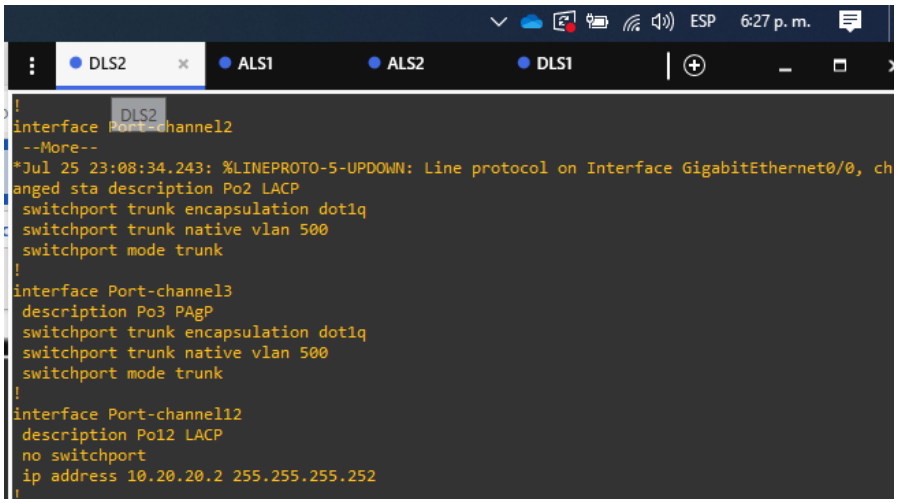

Figura 67. Configurar todos los puertos como troncales DLS2

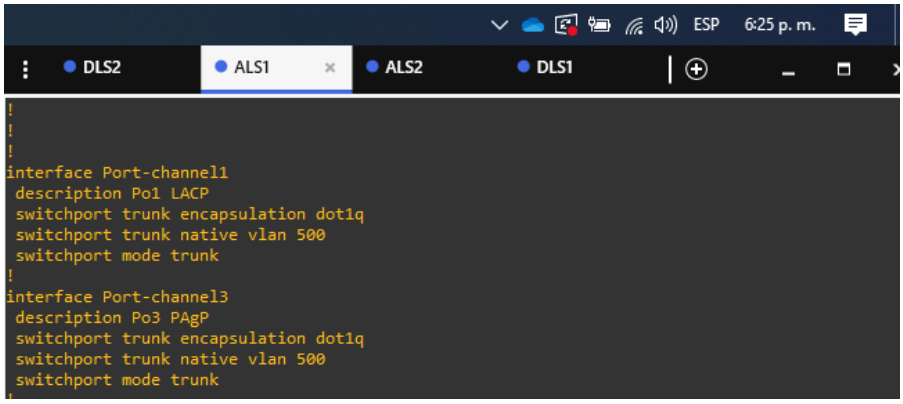

Figura 68. Configurar todos los puertos como troncales ALS1

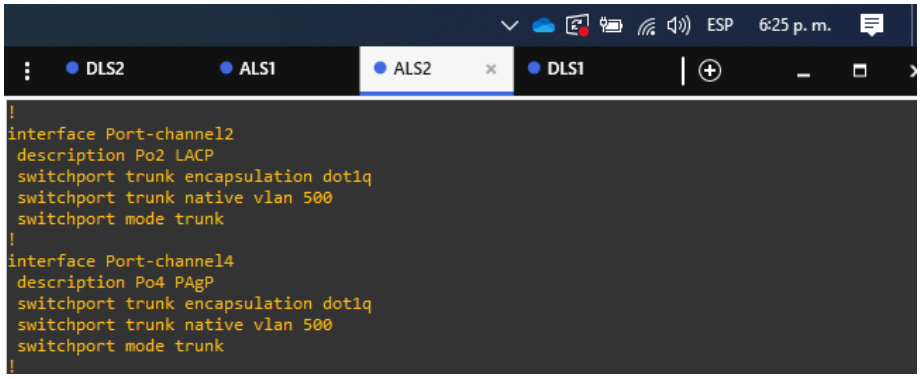

Figura 69. Configurar todos los puertos como troncales ALS2

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

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Gi1/3	350	15, 150	100, 150	240
Interfaz Gi1/2	112	112	112	112
No tiene más Interface		567		

