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

JANETH VIVIANA GIRALDO GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
DOSQUEBRADAS
2020

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

JANETH VIVIANA GIRALDO GARCIA

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO ELECTRÓNICO

PAULITA FLOR SALAZAR
DIRECTORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
DOSQUEBRADAS
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Dosquebradas, Julio 27 de 2020

TABLA DE CONTENIDO

LISTA DE FIGURAS

GLOSARIO

ADSL: Es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa. [1]

DTP: Dynamic Trunking Protocol es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE. [2]

EIGRP: Es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. [3]

ETHERNET: Es un estándar de redes de área local para computadores, por sus siglas en español Acceso Múltiple con Escucha de Portadora y Detección de Colisiones. [4]

LAN: Es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio. La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. [5]

OSPF: Open Shortest Path First (OSPF), es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol para calcular la ruta más corta entre dos nodos. Su medida de métrica se denomina cost,

y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF mantiene actualizada la capacidad de encaminamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. [6]

PROTOCOLOS DE RED: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. [7]

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red. es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática. [8]

SERVIDOR: Es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. [9]

SWITCH: "Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas. [10]

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local. [11]

VTP: 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. [12]

WLAN: "Una red de área local inalámbrica, también conocida como WLAN (del inglés wireless local area network), es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas. [13]

RESUMEN

La implementación de las comunicaciones y redes son importantes debido al intercambio constante de datos en las organizaciones, haciendo indispensable garantizar la integridad, velocidad de transmisión y disponibilidad de la información a través de la creación de redes robustas y seguras por medio de los dispositivos, módulos y protocolos de redes.

El desarrollo del trabajo se centró en dos escenarios LAN/WAN, que son habituales en las empresas y que permiten realizar un análisis sobre el procedimiento de múltiples protocolos y valorar el desempeño de los router, mediante el uso de comandos de administración avanzados.

La configuración e interconexión entre sí de cada uno de los dispositivos que forman parte del escenario, se realiza acorde con los lineamientos establecidos para el direccionamiento IP, IPv4 e IPv6, protocolos de enrutamiento como: OSPFv3, EIGRP, BGP y demás aspectos que forman parte de la topología de red con el fin de aprender a construir e implementar redes LAN/WAN.

Palabras Claves: Comunicaciones, Redes, LAN, WAN, Protocolos, Router, Direccionamiento.

ABSTRACT

The implementation of communications and networks are important due to the constant exchange of data in organizations, making it essential to ensure the integrity, transmission speed and availability of information through the creation of robust and secure networks by means of devices, modules and network protocols.

The development of the work was focused on two LAN/WAN scenarios, which are common in companies and that allow an analysis on the procedure of multiple protocols, assess the performance of the routers, through the use of advanced management commands.

The configuration and interconnection between each of the devices that are part of the scenario, is done according to the guidelines established for IP addressing, IPv4 and IPv6, routing protocols such as: OSPFv3, EIGRP, BGP and other aspects that are part of the network topology in order to learn how to build and implement LAN/WAN networks.

Keywords: Communications, Networks, LAN, WAN, Protocols, Router, Addressing.

INTRODUCCIÓN

Este trabajo tendrá como objetivo la realización de la prueba de habilidades prácticas profundizando en CCNP por medio del programa de Cisco Packet Tracer, inicialmente se realizará el desarrollo del primer escenario donde se configurará e interconectará entre sí cada uno de los dispositivos. Se realizarán las configuraciones básicas de los Router y se configurarán las interfaces con las direcciones IPv4 e IPv6, se aplicará el protocolo de enrutamiento EIGRP y el protocolo de direccionamiento OSPF. Posteriormente se desarrollará el segundo escenario en el cual, se configurará e interconectará entre sí cada uno de los dispositivos, acorde con los lineamientos establecidos para el direccionamiento IP, etherchannels y VLANs,

Para esto se registrará el proceso de configuración y verificación punto por punto, buscando poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking actuales.

1. PRIMER ESCENARIO

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.

1.1 TOPOLOGÍA DE RED

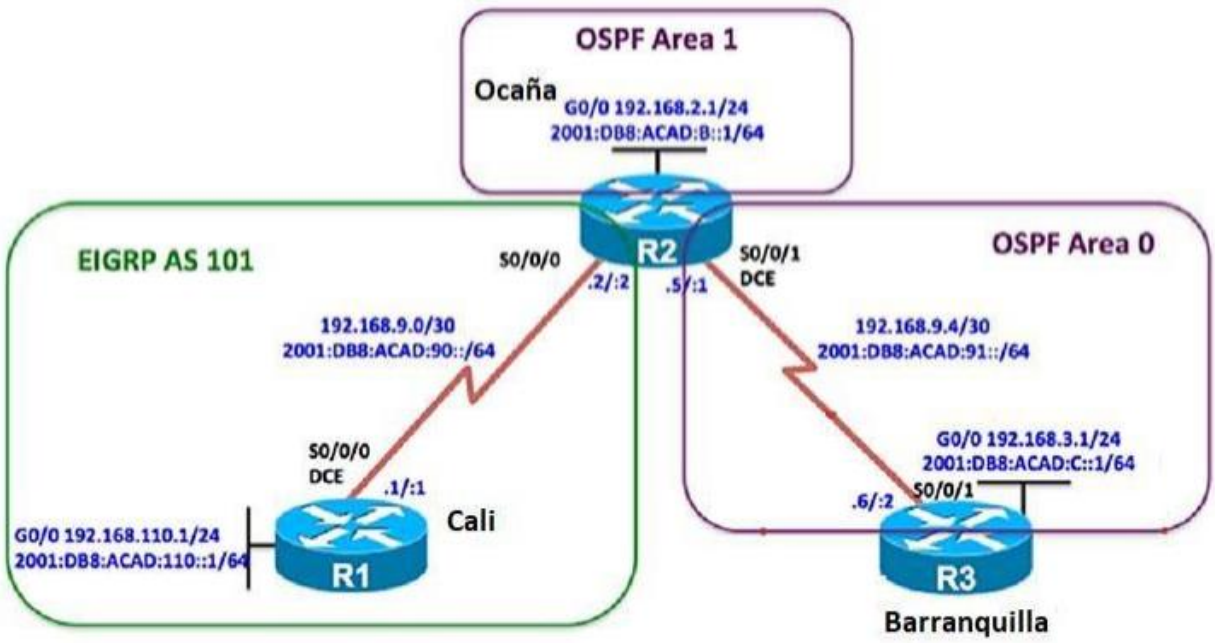

Figura 1 Topología del primer escenario

1.2 PROCEDIMIENTO DEL DESARROLLO

Para realizar la solución de este escenario seguiremos el siguiente procedimiento.

1. Agregar a la pantalla principal del programa Packet Tracer los router, teniendo en cuenta la topología de la red y según sea el caso borrar cualquier configuración del router, si es necesario.

2. Para realizar la topología de la red, tal como se muestra en la figura 1, inicialmente agregamos a la pantalla principal del programa Packet Tracer el router 2901 y un PC, luego agregamos los módulos HWIC-2T y HWIC-4ESW al router. Para ello primero debemos apagar el Router, luego agregar los módulos y volver a encender el router, además los dispositivos se encuentran unidos por cable ethernet por el puerto serial, como podemos observar en la topología de la red.

   Hay que asegurarnos que el switch no tenga configuraciones, por medio del comando **erase startup-config** eliminamos los archivos y con el comando **reload** se volverán a cargar los dispositivos.

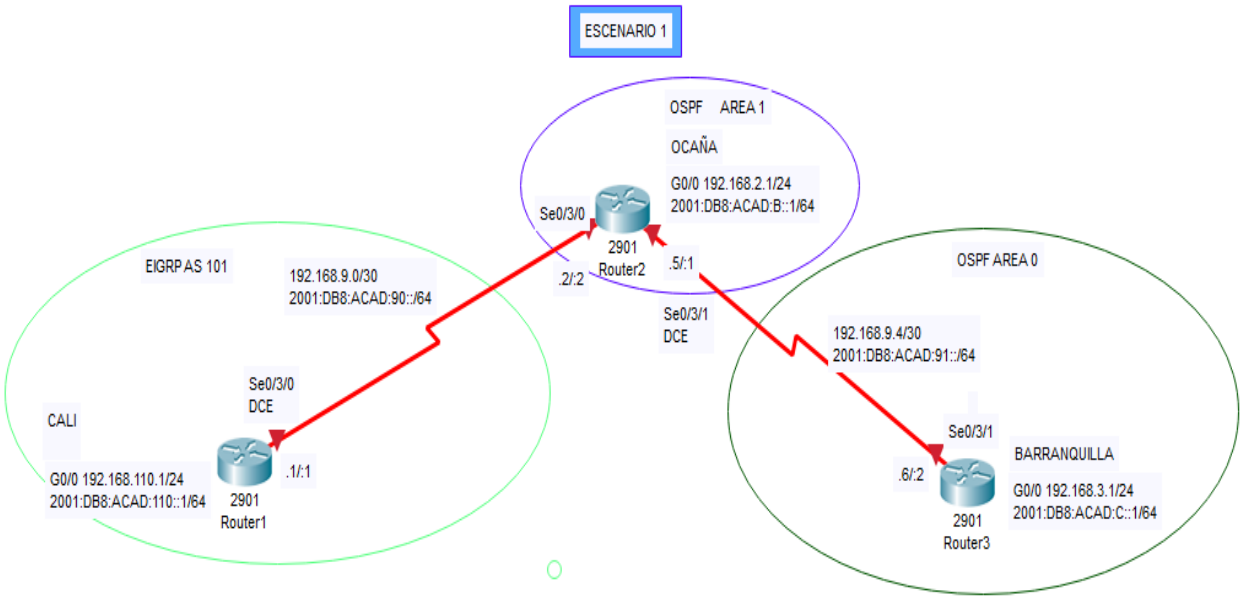

Figura 2 Topología del primer escenario en Packet Tracer

3. Realizar las configuraciones básicas de un router, para ello primero vamos a la pestaña **CLI** que es la línea de comando, donde vamos a realizar las configuraciones básicas. Cuando inicia el sistema operativo del router, nos pregunta si queremos usar el asistente de configuración, en este caso escribiremos **no,** ya que las configuraciones se harán manualmente.

   Para realizar estas configuraciones basicas en los dispositivos, inicialmente, nos aparecerá la línea de comando **router>** que quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando **enable** para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el

símbolo ha cambiado **router#.** después cambiamos el nombre de usuario, en este caso su nombre es router y lo cambiaremos por medio del comando **hostname** seguido del nombre que le colocaremos al router, en este caso **R1.**

Luego escribimos el comando **service password-encryption** para encriptar las contraseñas y le colocamos una contraseña secreta, que no se podrá visualizar por medio del comando **enable secret cisco**.

Otras configuraciones basicas que se agregan son las contraseñas a las líneas de consola y línea vty por medio de los comandos **line console 0** y **line vty 0 4** enter **password cisco** después tenemos que escribir el comando **login** para que acepte y aplique las contraseñas. También se debe restringir el acceso del puerto de consola y se configuran las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet. Si no configura una contraseña de vty, no podrá hacer Telnet al switch, ahora se puede observar a continuación como se escribirían estas líneas en el router por medio los siguientes comandos.

- **Router 1**

```
Router> enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#enable secret cisco.
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config)#service password-encryption
```

- **Router 2**

```
Router> enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#enable secret cisco.
R2(config-line)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config)#service password-encryption
```

- **Router 3**

  Router> enable
  Router#configure terminal
  Router(config)#hostname R3
  R3(config-line)#enable secret cisco.
  R3(config-line)#line console 0
  R3(config-line)#password cisco
  R3(config-line)#login
  R3(config-line)#line vty 0 4
  R3(config-line)#password cisco
  R3(config-line)#login
  R3(config)#service password-encryption

4. Configurar las interfaces con las direcciones IPv4 e IPv6 que se muestran en la topología de red usando las siguientes líneas de comandos en cada Router según corresponda. Como vemos a continuación.

   Se escribe el comando **no shutdown** debido a que por defecto las interfaces ya están encendidas.

