

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

CAMILO ANDRÉS PÉREZ

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

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

CAMILO ANDRÉS PÉREZ

**Diplomado de opción de grado presentado para optar el
título de INGENIERO ELECTRONICO**

DIRECTOR:

MSc. GERARDO GRANADOS ACUÑA

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

NEIVA - HUILA

2020

NOTA DE ACEPTACIÓN

Presidente del jurado

Jurado

Neiva, 30 de noviembre de 2020

CONTENIDO

GLOSARIO	7
RESUMEN.....	9
Palabras claves:	9
ABSTRACT.....	9
Keywords:	9
INTRODUCCIÓN	10
DESARROLLO DE LA ACTIVIDAD	11
Primer Escenario	11
Segundo Escenario	23
CONCLUSIONES	43
REFERENCIAS BIBLIOGRÁFICAS.....	44

LISTA DE TABLAS

Tabla 1. Interfaces Loopback R1	17
Tabla 2. Interfaces Loopback R5	18
Tabla 3. Esquema de VLAN	29
Tabla 4. Ajuste de VLAN	30
Tabla 5. Asignación de interfaces a las VLAN	33

LISTA DE FIGURAS

Fig. 1. Topología escenario 1.....	11
Fig. 2. Esquema inicial pka.....	12
Fig. 3. Verificación de conexión.....	16
Fig. 4. Show ip route R3	19
Fig. 5. Tabla de enrutamiento R1	21
Fig. 6. Tabla de enrutamiento R5	22
Fig. 7. Esquema escenario 2	23
Fig. 8. Escenario 2 en Packet Tracer.....	23
Fig. 9. Verificación de vlan en DLS1	35
Fig. 10. Verificación de vlan en DLS2	36
Fig. 11. Verificación de vlan en ALS1	37
Fig. 12. Verificación de vlan en ALS2	38
Fig. 13. Verificación de EtherChannel entre DLS1 y ALS1 (Parte 1)	39
Fig. 14. Verificación de EtherChannel entre DLS1 y ALS1 (Parte 2)	40
Fig. 15. Verificación de spanning tree en DLS1.....	41
Fig. 16. Verificación de spanning tree en DLS2.....	42

GLOSARIO

BGP: (Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

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.

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.

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.

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.

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.

RESUMEN

El presente documento muestra el desarrollo del documento final de prácticas del diplomado de profundización CISCO, en el se contemplan dos escenarios que involucran prácticas de enrutamiento avanzado, con protocolos como OSPF, EIGRP, VTP, entre otros, que permiten poner en practica todo lo visto a lo largo de dicho diplomado.

Con el desarrollo de estos ejercicios también se demuestra a nivel general el manejo de las herramientas trabajadas en el curso como lo son PACKET TRACER y GNS3. En cada uno de los escenarios se muestran las soluciones paso a paso, con la ayuda de imágenes que permiten ver la programación de los equipos y comprobar su adecuada conexión y configuración.

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

ABSTRACT

This document shows the development of the final document of the CISCO in-depth training practices, in which two scenarios are contemplated that involve advanced routing practices, with protocols such as OSPF, EIGRP, VTP, among others, that allow putting everything seen into practice throughout the course.

With the development of these exercises, the management of the tools worked in the course such as PACKET TRACER and GNS3 is also demonstrated at a general level. In each one of the scenarios, the solutions are shown step by step, with the help of images that allow to see the programming of the equipment and to verify its adequate connection and configuration.

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

INTRODUCCIÓN

Este trabajo es realizado con el fin de cumplir las Pruebas de Habilidades prácticas implementada como parte de las actividades evaluativas del Diplomado de Profundización CCNP, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se requiere que los estudiantes para el desarrollo de las actividades planteadas, apliquen el contenido de las temáticas abordadas a lo largo del curso, correspondientes a Protocolos de Enrutamiento Avanzado, Implementación de soluciones soportadas en enrutamiento avanzado, configuración de sistemas de red soportados en VLANs, y Administración, Seguridad y Escalabilidad en redes conmutadas.

En el escenario 1, se abordan temas como: protocolos de enrutamiento entre áreas de OSPF y EIGRP y la distribución de rutas entre ambos protocolos. En el escenario 2: VTP, spanning tree, direccionamiento IP, etherchannels, VLANs, entre otros.

DESARROLLO DE LA ACTIVIDAD

Primer Escenario

Teniendo en la cuenta la siguiente imagen:

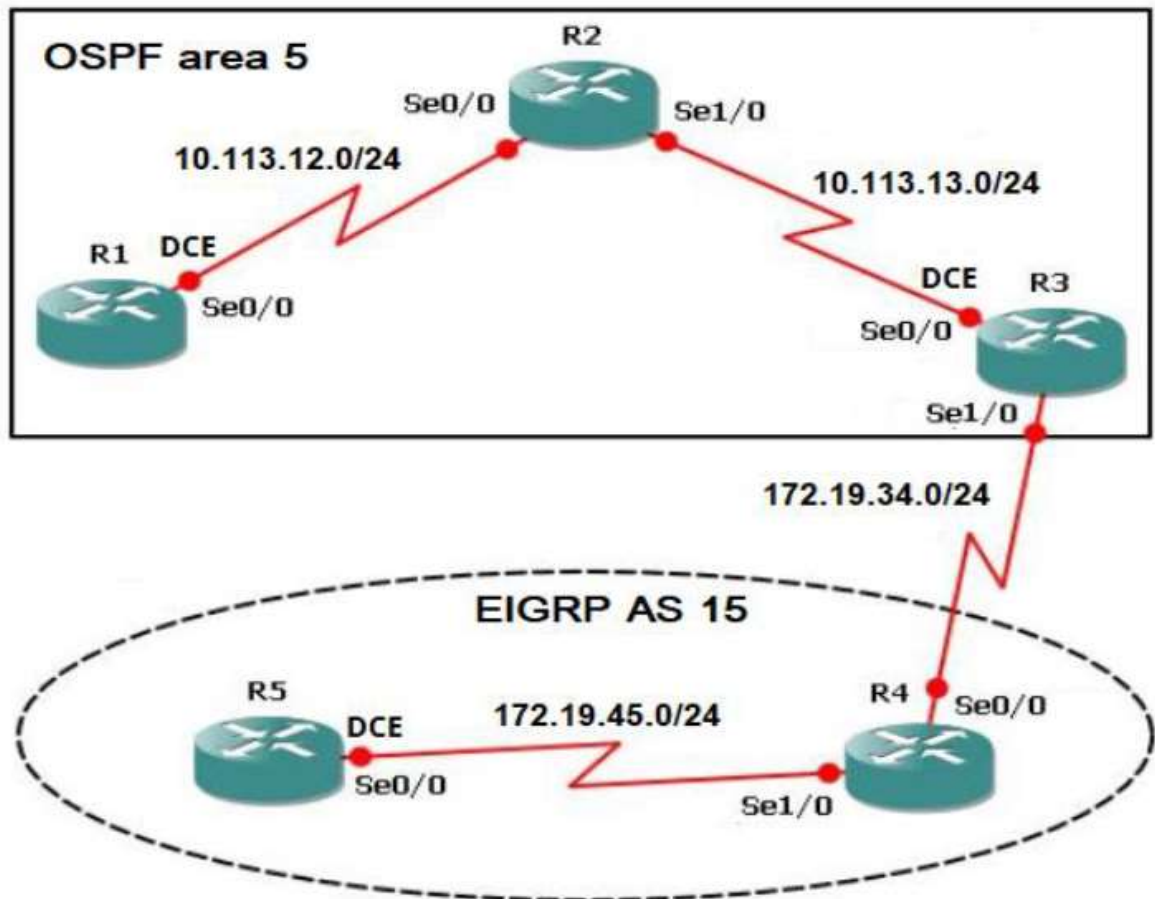


Fig. 1. Topología escenario 1

1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Se realiza el esquema:

