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

NIGER ANDRES CARRILLO GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
DOSQUEBRADAS
2021

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

NIGER ANDRES CARRILLO GARCIA

Diplomado de opción de grado presentado para optar el título de
INGENIERO EN TELECOMUNICACIONES

DIRECTOR:
ING. DIEGO EDINSON RAMIREZ CLAROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
DOSQUEBRADAS, RISARALDA
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

DOSQUEBRADAS, 04 de agosto de 2021

AGRADECIMIENTOS

Primeramente gracias al primer Ingeniero y creador por las oportunidades de cada nuevo día de vida y las habilidades intelectuales que concede a nuestra disposición, infinitas gracias también a mi madre Esperanza y hermanos Juan y Rober por los consejos, la motivación, la compañía y los afectos permanentes que amenizan las responsabilidades diarias y retos de esfuerzo prolongado como el estudio a consciencia de un avanzado programa de estudios como el diplomado de CCNP. Agradezco profundamente a todo el equipo de trabajo académico de la UNAD asociados a la academia del proveedor tecnológico CISCO, en especial al Ingeniero director de curso Alejandro Pérez y los Ingenieros tutores Diego Ramírez, John Pérez y Raúl Bareno, quienes estuvieron presentes acompañando el proceso formativo de manera comprometida y atenta a través de diferentes medios, durante el desarrollo del programa fueron notorios los sinceros esfuerzos por parte de ellos para prestar una enseñanza efectiva, clara y sincera de los contenidos del diplomado CCNP y por guiar al estudiante en la relativa complejidad técnica y administrativa que conlleva la coordinación de las plataformas virtuales y herramientas tecnológicas de la UNAD con las de la academia CISCO, mientras estas facilidades tecnológicas continúen su necesario proceso de integración y perfeccionamiento los esfuerzos de los docentes seguirán motivando al estudiante a enfocarse en el cumplimiento de los objetivos esperados pese a toda dificultad.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Adyacencia: relación exitosa de proximidad entre dos o más routers que comparten una conexión física adyacente y el mismo segmento de subred que permite intercambio continuo de información usada como punto de partida para el correcto funcionamiento de protocolos de enrutamiento dinámico

Agregación: capacidad de algunos switches de asociar de hasta 8 conexiones físicas cableadas en un solo enlace lógico entre dos switches adyacentes, con el propósito de sumar las capacidades físicas de transmisión de información de varios enlaces en uno solo y proveer tolerancia a fallas con varias conexiones físicas redundantes

Convergencia: estado estable que alcanza un grupo de routers dentro de un sistema autónomo de enrutamiento de tal manera que cada uno tiene pleno conocimiento de la mejor ruta hacia cada destino interno y externo y de las posibles rutas alternativas en caso de fallas o cambios repentinos, dicho estado se logra después de un proceso de intercambio de información cuyo algoritmo y tiempo de reacción ante cambios repentinos en la red depende del protocolo de enrutamiento en cuestión y su enfoque.

Encriptación: proceso que mediante ciertos algoritmos matemáticos cada vez más avanzados transforma la información transmitida en formatos ilegibles para terceros pero de fácil lectura para los usuarios finales mediante un proceso simple de autenticación, se garantiza así la confidencialidad de la información impidiendo o inutilizando la manipulación indebida de la información sensible mientras que es transportada por redes que pueden ser inseguras como el internet

Enrutamiento: tarea imprescindible para las comunicaciones remotas ejecutada por routers y switches multinivel que interconectan diferentes redes, mediante tablas de enrutamiento y rutas predefinidas o automáticas con protocolos de enrutamiento deciden la mejor ruta para cada paquete con base en su información de red destino

Loop: condición desfavorable ocasionada por una conexión redundante entre dos o más enlaces donde las tramas o paquetes de información no fluyen normalmente hacia su destino sino que quedan “rebotando” en una zona generando consumo de recursos de red sin sentido y entorpeciendo el buen rendimiento de la red, esto puede ocurrir en capa 2 y capa 3 y se evita implementando protocolos de control de redundancia como STP en capa 2 y protocolos de enrutamiento dinámico en capa 3

Redistribución: herramienta que permite interconectar diferentes sistemas autónomos de enrutamiento con el propósito de intercambiar información de rutas, mediante una serie de simples comandos se logra la integración y correcta funcionalidad de diferentes protocolos de enrutamiento como si se tratara de uno solo