   - **R1**

     R1(config)#interface Se0/3/0
     R1(config-if)#ip address 192.168.9.1 255.255.255.252
     R1(config-if)#no shutdown
     R1(config-if)#interface gi0/0
     R1(config-if)#ip address 192.168.110.1 255.255.255.0
     R1(config-if)#no shutdown
     R1(config-if)#exit
     R1(config)#ipv6 unicast-routing
     R1(config)#interface Se0/3/0
     R1(config-if)#ipv6 address 2001:DB8:ACAD:90::1/64
     R1(config-if)#ipv6 address FE80::1 link-local
     R1(config-if)#no shutdown
     R1(config-if)#interface gi0/0
     R1(config-if)#ipv6 address 2011:DB8:ACAD:110::1/64
     R1(config-if)#ipv6 address FE80::1 link-local
     R1(config-if)#no shutdown

   - **R2**

     R2(config)#interface Se0/3/0

```
R2(config-if)#ip address 192.168.9.2 255.255.255.252
R2(config-if)#no shutdown
R2(config)#interface Se0/3/1
R2(config-if)#ip address 192.168.9.5 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#interface gi0/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ipv6 unicast-routing
R2(config)#interface Se0/3/0
R2(config-if)#ipv6 address 2001:DB8:ACAD:90::2/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Se0/3/1
R2(config-if)#ipv6 address 2001:DB8:ACAD:91::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface gi0/0
R2(config-if)#ipv6 address 2011:DB8:ACAD:B::1/64
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#no shutdown
R2(config-if)#exit
```

- **R3**

```
R3(config)#interface Se0/3/1
R3(config-if)#ip address 192.168.9.6 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#interface gi0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ipv6 unicast-routing
R3(config)#interface Se0/3/1
R3(config-if)#ipv6 address 2001:DB8:ACAD:91::2/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown
R3(config-if)#interface gi0/0
R3(config-if)#ipv6 address 2011:DB8:ACAD:C::1/64
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#no shutdown
```

5. 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, usando las siguientes líneas de comandos en cada router según corresponda.

   - **R1**

     ```
     R1(config)#interface Se0/3/0
     R1(config-if)#bandwidth 128
     R1(config-if)#clock rate 128000
     R1(config-if)#exit
     ```

   - **R2**

     ```
     R2(config)#interface Se0/3/0
     R2(config-if)#bandwidth 128
     R2(config-if)#exit
     R2(config)#interface Se0/3/1
     R2(config-if)#clock rate 128000
     R2(config-if)#bandwidth 128
     R2(config-if)#exit
     ```

   - **R3**

     ```
     R3(config)#interface Se0/3/1
     R3(config-if)#bandwidth 128
     R3(config-if)#exit
     ```

6. 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, usando las siguientes líneas de comandos en cada Router según corresponda.

   - **R2**

     ```
     R2(config)#router ospf 1
     R2(config-router)#router-id 2.2.2.2
     R2(config-router)#exit
     ```

   - **R3**

     ```
     R3(config)#router ospf 1
     R3(config-router)#router-id 3.3.3.3
     R3(config-if)#exit
     ```

7. 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, usando las siguientes líneas de comandos en cada Router según corresponda.

   - **R2**

     R2(config)#router ospf 1
     R2(config-router)#network 192.168.9.0 0.0.0.3 area 0
     R2(config-router)#network 192.168.4.0 0.0.0.3 area 0
     R2(config-router)#network 192.168.2.1 0.0.0.3 area 1
     R2(config-router)#exit

8. En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área 0, usando las siguientes líneas de comandos en cada Router según corresponda.

   - **R3**

     R3(config)#router ospf 1
     R2(config-router)#network 192.168.9.4 0.0.0.3 area 0
     R2(config-router)#exit

9. Realizar la configuración del protocolo EIGRP para IPv4 como IPv6. Hay que 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, usando las siguientes líneas de comandos en cada Router según corresponda.

   - **R1**

     R1(config)#router eigrp 101
     R1(config-router)#network 192.168.9.0
     R1(config-router)#exit

   - **R2**

     R2(config)#router eigrp 101
     R2(config-router)#network 192.168.9.0
     R2(config-router)#exit

10. En R2, de hacer publicidad de la ruta 192.168.3.0/24 a R1 mediante una lista de distribución y ACL, usando las siguientes líneas de comandos en cada Router según corresponda.

- **R2**

  R2(config)#access-list 1 permit 192.168.3.0 255.255.255.0

1.3 VERIFICACION DE CONECTIVIDAD EN LA RED

Verificar conectividad de red y control de la trayectoria, por medio de los siguientes pasos:

1. Registrar las tablas de enrutamiento en cada uno de los Router, acorde con los parámetros de configuración establecidos en el escenario propuesto. Por medio del comando **show ip route**, podemos observar los enrutamientos.

- **R1**

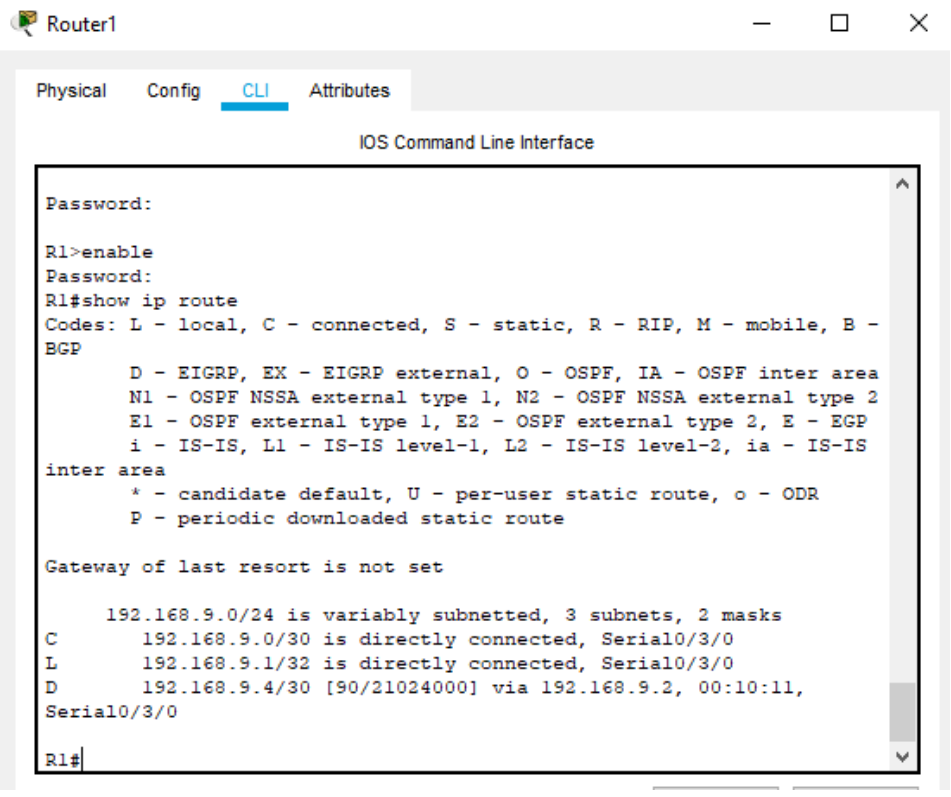

Figura 3 Comprobación de enrutamiento en el Router R1

- **R2**

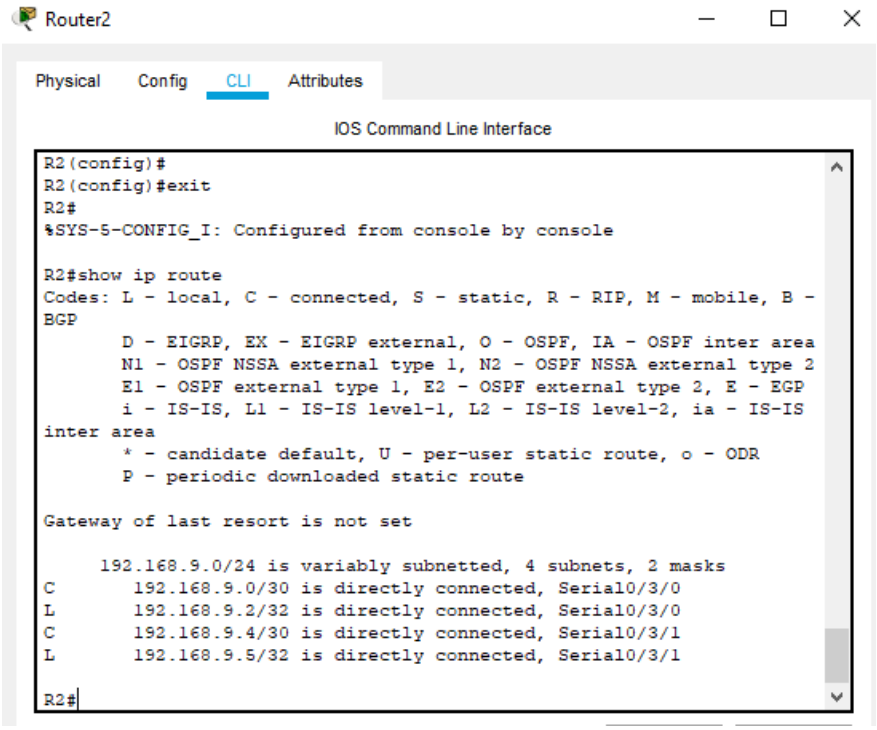

Figura 4 Comprobación de enrutamiento en el Router R2

- **R3**

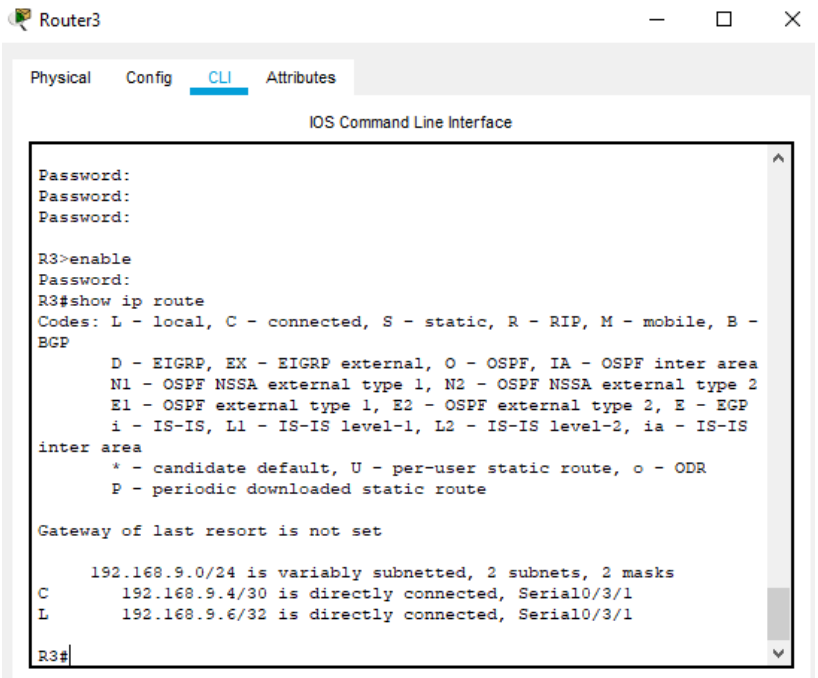

Figura 5 Comprobación de enrutamiento en el Router R3

En las figuras se puede observar los enrutamientos que se realizaron en cada uno de los router según correspondía en las configuraciones realizadas según el procedimiento anterior, además el comando show ip route nos permite verificar que las direcciones IP que se asignaron a los puertos seriales.