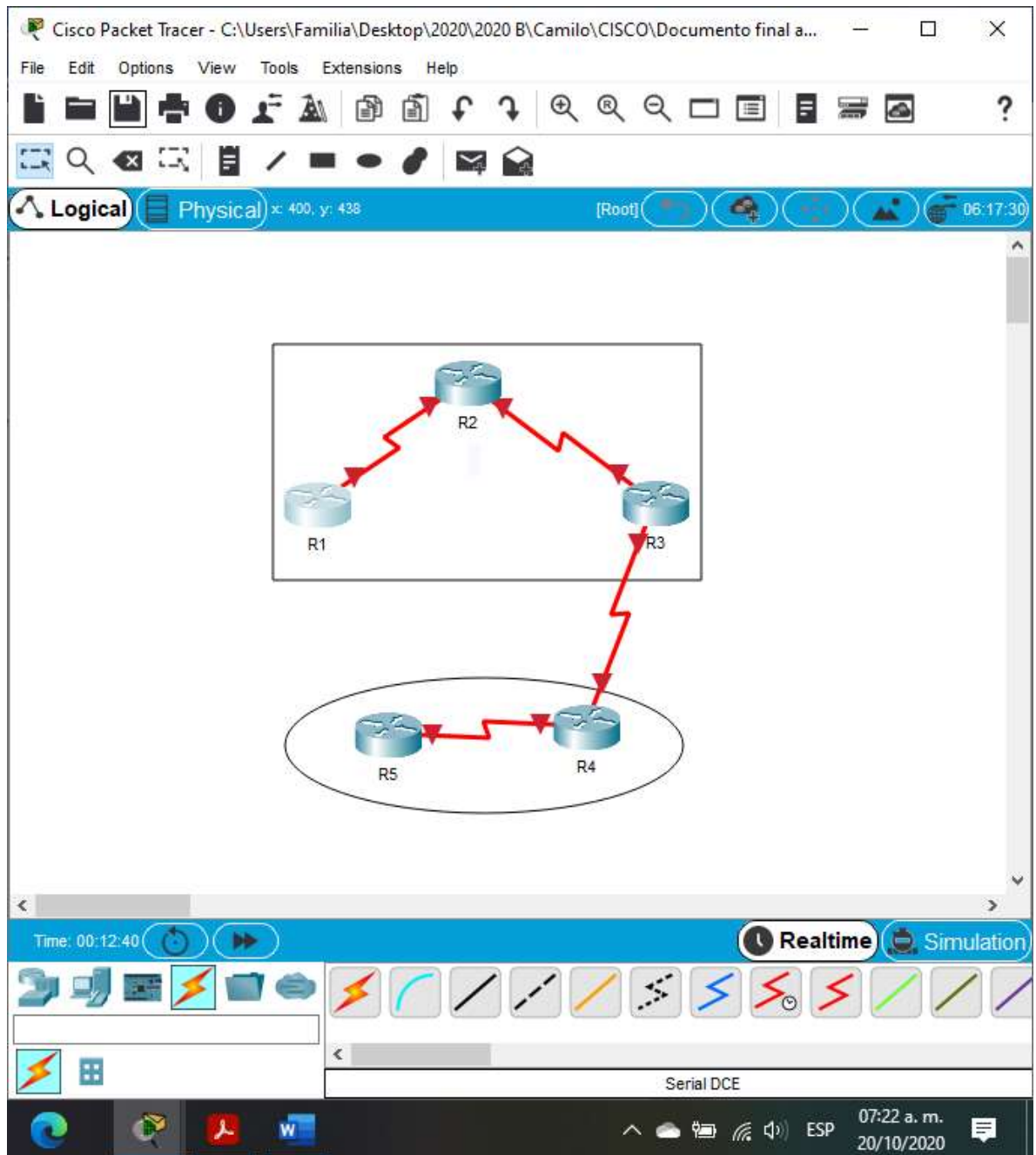


Fig. 2. Esquema inicial pka

Se realiza la configuración de interfaces en cada router según las direcciones de red dadas en el esquema:

Para R1:

Router>	
Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#hostname R1	Asignación de nombre al router
R1(config)#int s0/0/0	Ingreso a la interfaz s0/0/0
R1(config-if)#bandwidth 128000	Asignación de ancho de banda
R1(config-if)#ip address 10.113.12.1 255.255.255.0	Asignación de la dirección IP
R1(config-if)#clock rate 64000	Asignación de reloj
R1(config-if)#no sh	Activación de la interfaz
R1(config-if)#exit	Salida de la interfaz s0/0/0
R1(config)#router ospf 1	Ingreso para configurar el protocolo OSPF en el router
R1(config-router)#network 10.113.12.0 0.0.0.255 area 5	Asignación de la red
R1(config-router)#exit	Salida de la configuración OSPF

Para R2:

Router>	
Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#hostname R2	Asignación de nombre al router
R2(config)#int s0/0/0	Ingreso a la interfaz s0/0/0
R2(config-if)#ip address 10.113.12.2 255.255.255.0	Asignación de la dirección IP
R2(config-if)#no sh	Activación de la interfaz
R2(config-if)#exit	Salida de la interfaz s0/0/0
R2(config)#int s0/0/1	Ingreso a la interfaz s0/0/1
R2(config-if)#ip address 10.113.13.1 255.255.255.0	Asignación de la dirección IP
R2(config-if)#clock rate 64000	Asignación de reloj

R2(config-if)#no sh	Activación de la interfaz
R2(config-if)#exit	Salida de la interfaz s0/0/1
R2(config)#router ospf 1	Ingreso para configurar el protocolo OSPF en el router
R2(config-router)#network 10.113.12.0 0.0.0.255 area 5	Asignación de la red
R2(config-router)#network 10.113.13.0 0.0.0.255 area 5	Asignación de la red
R2(config-router)#exit	Salida de la configuración OSPF

Para R3:

