

**DIPLOMADO DE PROFUNDIZACIÓN CISCO CERTIFIED NETWORK
PROFESSIONAL - CCNP**

PRUEBA DE HABILIDADES PRÁCTICAS

JORGE ANDES JACOME SARABIA

**Universidad Nacional Abierta y a Distancia - UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI
Programa de Ingeniería Electrónica
Santa Marta D.T.C.H.
2020**

**DIPLOMADO DE PROFUNDIZACIÓN CISCO CERTIFIED NETWORK
PROFESSIONAL - CCNP**

PRUEBA DE HABILIDADES PRÁCTICAS

JORGE ANDES JACOME SARABIA

COD: 1091656101

**DIPLOMADO DE PROFUNDIZACIÓN COMO OPCIÓN DE GRADO PARA LA
OBTENCIÓN DE TÍTULO DE
INGENIERO ELECTRÓNICO**

ING. PAULITA FLOR

TUTORA ASIGNADA

**Universidad Nacional Abierta y a Distancia - UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI
Programa de Ingeniería Electrónica
Santa Marta D.T.C.H.
2020**

Nota de aceptación:

Presidente del Jurado

Jurado

Jurado

Santa Marta D.T.C.H, Julio de 2020

Agradecimientos

Agradezco inicialmente a Dios que me permite despertar cada día lleno de vida, energía y anhelos en mi corazón, a mi madre Alcira Sarabia quien ayudo a forjar mi carácter, mis ganas de salir adelante y sobre todo quien me heredó su espíritu de superación, a mi esposa Yissan Zuleta que me acompaña cada día, quien me brinda su respeto, su comprensión, su tolerancia y su amor, igualmente agradezco a mi tía Estela Jácome y mi abuela Yolanda Cogollo quienes fueron pilar fundamental cuando inicie este proyecto de vida, a la UNAD y todos esos tutores que me acompañaron en este proceso y me brindaron las herramientas necesarias para apropiarme de los conocimientos, a aquellos quienes estuvieron siempre atentos a solucionar cualquier problema, Ing. Camilo Acuña, Ing. Alexander Flórez, Ing. Pedro Fuentes, especialmente a la Ingeniera Nancy Guaca y a la Ingeniera Paulita Flor quien me acompaña en este proceso formativo presta a solventar mis interrogantes.

Finalmente agradezco a mis amigos más cercanos quienes me han acompañado a lo largo de mi carrera universitaria y hoy están felices con mis logros. Infinitas gracias a todos.

Contenido

Agradecimientos	4
Contenido.....	5
Listas de Tablas.....	5
Listas de Figuras.....	5
Glosario.....	7
Resumen.....	8
Abstract.....	8
Introducción	9
Escenario 1	10
Topología de Red - Escenario 1.....	10
Escenario 2	33
Topología de Red - Escenario 2.....	33
Conclusión	59
Bibliografía	60
Anexos	62
Simulación de Escenario 1	62
Simulación de Escenario 2	62

Listas de Tablas

Tabla 1. Tabla de direccionamiento IPv4 e IPv6.....	12
Tabla 2. Configuración de VLAN en el servidor principal.....	44
Tabla 3. Configuración de las interfaces como puertos de acceso, asignados a las VLAN	51

Listas de Figuras

Figura 1. Topología de Red propuesta – escenario 1.....	10
Figura 2. Simulación de la topología de Red especificada en GNS3 v.2.2.8	11
Figura 3. Tabla de enrutamiento ipv4 en R1-CALI.....	21
Figura 4. Tabla de enrutamiento ipv6 en R1-CALI.....	22
Figura 5. Tabla de enrutamiento ipv4 en R2-OCAÑA	23
Figura 6. Tabla de enrutamiento ipv6 en R2-OCAÑA	24

Figura 7. Tabla de enrutamiento ipv4 en R3-BARRANQUILLA	25
Figura 8. Tabla de enrutamiento ipv6 en R3-BARRANQUILLA	26
Figura 9. Verificación de comunicación desde R1-CALI	27
Figura 10. Verificación de comunicación desde R2-OCAÑA	28
Figura 11. Verificación de comunicación desde R3-BARRANQUILLA.	29
Figura 12. Verificación de rutas en R1-CALI.....	30
Figura 13. Verificación de rutas en R2-OCAÑA.	31
Figura 14. Verificación de rutas en R3-BARRANQUILLA	32
Figura 15. Topología de Red propuesta – escenario 2.	33
Figura 16. Simulación de la topología de Red especificada en Cisco Packet Tracer v.7.3.0.0837	34
Figura 17. Packet Tracer - Switch no soporta vlans extendidas.	45
Figura 18. Verificación de Vlans en Switch DLS1	54
Figura 19. Verificación de Vlans en Switch DLS2	54
Figura 20. Verificación de Vlans en Switch ALS1	55
Figura 21. Verificación de Vlans en Switch ALS2.	55
Figura 22. Verificación de EtherChannel en DLS1.....	56
Figura 23. Verificación de EtherChannel en ALS1.	56
Figura 24. Verificación de configuración de Spanning tree en DLS1	57
Figura 25. Verificación de configuración de Spanning tree en DLS2	58

Glosario

CCNA (Cisco Certified Networking Associate): Considerada actualmente como una de las certificaciones más importantes a nivel de la tecnología de la información, específicamente en redes.

CCNP: (Cisco Certified Networking Professional): A nivel profesional, este módulo de CISCO brinda todas las herramientas para diseñar y dar solución a todo lo referente a redes empresariales.

Router: Definido como un módulo que permite la conectividad entre los diferentes dispositivos conformados por varias redes, su función principal es establecer una ruta por donde viajaran los paquetes de datos de una red a otra. Su nombre proviene de enrutador o Router en Ingles.

Switch: Se considera un dispositivo de interconexión, pero a diferencia del Router, este se encarga de conectar equipos de una misma red.

EIGRP (Enhanced Interior Gateway Routing Protocol): Es un protocolo de ruteo de tipo versión distancia. Su implementación aumenta el potencial de las redes reduciendo los tiempos de convergencia.

OSPF (Open Shortest Path First): Este es un protocolo de direccionamiento tipo enlace-estado, su función es calcular la ruta más corta entre dos nodos.

VLAN (Virtual Local Area Network): Crea redes virtuales dentro de una sola red física su función es disminuir el domino de difusión y mejorar la administración de la red.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus

Etherchannel: Hace parte de las tecnologías de CISCO, basada en los estándares 802.3 Full-Duplex y Fast Ethernet; su función principal es la agrupación lógica de varios enlaces físicos Ethernet.

PAgP: Es un protocolo de CISCO, se encarga de agrupar puertos con características similares.

LACP: Igual que PAgP es un protocolo de CISCO que puede agrupar puertos con características similares. Es un protocolo definido en el estándar 802.3ad. Sus modos de configuración son activo y pasivo.

Resumen

El objeto de este documento, consiste fundamentalmente en la aplicación de los conocimientos adquiridos en el campo profesional de las Redes demostrando amplia habilidad, capacidad de planificación, implementación y verificación de soluciones de redes complejas.

Como consecuencia, se ha dado solución práctica y concreta a los escenarios propuestos, en ellos se implementa el uso del simulador GNS3 v2.2.8 donde se aplican las temáticas relacionadas con los principios básico de redes y sus protocolos de enrutamiento IP en versiones IPv4 e IPv6, protocolo EIGRP, OSPF y BGP.

Por otro lado, se evidencia el conocimiento mediante la función de las distintas técnicas en cuanto a la administración de la conmutación en la arquitectura de una red empresarial mediante la implementación de VLANs, configuración de Switches capa 2 y capa 3 y disposición de seguridad en redes LAN y WAN, de tal forma que se evidencia la amplia comprensión arquitectónica y profundización de habilidades requeridas por las redes empresariales

Palabras claves: *Redes, GNS3, Packet Tracer, IPv4, IPv6, EIGRP, OSPF, BGP, VLANS*

Abstract

The purpose of this document is the application of the knowledge acquired in the professional field of Networks, demonstrating ample ability, planning, and implementation and verification capacity for complex network solutions.

As a consequence, the practical and concrete solution to the proposed scenarios has been given, in them the use of the GNS3 v2.2.8 simulator is implemented, where the topics related to the basic principles of networks and their IP routing protocols are seen in IPv4 versions and IPv6, EIGRP protocol, OSPF and BGP.

On the other hand, the knowledge is evidenced by the function of the different techniques in terms of the management of the switch in the architecture of an enterprise network through the implementation of VLANs, configuration of layer 2 and layer 3 switches and provision of security in networks LAN and WAN, in such a way that the broad architectural understanding and depth of skills required by business networks is evident

Keywords: *Networks, GNS3, Packet Tracer, IPv4, IPv6, EIGRP, OSPF, BGP, VLANS*

Introducción

Según el informe de Cisco 2011 Cisco Connected World Technology Report, la importancia de las redes es considerado como un recurso fundamental en la vida diaria, vemos como día a día el internet se vuelve un recurso básico, cada vez hay más demanda, más consumo, el uso de dispositivos como teléfonos móviles o computadoras portátiles es masivo, e incluso gracias a esta tecnología es habitual hablar educación a distancia o de teletrabajo, pero, detrás de esto existen una serie de herramientas tecnológicas y protocolos encargadas de hacer esto posible, dichas herramientas se presentan en este documento donde se profundizan los conocimientos básicos de CCNA, Router, Switch dando un nuevo salto a CCNP.

Este informe documenta los pasos el desarrollo de la solución a los escenarios propuestos como diseño pedagógico; En el primer escenario, se tratan los contenidos del Módulo CCNP ROUTE CISCO, evidenciando el aprendizaje en los temas de principios básicos de Red, protocolos de enrutamiento IPv4 e IPv6, enrutamiento Gateway, EIGRP, OSPF y BGP; en el segundo escenario, se estudian los temas del módulo CCNP SWITCH CISCO, el cual apropia temáticas relacionadas con la implementación, conmutación en una arquitectura de Red, redes VLAN's, disponibilidad y redundancia de Switches de capa 2 y capa 3 y características de redes LAN y WAN.

Su objeto principal es demostrar los conocimientos adquiridos en el uso de comandos IOS, configuración de Routers, uso de protocolos de enrutamiento, direccionamiento, diseño e implementación de soluciones prácticas en ambientes LAN y WAN, para esto se emplean la herramienta de simulación y laboratorio GNS3 y Packet Tracer, el cual permite configurar los escenarios propuestos y analizar su comportamiento, identificar situaciones y resolver problemas.

Escenario 1

Una empresa de confecciones posee tres sucursales distribuidas en las ciudades de Cali, Barranquilla y Ocaña, 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, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Topología de Red - Escenario 1.

