

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

MIGUEL ANGEL VERGARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA
ELECTRÓNICA

YOPAL 2020

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

Diplomado de opción de grado presentado para optar el título de INGENIERO
ELECTRÓNICO

DIRECTOR: MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA
ELECTRONICA

YOPAL

2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado.

Firma del Jurado

Firma del Jurado

Yopal – Casanare, 26 noviembre de 2020

AGRADECIMIENTOS

Quiero agradecer a mi familia por el apoyo durante todo este proceso y de igual manera agradecer a los Tutores de la UNAD que me han animado a seguir adelante.

CONTENIDO

AGRADECIMIENTOS.....	2
CONTENIDO	3
LISTA DE TABLAS	4
LISTA DE FIGURAS	5
GLOSARIO	6
RESUMEN.....	7
ABSTRACT.....	7
INTRODUCCIÓN	8
DESARROLLO	9
Escenario 1.....	9
Escenario 2.....	23
CONCLUSIONES	43
BIBLIOGRAFIA.....	44

LISTA DE TABLAS

Tabla 1. Configuración VLAN	32
Tabla 2. Configuración de Interfaces	35

LISTA DE FIGURAS

Figura 1. Escenario 1.....	9
Figura 2. Configuración R1	11
Figura 3. Configuración R2	12
Figura 4. Protocolos en R3	14
Figura 5. Protocolos en R5	16
Figura 6. Evidencia del montaje.....	17
Figura 7. Interfaces en R1	18
Figura 8. Enrutamiento en R5.....	19
Figura 9. Enrutamiento en R3.....	20
Figura 10. Configuración en R3.....	22
Figura 11. Enrutamiento en R1	22
Figura 12. Enrutamiento en R5.....	23
Figura 13. Escenario 2.....	24
Figura 14. Interfaces en DLS1	26
Figura 15. Interfaces DLS2	27
Figura 16. VLAN en DLS1	30
Figura 17. VTP STATUTS	31
Figura 18. VLAN DLS1	33
Figura 19. Verificación en DSL1	37
Figura 20. Verificación en DSL2	38
Figura 21. Verificación en ALS1	38
Figura 22. EtherChannel DLS1.....	39
Figura 23. EtherChannel ALS1	40
Figura 24. Spanning tree DLS1	41
Figura 24. Spanning tree DLS2	42

GLOSARIO

EIGRP: El Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado (en inglés, Enhanced Interior Gateway Routing Protocol o EIGRP) es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de Vector de distancias.

EtherChannel: es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad.

OSPF: Open Shortest Path First (OSPF), Abrir el camino más corto primero en español, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), 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.

VTP: son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

RESUMEN

En el presente trabajo el lector encontrará dos escenarios planteados en el diplomado CCNP, el primer escenario hace referencia a protocolos de enrutamiento, OSPF y EIGRP y cómo podemos hacer diseño de redes con áreas distintas. El segundo escenario está enfocado a la parte de switch y la creación de vlans, la configuración de este escenario.

Para el segundo escenario se configura una red en la cual existen varias Vlan, y en estas vlans se hace uso de protocolos propietarios para agrupar los enlaces Etherchannel, usando dos tecnologías que son PAGP Y LACP.

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

ABSTRACT

In this work, the reader will find two scenarios raised in the CCNP course, the first scenario refers to routing protocols, OSPF and EIGRP and how we can design networks with different areas. The second scenario is focused on the switch part and the creation of vlans, the configuration of this scenario.

For the second scenario, a network is configured in which there are several Vlan, and in these vlans, proprietary protocols are used to group the Etherchannel links, using two technologies that are PAGP and LACP.

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

INTRODUCCIÓN

El presente trabajo final tiene como objetivo principal mostrar los avances del proceso a lo largo del diplomado CCNP, en el cual hubo una parte teórica y una parte práctica, en este trabajo se puede decir que es más de la parte práctica, ya que aquí se utiliza un modelo de simulación basado en Packet tracer , el cual es una herramienta de modelamiento de redes, la cual nos permite tener un acercamiento muy detallado del funcionamiento de estos equipos cisco, muy parecidos a la parte real.

Para el desarrollo del primer escenario se ejecutó toda la configuración de enrutamiento aprendidos en el diplomado, por medio protocolos de enrutamiento de Cisco, con EIGRP y OSPF llamados protocolos de enrutamiento interno, se realizó la integración para redistribuir las rutas entre estos protocolos mostrando la interoperabilidad entre dos protocolos diferentes.

En el desarrollo del segundo escenario se utilizará los conocimientos adquiridos sobre Switching, donde se abordará la temática de Canales Etherchannel que permiten la adición de uno o más interfaces con el fin de entregar más ancho de banda y redundancia de canales a través de protocolos Proprietarios como LACP o PAgP, PAgP (Port Aggregation Protocol) es un protocolo propietario de Cisco. Los paquetes son intercambiados entre switch a través de los enlaces configurados para ello y por último el Protocolo de control de agregación de enlaces (LACP) que es un protocolo estándar de la industria (IEEE 802.3ad) que se utiliza para agrupar dos o más enlaces y puede funcionar con dispositivos de diferentes proveedores.

DESARROLLO

Escenario 1

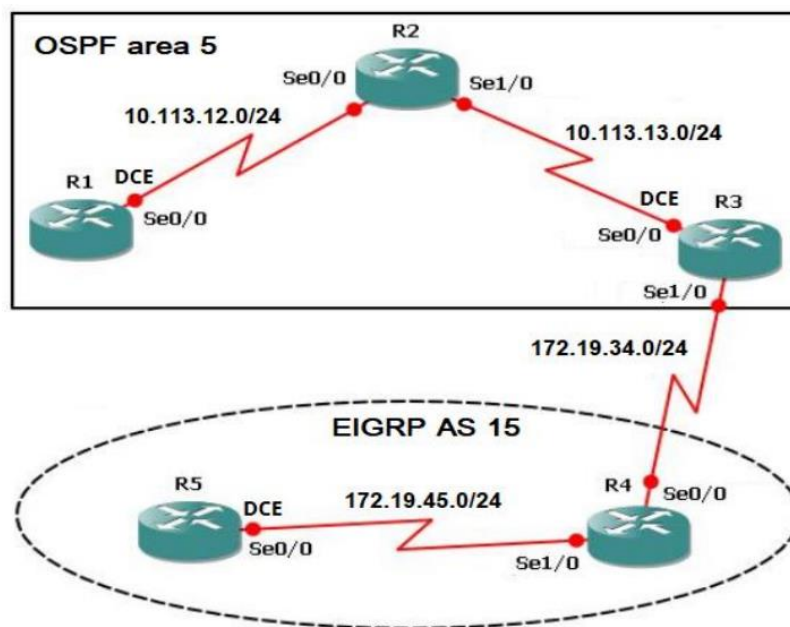


Figura 1. Escenario 1.

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 del Router 1.

```
Router>
Router>enable           Se configura el ingreso a modo privilegiado
Router#configure terminal Se configura el Ingreso a modo de configuración
Router(config)#hostname R1 Se configura para asignar nombre al router
R1(config)#router ospf 1 Se asigna protocolo ospf R1(config-router)
#router-id 1.1.1.1      La configuración nos permite Identificar el router
R1(config-router)
#network 10.103.12.0 255.255.255.0 area 5 Asignamos configuración IP R1(config-
router)
#exit R1(config)
#interface s0/0         se configura interfaz serial.
R1(config-if)description to R2
R1(config-if)
#ip address 10.103.12.1 255.255.255.0 se configura la ip
R1(config-if)
#clock rate 128000      se configura sincronismo
R1(config-if)
#bandwidth 128         se asigna baudios
(config-if)#
no shutdown            se activa interface.
#exit
R1(config)
#end
```

En la grafica de abajo podemos observar la evidencia de la configuracion que se hizo en el router 1, comocambio de nombre , ajuste de parámetros como interfaces, rels, sincronizmo, ancho de banda, direccionamiento ip y demás.

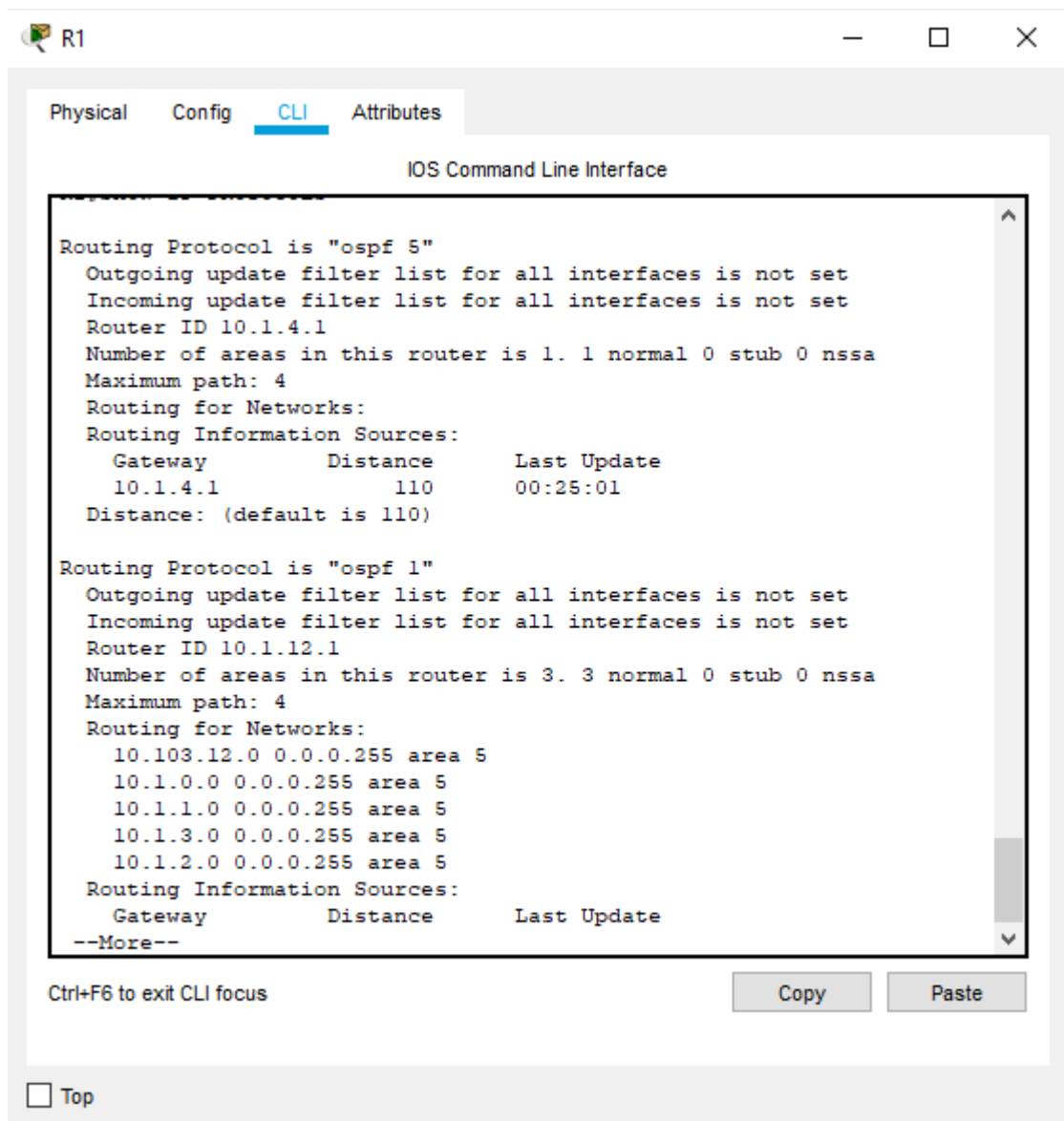


Figura 2. Configuración R1

Configuración del Router 2.