2. Verificar comunicación entre router mediante el comando **ping y traceroute**

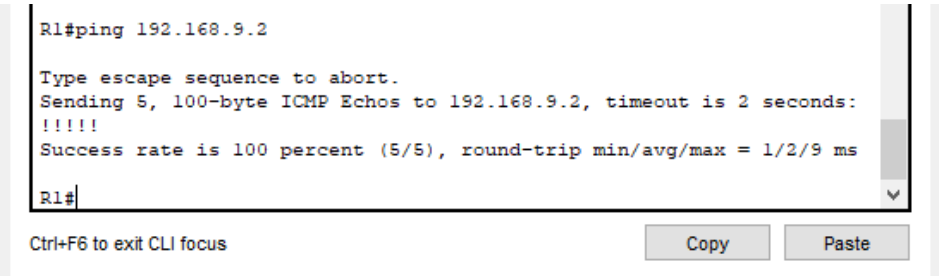

Figura 6 Verificación de comunicación de R1 con R2

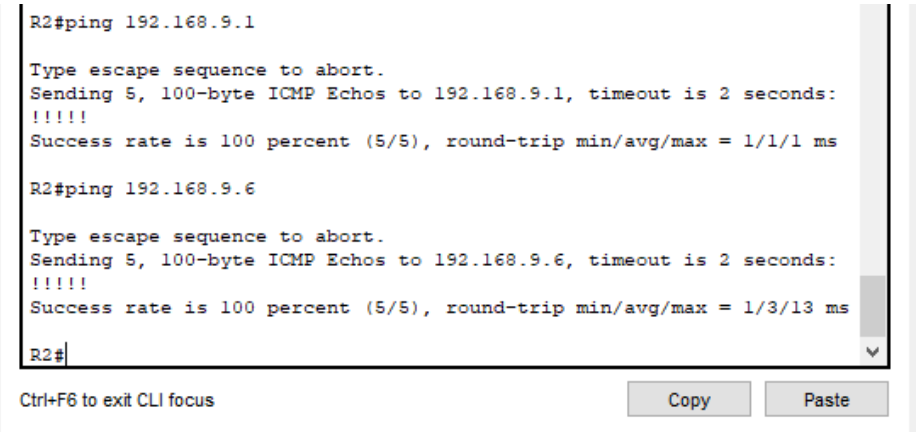

Figura 7 Verificación de comunicación de R2 con R1 y R3

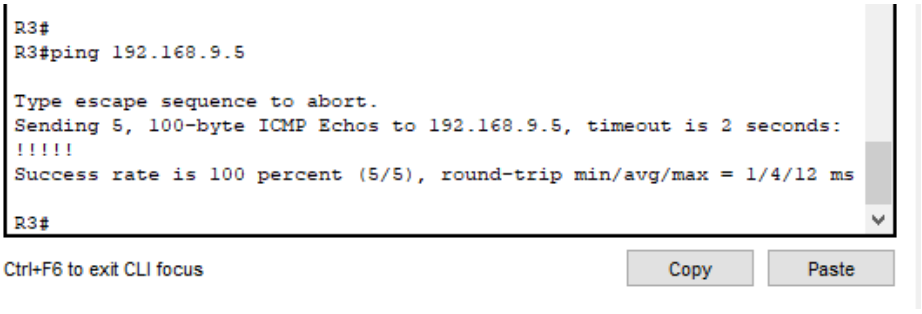

Figura 8 Verificación de comunicación de R3 con R2

Al hacer ping en cada uno de los router, efectivamente se comprobó que hay comunicación entre ellos y como se puede observar en las figuras el porcentaje de conexión es cien por ciento.

3. Verificar que las rutas filtradas no están presentes en las tablas de enrutamiento de los router correctas, por medio del comando **show ipv6 route** podemos verificar.
    - **R1**

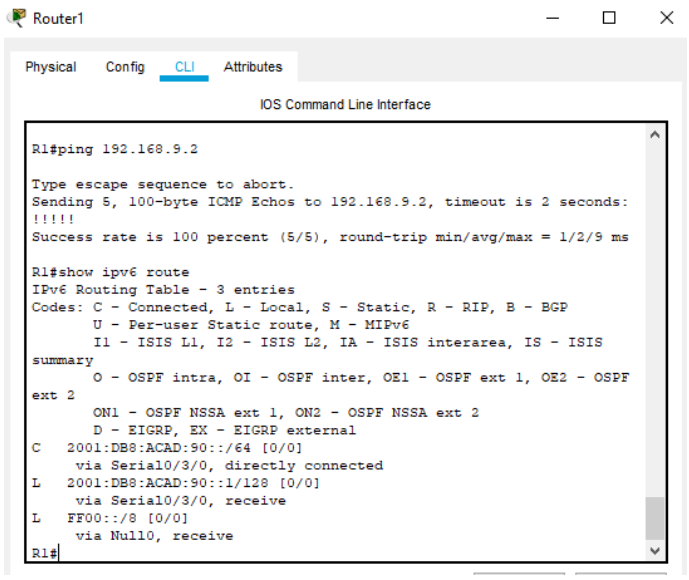

Figura 9 Verificación de las rutas filtradas en R1

    - **R2**

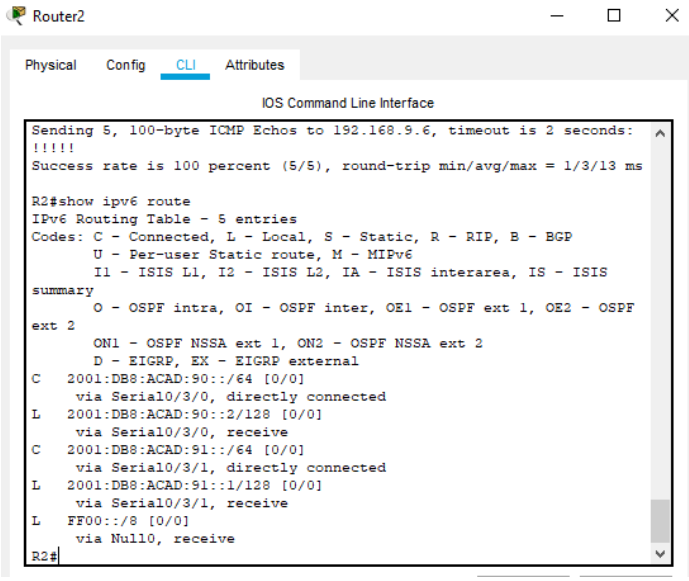

Figura 10 Verificación de las rutas filtradas en R2

- **R3**

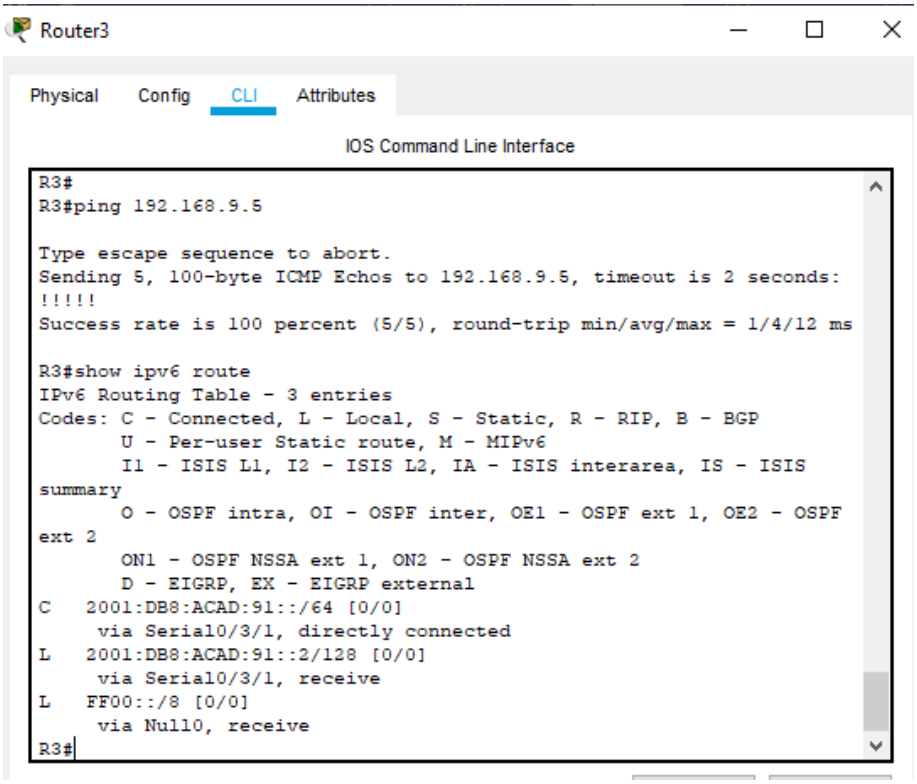

Figura 11 Verificación de las rutas filtradas en R3

Por medio del comando show ipv6 route, observamos y comprobamos que las rutas fuesen sido bien establecidas, el desarrollo paso a paso del procedimiento permitió cumplir satisfactoriamente con el desarrollo del primer escenario por medio del programa packet tracer.

2. SEGUNDO ESCENARIO

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

2.1 TOPOLOGÍA DE RED

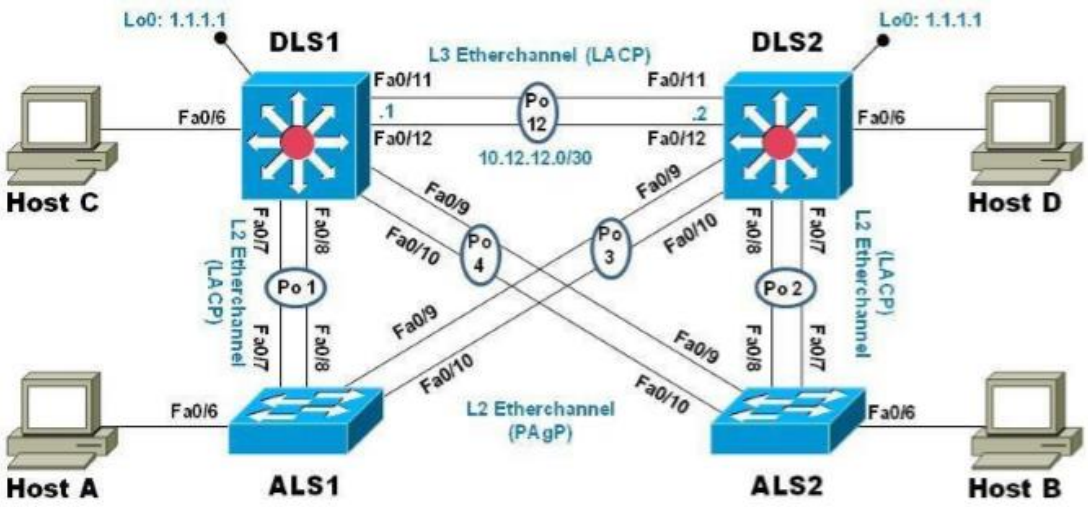

Figura 12 Topología de la Red Escenario 2

2.2 PROCEDIMIENTO DEL DESARROLLO

1. Agregar a la pantalla principal del programa Packet Tracer los router, teniendo en cuenta la topología de la red y según sea el caso borrar cualquier configuración del switch, si es necesario.
2. Para realizar la topología de la red, tal como se muestra en la figura 12, inicialmente agregamos a la pantalla principal del programa Packet Tracer el switch 2960, el switch 3560 24PS y los PC's, los dispositivos se encuentran unidos por cable ethernet, como podemos observar en la topología de la red.

Asegurar que el switch no tenga configuraciones, si es necesario por medio del comando **erase startup-config** eliminamos los archivos y con el comando **reload** se volverán a cargar los dispositivos.

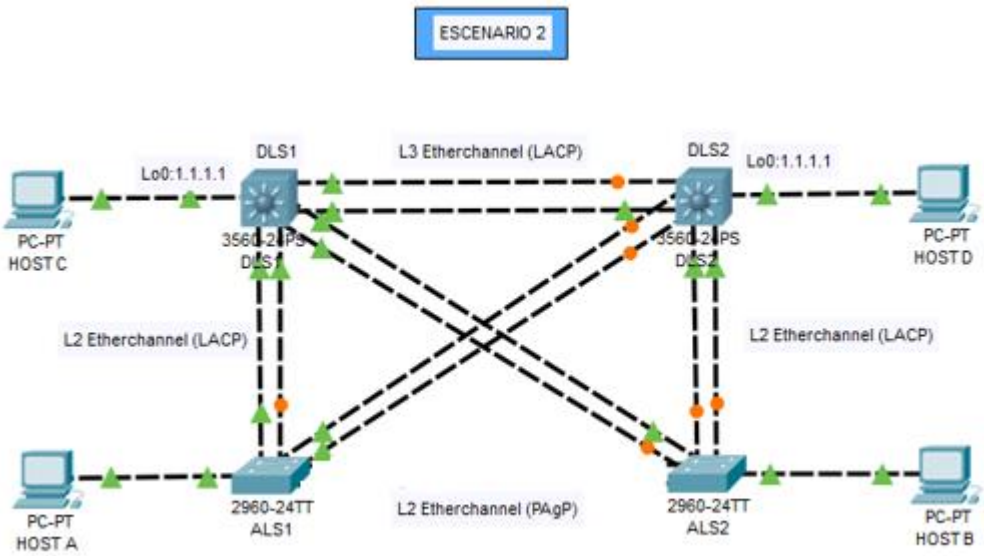

Figura 13 Topología del segundo escenario en Packet Tracer

3. Realizar las configuraciones básicas de los switch usando los siguientes comandos.

Para realizar estas configuraciones basicas en los dispositivos, inicialmente, nos aparecerá la línea de comando **switch>** que quiere decir usuario modo normal, en este usuario no podemos realizar ninguna configuración, por lo que comenzamos colocando el comando **enable** para cambiar de usuario y damos enter para pasar a un usuario con privilegios, ahora podemos observar que el símbolo ha cambiado **switch#.** después cambiamos el nombre de usuario, en este caso su nombre es router y lo cambiaremos por medio del comando **hostname** seguido del nombre que le colocaremos al **switch**, en este caso DLS1DLS2 según corresponda.