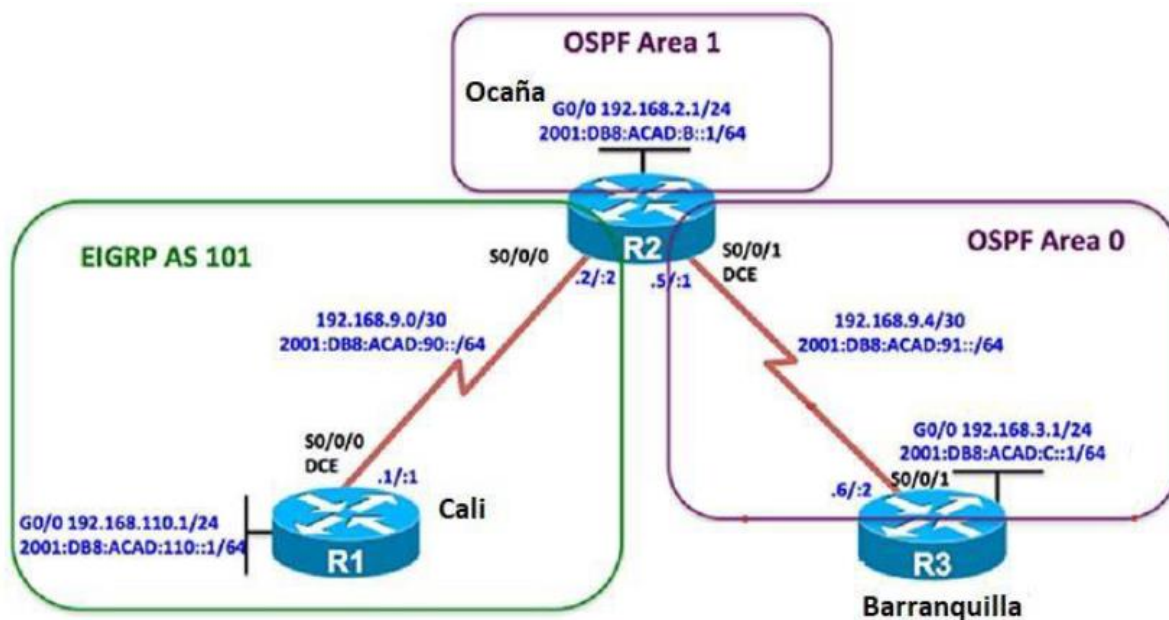


Figura 1. Topología de Red propuesta – escenario 1.

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Parte 1: Configuración del escenario propuesto

En este primer escenario, se utiliza el simulador GNS3 versión 2.2.8, con IOS actualizados, los conmutadores utilizados son:

- Tres Router C7200 versión 15.2
- Ethernet Switch versión 12.0

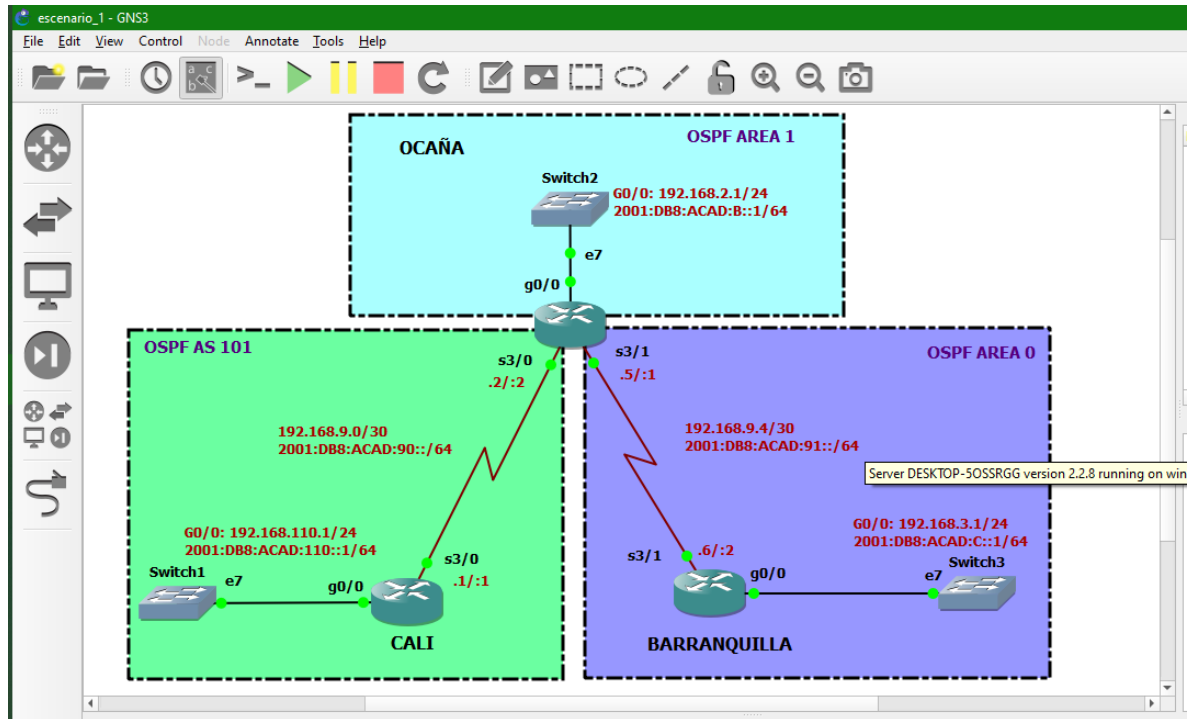


Figura 2. Simulación de la topología de Red especificada en GNS3 v.2.2.8

A continuación, se presenta una tabla de direccionamiento tomada de la topología de red indicada.

Tabla 1. Tabla de direccionamiento IPv4 e IPv6

Dispositivo	Interfaz	Dirección IP
R1 (CALI)	G0/0	192.168.110.1/24 2001:DB8:ACAD:110::1/64
	S3/0 DCE	192.168.110.9.1/30 2001:DB8:ACAD:90::1/64
R2 (OCAÑA)	G0/0	192.168.2.1/24 2001:DB8:ACAD:B::1/64
	S3/0	192.168.9.2/24 2001:DB8:ACAD:90::2/64
	S3/1 DCE	192.168.9.5/30 2001:DB8:ACAD:91::1/64
R3 (BARRANQUILLA)	G0/0	192.168.3.1/24 2001:DB8:ACAD:C::1/64
	S1/1	192.168.9.6/30 2001:DB8:ACAD:91::2/64

- 1. Configurar las interfaces con las direcciones IPv4 e IPv6 que se muestran en la topología de red.**
- 2. Ajustar el ancho de banda a 128 kbps sobre cada uno de los enlaces seriales ubicados en R1, R2, y R3 y ajustar la velocidad de reloj de las conexiones de DCE según sea apropiado.**

Estas primeras configuraciones son básicas, se realizan desde la configuración principal.

Basados en el direccionamiento de la tabla anterior, se realiza la asignación de direcciones IPv4 e IPv6 en cada Router.

R1 (CALI):

Router#conf t

Router(config)#hostname CALI

CALI(config)#ipv6 unicast-routing

CALI(config)#interface g0/0

```
CAL1(config-if)#ip add 192.168.110.1 255.255.255.0
CAL1(config-if)#ipv6 add 2001:db8:acad:110::1/64
CAL1(config-if)#no shutdown
CAL1(config-if)#exit
CAL1(config)#interface s3/0
CAL1(config-if)#ip add 192.168.9.1 255.255.255.252
CAL1(config-if)#ipv6 add 2001:db8:acad:90::1/64
CAL1(config-if)#clock rate 128000
CAL1(config-if)#bandwidth 128
CAL1(config-if)#no shutdown
CAL1(config-if)#exit
```

R2 (OCAÑA):

```
Router#conf t
```

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

```
Router(config)#hostname OCANA
OCANA(config)#interface g0/0
OCANA(config-if)#ip add 192.168.2.1 255.255.255.0
OCANA(config-if)#ipv6 add 2001:db8:acad:b::1/64
OCANA(config-if)#no shutdown
OCANA(config-if)#exit
OCANA(config)#interface s3/0
OCANA(config-if)#ip add 192.168.9.2 255.255.255.252
OCANA(config-if)#ipv6 add 2001:db8:acad:90::2/64
OCANA(config-if)#bandwidth 128
OCANA(config-if)#no shutdown
OCANA(config-if)#exit
OCANA(config)#interface s3/1
OCANA(config-if)#ip add 192.168.9.5 255.255.255.252
```

```
OCANA(config-if)#ipv6 add 2001:db8:acad:91::1/64
OCANA(config-if)#clock rate 128000
OCANA(config-if)#bandwidth 128
OCANA(config-if)#no shutdown
OCANA(config-if)#exit
```

R3 (B/QUILLA):

```
Router#conf t
Router(config)#hostname BARRANQUILLA
BARRANQUILLA(config)#interface g0/0
BARRANQUILLA(config-if)#ip add 192.168.3.1 255.255.255.0
BARRANQUILLA(config-if)#ipv6 add 2001:db8:acad:c::1/64
BARRANQUILLA(config-if)#no shutdown
BARRANQUILLA(config-if)#exit
BARRANQUILLA(config)#interface s3/1
BARRANQUILLA(config-if)#ip add 192.168.9.6 255.255.255.252
BARRANQUILLA(config-if)#ipv6 add 2001:db8:acad:91::2/64
BARRANQUILLA(config-if)#no shutdown
BARRANQUILLA(config-if)#exit
BARRANQUILLA(config)#
```

3. En R2 y R3 configurar las familias de direcciones OSPFv3 para IPv4 e IPv6. Utilice el identificador de enrutamiento 2.2.2.2 en R2 y 3.3.3.3 en R3 para ambas familias de direcciones.

OSPF hace parte de los protocolos de enrutamiento IP. OSPF En su versión 3 permite la compatibilidad para IPv4 e Ipv6. Para este primer escenario, aprovecharemos las ventajas que nos brinda OSPFv3 y configuraremos la red con este enrutamiento. El comando requerido es **router ospfv3**, pero se requiere que el enrutamiento Ipv6 este habilitado por lo que se hace fundamental utilizar el comando **ipv6 unicast-routing** antes de comenzar con las configuraciones.