Tabla 2. Configuración Interfaces con las VLAN de acceso

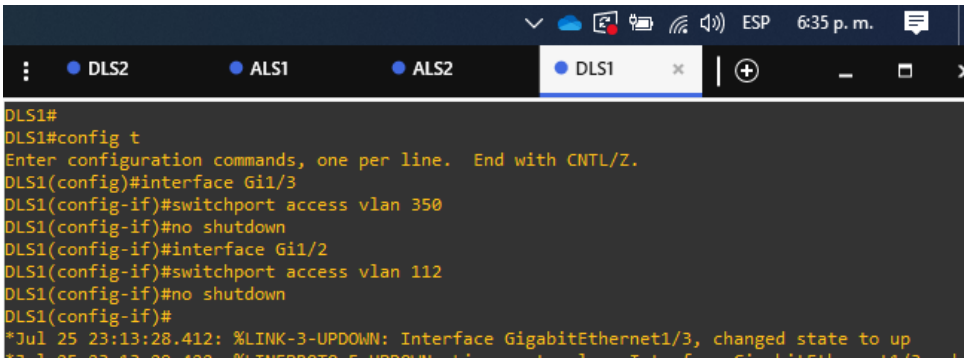

Figura 70. Configuración VLAN 350, 112 en interfaces DLS1

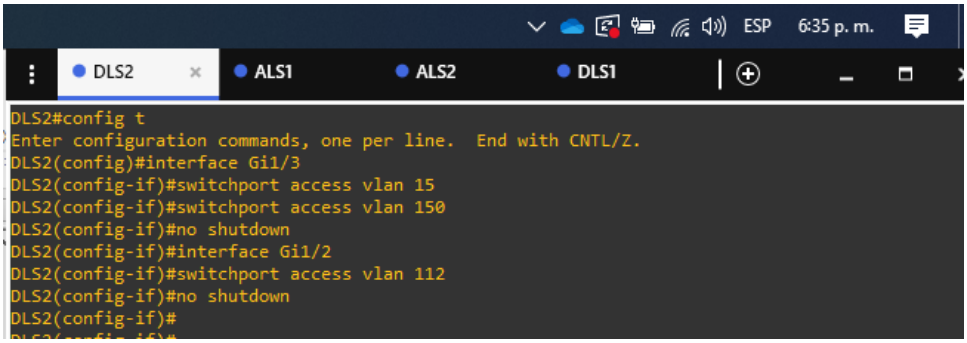

Figura 71. Configuración VLAN 15, 150, 112, 567 en interfaces DLS2

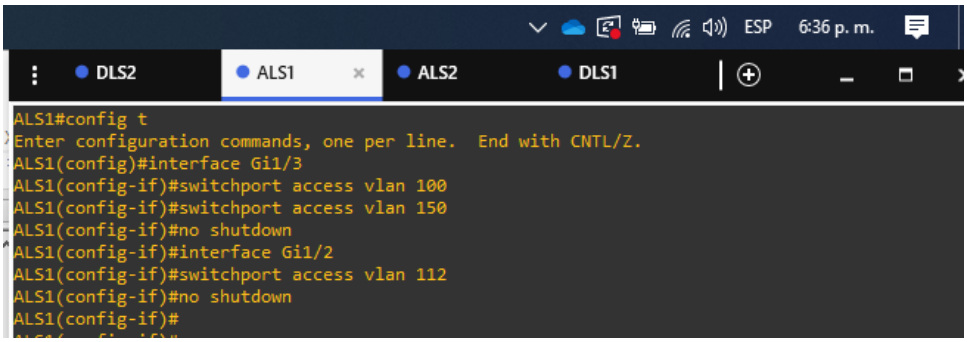

Figura 72. Configuración VLAN 100, 150, 112, en interfaces ALS1

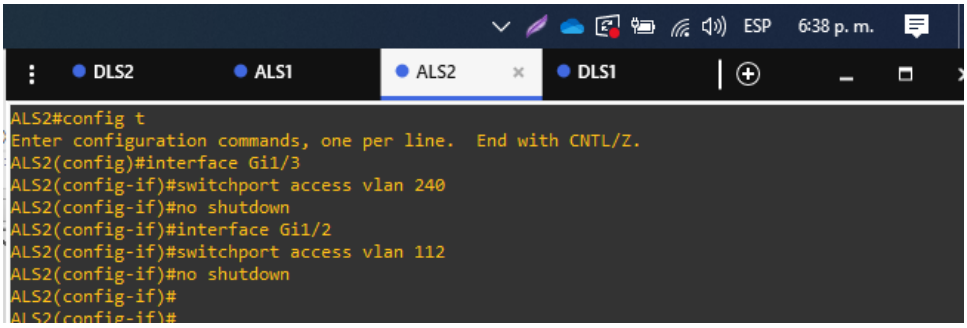

Figura 73. Configuración VLAN 240, 112, en interfaces ALS2

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

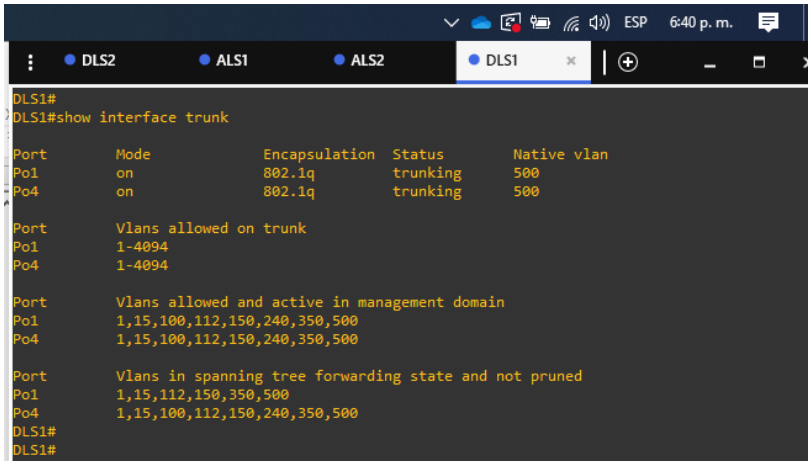

Figura 74. Verificación de troncales y VLAN de DLS1

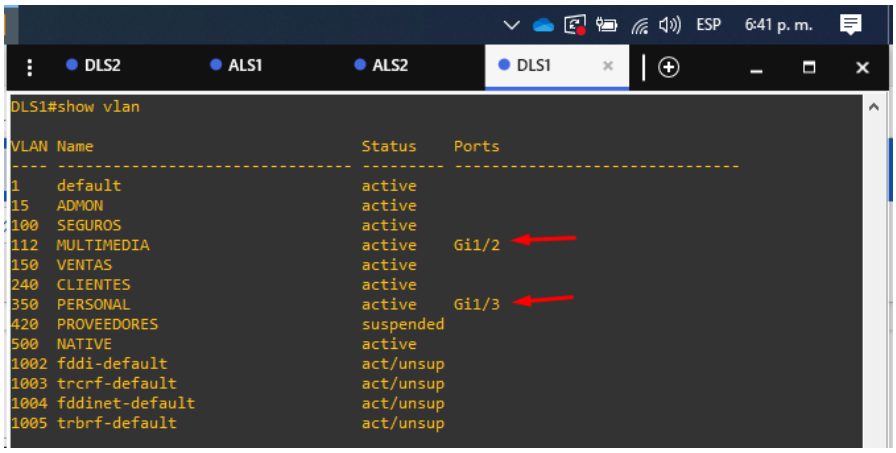

Figura 75. Verificación de VLAN de acceso en las fastethernet de DLS1

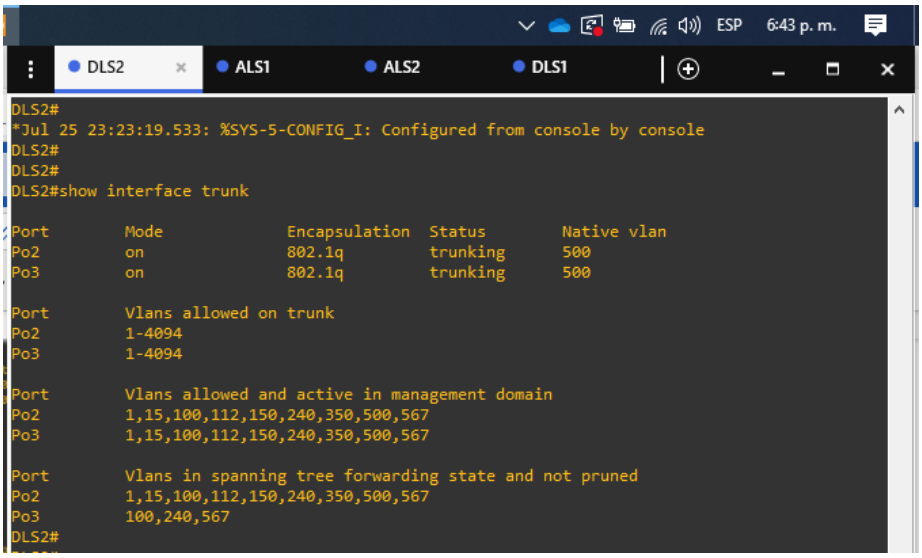

Figura 76. Verificación de troncales y VLAN de DLS2

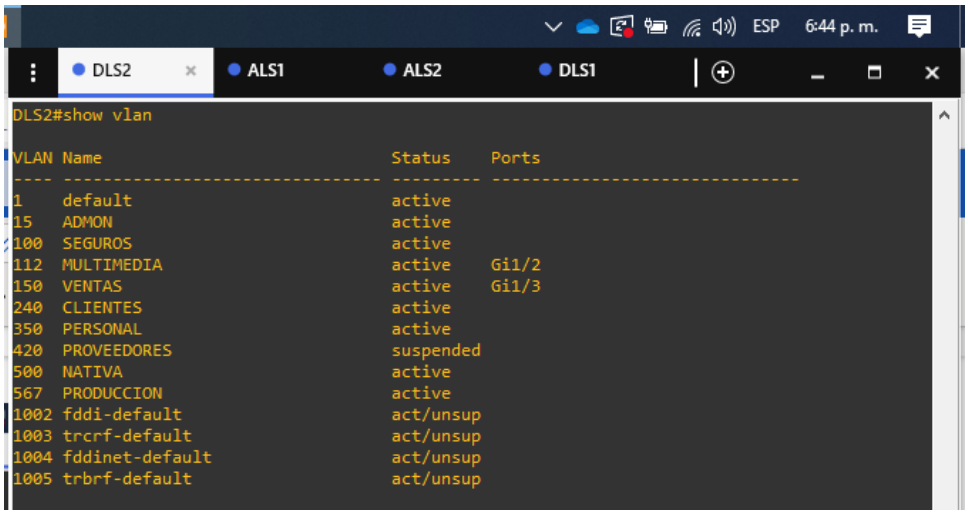

Figura 77. Verificación de VLAN de acceso en las fastethernet de DLS2