Luego escribimos el comando **service password-encryption** para encriptar las contraseñas y le colocamos una contraseña secreta que no se podrá visualizar por medio del comando **enable secret cisco.**

Otras configuraciones basicas que se agregan son las contraseñas a las líneas de consola y línea vty por medio de los comandos **line console 0** y **line vty 0 15** enter **password cisco** después tenemos que escribir el comando **login** para que acepte y aplique las contraseñas. También se debe restringir el acceso del puerto de

consola y se configuran las líneas de terminal virtual (vty) para que el switch permita el acceso por Telnet.

Si no configura una contraseña de vty, no podrá hacer Telnet al switch, ahora se puede observar a continuación como se escribirían estas líneas en el switch por medio los siguientes comandos.

- **DLS1**

```
Switch> enable
Switch #configure terminal
Switch(config) #hostname DLS1
DLS1(config) #enable secret cisco.
DLS1(config) #line console 0
DLS1(config-line)#password cisco
DLS1(config-line)#login
DLS1(config-line)#line vty 0 15
DLS1(config-line)#password cisco
DLS1(config-line)#login
DLS1(config-line)#service password-encryption
```

- **DLS2**

```
Switch> enable
Switch #configure terminal
Switch(config) #hostname DLS2
DLS2(config) #enable secret cisco.
DLS2(config) #line console 0
DLS2(config-line)#password cisco
DLS2(config-line)#login
DLS2(config-line)#line vty 0 15
DLS2(config-line)#password cisco
DLS2(config-line)#login
DLS2(config-line)#service password-encryption
```

- **ALS1**

```
Switch> enable
Switch #configure terminal
Switch(config) #hostname ALS1
ALS1(config) #enable secret cisco.
```

```
ALS1(config) #line console 0
ALS1(config-line)#password cisco
ALS1(config-line)#login
ALS1(config-line)#line vty 0 15
ALS1(config-line)#password cisco
ALS1(config-line)#login
ALS1(config-line)#service password-encryption
```

- **ALS2**

```
Switch> enable
Switch #configure terminal
Switch(config) #hostname ALS2
ALS2(config) #enable secret cisco.
ALS2(config) #line console 0
ALS2(config-line)#password cisco
ALS2(config-line)#login
ALS2(config-line)#line vty 0 15
ALS2(config-line)#password cisco
ALS2(config-line)#login
ALS2(config-line)#service password-encryption
```

4. Apagar todas las interfaces en cada switch, usando las siguientes líneas de comandos en cada switch según corresponda.

Para realizar este ítem en cada switch y reducir las líneas de código, utilizamos el comando **interface range,** que nos permite configurar un grupo de interfaces, en este caso serán las interfaces **f0/1-24**. Luego colocamos el comando **shutdown** para que se apague este rango de interfaces, debido a que por defecto las interfaces ya están encendidas.

- **DLS1**

```
DLS1(config)#interface range f0/1-24
DLS1(config-if-range)#shutdown
```

- **DLS2**

```
DLS2(config)#interface range f0/1-24
DLS2(config-if-range)#shutdown
```

- **ALS1**

  ALS1(config)#interface range f0/1-24
  ALS1(config-if-range)#shutdown

- **ALS2**

  ALS2(config)#interface range f0/1-24
  ALS2(config-if-range)#shutdown

5. Configurar los puertos troncales y Port-channels tal como se muestra en el diagrama, usando las siguientes líneas de comandos.

Los puertos troncales que vamos a configurar son enlaces punto a punto entre DLS1 y DLS2 permitiendo que pase más de una VLAN, hacia toda la red.

Por medio del comando **interface range** le podemos asignar más fácilmente a un grupo una orden, como es el caso las interfaces f0/11-12 se activarán por medio del comando **no shutdown**, luego se asignará una dirección IP con el comando **ip address** seguidamente la dirección espacio y la puerta de enlace al EtherChannel, como podemos observar en los comandos que se muestran a continuación. Estos comandos se escriben tal cual en la pestaña CLI del switch.

Configurar EtherChannel provee más velocidad a los puertos, más capacidad y mayor rendimiento debido a que está compuesto por varios enlaces que reparten los datos para hacer más rápido el proceso.

a. 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**

  DLS1(config)#interface range f0/11-12
  DLS1(config-if-range)#channel-group 12 mode active
  DLS1(config-if-range)#no shutdown
  DLS1(config-if-range)#exit
  DLS1(config)#interface port-channel 12
  DLS1(config)#ip address 10.12.12.1 255.255.255.252
  DLS1(config)#exit

- **DLS2**

```
DLS2(config)#interface range f0/11-12
DLS2(config-if-range)#channel-group 12 mode active
DLS2(config-if-range)#no shutdown
DLS2(config-if-range)#exit
DLS2(config)#interface port-channel 12
DLS2(config)#ip address 10.12.12.2 255.255.255.252
DLS2(config)#exit
```

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

En cada switch se ingresa las interfaces f0/7 y f0/8, utilizando el comando **interface range f0/7-8**, después se activará un Etherchannel por medio del protocolo **LACP** donde la configuración de los puertos se hará agrupando los que cuenten con características similares y por último se activaran las interfaces con el comando **no shutdown.**

- **DLS1**

```
DLS1(config)#interface range f0/7-8
DLS1(config-if-range)#channel-group 1 mode active
DLS1(config-if-range)#no shutdown
```

- **ALS1**

```
ALS1(config)#interface range f0/7-8
ALS1(config-if-range)#channel-group 1 mode active
ALS1(config-if-range)#no shutdown
```

- **DLS2**

```
DLS2(config)#interface range f0/7-8
DLS2(config-if-range)#channel-group 2 mode active
DLS2(config-if-range)#no shutdown
```

- **ALS2**

```
ALS2(config)#interface range f0/7-8
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#no shutdown
```

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

En cada switch se ingresa a las interfaces f0/9 y f0/10, utilizando el comando **interface range f0/9-10,** después se activará un Etherchannel por medio del protocolo **PAgP** donde la configuración de los puertos se hará agrupando los puertos que cuenten con características similares. El protocolo **PAgP** se encomendará la tarea de agrupar estos puertos ya sea por características como la velocidad, puertos troncales comunes o pertenecer a la misma VLAN.

Este protocolo se puede configurar de dos modos auto y **desirable** como lo realizaremos en este paso. Se establecerá el puerto en modo activo y negociara el estado cuando reciba datos y por último se activarán las interfaces con el comando **no shutdown**.

- **DLS1**

```
DLS1(config)#interface range f0/9-10
DLS1(config-if-range)#channel-group 4 mode desirable
DLS1(config-if-range)#no shutdown
```

- **ALS2**

```
ALS2(config)#interface range f0/9-10
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#no shutdown
```

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

En este paso asignaremos a la VLAN 800 como la VLAN nativa, ya que por defecto la VLAN establecida es la VLAN 1 usando el comando **switchport trunk native vlan 800**. Al configurar la interface f0/7-12 como un puerto troncal con el comando **switchport mode trunk**, la información transitara por este puerto.

- **DLS1**

```
DLS1(config)#interface range f0/7-12
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport trunk native vlan 800
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#switchport nonegotiate
DLS1(config-if-range)#no shutdown
```

- **DLS2**

  DLS2(config)#interface range f0/7-12
  DLS2(config-if-range)#switchport trunk encapsulation dot1q
  DLS2(config-if-range)#switchport trunk native vlan 800
  DLS2(config-if-range)#switchport mode trunk
  DLS2(config-if-range)#switchport nonegotiate
  DLS2(config-if-range)#no shutdown

- **ALS1**

  ALS1(config)#interface range f0/7-12
  ALS1(config-if-range)#switchport mode trunk
  ALS1(config-if-range)#switchport trunk native vlan 800
  ALS1(config-if-range)#switchport nonegotiate
  ALS1(config-if-range)#no shutdown

- **ALS1**

  ALS1(config)#interface range f0/7-12
  ALS1(config-if-range)#switchport mode trunk
  ALS1(config-if-range)#switchport trunk native vlan 800
  ALS1(config-if-range)#switchport nonegotiate
  ALS1(config-if-range)#no shutdown

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

Para realizar la configuración VTP, debemos configurar el switch DLS1 como servidor principal por medio del comando **vtp mode server**. Luego se configura el nombre del dominio VTP con el comando **vtp domain UNAD,** donde UNAD es el nombre del dominio y por último configurar la contraseña de dominio VTP usando el comando **vtp password cisco**, donde cisco es la contraseña.

a. Utilizar el nombre de dominio UNAD con la contraseña cisco123

   DLS1(config)#vtp domain UNAD
   DLS1(config)#vtp password cisco123

b. Configurar DLS1 como servidor principal para las VLAN

   DLS1(config)#vtp mode server

c. Configurar ALS1 y ALS2 como clientes VTP.

Ahora hay que configurar el switch ALS1 y ALS2 como clientes VTP por medio del comando **vtp mode client.**

- **ALS1**

  ALS1(config)# vtp mode client

- **ALS2**

  ALS2(config)# vtp mode client

7. Configurar en el servidor principal las siguientes VLAN:

Antes de poder administrar el switch ALS1 Y ALS2 en forma remota desde HOST A y HOST B, se debe asignar una dirección IP al switch. El switch está configurado de manera predeterminada para que la administración de este se realice a través de VLAN 1.

A partir de la tabla que observamos a continuación, crearemos las VLAN con su respectivo nombre para DLS1 Y DLS2. Las VLAN se crean simplemente colocando cuando el switch está en modo configuración **vlan** y seguidamente el numero que se le asignara y con el comando **name** le podemos asignar un nombre. A continuación, observamos los comandos tal como se escriben en la pestaña CLI del switch.

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	ADMINISTRACIÓN

- **DLS1**

  DLS1(config)#vlan 800
  DLS1(config-vlan)#name NATIVA
  DLS1(config-vlan)#exit
  DLS1(config)#vlan 12
  DLS1(config-vlan)#name EJECUTIVOS
  DLS1(config-vlan)#exit

```
DLS1(config)#vlan 234
DLS1(config-vlan)#name HUESPEDES
DLS1(config-vlan)#exit
DLS1(config)#vlan 1111
DLS1(config-vlan)#name VIDEONET
DLS1(config-vlan)#exit
DLS1(config)#vlan 434
DLS1(config-vlan)#name ESTACIONAMIENTO
DLS1(config-vlan)#exit
DLS1(config)#vlan 123
DLS1(config-vlan)#name MANTENIMIENTO
DLS1(config-vlan)#exit
DLS1(config)#vlan 1010
DLS1(config-vlan)#name VOZ
DLS1(config-vlan)#exit
DLS1(config)#vlan 3456
DLS1(config-vlan)#name ADMINISTRACION
DLS1(config-vlan)#exit
```

8. En DLS1, suspender la VLAN 434.

Por medio del comando **state suspend,** colocamos la VLAN en un estado suspendido.

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

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

En el switch DS2 primero vamos a realizar la configuración VTP, medio del comando **vtp mode server**. Luego se configura el nombre del dominio VTP con el comando **vtp domain UNAD**, donde UNAD es el nombre del dominio y por último se configura la contraseña de dominio VTP usando el comando **vtp password cisco**, donde cisco es la contraseña.

```
DLS2(config)#vtp domain UNAD
DLS2(config)#vtp password cisco123
DLS2(config)#vtp mode server
```

Ahora se crearán y se le asignarán nombres a las VLAN como en DLS1.

- **DLS2**

```
DLS2(config)#vlan 800
DLS2(config-vlan)#name NATIVA
DLS2(config-vlan)#exit
DLS2(config)#vlan 12
DLS2(config-vlan)#name EJECUTIVOS
DLS2(config-vlan)#exit
DLS2(config)#vlan 234
DLS2(config-vlan)#name HUESPEDES
DLS2(config-vlan)#exit
DLS2(config)#vlan 1111
DLS2(config-vlan)#name VIDEONET
DLS2(config-vlan)#exit
DLS2(config)#vlan 434
DLS2(config-vlan)#name ESTACIONAMIENTO
DLS2(config-vlan)#exit
DLS2(config)#vlan 123
DLS2(config-vlan)#name MANTENIMIENTO
DLS2(config-vlan)#exit
DLS2(config)#vlan 1010
DLS2(config-vlan)#name VOZ
DLS2(config-vlan)#exit
DLS2(config)#vlan 3456
DLS2(config-vlan)#name ADMINISTRACION
DLS2(config-vlan)#exit
```

10. Suspender VLAN 434 en DLS2.

Por medio del comando **state suspend**, colocamos la VLAN en un estado suspendido.