R2 (OCAÑA):

```
OCANA(config)#ipv6 unicast-routing
OCANA(config)#router ospfv3 1
OCANA(config-router)#address-family ipv4 unicast
OCANA(config-router-af)#router-id 2.2.2.2
OCANA(config-router-af)#exit-address-family
OCANA(config-router)#address-family ipv6 unicast
OCANA(config-router-af)#router-id 2.2.2.2
OCANA(config-router-af)#exit-address-family
OCANA(config-router)#exit
OCANA(config)#
```

R3 (B/QUILLA):

```
BARRANQUILLA(config)#router ospfv3 1
BARRANQUILLA(config-router)#address-family ipv4 unicast
BARRANQUILLA(config-router-af)#router-id 3.3.3.3
BARRANQUILLA(config-router-af)#passive-interface g0/0
BARRANQUILLA(config-router-af)#exit-address-family
BARRANQUILLA(config-router)#address-family ipv6 unicast
BARRANQUILLA(config-router-af)#router-id 3.3.3.3
```

4. En R2, configurar la interfaz F0/0 en el área 1 de OSPF y la conexión serial entre R2 y R3 en OSPF área 0.

Para una correcta habilitación de las interfaces, usaremos el comando **ospfv3 pid [ipv4 | ipv6] area area-id**, ya que este comando nos permite la habilitación de ambas interfaces.

R2 (OCAÑA):

```
OCANA(config)#interface g0/0
OCANA(config-if)#ospfv3 1 ipv4 area 1
OCANA(config-if)#ospfv3 1 ipv6 area 1
```

```
OCANA(config-if)#interface s3/1
OCANA(config-if)#ospfv3 1 ipv4 area 0
OCANA(config-if)#ospfv3 1 ipv6 area 0
OCANA(config-if)#exit
```

5. En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área 0.

R3 (B/QUILLA):

```
BARRANQUILLA(config)#interface g0/0
BARRANQUILLA(config-if)#ospfv3 1 ipv4 area 0
BARRANQUILLA(config-if)#ospfv3 1 ipv6 area 0
BARRANQUILLA(config-if)#exit
BARRANQUILLA(config)#int s3/1
BARRANQUILLA(config-if)#ospfv3 1 ipv4 area 0
BARRANQUILLA(config-if)#ospfv3 1 ipv6 area 0
BARRANQUILLA(config-if)#exit
```

6. Configurar el área 1 como un área totalmente Stubby.

7. Propagar rutas por defecto de IPv4 y IPv6 en R3 al interior del dominio OSPFv3. Nota: Es importante tener en cuenta que una ruta por defecto es diferente a la definición de rutas estáticas.

CISCO nos ofrece el área Stubby la cual envía una ruta sumariada. Para definir un área totalmente stubby, utilizaremos el comando **area xx stub no-summary**.

R2 (OCAÑA):

```
OCANA(config)#router ospfv3 1
OCANA(config-router)#address-family ipv4 unicast
OCANA(config-router-af)#area 1 stub no-summary
OCANA(config-router-af)#default-information originate always
OCANA(config-router-af)#exit-address-family
```



```
OCANA(config-router)#address-family ipv6 unicast
OCANA(config-router-af)#area 1 stub no-summary
OCANA(config-router-af)#exit-address-family
OCANA(config-router)#exit
```

R3 (B/QUILLA):

```
BARRANQUILLA(config)#router ospfv3 1
BARRANQUILLA(config-router)#address-family ipv4 unicast
BARRANQUILLA(config-router-af)#default-information originate always
BARRANQUILLA(config-router-af)#exit-address-family
BARRANQUILLA(config-router)#address-family ipv6 unicast
BARRANQUILLA(config-router-af)#default-information originate always
BARRANQUILLA(config-router-af)#exit-address-family
BARRANQUILLA(config-router)#exit
```

8. Realizar la configuración del protocolo EIGRP para IPv4 como IPv6. Configurar la interfaz F0/0 de R1 y la conexión entre R1 y R2 para EIGRP con el sistema autónomo 101. Asegúrese de que el resumen automático está desactivado.

9. Configurar las interfaces pasivas para EIGRP según sea apropiado.

EIGRP permite configurar los dos tipos de familia de direcciones mediante los tres siguientes modos, **address-family configuration mode**, **address-family interface configuration mode** y **address-family topology configuration mode**.

Para entrar a estos modos, requerimos la utilización del siguiente comando **address-family ipv4 unicast autonomous-system 1**

Basados en esto, procedemos con la realización de los siguientes puntos de este primer escenario.

R1 (CALI):

```
CALI(config)#router eigrp dual-stack
CALI(config-router)#address-family ipv4 unicast autonomous-system 4
CALI(config-router-af)#af-interface g0/0
CALI(config-router-af-interface)#passive-interface
CALI(config-router-af-interface)#exit-af-interface
CALI(config-router-af)#network 192.168.9.0 0.0.0.3
CALI(config-router-af)#network 192.168.110.0 0.0.0.3
CALI(config-router-af)#eigrp router-id 1.1.1.1
CALI(config-router-af)#no shutdown
CALI(config-router-af)#address-family ipv6 unicast autonomous-system 6
CALI(config-router-af)#af-interface g0/0
CALI(config-router-af-interface)#passive-interface
CALI(config-router-af-interface)#exit-af-interface
CALI(config-router-af)#eigrp router-id 1.1.1.1
CALI(config-router-af)#no shutdown
CALI(config-router-af)#exit-address-family
CALI(config-router)#exit
CALI(config)#
```

R2 (OCAÑA):

```
OCANA(config)#router eigrp dual-stack
OCANA(config-router)#address-family ipv4 unicast autonomous-system 4
OCANA(config-router-af)#network 192.168.9.0 0.0.0.3
OCANA(config-router-af)#eigrp router-id 2.2.2.2
OCANA(config-router-af)#no shutdown
OCANA(config-router-af)#exit-address-family
OCANA(config-router)#address-family ipv6 unicast autonomous-system 6
OCANA(config-router-af)#af-interface g0/0
```

```
OCANA(config-router-af-interface)#shutdown
OCANA(config-router-af-interface)#exit-af-interface
OCANA(config-router-af)#af-interface s3/1
OCANA(config-router-af-interface)#shutdown
OCANA(config-router-af-interface)#exit-af-interface
OCANA(config-router-af)#eigrp router-id 2.2.2.2
OCANA(config-router-af)#no shutdown
OCANA(config-router-af)#exit-address-family
OCANA(config-router)#exit
OCANA(config)#
```

10. En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.

R2 (OCAÑA):

```
OCANA(config)#router eigrp dual-stack
OCANA(config-router)#address-family ipv4 unicast autonomous-system 4
OCANA(config-router-af)#topology base
OCANA(config-router-af-topology)#distribute-list 10 out
OCANA(config-router-af-topology)#$e ospfv3 1 metric 10000 100 255 1 1500
OCANA(config-router-af-topology)#exit-af-topology
OCANA(config-router-af)#address-family ipv6 unicast autonomous-system 6
OCANA(config-router-af)#topology base
OCANA(config-router-af-topology)#$e ospf 1 metric 10000 100 255 1 1500
OCANA(config-router-af-topology)#exit-af-topology
OCANA(config-router-af)#exit
```

11. En R2, de hacer publicidad de la ruta 192.168.3.0/24 a R1 mediante una lista de distribución y ACL.

Las ACL o listas de control de acceso nos permiten bloquear o permitir los paquetes de datos IP, además que proporcionan seguridad para el acceso a la red y filtran el tráfico según sean configuradas

R2 (OCAÑA):

```
OCANA(config-router)#ip access-list standard 10
```

```
OCANA(config-std-nacl)#remark acl to filter 192.168.3.0/24
```

```
OCANA(config-std-nacl)#deny 192.168.3.0 0.0.0.255
```

```
OCANA(config-std-nacl)#permit any
```

Parte 2: Verificar conectividad de red y control de la trayectoria.

- a. Registrar las tablas de enrutamiento en cada uno de los routers, acorde con los parámetros de configuración establecidos en el escenario propuesto.**

```

CALI#show 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

D EX  192.168.2.0/24 [170/50752000] via 192.168.9.2, 00:01:54, Serial3/0
      192.168.9.0/24 is variably subnetted, 3 subnets, 2 masks
C      192.168.9.0/30 is directly connected, Serial3/0
L      192.168.9.1/32 is directly connected, Serial3/0
D EX  192.168.9.4/30 [170/50752000] via 192.168.9.2, 00:01:54, Serial3/0
      192.168.110.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.110.0/24 is directly connected, GigabitEthernet0/0
L      192.168.110.1/32 is directly connected, GigabitEthernet0/0
CALI#
```

Figura 3. Tabla de enrutamiento ipv4 en R1-CALI

```
CALI#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
EX ::/0 [170/50752000]
   via FE80::C802:14FF:FEFC:6, Serial3/0
EX 2001:DB8:ACAD:C::/64 [170/50752000]
   via FE80::C802:14FF:FEFC:6, Serial3/0
C 2001:DB8:ACAD:90::/64 [0/0]
   via Serial3/0, directly connected
L 2001:DB8:ACAD:90::1/128 [0/0]
   via Serial3/0, receive
C 2001:DB8:ACAD:110::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:110::1/128 [0/0]
   via GigabitEthernet0/0, receive
L FF00::/8 [0/0]
   via Null0, receive
CALI#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 4. Tabla de enrutamiento ipv6 en R1-CALI

```

Router#show 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0
O       192.168.3.0/24 [110/782] via 192.168.9.6, 00:04:16, Serial3/1
192.168.9.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.9.0/30 is directly connected, Serial3/0
L       192.168.9.2/32 is directly connected, Serial3/0
C       192.168.9.4/30 is directly connected, Serial3/1
L       192.168.9.5/32 is directly connected, Serial3/1
D       192.168.110.0/24 [90/50245120] via 192.168.9.1, 00:04:00, Serial3/0
Router#

```

Figura 5. Tabla de enrutamiento ipv4 en R2-OCAÑA

```
Router#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
OE2 ::/0 [110/1], tag 1
   via FE80::C803:DFF:FE7C:6, Serial3/1
C 2001:DB8:ACAD:B::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:B::1/128 [0/0]
   via GigabitEthernet0/0, receive
O 2001:DB8:ACAD:C::/64 [110/782]
   via FE80::C803:DFF:FE7C:6, Serial3/1
C 2001:DB8:ACAD:90::/64 [0/0]
   via Serial3/0, directly connected
L 2001:DB8:ACAD:90::2/128 [0/0]
   via Serial3/0, receive
C 2001:DB8:ACAD:91::/64 [0/0]
   via Serial3/1, directly connected
L 2001:DB8:ACAD:91::1/128 [0/0]
   via Serial3/1, receive
D 2001:DB8:ACAD:110::/64 [90/50245120]
   via FE80::C801:13FF:FE7C:6, Serial3/0
L FF00::/8 [0/0]
   via Null0, receive
Router#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 6. Tabla de enrutamiento ipv6 en R2-OCAÑA


```
BARRANQUILLA#show 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O IA  192.168.2.0/24 [110/65] via 192.168.9.5, 00:05:19, Serial3/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.3.0/24 is directly connected, GigabitEthernet0/0
L      192.168.3.1/32 is directly connected, GigabitEthernet0/0
      192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.9.4/30 is directly connected, Serial3/1
L      192.168.9.6/32 is directly connected, Serial3/1
BARRANQUILLA#
```