Router>
 Router>enable *Se configura el ingreso a modo privilegiado*
 Router#configure *Se configura el Ingreso a modo de configuración*
 Router(config)
 #hostname R2 *Se configura para asignar nombre al router*
 R2(config)#router ospf 1 *asigna protocolo OSPF*
 R2(config-router)

```
R2(config-router) #network 10.103.12.0 255.255.255.0 area 5
R2(config-router)#network 10.103.23.0 255.255.255.0 area 5
R2(config-router)
#exit
```

```
R2(config)#interface s0/0 / La Configuración del interfaz serial
R2(config-if)description to R1
R2(config-if)#ip address 10.103.12.2 255.255.255.0
```

Aquí en la figura de abajo podemos observar que la evidencia de que se configuro el protocolo OSPF, aquí se hizo uso del comando show ip protocols

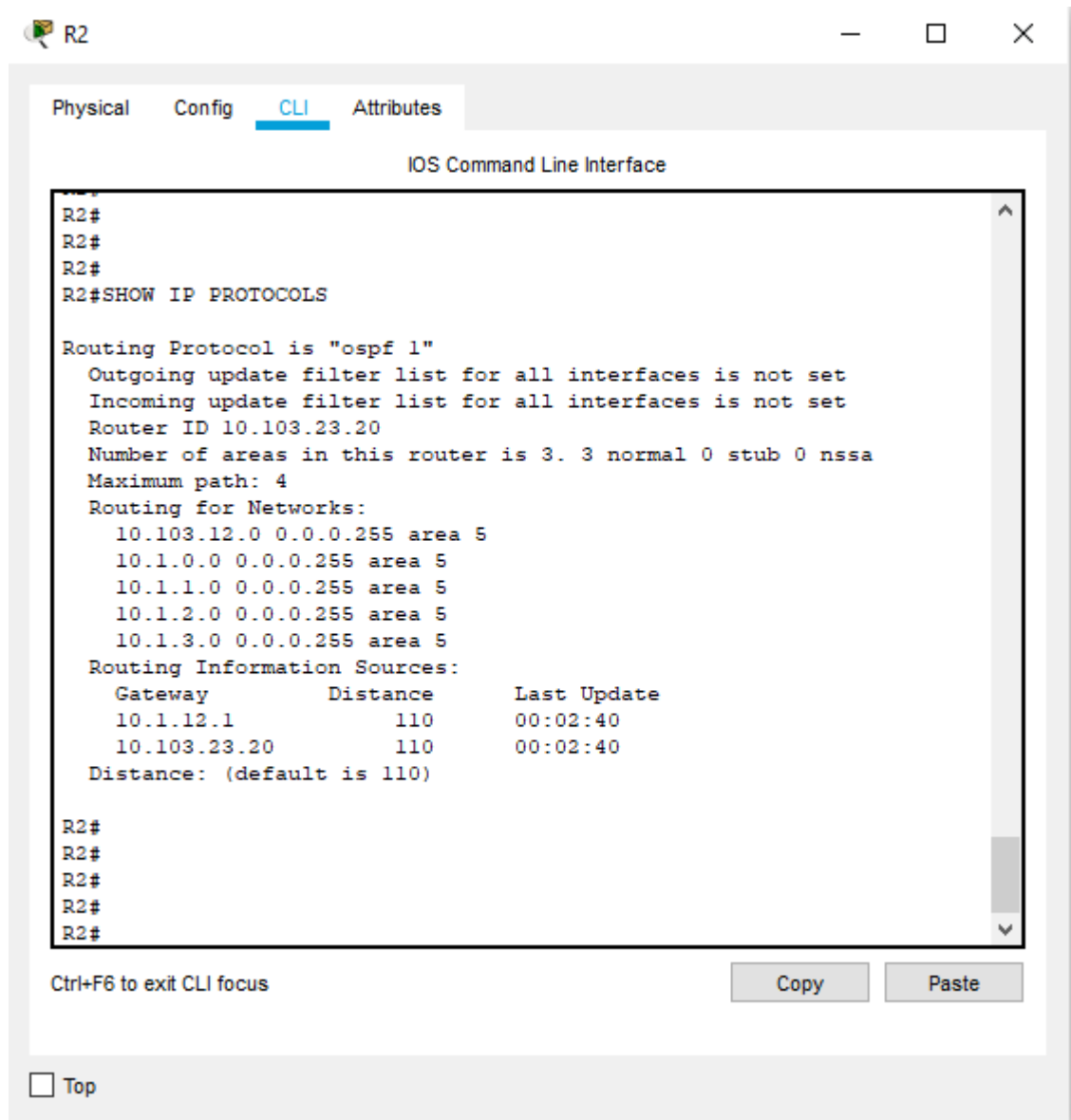


Figura 3. Configuración R2

Aquí encontraremos los comandos para darle un nombre a cada uno de los routers, así como para ingresar las direcciones IP de la interfaces, se ha tomado como referencia la figura principal del trabajo. Aquí a continuación tomamos como ejemplo la configuración del R2.

```
R2(config-if)#no shutdown           Activamos interface
R2(config-if)
#exit
R2(config)#interface s0/1          Ingresamos interface
R2(config-if)description to R3
R2(config-if)#ip address 10.103.23.1 255.255.255.0 se le da dirección
R2(config-if)#no shutdown          Activamos interfaz R2
(config-if)#exit
R2(config)#end
R2#wr
```

Aquí encontramos un ejemplo de un router que además requiere configuración de su interface serial, entonces se le configura el reloj y el ancho de banda para su óptimo funcionamiento.

```
Router>enable                       Se configura el ingreso a modo privilegiado
Router#configure                     Se configura el Ingreso a modo de configuración
Router(config)#hostname R3          Se configura para asignar nombre al router
R3(config)#router ospf 1            Se asigna protocolo ospf
R3(config-router)#network 10.103.23.0 255.255.255.0 area 5 Asignamos configuración IP
R3(config-router)#exit
R3(config)#interface s0/0
R3(config-if)description to R2
R3(config-if)#ip address 10.103.23.2 255.255.255.0
R3(config-if)#clock rate 128000     Asignamos configuración de clock
R3(config-if)#bandwidth 128         Se asigna bandwidth
R3(config-if)#no shutdown           Activamos interface
```

En el router R5 se puede evidenciar la correcta configuración del protocolo

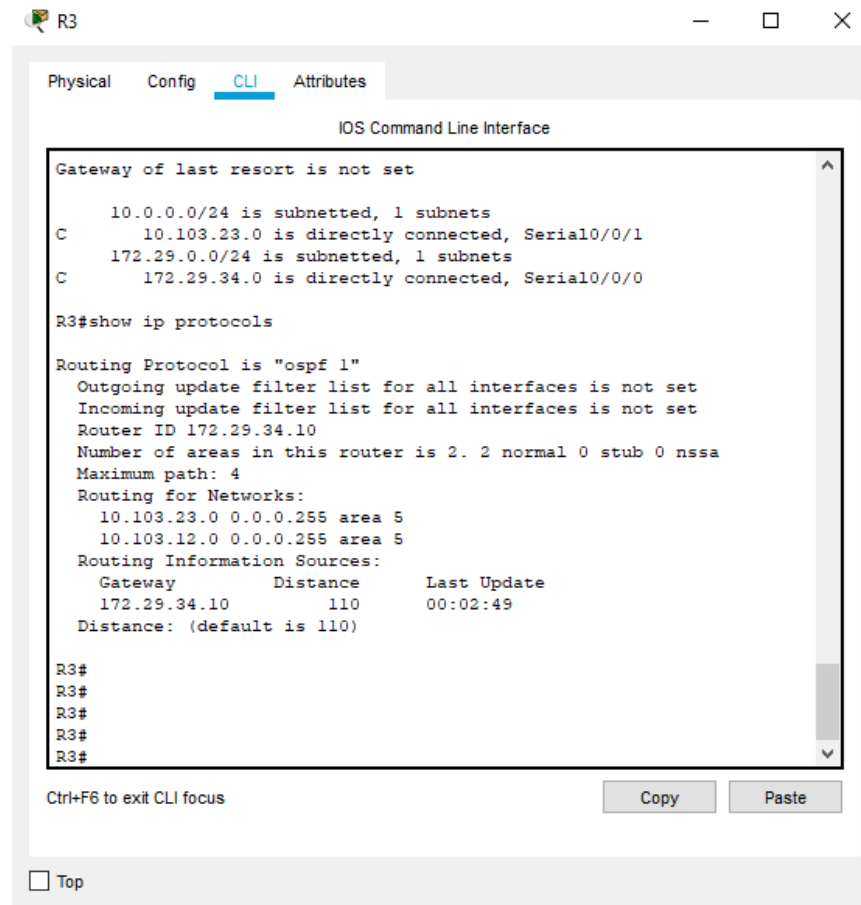


Figura 4. Protocolos en R3

Se muestra la evidencia del código en los demás routers, en este caso la configuración de router 4, aquí se configura lo básico y también características del protocolo EIGRP

```

Router>
Router>enable           ingreso a modo privilegiado
Router#configure       Modo de configuración
Router(config)#hostname R4   Nombre de router
R4(config)#router eigrp 15   Configuramos protocolo eigrp
R4(config-rtr)#network 172.29.34.0 255.255.255.0 configuración IP
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R4(config-rtr)#exit
R4(config)#interface s0/0   La Configuración del interfaz serial 0