VLAN: significa red de área local virtual, es una etiqueta agregada en las tramas de información de capa 2 que permiten separar de manera lógica varias redes lógicas dentro de un mismo switch físico o enlace físico por motivos de seguridad y optimización de recursos de red

RESUMEN

Este documento muestra la aplicabilidad en escenarios reales de los conocimientos adquiridos en el diplomado CCNP de CISCO Routing & Switching al implementar dos escenarios típicos de ejemplo diseñados para la prestación eficiente y escalable de servicios de telecomunicaciones para organizaciones que requieren mayores volúmenes de información y esperan mejores condiciones de servicio.

La primera parte se enfoca en aplicar los conocimientos de Routing para integrar funcionalmente dos sistemas autónomos de enrutamiento, situación que puede presentarse en la unión o asociación de dos organizaciones que quieren compartir información y recursos en red sin la necesidad de modificar las redes ya implementadas de cada organización. La segunda parte aplica los conocimientos de Switching para implementar a base de switches una red de alta fiabilidad, disponibilidad y escalabilidad entre diferentes departamentos típicos de una organización y sus servicios centralizados.

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

ABSTRACT

This document shows the applicability in real scenarios of the knowledge acquired in the CISCO Routing & Switching CCNP diploma by implementing two typical example scenarios designed for the efficient and scalable provision of telecommunications services for organizations that require greater volumes of information and expect better Terms of Service.

The first part focuses on applying Routing knowledge to functionally integrate two autonomous routing systems, a situation that can occur in the union or association of two organizations that want to share information and resources in the network without the need to modify the networks already implemented by each organization. The second part applies the knowledge of Switching to implement a network of high reliability, availability and scalability based on switches between different typical departments of an organization and their centralized services.

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

INTRODUCCION

El diplomado CCNP de CISCO se compone de los apartados de Routing & Switching y se trata de un programa de entrenamiento de carácter profesional destinado a adquirir y poner en practica conocimientos avanzados y a profundidad para la implementación efectiva de redes en múltiples escenarios incluyendo entornos corporativos de gran escala aprovechando el potencial, la versatilidad y escalabilidad de equipos como Routers y Switches principalmente del proveedor de CISCO pero también de una amplia variedad de herramientas, técnicas, protocolos y servicios relacionados de otros proveedores que complementan sus funcionalidades, para poner a prueba tales conocimientos y comprobar su aplicabilidad en escenarios reales se implementaron y analizaron dos escenarios para Routing y Switching respectivamente con ayuda de los simuladores Packet Tracer y GNS3.