Figura 7. Tabla de enrutamiento ipv4 en R3-BARRANQUILLA

```
BARRANQUILLA#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
OI 2001:DB8:ACAD:B::/64 [110/65]
   via FE80::C802:14FF:FEFC:6, Serial3/1
C  2001:DB8:ACAD:C::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:C::1/128 [0/0]
   via GigabitEthernet0/0, receive
C  2001:DB8:ACAD:91::/64 [0/0]
   via Serial3/1, directly connected
L  2001:DB8:ACAD:91::2/128 [0/0]
   via Serial3/1, receive
L  FF00::/8 [0/0]
   via Null0, receive
BARRANQUILLA#
```

solarwinds | Solar-PuTTY free tool | © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 8. Tabla de enrutamiento ipv6 en R3-BARRANQUILLA

b. Verificar comunicación entre routers mediante el comando ping y traceroute

```
● CALI x ● OCAÑA ● BARRANQUILLA | + - □ ×
CALI#tclsh
CALI(tcl)#foreach address {
+>192.168.110.1
+>192.168.9.0
+>192.168.9.2
+>192.168.2.1
+>192.168.9.5
+>192.168.9.6
+>192.168.3.1
+>} {ping $address
+>}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.0, timeout is 2 seconds:

Reply to request 0 from 192.168.9.2, 28 ms
Reply to request 1 from 192.168.9.2, 36 ms
Reply to request 2 from 192.168.9.2, 16 ms
Reply to request 3 from 192.168.9.2, 48 ms
Reply to request 4 from 192.168.9.2, 20 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/24 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/18/24 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/23/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CALI(tcl)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 9. Verificación de comunicación desde R1-CALI

```
Router#tclsh
Router(tcl)#foreach address {
+>192.168.2.1
+>192.168.9.1
+>192.168.110.1
+>192.168.9.4
+>192.168.9.6
+>192.168.3.1
+>} {ping $address
+>}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/22/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/21/36 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.4, timeout is 2 seconds:

Reply to request 0 from 192.168.9.6, 16 ms
Reply to request 1 from 192.168.9.6, 16 ms
Reply to request 2 from 192.168.9.6, 24 ms
Reply to request 3 from 192.168.9.6, 20 ms
Reply to request 4 from 192.168.9.6, 20 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/20/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/37/84 ms
Router(tcl)#
```

Figura 10. Verificación de comunicación desde R2-OCAÑA

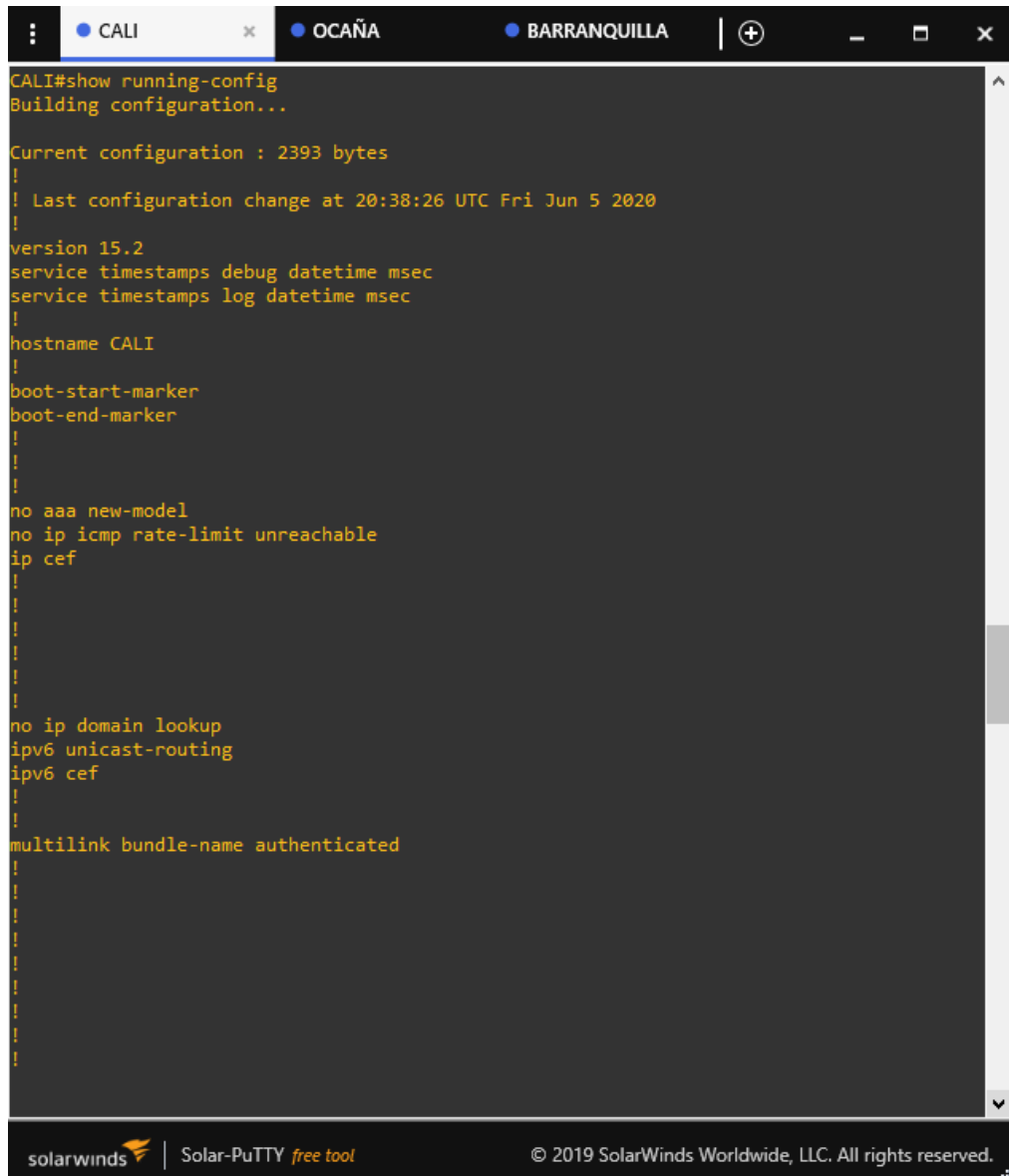
```
BARRANQUILLA#tclsh
BARRANQUILLA(tc1)#foreach address {
+>192.168.3.1
+>192.168.9.6
+>192.168.9.5
+>192.168.2.1
+>192.168.9.2
+>192.168.9.1
+>192.168.110.1
+>} {ping $address
+>}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/30/40 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/14/32 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/19/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
BARRANQUILLA(tc1)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 11. Verificación de comunicación desde R3-BARRANQUILLA.

c. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los routers correctas.

Nota: Puede ser que Una o más direcciones no serán accesibles desde todos los routers después de la configuración final debido a la utilización de listas de distribución para filtrar rutas y el uso de IPv4 e IPv6 en la misma red.



```
CALI#show running-config
Building configuration...

Current configuration : 2393 bytes
!
! Last configuration change at 20:38:26 UTC Fri Jun 5 2020
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CALI
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!
!
```

Figura 12. Verificación de rutas en R1-CALI.

```
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 192.168.2.1 255.255.255.0
media-type gbic
speed 1000
duplex full
negotiation auto
ipv6 address 2001:DB8:ACAD:B::1/64
ospfv3 1 ipv6 area 1
ospfv3 1 ipv4 area 1
!
interface GigabitEthernet1/0
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface Serial3/0
bandwidth 128
ip address 192.168.9.2 255.255.255.252
ipv6 address 2001:DB8:ACAD:90::2/64
serial restart-delay 0
!
interface Serial3/1
bandwidth 128
ip address 192.168.9.5 255.255.255.252
ipv6 address 2001:DB8:ACAD:91::1/64
ospfv3 1 ipv6 area 0
ospfv3 1 ipv4 area 0
serial restart-delay 0
clock rate 128000
!
interface Serial3/2
--More--
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 13. Verificación de rutas en R2-OCAÑA.

```
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
ip address 192.168.3.1 255.255.255.0
media-type gbic
speed 1000
duplex full
negotiation auto
ipv6 address 2001:DB8:ACAD:C::1/64
ospfv3 1 ipv6 area 0
ospfv3 1 ipv4 area 0
!
interface GigabitEthernet1/0
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface Serial3/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/1
ip address 192.168.9.6 255.255.255.252
ipv6 address 2001:DB8:ACAD:91::2/64
ospfv3 1 ipv6 area 0
ospfv3 1 ipv4 area 0
serial restart-delay 0
!
interface Serial3/2
no ip address
shutdown
--More-- █
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

Figura 14. Verificación de rutas en R3-BARRANQUILLA

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.

Topología de Red - Escenario 2.

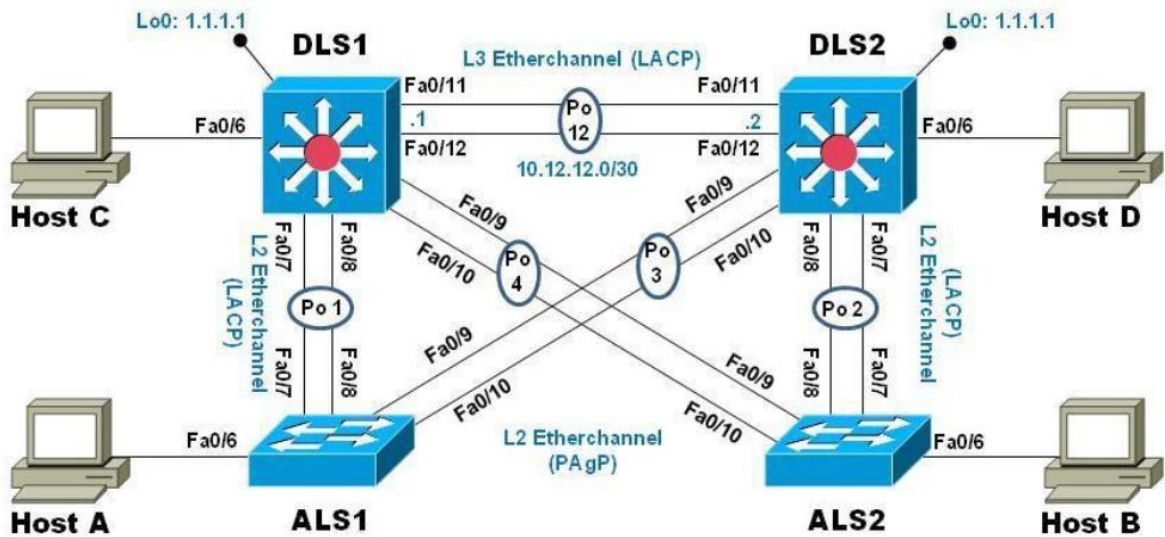


Figura 15. Topología de Red propuesta – escenario 2.