```

```

R4(config-if)#ip address 172.29.34.2 255.255.255.0
R5(config-if)#no shutdown           Activamos interface
R4(config-if)#exit
R4(config)#interface s0/1           La Configuración del interfaz serial0/1
R4(config-if)#ip address 172.29.45.1 255.255.255.0
R5(config-if)#no shutdown           Activamos interface.
R4(config-if)#exit
R4(config)
#end

```

Como se puede observar el protocolo eigrp quedo bien configurado con su respectiva área 15

Aquí podemos observar la configuración del router 5, en este caso con protocolo EIGRP 15.

```

Router>enable                       Se configura el ingreso a modo privilegiado
Router#configure                     Se configura el Ingreso a modo de configuración
Router(config)#hostname R5           nombre al router
R5(config)#router eigrp 15           Configuramos Protocolo eigrp
R5(config-rtr)#eigrp router-id 5.5.5.5 La configuración nos permite Identificar el router
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R5(config)#interface s0/0 /          La Configuración del interfaz serial
R5(config-if)#ip address 172.29.45.2 255.255.255.0 Asignamos IP
R5(config-if)#no shutdown           Activamos interface
R5(config-if)#exit
R5(config)#end
R5#wr

```

Como se puede observar el protocolo eigrp quedo bien configurado con su respectiva área 15

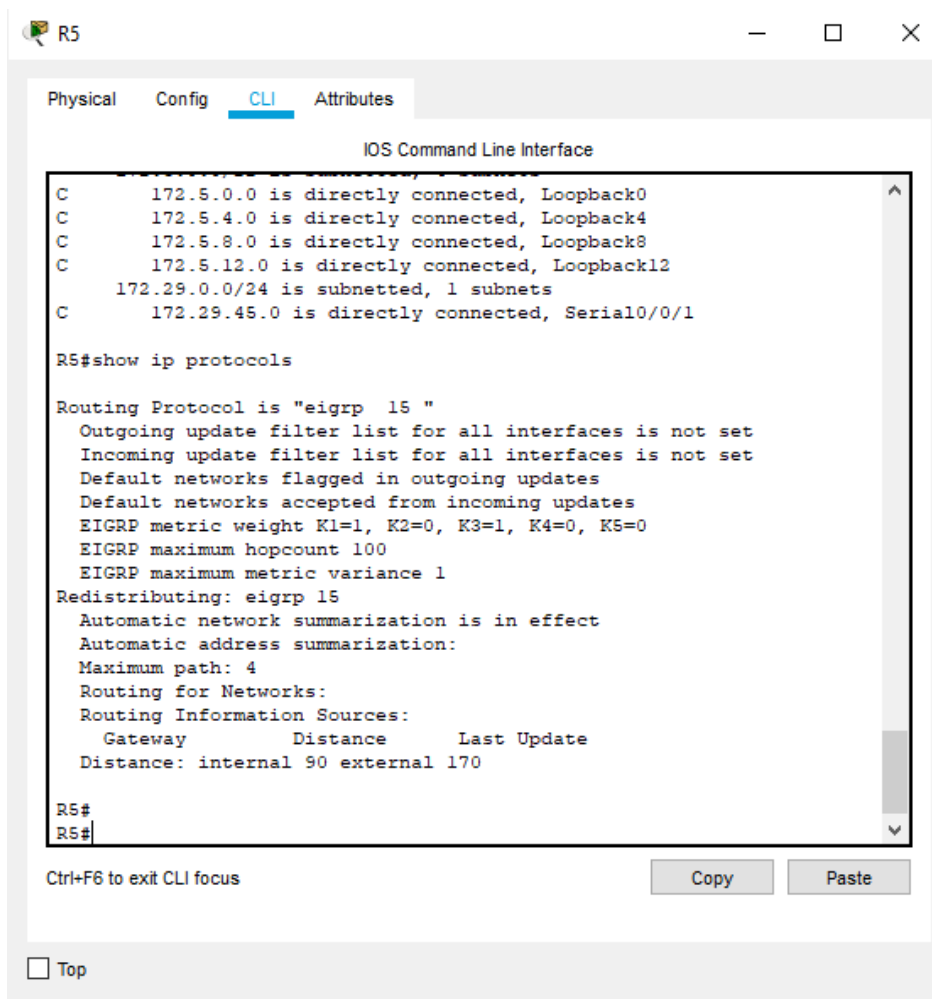


Figura 5. Protocolos en R5

En la figura de abajo se puede observar que la red empieza a converger por eso los pilotos verdes que indican que está en buen funcionamiento

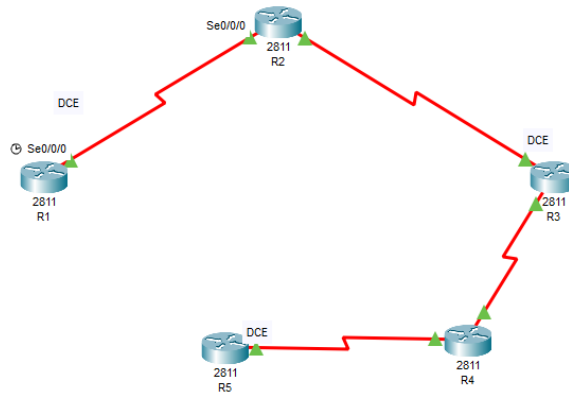


Figura 6. Evidencia del montaje

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.

Loopback en R1

R1#conf t

R1(config)#interface loopback 0
loopback 0

Configuramos y creamos la interfaz

R1(config-if)#ip address 10.1.0.1 255.255.252.0

Asignamos configuración IP

R1(config-if)#ip ospf 1 area 5

Configuramos en OSPF

R1(config-if)#exit

R1(config)# interface loopback 4
loopback 4

Configuramos y creamos la interfaz

R1(config-if)#ip address 10.1.4.1 255.255.252.0

Asignamos configuración IP

R1(config-if)#ip ospf 1 area 5

configuración en OSPF

R1(config-if)#exit

R1(config)# interface loopback 8
loopback 8

Configuramos y creamos la interfaz

R1(config-if)#ip address 10.1.8.1 255.255.252.0

Asignamos configuración IP

R1(config-if)#ip ospf 1 area 5

Configuración en OSPF

R1(config-if)#exit

R1(config)# interface loopback 12
loopback 12

Configuramos y creamos la interface

R1(config-if)#ip address 10.1.12.1 255.255.252.0

Asignamos IP

```
R1(config-if)#ip ospf 1 area 5
R1(config-if)#exit
R1(config)#end R1#wr
```

configuración en OSPF

A continuación, se muestra la evidencia de la configuración de las interfaces loopback en R1

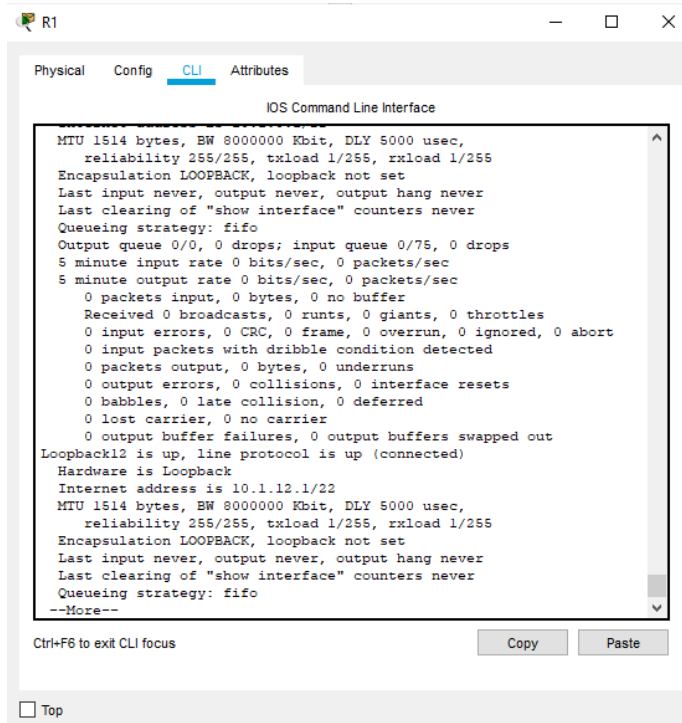


Figura 7. Interfaces en R1

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

```
R5#conf t
R5(config)#int Lo0
R5(config-if)#
R5(config-if)#ip address 172.5.0.1 255.255.252.0
R5(config-if)#exit
R5(config)#int Lo4
R5(config-if)#
R5(config-if)#ip address 172.5.0.2 255.255.252.0
```

Se configura interface loopB

Se le asigna IP

```

R5(config-if)#exit
R5(config)#int Lo8 Se configura interface loopB3
R5(config-if)#
R5(config-if)#ip address 172.5.0.3 255.255.252.0
R5(config-if)#exit
R5(config)#int Lo12 Se configura interface loopB4
R5(config-if)#
R5(config-if)#ip address 172.5.0.4 255.255.255.252
R5(config-if)#exit
R5(config)#router eigrp 15
R5(config-router)#no auto-summary
R5(config-router)#network 172.5.0.0 0.0.3.255 se publica red
R5(config-router)#exit
R5(config)#end

