

PRUEBA DE HABILIDADES CCNP 2020

JOHN FREDY PINEDA MONROY

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
IBAGUE-JULIO
2020

PRUEBA DE HABILIDADES CCNP 2020

JOHN FREDY PINEDA MONROY

Trabajo de grado para optar por el título de Ingeniero de Telecomunicaciones

PAULITA FLOR SALAZAR

Directora de curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
CIENCIAS BASICAS, DE LA TECNOLOGIA E INGENIERIA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
IBAGUE-JULIO
2020

Nota de Aceptación

Jurado

Jurado

Jurado

Ibagué, Tolima Julio 10 de 2020

AGRADECIMIENTOS

Agradezco a Dios por brindarme la oportunidad de llegar a esta etapa de mi proceso de formación profesional, a mi familia por su valioso apoyo durante mi proceso de aprendizaje, de igual forma agradezco al cuerpo de docentes de la Universidad Nacional Abierta y a Distancia UNAD por la orientación brindada.

TABLA DE CONTENIDO

INTRODUCCION	12
OBJETIVOS.....	13
General	13
Específicos.....	13
DESCRIPCION DE LOS ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES.....	14
ESCENARIO 1.....	14
Parte 1. Configuración del escenario propuesto	15
Parte 2. Verificar la conectividad de red y control de la trayectoria.....	22
ESCENARIO 2.....	31
Parte 1. Configuración de la red de acuerdo con las especificaciones	31
Parte 2. Conectividad de la red de prueba y las opciones configuradas.....	45
CONCLUSIONES	54
BIBLIOGRAFIA.....	55
ANEXO	56

LISTA DE FIGURAS

Figura 1. Topología de Red del Escenario 1	14
Figura 2. Tablas de Enrutamiento en R1	23
Figura 3. Tablas de Enrutamiento en R2	23
Figura 4. Tablas de Enrutamiento en R3	24
Figura 5. Verificación de conectividad desde R1 a R2 y R3	24
Figura 6. Verificación de conectividad desde R2 a R1 y R3	25
Figura 7. Verificación de conectividad desde R3 a R1 y R2	25
Figura 8. Archivo de configuración activo en R1. (Parte 1).....	26
Figura 9. Archivo de configuración activo en R1. (Parte 2).....	27
Figura 10. Archivo de configuración activo en R1. (Parte 3).....	27
Figura 11. Archivo de configuración activo en R2. (Parte 1).....	28
Figura 12. Archivo de configuración activo en R2. (Parte 2).....	28
Figura 13. Archivo de configuración activo en R2. (Parte 3).....	29
Figura 14. Archivo de configuración activo en R3. (Parte 1).....	29
Figura 15. Archivo de configuración activo en R3. (Parte 2).....	30
Figura 16. Archivo de configuración activo en R3. (Parte 3).....	30
Figura 17. Topología de Red del Escenario 2.....	31
Figura 18. VLANS existentes en DLS1	45
Figura 19. VLANS existentes en DLS2	46
Figura 20. VLANS existentes en ALS1	46
Figura 21. VLANS existentes en ALS2	47
Figura 22. Etherchannel en DLS1	47
Figura 23. Etherchannel en ALS1	48
Figura 24. Verificación de la configuración de STP en DLS1. (Parte 1).....	48
Figura 25. Verificación de la configuración de STP en DLS1. (Parte 2).....	49
Figura 26. Verificación de la configuración de STP en DLS1. (Parte 3).....	49
Figura 27. Verificación de la configuración de STP en DLS1. (Parte 4).....	50
Figura 28. Verificación de la configuración de STP en DLS1. (Parte 5).....	50
Figura 29. Verificación de la configuración de STP en DLS2. (Parte 1).....	51
Figura 30. Verificación de la configuración de STP en DLS2. (Parte 2).....	51
Figura 31. Verificación de la configuración de STP en DLS2. (Parte 3).....	52
Figura 32. Verificación de la configuración de STP en DLS2. (Parte 4).....	52
Figura 33. Verificación de la configuración de STP en DLS2. (Parte 5).....	53

LISTA DE TABLAS

Tabla 1. Configuración Básica de Interfaces	15
Tabla 2. Ajuste del ancho de banda.....	17
Tabla 3. Familias de direcciones OSPFv3	17
Tabla 4. Configuración de Interfaces en R2.....	18
Tabla 5. Configuración de Interfaces en R3.....	18
Tabla 6. Configuración del área 1	19
Tabla 7. Propagación de rutas en R3 en el dominio OSPF	19
Tabla 8. Configuración del protocolo EIGRP	20
Tabla 9. Configuración de interfaces pasivas para EIGRP	21
Tabla 10. Redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6	22
Tabla 11. Asignación de nombre y apagado de interfaces	32
Tabla 12. Conexión entre DLS1 y DLS2	33
Tabla 13. Port-channels en interfaces Fa0/7 y Fa0/8 utilizando LACP	33
Tabla 14. Port-channels en interfaces Fa0/7 y Fa0/8 utilizando PAgP	34
Tabla 15. Asignación de troncales a la VLAN 800	35
Tabla 16. Configuración en DLS1 para utilizar VTPv2.....	36
Tabla 17. DLS1 servidor principal para las VLANS.....	37
Tabla 18. Configuración de ALS1 y ALS2 como clientes VTP	37
Tabla 19. Configuración de VLANS en el servidor principal	38
Tabla 20. Configuración de VLANS en DLS1	38
Tabla 21. Suspensión de la VLAN 434 en DLS1	39
Tabla 22. Configuración de VLANS en DLS2	39
Tabla 23. Suspensión de la VLAN 434 en DLS2	40
Tabla 24. Creación de la VLAN 567 en DLS2.....	40
Tabla 25. Configuración de Spanning tree root en DLS1.....	41
Tabla 26. Configuración de Spanning tree root en DLS2.....	41
Tabla 27. Configuración de los puertos troncales	42
Tabla 28. Asignación de interfaces como puertos de acceso a las VLANS	43
Tabla 29. Asignación de puertos de acceso a las VLANS	43

GLOSARIO

EIGRP: Es utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI) como un protocolo de enrutamiento del tipo vector distancia avanzado, propiedad de Cisco. El concepto es que cada router sólo conoce la dirección (dirección de próximo salto) y la distancia (métrica) hacia cada red remota.

IPv4: Una dirección IPv4 es un número de 32 bits formado por cuatro octetos (números de 8 bits) en una notación decimal, separados por puntos. Un bit puede ser tanto un 1 como un 0 (2 posibilidades), Los posibles valores de un octeto en una dirección IP van de 0 a 255.

IPv6: Protocolo de capa de red para trabajos de Internet conmutados por paquetes. Sucesor de IPv4 para uso general en Internet. Las direcciones IPv6 están basadas en 128 bits.

LACP: Es similar a PAgP ya que también puede agrupar puertos con características similares. Es un protocolo definido en el estándar 802.3ad.

OSPF: (Open Shortest Path First). Protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF).

PAgP: Protocolo de Cisco. El switch negocia con el otro extremo cuales son los puertos que deben ponerse activos. El propio protocolo se encarga de agrupar puertos con características similares.

ROUTER: Dispositivo que proporciona conectividad a nivel de la capa 3 de modelo OSI. Su función es enviar paquetes de datos de una red a otra.

SWITCH: Dispositivo diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes y reducir tiempo de espera.

VLAN: Red de área local virtual (Virtual LAN) agrupa lógicamente dispositivos en un mismo dominio de broadcast, creando lógicamente distintas redes como si fueran distintas redes físicas.

VTP: Dominio de gestión de VLAN. Un conmutador puede estar en un solo dominio VTP, y el contenido de la base de datos de la VLAN en el dominio está sincronizado globalmente. La información de la VLAN no se propaga hasta que se especifica un nombre de dominio y se establecen troncales entre los dispositivos.

RESUMEN

Para el proceso de la prueba de habilidades en el desarrollo del escenario 1 se utilizó la herramienta de simulación GNS3 sobre una imagen IOS Cisco C7200 de línea principal con el fin de reconocer el protocolo ospfv3 y la direccionamiento familia OSPFv3 con la familia de direcciones (AF) que unifica la configuración de OSPF tanto para IPv4 como para IPv6.

En el escenario 2 se utilizó la herramienta de simulación desarrollada por CISCO Packet Tracer. Se configuran los protocolos PAgP, EtherChannel de Cisco, y el protocolo LACP. LACP y PAgP son protocolos que permiten a dos conmutadores negociar el uso de puertos físicos seleccionados como miembros de un único paquete EtherChannel.

Abstract

For the process of the skills test in the development of scenario 1, the simulation tool GNS3 on an IOS Cisco C7200 main line image was used in order to recognize the ospfv3 protocol and the OSPFv3 family addressing with the address family (AF) that unifies the OSPF configuration for both IPv4 and IPv6.

In scenario 2 the simulation tool developed by CISCO Packet Tracer was used. The PAgP, Cisco EtherChannel, and LACP protocols are configured. LACP and PAgP are protocols that allow two switches to negotiate the use of selected physical ports as members of a single EtherChannel packet.

PALABRAS CLAVES

Summary: Permite a la función de enrutamiento de EIGRP enviar rutas de resumen.

Passive-interface: Modo de configuración del router para evitar la transmisión de mensajes de routing a través de una interfaz del router, pero sin dejar de permitir que se anuncie esa red a otros routers.

Redistributed: Permite que la función de enrutamiento de la EIGRP envíe otros protocolos de enrutamiento y sistemas autónomos. Sin la configuración de esta opción, EIGRP no anunciará las rutas redistribuidas.

Unicast: El tráfico es dirigido hacia un único equipo en la red.

Multicast: El tráfico es dirigido hacia un grupo de equipos en la red.

INTRODUCCIÓN

El entorno de las redes de voz y datos es cada vez mayor y es por eso que surgen nuevos protocolos de enrutamiento para la implementación de redes más extensas. Se desarrollaron protocolos de enrutamiento avanzados IGRP y EIGRP desarrollados por CISCO y surge también OSPF que puede ser utilizado por equipos que no pertenezcan a la marca CISCO. Así mismo también surge la necesidad de interconectar estos protocolos.

La presente actividad se desarrolla teniendo en cuenta la descripción detallada de la prueba de habilidades del curso del diplomado de profundización CISCO CCNP donde se abordan los protocolos de ruteo (OSPFv3-EIGRP), y la aplicación de tecnologías que mejoran la eficacia de la red como lo es Etherchannel para crear enlaces troncales. La prueba está conformada por dos escenarios, para el proceso de configuración en el primer escenario se hace uso de la herramienta de simulación GNS3 y en el segundo escenario se utiliza Packet Tracer.

OBJETIVOS

General

Profundizar los conocimientos adquiridos en los cursos CCNA Routing y Switching, desarrollando los protocolos de enrutamiento exteriores e interiores tales como, IGP, EIGRP y OSPF en diferentes tecnologías de red, utilizando listas de distribución y redistribución de enrutamiento.

Específicos

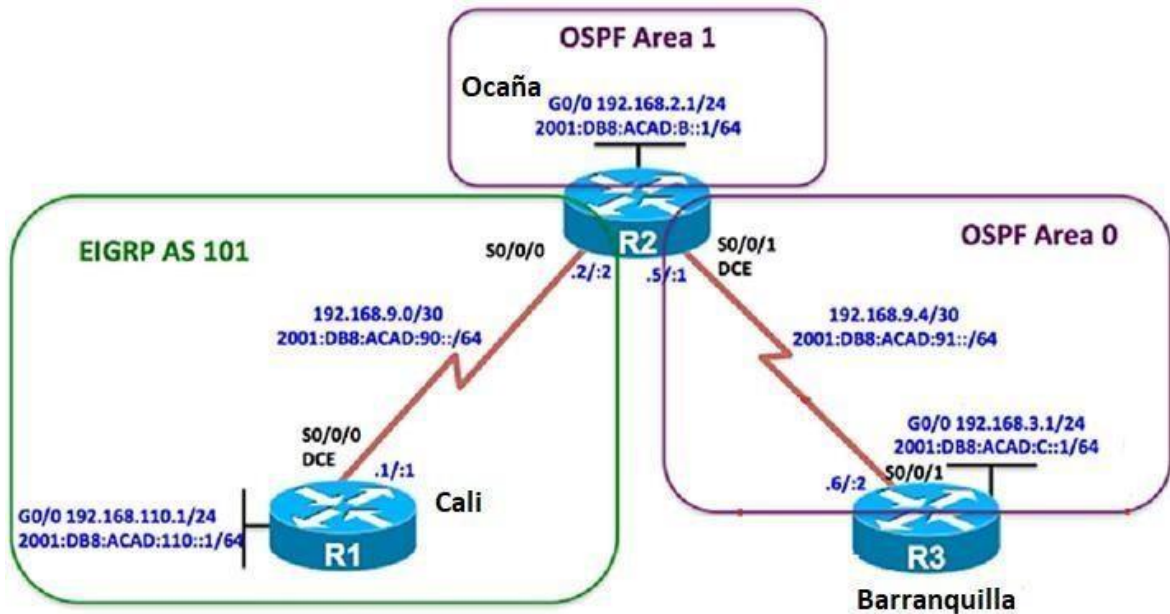
- Configurar EIGRP para IPV4 e IPV6
- Configurar y verificar las rutas pasivas usando EIGRP
- Configurar un dominio VTP v2
- Crear VLANs
- Crear enlaces de EtherChannel
- Configurar el protocolo de Agregación de Puertos (PAgP)
- Configurar el protocolo de Control de Agregación de Enlaces (LACP)
- Asignar interfaces como puertos de acceso a las a las VLAN creadas
- Verificar la configuración y el funcionamiento utilizando comandos de visualización

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

Una empresa de confecciones posee tres sucursales distribuidas en las ciudades de Cali, Barranquilla y Ocaña, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Figura 1. Topología de Red del Escenario 1



Parte 1. Configuración del Escenario Propuesto

Configurar las interfaces con las direcciones IPv4 e IPv6 que se muestran en la topología de red.

A continuación se relacionan los comandos de configuración básica para asignación del direccionamiento ipv4 e ipv6 en las interfaces seriales y Ethernet.

Tabla 1. Configuración Básica de Interfaces

Dispositivo	Configuración Básica de Interfaces IPv4-IPv6
R1 CALI	<pre> CALI# config t CALI (config) # interface s3/0 CALI (config-if) # ip address 192.168.9.1 255.255.255.252 CALI (config-if) # no shutdown CALI (config) # interface g1/0 CALI (config-if) # ip address 192.168.110.1 255.255.255.0 CALI (config-if) # no shutdown CALI (config-if) # exit CALI (config) # ipv6 unicast-routing CALI (config) # interface s3/0 CALI (config-if) # ipv6 address 2001:DB8:ACAD:90::1/64 CALI (config-if) # ipv6 address FE80::1 link-local CALI (config-if) # no shutdown CALI (config-if) # interface g1/0 CALI (config-if) # ipv6 address 2001:DB8:ACAD:110::1/64 CALI (config-if) # ipv6 address FE80::1 link-local CALI (config-if) # no shutdown CALI (config-if) # exit CALI (config) # exit CALI# copy running-config startup-config </pre>
R2 OCAÑA	<pre> OCAÑA# config t OCAÑA (config) # interface s3/0 OCAÑA (config-if) # ip address 192.168.9.2 255.255.255.252 OCAÑA (config-if) # no shutdown OCAÑA (config) # interface s3/1 OCAÑA (config-if) # ip address 192.168.9.5 255.255.255.252 OCAÑA (config-if) # no shutdown OCAÑA (config) # interface g1/0 OCAÑA (config-if) # ip address 192.168.2.1 255.255.255.0 OCAÑA (config-if) # no shutdown OCAÑA (config-if) # exit OCAÑA (config) # ipv6 unicast-routing OCAÑA (config) # interface s3/0 OCAÑA (config-if) # ipv6 address 2001:DB8:ACAD:90::2/64 OCAÑA (config-if) # ipv6 address FE80::2 link-local </pre>

	<pre>OCAÑA (config-if) # no shutdown OCAÑA (config-if) # interface s3/1 OCAÑA (config-if) # ipv6 address 2001:DB8:ACAD:91::1/64 OCAÑA (config-if) # ipv6 address FE80::2 link-local OCAÑA (config-if) # no shutdown OCAÑA (config-if) # interface g1/0 OCAÑA (config-if) # ipv6 address 2001:DB8:ACAD:8::1/64 OCAÑA (config-if) # ipv6 address FE80::2 link-local OCAÑA (config-if) # no shutdown OCAÑA (config-if) # exit OCAÑA (config) # exit OCAÑA# copy running-config startup-config</pre>
<p>R3 BARRANQUILLA</p>	<pre>BARRANQUILLA# config t BARRANQUILLA (config) # interface s3/1 BARRANQUILLA(config-if)# ip address 192.168.9.6 255.255.255.252 BARRANQUILLA (config-if) # no shutdown BARRANQUILLA (config) # interface g1/0 BARRANQUILLA(config-if)# ip address 192.168.3.1 255.255.255.0 BARRANQUILLA (config-if) # no shutdown BARRANQUILLA (config-if) # exit BARRANQUILLA (config) # ipv6 unicast-routing BARRANQUILLA (config) # interface s3/1 BARRANQUILLA(config-if)#ipv6address 2001:DB8:ACAD:91::2/64 BARRANQUILLA (config-if) # ipv6 address FE80::3 link-local BARRANQUILLA (config-if) # no shutdown BARRANQUILLA (config-if) # interface g1/0 BARRANQUILLA(config-if)# ipv6 address 2001:DB8:ACAD:C::1/64 BARRANQUILLA (config-if) # ipv6 address FE80::3 link-local BARRANQUILLA (config-if) # no shutdown BARRANQUILLA (config-if) # exit BARRANQUILLA (config) # exit BARRANQUILLA# copy running-config startup-config</pre>

Ajustar el ancho de banda a 128 kbps sobre cada uno de los enlaces seriales ubicados en R1, R2, y R3 y ajustar la velocidad de reloj de las conexiones de DCE según sea apropiado.

Con los siguientes comandos se ajusta el ancho de banda a 128kbps. Si tiene interfaces seriales WIC-2A/S, la máxima velocidad de reloj es de 128 kb/s. las interfaces seriales WIC-2T, la máxima velocidad es más alta 2.048 Mb/s o más.

Tabla 2. Ajuste del ancho de banda

Dispositivo	Ajuste del ancho de banda a 128 kbps
R1 CALI	CALI# config t CALI (config) # interface s3/0 CALI (config-if) # clock rate 128000 CALI (config-if) # bandwidth 128 CALI (config-if) # exit CALI (config) # exit CALI# copy running-config startup-config
R2 OCAÑA	OCAÑA# config t OCAÑA (config) # interface s3/0 OCAÑA (config-if) # bandwidth 128 OCAÑA (config-if) # exit OCAÑA (config) # interface s3/1 OCAÑA (config-if) # clock rate 128000 OCAÑA (config-if) # bandwidth 128 OCAÑA (config-if) # exit OCAÑA (config) # exit OCAÑA# copy running-config startup-config
R3 BARRANQUILLA	BARRANQUILLA# config t BARRANQUILLA (config) # interface s3/1 BARRANQUILLA (config-if) # bandwidth 128 BARRANQUILLA (config-if) # exit BARRANQUILLA (config) # exit BARRANQUILLA# copy running-config startup-config

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

A continuación se relacionan los comandos para la configuración de las familias de direcciones OSPF, se utiliza el comando **router-id** para configurar el ID del router.

Tabla 3. Familias de direcciones OSPFv3

Dispositivo	Familias de direcciones OSPFv3 para IPv4 e IPv6
R2 OCAÑA	OCAÑA# config t OCAÑA (config) # ipv6 unicast-routing OCAÑA (config) # router ospfv3 1 OCAÑA (config-router) # address-family ipv4 unicast OCAÑA (config-router-af) # router-id 2.2.2.2 OCAÑA (config-router-af) # exit-address-family OCAÑA (config-router) # address-family ipv6 unicast OCAÑA (config-router-af) # router-id 2.2.2.2 OCAÑA (config-router-af) # exit-address-family OCAÑA (config-router) #exit

	OCAÑA (config) # exit OCAÑA# copy running-config startup-config
R3 BARRANQUILLA	BARRANQUILLA# config t BARRANQUILLA (config) # ipv6 unicast-routing BARRANQUILLA (config) # router ospfv3 1 BARRANQUILLA (config-router) # address-family ipv4 unicast BARRANQUILLA (config-router-af) # router-id 3.3.3.3 BARRANQUILLA (config-router-af) # exit-address-family BARRANQUILLA (config-router) # address-family ipv6 unicast BARRANQUILLA (config-router-af) # router-id 3.3.3.3 BARRANQUILLA (config-router-af) # exit-address-family BARRANQUILLA (config-router) #exit BARRANQUILLA (config) # exit BARRANQUILLA# copy running-config startup-config

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

En esta etapa utilizamos el comando de **network** en el modo de configuración del enrutador para configurar la interfaces seriales y Ethernet en el área determinada del protocolo OSPF.

Tabla 4. Configuración de Interfaces en R2

Dispositivo	Configuración de las interfaces seriales y LAN de R2
R2 OCAÑA	OCAÑA# config t OCAÑA (config) # router ospf 1 OCAÑA (config-router) # network 192.168.9.0 0.0.0.3 area 0 OCAÑA (config-router) # network 192.168.2.0 0.0.0.255 area 1 OCAÑA (config-router) # exit OCAÑA (config) # exit OCAÑA# copy running-config startup-config

En R3, configurar la interfaz F0/0 y la conexión serial entre R2 y R3 en OSPF área0.

Tabla 5. Configuración de Interfaces en R3

Dispositivo	Configuración de las interfaces seriales y LAN de R3
R3 BARRANQUILLA	BARRANQUILLA# config t BARRANQUILLA (config) # router ospf 1 BARRANQUILLA (config-router) # network 192.168.9.0 0.0.0.3 area 0 BARRANQUILLA (config-router) # network 192.168.3.0 0.0.0.255

	<pre> area 0 BARRANQUILLA (config-router) # exit BARRANQUILLA (config) # exit BARRANQUILLA# copy running-config startup-config </pre>
--	---

Configurar el área 1 como un área totalmente Stubby

Se utiliza el comando **no-summary** para mostrarle al router que el área 1 no recibir rutas sumarias.

Tabla 6. Configuración del área 1

Dispositivo	Configuración del área 1 totalmente Stubby
R2 OCAÑA	<pre> OCAÑA# config t OCAÑA (config) # router ospf 1 OCAÑA (config-router) # area 1 nssa no-summary OCAÑA (config-router) # exit OCAÑA (config) # exit OCAÑA# copy running-config startup-config </pre>
R3 BARRANQUILLA	<pre> BARRANQUILLA# config t BARRANQUILLA (config) # router ospf 1 BARRANQUILLA (config-router) # area 1 nssa no-summary BARRANQUILLA (config-router) # exit BARRANQUILLA (config) # exit BARRANQUILLA# copy running-config startup-config </pre>

Propagar rutas por defecto de IPv4 e IPv6 en R3 al interior del dominio OSPFv3.

A continuación se relacionan los comandos para propagar las rutas tanto en ipv4 como ipv6 en el dominio OSPFv3. El comando **default-information originate** establece las rutas predeterminadas a los routers vecinos.

Tabla 7. Propagación de rutas en R3 en el dominio OSPF

Dispositivo	Propagación de rutas por defecto en R3 en el dominio OSPF
R3	<pre> BARRANQUILLA# config t BARRANQUILLA (config) # ipv6 unicast-routing BARRANQUILLA (config) # router ospfv3 1 BARRANQUILLA (config-router) # address-family ipv4 unicast BARRANQUILLA (config-router-af) # default-information originate BARRANQUILLA (config-router-af) # exit-address-family BARRANQUILLA (config-router) # address-family ipv6 unicast </pre>

BARRANQUILLA	<pre> BARRANQUILLA (config-router-af)# default-information originate BARRANQUILLA (config-router-af) # exit-address-family BARRANQUILLA (config-router-af) # exit BARRANQUILLA (config-router) # exit BARRANQUILLA (config) # exit BARRANQUILLA# copy running-config startup-config </pre>
--------------	--

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

A continuación se relacionan los comandos para configurar el protocolo EIGRP, ya teniendo la familia de direcciones definida el protocolo EIGRP puede iniciar en el sistema autónomo definido. Utilizamos el comando **address-family ipv4 unicast autonomous-system 4**. Este comando le pone en el modo de configuración de la familia de direcciones.

Tabla 8. Configuración del protocolo EIGRP

Dispositivo	Configuración del protocolo EIGRP para IPv4-IPv6 en R1
R1 CALI	<pre> CALI# config t CALI (config) # ipv6 unicast-routing CALI (config) # router eigrp DUAL-STACK CALI (config-router) #address-family ipv4 unicast autonomous- system 4 CALI (config-router-af) # eigrp router-id 1.1.1.1 CALI (config-router-af) # network 192.168.110.0 CALI (config-router-af) # network 192.168.9.0 0.0.0.3 CALI (config-router-af) # exit-address-family CALI (config-router) #address-family ipv6 unicast autonomous- system 6 CALI (config-router-af) # eigrp router-id 1.1.1.1 CALI (config-router-af) # exit-address-family CALI (config-router) # exit CALI (config) # exit CALI# copy running-config startup-config </pre>

Configurar la interfaces pasivas para EIGRP según sea apropiado.

Se utiliza el comando **af-interface** para entrar en el modo de configuración de la interfaz de la familia de direcciones y el comando **passive-interface** para configurar las interfaces LAN por donde no se va a propagar tablas de enrutamiento es decir la vamos a configurar como pasiva para la familia de direcciones EIGRP IPv4 e IPv6.

Tabla 9. Configuración de interfaces pasivas para EIGRP

Dispositivo	Configuración Interfaces Pasivas en R1
R1 CALI	<pre> CALI# config t CALI (config) # router eigrp DUAL-STACK CALI (config-router) #address-family ipv4 unicast autonomous- system 4 CALI (config-router-af) # af-interface g1/0 CALI (config-router-af-interface) # passive-interface CALI (config-router-af-interface) # exit-af-interface CALI (config-router-af) # exit-address-family CALI (config-router) #address-family ipv6 unicast autonomous- system 6 CALI (config-router-af) # af-interface g1/0 CALI (config-router-af-interface) # passive-interface CALI (config-router-af-interface) # exit-af-interface CALI (config-router-af) # exit-address-family CALI (config-router) # exit CALI (config) # exit CALI# copy running-config startup-config </pre>

En R2, configurar la redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6. Asignar métricas apropiadas cuando sea necesario.1

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

A continuación se relaciona la serie de comandos para configurar la redistribución mutua entre OSPF y EIGRP utilizando el comando **topología base** para introducir la topología base del EIGRP.

Tabla 10. Redistribución mutua entre OSPF y EIGRP para IPv4 e IPv6

Dispositivo	Configuración la redistribución mutua entre OSPF y EIGRP en R2
R2 OCAÑA	<pre> OCAÑA# config t OCAÑA (config) # router eigrp DUAL-STACK OCAÑA(config-router)#address-family ipv4 unicast autonomous- system 4 OCAÑA (config-router-af) # topology base OCAÑA(config-router-af-topology)#distribute-list BARRANQUILLA- to-CALI out OCAÑA (config-router-af-topology) # redistribute ospfv3 1 metric 10000 100 255 1 1500 OCAÑA (config-router-af-topology) # exit-af-topology OCAÑA(config-router-af)#address-family ipv6 unicast autonomous- system 6 OCAÑA (config-router-af) # topology base OCAÑA (config-router-af-topology) # redistribute ospf 1 metric 10000 100 255 1 1500 OCAÑA (config-router-af-topology) # exit-af-topology OCAÑA (config-router) # exit OCAÑA(config-router)# ip access-list standard BARRANQUILLA- to-CALI OCAÑA (config-std-nacl) #remark ACL to filter 192.168.3.0/24 OCAÑA (config-std-nacl) #deny 192.168.3.0 0.0.0.255 OCAÑA (config-std-nacl) #permit any OCAÑA (config-std-nacl) # exit OCAÑA (config) # exit OCAÑA# copy running-config startup-config </pre>

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

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

En esta etapa utilizamos comandos **show ip route** para Ipv4 y **show ipv6 route** para Ipv6 para verificar la conectividad de red y el control de trayectoria.

Figura 2. Tablas de Enrutamiento en R1

```
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#
*May 26 20:50:15.207: %QUAL-5-NBRCHANGE: EIGRP-IPv6 0: Neighbor FE80::2 (Serial3/0) is up: new adjacency
CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       * - replicated route, % - next hop override

Gateway of last resort is not set

 192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
   C   192.168.9.0/30 is directly connected, Serial3/0
   L   192.168.9.1/32 is directly connected, Serial3/0
   C   192.168.110.0/24 is variably subnetted, 2 subnets, 2 masks
   C   192.168.110.0/24 is directly connected, GigabitEthernet1/0
   L   192.168.110.1/32 is directly connected, GigabitEthernet1/0
CALI#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, O - EIGRP, EX - EIGRP external, NW - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
D 2001:DB8:ACAD:8::/64 [90/50245120]
   via FE80::2, Serial3/0
C 2001:DB8:ACAD:90::/64 [0/0]
   via Serial3/0, directly connected
L 2001:DB8:ACAD:90:1/128 [0/0]
   via Serial3/0, receive
D 2001:DB8:ACAD:91::/64 [90/60480000]
   via FE80::2, Serial3/0
C 2001:DB8:ACAD:118::/64 [0/0]
   via GigabitEthernet1/0, directly connected
L 2001:DB8:ACAD:118:1/128 [0/0]
   via GigabitEthernet1/0, receive
L FF00::/8 [0/0]
   via Null0, receive
CALI#
```

Diseño propio herramienta de simulación GNS3-2.2.2

Figura 3. Tablas de Enrutamiento en R2

```
OCAÁ#
OCAÁ#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       * - replicated route, % - next hop override

Gateway of last resort is not set

 192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
   C   192.168.2.0/24 is directly connected, GigabitEthernet1/0
   L   192.168.2.1/32 is directly connected, GigabitEthernet1/0
   C   192.168.9.0/24 is variably subnetted, 4 subnets, 2 masks
   C   192.168.9.0/30 is directly connected, Serial3/0
   L   192.168.9.2/32 is directly connected, Serial3/0
   C   192.168.9.4/30 is directly connected, Serial3/1
   L   192.168.9.5/32 is directly connected, Serial3/1
OCAÁ#show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, O - EIGRP, EX - EIGRP external, NW - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
C 2001:DB8:ACAD:8::/64 [0/0]
   via GigabitEthernet1/0, directly connected
L 2001:DB8:ACAD:8:1/128 [0/0]
   via GigabitEthernet1/0, receive
C 2001:DB8:ACAD:90::/64 [0/0]
   via Serial3/0, directly connected
L 2001:DB8:ACAD:90:12/128 [0/0]
   via Serial3/0, receive
C 2001:DB8:ACAD:91::/64 [0/0]
   via Serial3/1, directly connected
L 2001:DB8:ACAD:91:1/128 [0/0]
   via Serial3/1, receive
D 2001:DB8:ACAD:118::/64 [90/50245120]
   via FE80::1, Serial3/0
L FF00::/8 [0/0]
   via Null0, receive
OCAÁ#
```

Diseño propio herramienta de simulación GNS3-2.2.2

Figura 4. Tablas de Enrutamiento en R3

```
BARRANQUILLA
BARRANQUILLA(config-router-af)#exit-address-family
BARRANQUILLA(config-router)#exit
BARRANQUILLA(config)#exit
BARRANQUILLA#copy running-config startup-config
*May 26 20:25:06.223: %SYS-5-CONFIG I: Configured from console by console
BARRANQUILLA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BARRANQUILLA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet1/0
L       192.168.3.1/32 is directly connected, GigabitEthernet1/0
L       192.168.9.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.9.4/30 is directly connected, Serial3/1
L       192.168.9.6/32 is directly connected, Serial3/1
BARRANQUILLA#show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
        H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
        IS - ISIS summary, O - EIGRP, EX - EIGRP external, NH - NHOP
        ND - ND Default, ND0 - ND Prefix, DCE - Destination, DR - Redirect
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
C       2001:DB8:ACAD:C::/64 [0/0]
        via GigabitEthernet1/0, directly connected
L       2001:DB8:ACAD:C::1/128 [0/0]
        via GigabitEthernet1/0, receive
C       2001:DB8:ACAD:91::/64 [0/0]
        via Serial3/1, directly connected
L       2001:DB8:ACAD:91::2/128 [0/0]
        via Serial3/1, receive
L       FF00::/8 [0/0]
        via Null0, receive
BARRANQUILLA#
```

Diseño propio herramienta de simulación GNS3-2.2.2

Verificar comunicación entre routers mediante el comando ping y traceroute

Figura 5. Verificación de conectividad desde R1 a R2 y R3

```
CALI
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/109/144 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:8::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/100/148 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CALI(tcl)#foreach ips {
+>192.168.9.2
+>192.168.110.1
+>2001:DB8:ACAD:110::1
+>2001:DB8:ACAD:90::2
+>2001:DB8:ACAD:91::1
+>2001:DB8:ACAD:8::1
+>}
+ping $ips
+>}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/176/280 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:110::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:90::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/92/180 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:91::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/120/212 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:8::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/94/188 ms
CALI(tcl)#
CALI(tcl)#
CALI(tcl)#
```

Diseño propio herramienta de simulación GNS3-2.2.2

Figura 6. Verificación de conectividad desde R2 a R1 y R3

```
OCAÁA
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:91::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/151/208 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:C::1, timeout is 2 seconds:
.....

% No valid route for destination
Success rate is 0 percent (0/1)
OCAÑA(tcl)#foreach ips {
+>192.168.9.1
+>2001:DB8:ACAD:90::1
+>2001:DB8:ACAD:110::1
+>192.168.9.6
+>2001:DB8:ACAD:91::2
+>2001:DB8:ACAD:C::1
+>} {
+>ping $ips
+>}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/148/360 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:90::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/141/228 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:110::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/136/188 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/151/268 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:91::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/72/108 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:C::1, timeout is 2 seconds:
.....

% No valid route for destination
Success rate is 0 percent (0/1)
OCAÑA(tcl)#
```

Diseño propio herramienta de simulación GNS3-2.2.2

Figura 7. Verificación de conectividad desde R3 a R1 y R2

```
BARRANQUILLA
+>ping $ips
+>}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:90::1, timeout is 2 seconds:
.....

% No valid route for destination
Success rate is 0 percent (0/1)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:110::1, timeout is 2 seconds:
.....

% No valid route for destination
Success rate is 0 percent (0/1)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/105/212 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:90::2, timeout is 2 seconds:
.....

% No valid route for destination
Success rate is 0 percent (0/1)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:91::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/116/172 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:8::1, timeout is 2 seconds:
.....

% No valid route for destination
Success rate is 0 percent (0/1)
BARRANQUILLA(tcl)#
```

Diseño propio herramienta de simulación GNS3-2.2.2

Figura 9. Archivo de configuración activo en R1. (Parte 2)

```
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface GigabitEthernet1/0
ip address 192.168.110.1 255.255.255.0
negotiation auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:110::1/64
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface Serial3/0
bandwidth 128
ip address 192.168.9.1 255.255.255.252
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:90::1/64
serial restart-delay 0
clock rate 128000
!
interface Serial3/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/2
no ip address
shutdown
--More--
```

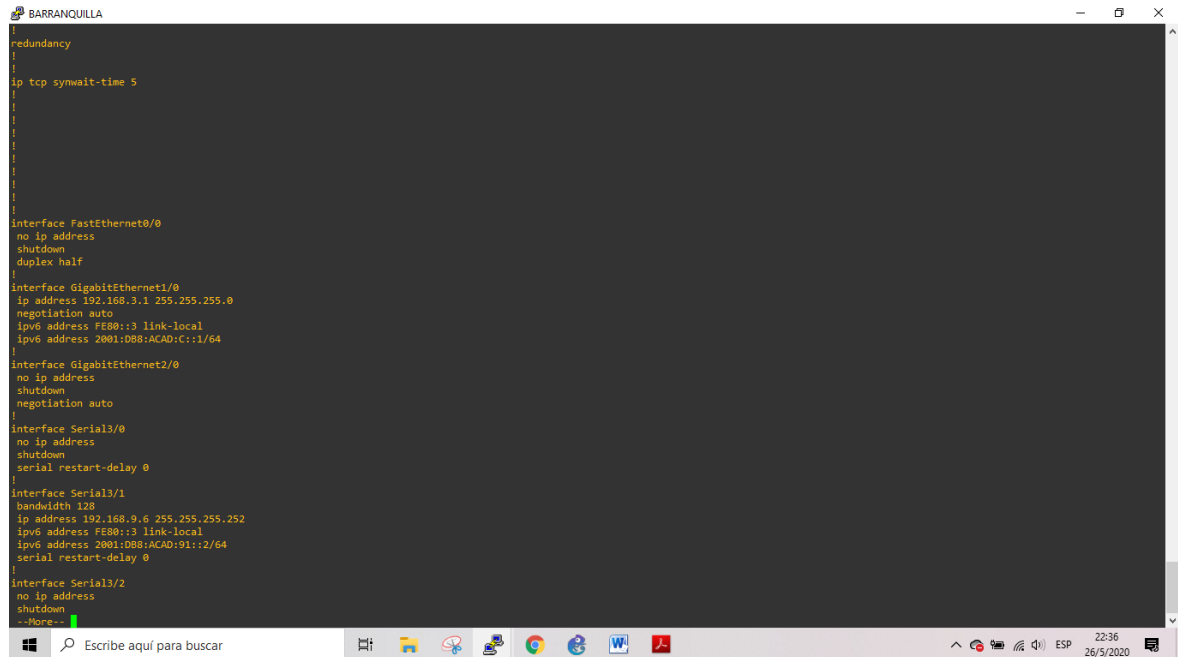
Diseño propio herramienta de simulación GNS3-2.2.2

Figura 10. Archivo de configuración activo en R1. (Parte 3)

```
interface Serial3/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
!
router eigrp DUAL-STACK
!
address-family ipv4 unicast autonomous-system 4
!
af-interface GigabitEthernet1/0
passive-interface
exit-af-interface
!
topology base
exit-af-topology
network 192.168.9.0 0.0.0.3
network 192.168.110.0
eigrp router-id 1.1.1.1
exit-address-family
!
address-family ipv6 unicast autonomous-system 6
!
af-interface GigabitEthernet1/0
passive-interface
exit-af-interface
!
topology base
exit-af-topology
eigrp router-id 1.1.1.1
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
no cdp log mismatch duplex
!
--More--
```

Diseño propio herramienta de simulación GNS3-2.2.2

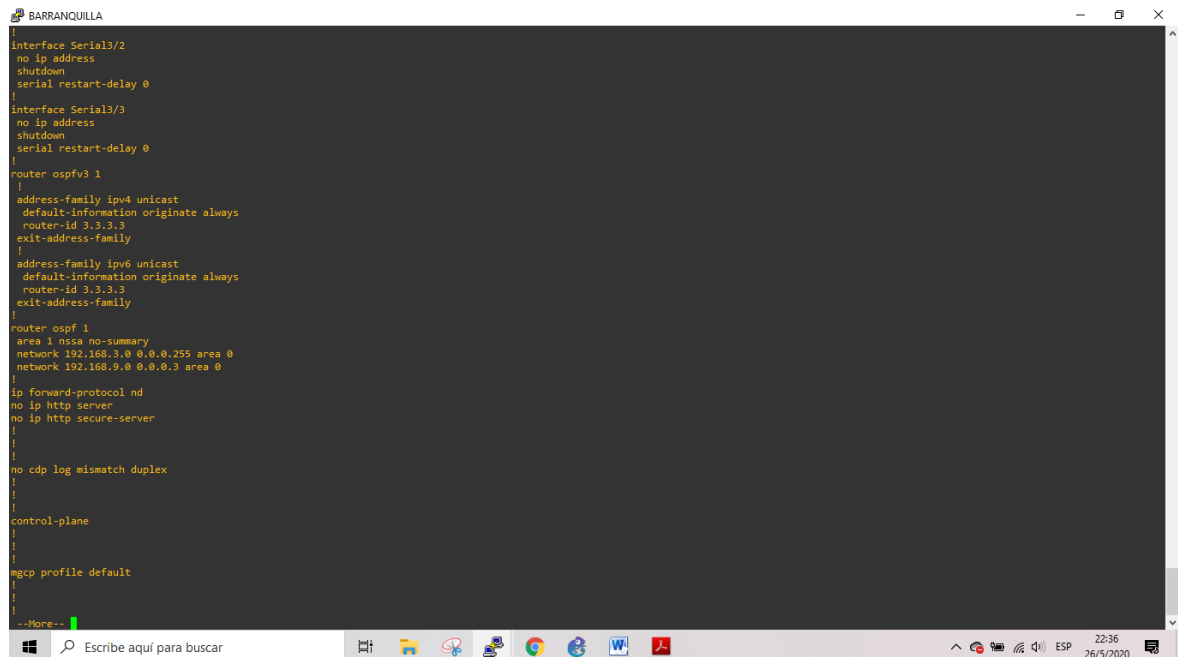
Figura 15. Archivo de configuración activo en R3. (Parte 2)



```
!
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface GigabitEthernet1/0
ip address 192.168.3.1 255.255.255.0
negotiation auto
ipv6 address FE80::3 link-local
ipv6 address 2001:DB8:ACAD:C::1/64
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface Serial3/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/1
bandwidth 120
ip address 192.168.9.6 255.255.255.252
ipv6 address FE80::3 link-local
ipv6 address 2001:DB8:ACAD:91::2/64
serial restart-delay 0
!
interface Serial3/2
no ip address
shutdown
--More--
```

Diseño propio herramienta de simulación GNS3-2.2.2

Figura 16. Archivo de configuración activo en R3. (Parte 3)



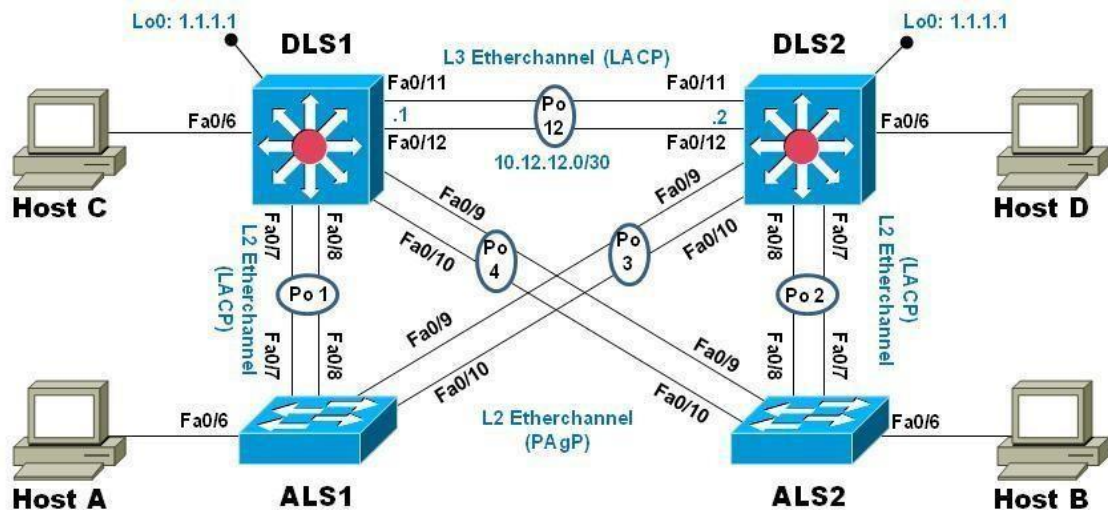
```
interface Serial3/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
router ospfv3 1
!
address-family ipv4 unicast
default-information originate always
router-id 3.3.3.3
exit-address-family
!
address-family ipv6 unicast
default-information originate always
router-id 3.3.3.3
exit-address-family
!
router ospf 1
area 1 nssa no-summary
network 192.168.3.0 0.0.0.255 area 0
network 192.168.9.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
no cdp log mismatch duplex
!
!
control-plane
!
!
mgcp profile default
!
!
--More--
```

Diseño propio herramienta de simulación GNS3-2.2.2

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, etherchannels, VLANs y demás aspectos que forman parte del escenario propuesto.

Figura 17. Topología de Red del Escenario 2



Parte 1. Configurar la red de acuerdo con las especificaciones

Apagar todas las interfaces en cada switch.

Asignar un nombre a cada switch acorde al escenario establecido.

Utilizamos el comando **hostname** para asignar un nombre a cada switch, el comando **int ran f0/# - #** para configurar un rango de interfaces y el comando **shutdown** para apagar las interfaces.

Tabla 11. Asignación de nombre y apagado de interfaces

Dispositivo	Asignación de Nombre y des habilitación de interfaces
Switch DLS 1	<pre>Switch # config t Switch (config) # hostname DLS1 DLS1 (config) # int ran f0/6 - 12 DLS1 (config-if-range) # shutdown DLS1 (config-if-range) # exit DLS1 (config) # exit</pre>
Switch DLS 2	<pre>Switch # config t Switch (config) # hostname DLS2 DLS2 (config) # int ran f0/6 - 12 DLS2 (config-if-range) # shutdown DLS2 (config-if-range) # exit DLS2 (config) # exit</pre>
Switch ALS 1	<pre>Switch # config t Switch (config) # hostname ALS1 ALS1 (config) # int ran f0/6 - 10 ALS1 (config-if-range) # shutdown ALS1 (config-if-range) # exit ALS1 (config) # exit</pre>
Switch ALS 2	<pre>Switch # config t Switch (config) # hostname ALS2 ALS2 (config) # int ran f0/6 - 10 ALS2 (config-if-range) # shutdown ALS2 (config-if-range) # exit ALS2 (config) # exit</pre>

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

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.

En esta etapa utilizamos el comando **channel-group 1 mode active** para configurar los puertos troncales, el modo **active** lo usamos agrupar los puertos mediante el protocolo LACP.

Tabla 12. Conexión entre DLS1 y DLS2

Dispositivo	Conexión entre DLS1 y DLS2 a través de EtherChannel
Switch DLS 1	<pre>DLS1 # config t DLS1 (config) # int ran f0/11 - 12 DLS1 (config-if-range) # channel-group 1 mode active DLS1 (config-if-range) # no shutdown DLS1 (config-if-range) # interface port-channel 1 DLS1 (config-if) # no switchport DLS1 (config-if) # ip address 10.12.12.1 255.255.255.252 DLS1 (config-if) # exit DLS1 (config) # exit DLS1# copy running-config startup-config</pre>
Switch DLS 2	<pre>DLS2 # config t DLS2 (config) # int ran f0/11 - 12 DLS2 (config-if-range) # channel-group 12 mode active DLS2 (config-if-range) # no shutdown DLS2 (config-if-range) # 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) # exit DLS2# copy running-config startup-config</pre>

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

Ahora utilizamos el comando **channel-group 1 mode active** para configurar los puertos troncales, el **mode active** lo usamos agrupar los puertos mediante el protocolo LACP.

Tabla 13. Port-channels en interfaces Fa0/7 y Fa0/8 utilizando LACP

Dispositivo	Port-channels en las interfaces Fa0/7 y Fa0/8 utilizando LACP
Switch DLS 1	<pre>DLS1 # config t DLS1 (config) # int ran f0/7 - 8 DLS1 (config-if-range) # channel-group 1 mode active DLS1 (config-if-range) # no shutdown DLS2 (config-if-range) # interface port-channel 1 DLS1 (config-if-range) # exit DLS1 (config) # exit DLS1# copy running-config startup-config</pre>
	<pre>DLS2 # config t DLS2 (config) # int ran f0/7 - 8 DLS2 (config-if-range) # channel-group 2 mode active</pre>

Switch DLS 2	DLS2 (config-if-range) # no shutdown DLS2 (config-if-range) # interface port-channel 2 DLS1 (config-if-range) # exit DLS2 (config) # exit DLS2# copy running-config startup-config
--------------	--

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

Ahora utilizamos el comando **channel-group 1 mode desirable** para configurar los puertos troncales, el **mode desirable** lo usamos agrupar los puertos mediante el protocolo PAgP.

Tabla 14. Port-channels en interfaces Fa0/7 y Fa0/8 utilizando PAgP

Dispositivo	Port-channels en las interfaces Fa0/7 y Fa0/8 utilizando PAgP
Switch DLS 1	DLS1 # config t DLS1 (config) # int ran f0/9 - 10 DLS1 (config-if-range) # channel-group 4 mode desirable DLS1 (config-if-range) # no shutdown DLS1 (config-if) # exit DLS2 (config) # int ran f0/9 - 10 DLS2 (config-if-range) # channel-group 3 mode desirable DLS2 (config-if-range) # no shutdown DLS2 (config-if) # exit DLS2 (config) # exit DLS2# copy running-config startup-config
Switch ALS 1	ALS1 # config t ALS1 (config) # int ran f0/9 - 10 ALS1 (config-if-range) # channel-group 3 mode desirable ALS1 (config-if-range) # no shutdown ALS1 (config-if) # exit ALS1 (config) # exit ALS1# copy running-config startup-config
Switch ALS 2	ALS2 # config t ALS2 (config) # int ran f0/9 - 10 ALS2 (config-if-range) # channel-group 4 mode desirable ALS2 (config-if-range) # no shutdown ALS2 (config-if) # exit ALS2 (config) # exit ALS2# copy running-config startup-config

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

En esta etapa utilizamos el comando **encapsulation** para encapsular la interfaz en DLS1 y DLS2 ya que son Catalyst 3560. Utilizamos el comando **switchport nonegotiate** para que las interfaces estén en modo troncal, y el comando **no shutdown** para habilitar el rango de interfaces.

Tabla 15. Asignación de troncales a la VLAN 800

Dispositivo	Asignación de troncales a la VLAN Nativa
Switch DLS 1	<pre>DLS1# config t DLS1 (config) # interface range f0/7-12 DLS1 (config-if-range) # switchport trunk encapsulation dot1q DLS1 (config-if-range) # switchport trunk native vlan 800 DLS1 (config-if-range) # switchport mode trunk DLS1 (config-if-range) # switchport nonegotiate DLS1 (config-if-range) # no shutdown DLS1 (config-if-range) # exit DLS1 (config) # exit DLS1# copy running-config startup-config</pre>
Switch DLS 2	<pre>DLS2 # config t DLS2 (config) # interface range f0/7-12 DLS2 (config-if-range) # switchport trunk encapsulation dot1q DLS2 (config-if-range) # switchport trunk native vlan 800 DLS2 (config-if-range) # switchport mode trunk DLS2 (config-if-range) # switchport nonegotiate DLS2 (config-if-range) # no shutdown DLS2 (config-if-range) # exit DLS2 (config) # exit DLS2# copy running-config startup-config</pre>
Switch ALS 1	<pre>ALS1# config t ALS1 (config) # interface range f0/7-10 ALS1 (config-if-range) # switchport trunk native vlan 800 ALS1 (config-if-range) # switchport mode trunk ALS1 (config-if-range) # switchport nonegotiate ALS1 (config-if-range) # no shutdown ALS1 (config-if-range) # exit ALS1 (config) # exit ALS1# copy running-config startup-config</pre>
Switch ALS 2	<pre>ALS2# config t ALS2 (config) # interface range f0/7-10 ALS2 (config-if-range) # switchport trunk native vlan 800 ALS2 (config-if-range) # switchport mode trunk ALS2 (config-if-range) # switchport nonegotiate ALS2 (config-if-range) # no shutdown ALS2 (config-if-range) # exit ALS2 (config) # exit</pre>

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

Utilizar el nombre de dominio UNAD con la contraseña cisco123

En esta etapa se establece el nombre de dominio VTP y la versión 2. Configuramos una contraseña para evitar que el nombre de dominio se aprenda automáticamente por los vecinos.

Tabla 16. Configuración en DLS1 para utilizar VTPv2

Dispositivo	Configuración en DLS1 para utilizar VTPv2
Switch DLS 1	DLS1# config t DLS1 (config) # vtp version? < 1 – 2 > DLS1 (config) # vtp version 2 DLS1 (config) # exit DLS1# config t DLS1 (config) # vtp version 2 DLS1 (config) # vtp domain UNAD DLS1 (config) # vtp password cisco123 DLS1 (config) # exit DLS1# copy running-config startup-config
Switch ALS 1	ALS1# config t ALS1 (config) # vtp version 2 ALS1 (config) # vtp domain UNAD ALS1 (config) # vtp password cisco123 ALS1 (config) # exit ALS1# copy running-config startup-config
Switch ALS 2	ALS2# config t ALS2 (config) # vtp version 2 ALS2 (config) # vtp domain UNAD ALS2 (config) # vtp password cisco123 ALS2 (config) # exit ALS2# copy running-config startup-config

Configurar DLS1 como servidor principal para las VLAN.

Ahora utilizamos el comando **mode server** para configurar DLS1 como servidor principal en el modo VTP y la versión 2.

Tabla 17. DLS1 servidor principal para las VLANS

Dispositivo	Configuración de DLS1 como servidor principal para las VLANS
Switch DLS 1	DLS1# config t DLS1 (config) # vtp version 2 DLS1 (config) # vtp mode server DLS1 (config) # vtp password cisco123 DLS1 (config) # exit DLS1# copy running-config startup-config

Configurar ALS1 y ALS2 como clientes VTP.

Ahora utilizamos el comando **mode client** para configurar ALS1 y ALS2 como clientes en el modo VTP y la versión 2.

Tabla 18. Configuración de ALS1 y ALS2 como clientes VTP

Dispositivo	Configuración de ALS1 y ALS2 como clientes VTP
Switch ALS 1	ALS1# config t ALS1 (config) # vtp version 2 ALS1 (config) # vtp mode client ALS1 (config) # vtp password cisco123 ALS1 (config) # exit ALS1# copy running-config startup-config
Switch ALS 2	ALS2# config t ALS2 (config) # vtp version 2 ALS2 (config) # vtp mode client ALS2 (config) # vtp password cisco123 ALS2 (config) # exit ALS2# copy running-config startup-config

Configurar en el servidor principal las siguientes VLAN:

Tabla 19. Configuración de VLANS en el servidor principal

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
800	Nativa	434	Estacionamiento
12	Ejecutivos	123	Mantenimiento
234	Huéspedes	101	Voz
111	Videonet	345	Administración

A continuación se relacionan los comandos utilizados para configurar las VLANS en el servidor principal.

Tabla 20. Configuración de VLANS en DLS1

Dispositivo	Configuración de VLANS en el servidor principal
Switch DLS 1	<pre> DLS1# config t DLS1 (config) # vlan 800 DLS1 (config-vlan) # name NATIVA DLS1 (config-vlan) # exit DLS1 (config) # vlan 12 DLS1 (config-vlan) # name EJECUTIVOS DLS1 (config-vlan) # exit DLS1 (config) # vlan 234 DLS1 (config-vlan) # name HUESPEDES DLS1 (config-vlan) # exit DLS1 (config) # vlan 111 DLS1 (config-vlan) # name VIDEONET DLS1 (config-vlan) # exit DLS1 (config) # vlan 434 DLS1 (config-vlan) # name ESTACIONAMIENTO DLS1 (config-vlan) # exit DLS1 (config) # vlan 123 DLS1 (config-vlan) # name MANTENIMIENTO DLS1 (config-vlan) # exit DLS1 (config) # vlan 101 DLS1 (config-vlan) # name VOZ DLS1 (config-vlan) # exit DLS1 (config) # vlan 345 DLS1 (config-vlan) # name ADMINISTRACION DLS1 (config-vlan) # exit </pre>

En DLS1, suspender la VLAN 434.

Ahora desde el modo de configuración global indicamos el número de la VLAN y utilizamos el comando **state suspend** para suspenderla.

Tabla 21. Suspensión de la VLAN 434 en DLS1

Dispositivo	Configuración para suspender la VLAN 434 en DLS1
Switch DLS 1	DLS1 (config) # vlan 434 DLS1 (config-vlan) # state? DLS1 (config-vlan) # state suspend DLS1 (config-vlan) # exit DLS1 (config) # exit DLS1# copy running-config startup-config

NOTA: La herramienta de simulación Packet Tracer no soporta el comando “state”, por lo tanto no es posible suspender la VLAN.

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

En esta etapa utilizamos los comandos del paso anterior para crear las VLANS en DLS2, y el comando **mode transparent** en el modo VTP y la versión 2.

Tabla 22. Configuración de VLANS en DLS2

Dispositivo	Configuración de VLANS en DLS2 y configuración de DLS2 en modo VTP transparente VTPv2
Switch DLS 2	DLS2# config t DLS2 (config) # vlan 800 DLS2 (config-vlan) # name NATIVA DLS2 (config-vlan) # exit DLS2 (config) # vlan 12 DLS2 (config-vlan) # name EJECUTIVOS DLS2 (config-vlan) # exit DLS2 (config) # vlan 234 DLS2 (config-vlan) # name HUESPEDES DLS2 (config-vlan) # exit DLS2 (config) # vlan 111 DLS2 (config-vlan) # name VIDEONET DLS2 (config-vlan) # exit DLS2 (config) # vlan 434 DLS2 (config-vlan) # name ESTACIONAMIENTO DLS2 (config-vlan) # exit DLS2 (config) # vlan 123

	<pre> DLS2 (config-vlan) # name MANTENIMIENTO DLS2 (config-vlan) # exit DLS2 (config) # vlan 101 DLS2 (config-vlan) # name VOZ DLS2 (config-vlan) # exit DLS2 (config) # vlan 345 DLS2 (config-vlan) # name ADMINISTRACION DLS2 (config-vlan) # exit DLS2 (config) # vtp version 2 DLS2 (config) # vtp mode transparent DLS2 (config) # vtp password cisco123 DLS2 (config) # exit DLS2# copy running-config startup-config </pre>
--	--

Suspender VLAN 434 en DLS2.

Desde el modo de configuración global indicamos el número de la VLAN y utilizamos el comando **state suspend** para suspenderla.

Tabla 23. Suspensión de la VLAN 434 en DLS2

Dispositivo	Configuración para suspender la VLAN 434 en DLS2
Switch DLS 2	<pre> DLS2 (config) # vlan 434 DLS2 (config-vlan) # state? DLS2 (config-vlan) # state suspend DLS2 (config-vlan) # exit DLS2 (config) # exit DLS2# copy running-config startup-config </pre>

NOTA: La herramienta de simulación Packet Tracer no soporta el comando “state”, por lo tanto no es posible suspender la VLAN.

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

A continuación se relacionan los comandos para crear la VLAN 567 en DLS2

Tabla 24. Creación de la VLAN 567 en DLS2

Dispositivo	Configuración de la VLAN CONTABILIDAD en DLS2
Switch DLS 2	<pre> DLS2# config t DLS2 (config) # vlan 567 DLS2 (config-vlan) # name CONTABILIDAD DLS2 (config-vlan) # exit DLS2 (config) # interface port-channel 2 </pre>

	<pre> 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) # interface port-channel 12 DLS2 (config-if) #switchport trunk allowed vlan except 567 DLS2 (config) # exit </pre>
--	---

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

El comando `spanning-tree vlan-id root primary` y `secondary` puede ser usado para establecer automáticamente un valor de prioridad.

En esta etapa utilizamos el comando **spanning-tree** en el modo de configuración global. El comando **root secondary** establece la prioridad del puente local, el comando **root primary** establecerá la prioridad del conmutador

Tabla 25. Configuración de Spanning tree root en DLS1

Dispositivo	Configuración de Spanning tree root en DLS2
Switch DLS 1	<pre> DLS1# config t DLS1 (config) # spanning-tree vlan 1,12,434,800,101,111,345 root primary DLS1 (config) # spanning-tree vlan 123,234 root secondary DLS1 (config) # exit DLS1# copy running-config startup-config </pre>

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

Tabla 26. Configuración de Spanning tree root en DLS2

Dispositivo	Configuración de Spanning tree root en DLS2
Switch DLS 2	<pre> DLS2# config t DLS2 (config) # spanning-tree vlan 123,234 root primary DLS2 (config) # spanning-tree vlan 1,12,434,800,101,111,345 root secondary DLS2 (config) # exit DLS2# copy running-config startup-config </pre>

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

A continuación se relacionan los comandos para configurar todos los puertos como troncales

Tabla 27. Configuración de los puertos troncales

Dispositivo	Configuración de los puertos troncales
Switch DLS 1	<pre>DLS1# config t DLS1 (config) # interface range f0/7-12 DLS1 (config-if-range) # switchport trunk encapsulation dot1q DLS1 (config-if-range) # switchport trunk native vlan 800 DLS1 (config-if-range) # switchport mode trunk DLS1 (config-if-range) # switchport nonegotiate DLS1 (config-if-range) # no shutdown DLS1 (config-if-range) # exit DLS1 (config) # exit DLS1# copy running-config startup-config</pre>
Switch DLS 2	<pre>DLS2# config t DLS2 (config) # interface range f0/7-12 DLS2 (config-if-range) # switchport trunk encapsulation dot1q DLS2 (config-if-range) # switchport trunk native vlan 800 DLS2 (config-if-range) # switchport mode trunk DLS2 (config-if-range) # switchport nonegotiate DLS2 (config-if-range) # no shutdown DLS2 (config-if-range) # exit DLS2 (config) # exit DLS2# copy running-config startup-config</pre>
Switch ALS 1	<pre>ALS1# config t ALS1 (config) # interface range f0/7-10 ALS1 (config-if-range) # switchport trunk native vlan 800 ALS1 (config-if-range) # switchport mode trunk ALS1 (config-if-range) # switchport nonegotiate ALS1 (config-if-range) # no shutdown ALS1 (config-if-range) # exit ALS1 (config) # exit ALS1# copy running-config startup-config</pre>
Switch ALS 2	<pre>ALS2# config t ALS2 (config) # interface range f0/7-10 ALS2 (config-if-range) # switchport trunk native vlan 800 ALS2 (config-if-range) # switchport mode trunk ALS2 (config-if-range) # switchport nonegotiate ALS2 (config-if-range) # no shutdown ALS2 (config-if-range) # exit ALS2 (config) # exit ALS2# copy running-config startup-config</pre>

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

Tabla 28. Asignación de interfaces como puertos de acceso a las VLANS

Interfaz	DLS1	DLS2	ALS1	ALS2
Fa 0/6	345	12, 101	123, 101	234
Fa 0/15	111	111	111	111
Fa 0/16-18		567		

A continuación se relaciona la serie de comandos necesarios para asignar los puertos de acceso a cada VLAN. Los comandos configuran el modo del puerto como acceso y activan **spanning-tree PortFast**.

Tabla 29. Asignación de puertos de acceso a las VLANS

Dispositivo	Asignación de puertos de acceso a las VLANS
Switch DLS 1	<pre> DLS1# config t DLS1 (config) #int f 0/6 DLS1 (config-if) #switchport mode access DLS1 (config-if) #switchport access vlan 345 DLS1 (config-if) #spanning-tree portfast DLS1 (config-if) #no shutdown DLS1 (config-if) #exit DLS1 (config) #int f 0/15 DLS1 (config-if) #switchport mode access DLS1 (config-if) #switchport access vlan 111 DLS1 (config-if) #spanning-tree portfast DLS1 (config-if) #no shutdown DLS1 (config-if) #exit DLS1 (config) #exit DLS1 # copy running-config startup-config </pre>
Switch DLS 2	<pre> DLS2# config t DLS2 (config) #int f 0/6 DLS2 (config-if) #switchport mode access DLS2 (config-if) #switchport access vlan 12 DLS2 (config-if) #switchport access vlan 101 DLS2 (config-if) #spanning-tree portfast DLS2 (config-if) #no shutdown DLS2 (config-if) #exit DLS2 (config) #int f 0/15 DLS2 (config-if) #switchport mode access DLS2 (config-if) #switchport access vlan 111 DLS2 (config-if) #spanning-tree portfast DLS2 (config-if) #no shutdown </pre>

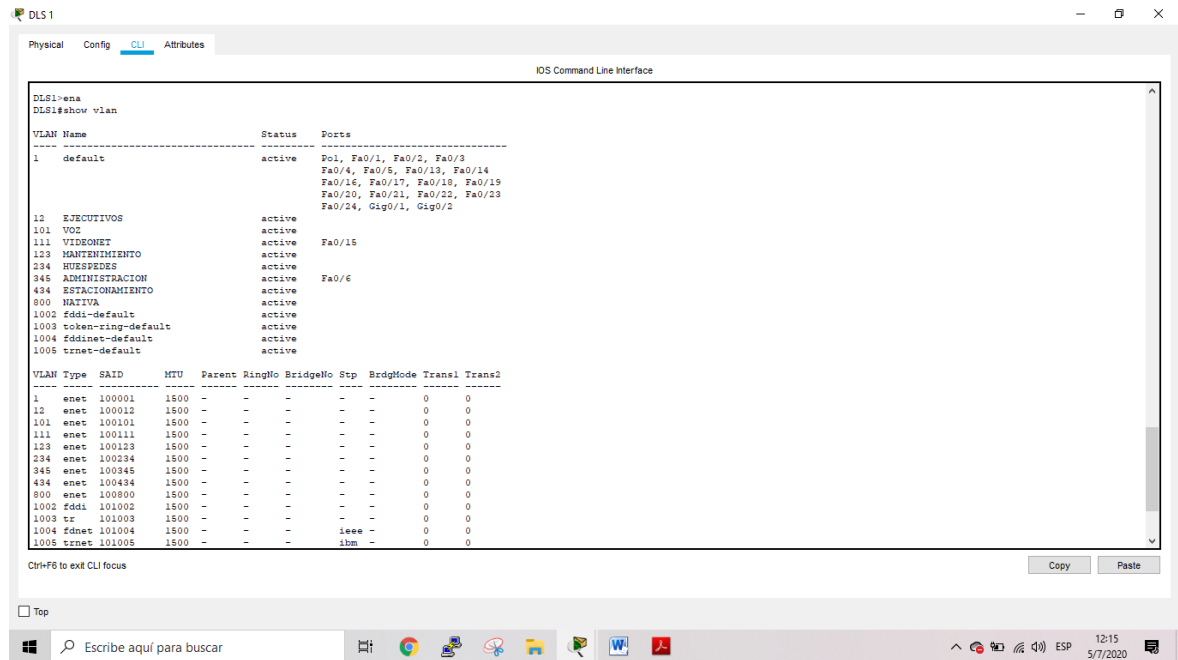
	<pre> DLS2 (config-if) #exit DLS2 (config) # interface range f0/16 - 18 DLS2 (config-if) #switchport mode access DLS2 (config-if) #switchport access vlan 567 DLS2 (config-if) #spanning-tree portfast DLS2 (config-if) #no shutdown DLS2 (config-if) #exit DLS2 (config) #exit DLS2 # copy running-config startup-config </pre>
Switch ALS 1	<pre> ALS1# config t ALS1 (config) #int f 0/6 ALS1 (config-if) #switchport mode access ALS1 (config-if) #switchport access vlan 123 ALS1 (config-if) #switchport access vlan 101 ALS1 (config-if) #spanning-tree portfast ALS1 (config-if) #no shutdown ALS1 (config-if) #exit ALS1 (config) #int f 0/15 ALS1 (config-if) #switchport mode access ALS1 (config-if) #switchport access vlan 111 ALS1 (config-if) #spanning-tree portfast ALS1 (config-if) #no shutdown ALS1 (config-if) #exit ALS1 (config) #exit ALS1 # copy running-config startup-config </pre>
Switch ALS 2	<pre> ALS2# config t ALS2 (config) #int f 0/6 ALS2 (config-if) #switchport mode access ALS2 (config-if) #switchport access vlan 234 ALS2 (config-if) #spanning-tree portfast ALS2 (config-if) #no shutdown ALS2 (config-if) #exit ALS2 (config) #int f 0/15 ALS2 (config-if) #switchport mode access ALS2 (config-if) #switchport access vlan 111 ALS2 (config-if) #spanning-tree portfast ALS2 (config-if) #no shutdown ALS2 (config-if) #exit ALS2 (config) #exit ALS2 # copy running-config startup-config </pre>

Parte 2. Conectividad de red de prueba y las opciones configuradas

Verificar la existencia de las VLAN correctas en todos los switches y la asignación de puertos troncales y de acceso

En esta etapa utilizamos el comando **show running-config** en cada Router para verificar las tablas de enrutamiento.

Figura 18. VLANS existentes en DLS1



```
DLS1>ena
DLS1#show vlan

VLAN Name                Status Ports
-----
1    default                 active Fa0/1, Fa0/3, Fa0/2, Fa0/3
    Fa0/4, Fa0/5, Fa0/13, Fa0/14
    Fa0/16, Fa0/17, Fa0/18, Fa0/19
    Fa0/20, Fa0/21, Fa0/22, Fa0/23
    Fa0/24, Giga0/1, Giga0/2

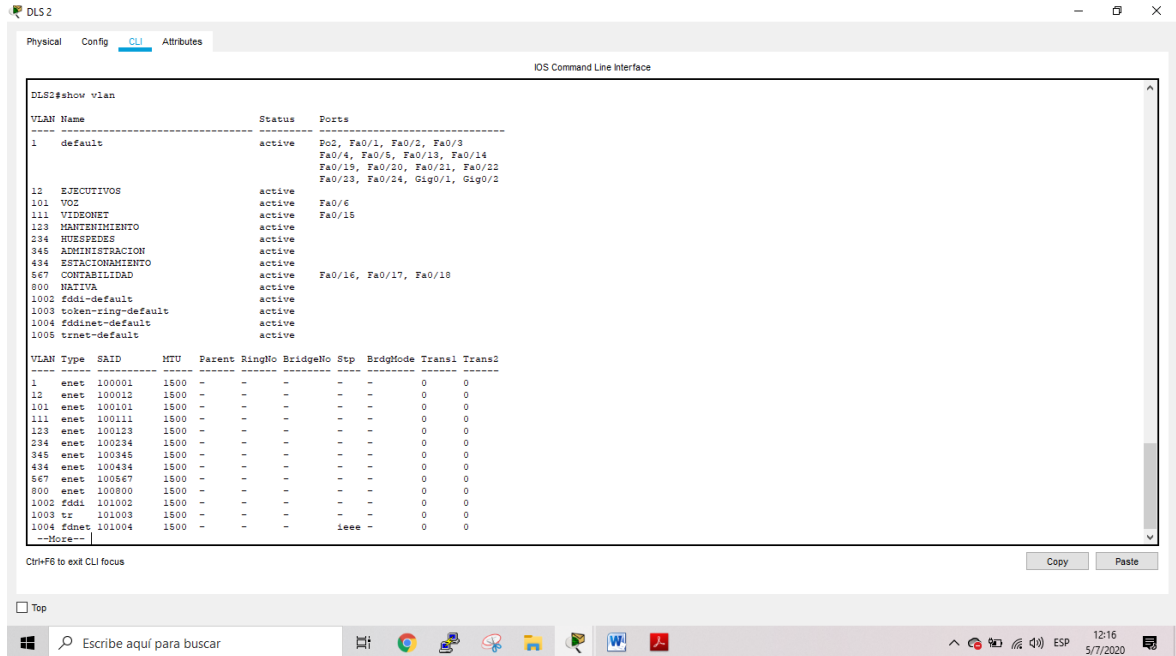
12   EJECUTIVOS              active
101  VOZ                      active
111  VIDEONET                 active Fa0/15
123  MANTENIMIENTO            active
234  HUESPEDES                active
945  ADMINISTRACION           active Fa0/6
434  ESTACIONAMIENTO          active
800  NATIVA                   active
1002 fdci-default            active
1003 token-ring-default     active
1004 fdinet-default        active
1005 trnet-default         active

VLAN Type SAID      MTU Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001  1500 - - - - - 0 0
12   enet  100012  1500 - - - - - 0 0
101  enet  100101  1500 - - - - - 0 0
111  enet  100111  1500 - - - - - 0 0
123  enet  100123  1500 - - - - - 0 0
234  enet  100234  1500 - - - - - 0 0
945  enet  100345  1500 - - - - - 0 0
434  enet  100434  1500 - - - - - 0 0
800  enet  100800  1500 - - - - - 0 0
1002 fdci  101002  1500 - - - - - 0 0
1003 tr   101003  1500 - - - - - 0 0
1004 fdnet 101004  1500 - - - - - ieee 0 0
1005 trnet 101005  1500 - - - - - ibm   0 0

Ctrl+F6 to exit CLI focus
```

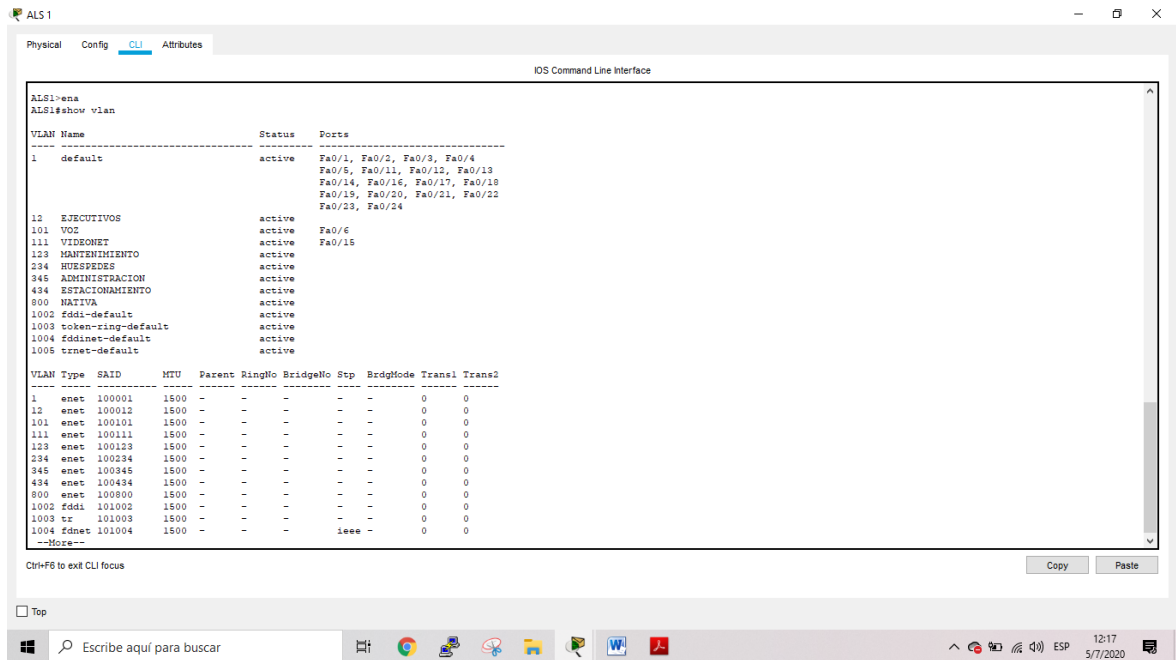
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 19. VLANS existentes en DLS2



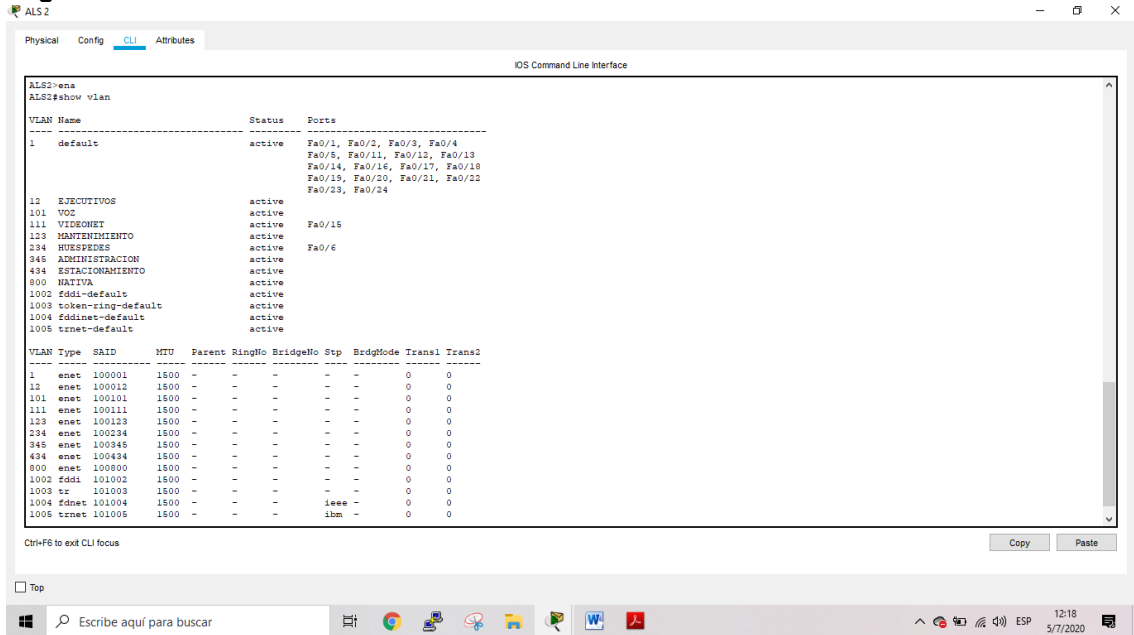
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 20. VLANS existentes en ALS1



Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 21. VLANs existentes en ALS2

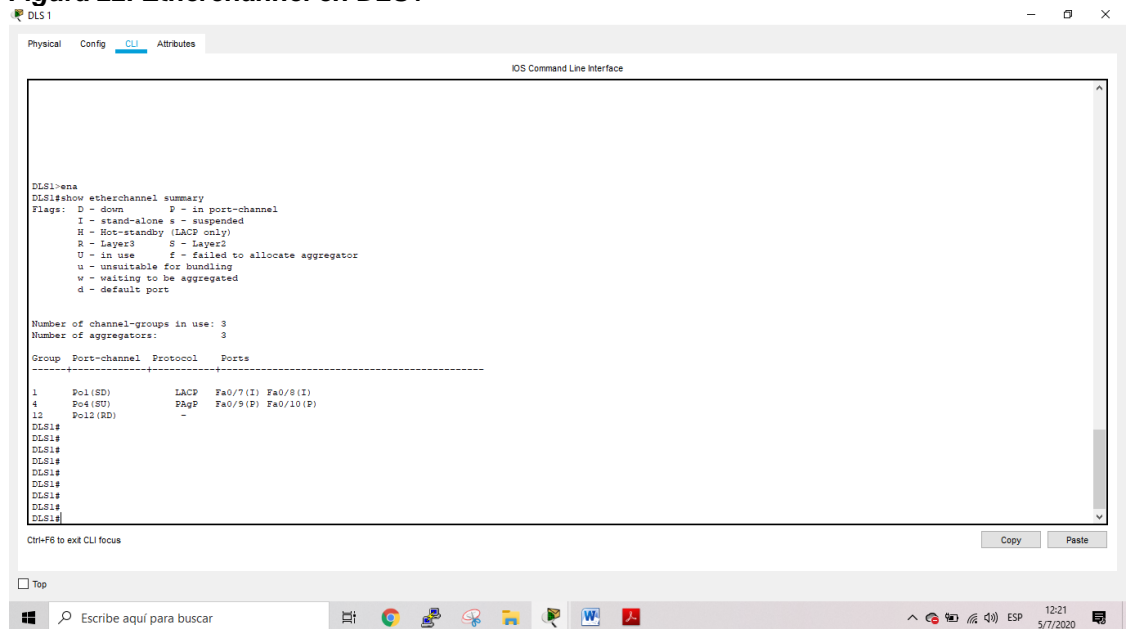


Diseño propio herramienta de simulación Packet Tracer 7.3

Verificar que el EtherChannel entre DLS1 y ALS1 está configurado correctamente

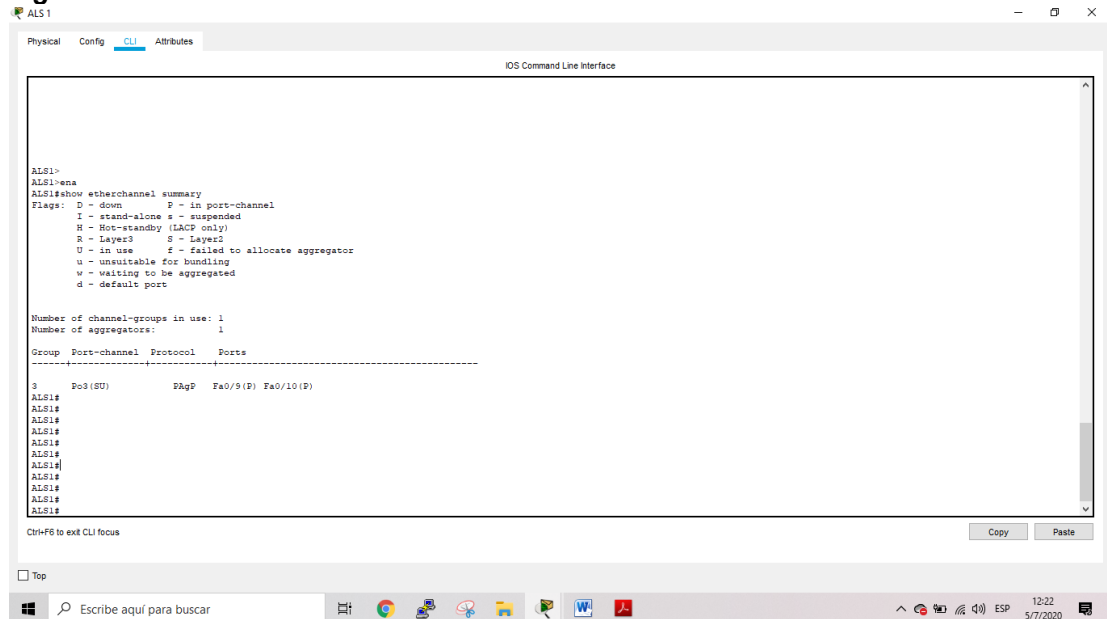
Con el comando **show etherchannel summary** visualizamos la línea de información por canal de puertos.

Figura 22. Etherchannel en DLS1



Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 23. Etherchannel en ALS1



```
ALS1>
ALS1>ena
ALS1#show etherchannel summary
Flags: D - down        P - in port-channel
       I - stand-alone s - suspended
       N - Not-scandby (LACP only)
       R - Layer3      S - Layer2
       U - in use      f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

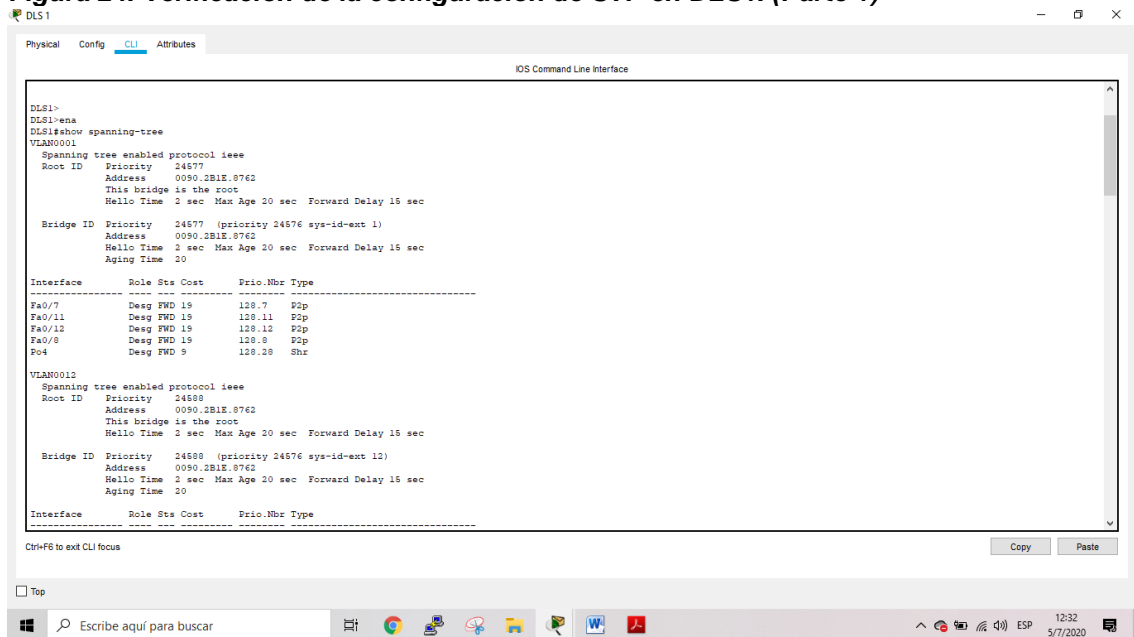
-----
Group  Port-channel  Protocol    Ports
-----
3      Po3 (SU)         PAgP       Fa0/9 (P) Fa0/10 (P)
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
ALS1#
Ctrl-F6 to exit CLI focus
```

Diseño propio herramienta de simulación Packet Tracer 7.3

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

Con el comando **show spanning-tree** visualizamos información sobre la configuración de STP en cada switch.

Figura 24. Verificación de la configuración de STP en DLS1. (Parte 1)



```
DLS1>
DLS1>ena
DLS1#show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 24577
Address 0090.2B1E.0762
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 0090.2B1E.0762
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
Fa0/11 Desg FWD 19 128.11 P2p
Fa0/12 Desg FWD 19 128.12 P2p
Fa0/8 Desg FWD 19 128.8 P2p
Po4 Desg FWD 9 128.28 Shr

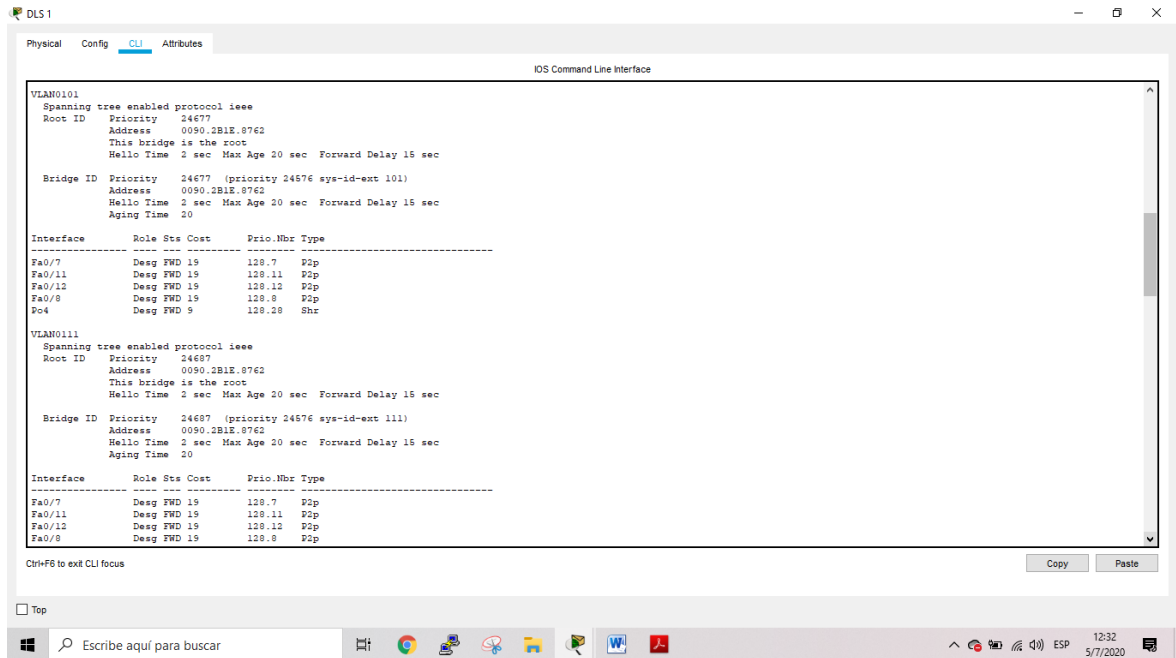
VLAN0012
Spanning tree enabled protocol ieee
Root ID Priority 24580
Address 0090.2B1E.0762
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24580 (priority 24576 sys-id-ext 12)
Address 0090.2B1E.0762
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

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

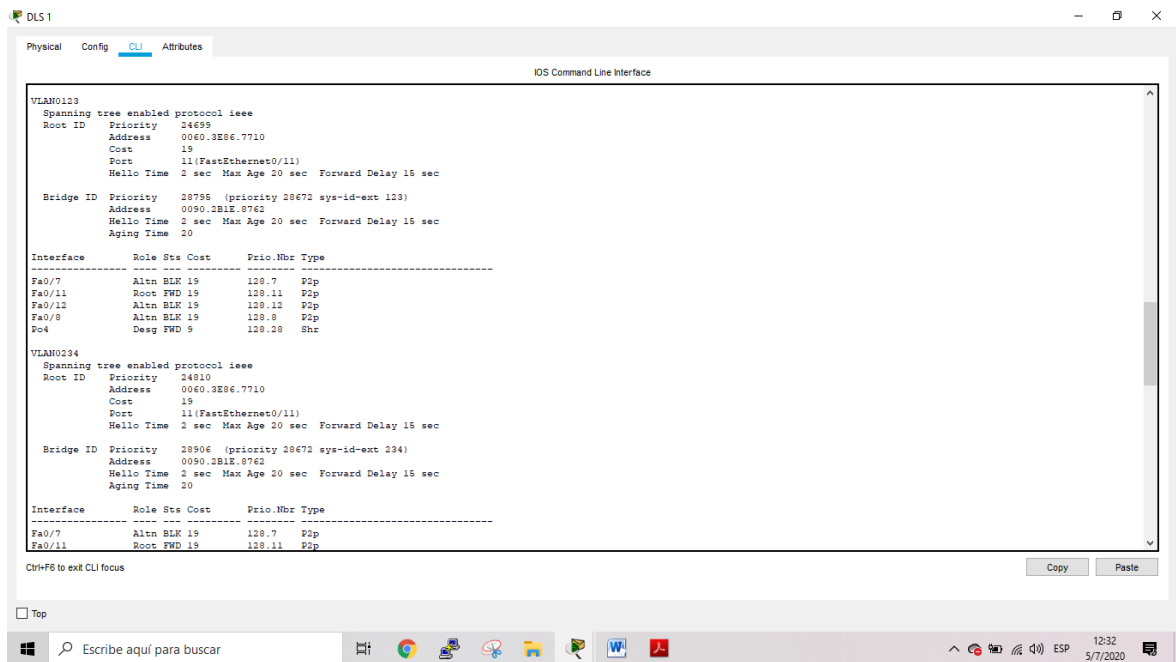
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 25. Verificación de la configuración de STP en DLS1. (Parte 2)



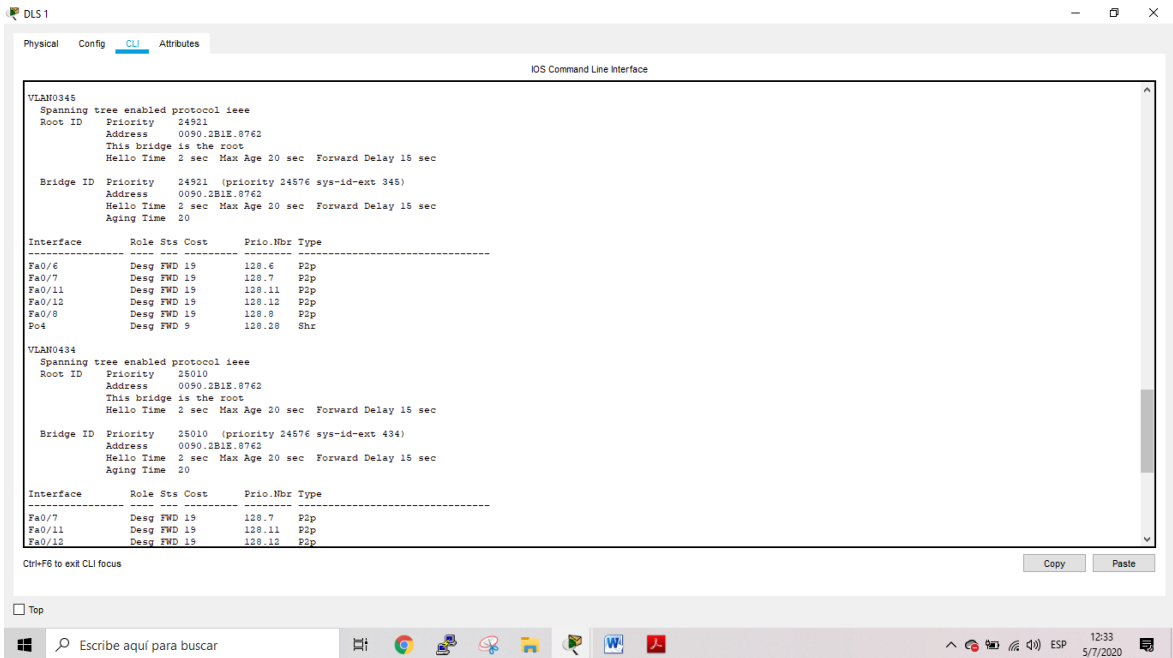
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 26. Verificación de la configuración de STP en DLS1. (Parte 3)



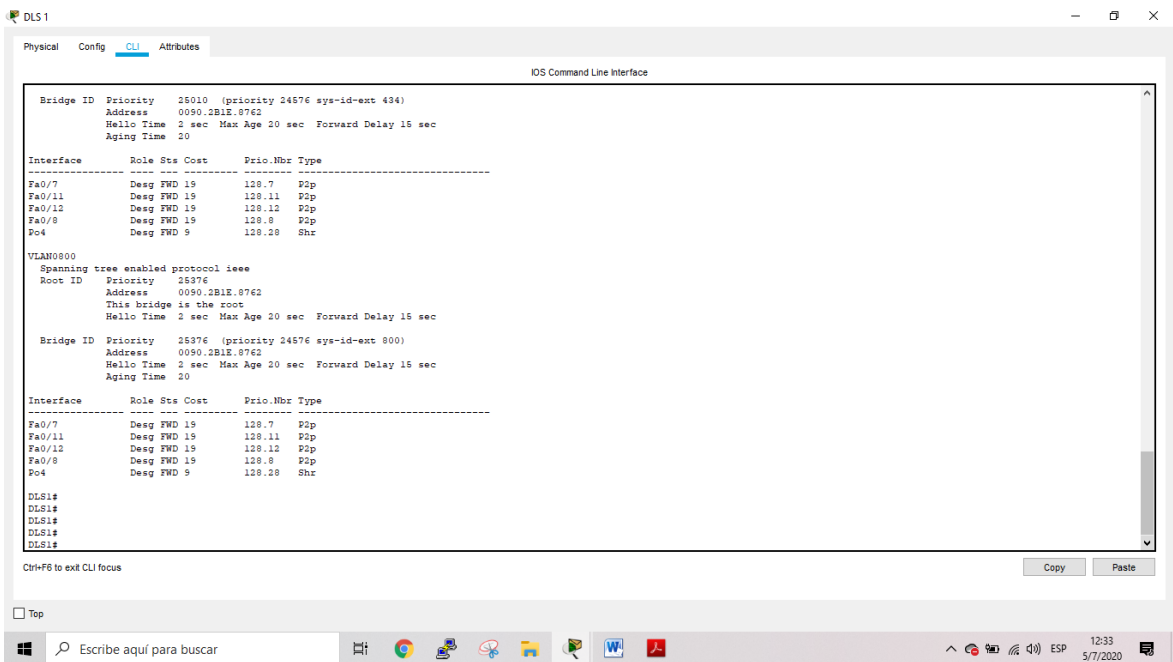
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 27. Verificación de la configuración de STP en DLS1. (Parte 4)



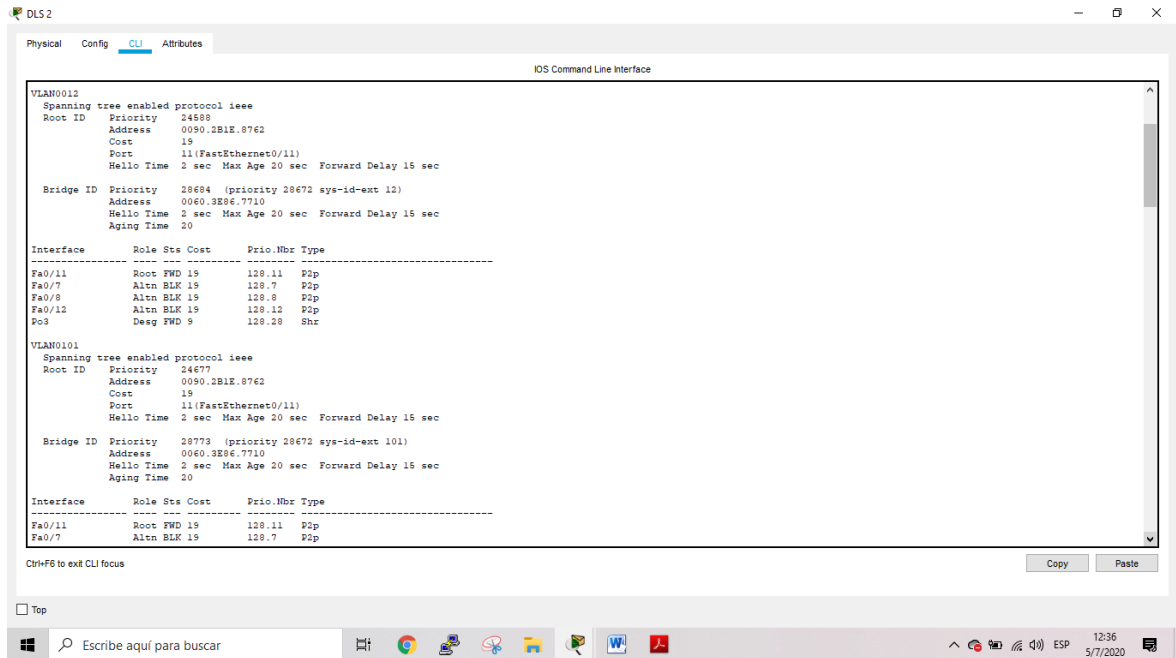
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 28. Verificación de la configuración de STP en DLS1. (Parte 5)



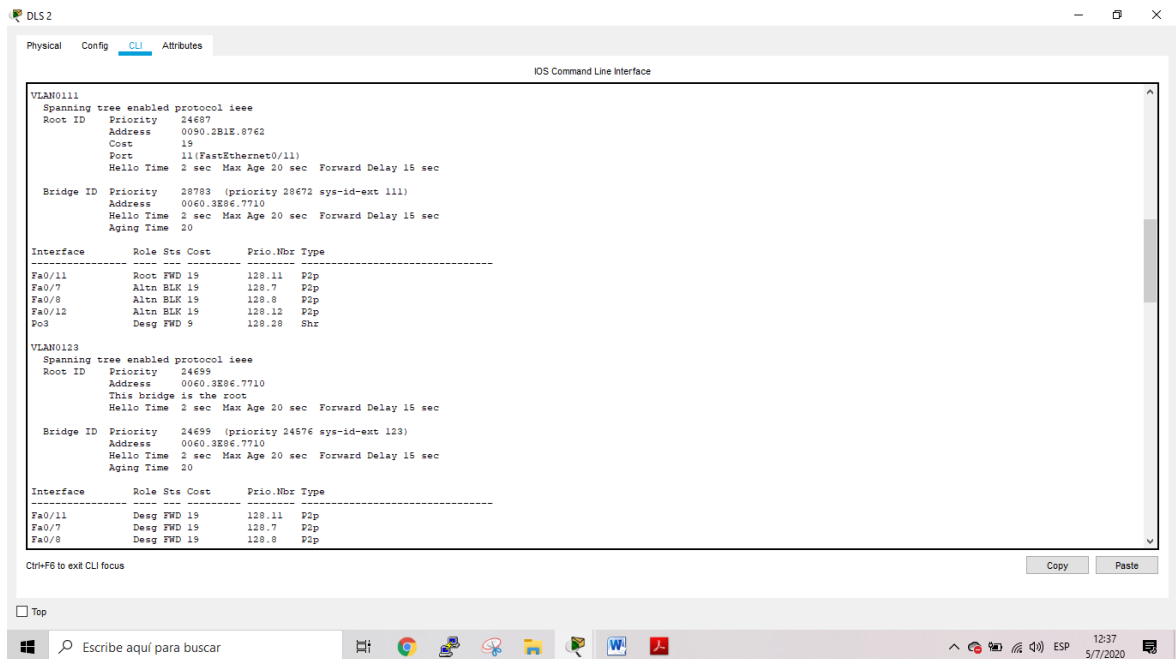
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 29. Verificación de la configuración de STP en DLS2. (Parte 1)



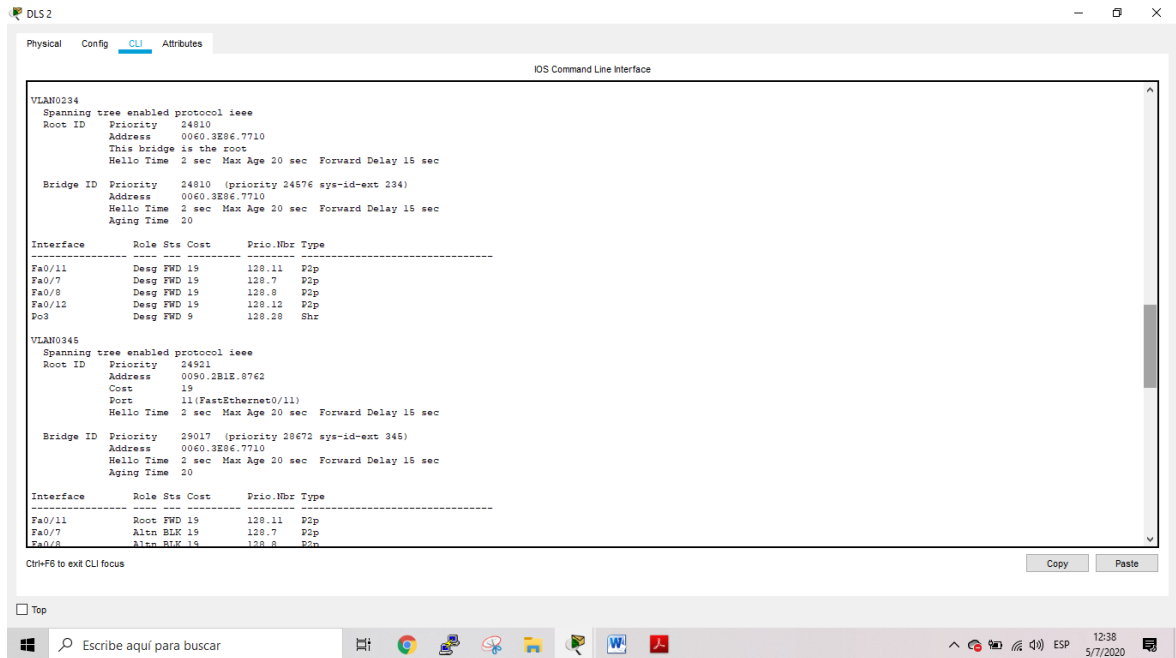
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 30. Verificación de la configuración de STP en DLS2. (Parte 2)



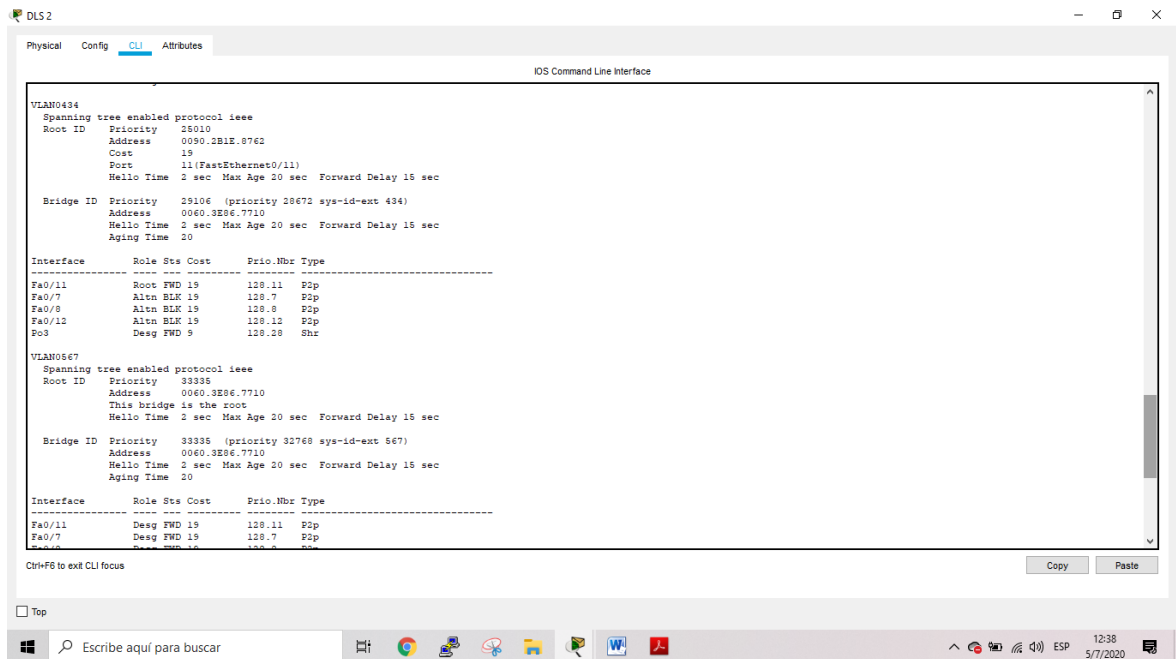
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 31. Verificación de la configuración de STP en DLS2. (Parte 3)



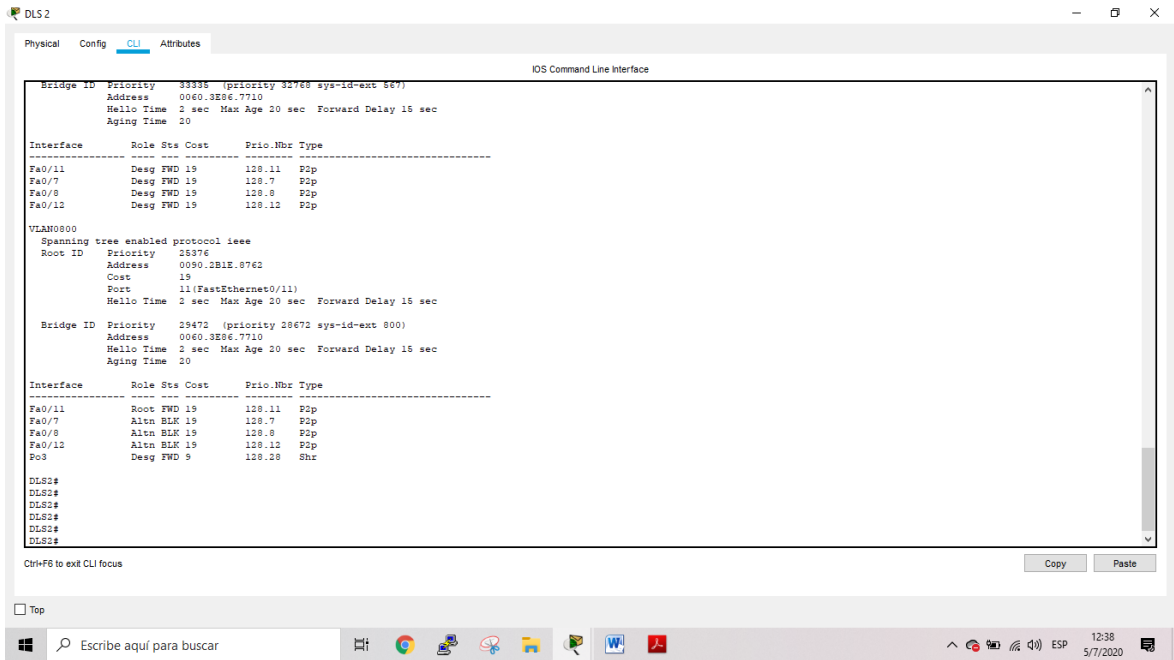
Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 32. Verificación de la configuración de STP en DLS2. (Parte 4)



Diseño propio herramienta de simulación Packet Tracer 7.3

Figura 33. Verificación de la configuración de STP en DLS2. (Parte 5)



Diseño propio herramienta de simulación Packet Tracer 7.3

CONCLUSIONES

Los protocolos de enrutamiento avanzado permiten mejorar la respuesta a los cambios en la topología de la red con la posibilidad de repartir el tráfico entre nodos por varios caminos y la posibilidad de comprender diferentes tipos de servicios que se establecen en la red.

EIGRP para IPv6 se configura directamente en las interfaces del router. En caso de que el router no tenga una dirección IPv4, se debe configurar un ID de router para que se inicie el proceso de enrutamiento.

En el escenario 1 utilizamos OSPF como protocolo de enrutamiento para propagar las tablas de enrutamiento a nivel interno solo de los puertos seriales ya que las conexiones LAN no requieren esta información.

En el escenario 2 agrupamos varios enlaces a través del protocolo Etherchannel para crear enlaces troncales, los cuales permiten mejorar la velocidad del tráfico de datos a través de los switch.

BIBLIOGRAFIA

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>

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>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Inter VLAN 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>

ANEXO

<https://drive.google.com/drive/folders/1BDI9oJyne0acoKU410NUkA26zS0bv6id?usp=sharing>