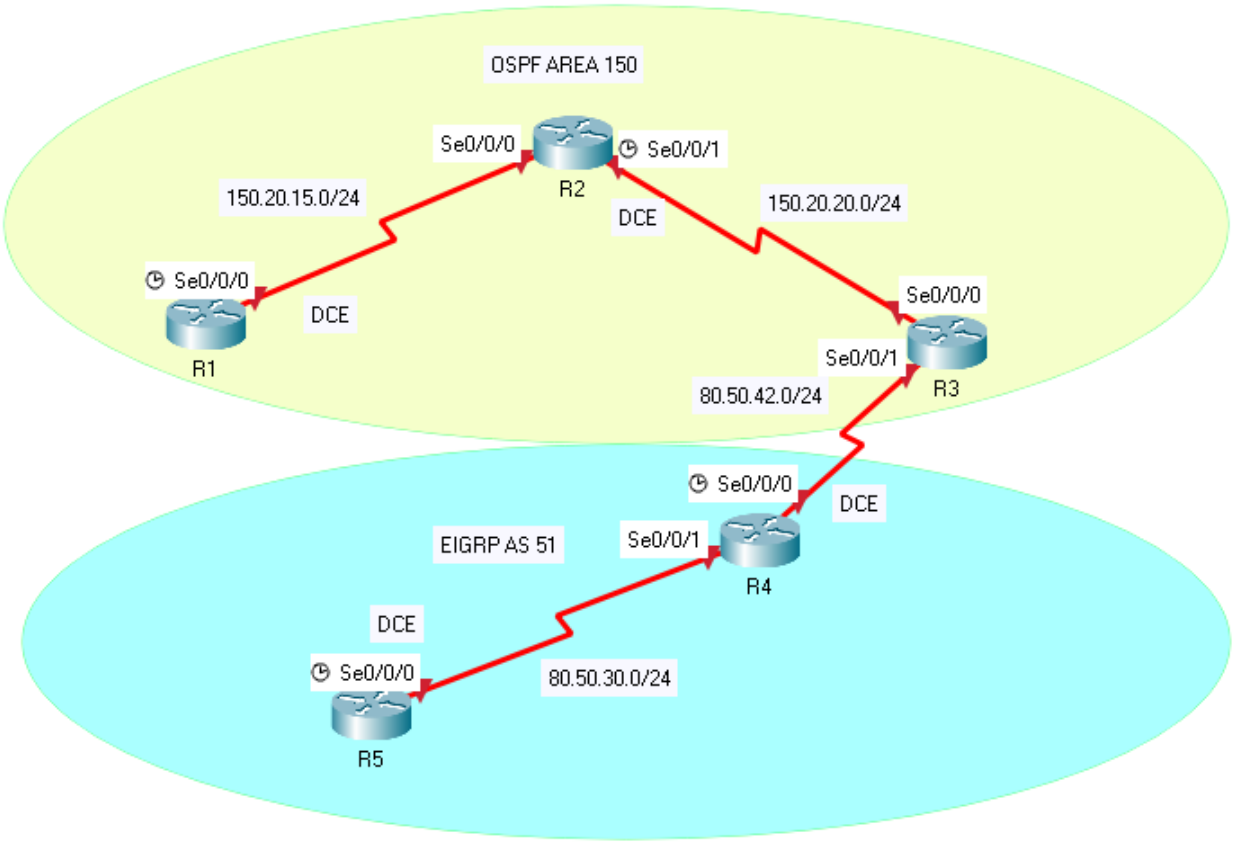
El primer escenario propuesto aplicable típicamente a redes de área amplia se implementó paso a paso una red de completa conectividad de extremo a extremo conformada por múltiples redes diferentes pertenecientes a dos sistemas autónomos que utilizan cada uno diferente protocolo de enrutamiento dinámico (OSPF vs EIGRP), para lograrlo fue clave la técnica de la redistribución de rutas que veremos cuan útil y versátil puede ser para todo tipo de integración eficiente de diferentes dominios de administración o escenarios de implementación. Para este escenario se mostraran capturas de pantalla de simulaciones solo en Packet Tracer con el cual basta para cumplir los objetivos.

Al apartado de Switching le corresponde su aplicación en el segundo escenario aplicable en capas de distribución y Core de organizaciones grandes que prestan servicios centralizados o buscan que la conectividad distribuida entre diferentes partes de su red tenga altos niveles de disponibilidad, escalabilidad y resiliencia, para lograr esto se aprovechan principalmente las técnicas de configuración VLAN centralizada VTP, control de redundancia de capa 2 STP y agregación de enlaces capa 2 y capa 3 mediante PAGP y LACP. Para este escenario se mostraran capturas de pantalla de simulaciones en Packet Tracer con el cual se cumplen parcialmente los objetivos por lo que además veremos capturas de pantalla de simulaciones en GNS3 que si permite cumplir totalmente los objetivos y con el fin de poner en practica distintos simuladores.