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

Para la realización de este segundo escenario, se decide utilizar el simulador de Cisco Packet Tracer en su última versión. Versión 7.3.0.0837.

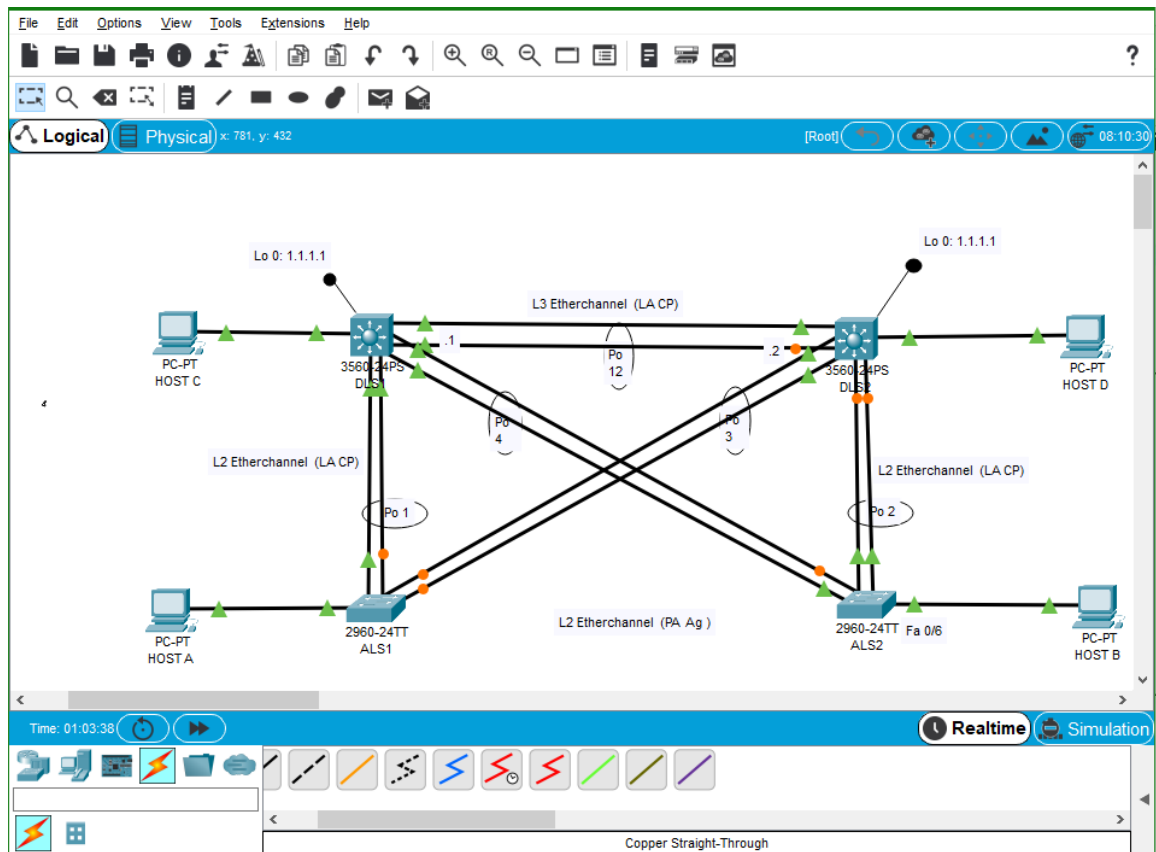


Figura 16. Simulación de la topología de Red especificada en Cisco Packet Tracer v.7.3.0.0837

- Apagar todas las interfaces en cada switch.**
- Asignar un nombre a cada switch acorde al escenario establecido.**

En esta primera parte utilizaremos en comando **interface range**, el cual nos ayudara a seleccionar varias interfaces al mismo tiempo que se aplica el mismo comando para cada una de ellas, así mismo, asignamos el nombre a cada switch utilizando desde la configuración global la sintaxis **hostname**.

DLS1:

```
Switch>enable
```

```
Switch#conf t
```

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

```
Switch(config)#interface range fastEthernet 0/1-24, gigabitEthernet 0/1-2
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#hostname DLS1
DLS1(config)#
```

DLS2:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-24, gigabitEthernet 0/1-2
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#hostname DLS2
DLS2(config)#
```

ALS1:

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-24, gigabitEthernet 0/1-2
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#hostname DLS2
DLS2(config)#
```

ALS2

```
Switch>enable
Switch#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface range fastEthernet 0/1-24, gigabitEthernet 0/1-2  
Switch(config-if-range)#shutdown  
Switch(config-if-range)#exit  
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.**

Cisco ofrece su tecnología de Etherchannel de acuerdo a los estándares 802.3, la cual, permite que los links Ethernet combinen en solo un canal lógico.

Crear un Port-channel significa aumentar el ancho de banda, ayudando así a la capacidad de comunicación entre los switch.

A continuación, aplicamos los comandos requeridos que nos permiten configurar los puertos troncales y port-channel para el canal Etherchannel (LACP), identificado en la topología de red.

DLS1:

```
DLS1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
DLS1(config)#interface port-channel 12  
DLS1(config-if)#no switchport  
DLS1(config-if)#ip address 10.12.12.1 255.255.255.252  
DLS1(config-if)#exit  
DLS1(config)#int range fa0/11-12  
DLS1(config-if-range)#no switchport  
DLS1(config-if-range)#channel-group 12 mode active  
DLS1(config-if-range)#exit  
DLS1(config)#
```

DLS2:

```
DLS2(config)#  
DLS2(config)#interface port-channel 12  
DLS2(config-if)#no switchport  
DLS2(config-if)#ip address 10.12.12.2 255.255.255.252  
DLS2(config-if)#exit  
DLS2(config)#interface range fa0/11-12  
DLS2(config-if-range)#no switchport  
DLS2(config-if-range)#channel-group 12 mode active  
DLS2(config-if-range)#exit  
DLS2(config)#
```

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

Para la configuración troncales y EtherChannel, utilizaremos el comando **switchport trunk encapsulation {isl | dot1q}**, sin embargo, es importante mencionar que Packet Tracer no soportara todos los comandos en sus dispositivos.

DLS1:

```
DLS1(config)#  
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)#exit  
Creating a port-channel interface Port-channel 1  
DLS1(config)#
```

DLS2:

```
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)#channel-group 2 mode active
DLS2(config-if-range)#no shutdown
```

ALS1:

```
ALS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#int range fa0/7-8
ALS1(config-if-range)#switchport trunk encapsulation dot1q
^
% Invalid input detected at '^' marker.
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 1 mode active
ALS1(config-if-range)#no shutdown
```

ALS2

```
ALS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#int range fa0/7-8
ALS2(config-if-range)#switchport trunk encapsulation dot1q
^
% Invalid input detected at '^' marker.
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#no shutdown
ALS2(config-if-range)#exit
```

En esta práctica de laboratorio, hemos utilizado switches Cisco Catalyst 3560 y 2960 que ejecutan servicios IP Cisco y versiones 12.2 y versión 15.2 respectivamente, sin embargo, luego de realizar la configuración, observamos que Packet Tracer en su actual versión, el conmutador 2960 (v.15.2) no soporta el comando switchport trunk encapsulation dot1q.

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

Igualmente, se realizan las configuraciones necesarias.

DLS1:

```
DLS1(config)#
```

```
DLS1(config)#int range fa0/9-10
```

```
DLS1(config-if-range)#switchport trunk encapsulation dot1q
```

```
DLS1(config-if-range)#switchport mode trunk
```

```
DLS1(config-if-range)#channel-group 4 mode desirable
```

```
DLS1(config-if-range)#
```

```
Creating a port-channel interface Port-channel 4
```

```
DLS1(config-if-range)#exit
```

```
DLS1(config)#
```

ALS2

```
ALS2(config)#int range fa0/9-10
```

```
ALS2(config-if-range)#switchport trunk encapsulation dot1q
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
ALS2(config-if-range)#switchport mode trunk
```

```
ALS2(config-if-range)#channel-group 4 mode desirable
```

```
ALS2(config-if-range)#
```

```
Creating a port-channel interface Port-channel 4
```

```
ALS2(config-if-range)#exit
```

```
ALS2(config)#
```

DLS2:

DLS2#conf t

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

DLS2(config)#int range fa0/9-10

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

%EC-5-CANNOT_BUNDLE2: Fa0/9 is not compatible with Fa0/10 and will be suspended (dtp mode of Fa0/9 is on, Fa0/10 is off)

DLS2(config-if-range)#exit

DLS2(config)#

ALS1:

ALS1#conf t

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

ALS1(config)#int range fa0/9-10

ALS1(config-if-range)#switchport trunk encapsulation dot1q

^

% Invalid input detected at '^' marker.

ALS1(config-if-range)#switchport mode trunk

ALS1(config-if-range)#channel-group 3 mode desirable

ALS1(config-if-range)#no shutdown

Creating a port-channel interface Port-channel 3

ALS1(config-if-range)#exit

ALS1(config)#

4) Todos los puertos troncales serán asignados a la VLAN 800 como la VLAN nativa.

DLS1:

DLS1#conf t

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

DLS1(config)#interface Po1

DLS1(config-if)#switchport trunk native vlan 800

DLS1(config-if)#exit

DLS1(config)#int Po4

DLS1(config-if)#switchport trunk native vlan 800

DLS1(config-if)#exit

DLS1(config)#

DLS2:

DLS2(config)#

DLS2(config)#int Po2

DLS2(config-if)#switchport trunk native vlan 800

DLS2(config-if)#exit

DLS2(config)#int Po3

DLS2(config-if)#switchport trunk native vlan 800

DLS2(config-if)#exit

DLS2(config)#

ALS1:

ALS1(config)#

ALS1(config)#int Po1

ALS1(config-if)#switchport trunk native vlan 800

ALS1(config-if)#exit

ALS1(config)#int Po3

ALS1(config-if)#switchport trunk native vlan 800

ALS2