Router>	
Router>enable	Ingreso a modo privilegiado
Router#configure terminal	Ingreso a modo de configuración
Router(config)#hostname R3	Asignación de nombre al router
R3(config)#int s0/0/0	Ingreso a la interfaz s0/0/0
R3(config-if)#ip address 10.113.13.2 255.255.255.0	Asignación de la dirección IP
R3(config-if)#no sh	Activación de la interfaz
R3(config-if)#exit	Salida de la interfaz s0/0/0
R3(config)#int s0/0/1	Ingreso a la interfaz s0/0/1
R3(config-if)#bandwidth 128000	Asignación de ancho de banda
R3(config-if)#ip address 172.19.34.1 255.255.255.0	Asignación de la dirección IP
R3(config-if)#clock rate 64000	Asignación de reloj
R3(config-if)#no sh	Activación de la interfaz
R3(config-if)#exit	Salida de la interfaz s0/0/1
R3(config)#router ospf 1	Ingreso para configurar el protocolo OSPF en el router
R3(config-router)#network 10.113.13.0 0.0.0.255 area 5	Asignación de la red
R3(config-router)#exit	Salida de la configuración OSPF
R3(config)#router eigrp 15	Ingreso para configurar el protocolo EIGRP en el router
R3(config-router)#network 172.19.34.0 0.0.0.255	Asignación de la red

R3(config-router)#exit

Salida de la configuración OSPF

Para R4:

Router>

Router>enable

Ingreso a modo privilegiado

Router#configure terminal

Ingreso a modo de configuración

Router(config)#hostname R4

Asignación de nombre al router

R4(config)#int s0/0/0

Ingreso a la interfaz s0/0/0

R4(config-if)#ip address 172.19.34.2 255.255.255.0

Asignación de la dirección IP

R4(config-if)#no sh

Activación de la interfaz

R4(config-if)#exit

Salida de la interfaz s0/0/0

R4(config)#int s0/0/1

Ingreso a la interfaz s0/0/1

R4(config-if)#bandwidth 128000

Asignación de ancho de banda

R4(config-if)#ip address 172.19.45.1 255.255.255.0

Asignación de la dirección IP

R4(config-if)#clock rate 64000

Asignación de reloj

R4(config-if)#no sh

Activación de la interfaz

R4(config-if)#exit

Salida de la interfaz s0/0/0

R4(config)#router eigrp 15

Ingreso para configurar el protocolo EIGRP en el router

R4(config-router)#network 172.19.45.0 0.0.0.255

Asignación de la red

R4(config-router)#exit

Salida de la configuración OSPF

Para R5:

Router>

Router>enable

Ingreso a modo privilegiado

Router#configure terminal

Ingreso a modo de configuración

Router(config)#hostname R5

Asignación de nombre al router

R5(config)#int s0/0/0

Ingreso a la interfaz s0/0/0

R5(config-if)#ip address 172.19.45.2 255.255.255.0	Asignación de la dirección IP
R5(config-if)#no sh	Activación de la interfaz
R5(config-if)#exit	Salida de la interfaz s0/0/0
R5(config)#router eigrp 15	Ingreso para configurar el protocolo EIGRP en el router
R5(config-router)#network 172.19.45.0 0.0.0.255	Asignación de la red
R5(config-router)#exit	Salida de la configuración OSPF

Se puede observar que las conexiones establecidas son correctas a través de los triángulos verdes que se muestran en los extremos de los cables.