DESARROLLO

ESCENARIO 1

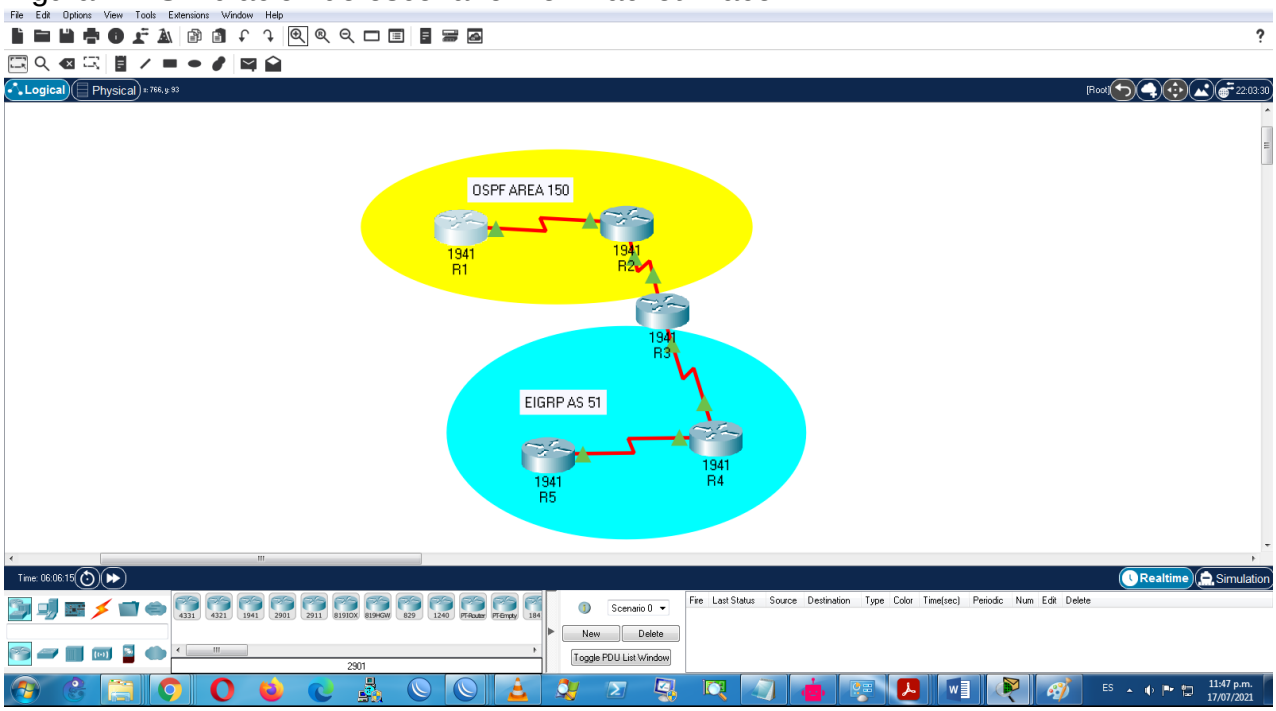
Figura 1.1 Topología de red de escenario 1



Fuente: UNAD

El esquema propuesto en la Figura 1.1 para el escenario 1 muestra dos sistemas autónomos de enrutamiento interconectados donde uno implementa el protocolo de enrutamiento dinámico OSPF mientras que el otro implementa EIGRP, el esquema podría interpretarse como si las interfaces en R3 estuvieran configuradas solo con OSPF y las de R4 solo con EIGRP, sin embargo para mayor claridad entre la interfaz s0/0/1 en R3 y s0/0/0 en R4 debe usarse el mismo protocolo de enrutamiento, esto implica que para garantizar la intercomunicación entre ambos dominios de enrutamiento se deben implementar ambos protocolos en R3 pero asignando una de sus interfaces en OSPF y otra en EIGRP como se observa en la Figura 1.2.

Figura 1.2 Simulación de escenario 1 en Packet Tracer



Fuente: Autor

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

Se configura cada router con la siguiente secuencia de comandos del lado izquierdo con su respectiva explicación de cada uno entre paréntesis al lado derecho:

Configuración router R1

```
hostname R1                                          (asigna nombre R1, modo configuración global)
interface s0/0/0                                     (cambia a modo interfaz serial 0/0/0)
    ip address 150.20.15.1 255.255.255.0             (asigna dirección IP y mascara de subred)
    clock rate 125000                                (asigna velocidad de reloj de interfaz serial DCE)
    no shutdown                                      (habilita la interfaz)
    exit                                             (cambiar a modo configuración global)
route ospf 1                                         (habilita OSPF ID 1, cambia a modo router)
    network 150.20.15.0 0.0.0.255 area 150           (asocia red R1-R2 en proceso OSPF ID 1 y area 150)
```

Configuración R2

```
hostname R2                                  (asigna nombre R2, modo configuración global)
interface s0/0/0                             (cambia a modo interfaz serial 0/0/0)
    ip address 150.20.15.2 255.255.255.0     (asigna dirección IP y mascara de subred)
    no shutdown                              (habilita la interfaz)
interface s0/0/1                             (cambia a modo interfaz s0/0/1)
    ip address 150.20.20.1 255.255.255.0     (asigna dirección IP y mascara de subred)
    clock rate 125000                        (asigna velocidad de reloj de interfaz serial DCE)
    no shutdown                              (habilita la interfaz)
    exit                                     (vuelve a modo configuración global)
route ospf 1                                 (habilita OSPF ID 1, cambia a modo router)
    network 150.20.15.0 0.0.0.255 area 150   (asocia red R1-R2 en proceso OSPF ID 1 y area 150)
    network 150.20.20.0 0.0.0.255 area 150   (asocia red R2-R3 en proceso OSPF ID 1 y area 150)
```

Configuración R3

```
hostname R3                                  (asigna nombre R3, modo configuración global)
interface s0/0/0                             (cambia a modo interfaz serial 0/0/0)
    ip address 150.20.20.2 255.255.255.0     (asigna dirección IP y mascara de subred)
no shutdown                                  (habilita la interfaz)
interface s0/0/1                             (cambia a modo interfaz serial 0/0/1)
    ip address 80.50.42.2 255.255.255.0      (asigna dirección IP y mascara de subred)
    no shutdown                              (habilita la interfaz)
    exit                                     (vuelve a modo configuración global)
route ospf 1                                 (habilita OSPF ID 1, cambia a modo router)
    network 150.20.20.0 0.0.0.255 area 150   (asocia red R2-R3 en proceso OSPF ID 1 y area 150)
route eigrp 51                               (habilita EIGRP AS 51, cambia a modo router)
    network 80.50.42.0 0.0.0.255             (asocia red R3-R4 en proceso EIGRP AS 51)
```

Configuración R4

```
hostname R4                                  (asigna nombre R4, modo configuración global)
interface s0/0/0                             (cambia a modo interfaz serial 0/0/0)
    ip address 80.50.42.1 255.255.255.0      (asigna dirección IP y mascara de subred)
    clock rate 125000                        (asigna velocidad de reloj de interfaz serial DCE)
    no shutdown                              (habilita la interfaz)
interface s0/0/1                             (cambia a modo interfaz serial 0/0/1)
    ip address 80.50.30.2 255.255.255.0      (asigna dirección IP y mascara de subred)
    no shutdown                              (habilita la interfaz)
    exit                                     (vuelve a modo configuración global)
route eigrp 51                               (habilita EIGRP AS 51, cambia a modo router)
    network 80.50.42.0 0.0.0.255             (asocia red R3-R4 en proceso EIGRP AS 51)
    network 80.50.30.0 0.0.0.255             (asocia red R4-R5 en proceso EIGRP AS 51)
```

Configuración R5

```
hostname R5                                  (asigna nombre R5, modo configuración global)
interface s0/0/0                             (cambia a modo interfaz serial 0/0/0)
    ip address 80.50.30.1 255.255.255.0      (asigna dirección IP y mascara de subred)
    clock rate 125000                        (asigna velocidad de reloj de interfaz serial DCE)
    no shutdown                              (habilita la interfaz)
    exit                                     (vuelve a modo configuración global)
route eigrp 51                               (habilita EIGRP AS 51, cambia a modo router)
    network 80.50.30.0 0.0.0.255             (asocia red R4-R5 en proceso EIGRP AS 51)
```

1.2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 20.1.0.0/22 y configure esas interfaces para participar en el área 150 de OSPF.

Configuración R1

```
interface loopback1                          (cambia a modo interfaz loopback1)
      Ip add 20.1.0.1 255.255.255.0          (asigna dirección IP y mascara de subred)
interface loopback2                          (cambia a modo interfaz loopback2)
      Ip add 20.1.1.2 255.255.255.0          (asigna dirección IP y mascara de subred)
interface loopback3                          (cambia a modo interfaz loopback3)
      Ip add 20.1.2.3 255.255.255.0          (asigna dirección IP y mascara de subred)
interface loopback4                          (cambia a modo interfaz loopback4)
      Ip add 20.1.3.4 255.255.255.0          (asigna dirección IP y mascara de subred)
      exit                                   (vuelve a modo configuración global)
route ospf 1                                 (cambia a modo router OSPF ID 1)
    network 20.1.0.0 0.0.3.255 area 150      (asocia red loopback en proceso OSPF ID 1 y area 150)
```

1.3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 180.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 51.