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

11. 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 **spanning tree tool** (STP) es un protocolo de capa 2 que se ejecuta en switch como es el caso, para prevenir que no se creen loops ya que estos son peligrosos para una red y mas cuando se tienen trayectorias redundantes. Es mejor controlar el acceso root para optimizar y controlar la red, por medio del comando **spanning-tree vlan** seguido las vlan y después se coloca **root primary** o **secondary** según corresponda, como veremos a continuación.

```
DLS1(config)#spanning-tree vlan 1,12,434,800,1010,1111,3456 root
primary
DLS1(config)#spanning-tree vlan 123,434 root secondary
```

12. 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.

```
DLS2(config)#spanning-tree vlan 123,234 root primary
DLS2(config)#spanning-tree vlan 12,434,800,1010,1111,3456 root
secondary
```

13. 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.

Se configura tanto en el switch DLS1 como el DLS2 la interface port-channel como un puerto troncal, por medio del comando **switchport trunk allowed** y las VLAN que estarán asociadas a este.

- **DLS1**

```
DLS1(config-if)#interface port-channel
DLS1(config-if)#switchport trunk allowed vlan 12, 123, 234, 800, 1010,
1111, 3456
DLS1(config-if)#interface port-channel 4
DLS1(config-if)#switchport trunk allowed vlan 12, 123, 234, 800, 1010,
1111, 3456
```

- **DLS2**

```
DLS2(config-if)#interface port-channel 1
DLS2(config-if)#switchport trunk allowed vlan 12, 123, 234, 800, 1010,
1111, 3456
DLS2(config-if)#interface port-channel 4
DLS2(config-if)#switchport trunk allowed vlan 12, 123, 234, 800, 1010,
1111, 3456
```

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

En este paso se configuran las interfaces como puertos de acceso a las VLAN según la tabla que tenemos a continuación por medio del comando **switchport access vlan**

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		

- **DLS1**

```
DLS1(config)#interface f0/6
DLS1(config-if)#switchport access vlan 3456
DLS1(config-if)#no shutdown
DLS1(config)#interface f0/15
DLS1(config-if)#switchport access vlan 1111
DLS1(config-if)#no shutdown
```

- **DLS2**

```
DLS2(config)#interface f0/6
DLS2(config-if)#switchport access vlan 12
DLS2(config-if)#no shutdown
DLS2(config)#interface f0/6
DLS2(config-if)#switchport access vlan 1010
DLS2(config-if)#no shutdown
DLS2(config)#interface f0/15
DLS2(config-if)#switchport access vlan 1111
DLS2(config-if)#no shutdown
DLS2(config)#interface f0/16-18
DLS2(config-if)#switchport access vlan 567
DLS2(config-if)#no shutdown
```

- **ALS1**

```
ALS1(config)#interface f0/6
ALS1(config-if)#switchport access vlan 123
ALS1(config-if)#no shutdown
ALS1(config)#interface f0/6
ALS1(config-if)#switchport access vlan 1010
ALS1(config-if)#no shutdown
ALS1(config)#interface f0/15
ALS1(config-if)#switchport access vlan 1111
ALS1(config-if)#no shutdown
```

- **ALS2**

  ALS2(config)#interface f0/6
  ALS2(config-if)#switchport access vlan 234
  ALS2(config-if)#no shutdown
  ALS2(config)#interface f0/6
  ALS2(config-if)#switchport access vlan 1111
  ALS2(config-if)#no shutdown

Ahora se apagan todas las interfaces que no son utilizadas o que no se les asigno alguna VLAN usando el comando **shutdown.**

- **DLS1**

  DLS1(config)#interface range f0/1-5,f0/13-14,f0/16-24,g0/1-2
  DLS1(config-if-range)#switchport Access vlan 434
  DLS1(config-if-range)#shutdown

- **DLS2**
  DLS2(config)#interface range f0/1-5,f0/13-14,f0/16-24,g0/1-2
  DLS2(config-if-range)#switchport Access vlan 434
  DLS2(config-if-range)#shutdown

2.3 VERIFICACION DE CONECTIVIDAD EN LA RED

Verificar conectividad de red y control de la trayectoria, por medio de los siguientes pasos:

1. Verificar la existencia de las VLAN correctas en todos los switch y la asignación de puertos troncales y de acceso. Esta verificación se realiza por medio del comando **show vlan**.

A través de este comando podemos observar las VLAN que se crearon en cada switch, si están activas o no y los puertos de acceso que se asignaron.

Al escribir el comando show vlan, primeramente, en la pestaña CLI de los switch, se consiguieron varios errores debidos a que a la hora de escribir los comandos que permiten crear las VLAN se omitieron, Errores pequeños que afectan los buenos resultados que se esperan obtener a partir de las configuraciones realizadas y que se pasaron por alto, pero que pueden provocar que la red no funcione correctamente como es el caso, por ello es importante realizar verificaciones después de cada configuración o modificación que se realice en los dispositivos.

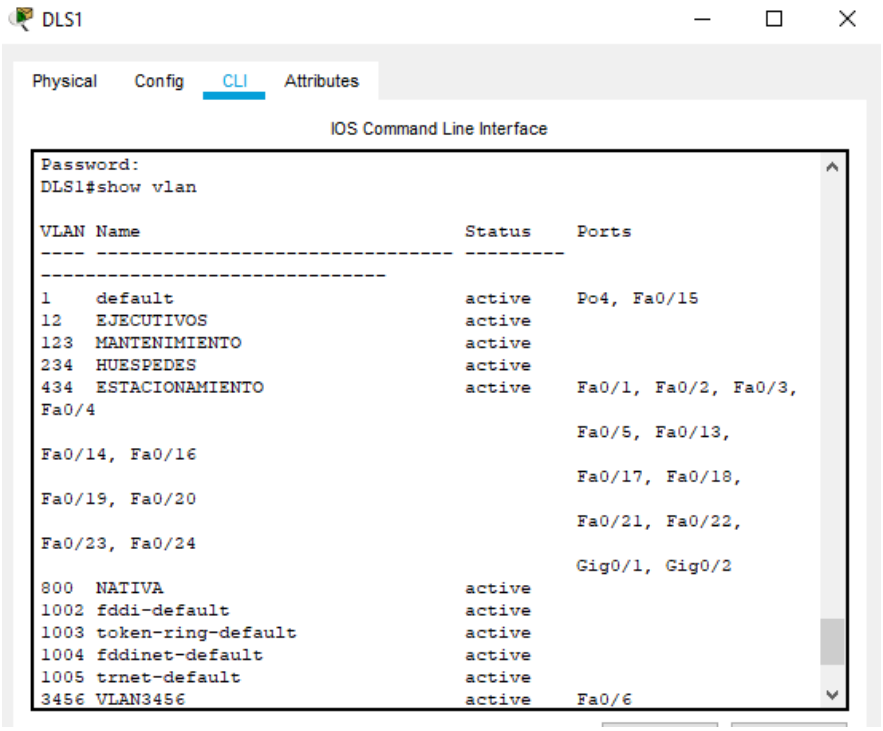

Figura 14 Verificación de las VLAN en DSL1

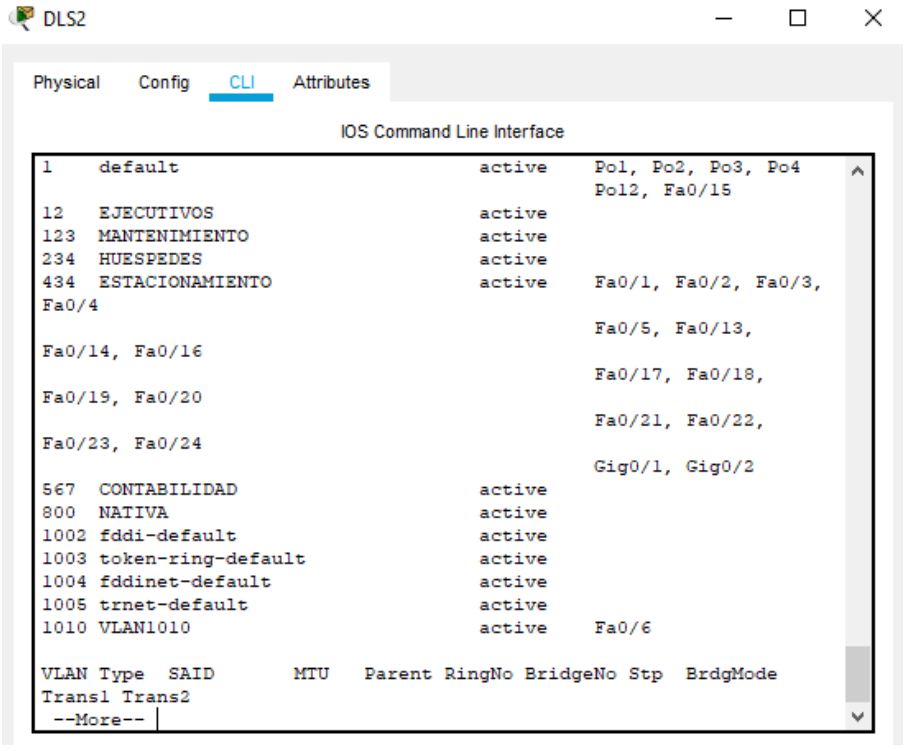

Figura 15 Verificación de las VLAN en DSL2

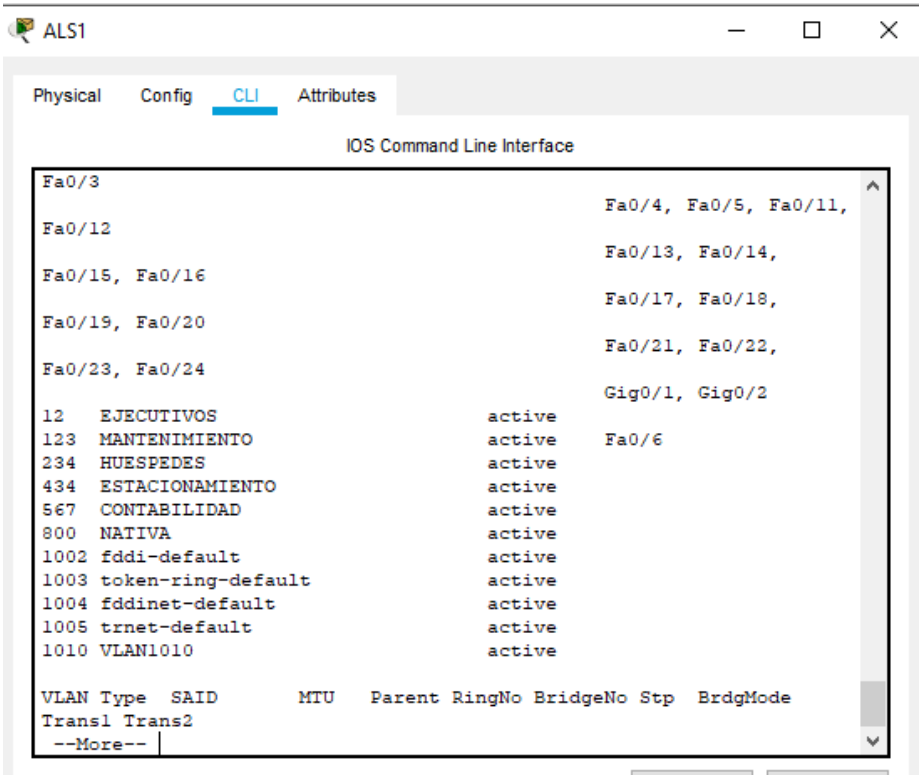

Figura 16 Verificación de las VLAN en ASL1

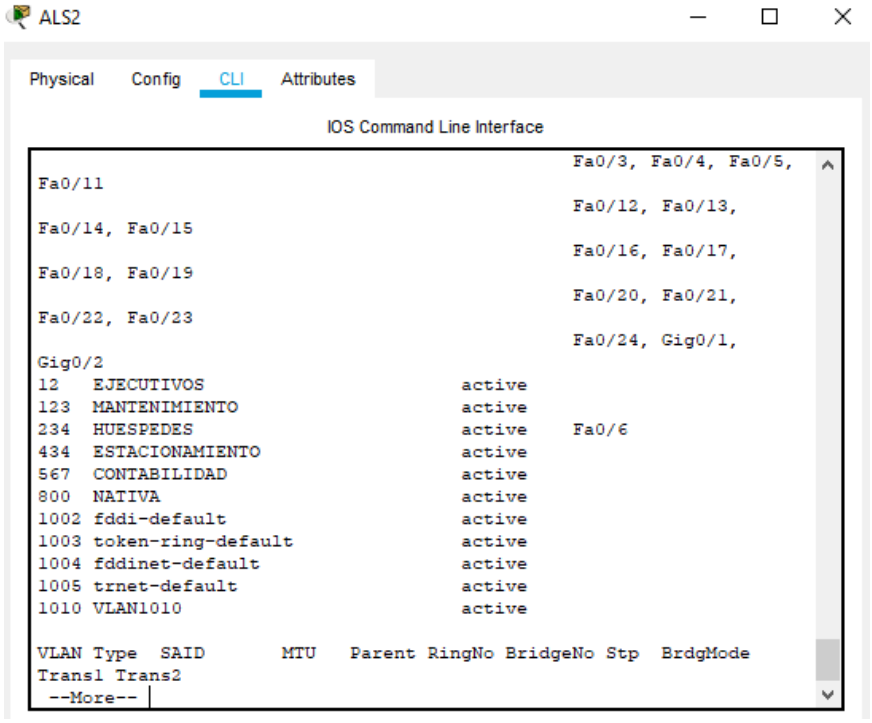

Figura 17 Verificación de las VLAN en ASL2

2. Verificar que el EtherChannel entre DLS1 y ALS1 está configurado correctamente. Esta verificación se realiza por medio del comando **show interface etherchannel.**