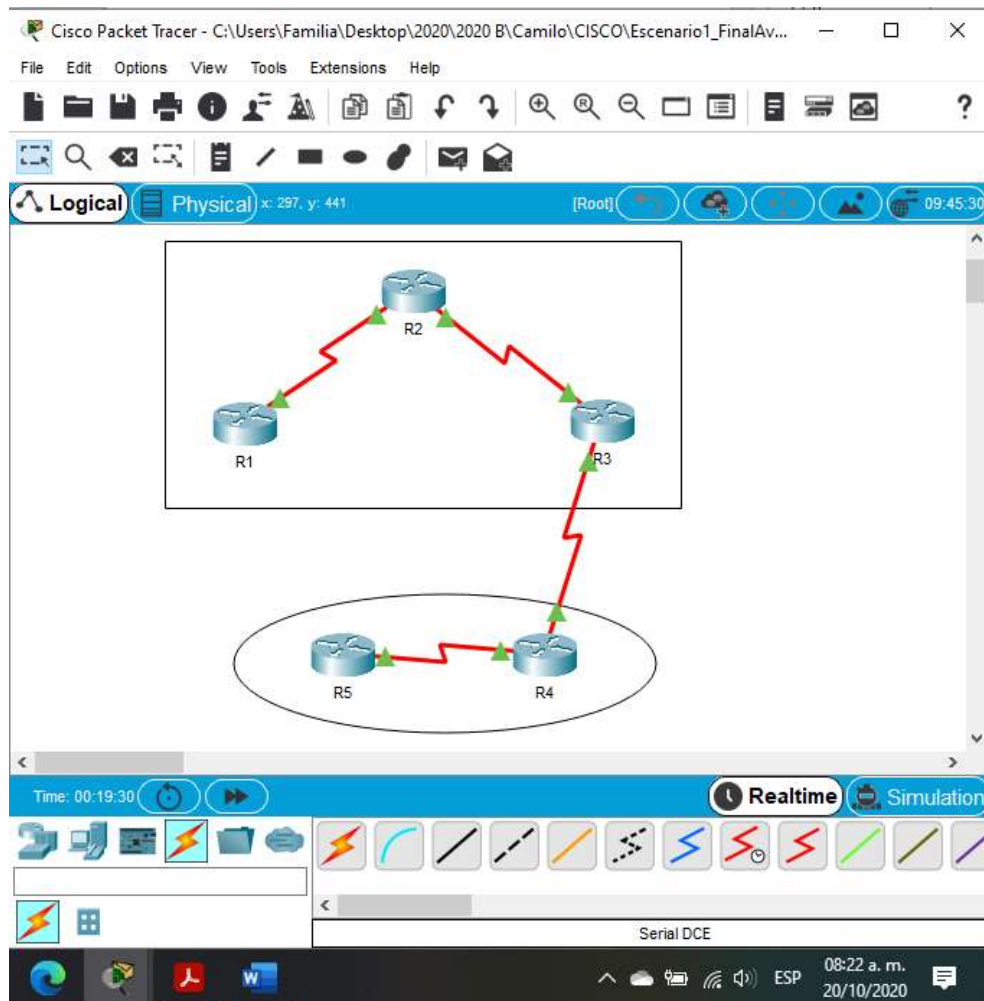


Fig. 3. Verificación de conexión

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

Tabla 2. Interfaces Loopback R5

Red	Rango Host	Broadcast
172.5.0.0/22	172.5.0.1 – 172.5.0.254	172.5.0.255
172.5.4.0/22	172.5.4.1 – 172.5.4.254	172.5.4.255
172.5.8.0/22	172.5.8.1 – 172.5.8.254	172.5.8.255
172.5.12.0/22	172.5.12.1 – 172.5.12.254	172.5.12.255

```

R5(config)#int Lo10                               Ingreso a la interfaz Loopback 10
R5(config-if)#ip address 172.5.0.1 255.255.252.0  Asignación de la dirección IP
R5(config-if)#no sh                               Activación de la interfaz
R5(config)#int Lo20                               Ingreso a la interfaz Loopback 20
R5(config-if)#ip address 172.5.4.1 255.255.252.0  Asignación de la dirección IP
R5(config-if)#no sh                               Activación de la interfaz
R5(config)#int Lo30                               Ingreso a la interfaz Loopback 30
R5(config-if)#ip address 172.5.8.1 255.255.252.0  Asignación de la dirección IP
R5(config-if)#no sh                               Activación de la interfaz
R5(config)#int Lo40                               Ingreso a la interfaz Loopback 40
R5(config-if)#ip address 172.5.12.1 255.255.252.0  Asignación de la dirección IP
R5(config-if)#no sh                               Activación de la interfaz
R5(config-if)#exit                                Salida de la interfaz Loopback 40
R5(config)#router eigrp 15                        Ingreso para configurar el protocolo EIGRP en el router
R5(config-router)#network 172.5.0.0 255.255.252.0  Asignación de la red
R5(config-router)#network 172.5.4.0 255.255.252.0  Asignación de la red
R5(config-router)#network 172.5.8.0 255.255.252.0  Asignación de la red
R5(config-router)#network 172.5.12.0 255.255.252.0  Asignación de la red

```

R5(config-router)#exit

Salida de la configuración EIGRP

4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando show ip route.

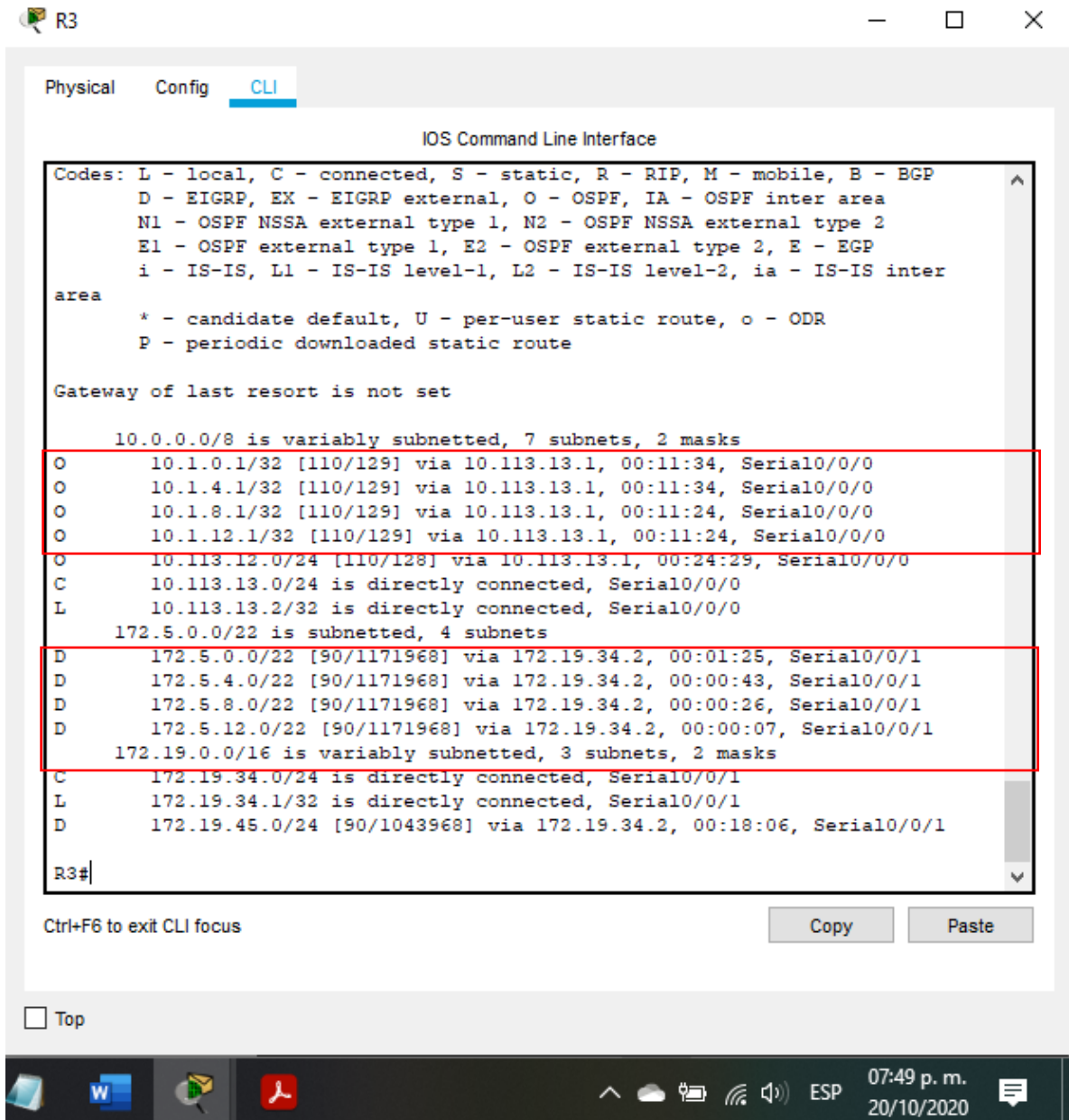


Fig. 4. Show ip route R3

R3 si aprendió las rutas de los Loopbacks de R1 y R5 como se ve en las regiones subrayadas.

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

R3#configure terminal	Ingreso a modo de configuración
R3(config)#router ospf 1	Ingreso para configurar el protocolo OSPF en el router
R3(config-router)#redistribute eigrp 15 metric 50000 subnets	Redistribución de rutas EIGRP
R3(config-router)#exit	Salida de la configuración OSPF
R3(config)#router eigrp 15	Ingreso para configurar el protocolo EIGRP en el router
R3(config-router)#redistribute ospf 1 metric 1544 20000 255 1 1500	Redistribución de rutas OSPF
R3(config-router)#exit	Salida de la configuración OSPF