```
ALS2(config)#  
ALS2(config)#interface Po2  
ALS2(config-if)#switchport trunk native vlan 800  
ALS2(config-if)#exit  
ALS2(config)#interface Po4  
ALS2(config-if)#switchport trunk native vlan 800  
ALS2(config-if)#exit  
ALS2(config)#
```

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

- 1) Utilizar el nombre de dominio UNAD con la contraseña cisco123***
- 2) Configurar DLS1 como servidor principal para las VLAN.***
- 3) Configurar ALS1 y ALS2 como clientes VTP***

El Vlan Trunk Protocol permite configurar y administrar las vlans, la contraseña debe estar presente en todos los switches en el dominio VTP.

Para la realización de estos tres pasos, hemos usado los comandos ***vtp domain, vtp version 2, vtp mode server*** y ***vtp mode client***. A continuación, se muestra la configuración realizada.

DLS1:

```
DLS1(config)#  
DLS1(config)#vtp domain UNAD  
Domain name already set to UNAD.  
DLS1(config)#vtp password cisco123  
Password already set to cisco123  
DLS1(config)#vtp version 2  
VTP mode already in V2.  
DLS1(config)#vtp mode server  
Device mode already VTP SERVER.  
DLS1(config)#
```

ALS1:

ALS1(config)#

ALS1(config)#vtp domain UNAD

Changing VTP domain name from NULL to UNAD

ALS1(config)#vtp pass cisco123

Setting device VLAN database password to cisco123

ALS1(config)#vtp version 2

ALS1(config)#vtp mode client

Setting device to VTP CLIENT mode.

ALS1(config)#

ALS2

ALS2#conf t

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

ALS2(config)#vtp domain UNAD

Domain name already set to UNAD.

ALS2(config)#vtp pass cisco123

Setting device VLAN database password to cisco123

ALS2(config)#vtp version 2

ALS2(config)#vtp mode client

Setting device to VTP CLIENT mode.

ALS2(config)#

e. Configurar en el servidor principal las siguientes VLAN:

Tabla 2. Configuración de VLAN en el servidor principal.

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
800	NATIVA	434	ESTACIONAMIENTO
12	EJECUTIVOS	123	MANTENIMIENTO
234	HUESPEDES	1010	VOZ
1111	VIDEONET	3456	ADMINISTRACION

Es importante recordar que el hemos utilizado los switches Cisco Catalyst 3560 en su versión 12.2 como servidor principal, pero este switch no soporta un rango mayor a 1005 VLANS, en su defecto no soporta VLANS extendidas. Para fines prácticos, se anula el ultimo digito de las VLANS para continuar con la realización de este escenario de laboratorio.

Para la confirmación de la anterior anotación, se agrega la siguiente figura que argumenta el punto mencionado.

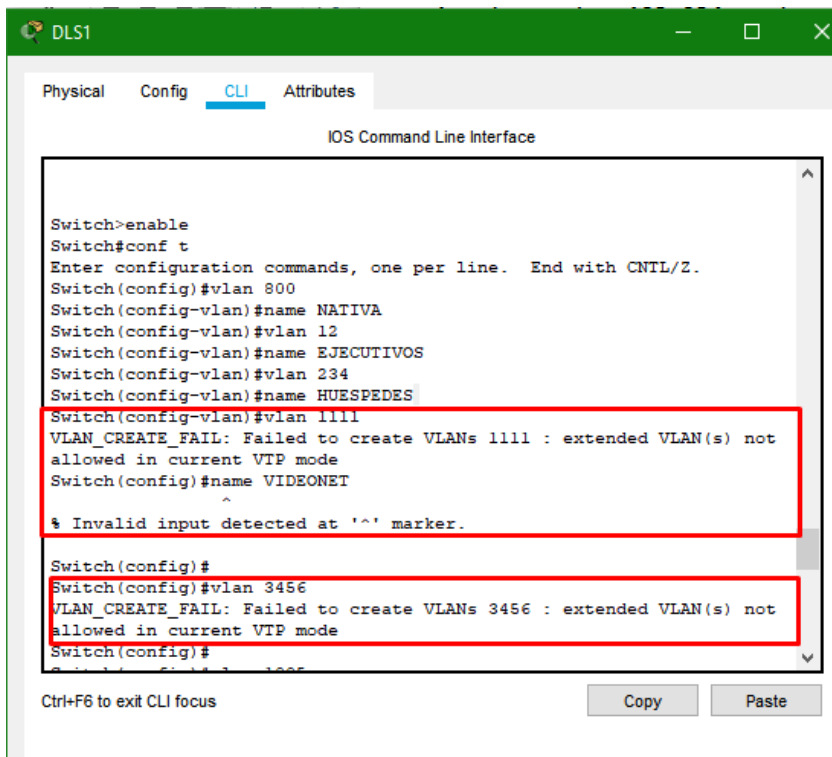


Figura 17. Packet Tracer - Switch no soporta vlans extendidas.

DLS1:

DLS1#conf t

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

DLS1(config)#vlan 800

DLS1(config-vlan)#name NATIVA

DLS1(config-vlan)#vlan 12

DLS1(config-vlan)#name EJECUTIVOS

DLS1(config-vlan)#vlan 234

DLS1(config-vlan)#name HUESPEDES

DLS1(config-vlan)#vlan 111

DLS1(config-vlan)#name VIDEONET

DLS1(config)#vlan 434

DLS1(config-vlan)#name ESTACIONAMIENTO

DLS1(config-vlan)#vlan 123

```
DLS1(config-vlan)#name MANTENIMIENTO
DLS1(config-vlan)#vlan 101
DLS1(config-vlan)#name VOZ
DLS1(config)#vlan 346
DLS1(config-vlan)#name ADMINISTRACION
DLS1(config)#
```

f. En DLS1, suspender la VLAN 434.

El comando requerido para suspender una vlan es **state suspend**, pero tampoco es soportado por Packet Tracer.

DLS1:

```
DLS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#vlan 434
DLS1(config-vlan)#state suspend
^
% Invalid input detected at '^' marker.
DLS1(config-vlan)#exit
DLS1(config)#
```

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

Sabemos que los conmutadores transparentes VTP no participan en VTP, no anuncia su base de datos VLAN ni sincroniza su base de datos VLAN. Para configurar un conmutador en modo VTP transparente solo debemos aplicar el comando **vtp mode transparent** en el modo de configuración general.

h. Suspender VLAN 434 en DLS2.

DLS2:

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

```
^
% Invalid input detected at '^' marker.
DLS2(config-vlan)#exit
DLS2(config)#
DLS2(config)#vlan 800
DLS2(config-vlan)#name NATIVA
DLS2(config-vlan)#vlan 12
DLS2(config-vlan)#name EJECUTIVOS
DLS2(config-vlan)#vlan 234
DLS2(config-vlan)#name HUESPEDES
DLS2(config-vlan)#vlan 111
DLS2(config-vlan)#name VIDEONET
DLS2(config-vlan)#vlan 434
DLS2(config-vlan)#name ESTACIONAMIENTO
DLS2(config-vlan)#vlan 123
DLS2(config-vlan)#name MANTENIMIENTO
DLS2(config-vlan)#vlan 101
DLS2(config-vlan)#name VOZ
DLS2(config-vlan)#vlan 345
DLS2(config-vlan)#name ADMINISTRACION
DLS2(config-vlan)#exit
DLS2(config)#
```

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

En este punto se requiere que la nueva VLAN sea restringida, por lo que usaremos en comando ***switchport allowed vlan except***

DLS2:

```
DLS2(config)#  
DLS2(config)#vlan 567  
DLS2(config-vlan)#name CONTABILIDAD  
DLS2(config-vlan)#exit  
DLS2(config)#int port-channel 2  
DLS2(config-if)#switchport trunk allowed vlan except 567  
DLS2(config-if)#int port-channel 3  
DLS2(config-if)#switchport trunk allowed vlan except 567  
DLS2(config-if)#exit  
DLS2(config)#
```

j. Configurar DLS1 como Spanning tree root para las VLAN 1, 12, 434, 800, 1010, 1111 y 3456 y como raíz secundaria para las VLAN 123 y 234.

El comando de Spanning *tree* debe ser utilizado solo en los conmutadores de red troncal. Para su habilitación se debe ingresar a la configuración general. El ***spanning-tree vlan vlan-id root { primary | secondary }*** se puede usar para establecer automáticamente un valor de prioridad como lo realizamos a continuación.

DLS1:

```
DLS1#conf t  
  
Enter configuration commands, one per line. End with CNTL/Z.  
DLS1(config)#spanning-tree vlan 1,12,434,800,101,111,345 root primary  
DLS1(config)#spanning-tree vlan 123,234 root secondary  
DLS1(config)#
```

k. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 800, 1010, 1111 y 3456.

DLS1:

```
DLS2#conf t  
  
Enter configuration commands, one per line. End with CNTL/Z.  
DLS2(config)#spanning-tree vlan 123,234 root primary  
DLS2(config)#spanning-tree vlan 12,434,800,101,111,345 root secondary
```


- I. **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:

```
DLS1(config)#int port-channel1
DLS1(config-if)#switchport trunk native vlan 800
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS1(config-if)#exit
DLS1(config)#int port-channel4
DLS1(config-if)#switchport trunk native vlan 800
DLS1(config-if)#switchport trunk encapsulation dot1q
DLS1(config-if)#switchport mode trunk
DLS1(config-if)#exit
DLS1(config)#int port-channel2
DLS1(config-if)#no switchport
DLS1(config-if)#ip address 10.12.12.1 255.255.255.252
% 10.12.12.0 overlaps with Port-channel12
DLS1(config-if)#exit
DLS1(config)#int range fa0/7-10
DLS1(config-if-range)#switchport trunk native vlan 800
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)#exit
DLS1(config)#
```

DLS2

```
DLS2(config)#int range fa0/7-12
DLS2(config-if-range)#switchport trunk native vlan 800
```

```
DLS2(config-if-range)#switchport trunk allowed vlan 1-566-1005
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)#exit
```

ALS1:

```
ALS1(config)#int range fa0/7-10
ALS1(config-if-range)#switchport trunk native vlan 800
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#exit
```

ALS2:

```
ALS2(config)#int port-channel2
ALS2(config-if)#switchport trunk native vlan 800
ALS2(config-if)#switchport mode trunk
ALS2(config-if)#exit
ALS2(config)#int port-channel4
ALS2(config-if)#switchport trunk native vlan 800
ALS2(config-if)#switchport mode trunk
ALS2(config-if)#exit
ALS2(config)#int range fa0/7
ALS2(config-if-range)#switchport trunk native vlan 800
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#exit
ALS2(config)#int range fa0/8
ALS2(config-if-range)#switchport trunk native vlan 800
ALS2(config-if-range)#switchport mode trunk
```