Figura 18 Verificación EtherChannel en DLS1

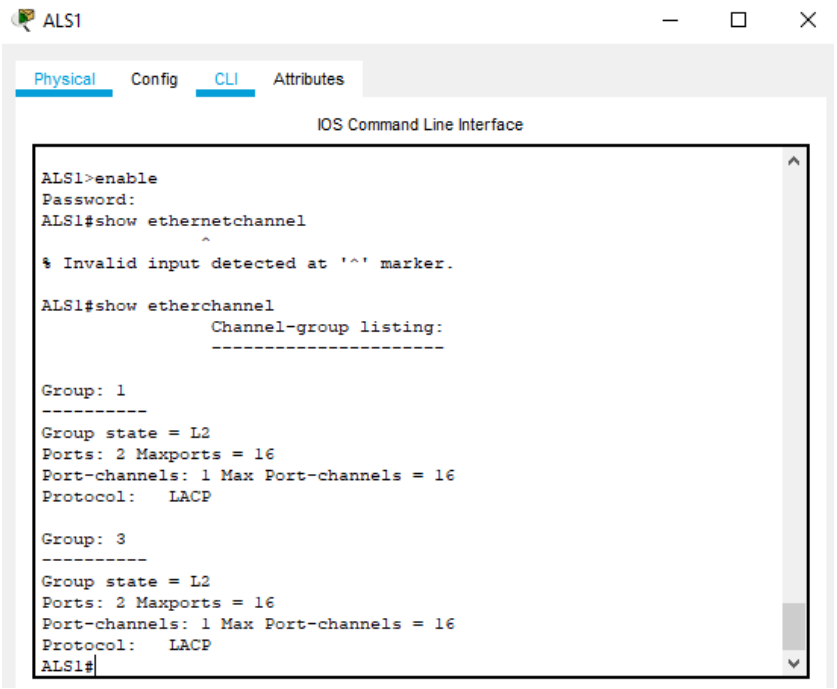

Figura 19 verificación EtherChannel en ALS1

El comando show Ehernetchannel, permite ver las configuraciones que se realizaron en este puerto, podemos ver la lista de grupos de los puertos y la información de cada uno de ellos.

3. Verificar la configuración de Spanning tree entre DLS1 o DLS2 para cada VLAN. Esta verificación se realiza por medio del comando **show spanning**

Como resultado de ejecutar el comando show spanning, se obtiene la información del estado actual de cada VLAN, información que se utilizo para comprobar que las configuraciones de este protocolo se realizaron correctamente.

Se debe tener en cuenta cuando realizamos la topología y conectamos los switch en la red, estos empiezan a comunicarse y publican un numero de revisión, si este número es mayor en un switch de la red, este se convertirá en switch root por lo que la red no funcionaria hasta que esta revisión no sea cero. En las configuraciones que realizamos por medio del comando spanning-tree vlan 1 root primay/secondary como correspondía se realiza automáticamente este proceso, por lo tanto, en la figura podemos observar como se ha configurado el Bridge ID Priority que automáticamente le da un valor de 0.

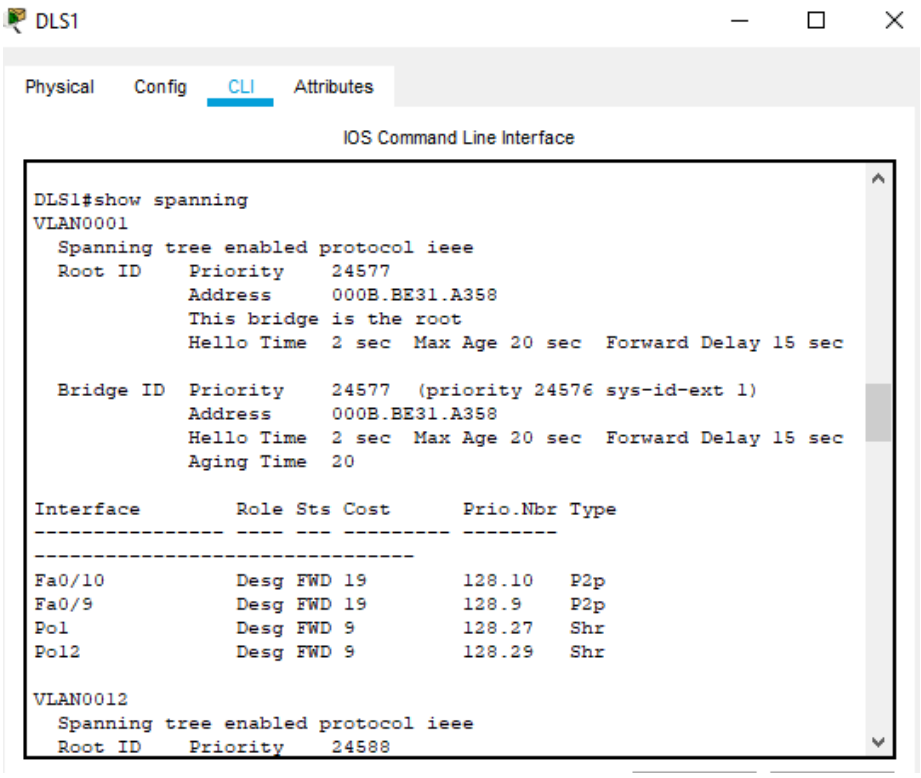

Figura 20 Verificación de la configuración spanning tree de la vlan 0001 en DLS1

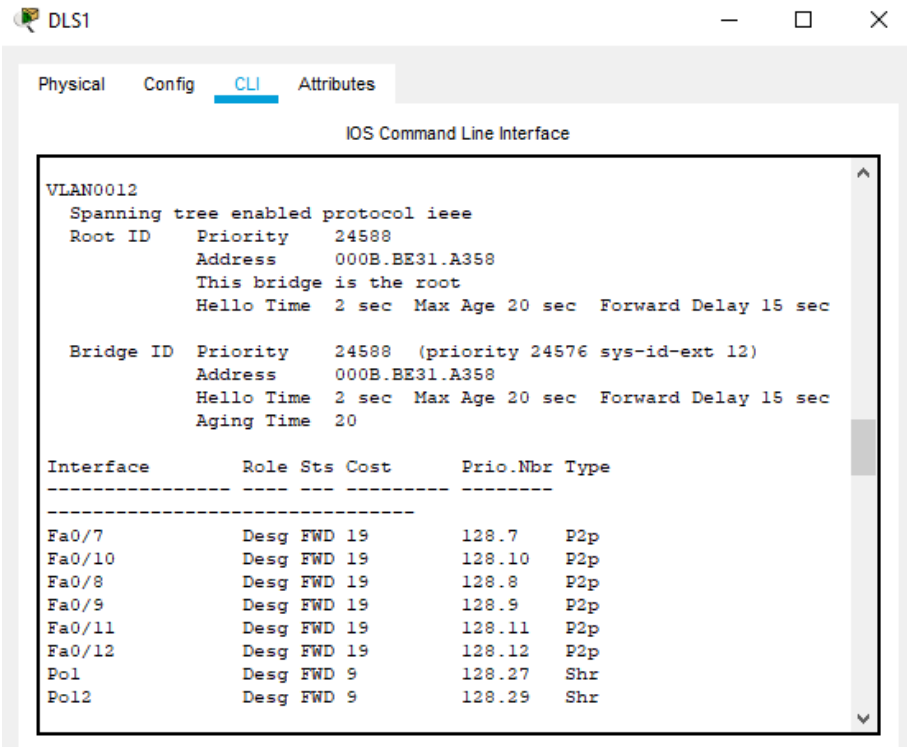

Figura 21 Verificación de la configuración spanning tree de la vlan 00012 en DLS1