```

a continuación, veremos cómo quedaron configuradas las interfaces loopback por medio del comando show ip route:

```

R5
Physical Config CLI Attributes
IOS Command Line Interface
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

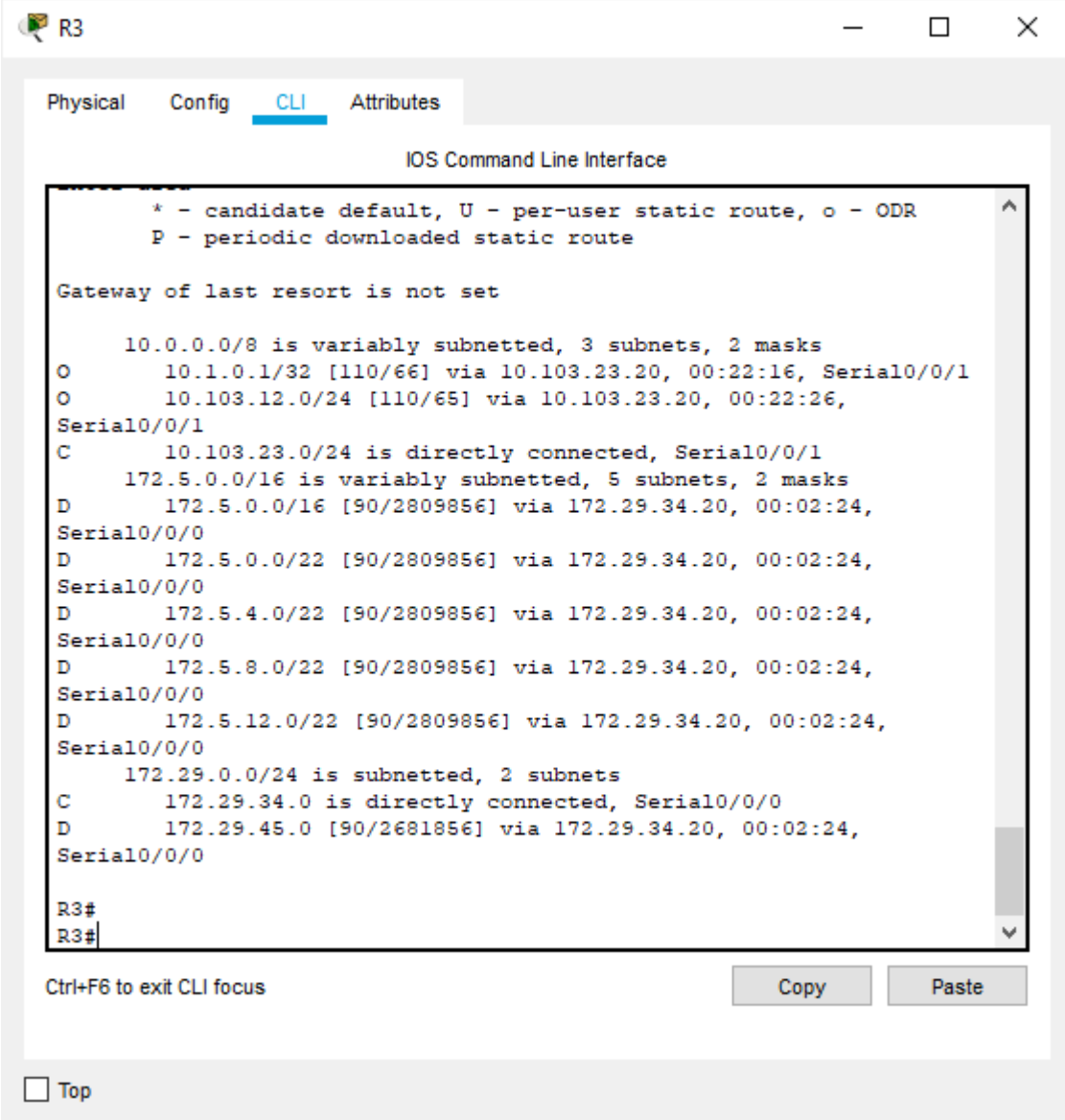
  10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX  10.1.0.1/32 [170/2707456] via 172.29.45.20, 00:01:10,
Serial10/0/1
D EX  10.103.12.0/24 [170/2707456] via 172.29.45.20, 00:01:10,
Serial10/0/1
D EX  10.103.23.0/24 [170/2707456] via 172.29.45.20, 00:01:10,
Serial10/0/1
  172.5.0.0/16 is variably subnetted, 5 subnets, 2 masks
D    172.5.0.0/16 [90/2809856] via 172.29.45.20, 00:02:48,
Serial10/0/1
C    172.5.0.0/22 is directly connected, Loopback0
C    172.5.4.0/22 is directly connected, Loopback4
C    172.5.8.0/22 is directly connected, Loopback8
C    172.5.12.0/22 is directly connected, Loopback12
  172.29.0.0/24 is subnetted, 2 subnets
D    172.29.34.0 [90/2681856] via 172.29.45.20, 00:02:48,
Serial10/0/1
C    172.29.45.0 is directly connected, Serial10/0/1

R5#
R5#
R5#

```

Figura 8. Enrutamiento en R5

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
Physical Config CLI Attributes
IOS Command Line Interface
* - 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
O 10.1.0.1/32 [110/66] via 10.103.23.20, 00:22:16, Serial0/0/1
O 10.103.12.0/24 [110/65] via 10.103.23.20, 00:22:26,
Serial0/0/1
C 10.103.23.0/24 is directly connected, Serial0/0/1
172.5.0.0/16 is variably subnetted, 5 subnets, 2 masks
D 172.5.0.0/16 [90/2809856] via 172.29.34.20, 00:02:24,
Serial0/0/0
D 172.5.0.0/22 [90/2809856] via 172.29.34.20, 00:02:24,
Serial0/0/0
D 172.5.4.0/22 [90/2809856] via 172.29.34.20, 00:02:24,
Serial0/0/0
D 172.5.8.0/22 [90/2809856] via 172.29.34.20, 00:02:24,
Serial0/0/0
D 172.5.12.0/22 [90/2809856] via 172.29.34.20, 00:02:24,
Serial0/0/0
172.29.0.0/24 is subnetted, 2 subnets
C 172.29.34.0 is directly connected, Serial0/0/0
D 172.29.45.0 [90/2681856] via 172.29.34.20, 00:02:24,
Serial0/0/0
R3#
R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

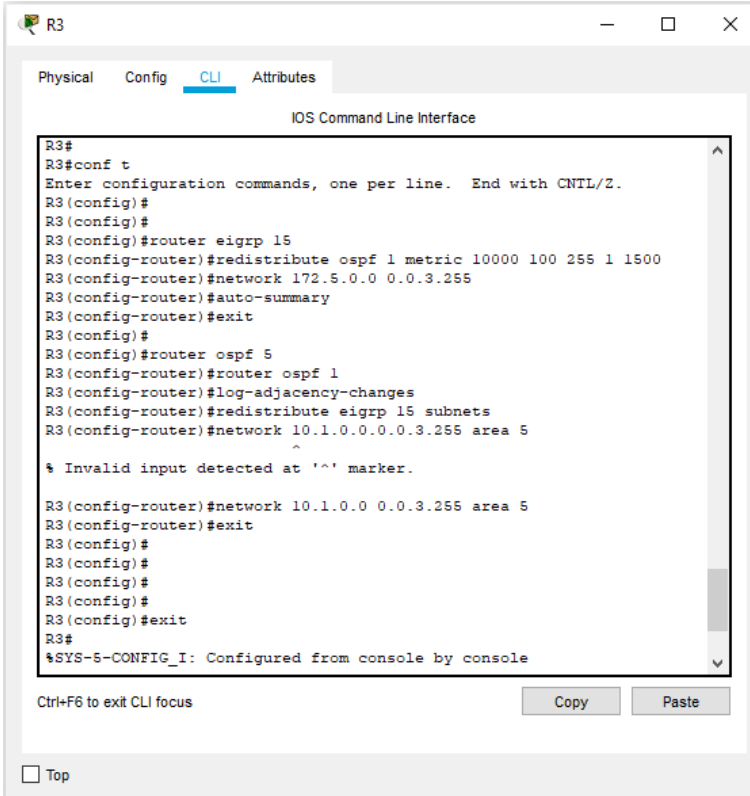
Figura 9. Enrutamiento en R3

En la figura se puede observar que el router ha logrado obtener información de las interfaces de loopback de los otros routers a través del protocolo OSPF, veamos que la loopback 10.1.3.12 la aprendió vía OSPF y también la 172.29.45.0 la adquirió por medio del protocolo EIGRP.

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

```
R3>en
R3#conf t
R3(config)#router eigrp 15                se configura protocolo
R3(config-router)#redistribute ospf 1 metric 10000 100 255 1 1500
R3(config-router)#network 172.5.0.0 0.0.3.255
R3(config-router)#auto-summary           se hacen publicacion auto
R3(config-router)#exit
R3(config)#router ospf 1
R3(config-router)#log-adjacency-changes
R3(config-router)#redistribute eigrp 15 subnets
R3(config-router)#network 10.1.0.0 0.0.3.255 area 5 se publica la red
R3(config-router)#exit
```