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

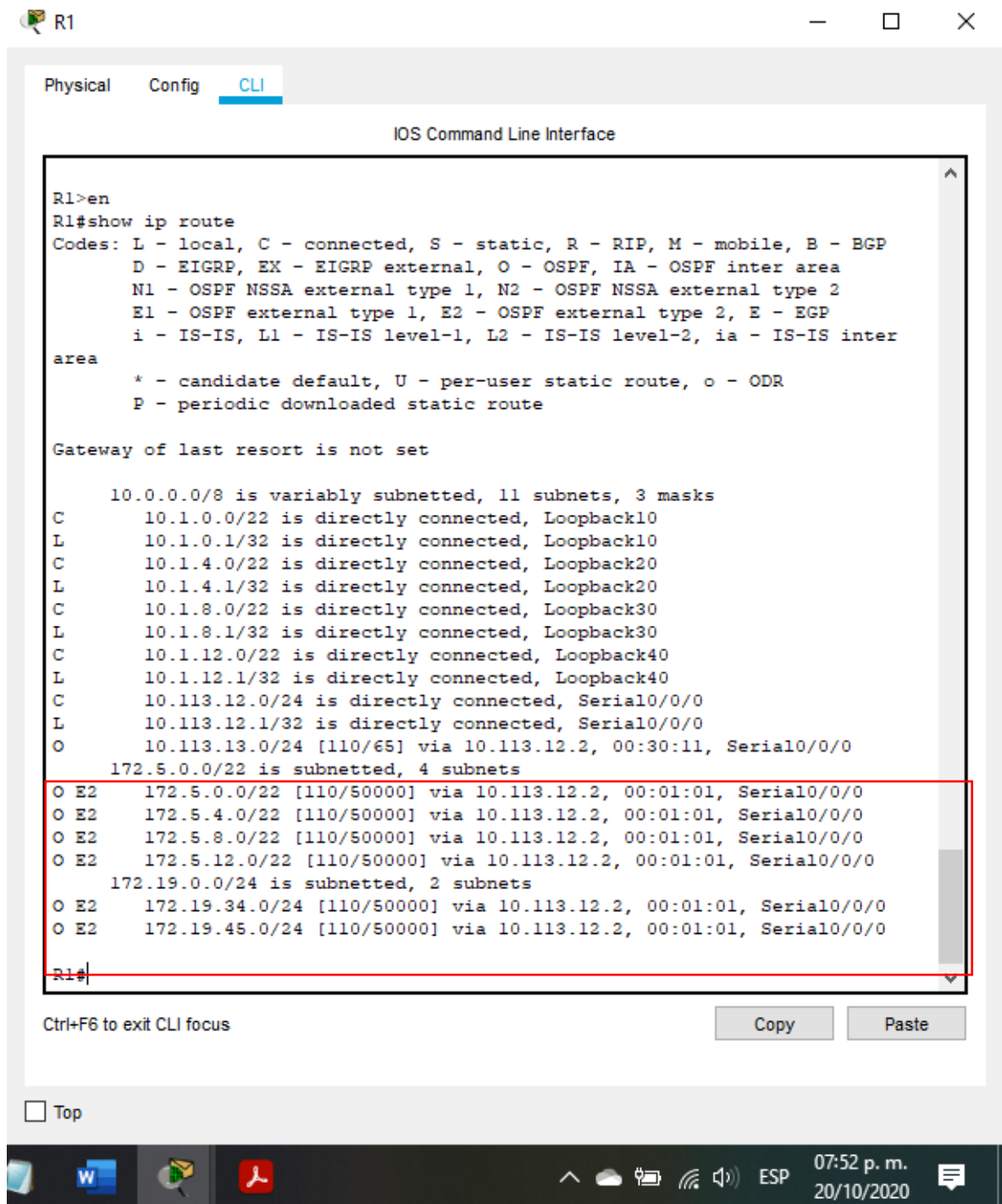


Fig. 5. Tabla de enrutamiento R1

```

R5#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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D EX  10.1.0.1/32 [170/7801856] via 172.19.45.1, 00:01:20, Serial0/0/0
D EX  10.1.4.1/32 [170/7801856] via 172.19.45.1, 00:01:20, Serial0/0/0
D EX  10.1.8.1/32 [170/7801856] via 172.19.45.1, 00:01:20, Serial0/0/0
D EX  10.1.12.1/32 [170/7801856] via 172.19.45.1, 00:01:20, Serial0/0/0
D EX  10.113.12.0/24 [170/7801856] via 172.19.45.1, 00:01:20, Serial0/0/0
D EX  10.113.13.0/24 [170/7801856] via 172.19.45.1, 00:01:20, Serial0/0/0
    172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C     172.5.0.0/22 is directly connected, Loopback10
L     172.5.0.1/32 is directly connected, Loopback10
C     172.5.4.0/22 is directly connected, Loopback20
L     172.5.4.1/32 is directly connected, Loopback20
C     172.5.8.0/22 is directly connected, Loopback30
L     172.5.8.1/32 is directly connected, Loopback30
C     172.5.12.0/22 is directly connected, Loopback40
L     172.5.12.1/32 is directly connected, Loopback40
    172.19.0.0/16 is variably subnetted, 3 subnets, 2 masks
D     172.19.34.0/24 [90/2681856] via 172.19.45.1, 00:21:34, Serial0/0/0
C     172.19.45.0/24 is directly connected, Serial0/0/0
L     172.19.45.2/32 is directly connected, Serial0/0/0

R5#

```

Fig. 6. Tabla de enrutamiento R5

Como se observa las rutas de R5 aparecen en la tabla de enrutamiento de R1 y las de R1 aparecen en la tabla de enrutamiento de R5.

Segundo Escenario

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

Topología de red

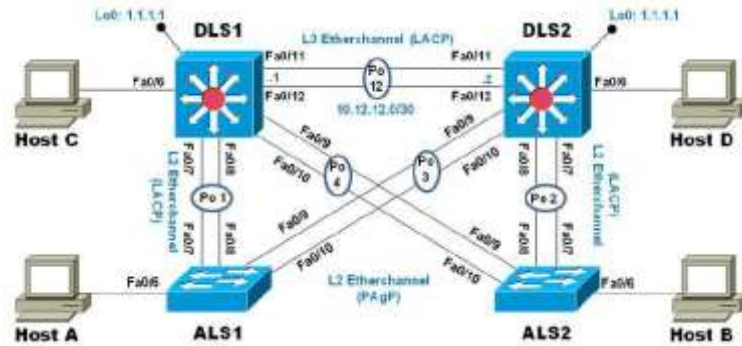


Fig. 7. Esquema escenario 2

La implementación en Packet Tracer es:

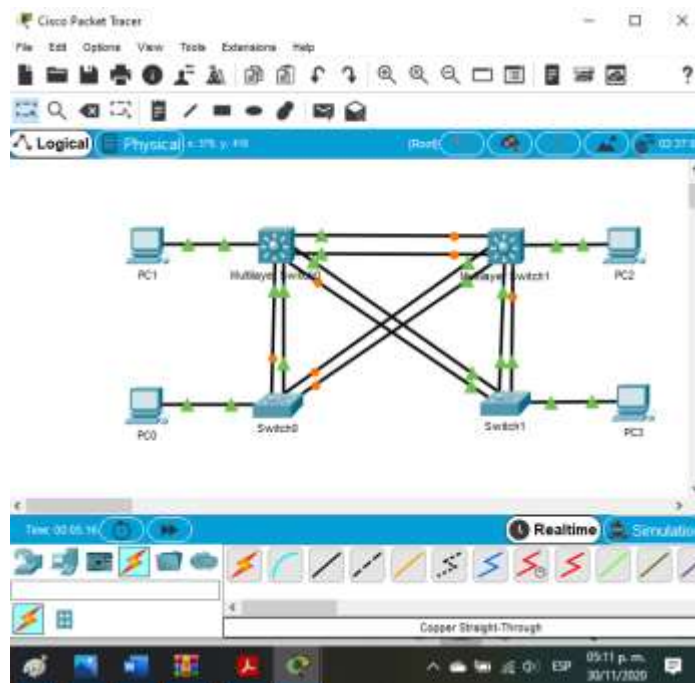


Fig. 8. Escenario 2 en Packet Tracer

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

- a. Apagar todas las interfaces en cada switch.

Switch>

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#int ran f0/1-24, g0/1-2	Ingreso a todas las interfaces del Switch
Switch(config-if-range)#sh	Desactivación de las interfaces

Nota: Se repite este proceso en los 4 Switchs

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

Para DLS1:

Switch>

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname DLS1	Asignación de nombre al Switch
DLS1(config)#	

Para DLS2:

Switch>

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname DLS2	Asignación de nombre al Switch
DLS2(config)#	

Para ALS1:

Switch>

Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname ALS1	Asignación de nombre al Switch
ALS1(config)#	

Para ALS2:

Switch>	
Switch>enable	Ingreso a modo privilegiado
Switch#configure terminal	Ingreso a modo de configuración
Switch(config)#hostname ALS2	Asignación de nombre al Switch
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.
- 2) Los Port-channels en las interfaces Fa0/7 y Fa0/8 utilizarán LACP.
- 3) Los Port-channels en las interfaces F0/9 y fa0/10 utilizará PAgP.
- 4) Todos los puertos troncales serán asignados a la VLAN 500 como la VLAN nativa.

Para DLS1:

DLS1(config)#int port-channel 12	Ingreso al Port-Channel 12
DLS1(config-if)#ip address 10.12.12.1 255.255.255.252	Asignación de dirección Ip
DLS1(config-if)#exit	Salida del Port-Chacel 12
DLS1(config)#int ran f0/7-10	Ingreso al rango de interfaces f0/7-10
DLS1(config-if-range)# switchport trunk encapsulation dot1q	Configuración de las troncales
DLS1(config-if-range)# switchport trunk native vlan 500	Establece la vlan como nativa
DLS1(config-if-range)# switchport mode trunk	

DLS1(config-if-range)# switchport nonnegotiate	
DLS1(config-if-range)# no sh	Activa la configuración realizada
DLS1(config-if-range)# exit	Salida del rango f0/7-10
DLS1(config)#int ran f0/7-8	Ingreso al rango de interfaces f0/7-8
DLS1(config-if-range)# channel-group 1 mode active	Activa en el rango el modo active
DLS1(config-if-range)# exit	Salida del rango f0/7-8
DLS1(config)#int ran f0/9-10	Ingreso al rango de interfaces f0/7-8
DLS1(config-if-range)# channel-group 4 mode desirable	Activa en el rango el modo desirable
DLS1(config-if-range)# exit	Salida del rango f0/9-10

Para DLS2:

DLS2(config)#int port-channel 12	Ingreso al Port-Channel 12
DLS2(config-if)#ip address 10.12.12.2 255.255.255.252	Asignación de dirección Ip
DLS2(config-if)#exit	Salida del Port-Channel 12
DLS2(config)#int ran f0/7-10	Ingreso al rango de interfaces f0/7-10
DLS2(config-if-range)# switchport trunk encapsulation dot1q	Configuraripon de las troncales
DLS2(config-if-range)# switchport trunk native vlan 500	Establece la vlan como nativa
DLS2(config-if-range)# switchport mode trunk	
DLS2(config-if-range)# switchport nonnegotiate	
DLS2(config-if-range)# no sh	Activa la configuración realizada
DLS2(config-if-range)# exit	Salida del rango f0/7-10
DLS2(config)#int ran f0/7-8	Ingreso al rango de interfaces f0/7-8
DLS2(config-if-range)# channel-group 2 mode active	Activa en el rango el modo active
DLS2(config-if-range)# exit	Salida del rango f0/7-8
DLS2(config)#int ran f0/9-10	Ingreso al rango de interfaces f0/7-8
DLS2(config-if-range)# channel-group 3 mode desirable	Activa en el rango el modo desirable
DLS2(config-if-range)# exit	

DLS2(config-if-range)# exit Salida del rango f0/9-10

Para ALS1:

ALS1(config)#int ran f0/7-10 Ingreso al rango de interfaces f0/7-10
ALS1(config-if-range)# switchport trunk native vlan 500 Establece la vlan como nativa
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)# switchport nonnegotiate
ALS1(config-if-range)# no sh Activa la configuración realizada
ALS1(config-if-range)# exit Salida del rango f0/7-10
ALS1(config)#int ran f0/7-8 Ingreso al rango de interfaces f0/7-8
ALS1(config-if-range)# channel-group 1 mode active Activa en el rango el modo active
ALS1(config-if-range)# exit Salida del rango f0/7-8
ALS1(config)#int ran f0/9-10 Ingreso al rango de interfaces f0/7-8
ALS1(config-if-range)# channel-group 4 mode desirable Activa en el rango el modo desirable
ALS1(config-if-range)# exit Salida del rango f0/9-10

Para ALS2

ALS2(config)#int ran f0/7-10 Ingreso al rango de interfaces f0/7-10
ALS2(config-if-range)# switchport trunk native vlan 500 Establece la vlan como nativa
ALS2(config-if-range)# switchport mode trunk
ALS2(config-if-range)# switchport nonnegotiate
ALS2(config-if-range)# no sh Activa la configuración realizada
ALS2(config-if-range)# exit Salida del rango f0/7-10
ALS2(config)#int ran f0/7-8 Ingreso al rango de interfaces f0/7-8
ALS2(config-if-range)# channel-group 2 mode active Activa en el rango el modo active
ALS2(config-if-range)# exit Salida del rango f0/7-8
ALS2(config)#int ran f0/9-10 Ingreso al rango de interfaces f0/7-8

ALS2(config-if-range)# channel-group 3 mode desirable Activa en el rango el modo
desirable

ALS2(config-if-range)# exit Salida del rango f0/9-10

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

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

2) Configurar DLS1 como servidor principal para las VLAN.

3) Configurar ALS1 y ALS2 como clientes VTP.