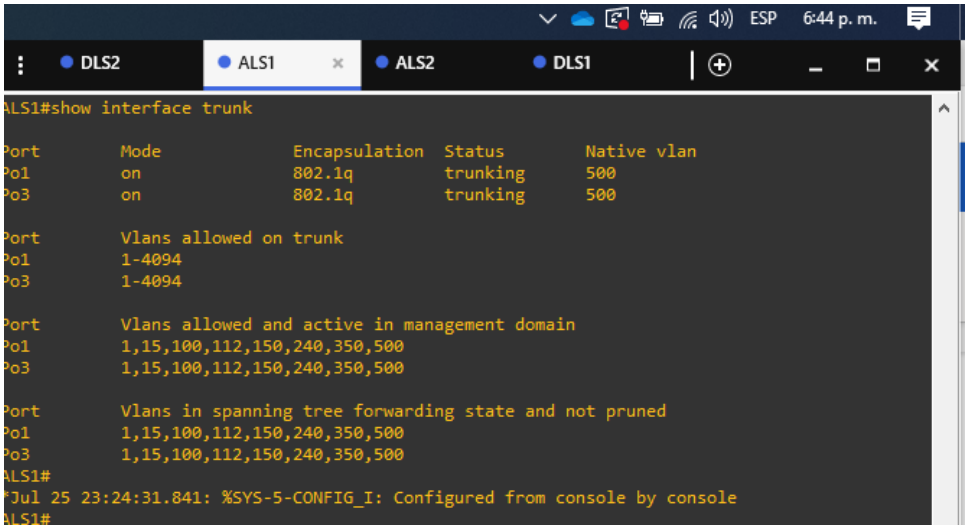

Figura 78. Verificación de troncales y VLAN de ALS1

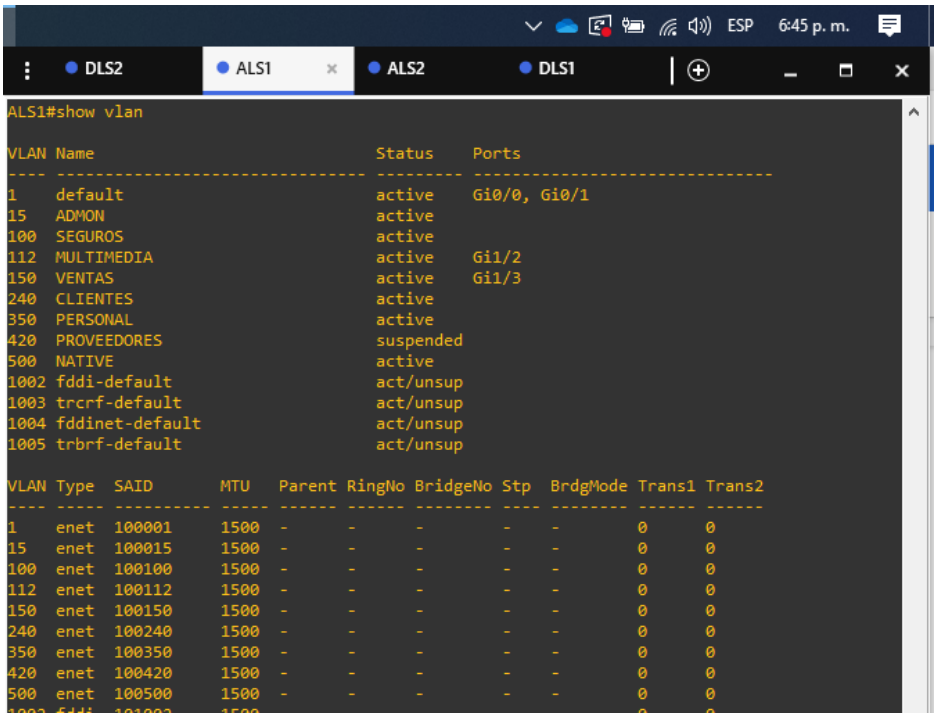

Figura 79. Verificación de VLAN de acceso en las fastethernet de ALS1

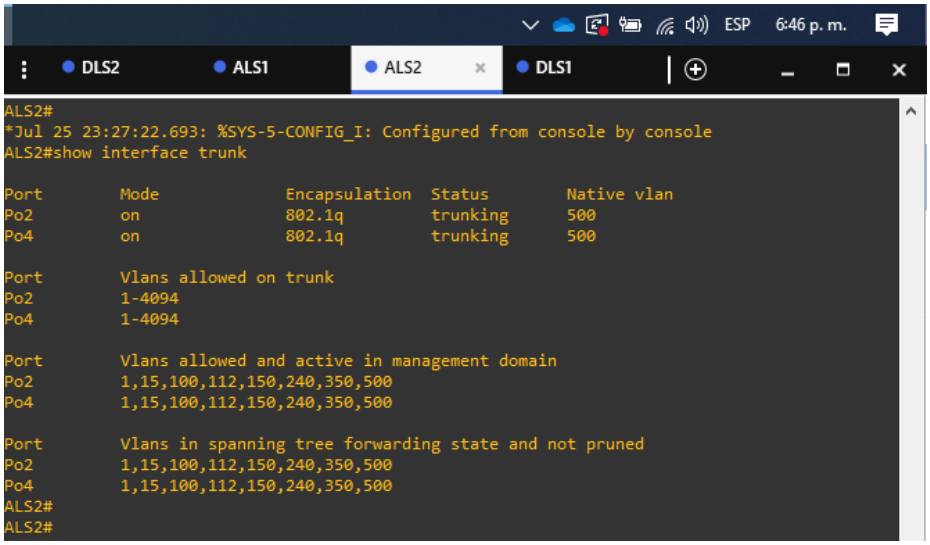

Figura 80. Verificación de troncales y VLAN de ALS2

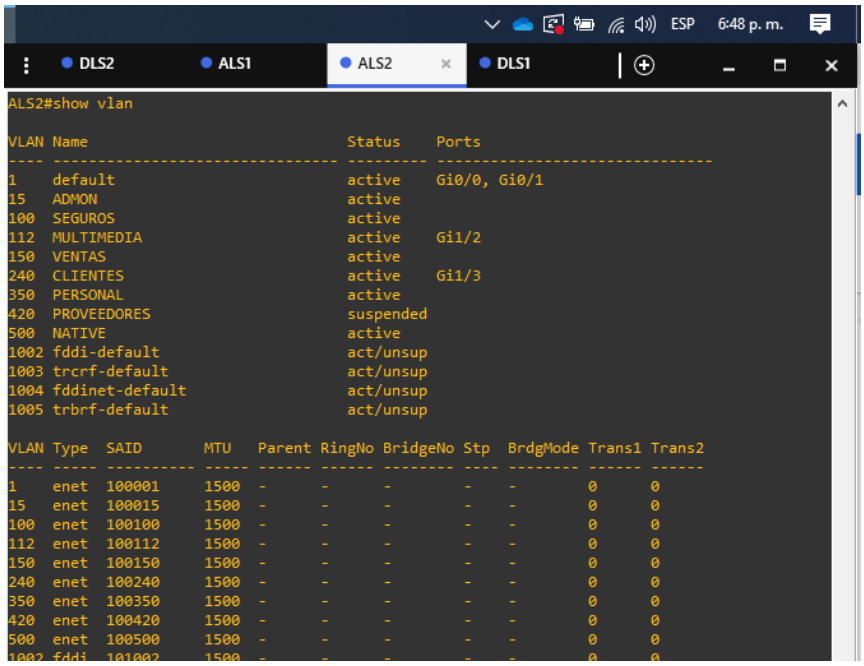

Figura 81. Verificación de VLAN de acceso en las fastethernet de ALS2

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

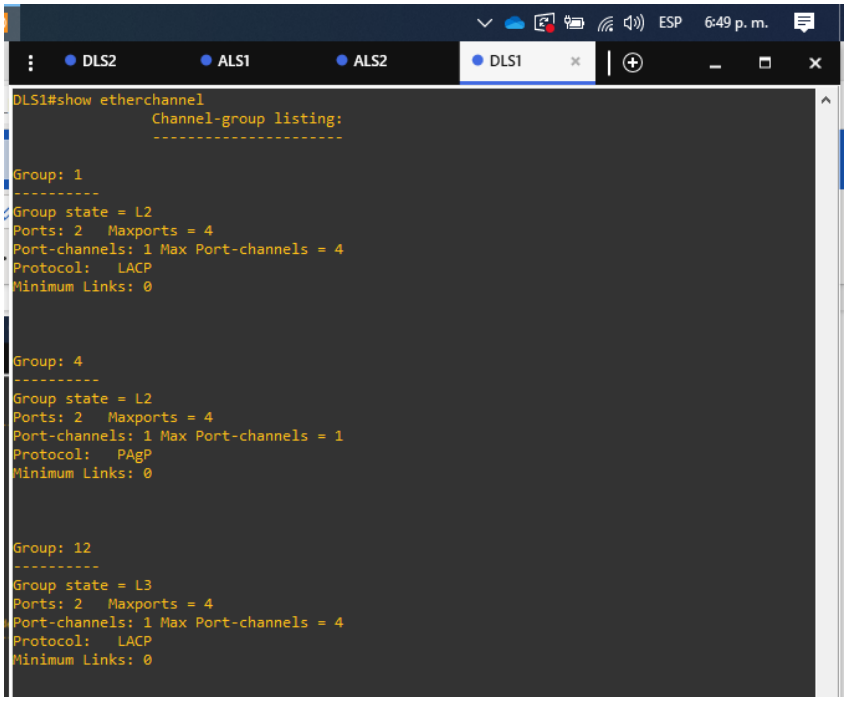

Figura 82. Verificación de EtherChannel en DLS1

Figura 83. Verificación de EtherChannel en ALS1

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

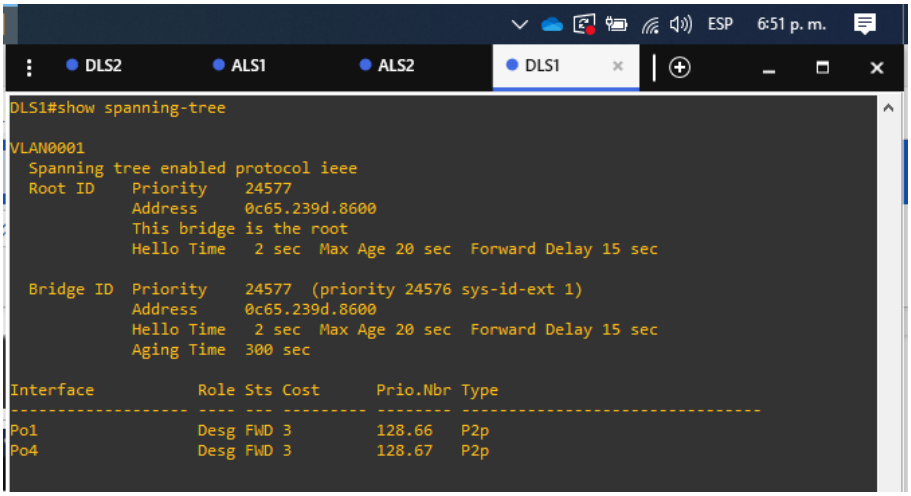

Figura 84. Verificación de Spanning tree DLS1 VLAN 1

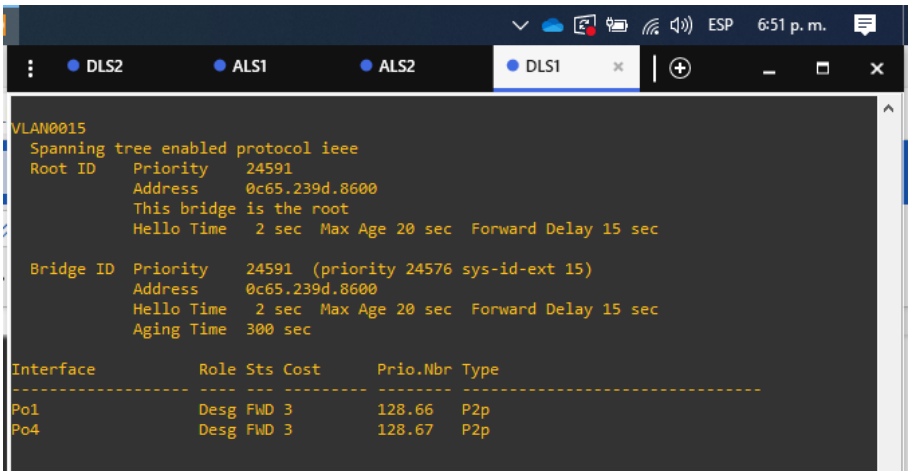

Figura 85. Verificación de Spanning tree DLS1 VLAN 15

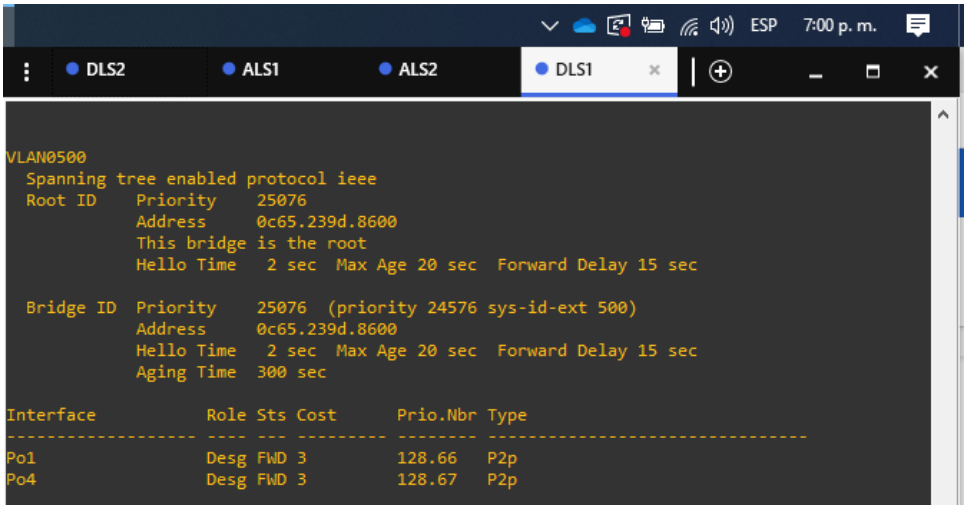

Figura 86. Verificación de Spanning tree DLS1 VLAN 500