R3(config)#



```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3#
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3 (config)#
R3 (config)#
R3 (config)#router eigrp 15
R3 (config-router)#redistribute ospf 1 metric 10000 100 255 1 1500
R3 (config-router)#network 172.5.0.0 0.0.3.255
R3 (config-router)#auto-summary
R3 (config-router)#exit
R3 (config)#
R3 (config)#router ospf 5
R3 (config-router)#router ospf 1
R3 (config-router)#log-adjacency-changes
R3 (config-router)#redistribute eigrp 15 subnets
R3 (config-router)#network 10.1.0.0 0.0.3.255 area 5
R3#
^
% Invalid input detected at '^' marker.
R3 (config-router)#network 10.1.0.0 0.0.3.255 area 5
R3 (config-router)#exit
R3 (config)#
R3 (config)#
R3 (config)#
R3 (config)#
R3 (config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figura 10. Configuración en R3

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

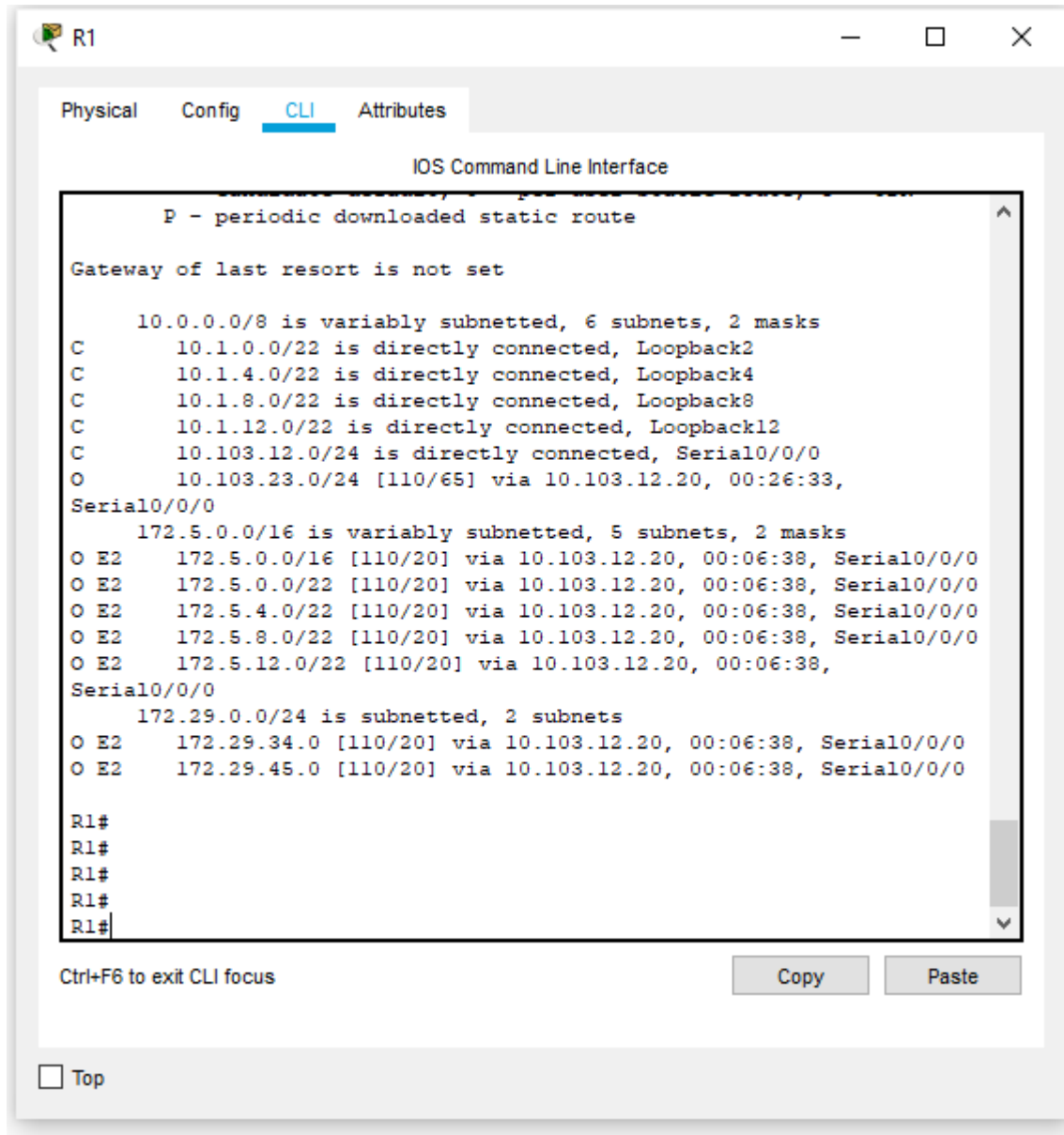


Figura 11. Enrutamiento en R1

En R1 se observa las rutas de las interfaces loopback configuradas en el otro router destino, es decir en R5, significa que desde aquí puedo contactar a el otro router

que está en otra área. En R5 se observa las rutas de las interfaces loopback configuradas en el otro router destino, es decir en R1, significa que desde aquí puedo contactar a el otro router que está en otra área.

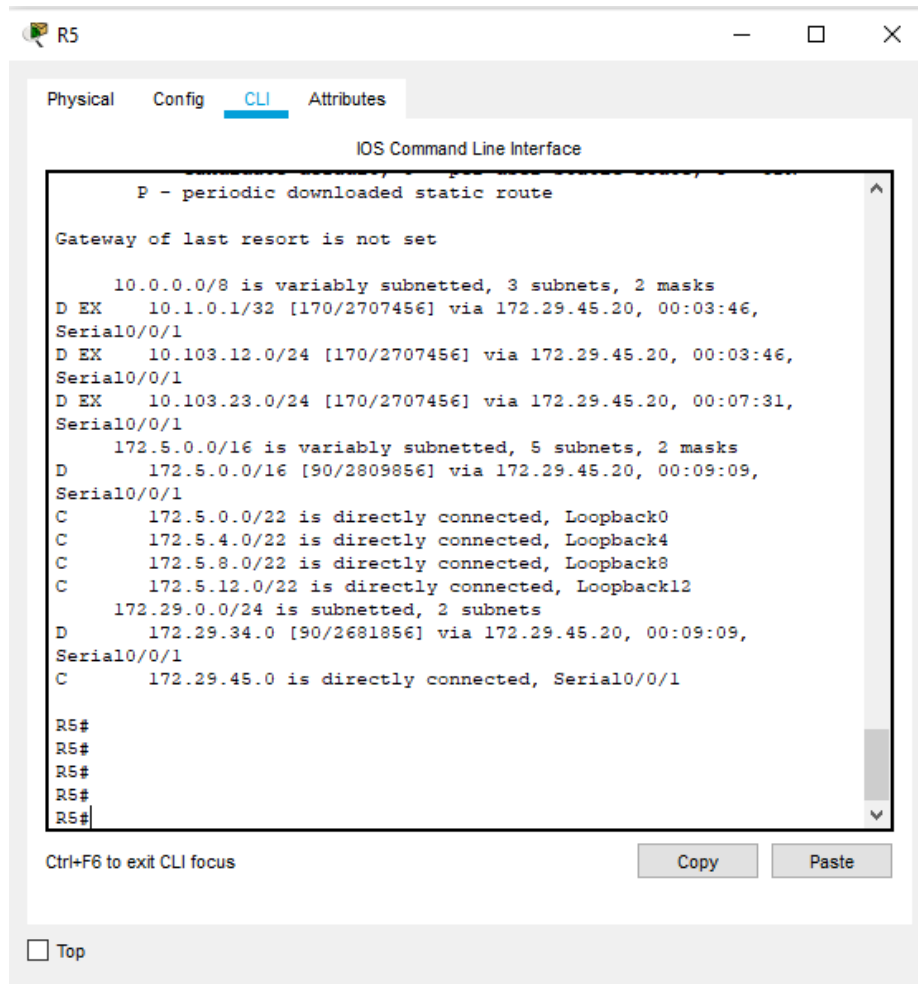


Figura 12. Enrutamiento en R5

Entre los dos router se puede tener una comunicación punto a punto desde las interfaces loopback, esto gracias a la buena configuración de los protocolos de enrutamiento.

Escenario 2

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

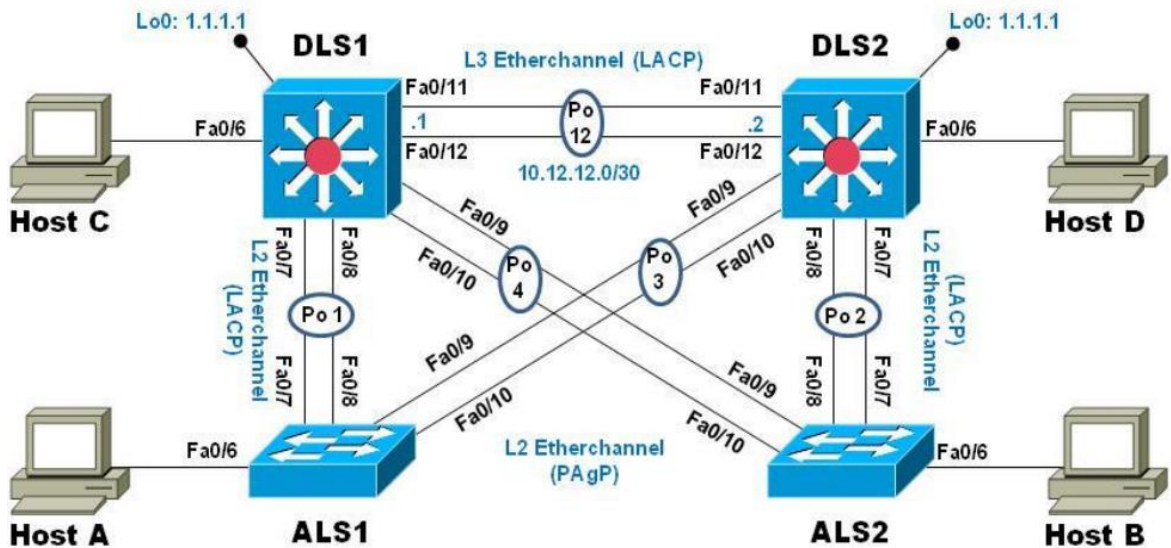


Figura 13. Escenario 2

Parte 1: Configurar la red de acuerdo con las especificaciones. a. Apagar todas las interfaces en cada switch. b. Asignar un nombre a cada switch acorde con el escenario establecido. c. Configurar los puertos troncales y Port-channels tal como se muestra en el diagrama.

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

a. Apagar todas las interfaces en cada switch.

Se ejecuta el comando para cada sw
Switch (config)# Interface range fa0/1-24
Switch (config-if-range)#sh

b. Asignar un nombre a cada switch acorde al escenario establecido.

Switch(config)#hostname DLS1
DLS1(config)#

```
Switch(config)#hostname DLS2
DLS2(config)#
Switch(config-if-range)#hostname ALS1
ALS1(config)#
Switch(config)#hostname ALS2
ALS2(config)#
```

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

```
DLS1(config-if)# int range fa0/7 - 8
DLS1(config-if-range)#no shutdown
DLS2(config-if-range)# int range fa0/7 - 10
DLS2(config-if-range)#no shutdown
ALS1(config)#int range fa0/7 - 10
ALS1(config-if-range)#no shutdown
ALS2(config-if-range)#int range fa0/7 - 10
ALS2(config-if-range)#no shutdown
```

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-if)# int range fa0/11 - 12
DLS1(config-if-range)#no switchport
DLS1(config-if-range)#no shutdown
DLS1(config-if-range)#channel-group 12 mode active
DLS1(config-if-range)#int po12
DLS1(config-if)#no sh
DLS1(config-if)#ip addr 10.12.12.1 255.255.255.252
```

En la figura 14, se puede evidenciar el uso del comando show etherchannel para revisar la encapsulación, el tamaño de los datos de tráfico en DLS1.

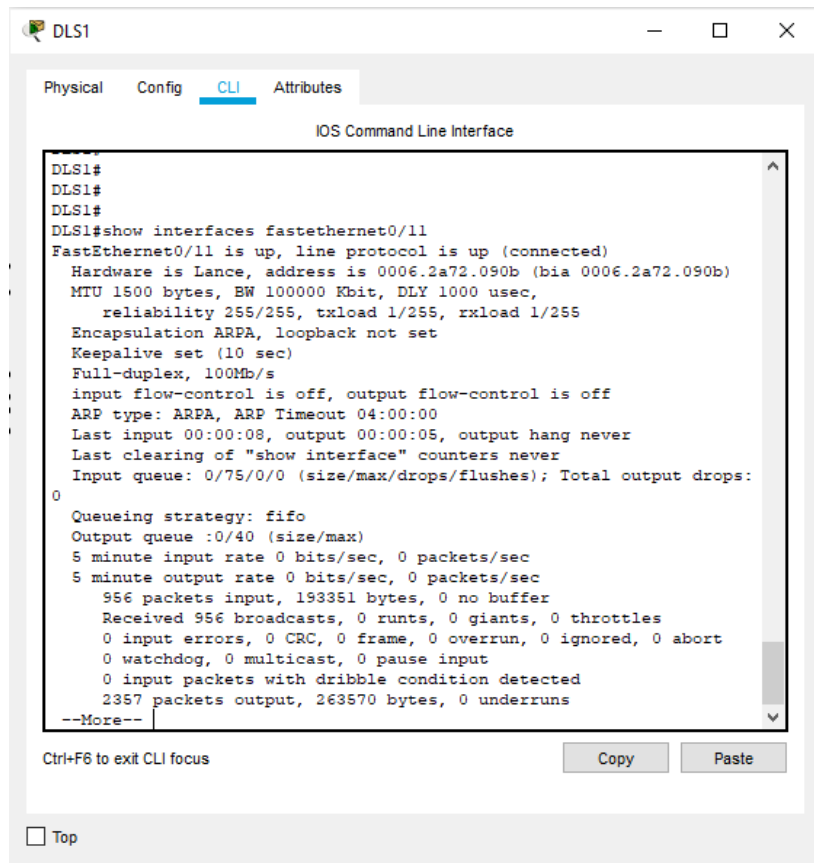


Figura 14. Interfaces en DLS1

```

DLS2(config-if-range)# int range fa0/11 - 8
DLS2(config-if-range)#no switchpor
DLS2(config-if-range)#
DLS2(config-if-range)#int po12
DLS2(config-if)#no sh
DLS2(config-if)#ip addr 10.12.12.2 255.255.255.252

```

El comando show interfaces es muy útil en este caso , aquí se puede observar que quedo bien configurado los puertos ya que nos indica que numero de interfaz y cual esta activada o desactivada.

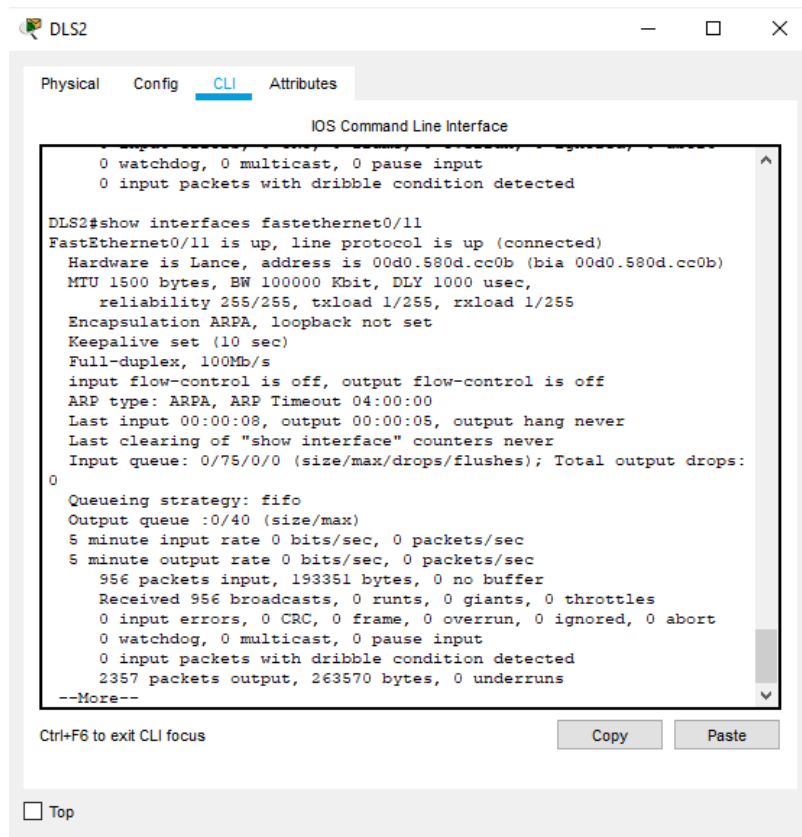


Figura 15. Interfaces DLS2

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

```

DLS1(config)# int range fa0/7 - 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)#int po1
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS2(config)# int range fa0/7 - 8
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#
DLS2(config-if-range)#channel-group 2 mode active
DLS2(config-if-range)#Creating a port-channel interface Port-channel 2
DLS2(config-if-range)#int po2
DLS2(config-if)#switchport trunk encapsulation dot1
DLS2(config-if)#switchport mode trunk

```

```
ALS1(config-if-range)#int range fa0/7 - 8
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 1 mode active
ALS1(config-if)#sw mode trunk
ALS2(config-if-range)#int range fa0/7 - 8
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#int po2
ALS2(config-if)#switchport mode trunk
ALS2(config-if)#
```

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

```
DLS1(config)# int range fa0/9-10
DLS1(config-if-range)#switch trunk encap dot1
DLS1(config-if-range)#sw mode trunk
DLS1(config-if-range)#channel-group 4 mode desirable
Creating a port-channel interface Port-channel 4
DLS1(config-if-range)#int po4
DLS1(config-if)#sw trunk encap dot
DLS1(config-if)#sw mode trun
DLS1(config-if)#
DLS2(config-if)# int range fa0/9-10
DLS2(config-if-range)#switch trunk encap dot1
DLS2(config-if-range)#sw mode trunk
DLS2(config-if-range)#channel-group 3 mode desirable
DLS2(config-if-range)#int po3
DLS2(config-if)#switch trunk encap dot1
DLS2(config-if)#sw mode trunk
ALS1(config-if)#int range fa0/9 - 10
ALS1(config-if-range)#sw mode trunk
ALS1(config-if-range)#channel-group 3 mode desirable
ALS1(config-if-range)#int po3
ALS1(config-if)#sw mode trunk
ALS2(config-if)#int range fa0/9 - 10
ALS2(config-if-range)#sw mode trunk
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#int po4
ALS2(config-if)#sw mode trun
```

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

```
DLS1(config)# int range fa0/7 - 10
DLS1(config-if-range)#switchport trunk native vlan 500
DLS1(config-if)#int po1
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#int po4
DLS1(config-if)#switchport trunk native vlan 500
DLS2(config-if)# int range fa0/7 - 10
DLS2(config-if-range)#switchport trunk native vlan 500
DLS2(config-if-range)#int po2
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#int po3
DLS2(config-if)#switchport trunk native vlan 500
ALS1(config-if-range)#int range fa0/7 - 10
ALS1(config-if-range)#switchport trunk native vlan 500
ALS1(config-if-range)#interface Port-channel1
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#interface Port-channel3
ALS1(config-if)#switchport trunk native vlan 500
ALS2(config-if)#int range fa0/7 - 10
ALS2(config-if-range)#switchport trunk native vlan 500
ALS2(config-if-range)#interface Port-channel2
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#interface Port-channel4
ALS2(config-if)#switchport trunk native vlan 500
```

En la figura queda evidenciado la creación de las vlans de forma satisfactoria, esto se logra por medio del comando show vlan.

DLS1#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Po4, Fa0/1, Fa0/2, Fa0/3 Fa0/4, Fa0/5, Fa0/13, Fa0/14 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
12 ADMON	active	
101 VENTAS	active	
111 MULTIMEDIA	active	Fa0/15
123 SEGUROS	active	
234 CLIENTES	active	
345 PERSONAL	active	
434 PROVEEDORES	active	
500 NATIVA	active	
567 VLAN0567	active	Fa0/16
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	
3456 VLAN3456	active	Fa0/6

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
12	enet	100012	1500	-	-	-	-	-	0	0
101	enet	100101	1500	-	-	-	-	-	0	0
111	enet	100111	1500	-	-	-	-	-	0	0
123	enet	100123	1500	-	-	-	-	-	0	0
234	enet	100234	1500	-	-	-	-	-	0	0
345	enet	100345	1500	-	-	-	-	-	0	0
434	enet	100434	1500	-	-	-	-	-	0	0
500	enet	100500	1500	-	-	-	-	-	0	0
567	enet	100567	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
3456	enet	103456	1500	-	-	-	-	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports
---------	-----------	------	-------

Figura 16. VLAN en DLS1

d) Configurar DLS1, ALS1, y ALS2 para utilizar VTP versión 3
DLS1(config)# vtp domain CISCO vtp ver 3
DLS1(config)# vtp password ccnp321
DLS2(config)#vtp version 3
ALS1(config)#vtp version 3
ALS2(config)#vtp version 3

Se aplica el comando VTP status para dilucidar las características de la configuración del protocolo VTP.

```
DLS1#SHOW VTP STATUS
VTP Version capable      : 1 to 2
VTP version running     : 2
VTP Domain Name         : UNAD
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 0001.C93A.BC30
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
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 : 15
Configuration Revision  : 40
MDS digest              : 0x01 0x3B 0x56 0x1B 0x2C 0x43 0x45 0x6C
                        : 0xB3 0xB1 0x8D 0xEA 0xD3 0xF5 0xDB 0xBC
```

Figura 17. VTP STATUTS

1) Utilizar el nombre de dominio CISCO con la contraseña ccnp321
DLS1(config)#vtp domain CISCO
DLS1(config)#vtp password ccnp321

2) Configurar DLS1 como servidor principal para las VLAN.
DLS1(config)#vtp mode server
Device mode already VTP SERVER.

3) Configurar ALS1 y ALS2 como clientes VTP.
ALS2(config)#vtp domain CISCO
Domain name already set to CISCO
ALS2(config)#vtp password ccnp321
Setting device VLAN
database password to ccnp321
ALS2(config)#vtp mode client
Setting device to VTP CLIENT mode.
ALS1(config)#vtp domain CISCO
Domain name already set to CISCO
ALS1(config)#vtp password ccnp321
Setting device VLAN database password to ccnp321

```
ALS1(config)#vtp mode client
Setting device to VTP CLIENT mode
```

```
ALS2#show vtp password
VTP Password: ccnp321
```

e) Configurar en el servidor principal las siguientes VLAN:

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

Tabla 1. Configuración VLAN

```
DLS1(config)#
DLS1(config-vlan)#name nativa
DLS1(config-vlan)#do wr
DLS1(config-vlan)#vlan 12
DLS1(config-vlan)#name admon
DLS1(config-vlan)#vlan 234
DLS1(config-vlan)#name clientes
DLS1(config-vlan)#vlan 1111
DLS1(config-vlan)#name multimedia
DLS1(config)#vlan 434
DLS1(config-vlan)#name proveedores
DLS1(config-vlan)#vlan 123
DLS1(config-vlan)#name seguros
```

```

DLS1(config-vlan)#vlan 1010
DLS1(config-vlan)#name ventas
DLS1(config)#vlan 3456
DLS1(config-vlan)#name personal

```

El comando show vlan aplicado al switch DLS1 nos permite ver las VLAN activas, el numero que las identifica.