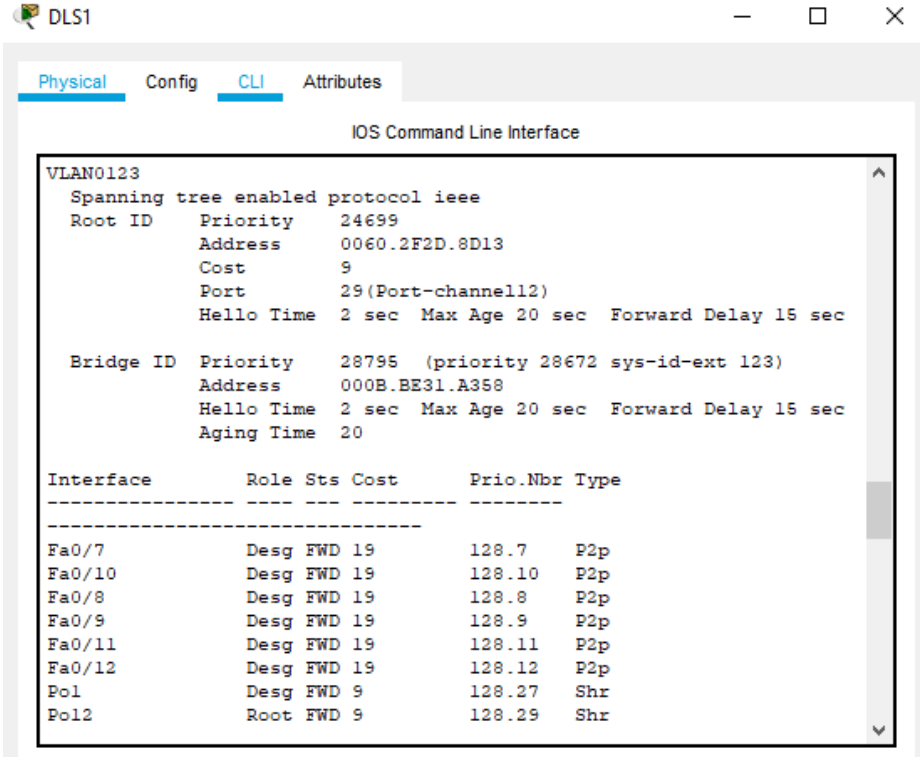

Figura 22 Verificación de la configuración spanning tree de la vlan 123 en DLS1

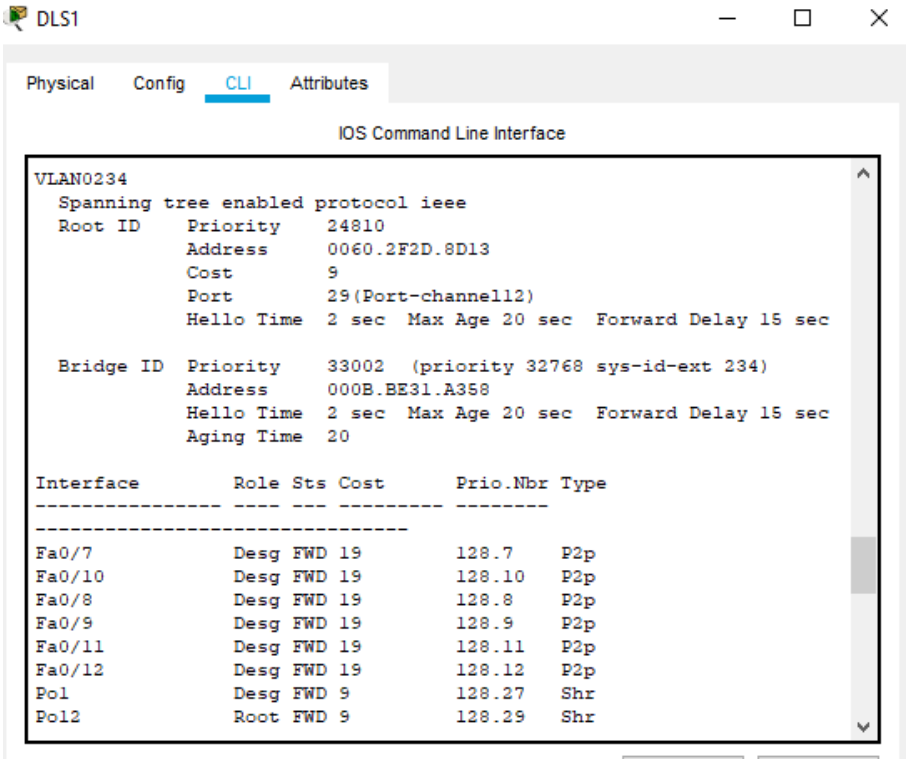

Figura 23 Verificación de la configuración spanning tree de la vlan 234 en DLS1

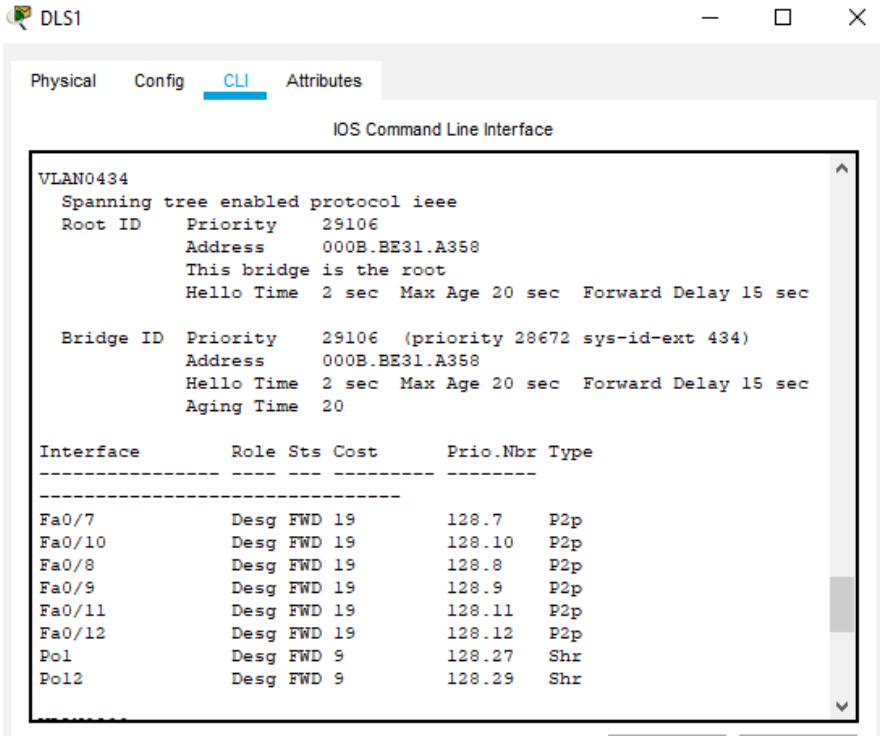

Figura 24 Verificación de la configuración spanning tree de la vlan 434 en DLS1

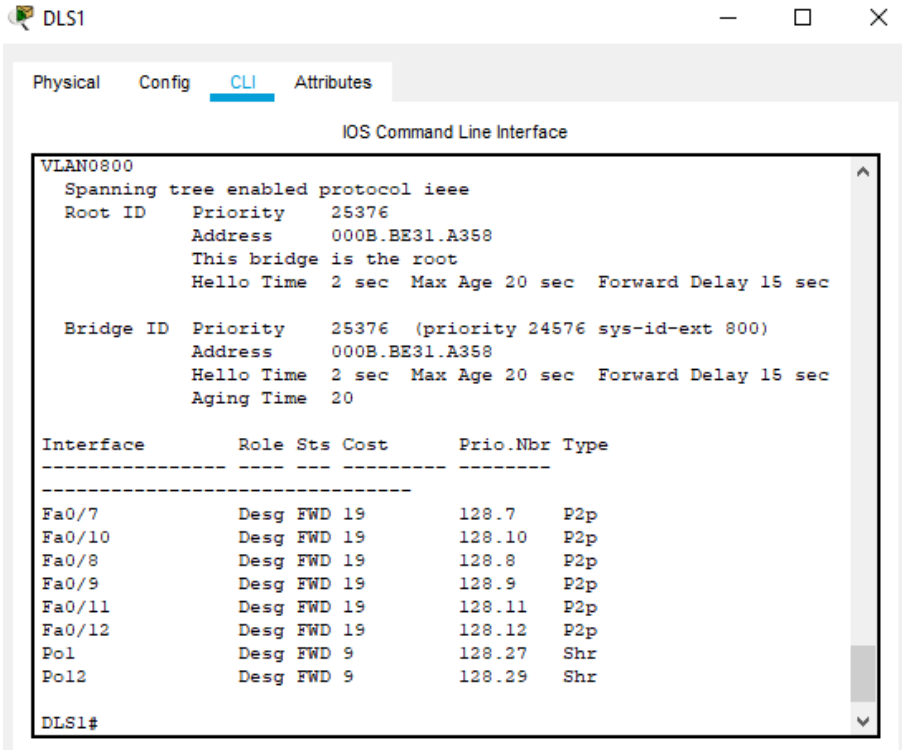

Figura 25 Verificación de la configuración spanning tree de la vlan 800 en DLS1

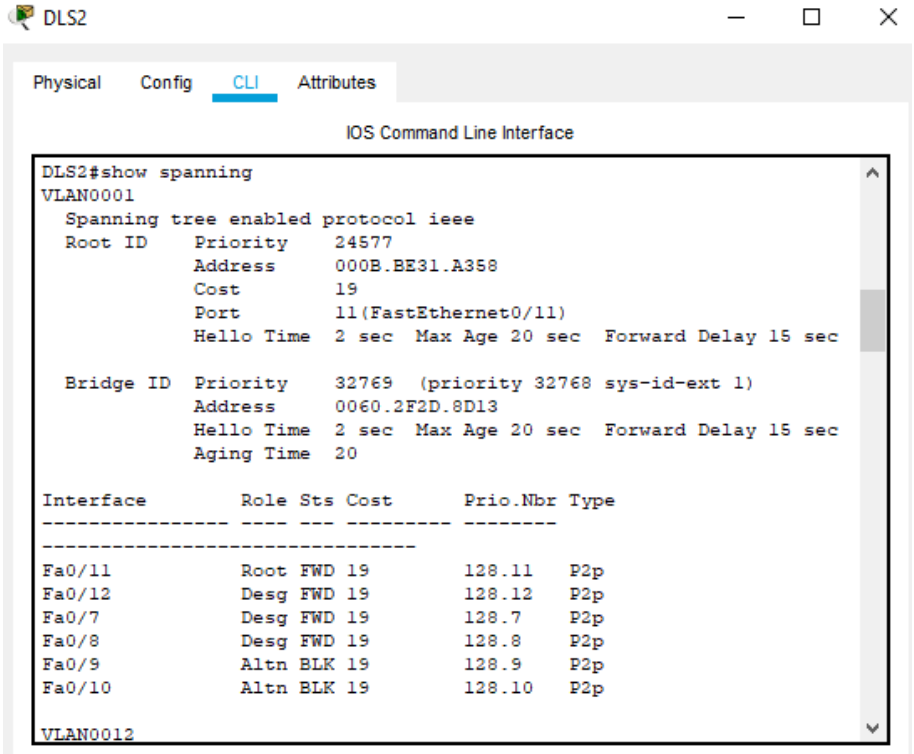

Figura 26 Verificación de la configuración spanning tree de la vlan 001 en DLS2

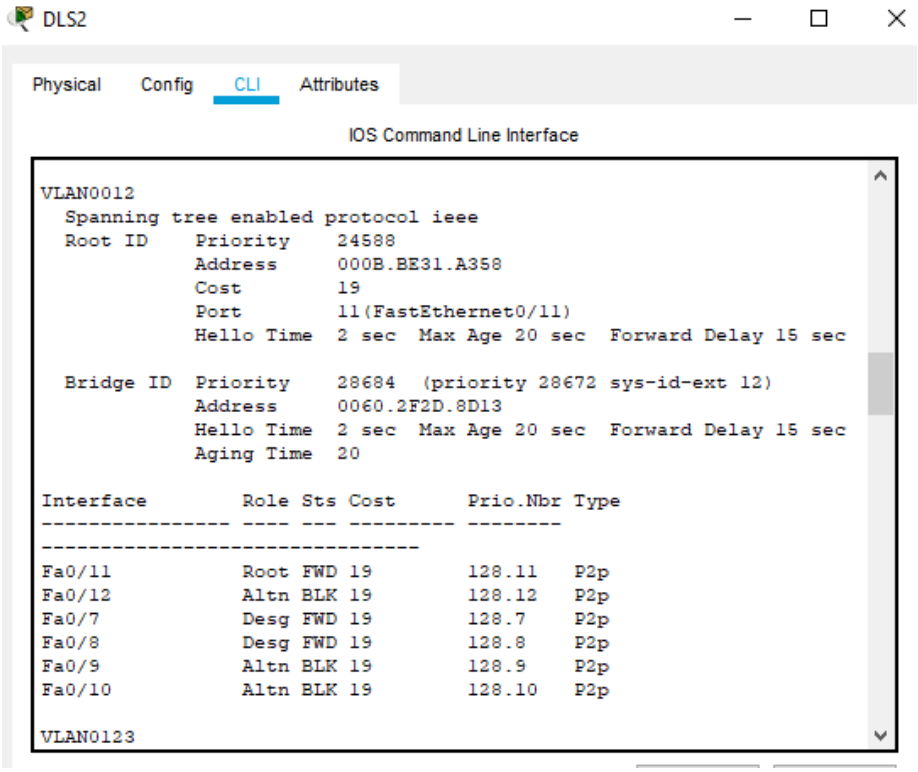

Figura 27 Verificación de la configuración spanning tree de la vlan 0012 en DLS2

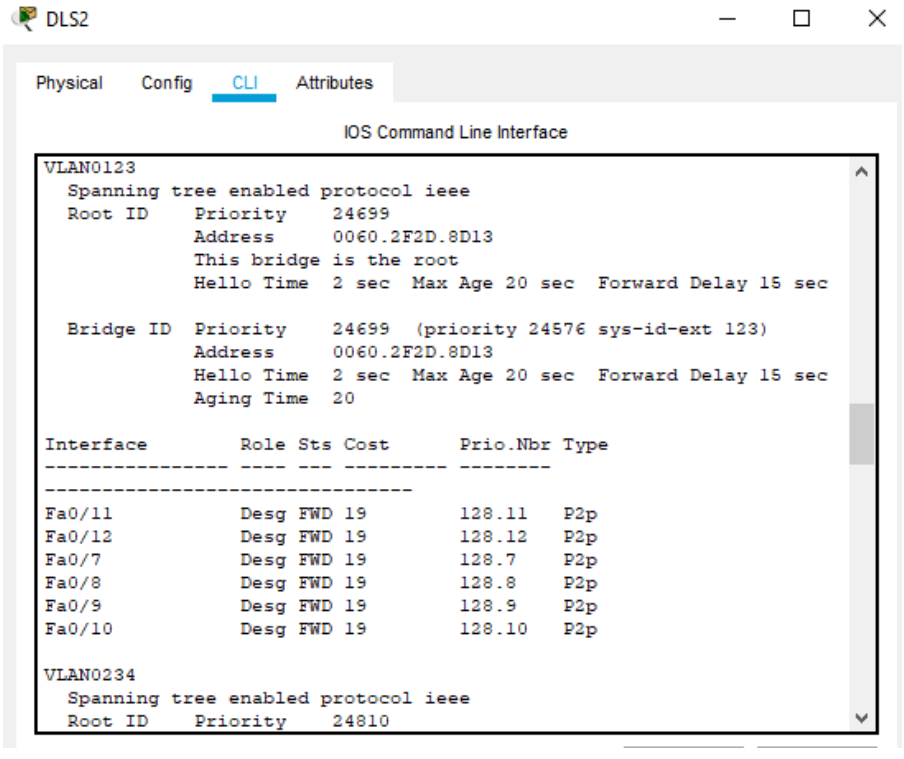

Figura 28 Verificación de la configuración spanning tree de la vlan 123 en DLS2

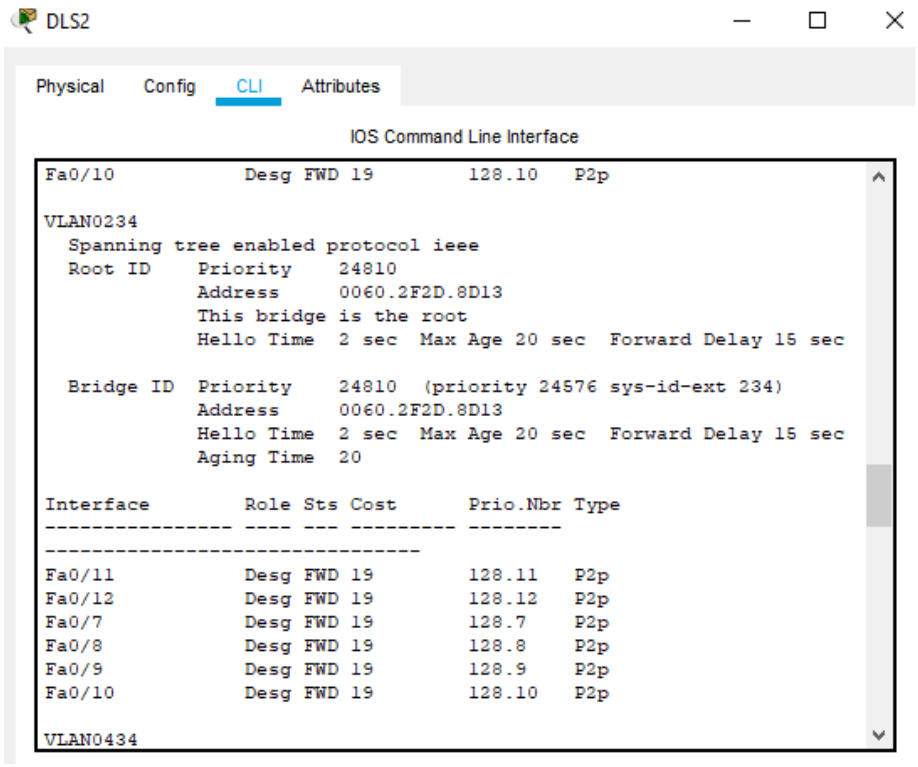

Figura 29 Verificación de la configuración spanning tree de la vlan 234 en DLS2

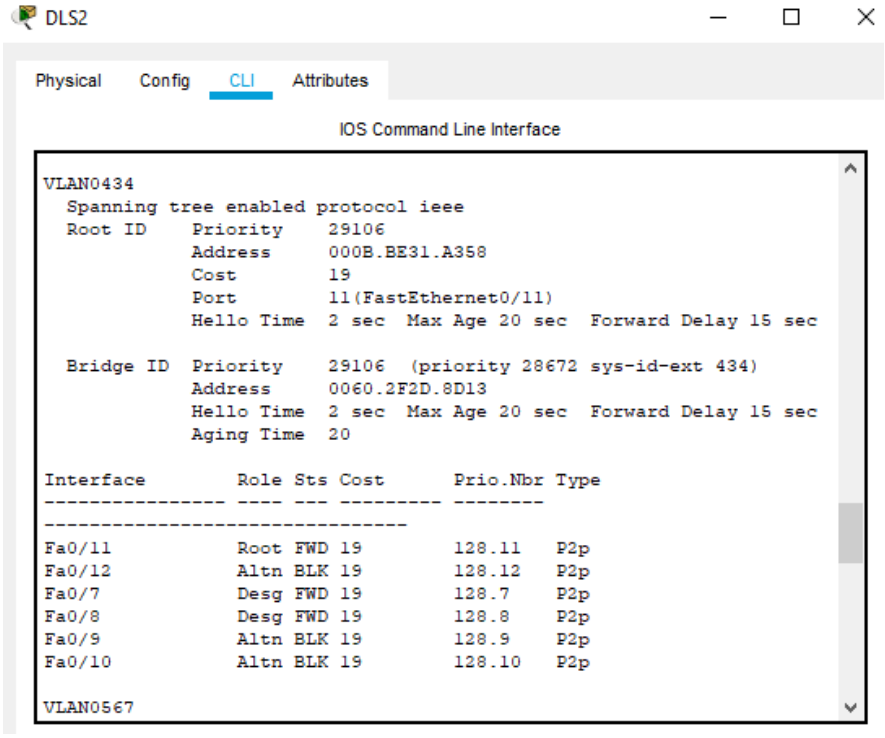

Figura 30 Verificación de la configuración spanning tree de la vlan 434 en DLS1

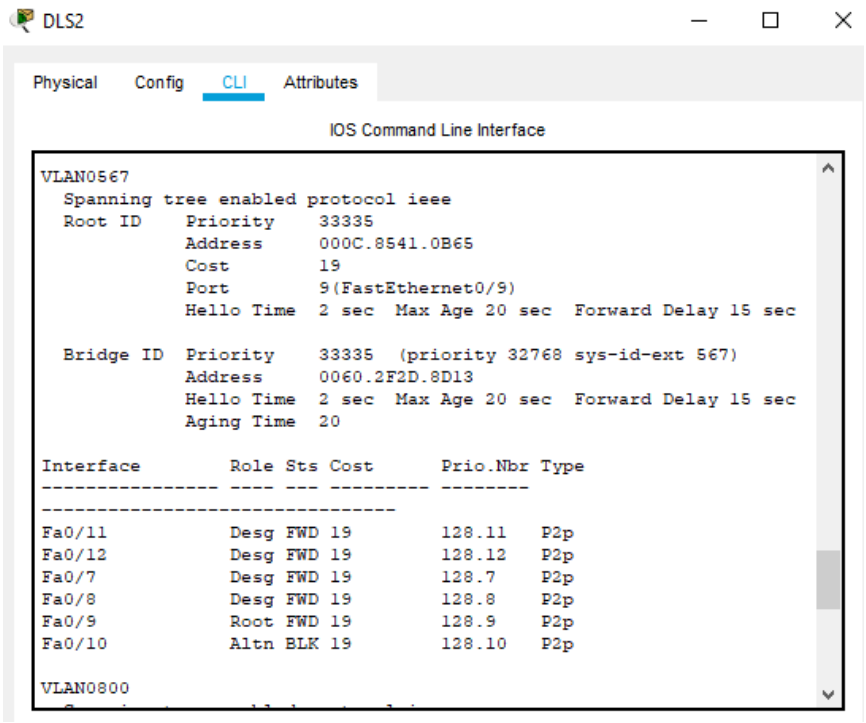

Figura 31 Verificación de la configuración spanning tree de la vlan 567 en DLS2

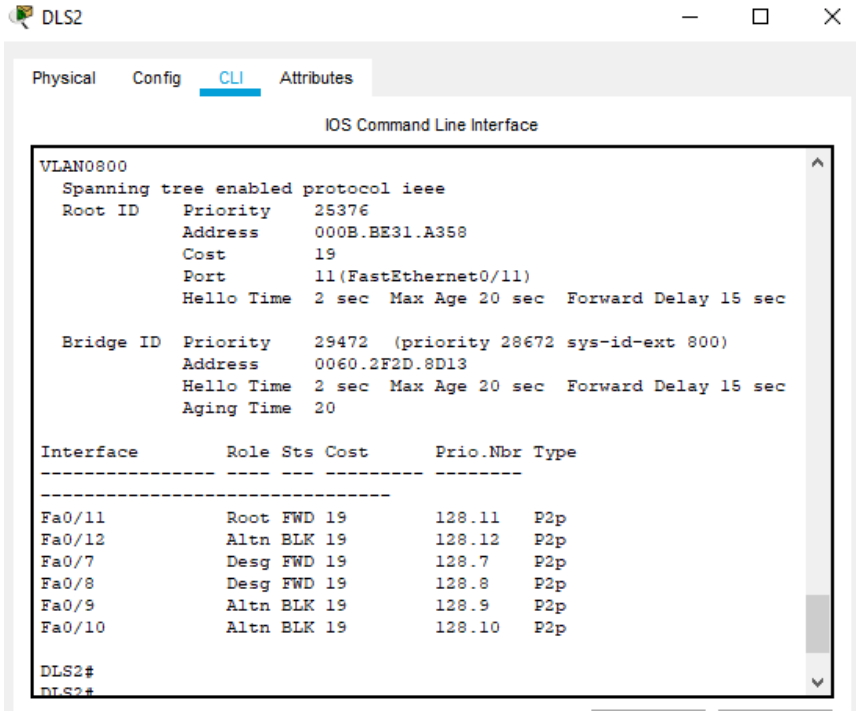

Figura 32 Verificación de la configuración spanning tree de la vlan 800 en DLS2

CONCLUSIONES

Las configuraciones basicas realizadas en los router y en los switch, permiten que la conexión sea más optima y que además tengamos seguridad de acceso en las diferentes formas para configurar los dispositivos, unas de las formas para acceder a las configuraciones, puede ser vía telnet o a través de la consola por lo que es importante en los dispositivos inicialmente establecer contraseñas y encriptarlas para mayor seguridad.

El procedimiento realizado en el primer escenario, donde se administró una red que conectaba a tres grandes ciudades, permitió concluir que el protocolo OSPF, es bastante manipulado para el control de redes robustas por su facilidad de encaminar la información rápidamente, pero también se observó que el protocolo EIGRP, es mejor para implementar en las redes, ya que su configuración es más sencilla de realizar que la del protocolo OSPF, asimismo estos son protocolos que permiten gestionar de manera segura y eficiente la información que se maneja en las empresas.

A partir de las verificaciones se evidenció los enrutamientos que se realizaron en cada uno de los router por medio del comando show ip route y además este nos permite verificar que las direcciones IP que se asignaron a los puertos seriales estén correctas y al hacer ping en cada uno de los router, se prestó atención a qué el porcentaje de conexión es cien por ciento, por lo tanto, hay una buena comunicación entre ellos.