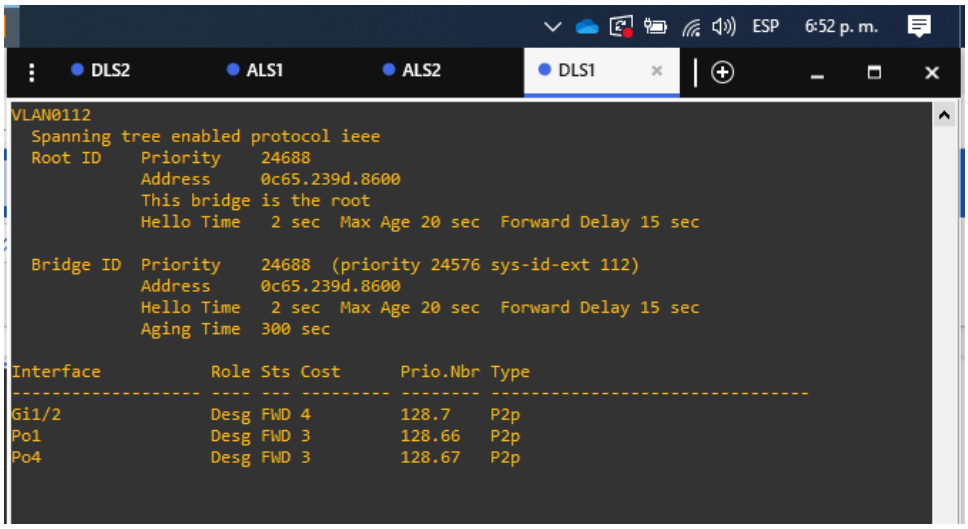

Figura 87. Verificación de Spanning tree DLS1 VLAN 112

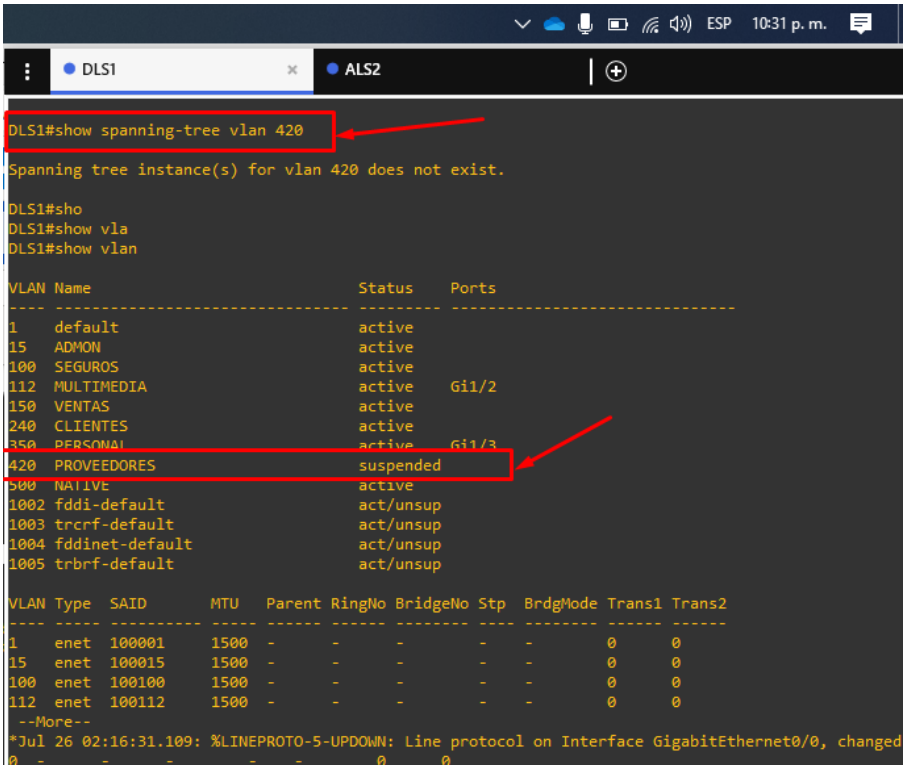

Figura 88. Verificación de Spanning tree DLS1 VLAN 420 esta suspendida

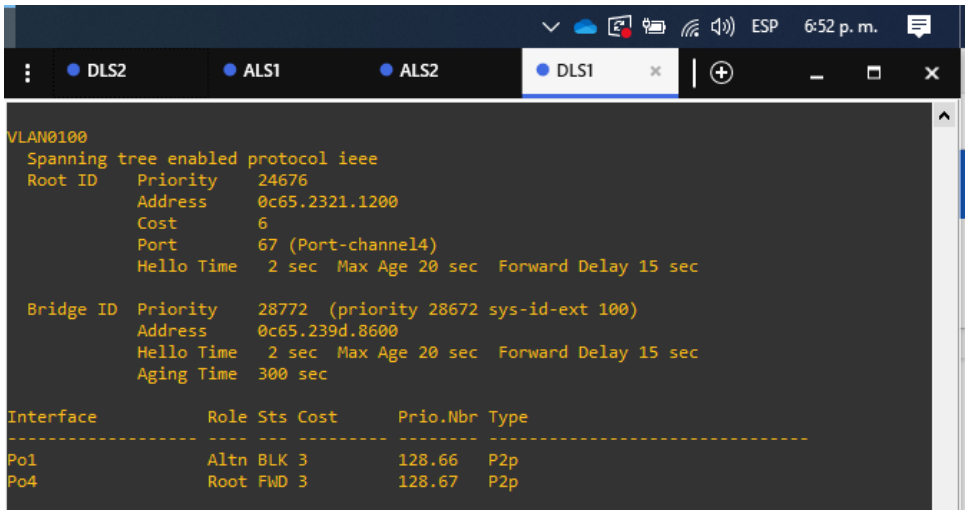

Figura 89. Verificación de Spanning tree DLS1 VLAN 100

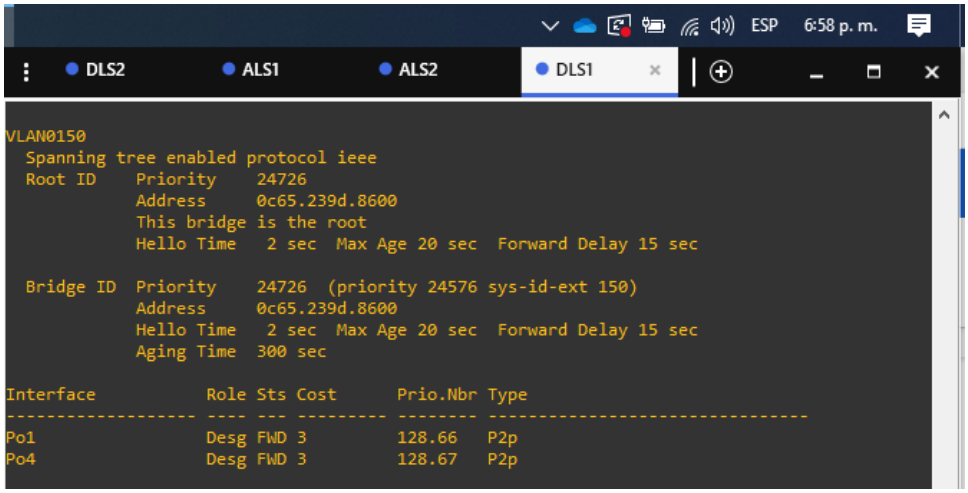

Figura 90. Verificación de Spanning tree DLS1 VLAN 150

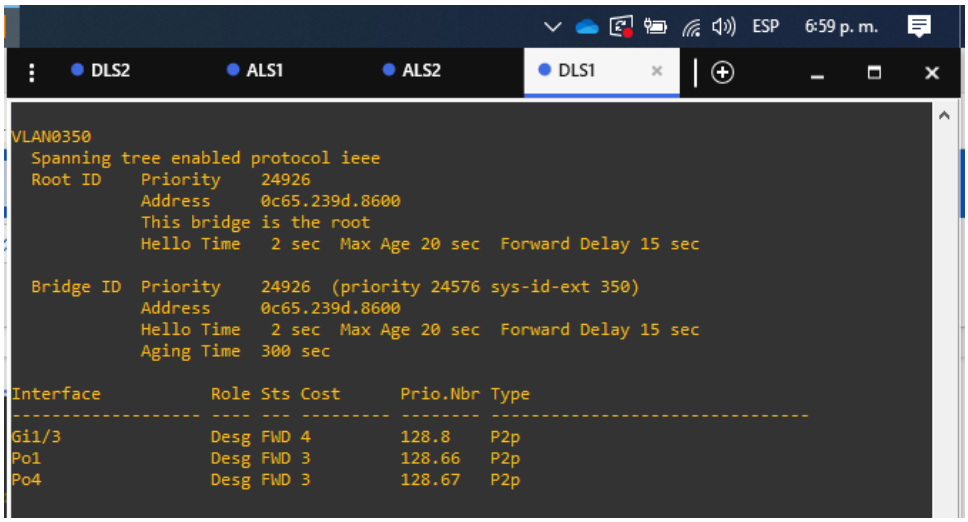

Figura 91. Verificación de Spanning tree DLS1 VLAN 350

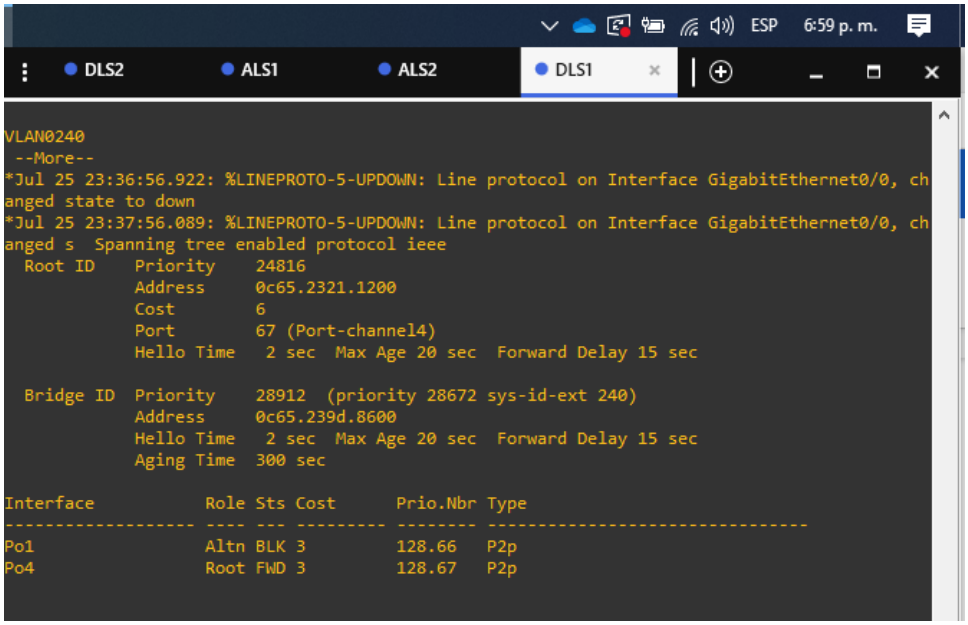

Figura 92. Verificación de Spanning tree DLS1 VLAN 240

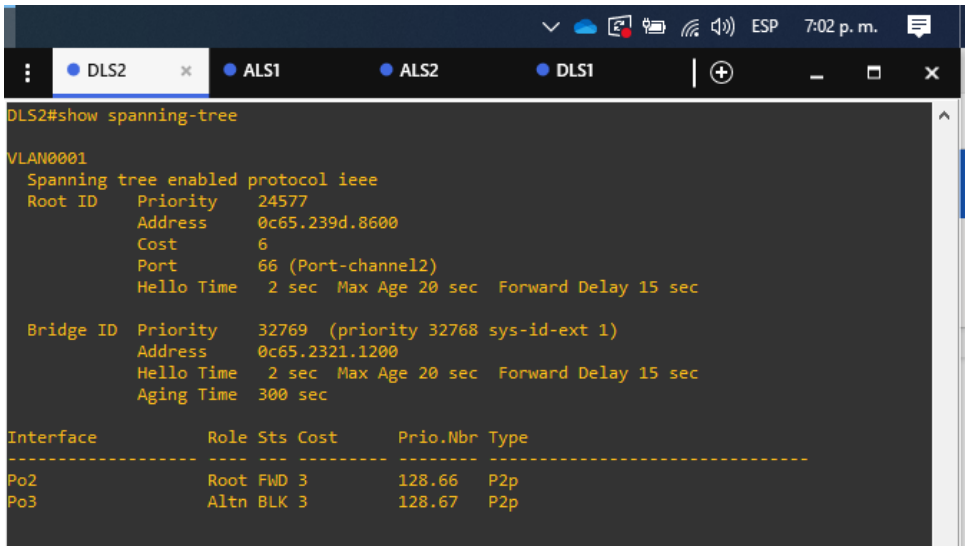

Figura 93. Verificación de Spanning tree DLS2 VLAN 1

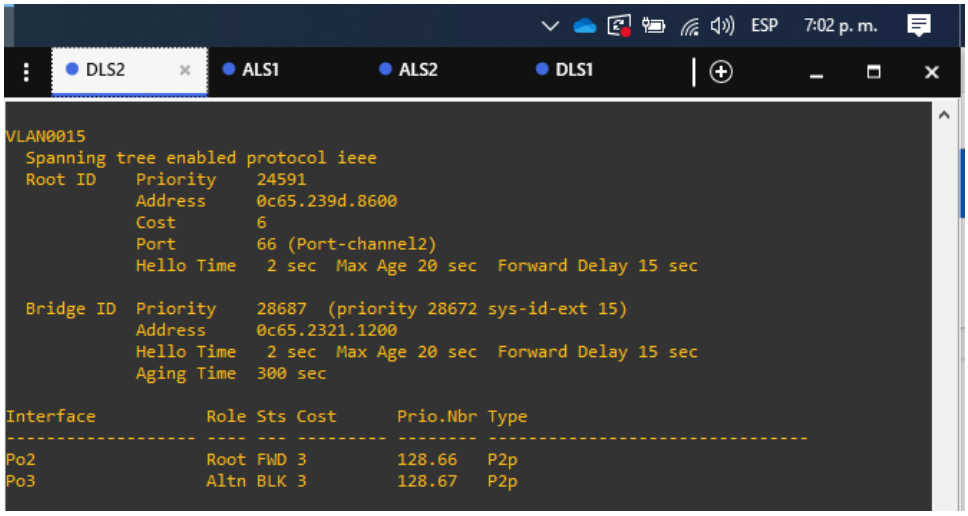

Figura 94. Verificación de Spanning tree DLS2 VLAN 15

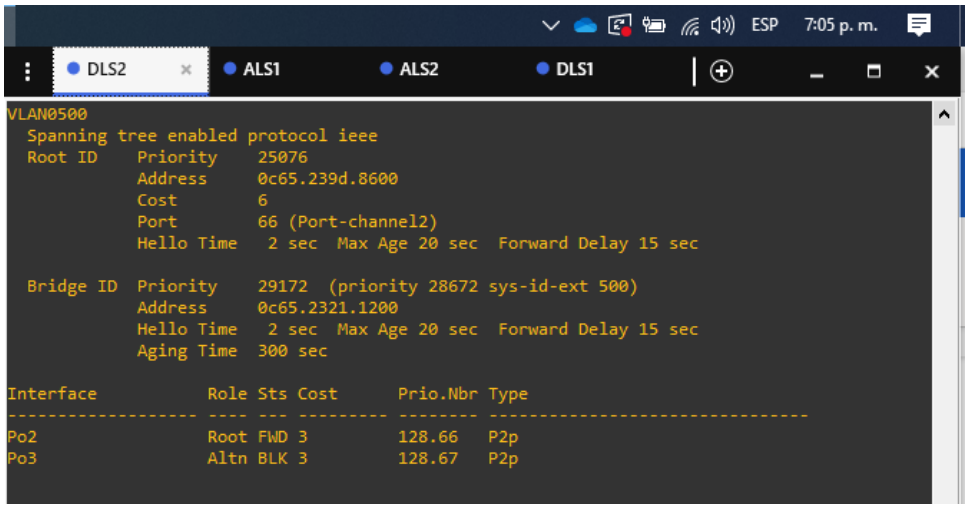

Figura 95. Verificación de Spanning tree DLS2 VLAN 500

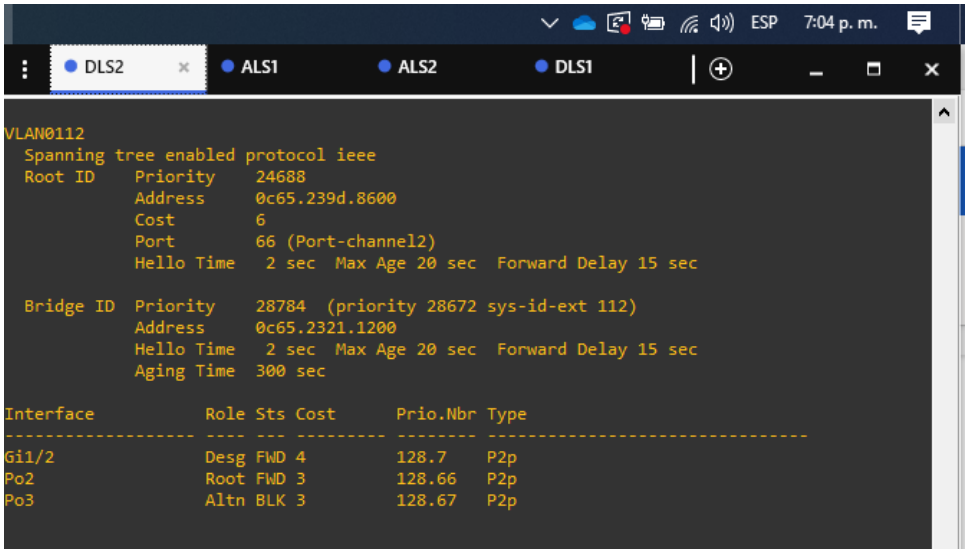

Figura 96. Verificación de Spanning tree DLS2 VLAN 112

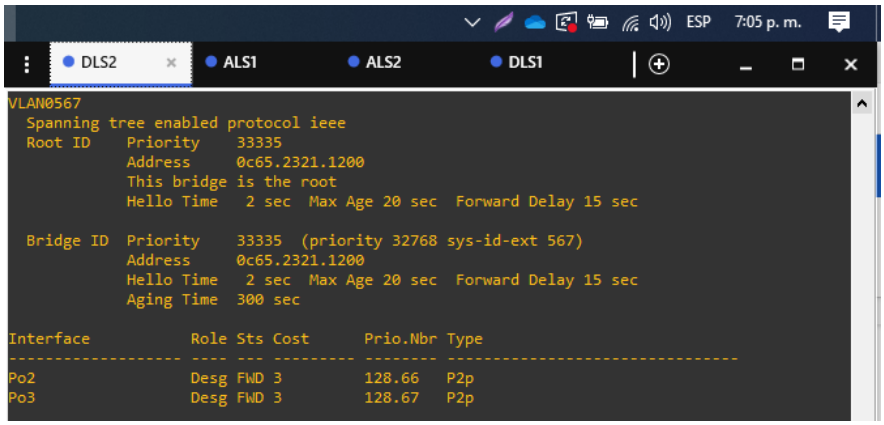

Figura 97. Verificación de Spanning tree DLS2 VLAN 420

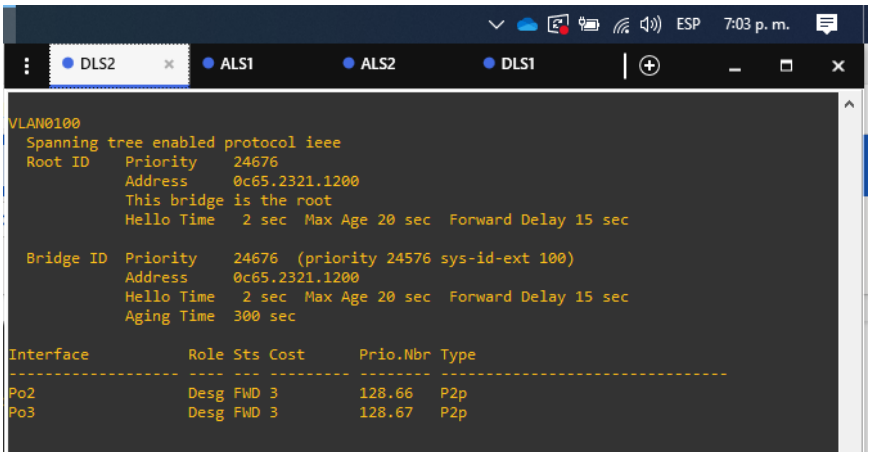

Figura 98. Verificación de Spanning tree DLS1 VLAN 100

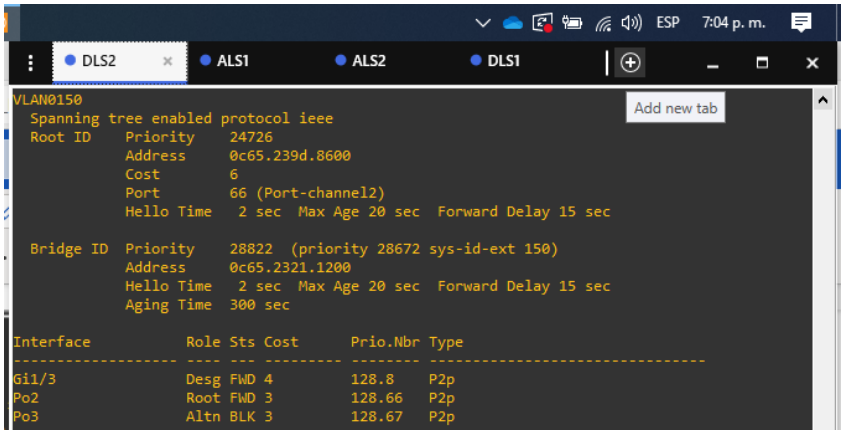

Figura 99. Verificación de Spanning tree DLS2 VLAN 150

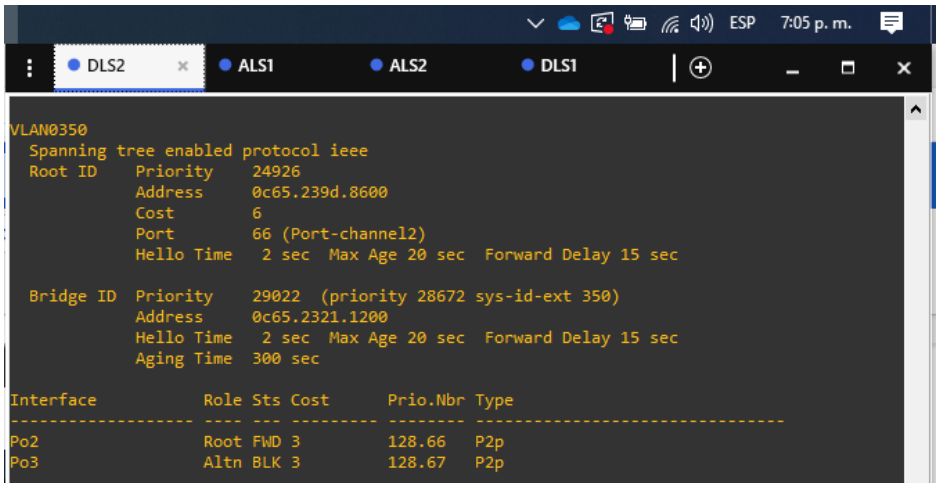

Figura 100. Verificación de Spanning tree DLS2 VLAN 350

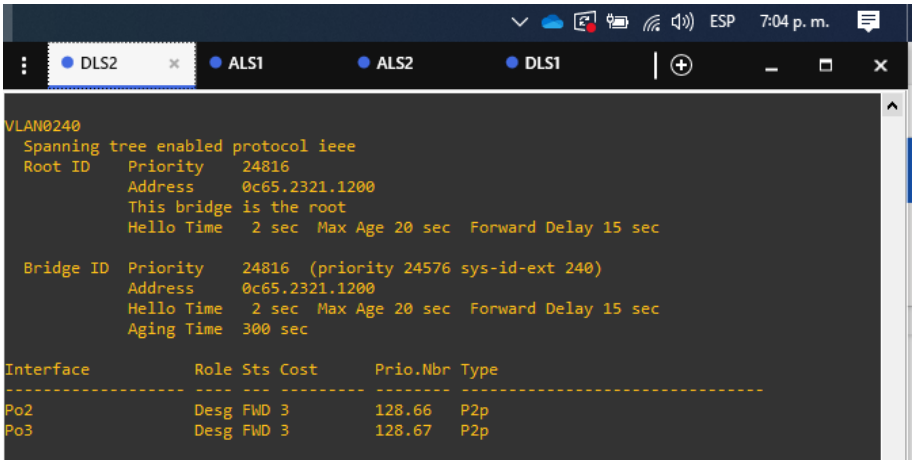

Figura 101. Verificación de Spanning tree DLS2 VLAN 240

Figura 102. Verificación VLAN Conectividad PC1 en DLS1

```
ALS2#show interfaces  status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        disabled     1            auto   auto RJ45
Gi0/1                        disabled     1            auto   auto RJ45
Gi0/2                        connected    trunk      a-full   auto RJ45
Gi0/3                        connected    trunk      a-full   auto RJ45