```

ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#exit
ALS2(config)#int range fa0/9
ALS2(config-if-range)#switchport trunk native vlan 800
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#exit
ALS2(config)#int range fa0/10
ALS2(config-if-range)#switchport trunk native vlan 800
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#exit

```

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

Tabla 3. Configuración de las interfaces como puertos de acceso, asignados a las VLAN

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

Según la tabla anterior se procede con la configuración de las interfaces como puertos de acceso, para esto utilizamos en comando **switchport access vlan** y encendemos la interfaz. Es importante recordar que la VLAN 1111 fue cambiada por la 111 y la VLAN 3456 fue cambiada por 345.

DLS1:

```
DLS1(config)#int fa0/6
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 345
DLS1(config-if)#spanning-tree portfast
DLS1(config-if)#exit
DLS1(config)#int fa0/15
DLS1(config-if)#switchport mode access
DLS1(config-if)#switchport access vlan 111
DLS1(config-if)#spanning-tree portfast
DLS1(config-if)#exit
```

DLS2:

```
DLS2(config)#int fa0/6
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 12
DLS2(config-if)#switchport access vlan 101
DLS2(config-if)#spanning-tree portfast
DLS2(config-if)#exit
DLS2(config)#int fa0/15
DLS2(config-if)#switchport mode access
DLS2(config-if)#switchport access vlan 111
DLS2(config-if)#spanning-tree portfast
DLS2(config-if)#exit
DLS2(config)#int range fa0/16-18
DLS2(config-if-range)#switchport mode access
DLS2(config-if-range)#switchport access vlan 567
DLS2(config-if-range)#spanning-tree portfast
DLS2(config-if-range)#exit
```

ALS1:

```
ALS1(config)#int fa0/6
ALS1(config-if)#switchport mode access
ALS1(config-if)#switchport access vlan 123
ALS1(config-if)#switchport access vlan 101
ALS1(config-if)#spanning-tree portfast
ALS1(config-if)#exit
ALS1(config)#int fa0/15
ALS1(config-if)#switchport mode access
ALS1(config-if)#switchport access vlan 111
ALS1(config-if)#spanning-tree portfast
ALS1(config-if)#exit
ALS1(config)#
```

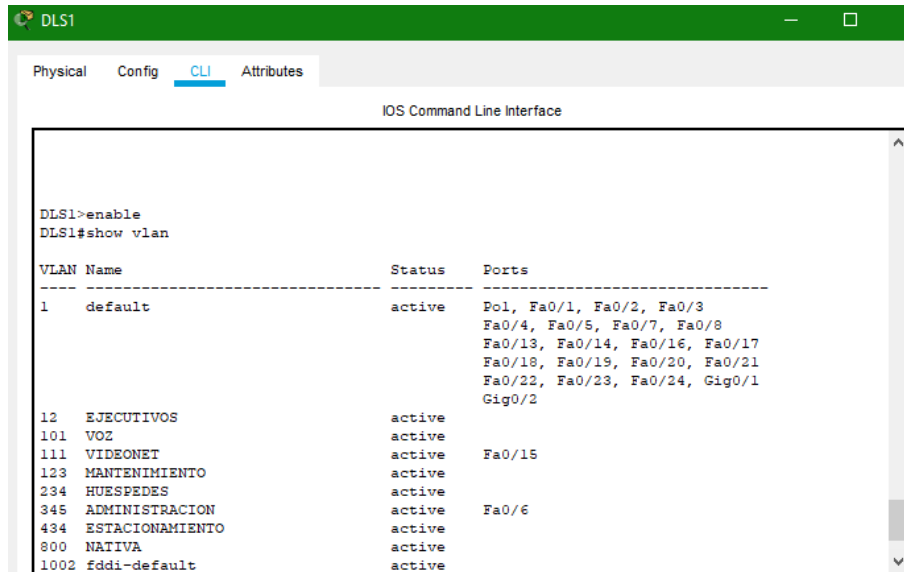
ALS2:

```
ALS2(config)#int fa0/6
ALS2(config-if)#switchport mode access
ALS2(config-if)#switchport access vlan 234
ALS2(config-if)#spanning-tree portfast
ALS2(config-if)#exit
ALS2(config)#int fa0/15
ALS2(config-if)#switchport mode access
ALS2(config-if)#switchport access vlan 111
ALS2(config-if)#spanning-tree portfast
ALS2(config-if)#exit
ALS2(config)#
```

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

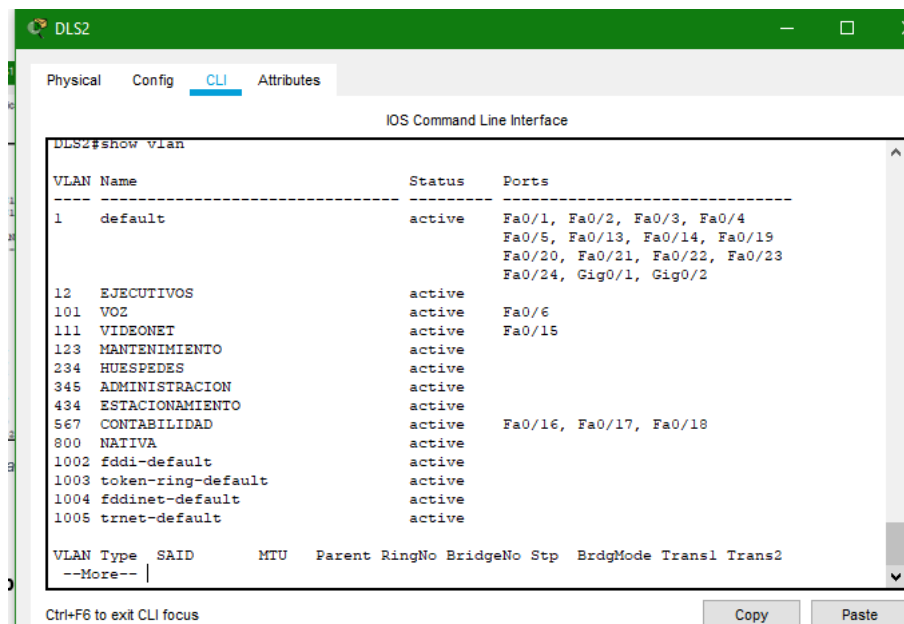
Para realizar la verificación de la existencia de las VLANs en todos los switches, utilizamos en comando **show vlan**, este comando permitirá ver la información de las VLANs incluidas las VLANs privadas.



```
DLS1>enable
DLS1#show vlan

VLAN Name                Status    Ports
-----
1    default                 active    Po1, Fa0/1, Fa0/2, Fa0/3
                    Fa0/4, Fa0/5, Fa0/7, Fa0/8
                    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   EJECUTIVOS              active
101  VOZ                     active
111  VIDEONET                 active    Fa0/15
123  MANTENIMIENTO            active
234  HUESPEDES                active
345  ADMINISTRACION            active    Fa0/6
434  ESTACIONAMIENTO          active
800  NATIVA                   active
1002 fddi-default             active
```

Figura 18. Verificación de Vlan en Switch DLS1



```
DLS2#show vlan

VLAN Name                Status    Ports
-----
1    default                 active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                    Fa0/5, Fa0/13, Fa0/14, Fa0/19
                    Fa0/20, Fa0/21, Fa0/22, Fa0/23
                    Fa0/24, Gig0/1, Gig0/2
12   EJECUTIVOS              active
101  VOZ                     active    Fa0/6
111  VIDEONET                 active    Fa0/15
123  MANTENIMIENTO            active
234  HUESPEDES                active
345  ADMINISTRACION            active
434  ESTACIONAMIENTO          active
567  CONTABILIDAD              active    Fa0/16, Fa0/17, Fa0/18
800  NATIVA                   active
1002 fddi-default             active
1003 token-ring-default      active
1004 fddinet-default          active
1005 trnet-default           active

VLAN Type SAID          MTU   Parent RingNo BridgeNo Stp   BrdgMode Transl Trans2
--More-- |
```

Figura 19. Verificación de Vlan en Switch DLS2

```

ALS1#show vlan
VLAN Name                Status    Ports
-----
1    default                 active    Po1, Fa0/1, Fa0/2, Fa0/3
                                   Fa0/4, Fa0/5, Fa0/7, Fa0/8
                                   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   EJECUTIVOS              active
101  VOZ                     active    Fa0/6
111  VIDEONET                active    Fa0/15
123  MANTENIMIENTO           active
234  HUESPEDES               active
345  ADMINISTRACION           active
434  ESTACIONAMIENTO         active
800  NATIVA                  active
1002 fddi-default             active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default         active

--More-- |

```

Figura 20. Verificación de Vlan en Switch ALS1

```

ALS2#show vlan
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   EJECUTIVOS              active
101  VOZ                     active
111  VIDEONET                active    Fa0/15
123  MANTENIMIENTO           active
234  HUESPEDES               active    Fa0/6
345  ADMINISTRACION           active
434  ESTACIONAMIENTO         active
800  NATIVA                  active
1002 fddi-default             active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default         active