Por otro lado, en el segundo escenario se manejaron las VLAN que son redes de área local virtuales en la configuración global del switch, las cuales son bastante útiles al momento de proteger una red de comunicaciones, además se usó, el protocolo spanning tree, que permite garantizar que no se creen loops cuando se tengan trayectorias redundantes en la red, ya que estos son peligrosos para las redes y por medio del comando show spanning conseguimos comprobar que estaban bien configuradas las vlan en DLS1 o DLS2.

Se pudo observar mediante el desarrollo de los escenarios acá propuestos, que se encuentran orientados al ámbito profesional, analizando las ventajas que se tiene al aplicar los protocolos de seguridad en las redes por medio del software Cisco Packet Tracer, este programa permitió desarrollar y comprender los escenarios propuestos dando soluciones basadas en enrutamiento avanzado y siendo esta la mejor manera de compartir la información en las industrias de la actualidad.

BIBLIOGRAFIA

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

Reyes, G. (2019). Fundamentos de BGP - Sea CCNA. Retrieved 2 August 2019, from https://www.seaccna.com/fundamentos-de-bgp/

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

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

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-NT1IlnMfy2rhPZHwEoWx

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

REFERENCIAS

[1] WIKIPEDIA. (s.f.). *ADSL*. Recuperado de https://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital_asim%C3%A9trica

[2] THEFREEDICTIONARY. DTP. Recuperado de https://es.thefreedictionary.com/DTP

[3]RED PROYDESA. EIGRP. Recuperado de https://www.proydesa.org/portal/index.php/noticias/1764-que-es-y-como-funciona-el-protocolo-eigrp-2

[4] WIKIPEDIA. (s.f.). ETHERNET. Recuperado de https://es.wikipedia.org/wiki/Ethernet

[5] WIKIPEDIA (s.f). Recuperado de LAN https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

[6] CISCO. OSPF. Recuperado de https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

[7] WIKIPEDIA (s.f). PROTOCOLOS DE RED. Recuperado de https://es.wikipedia.org/wiki/Anexo:Protocolos_de_red#:~:text=Un%20protocolo%20de%20red%20designa,de%20una%20red%20de%20computadoras.

[8] WIKIPEDIA (s.f). ROUTER. Recuperado de https://es.wikipedia.org/wiki/Router#:~:text=Un%20r%C3%BAter%2C%E2%80%8B%20enrutador%2C%E2%80%8B,dentro%20de%20una%20red%20inform%C3%A1tica.

[9] WIKIPEDIA. (s.f.). Servidor. Recuperado de https://es.wikipedia.org/wiki/Servidor#cite_note-1

[10] REDES TELEMATICAS. SWITCH. Recuperado de http://redestelematicas.com/el-switchcomofuncionaysusprincipalescaracteristicas/#:~:text=Un%20switch%20o%20conmutador%20es,(o%20t%C3%A9cnicamente%20IEEE%20802.3).&text=Los%20switches%20realizan%20esta%20funci%C3%B3n%20para%20medios%20cableados.

[11] WIKIPEDIA. (s.f.). *VLAN*. Recuperado de http://redestelematicas.com/

[12] CISCO. VTP. Recuperado de https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html

[13] WIKIPEDIA. (s.f). WAN. Recuperado de https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia