

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

GENDERSON MAURICIO OROZCO RENDÓN

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

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

GENDERSON MAURICIO OROZCO RENDÓN

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Villavicencio Meta, 30 de noviembre de 2020

AGRADECIMIENTOS

En primer lugar, agradezco a Dios por brindarme el don de la sabiduría y entendimiento, a toda mi familia en general; mis padres por su apoyo constante y por la disciplina inculcada en mí, a mis hermanos que siempre fueron un apoyo inmenso tanto en la responsabilidad con mi proceso educativo como en el apoyo financiero para lograrlo, a mi esposa que siempre me animaba a ser el mejor y a mi preciosa hija que ha sido el combustible para alcanzar todos mis logros propuestos.

A cada uno de los tutores y maestros que apoyaron todo mi proceso formativo durante todo este tiempo de aprendizaje autónomo, a cada uno de los compañeros que hicieron parte de todos los grupos colaborativos en los que compartimos vivencias y sobre todo muchas enseñanzas. Por último, agradezco a todas esas personas que hacen posible esta gran universidad y su excelente servicio en el fortalecimiento y entrega por la educación de nuestro país. Mil gracias y que Dios los bendiga siempre.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT	9
INTRODUCCIÓN.....	10
DESARROLLO	11
1. ESCENARIO 1.....	11
2. ESCENARIO 2.....	23
CONCLUSIONES	47
BIBLIOGRAFÍA.....	48

LISTA DE TABLAS

Tabla 1. Interfaces Loopback en R1	16
Tabla 2. Interfaces Loopback en R5	18
Tabla 3. Configuración de VLANs en el servidor principal	34
Tabla 4. Configuración de interfaces en puertos de acceso	39

LISTA DE FIGURAS

Figura 1. Esquema del primer escenario	11
Figura 2. Topología del primer escenario en GNS3	11
Figura 3. Interfaces Loopback en R1	18
Figura 4. Interfaces Loopback en R5	19
Figura 5. Comando Show IP Route R3	20
Figura 6. Verificación de rutas en R1	21
Figura 7. Verificación de rutas en R5	22
Figura 8. Esquema del segundo escenario	23
Figura 9. Topología del segundo escenario en Packet Tracer	23
Figura 10. Interfaces de cada switch apagadas	25
Figura 11. Verificación de las VLAN en DLS 1	42
Figura 12. Verificación de las VLAN en DLS 2	42
Figura 13. Verificación de las VLAN en ALS 1	43
Figura 14. Verificación de las VLAN en ALS 2	43
Figura 15. Verificación EtherChannel DLS 1	44
Figura 16. Verificación EtherChannel ALS 1	44
Figura 17. Verificación show spanning-tree en DLS 1	45
Figura 18. Verificación show spanning-tree en DLS 2	45
Figura 19. Verificación show spanning-tree en ALS 1	46
Figura 20. Verificación show spanning-tree en ALS 2	46

GLOSARIO

Cisco Packet Tracer: Es un programa de simulación de redes que permite experimentar con el comportamiento de la red de forma didáctica y educativa. Permite la configuración de redes con una gran cantidad de comandos utilizados en las redes físicas, de tal forma que se pueden desarrollar habilidades que posteriormente se aplicarán en la vida profesional.

GNS3: Simulador gráfico de red lanzado en 2008, que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

DHCP: Siglas del inglés (Dynamic Host Configuration Protocol) Protocolo Dinámico de configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a los diferentes computadores de la red.

Protocolos de red: Procedimientos que se encuentran definidos o estandarizados para el uso y configuración adecuada de una red con el fin de que funcione de la mejor manera posible dependiendo de su topología, cantidad de dispositivos en la red y de las necesidades de funcionamiento de la red.

EIGRP: Protocolo de enrutamiento de puerta de enlace interior mejorado, el cual usa como parámetro la distancia y calidad del canal.

OSPF: Protocolo de enrutamiento que proporciona la ruta más corta y así obtener beneficios para la comunicación gracias al camino más corto abierto.

Topología de red: Son las estructuras que están compuestas por los dispositivos de la red, para este trabajo conformadas routers y switches. Existen varios tipos: bus, estrella, anillo, árbol, malla, híbrida son algunas de las más importantes las cuales se seleccionan para construir una red de acuerdo a las necesidades requeridas.

Router: Permite interconectar computadoras que funcionan en el marco de una red, se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.

Switch: Son los encargados de la interconexión de equipos dentro de una misma red, también son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.

Dirección IP: Conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo (Internet Protocol) o, que corresponde al nivel de red del modelo TCP/IP.

RESUMEN

Esta actividad consta del previo estudio de dos módulos CCNP ROUTE y CCNP SWITCH avalados por Cisco Networking Academy. Los contenidos están articulados con múltiples temáticas que permiten crear redes empresariales eficaces y escalables; así como instalar, configurar, supervisar, y solucionar problemas en los equipos pertenecientes a la infraestructura de una red multipropósito y multiplataforma. Se plantean dos escenarios el cual siguiendo unos lineamientos específicos nos permiten poner en práctica todos los conocimientos adquiridos en el diplomado de profundización CCNP.

El primer escenario está relacionado con los principios básicos de la red y los protocolos de enrutamiento IP versión 4 (IPv4) e IP versión 6 (IPv6), el Protocolo de enrutamiento de gateway interior mejorado (EIGRP), el protocolo Primer camino más corto (OSPF) y el protocolo de puerta de enlace de frontera (BGP). El segundo escenario está relacionado con la implementación, monitoreo, seguridad y administración de la conmutación en una arquitectura de red empresarial, la implementación de VLANs en redes corporativas, y la configuración y optimización para una alta disponibilidad y redundancia en los switches de capa 2 y capa 3.

Palabras Clave: Cisco, CCNP, Conmutación, Enrutamiento, Redes.

ABSTRACT

This activity consists of the previous study of two modules CCNP ROUTE and CCNP SWITCH endorsed by Cisco Networking Academy. The contents are articulated with multiple themes that allow to create efficient and scalable business networks; as well as to install, configure, monitor, and troubleshoot the equipment belonging to the infrastructure of a multipurpose and multiplatform network. Two scenarios are proposed which following specific guidelines allow us to put into practice all the knowledge acquired in the CCNP deepening diploma.

The first scenario is related to the basic principles of the network and the IP version 4 (IPv4) and IP version 6 (IPv6) routing protocols, the Enhanced Interior Gateway Routing Protocol (EIGRP), the First Shortest Path protocol (OSPF) and Border Gateway Protocol (BGP). The second scenario is related to the implementation, monitoring, security and management of switching in an enterprise network architecture, the implementation of VLANs in corporate networks, and the configuration and optimization for high availability and redundancy in Layer 2 switches and layer 3.

Keywords: Cisco, CCNP, Routing, Swicthing, Networking.

INTRODUCCIÓN

El diplomado Cisco CCNP nos permite desarrollar habilidades y potenciar la experiencia a la hora de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia; a su vez a trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, redes inalámbricas etc. Proporcionando conocimientos profundos sobre routing avanzado, switching y mantenimiento; obteniendo capacidades y competencias necesarias para diseñar y soportar redes complejas empresariales. El estudio del primer módulo (CCNP ROUTE) nos permite apropiarse de las temáticas relacionadas con los principios básicos de la red y los protocolos de enrutamiento, el segundo módulo CCNP SWITCH nos permite apropiarse de las temáticas relacionadas con la implementación, seguridad, monitoreo y administración de la conmutación en una arquitectura de red empresarial, la implementación de VLANs en redes corporativas y las características de seguridad en redes LAN y WAN.

Se expone el desarrollo de un primer escenario donde se aplican los conceptos prácticos de red y routing, se aplican configuraciones iniciales a los protocolos de implementación de EIGRP y de implementación OSPF; del mismo modo se manipulan actualizaciones de routing. De igual manera, se explora la conectividad empresarial hacia Internet y se analiza la administración de las actualizaciones de enrutamiento y las rutas que toma el tráfico en la red. También se examinan las mejores prácticas de seguridad informática para los enrutadores Cisco. Este escenario se desarrolla por medio del empleo de la herramienta de simulación GNS3.

El segundo escenario nos expone un ejemplo aplicado de una posible compañía de comunicaciones que presenta una estructura Core acorde a la topología de red, en donde desempeñaremos de manera práctica el rol de administrador de la red, el cual debemos 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, VLAN's y demás aspectos que forman parte del escenario propuesto. Para este escenario se emplea la herramienta de simulación Cisco Packet Tracer. Cabe resaltar que para dar solución a los dos escenarios se debe poseer un amplio manejo y conocimiento de los módulos CCNP ROUTE y CCNP SWITCH.

DESARROLLO

1. ESCENARIO 1

Teniendo en la cuenta la siguiente imagen:

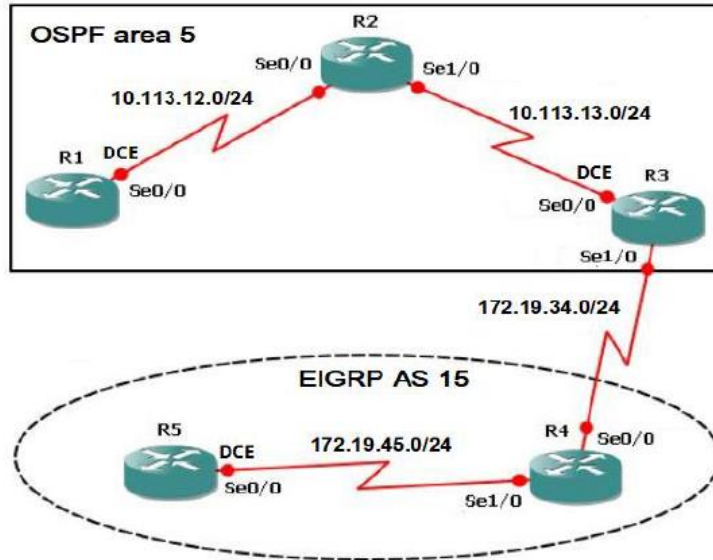


Figura 1. Esquema del primer escenario

Topología:

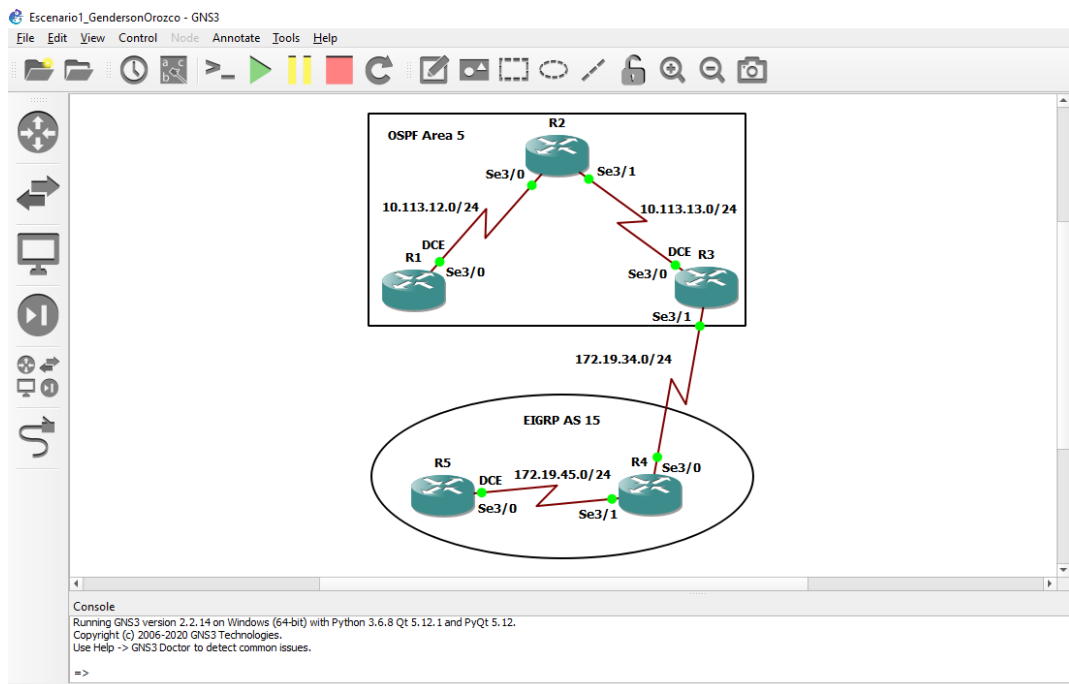


Figura 2. Topología del primer escenario en GNS3

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.

Para los dos primeros routers se realiza una configuración similar empezando con el código de ingreso a modo privilegiado, luego se aplica el código de modo de configuración, se asigna el nombre al router, de igual forma se establece el protocolo OSPF, determinamos la configuración IP junto con la configuración del interfaz serial. Se asigna la configuración de clockrate y bandwidth puesto que se configura solo para DCE con el fin de poder sincronizar la conexión; por último, activamos interfaz.

Configuración R1:

```
R1#conf term
```

```
R1(config)#hostname R1
```

```
R1(config)#router ospf 1
```

```
R1(config-router)#router-id 1.1.1.1
```

```
R1(config-router)#network 10.113.12.0 255.255.255.0 area 5
```

```
R1(config-router)#exit
```

```
R1(config)#interface s3/0
```

```
R1(config-if)#description to R2
```

```
R1(config-if)#ip address 10.113.12.1 255.255.255.0
```

```
R1(config-if)#clock rate 128000
```

```
R1(config-if)#bandwidth 128
```

```
R1(config-if)#no shutdown
```

```
R1(config-if)#exit
```

```
R1(config)#end
```

Configuración R2:

```
R2#conf term
```

```
R2(config)#hostname R2
```

```
R2(config)#router ospf 1
```

```
R2(config-router)#router-id 2.2.2.2
```

```
R2(config-router)#network 10.113.12.0 255.255.255.0 area 5
```

```
R2(config-router)#network 10.113.13.0 255.255.255.0 area 5
```

```
R2(config-router)#exit
```

```
R2(config)#interface s3/0
```

```
R2(config-if)#description to R1
```

```
R2(config-if)#ip address 10.113.12.2 255.255.255.0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
```

```
R2(config)#interface s3/1
```

```
R2(config-if)#description to R3
```

```
R2(config-if)#ip address 10.113.13.1 255.255.255.0
```

```
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
```

```
R2(config)#end
```

Realizamos la configuración inicial del Router R3 de la misma manera; teniendo en cuenta establecer el protocolo OSPF como EIGRP.

Configuración R3:

```
R3#conf term
```

```
R3(config)#hostname R3
```

```
R3(config)#router ospf 1
```

```
R3(config-router)#router-id 3.3.3.3
```

```
R3(config-router)#network 10.113.13.0 255.255.255.0 area 5
```

```
R3(config-router)#exit
```

```
R3(config)#interface s3/0
```

```
R3(config-if)#description to R2
```

```
R3(config-if)#ip address 10.113.13.2 255.255.255.0
```

```
R3(config-if)#clock rate 128000
```

```
R3(config-if)#bandwidth 128
```

```
R3(config-if)#no shutdown
```

```
R3(config-if)#exit
```

```
R3(config)#interface s3/1
```

```
R3(config-if)#description to R4
```

```
R3(config-if)#ip address 172.19.34.1 255.255.255.0
```

```
R3(config-if)#no shutdown
```

```
R3(config-if)#exit
```

```
R3(config)#end
```

```
R3#conf term
```

```
R3(config)#router eigrp 15
```

```
R3(config-rtr)#eigrp router-id 3.3.3.3
```

```
R3(config-rtr)#network 172.19.34.0 255.255.255.0
R3(config-rtr)#exit
R3(config)#end
```

Para los dos últimos routers se configura el ingreso a modo privilegiado siguiendo del modo configuración, se establece nombre al router, se configura el protocolo EIGRP, asignamos configuración IP, se configuran las interfaces seriales y finalmente las activamos.

Configuración R4:

```
R4#conf term
R4(config)#hostname R4
R4(config)#router eigrp 15
R4(config-rtr)#eigrp router-id 4.4.4.4
R4(config-rtr)#network 172.19.34.0 255.255.255.0
R4(config-rtr)#network 172.19.45.0 255.255.255.0
R4(config-rtr)#exit

R4(config)#interface s3/0
R4(config-if)#ip address 172.19.34.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit

R4(config)#interface s3/1
R4(config-if)#ip address 172.19.45.1 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
```

```
R4(config)#end
```

Configuración R5:

```
R5#conf term
```

```
R5(config)#hostname R5
```

```
R5(config)#router eigrp 15
```

```
R5(config-rtr)#eigrp router-id 5.5.5.5
```

```
R5(config-rtr)#network 172.19.45.0 255.255.255.0
```

```
R5(config-rtr)#exit
```

```
R5(config)#interface s3/0
```

```
R5(config-if)#ip address 172.19.45.2 255.255.255.0
```

```
R5(config-if)#no shutdown
```

```
R5(config-if)#exit
```

```
R5(config)#end
```

2.1 Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 5 de OSPF.

Configuramos y creamos la interfaz loopback 0, 4, 8 y 12, establecemos configuración IP y configuramos en OSPF usamos el comando ip ospf network point-to-point el cual permitirá que el protocolo OSPF forme una adyacencia con el vecino del otro lado de la interfaz a través de las líneas seriales determinadas.

Interfaces Loopback en R1	
Loopback 0	10.1.0.1/22
Loopback 4	10.1.4.1/22
Loopback 8	10.1.8.1/22
Loopback 12	10.1.12.1/22

Tabla 1. Interfaces Loopback en R1


```
R1#conf term
R1(config)#interface loopback 0
R1(config-if)#ip address 10.1.0.1 255.255.252.0
R1(config-if)#ip ospf 1 area 5
R1(config-if)#ip ospf network point-to-point
R1(config-if)#exit
```

```
R1(config)# interface loopback 4
R1(config-if)#ip address 10.1.4.1 255.255.252.0
R1(config-if)#ip ospf 1 area 5
R1(config-if)#ip ospf network point-to-point
R1(config-if)#exit
```

```
R1(config)# interface loopback 8
R1(config-if)#ip address 10.1.8.1 255.255.252.0
R1(config-if)#ip ospf 1 area 5
R1(config-if)#ip ospf network point-to-point
R1(config-if)#exit
```

```
R1(config)# interface loopback 12
R1(config-if)#ip address 10.1.12.1 255.255.252.0
R1(config-if)#ip ospf 1 area 5
R1(config-if)#ip ospf network point-to-point
R1(config-if)#exit
R1(config)#end
```

```

*Oct 20 10:47:56.707: %SYS-5-CONFIG_I: Configured from console by console
R1#
R1#sh ip ospf interface bri
Interface      PID  Area      IP Address/Mask    Cost  State  Nbrs F/C
Lo0            1    5         10.1.0.1/22        1     P2P    0/0
Lo4            1    5         10.1.4.1/22        1     P2P    0/0
Lo8            1    5         10.1.8.1/22        1     P2P    0/0
Lo12           1    5         10.1.12.1/22       1     P2P    0/0
Se3/0          1    5         10.113.12.1/24     781   P2P    1/1
R1#

```

Figura 3. Interfaces Loopback en R1

3.1 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.

Configuramos y creamos la interfaz loopback 0, 4, 8 y 12 y establecemos configuración IP.

Interfaces Loopback en R5	
Loopback 0	172.5.0.1/22
Loopback 4	172.5.4.1/22
Loopback 8	172.5.8.1/22
Loopback 12	172.5.12.1/22

Tabla 2. Interfaces Loopback en R5

```
R5#conf term
```

```
R5(config)#interface loopback 0
```

```
R5(config-if)#ip address 172.5.0.1 255.255.252.0
```

```
R5(config-if)#exit
```

```
R5(config)#interface loopback 4
```

```
R5(config-if)#ip address 172.5.4.1 255.255.252.0
```

```
R5(config-if)#exit
```

```
R5(config)#interface loopback 8
```

```
R5(config-if)#ip address 172.5.8.1 255.255.252.0
```

```
R5(config-if)#exit
```

```
R5(config)#interface loopback 12
```

```
R5(config-if)#ip address 172.5.12.1 255.255.252.0
```

```
R5(config-if)#exit
```

```
R5(config)#router eigrp 15
```

```
R5(config-router)#network 172.5.0.1 255.255.252.0
```

```
R5(config-router)#network 172.5.4.1 255.255.252.0
```

```
R5(config-router)#network 172.5.8.1 255.255.252.0
```

```
R5(config-router)#network 172.5.12.1 255.255.252.0
```

```
R5(config-router)#exit
```

```
R5(config)#end
```

```
*Oct 20 10:49:24.331: %SYS-5-CONFIG_I: Configured from console by console
R5#
R5#sh ip interface bri | include up
Serial3/0          172.19.45.2      YES manual up    up
Loopback0         172.5.0.1        YES manual up    up
Loopback4         172.5.4.1        YES manual up    up
Loopback8         172.5.8.1        YES manual up    up
Loopback12        172.5.12.1      YES manual up    up
R5#
```

Figura 4. Interfaces Loopback en R5

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

Se evidencia en la figura que se crearon las Loopback 0,4,8 y 12 con sus respectivas máscaras de subred /22 y se encuentran activas.

```
R3#show ip route
```

```
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router eigrp 15
R3(config-router)#eigrp router-id 3.3.3.3
R3(config-router)#network 172.19.34.0 255.255.255.0
R3(config-router)#exit
*Oct 20 10:39:52.387: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1, changed state to down
R3(config-router)#exit
R3(config)#end
R3#
*Oct 20 10:40:00.975: %SYS-5-CONFIG_I: Configured from console by console
R3#
*Oct 20 10:41:12.071: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 15: Neighbor 172.19.34.2 (Serial3/1) is up: new adjacency
*Oct 20 10:41:12.391: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1, changed state to up
R3#
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O    172.5.0.0/16 [90/2809856] via 172.19.34.2, 00:06:41, Serial3/1
    172.19.0.0/24 is subnetted, 2 subnets
O    172.19.45.0 [90/2681856] via 172.19.34.2, 00:14:23, Serial3/1
C    172.19.34.0 is directly connected, Serial3/1
O    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O    10.1.8.0/22 [110/846] via 10.113.13.1, 00:11:41, Serial3/0
O    10.1.12.0/22 [110/846] via 10.113.13.1, 00:11:31, Serial3/0
O    10.1.0.0/22 [110/846] via 10.113.13.1, 00:12:21, Serial3/0
O    10.1.4.0/22 [110/846] via 10.113.13.1, 00:11:58, Serial3/0
C    10.113.13.0/24 is directly connected, Serial3/0
O    10.113.12.0/24 [110/845] via 10.113.13.1, 00:18:19, Serial3/0
R3#
```

Figura 5. Comando Show IP Route R3

5.1 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.

Redistribución de rutas: OSPF en EIGRP

```
R3#conf term
```

```
R3(config)#router eigrp 15
```

```
R3(config-router)#redistribute ospf 1 metric 1544 20000 255 1 1500
```

```
R3(config-router)#exit
```

Redistribución de rutas: EIGRP en OSPF

```
R3(config)#router ospf 1
```

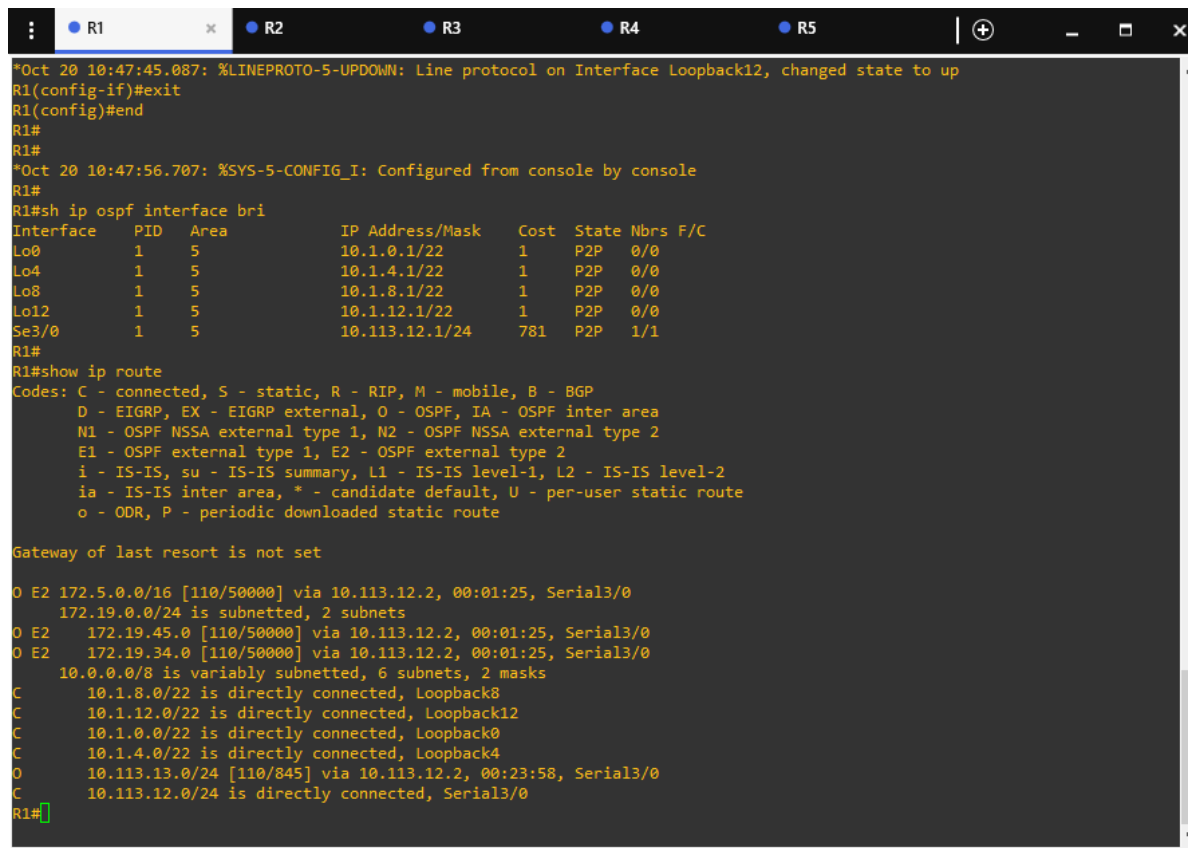
```
R3(config-router)#redistribute eigrp 15 metric 50000 subnets
```

```
R3(config-router)#exit
```

```
R3(config)#end
```

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

```
R1#show ip route
```



```
*Oct 20 10:47:45.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback12, changed state to up
R1(config-if)#exit
R1(config)#end
R1#
R1#
*Oct 20 10:47:56.707: %SYS-5-CONFIG_I: Configured from console by console
R1#
R1#sh ip ospf interface bri
Interface  PID  Area          IP Address/Mask  Cost  State Nbrs F/C
-----  ---  ---          -
Lo0        1    5             10.1.0.1/22      1     P2P   0/0
Lo4        1    5             10.1.4.1/22      1     P2P   0/0
Lo8        1    5             10.1.8.1/22      1     P2P   0/0
Lo12       1    5             10.1.12.1/22     1     P2P   0/0
Se3/0     1    5             10.113.12.1/24   781   P2P   1/1
R1#
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O E2 172.5.0.0/16 [110/50000] via 10.113.12.2, 00:01:25, Serial3/0
    172.19.0.0/24 is subnetted, 2 subnets
O E2   172.19.45.0 [110/50000] via 10.113.12.2, 00:01:25, Serial3/0
O E2   172.19.34.0 [110/50000] via 10.113.12.2, 00:01:25, Serial3/0
    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C     10.1.8.0/22 is directly connected, Loopback8
C     10.1.12.0/22 is directly connected, Loopback12
C     10.1.0.0/22 is directly connected, Loopback0
C     10.1.4.0/22 is directly connected, Loopback4
O     10.113.13.0/24 [110/845] via 10.113.12.2, 00:23:58, Serial3/0
C     10.113.12.0/24 is directly connected, Serial3/0
R1#
```

Figura 6. Verificación de rutas en R1

```
R5#show ip route
```

```
Oct 20 10:49:24.331: %SYS-5-CONFIG_I: Configured from console by console
R5#
R5#sh ip interface bri | include up
Serial3/0          172.19.45.2      YES manual up
Loopback0         172.5.0.1       YES manual up
Loopback4         172.5.4.1       YES manual up
Loopback8         172.5.8.1       YES manual up
Loopback12        172.5.12.1      YES manual up
R5#
R5#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    172.5.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.5.8.0/22 is directly connected, Loopback8
C       172.5.12.0/22 is directly connected, Loopback12
C       172.5.0.0/22 is directly connected, Loopback0
D       172.5.0.0/16 is a summary, 00:22:38, Null0
C       172.5.4.0/22 is directly connected, Loopback4
    172.19.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.19.45.0/24 is directly connected, Serial3/0
D       172.19.34.0/24 [90/2681856] via 172.19.45.1, 00:30:19, Serial3/0
D       172.19.0.0/16 is a summary, 00:22:38, Null0
    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D EX   10.1.8.0/22 [170/7801856] via 172.19.45.1, 00:05:20, Serial3/0
D EX   10.1.12.0/22 [170/7801856] via 172.19.45.1, 00:05:20, Serial3/0
D EX   10.1.0.0/22 [170/7801856] via 172.19.45.1, 00:05:27, Serial3/0
D EX   10.1.4.0/22 [170/7801856] via 172.19.45.1, 00:05:28, Serial3/0
D EX   10.113.13.0/24 [170/7801856] via 172.19.45.1, 00:05:28, Serial3/0
D EX   10.113.12.0/24 [170/7801856] via 172.19.45.1, 00:05:28, Serial3/0
R5#
```

Figura 7. Verificación de rutas en R5

2. ESCENARIO 2

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

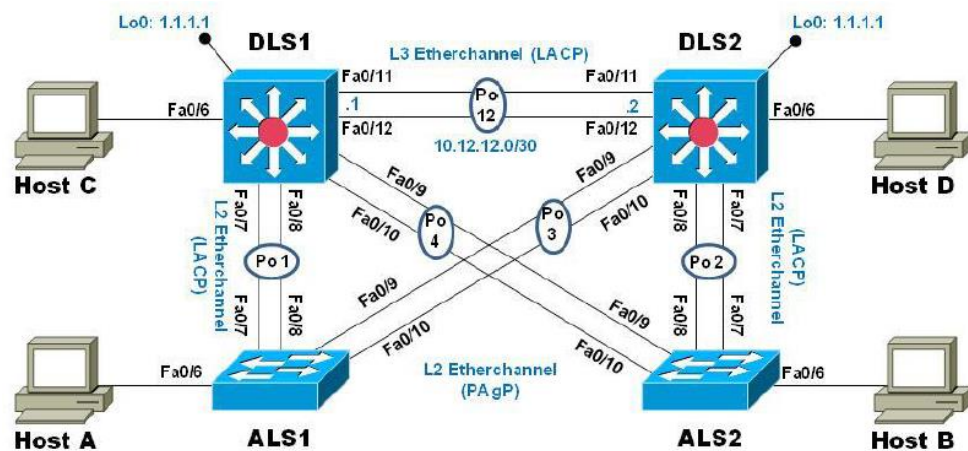


Figura 8. Esquema del segundo escenario

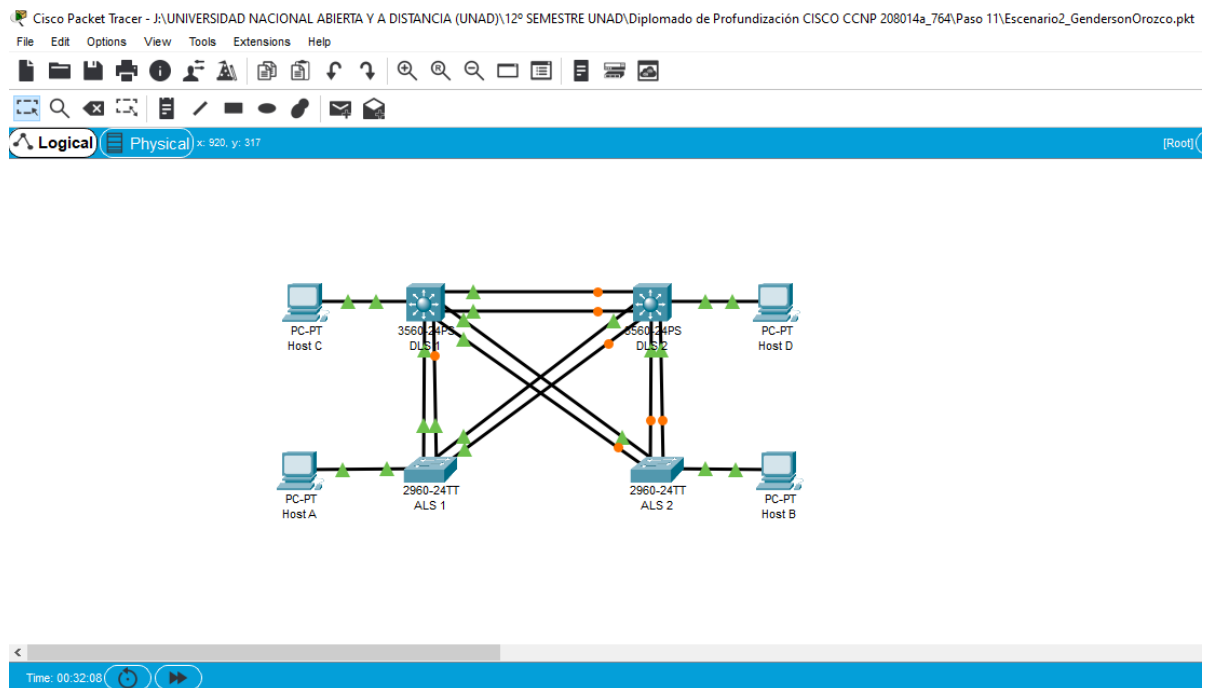


Figura 9. Topología del segundo escenario en Packet Tracer

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

a. Apagar todas las interfaces en cada switch.

Se inicia en modo privilegiado, se fija el rango y se utiliza el comando shutdown (apagar) para deshabilitar las interfaces.

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

Dentro del mismo modo privilegiado se utiliza el comando hostname + nombre para asignarlo.

```
Switch>enable
```

```
Switch#configure terminal
```

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

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

```
DLS1(config)#int ran f0/1-24, g0/1-2
```

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

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

```
Switch>enable
```

```
Switch#configure terminal
```

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

```
Switch(config)#hostname DLS2
```

```
DLS2(config)#int ran f0/1-24, g0/1-2
```

```
DLS2(config-if-range)#shutdown
```

```
DLS2(config-if-range)#exit
```

```
Switch>enable
```

```
Switch#configure terminal
```


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

```
Switch(config)#hostname ALS1
```

```
ALS1(config)#int ran f0/1-24, g0/1-2
```

```
ALS1(config-if-range)#shutdown
```

```
ALS1(config-if-range)#exit
```

```
Switch>enable
```

```
Switch#configure terminal
```

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

```
Switch(config)#hostname ALS2
```

```
ALS2(config)#int ran f0/1-24, g0/1-2
```

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

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

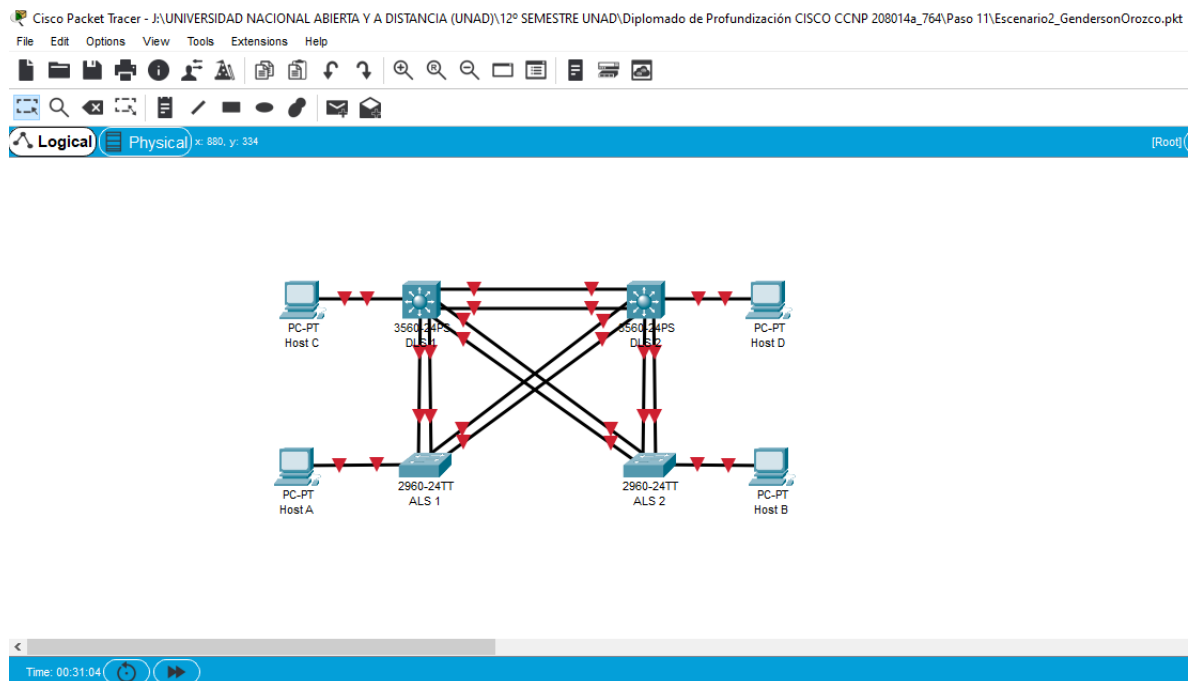


Figura 10. Interfaces de cada switch apagadas

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

Igualmente, en modo privilegiado se procede declarar el rango de interfaces y se procede a realizar las configuraciones port-channels.

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.

Se establece la declaración de la VLAN y la respectiva asignación de dirección IP según la descripción del escenario.

```
DLS1>en
```

```
DLS1#conf t
```

```
DLS1(config)#interface port-channel 12
```

```
DLS1(config-if)#no switchport
```

```
DLS1(config-if)#ip address 10.12.12.1 255.255.255.252
```

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

```
DLS1(config)#interface range fa0/11-12
```

```
DLS1(config-if-range)#no switchport
```

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

```
DLS1(config)#exit
```

```
DLS2>en
```

```
DLS2#conf t
```

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

```
DLS2(config)#interface port-channel 12
```

```
DLS2(config-if)#no switchport
```

```
DLS2(config-if)#ip address 10.12.12.2 255.255.255.252
```

```
DLS2(config-if)#exit
```

```
DLS2(config)#interface range fa0/11-12
DLS2(config-if-range)#no switchport
DLS2(config-if-range)#exit
DLS2(config)#exit
```

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

```
DLS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#interface range fa0/7-8
DLS1(config-if-range)#switchport trunk encapsulation dot1q
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 1 mode active
DLS1(config-if-range)#no shutdown
DLS1(config-if-range)#exit
DLS1(config)#exit
```

```
ALS1>en
ALS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#int range fa0/7-8
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 1 mode active
ALS1(config-if-range)#no shutdown
ALS1(config-if-range)#exit
ALS1(config)#exit
```

```
DLS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#interface range fa0/7-8
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 2 mode active
DLS2(config-if-range)#no shutdown
DLS2(config-if-range)#exit
DLS2(config)#exit
```

```
ALS2>en
ALS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#int range fa0/7-8
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 2 mode active
ALS2(config-if-range)#no shutdown
ALS2(config-if-range)#exit
ALS2(config)#exit
```

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

Se configuran las interfaces del f0/9 a f0/10 como protocolo del canal y se levanta.

```
DLS1>en
DLS1#conf t
DLS1(config)#interface range fa0/9-10
DLS1(config-if-range)#switchport trunk encapsulation dot1q
```

```
DLS1(config-if-range)#switchport mode trunk
DLS1(config-if-range)#channel-group 4 mode desirable
DLS1(config-if-range)#no shutdown
DLS1(config-if-range)#exit
```

```
ALS2>en
ALS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface range fa0/9-10
ALS2(config-if-range)#switchport mode trunk
ALS2(config-if-range)#channel-group 4 mode desirable
ALS2(config-if-range)#no shutdown
ALS2(config-if-range)#exit
```

```
DLS2>en
DLS2#conf t
DLS2(config)#interface range fa0/9-10
DLS2(config-if-range)#switchport trunk encapsulation dot1q
DLS2(config-if-range)#switchport mode trunk
DLS2(config-if-range)#channel-group 3 mode desirable
DLS2(config-if-range)#no shutdown
DLS2(config-if-range)#exit
```

```
ALS1>en
ALS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#interface range fa0/9-10
```

```
ALS1(config-if-range)#switchport mode trunk
ALS1(config-if-range)#channel-group 3 mode desirable
ALS1(config-if-range)#no shutdown
ALS1(config-if-range)#exit
```

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

Con la lista de comandos que se adjuntan a continuación los puertos troncales son asignados a la VLAN 500 como nativa.

```
DLS1>en
DLS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS1(config)#interface po1
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#exit
DLS1(config)#interface po4
DLS1(config-if)#switchport trunk native vlan 500
DLS1(config-if)#exit
DLS1(config)#exit
```

```
DLS2>en
DLS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DLS2(config)#interface po2
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#exit
DLS2(config)#interface po3
```

```
DLS2(config-if)#switchport trunk native vlan 500
DLS2(config-if)#exit
DLS2(config)#exit
```

```
ALS1>en
ALS1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS1(config)#interface po1
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#exit
ALS1(config)#interface po3
ALS1(config-if)#switchport trunk native vlan 500
ALS1(config-if)#exit
ALS1(config)#exit
```

```
ALS2>en
ALS2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ALS2(config)#interface Po2
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#exit
ALS2(config)#interface Po4
ALS2(config-if)#switchport trunk native vlan 500
ALS2(config-if)#exit
ALS2(config)#exit
```

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

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

```
DLS1>en
```

```
DLS1#conf t
```

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

```
DLS1(config)#vtp domain CISCO
```

```
DLS1(config)#vtp password ccnp321
```

```
DLS1(config)#vtp version 2
```

```
DLS1(config)#exit
```

```
ALS1>en
```

```
ALS1#conf t
```

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

```
ALS1(config)#vtp domain CISCO
```

```
ALS1(config)#vtp password ccnp321
```

```
ALS1(config)#vtp version 2
```

```
ALS1(config)#exit
```

```
ALS2>en
```

```
ALS2#conf t
```

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

```
ALS2(config)#vtp domain CISCO
```

```
ALS2(config)#vtp password ccnp321
```

```
ALS2(config)#vtp version 2
```

```
ALS2(config)#exit
```


2) Configurar DLS1 como servidor principal para las VLAN.

```
DLS1>en
```

```
DLS1#conf t
```

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

```
DLS1(config)#vtp mode server
```

Device mode already VTP SERVER.

```
DLS1(config)#exit
```

3) Configurar ALS1 y ALS2 como clientes VTP.

```
ALS1>en
```

```
ALS1#conf t
```

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

```
ALS1(config)#vtp mode client
```

Setting device to VTP CLIENT mode.

```
ALS1(config)#exit
```

```
ALS2>en
```

```
ALS2#conf t
```

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

```
ALS2(config)#vtp mode client
```

Setting device to VTP CLIENT mode.

```
ALS2(config)#exit
```

e. Configurar en el servidor principal las siguientes VLAN:

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
500	NATIVA	434	PROVEEDORES
12	ADMON	123	SEGUROS
234	CLIENTES	1010 (101)	VENTAS
1111 (111)	MULTIMEDIA	3456 (345)	PERSONAL

Tabla 3. Configuración de VLANs en el servidor principal

```
DLS1>en
```

```
DLS1#conf t
```

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

```
DLS1(config)#vlan 500
```

```
DLS1(config-vlan)#name NATIVA
```

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

```
DLS1(config-vlan)#vlan 12
```

```
DLS1(config-vlan)#name ADMON
```

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

```
DLS1(config-vlan)#vlan 234
```

```
DLS1(config-vlan)#name CLIENTES
```

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

```
DLS1(config-vlan)#vlan 111
```

```
DLS1(config-vlan)#name MULTIMEDIA
```

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

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

```
DLS1(config-vlan)#name PROVEEDORES
```

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

```
DLS1(config-vlan)#vlan 123
```

```
DLS1(config-vlan)#name SEGUROS
```

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

```
DLS1(config-vlan)#vlan 101
```

```
DLS1(config-vlan)#name VENTAS
```

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

```
DLS1(config-vlan)#vlan 345
```

```
DLS1(config-vlan)#name PERSONAL
```

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

f. En DLS1, suspender la VLAN 434.

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

```
DLS1(config-vlan)#name PROVEEDORES
```

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

Nota: En Pack Tracer no permite suspender la Vlan 434, pero si permite eliminarla. Por tal razón, se dejará habilitada.

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

Se procede a ejecutar las especificaciones anteriores DLS2 en modo transparente y a configurar las VLAN correspondientes.

```
DLS2#conf t
DLS2(config)#vtp version 2
DLS2(config)#vtp mode transparent
DLS2(config)#vlan 500
DLS2(config-vlan)#name NATIVA
DLS2(config-vlan)#exit
```

```
DLS2(config)#vlan 12
DLS2(config-vlan)#name ADMON
DLS2(config-vlan)#exit
```

```
DLS2(config)#vlan 234
DLS2(config-vlan)#name CLIENTES
DLS2(config-vlan)#exit
```

```
DLS2(config)#vlan 111
DLS2(config-vlan)#name MULTIMEDIA
DLS2(config-vlan)#exit
```

```
DLS2(config)#vlan 123
DLS2(config-vlan)#name SEGUROS
DLS2(config-vlan)#exit
```

```
DLS2(config)#vlan 101
DLS2(config-vlan)#name VENTAS
DLS2(config-vlan)#exit
```

```
DLS2(config)#vlan 345
DLS2(config-vlan)#name PERSONAL
DLS2(config-vlan)#exit
```

h. Suspende VLAN 434 en DLS2.

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

Nota: En Pack Tracer no permite suspender la Vlan 434, pero si permite eliminarla. Por tal razón, se dejará habilitada.

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>en
DLS2#conf t
DLS2(config)#interface port-channel 2
DLS2(config-if)#switchport trunk allowed vlan except 567
DLS2(config-if)#exit
DLS2(config)#interface port-channel 3
DLS2(config-if)#switchport trunk allowed vlan except 567
DLS2(config-if)#exit
DLS2(config)#vlan 567
DLS2(config-vlan)#name PRODUCCION
DLS2(config-vlan)#exit
```

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>en
```

```
DLS1#conf t
```

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

```
DLS1(config)#spanning-tree vlan 12,434,500,101,111,345 root primary
```

```
DLS1(config)#exit
```

```
DLS1>en
```

```
DLS1#conf t
```

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

```
DLS1(config)#spanning-tree vlan 123,234 root secondary
```

```
DLS1(config)#exit
```

k. Configurar DLS2 como Spanning tree root para las VLAN 123 y 234 y como una raíz secundaria para las VLAN 12, 434, 500, 10, 11 y 345.

```
DLS2>en
```

```
DLS2#conf t
```

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

```
DLS2(config)#spanning-tree vlan 123,234 root primary
```

```
DLS2(config)#exit
```

```
DLS2>en
```

```
DLS2#conf t
```

```
DLS2(config)#spanning-tree vlan 12,434,500,101,111,345 root secondary
```

```
DLS2(config)#exit
```

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

```
DLS1>en
DLS1#conf t
DLS1(config-if)#int port-channel 1
DLS1(config-if)#switchport trunk allowed vlan 12,123,234,500,101,111,345
DLS1(config-if)#exit
DLS1(config-if)#int port-channel 4
DLS1(config-if)#switchport trunk allowed vlan 12,123,234,500,101,111,345
DLS1(config-if)#exit
```

```
DLS2>en
DLS2#conf t
DLS2(config-if)#int port-channel 2
DLS2(config-if)#switchport trunk allowed vlan 12,123,234,500,101,111,345
DLS2(config-if)#exit
DLS2(config-if)#int port-channel 3
DLS2(config-if)#switchport trunk allowed vlan 12,123,234,500,101,111,345
DLS2(config-if)#exit
```

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

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3456 (345)	12, 1010 (101)	123, 1010 (101)	234
Interfaz Fa0/15	1111 (111)	1111 (111)	1111 (111)	1111 (111)
Interfaces F0 /16-18		567		

Tabla 4. Configuración de interfaces en puertos de acceso

```
DLS1>en
DLS1#conf t
DLS1(config)#interface fastethernet 0/6
DLS1(config-if)#switchport access vlan 345
DLS1(config-if)#no shutdown
DLS1(config-if)#exit
DLS1(config)#interface fastethernet 0/15
DLS1(config-if)#switchport access vlan 111
DLS1(config-if)#no shutdown
DLS1(config-if)#exit
```

```
DLS2>en
DLS2#conf t
DLS2(config)#interface fastethernet 0/6
DLS2(config-if)#switchport access vlan 12
DLS2(config-if)#switchport access vlan 101
DLS2(config-if)#no shutdown
DLS2(config-if)#exit
DLS2(config)#interface fastethernet 0/15
DLS2(config-if)#switchport access vlan 111
DLS2(config-if)#no shutdown
DLS2(config-if)#exit
```

```
DLS2>en
DLS2# conf t
DLS2(config)#int ran f0/16-18
DLS2(config-if)#switchport access vlan 567
```



```
DLS2(config-if)#no shutdown
```

```
DLS2(config-if)#exit
```

```
ALS1>en
```

```
ALS1#conf t
```

```
ALS1(config)#interface fastethernet 0/6
```

```
ALS1(config-if)#switchport access vlan 123
```

```
ALS1(config-if)#switchport access vlan 101
```

```
ALS1(config-if)#no shutdown
```

```
ALS1(config)#exit
```

```
ALS1(config)#interface fastethernet 0/15
```

```
ALS1(config-if)#switchport access vlan 111
```

```
ALS1(config-if)#no shutdown
```

```
ALS1(config-if)#exit
```

```
ALS2>en
```

```
ALS2#conf t
```

```
ALS2(config)#interface fastethernet 0/6
```

```
ALS2(config-if)#switchport access vlan 234
```

```
ALS2(config-if)#no shutdown
```

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

```
ALS2(config)#interface fastethernet 0/15
```

```
ALS2(config-if)#switchport access vlan 111
```

```
ALS2(config-if)#no shutdown
```

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

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.

Se emplea el comando `show vlan` para observar y verificar la información solicitada.

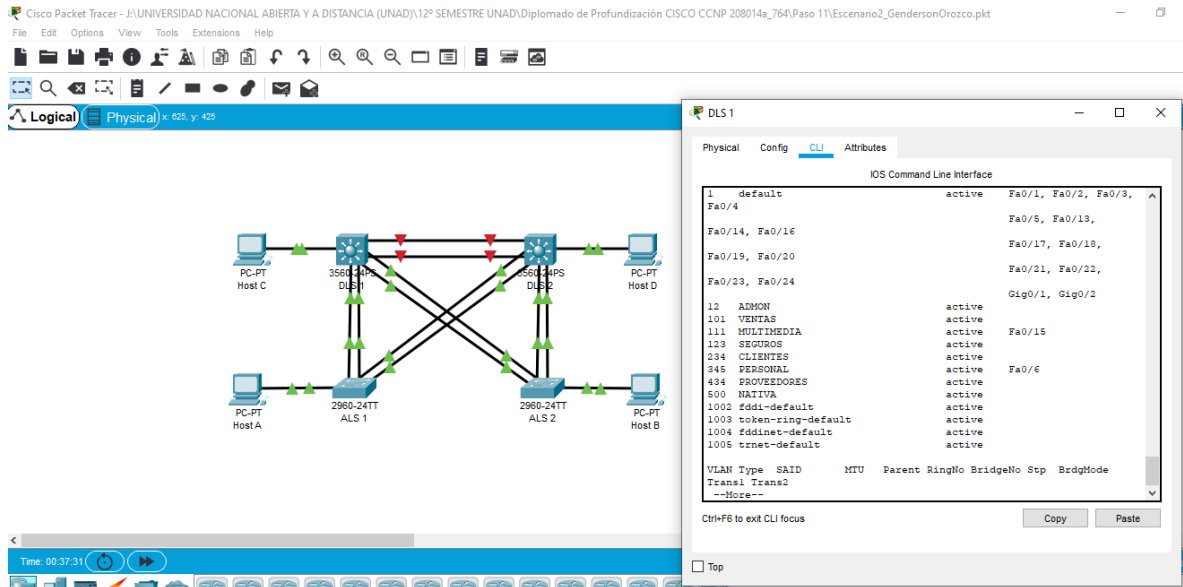


Figura 11. Verificación de las VLAN en DLS 1

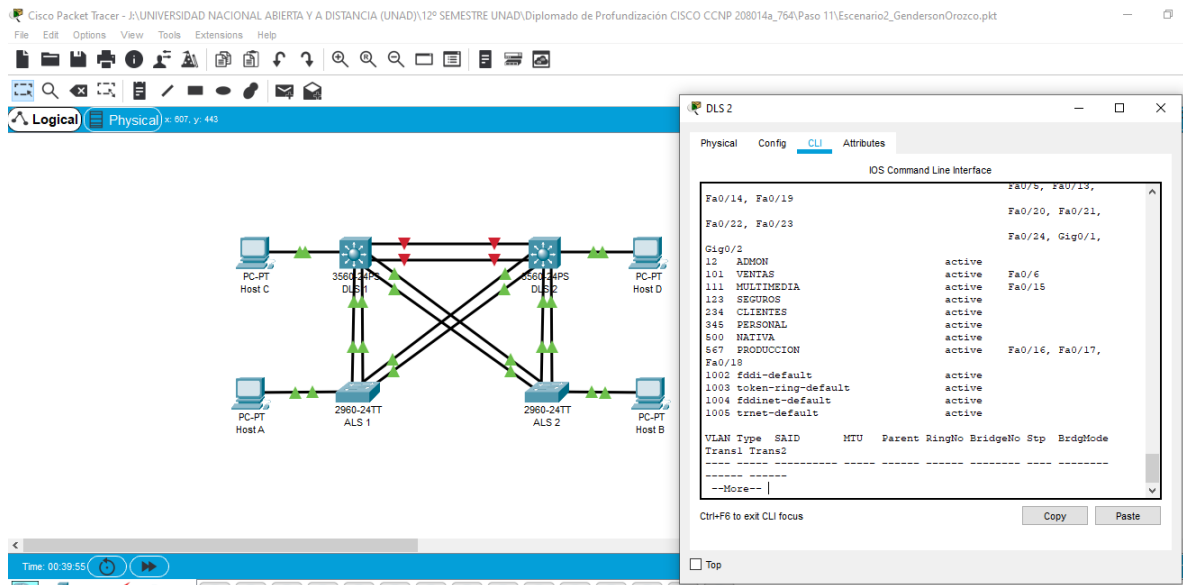


Figura 12. Verificación de las VLAN en DLS 2

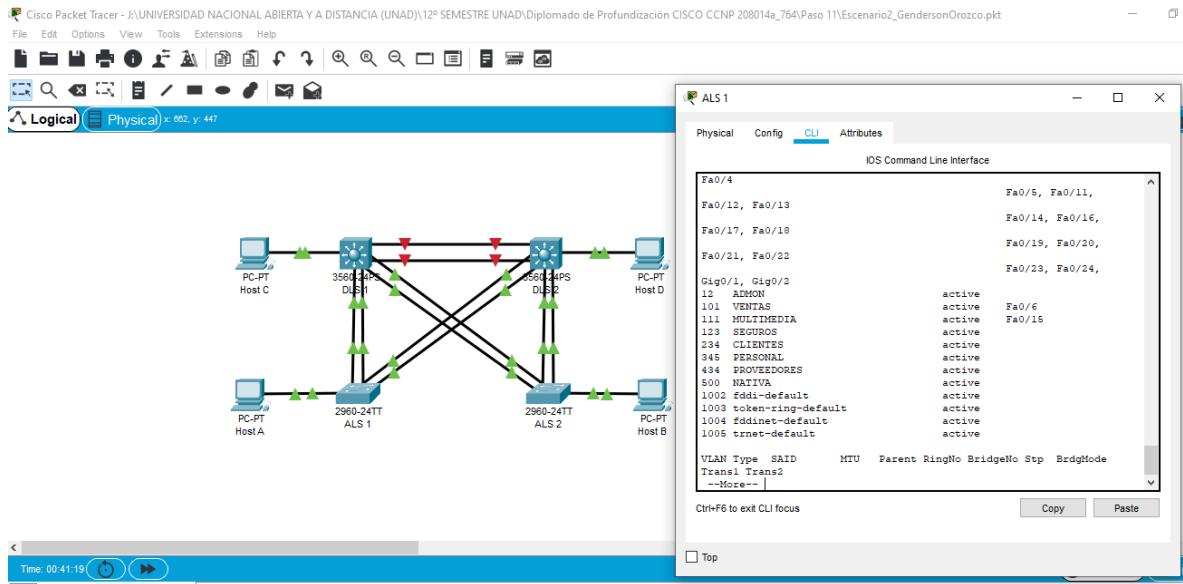


Figura 13. Verificación de las VLAN en ALS 1

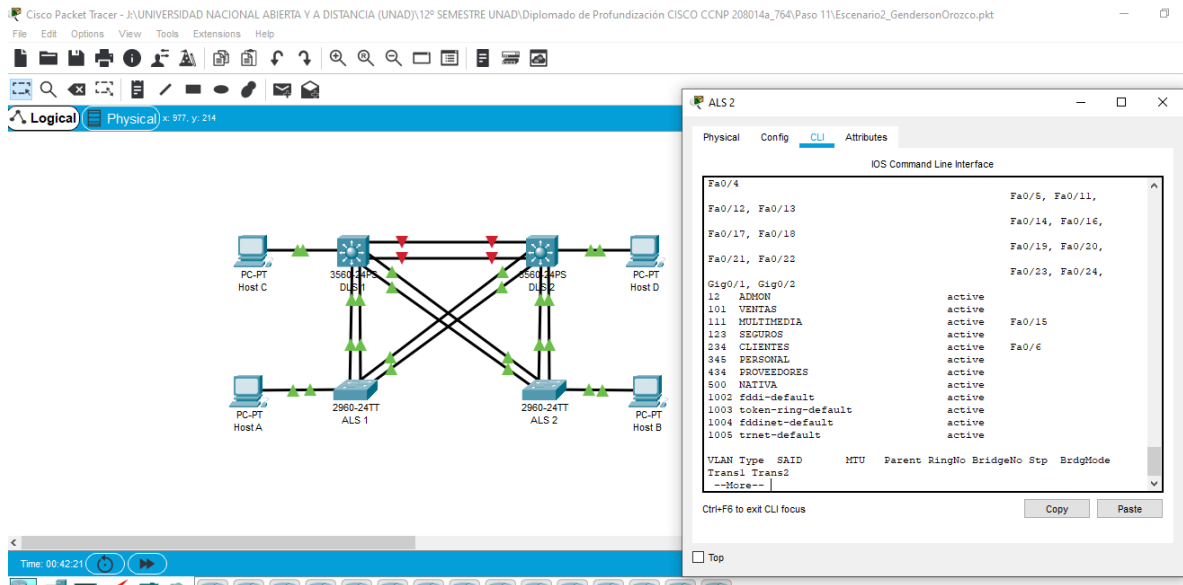


Figura 14. Verificación de las VLAN en ALS 2

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

Se utiliza el comando show etherchannel summary para observar y verificar la información solicitada.

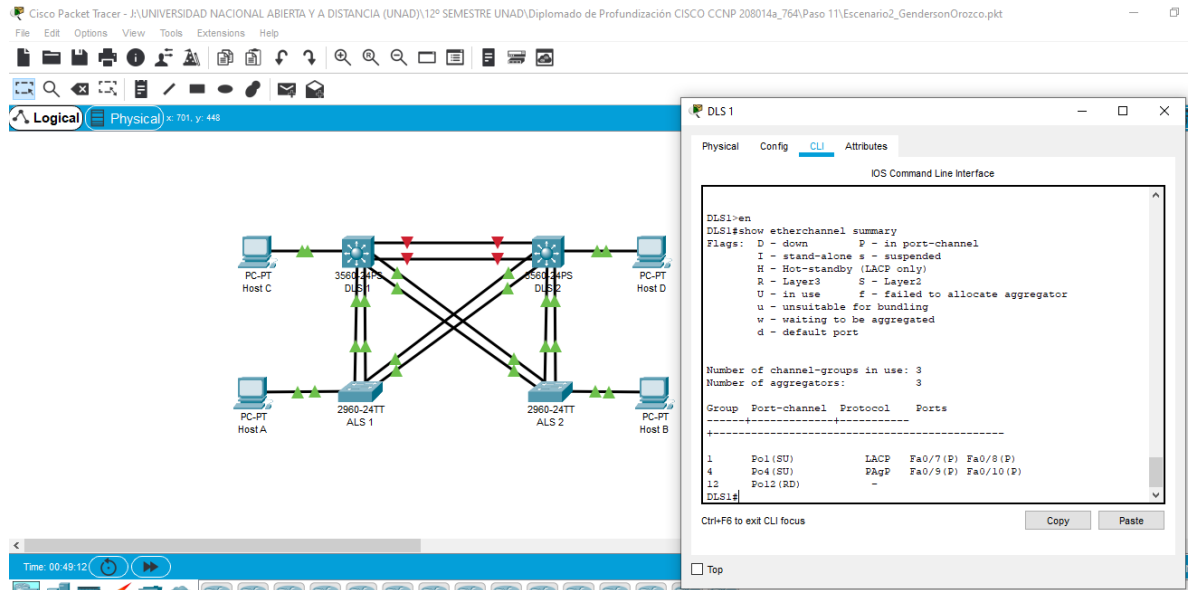


Figura 15. Verificación EtherChannel DLS 1.

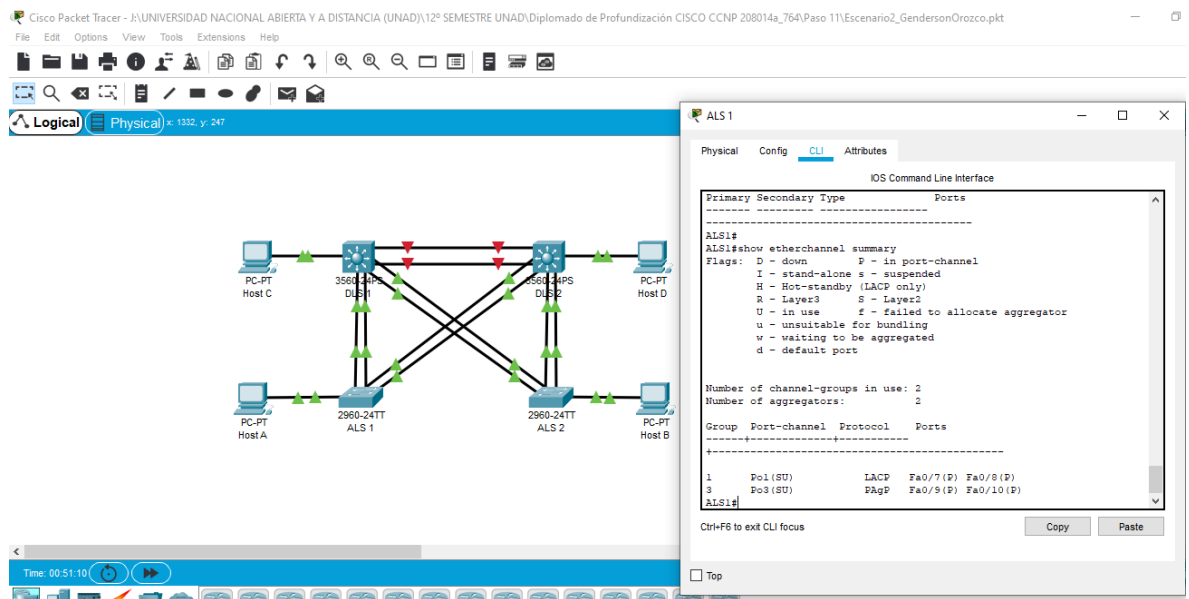


Figura 16. Verificación EtherChannel ALS 1.

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

Se utiliza el comando show spanning-tree para observar y verificar la información solicitada.

```

DLS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0030.F27D.C694
Cost 9
Port 28(Port-channel1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32769 sys-id-ext 1)
Address 00D0.583E.4D0C
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po4 Desg FWD 9 128.29 Shr
Po1 Root FWD 9 128.28 Shr

VLAN0013
Spanning tree enabled protocol ieee
Root ID Priority 24888
Address 00D0.583E.4D0C
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24888 (priority 24876 sys-id-ext 12)
Address 00D0.583E.4D0C
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/9 Desg FWD 19 128.9 P2p
Fa0/10 Desg FWD 19 128.10 P2p
Po4 Desg FWD 9 128.29 Shr
Po1 Desg FWD 9 128.28 Shr
  
```

Figura 17. Verificación show spanning-tree en DLS 1.

```

DLS2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0030.F27D.C694
Cost 9
Port 28(Port-channel13)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32769 sys-id-ext 1)
Address 00E0.F92B.1A87
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

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

VLAN0013
Spanning tree enabled protocol ieee
Root ID Priority 24888
Address 00D0.583E.4D0C
Cost 18
Port 29(Port-channel13)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24884 (priority 24672 sys-id-ext 12)
Address 00E0.F92B.1A87
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Root FWD 9 128.29 Shr
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/9 Desg FWD 19 128.9 P2p
Fa0/10 Desg FWD 19 128.10 P2p
  
```

Figura 18. Verificación show spanning-tree en DLS 2.

```

ALS1
Physical Config CLI Attributes
IDS Command Line Interface

ALS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0030.F27D.C594
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32769 sys-id-ext 1)
Address 0030.F27D.C594
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po3 Desg FWD 9 128.28 Shr
Po1 Desg FWD 9 128.27 Shr

VLAN0012
Spanning tree enabled protocol ieee
Root ID Priority 24588
Address 00D0.583E.4D0C
Cost 9
Port 27(Port-channel1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32780 (priority 32768 sys-id-ext 12)
Address 0030.F27D.C594
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Fa0/9 Desg FWD 19 128.5 P2p
Fa0/10 Desg FWD 19 128.10 P2p
Po3 Desg FWD 9 128.28 Shr
Po1 Root FWD 9 128.27 Shr

```

Figura 19. Verificación show spanning-tree en ALS 1

```

ALS2
Physical Config CLI Attributes
IDS Command Line Interface

ALS2#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0030.F27D.C594
Cost 19
Port 28(Port-channel14)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 00D0.FF6E.4304
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po4 Root FWD 9 128.28 Shr
Po2 Altn BLK 9 128.27 Shr

VLAN0012
Spanning tree enabled protocol ieee
Root ID Priority 24588
Address 00D0.583E.4D0C
Cost 9
Port 28(Port-channel14)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32780 (priority 32768 sys-id-ext 12)
Address 00D0.FF6E.4304
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Po4 Root FWD 9 128.28 Shr
Po2 Desg FWD 9 128.27 Shr
Fa0/10 Desg FWD 19 128.10 P2p
Fa0/7 Desg FWD 19 128.7 P2p
Fa0/8 Desg FWD 19 128.8 P2p

```

Figura 20. Verificación show spanning-tree en ALS 2

CONCLUSIONES

Se logra el objetivo de usar comandos IOS de configuración avanzada en routers (con direccionamiento IPv4 e IPv6) para protocolos de enrutamiento como: RIPng, OSPFv3, EIGRP y BGP, en entornos de direccionamiento sin clase, con el fin diseñar e implementar soluciones de red escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN. Se emplearon herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitieron realizar un análisis sobre el comportamiento de múltiples protocolos, evaluando el desempeño de los routers, mediante el uso de comandos de administración avanzados y bajo el uso de protocolos de vector distancia y estado enlace.

Se logra configurar plataformas de conmutación basadas en switches, mediante el uso de protocolos como STP y la configuración de VLANs en escenarios de red corporativos, para comprender el modo de operación de las subredes y los beneficios de administrar dominios de broadcast independientes, en múltiples escenarios al interior de una red jerárquica convergente. También se logra identificar situaciones problemáticas asociadas con aspectos de conmutación y enrutamiento, mediante el uso eficiente de estrategias basadas en comandos IOS y estadísticas de tráfico en las interfaces, con el fin de resolver conflictos de configuración y conectividad en contextos de redes LAN y WAN.

La implementación de VLAN en una red permite la optimización del tráfico de red, al separar a los usuarios en grupos con lo cual se puede tener una mejor administración. Al configurar una VLAN en un switch es importante tener en cuenta que éstas comparten el ancho de banda, por ello se requieren medidas de seguridad adicionales como la asignación de un número de VLAN nativo único a los puertos de enlace troncal, limitar las VLAN a transportar sobre los enlaces troncales, desactivar el protocolo de enlace troncal VTP, de lo contrario deben configurarse su dominio de gestión, contraseña y eliminación.

La utilización práctica de software especializado para la práctica nos brindó una mejor adaptación al entorno real y sabemos que Cisco Packet Tracer es una herramienta de simulación de redes innovadora y potente que se utiliza para prácticas, detecciones y resolución de problemas al igual que GNS3; un software utilizado a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. Nos permitió ejecutar desde una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube.

BIBLIOGRAFÍA

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

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-NT1InWR0hoMxgBNv1CJ>

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-NT1InWR0hoMxgBNv1CJ>

Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP [OVI]. Recuperado de <https://repository.unad.edu.co/handle/10596/24419>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Manipulating Routing Updates. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). OSPF Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Universidad nacional abierta y a distancia UNAD. (2020). Curso de Diplomado de Profundización Cisco CCNP. Syllabus del curso.

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de <http://hdl.handle.net/10596/24167>