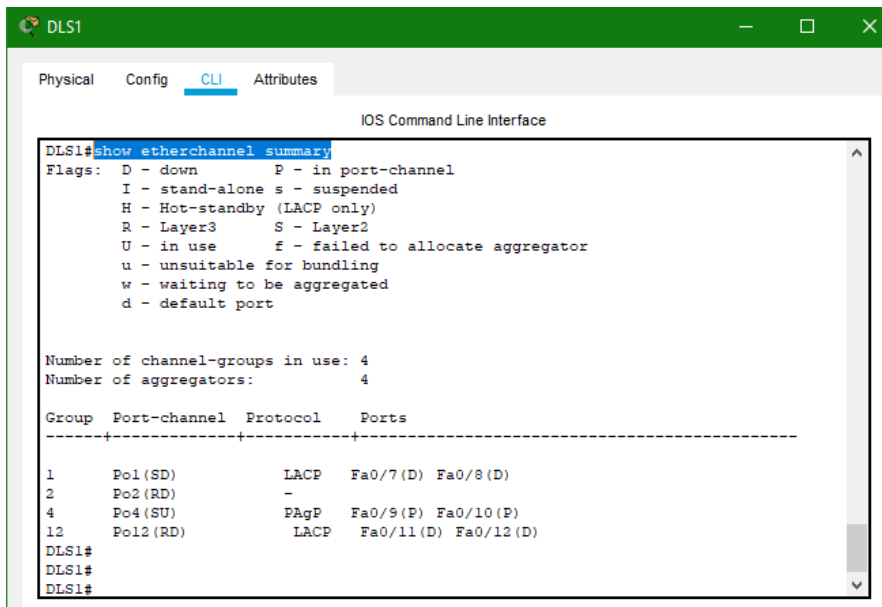
VLAN Type  SAID          MTU   Parent RingNo BridgeNo Stp  BrdgMode Transl Trans2
--More-- |

```

Figura 21. Verificación de Vlan en Switch ALS2.

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

Para verificar que el etherchannel está configurado correctamente, utilizamos en comando show *etherchannel summary*.



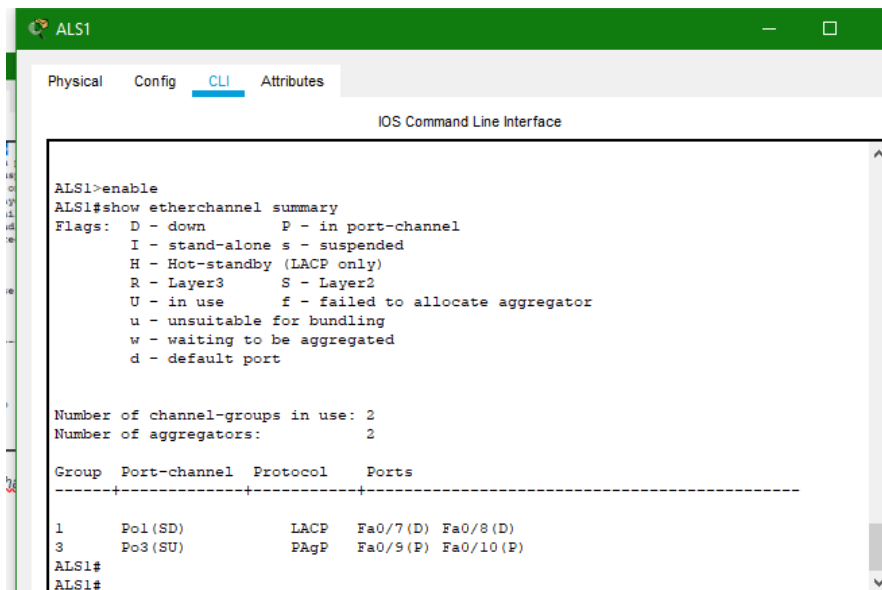
The screenshot shows the CLI of a switch named DLS1. The user has entered the command 'show etherchannel summary'. The output displays the status of four etherchannel groups. Group 1 is a LACP port-channel using ports Fa0/7 and Fa0/8. Group 2 is a stand-alone port-channel using port Po2. Group 4 is a PAgP port-channel using ports Fa0/9 and Fa0/10. Group 12 is a LACP port-channel using ports Fa0/11 and Fa0/12. The output also includes a legend for flags and summary statistics.

```
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: 4
Number of aggregators:          4

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SD)           LACP       Fa0/7(D) Fa0/8(D)
2      Po2(RD)           -          -
4      Po4(SU)           PAgP       Fa0/9(P) Fa0/10(P)
12     Po12(RD)          LACP       Fa0/11(D) Fa0/12(D)
DLS1#
DLS1#
DLS1#
```

Figura 22. Verificación de EtherChannel en DLS1.



The screenshot shows the CLI of a switch named ALS1. The user has entered the command 'show etherchannel summary'. The output displays the status of two etherchannel groups. Group 1 is a LACP port-channel using ports Fa0/7 and Fa0/8. Group 3 is a PAgP port-channel using ports Fa0/9 and Fa0/10. The output also includes a legend for flags and summary statistics.

```
ALS1>enable
ALS1#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

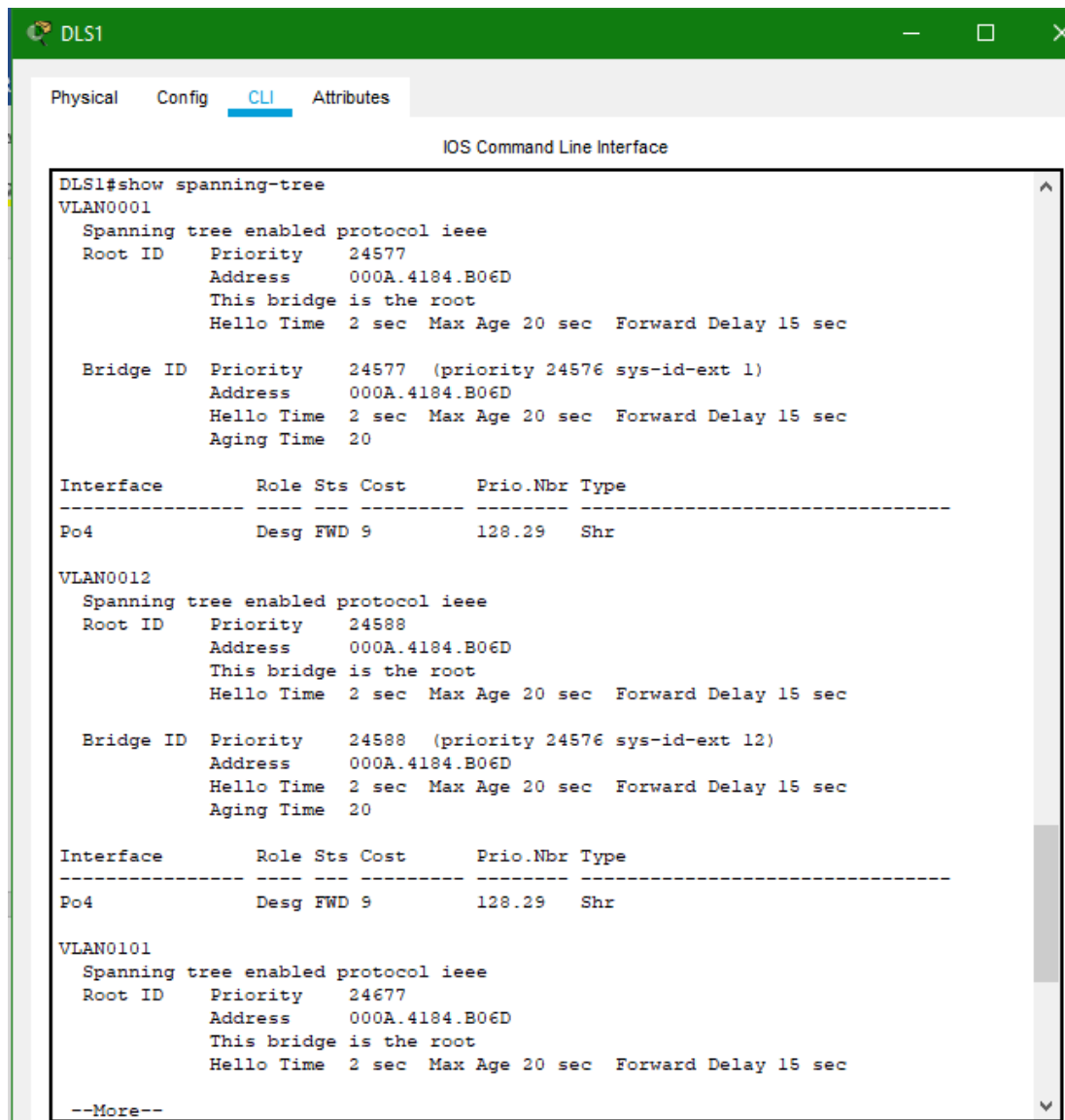
Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SD)           LACP       Fa0/7(D) Fa0/8(D)
3      Po3(SU)           PAgP       Fa0/9(P) Fa0/10(P)
ALS1#
ALS1#
```

Figura 23. Verificación de EtherChannel en ALS1.

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

Para verificar la configuración de Spanning tree utilizaremos en comando **show spanning-tree**, este comando, además, nos permitirá obtener toda la configuración de STP del switch e incluso la prioridad de puerto y costo del puerto.



```
DLS1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
            Address    000A.4184.B06D
            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    000A.4184.B06D
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Po4                Desg FWD 9        128.29  Shr

VLAN0012
  Spanning tree enabled protocol ieee
  Root ID    Priority    24588
            Address    000A.4184.B06D
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24588 (priority 24576 sys-id-ext 12)
            Address    000A.4184.B06D
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Po4                Desg FWD 9        128.29  Shr

VLAN0101
  Spanning tree enabled protocol ieee
  Root ID    Priority    24677
            Address    000A.4184.B06D
            This bridge is the root
            Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

--More--
```

Figura 24. Verificación de configuración de Spanning tree en DLS1

```

DLS2
Physical Config CLI Attributes
IOS Command Line Interface
DLS2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
            Address    000A.4184.B06D
            Cost      18
            Port      28 (Port-channel2)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
            Address    0030.A30E.0B47
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po2             Root FWD 9         128.28  Shr
Po3             Desg FWD 9         128.29  Shr

VLAN0012
  Spanning tree enabled protocol ieee
  Root ID    Priority    24588
            Address    000A.4184.B06D
            Cost      18
            Port      28 (Port-channel2)
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    28684 (priority 28672 sys-id-ext 12)
            Address    0030.A30E.0B47
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Po2             Root FWD 9         128.28  Shr
Po3             Desg FWD 9         128.29  Shr

VLAN0101
--More--

```

Figura 25. Verificación de configuración de Spanning tree en DLS2

Conclusión

- Dentro de los mejores protocolos de enrutamiento de propiedad de CISCO encontramos el EIGRP, este protocolo permite una rápida convergencia, permite su configuración en los diferentes dispositivos de manera sencilla utilizando un bajo ancho de banda.
- Otro importante protocolo de CISCO es el VTP (VLAN Trunking Protocol), su aporte significativo radica en su contribución con la administración de la red permitiendo la distribución de una VLAN en toda la red sin necesidad de la configuración en los diferentes conmutadores.
- OSPF en su última versión, OSPFv3 brinda excelentes características como el acoplamiento en direccionamientos IPv4 e IPv6, es una excelente herramienta para la actualización automática de las tablas de enrutamiento. Su desventaja radica en que solo es compatible en IOS v15.2.
- El uso de las VLAN dentro de una red es fundamental para la creación de redes no físicas independientes permitiendo la disposición de varias VLANS dentro de un mismo conmutador. Estas pueden ser estáticas con puerto asociado o dinámicas con configuración particular.
- Si bien es cierto que las herramientas virtuales como los simuladores constituyen un gran aporte para fines prácticos de academia, durante la realización de este laboratorio se evidenciaron algunas falencias en Packet Tracer como en GNS3 en cuanto al uso de comandos no soportados más exactamente en protocolos de VTP y OSPF en su versión 3.

Bibliografía

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

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

Anexos

Simulación de Escenario 1

<https://drive.google.com/drive/folders/1xVOmPJNy4zmAIR0yRkkMq9BOwtrhbqht?usp=sharing>

Simulación de Escenario 2

<https://drive.google.com/drive/folders/1PseR0myd77Fmnoj4nVz4SNaGReSk1YWXw?usp=sharing>