Gi1/0                        connected    trunk      a-full   auto RJ45
Gi1/1                        connected    trunk      a-full   auto RJ45
Gi1/2                        connected    112        a-full   auto RJ45
Gi1/3                        notconnect   240        a-full   auto RJ45
Po2       Po2 LACP           connected    trunk      a-full   auto
Po4       Po4 PAgP           connected    trunk      a-full   auto
ALS2#
```

Figura 103. Verificación VLAN Conectividad PC4 en ALS2

```
PC4> ping 10.30.30.1

84 bytes from 10.30.30.1 icmp_seq=1 ttl=64 time=17.567 ms
84 bytes from 10.30.30.1 icmp_seq=2 ttl=64 time=22.741 ms
84 bytes from 10.30.30.1 icmp_seq=3 ttl=64 time=22.118 ms
84 bytes from 10.30.30.1 icmp_seq=4 ttl=64 time=24.433 ms
84 bytes from 10.30.30.1 icmp_seq=5 ttl=64 time=27.183 ms
^C
PC4> tracer 10.30.30.1
trace to 10.30.30.1, 8 hops max, press Ctrl+C to stop
 1   *10.30.30.1   17.106 ms (ICMP type:3, code:3, Destination port unreachable)

PC4> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    10.30.30.2/24        255.255.255.0     00:50:79:66:68:03  20098  127.0.0.1:20099
       fe80::250:79ff:fe66:6803/64

PC4>
PC4>
```

Figura 104. Verificación PING Conexión PC1 a PC4

```
PC1> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    10.30.30.1/24        255.255.255.0     00:50:79:66:68:00  20092  127.0.0.1:20093
       fe80::250:79ff:fe66:6800/64

PC1> ping 10.30.30.2

84 bytes from 10.30.30.2 icmp_seq=1 ttl=64 time=24.448 ms
84 bytes from 10.30.30.2 icmp_seq=2 ttl=64 time=12.646 ms
84 bytes from 10.30.30.2 icmp_seq=3 ttl=64 time=15.666 ms
84 bytes from 10.30.30.2 icmp_seq=4 ttl=64 time=15.325 ms
84 bytes from 10.30.30.2 icmp_seq=5 ttl=64 time=18.061 ms

PC1>
```

Figura 105. Verificación PING Conexión PC4 a PC1

CONCLUSIONES

- Logramos implementar con éxito los escenarios planteados en el contexto del trabajo, usando herramientas que nos permitieron llevar un ambiente conceptual a lo real y práctico, usando aplicativos como GNS3 y PT para el desarrollo y visualización de resultados.

- Logramos aplicar los protocolos de enrutamientos vistos en el módulo de routing de CCNP, evidenciando como convergen protocolos de enrutamiento distintos que permitiera la comunicación entre áreas y sistemas autónomos (SA) distintos.

- Logramos implementar a cabalidad el escenario de switching identificando la necesidad de aplicar en entornos de redes de capa 2, como buena práctica el uso de Etherchannel, el cual permite y garantiza un mayor ancho de banda y redundancia en cuanto a disponibilidad del enlace, además de verificar la administración centralizada de la gestión de VLAN con el protocolo VTP.

BIBLIOGRAFIA

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Management. 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). 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-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