Para DLS1:

DLS1(config)#vtp domain CISCO Establecimiento del nombre de dominio

DLS1(config)#vtp ver 3 Establecimiento de la versión de vtp

DLS1(config)#vtp password ccnp321 Establecimiento de la contraseña

DLS1(config)#vtp primary vlan Establecimiento de DLS1 como servidor principal

Para ALS1:

ALS1(config)#vtp ver 3 Establecimiento de la versión de vtp

ALS1(config)#vtp mode client mst Establecimiento de ALS1 como cliente

Para ALS2:

ALS2(config)#vtp ver 3 Establecimiento de la versión de vtp

ALS2(config)#vtp mode client mst Establecimiento de ALS1 como cliente

Nota: A pesar de que intenté con diversas versiones de Cisco Packet Tracer, ninguna de ellas me permitió configurar el vtp versión 3 y por lo tanto tampoco se puede implementar DLS como servidor principal.

e. Configurar en el servidor principal las siguientes VLAN:

Tabla 3. Esquema de VLAN

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

DLS1(config)#vlan 500 Ingreso a la vlan 500
DLS1(config-vlan)#name NATIVA Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 500
DLS1(config)#vlan 434 Ingreso a la vlan 434
DLS1(config-vlan)#name PROVEEDORES Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 434
DLS1(config)#vlan 12 Ingreso a la vlan 12
DLS1(config-vlan)#name ADMON Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 12
DLS1(config)#vlan 234 Ingreso a la vlan 234
DLS1(config-vlan)#name CLIENTES Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 234
DLS1(config)#vlan 111 Ingreso a la vlan 111
DLS1(config-vlan)#name MULTIMEDIA Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 111
DLS1(config)#vlan 123 Ingreso a la vlan 123
DLS1(config-vlan)#name SEGUROS Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 123
DLS1(config)#vlan 101 Ingreso a la vlan 101
DLS1(config-vlan)#name VENTAS Asignación de nombre

DLS1(config-vlan)#exit Salida de la vlan 101
DLS1(config)#vlan 345 Ingreso a la vlan 345
DLS1(config-vlan)#name PERSONAL Asignación de nombre
DLS1(config-vlan)#exit Salida de la vlan 345

Nota: Debido a que hay conflicto para vlan mayores de 1004, se ajustaron

Tabla 4. Ajuste de VLAN

MULTIMEDIA	111
VENTAS	101
PERSONAL	345

f. En DLS1, suspender la VLAN 434.

DLS1(config)#vlan 434 Ingreso a la vlan 434
DLS1(config-vlan)#state suspend Suspende la vlan
DLS1(config-vlan)#exit Salida de la vlan 434

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

DLS2(config)#vtp mode transparent Establece vtp transparente en DLS2
DLS2(config-vlan)#vtp ver 2 Establece vtp versión 2
DLS2(config)#vlan 500 Ingreso a la vlan 500
DLS2(config-vlan)#name NATIVA Asignación de nombre
DLS2(config-vlan)#exit Salida de la vlan 500
DLS2(config)#vlan 434 Ingreso a la vlan 434
DLS2(config-vlan)#name PROVEEDORES Asignación de nombre
DLS2(config-vlan)#exit Salida de la vlan 434
DLS2(config)#vlan 12 Ingreso a la vlan 12
DLS2(config-vlan)#name ADMON Asignación de nombre

DLS2(config-vlan)#exit	Salida de la vlan 12
DLS2(config)#vlan 234	Ingreso a la vlan 234
DLS2(config-vlan)#name CLIENTES	Asignación de nombre
DLS2(config-vlan)#exit	Salida de la vlan 234
DLS2(config)#vlan 111	Ingreso a la vlan 111
DLS2(config-vlan)#name MULTIMEDIA	Asignación de nombre
DLS2(config-vlan)#exit	Salida de la vlan 111
DLS2(config)#vlan 123	Ingreso a la vlan 123
DLS2(config-vlan)#name SEGUROS	Asignación de nombre
DLS2(config-vlan)#exit	Salida de la vlan 123
DLS2(config)#vlan 101	Ingreso a la vlan 101
DLS2(config-vlan)#name VENTAS	Asignación de nombre
DLS2(config-vlan)#exit	Salida de la vlan 101
DLS2(config)#vlan 345	Ingreso a la vlan 345
DLS2(config-vlan)#name PERSONAL	Asignación de nombre
DLS2(config-vlan)#exit	Salida de la vlan 345

h. Suspender VLAN 434 en DLS2.

DLS2(config)#vlan 434	Ingreso a la vlan 434
DLS2(config-vlan)#state suspend	Suspende la vlan
DLS2(config-vlan)#exit	Salida de la vlan 434

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

DLS2(config)#vlan 567	Ingreso a la vlan 567
DLS2(config-vlan)#name PRODUCCIÓN	Asignación de nombre

DLS2(config-vlan)#private-vlan isolated	Establece la vlan como privada
DLS2(config-vlan)#exit	Salida de la vlan 567

j. Configurar DLS1 como Spanning tree root para las VLAN 1, 12, 434, 500, 1010, 1111 y 3456 y como raíz secundaria para las VLAN 123 y 234.

DLS1(config)#spanning-tree vlan 1,12,101,11,345,434,500 root primary	Configura las vlan como raíz primaria
DLS1(config)#spanning-tree vlan 123,234 root secondary	Configura las vlan como raíz secundaria

k. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 500, 1010, 1111 y 3456.

DLS2(config)#spanning-tree vlan 123,234 root primary	Configura las vlan como raíz primaria
DLS2(config)#spanning-tree vlan 12,101,11,345,434,500 root secondary	Configura las vlan como raíz secundaria

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

Para DLS1:

DLS1(config)#int port-channel 1	Ingresa al port-channel 1
DLS1(config-if)#swi tru allowed vlan 12,101,111,123,234,345,500	Permite a las vlan escritas circular en dicho puerto
DLS1(config-if)#exit	Salida del port-channel 1
DLS1(config)#int port-channel 4	Ingresa al port-channel 4
DLS1(config-if)#swi tru allowed vlan 12,101,111,123,234,345,500	Permite a las vlan escritas circular en dicho puerto
DLS1(config-if)#exit	Salida del port-channel 4

Para DLS2:

DLS2(config)#int port-channel 2	Ingresa al port-channel 2
DLS2(config-if)#swi tru allowed vlan 12,101,111,123,234,345,500	Permite a las vlan escritas circular en dicho puerto
DLS2(config-if)#exit	Salida del port-channel 2
DLS2(config)#int port-channel 3	Ingresa al port-channel 3
DLS2(config-if)#swi tru allowed vlan 12,101,111,123,234,345,500	Permite a las vlan escritas circular en dicho puerto
DLS2(config-if)#exit	Salida del port-channel 3

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

Tabla 5. Asignación de interfaces a las 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		

Para DLS1:

DLS1(config)#int f0/6	Ingresa a la interfaz f0/6
DLS1(config-if)#swi access vlan 345	Establece el acceso de vlan 345 a f0/6
DLS1(config-if)#no sh	Activa la configuración realizada
DLS1(config-if)#exit	Salida de la interfaz f0/6
DLS1(config)#int f0/15	Ingresa a la interfaz f0/15
DLS1(config-if)#swi access vlan 111	Establece el acceso de vlan 111 a f0/15
DLS1(config-if)#no sh	Activa la configuración realizada
DLS1(config-if)#exit	Salida de la interfaz f0/15

Para DLS2:

DLS2(config)#int f0/6	Ingresa a la interfaz f0/6
DLS2(config-if)#swi access vlan 12	Establece el acceso de vlan 12 a f0/6
DLS2(config-if)#swi access vlan 101	Establece el acceso de vlan 101 a f0/6
DLS2(config-if)#no sh	Activa la configuración realizada
DLS2(config-if)#exit	Salida de la interfaz f0/6
DLS2(config)#int f0/15	Ingresa a la interfaz f0/15
DLS2(config-if)#swi access vlan 111	Establece el acceso de vlan 111 a f0/15
DLS2(config-if)#no sh	Activa la configuración realizada
DLS2(config-if)#exit	Salida de la interfaz f0/15
DLS2(config)#int f0/16-18	Ingresa a la interfaz f0/16-18
DLS2(config-if-range)#swi access vlan 567	Establece el acceso de vlan 567 a f0/16-18
DLS2(config-if)#no sh	Activa la configuración realizada
DLS2(config-if)#exit	Salida de la interfaz f0/16-18

Para ALS1:

ALS1(config)#int f0/6	Ingresa a la interfaz f0/6
ALS1(config-if)#swi access vlan 123	Establece el acceso de vlan 123 a f0/6
ALS1(config-if)#swi access vlan 101	Establece el acceso de vlan 101 a f0/6
ALS1(config-if)#no sh	Activa la configuración realizada
ALS1(config-if)#exit	Salida de la interfaz f0/6
ALS1(config)#int f0/15	Ingresa a la interfaz f0/15
ALS1(config-if)#swi access vlan 111	Establece el acceso de vlan 111 a f0/15
ALS1(config-if)#no sh	Activa la configuración realizada
ALS1(config-if)#exit	Salida de la interfaz f0/15

Para ALS2:

ALS2(config)#int f0/6	Ingresa a la interfaz f0/6
ALS2(config-if)#swi access vlan 234	Establece el acceso de vlan 234 a f0/6

ALS2(config-if)#no sh	Activa la configuración realizada
ALS2(config-if)#exit	Salida de la interfaz f0/6
ALS2(config)#int f0/15	Ingresa a la interfaz f0/15
ALS2(config-if)#swi access vlan 111	Establece el acceso de vlan 111 a f0/15
ALS2(config-if)#no sh	Activa la configuración realizada
ALS2(config-if)#exit	Salida de la interfaz f0/15

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 DLS 1

```

DLS1>en
DLS1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active   Po1, Po4, Fa0/1,
Fa0/2, Fa0/3, Fa0/4, Fa0/5,
Fa0/9, Fa0/10, Fa0/13,
Fa0/14, Fa0/16, Fa0/17, Fa0/18,
Fa0/19, Fa0/20, Fa0/21, Fa0/22,
Fa0/23, Fa0/24, Gig0/1, Gig0/2
12   ADMON                  active
101  VENTAS                 active
111  MULTIMEDIA            active   Fa0/15
123  SEGUROS               active
234  CLIENTES              active
345  PERSONAL              active   Fa0/6
434  PROVEEDORES          active
500  NATIVA                active
1002 fddi-default          active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default      active
DLS1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:19 p. m. 30/11/2020

Fig. 9. Verificación de vlan en DLS1

Para DLS2

```
DLS2>en
DLS2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po2, Po3, Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/13, Fa0/14, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
12	ADMON	active	
101	VENTAS	active	Fa0/6
111	MULTIMENDIA	active	Fa0/15
123	SEGUROS	active	
234	CLIENTES	active	
345	PERSONAL	active	
434	PROVEEDORES	active	
500	NATIVA	active	
567	PRODUCCION	active	Fa0/16, Fa0/17, Fa0/18
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

DLS2#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:20 p. m. 30/11/2020

Fig. 10. Verificación de vlan en DLS2

Para ALS1

```
ALS1#show vlan brief
```

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

ALS1#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:20 p. m.
30/11/2020

Fig. 11. Verificación de vlan en ALS1

Para ALS2

```
ALS2#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
12 ADMON	active	
101 VENTAS	active	
111 MULTIMEDIA	active	Fa0/15
123 SEGUROS	active	
234 CLIENTES	active	Fa0/6
345 PERSONAL	active	
434 PROVEEDORES	active	
500 NATIVA	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

ALS2#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:21 p. m. 30/11/2020

Fig. 12. Verificación de vlan en ALS2

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

```
DLS1#show interface port-channel 1
Port-channell is down, line protocol is down (disabled)
  Hardware is EtherChannel, address is 0060.2fd7.438c (bia
0060.2fd7.438c)
  MTU 1500 bytes, BW 300000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 300Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel: Fa0/7 ,Fa0/8 ,
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

DLS1#
DLS1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:23 p. m.
30/11/2020

Fig. 13. Verificación de EtherChannel entre DLS1 y ALS1 (Parte 1)

```
DLS1#show interface port-channel 4
Port-channel4 is down, line protocol is down (disabled)
  Hardware is EtherChannel, address is 00e0.a36c.b565 (bia
00e0.a36c.b565)
  MTU 1500 bytes, BW 300000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 300Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel:
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    956 packets input, 193351 bytes, 0 no buffer
    Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    2357 packets output, 263570 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

DLS1#
DLS1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:23 p. m.
30/11/2020

Fig. 14. Verificación de EtherChannel entre DLS1 y ALS1 (Parte 2)

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


```
DLS1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address    000C.85D3.1397
             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    000C.85D3.1397
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----
Fa0/8              Desg FWD 19        128.8   P2p
Fa0/7              Desg FWD 19        128.7   P2p

VLAN0012
  Spanning tree enabled protocol ieee
  Root ID    Priority    24588
             Address    000C.85D3.1397
             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    000C.85D3.1397
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

Interface          Role Sts Cost      Prio.Nbr Type
-----

```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:24 p. m. 30/11/2020

Fig. 15. Verificación de spanning tree en DLS1

Para DLS2

```
DLS2#show spanning-tree
VLAN0101
  Spanning tree enabled protocol ieee
  Root ID    Priority    28773
             Address    0040.0BC2.E7A7
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28773 (priority 28672 sys-id-ext 101)
             Address    0040.0BC2.E7A7
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 20

Interface          Role Sts Cost          Prio.Nbr Type
-----
Fa0/6              Desg FWD 19          128.6   P2p

DLS2#
DLS2#
DLS2#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

08:24 p. m. 30/11/2020

Fig. 16. Verificación de spanning tree en DLS2

CONCLUSIONES

El protocolo del camino más corto primero (OSPF) utiliza el algoritmo Dijkstra para encontrar la mejor ruta hacia la red destino. Su métrica es el Cost y utiliza como variable el Bandwidth. OSPF es un protocolo Classless, lo que significa que soporta VLSM y CIDR. A diferencia de EIGRP, incluye el concepto de Área el cual sólo se aplica a routers y para este trabajo se refiere a un conjunto de redes inmediatas identificadas por la misma área ID.

El Protocolo de enrutamiento de pasarela interior mejorado (EIGRP) es un protocolo de pasarela interior adecuado para muchas topologías y medios diferentes. EIGRP se escala bien y proporciona tiempos de convergencia extremadamente rápidos con un tráfico de red mínimo. Se representa a la información de distancia en IGRP como un compuesto de ancho de banda disponible, demora, uso de carga y confiabilidad de link. Esto permite afinar las características del link para alcanzar trayectos óptimos.

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

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

REFERENCIAS BIBLIOGRÁFICAS

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

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

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

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

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