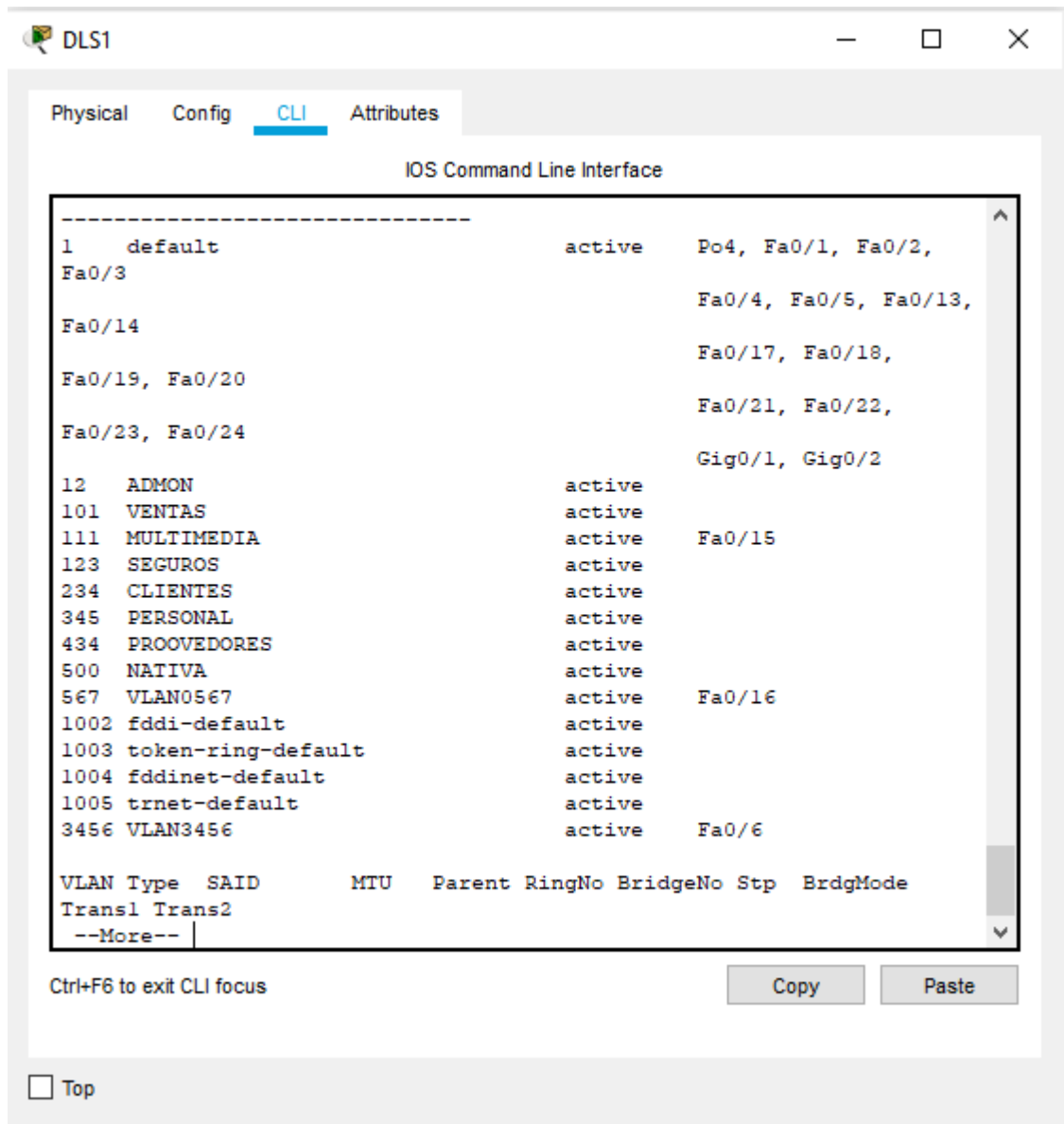


Figura 18. VLAN DLS1

f) En DLS1, suspender la VLAN 434.

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

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

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

```
DLS2(config)#vtp version 2
```

```
DLS2(config)#vtp mode transparent
```

```
Setting device to VTP TRANSPARENT mode.
```

```
DLS2(config)#vlan 500
```

```
DLS2(config-vlan)#name nativa
```

```
DLS2(config-vlan)#do wr
```

```
DLS2(config-vlan)#vlan 12
```

```
DLS2(config-vlan)#name admon
```

```
DLS2(config-vlan)#vlan 234
```

```
DLS2(config-vlan)#name clientes
```

```
DLS2(config-vlan)#vlan 1111
```

```
DLS2(config-vlan)#name multimedia
```

```
DLS2(config)#vlan 434
```

```
DLS2(config-vlan)#name proveedores
```

```
DLS2(config-vlan)#vlan 123
```

```
DLS2(config-vlan)#name seguros
```

```
DLS2(config-vlan)#vlan 1010
```

```
DLS2(config-vlan)#name ventas
```

```
DLS2(config)#vlan 3456
```

```
DLS2(config-vlan)#name personal
```

h) Suspender VLAN 434 en DLS2.

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

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

```
DLS2(config)#  
DLS2(config)#vlan 567  
DLS2(config-vlan)#name producción
```

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

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

```
DLS1(config-if-range)#switchport trunk allowed vlan all
```

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

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

Tabla 2. Configuración de Interfaces

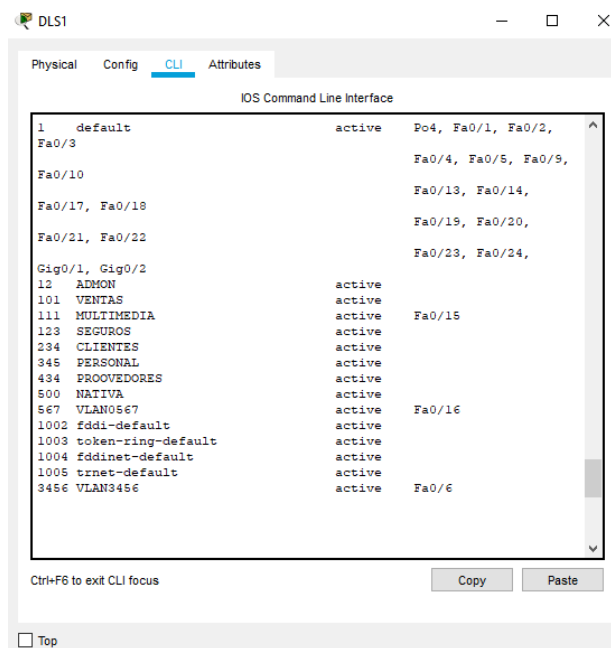
```
DLS1(config)#int fastethernet0/6
DLS1(config-if)#switchport mode access
DLS1(config-if)#sw access vlan 3456
DLS1(config-if)#int fastehernet0/15
DLS1(config-if)#switchport mode access
DLS1(config-if)#sw access vlan 1111
DLS1(config-if)#int fastethernet0/16
DLS1(config-if-range)#switchport mode access
DLS1(config-if-range)#sw access vlan 567
DLS2(config)# int fastethernet0/16
DLS2(config-if)#switchport mode access
DLS2(config-if)#sw access vlan 12
DLS2(config-if)#switchport access vlan 1010
ALS1(config)#int fa0/6
ALS1(config-if)#no sh
ALS1(config-if)#switchport mode access
ALS1(config-if)#sw access vlan 123
ALS1(config-if)#sw access vlan 1010
ALS1(config-if)#int fa0/15
ALS1(config-if)#switchport mode ac
ALS1(config-if)#switchport mode access
ALS1(config-if)#sw access vlan 1111
ALS2(config)#int fa0/6
ALS2(config-if)#no sh
ALS2(config-if)#sw mode access
ALS2(config-if)#sw access vlan 234
```

ALS2(config-if)#sw access vlan 1111

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.

Aquí podemos verificar que quedaron creadas correctamente.



```
IOS Command Line Interface
1  default          active  Po4, Fa0/1, Fa0/2,
Fa0/3              Fa0/4, Fa0/5, Fa0/9,
Fa0/10            Fa0/13, Fa0/14,
Fa0/17, Fa0/18    Fa0/19, Fa0/20,
Fa0/21, Fa0/22    Fa0/23, Fa0/24,
Gig0/1, Gig0/2
12  ADMON          active
101  VENTAS        active
111  MULTIMEDIA    active  Fa0/15
123  SEGUROS       active
234  CLIENTES     active
345  PERSONAL     active
434  PROVEEDORES  active
500  NATIVA        active
567  VLAN0567      active  Fa0/16
1002 fddi-default    active
1003 token-ring-default active
1004 fddinet-default active
1005 vtrnet-default active
3456 VLAN3456     active  Fa0/6
```

Figura 19. Verificación en DSL1

Aquí podemos verificar que quedaron creadas correctamente.

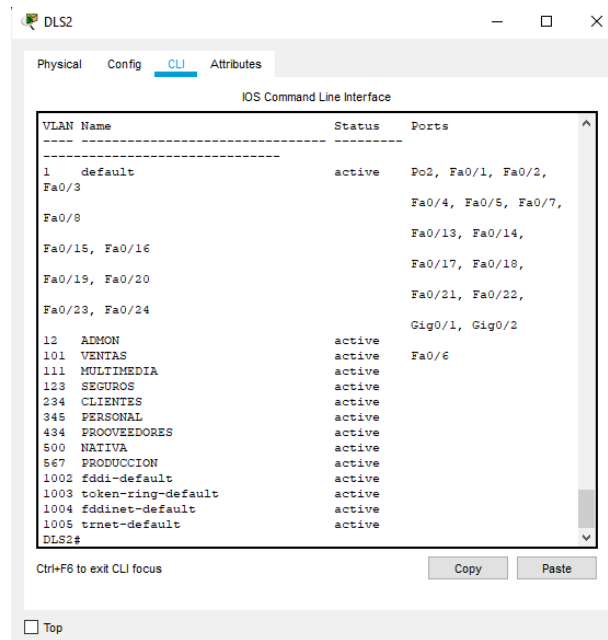


Figura 20. Verificación en DSL2

Aquí podemos verificar que quedaron creadas correctamente.

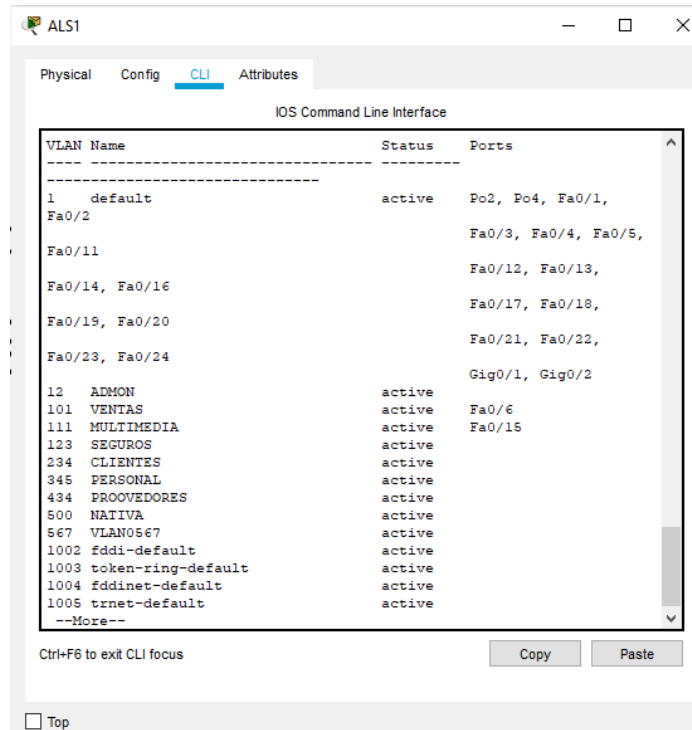


Figura 21. Verificación en ALS1

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

Por medio del comando show etherchannel podemos evidenciar en DLS1 la correcta configuración, así mismo detalles del protocolo propietario LACP.

```
DLS1# show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 3
Number of aggregators:          3

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          LACP       Fa0/7(P) Fa0/8(P)
4      Po4(SD)          -
12     Po12(RD)         -
DLS1#
```

Figura 22. EtherChannel DLS1

Por medio del comando show etherchannel podemos evidenciar en DLS1 la correcta configuración, así mismo detalles del protocolo propietario PAGP

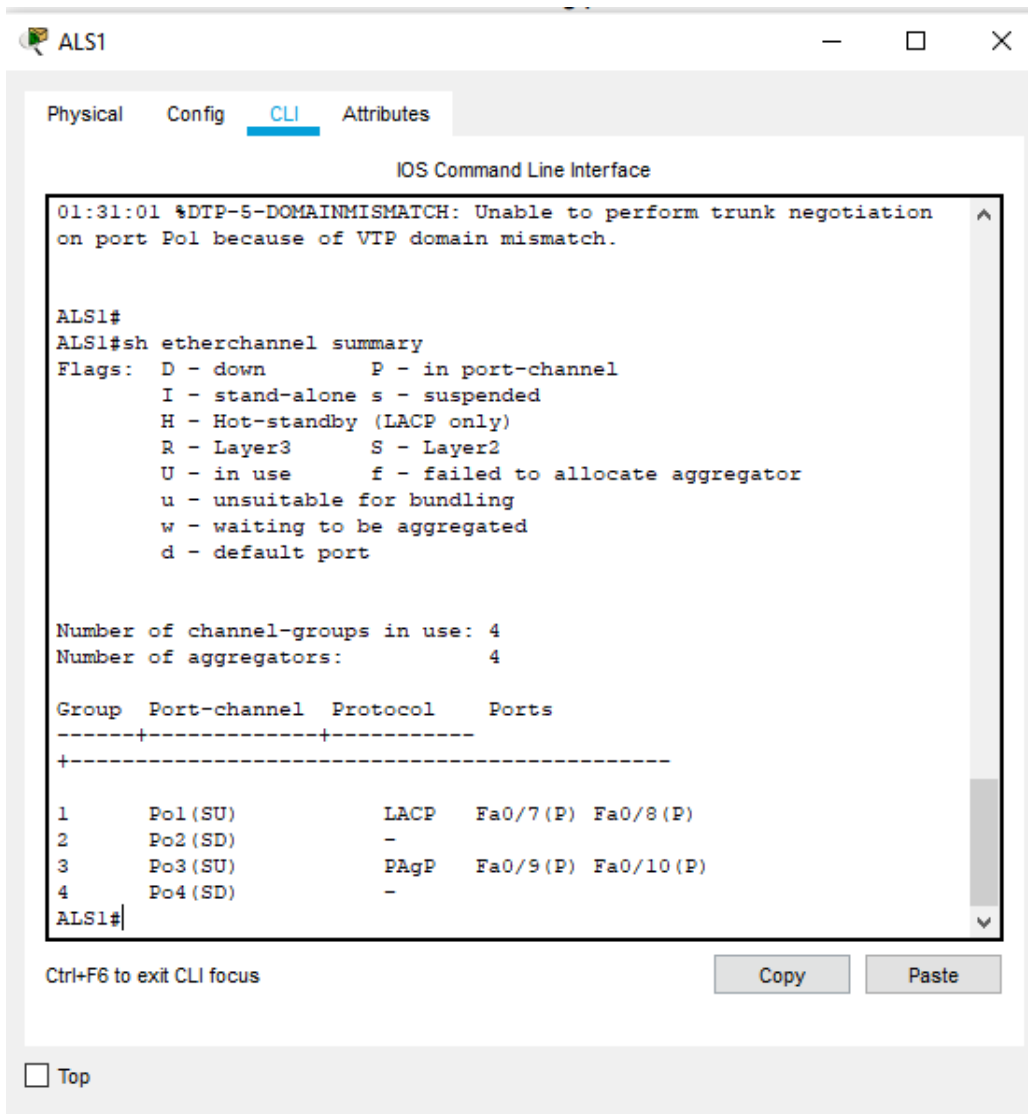


Figura 23. EtherChannel ALS1

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

En el switch DLS1 podemos ver la evidencia de como quedo configurado el protocolo STP al detalle en cada VLAN, y detalles de su interface.

DLS1:

```

Spanning tree enabled protocol ieee
Root ID Priority 24577
Address 00E0.F73E.2683
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24577 (priority 24576 sys-id-ext 1)
Address 00E0.F73E.2683
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Pol Root FWD 9 128.27 Shr

VLAN0345
Spanning tree enabled protocol ieee
Root ID Priority 33113
Address 0001.64E5.7A0D
Cost 18
Port 27 (Port-channel1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 33113 (priority 32768 sys-id-ext 345)
Address 00E0.F73E.2683
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Pol Root FWD 9 128.27 Shr

VLAN0434
Spanning tree enabled protocol ieee
Root ID Priority 25010
Address 00E0.F73E.2683
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 25010 (priority 24576 sys-id-ext 434)
Address 00E0.F73E.2683
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Pol Desg FWD 9 128.27 Shr

VLAN0500
Spanning tree enabled protocol ieee
Root ID Priority 25076
Address 00E0.F73E.2683
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 25076 (priority 24576 sys-id-ext 500)
Address 00E0.F73E.2683
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Pol Desg FWD 9 128.27 Shr

VLAN0101
Spanning tree enabled protocol ieee
Root ID Priority 24677
Address 00E0.F73E.2683
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24677 (priority 24576 sys-id-ext 101)
Address 00E0.F73E.2683
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Pol Desg FWD 9 128.27 Shr

VLAN0111
Spanning tree enabled protocol ieee
Root ID Priority 24687
Address 00E0.F73E.2683
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```

Figura 24. Spanning tree DLS1

En el switch DLS1 podemos ver la evidencia de como quedo configurado el protocolo STP al detalle en cada VLAN, y detalles de su interface.

DLS2:

```

VLAN0012
Spanning tree enabled protocol ieee
Root ID Priority 24599
Address 00E0.F73E.2683
Cost 18
Port 28 (Port-channel3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28694 (priority 28672 sys-id-ext 12)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Root FWD 9 128.28 Shr

VLAN0101
Spanning tree enabled protocol ieee
Root ID Priority 24677
Address 00E0.F73E.2683
Cost 18
Port 28 (Port-channel3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28773 (priority 28672 sys-id-ext 101)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Root FWD 9 128.28 Shr

VLAN0111
Spanning tree enabled protocol ieee
Root ID Priority 24697
Address 00E0.F73E.2683
Cost 18
Port 28 (Port-channel3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 28783 (priority 28672 sys-id-ext 111)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Root FWD 9 128.28 Shr

VLAN0123
Spanning tree enabled protocol ieee
Root ID Priority 24699
Address 0001.64E5.7A0D
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

VLAN0345
Spanning tree enabled protocol ieee
Root ID Priority 33113
Address 0001.64E5.7A0D
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 33113 (priority 32768 sys-id-ext 345)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Desg FWD 9 128.28 Shr

VLAN0434
Spanning tree enabled protocol ieee
Root ID Priority 28010
Address 00E0.F73E.2683
Cost 18
Port 28 (Port-channel3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 29106 (priority 28672 sys-id-ext 434)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Root FWD 9 128.28 Shr

VLAN0500
Spanning tree enabled protocol ieee
Root ID Priority 28076
Address 00E0.F73E.2683
Cost 18
Port 28 (Port-channel3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 29172 (priority 28672 sys-id-ext 500)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Root FWD 9 128.28 Shr

VLAN0567
Spanning tree enabled protocol ieee
Root ID Priority 33335
Address 0001.64E5.7A0D
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 33335 (priority 32768 sys-id-ext 567)
Address 0001.64E5.7A0D
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

```

Figura 25. Spanning tree DLS2

CONCLUSIONES

Para el primer escenario se trabajó con dos protocolos de enrutamiento fundamentalmente, uno de ellos OSPF, este protocolo requiere que el administrador tenga un conocimiento sobre lo que es un AS. un AS es un (sistema autónomo) en redes más pequeñas llamadas áreas. Las actualizaciones y el recálculo de la topología en este escenario se producen dentro de cada área. Esto hace que los cálculos de enrutamiento solo afecten a un solo área, excluyendo a las demás.

También es necesario recalcar la importancia de EIGRP en este escenario, ya que es un protocolo sencillo y fácil de implementar. Este protocolo ayuda a muchos procesos dentro de la implementación de red, ayuda a saber cuándo se presentan fallos en la topología, permite conocer dispositivos que son vecinos o están conectados adyacentemente y ayuda a enrutar de manera ordenada las direcciones de las redes aprendidas, estas características fueron de gran ayuda al empezar a resolver problemas en el escenario 1.

En el segundo escenario se utilizó la herramienta de vlan esta presenta grandes ventajas ya que, al reducir el dominio de broadcast, también se consigue un mejor rendimiento. De esta forma, los mensajes de difusión no tienen que atravesar toda la red. Cuando los mensajes son del mismo tipo para todos los participantes, pero solo tienen que llegar a un determinado grupo de personas, generan un tráfico innecesario. Con una VLAN, se minimiza la carga innecesaria del ancho de banda.

El rol de VTP en el segundo escenario fue el de mantener la configuración de VLAN de manera unificada en todo un dominio administrativo de red común. VTP es un protocolo de mensajería que usa tramas de enlace troncal de Capa 2 para agregar, borrar y cambiar el nombre de las VLAN en un solo dominio. VTP también admite cambios centralizados que se comunican a todos los demás switches de la red.

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). First Hop Redundancy Protocols. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de :

<https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ>

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). Campus Network Security. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de:

<https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ>

InterVLAN Routing Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de:

<https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

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