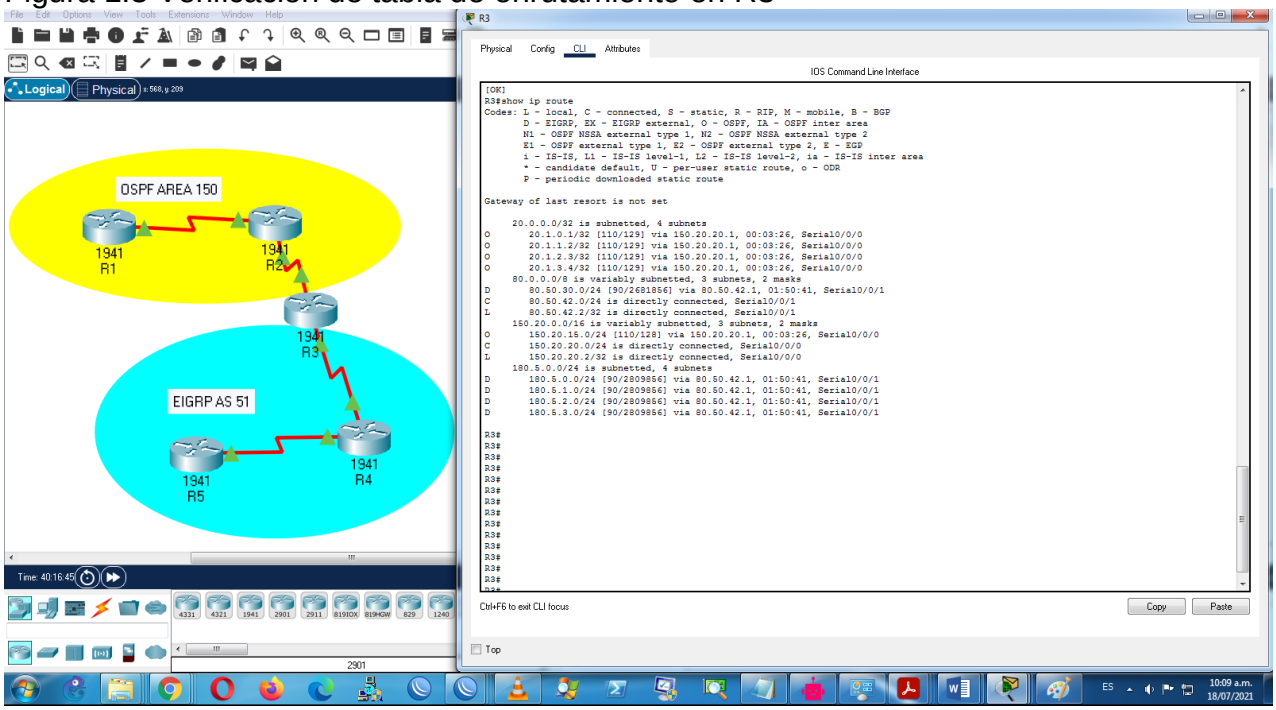
Configuración R5

```
interface loopback1                          (cambia a modo interfaz loopback1)
      Ip add 180.5.0.1 255.255.255.0         (asigna dirección IP y mascara de subred)
interface loopback2                          (cambia a modo interfaz loopback2)
      Ip add 180.5.1.2 255.255.255.0         (asigna dirección IP y mascara de subred)
interface loopback3                          (cambia a modo interfaz loopback3)
      Ip add 180.5.2.3 255.255.255.0         (asigna dirección IP y mascara de subred)
interface loopback4                          (cambia a modo interfaz loopback4)
      Ip add 180.5.3.4 255.255.255.0         (asigna dirección IP y mascara de subred)
      exit                                   (vuelve a modo configuración global)
route eigrp 51                               (cambia a modo router EIGRP AS 51)
      network 180.5.0.0 0.0.3.255            (asocia red loopback en proceso EIGRP AS 51)
```

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

De acuerdo a la tabla de enrutamiento, R3 efectivamente reconoce las redes loopback de R1 mediante OSPF (O) y también reconoce las de R5 mediante EIGRP (D) como se aprecia en la Figura 1.3.

Figura 1.3 Verificación de tabla de enrutamiento en R3



Fuente: Autor

1.5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 80000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

Para configurar la redistribución de rutas EIGRP en OSPF basta con asignar un costo para estas rutas externas en unidades de ancho de banda kbps (80000 en este caso) pero se debe incluir preferiblemente el parámetro “subnets” para que se reconozcan las subredes sin clase por una sumarización automática realizada por EIGRP, de forma inversa esto no es necesario para la redistribución de rutas OSPF en EIGRP.

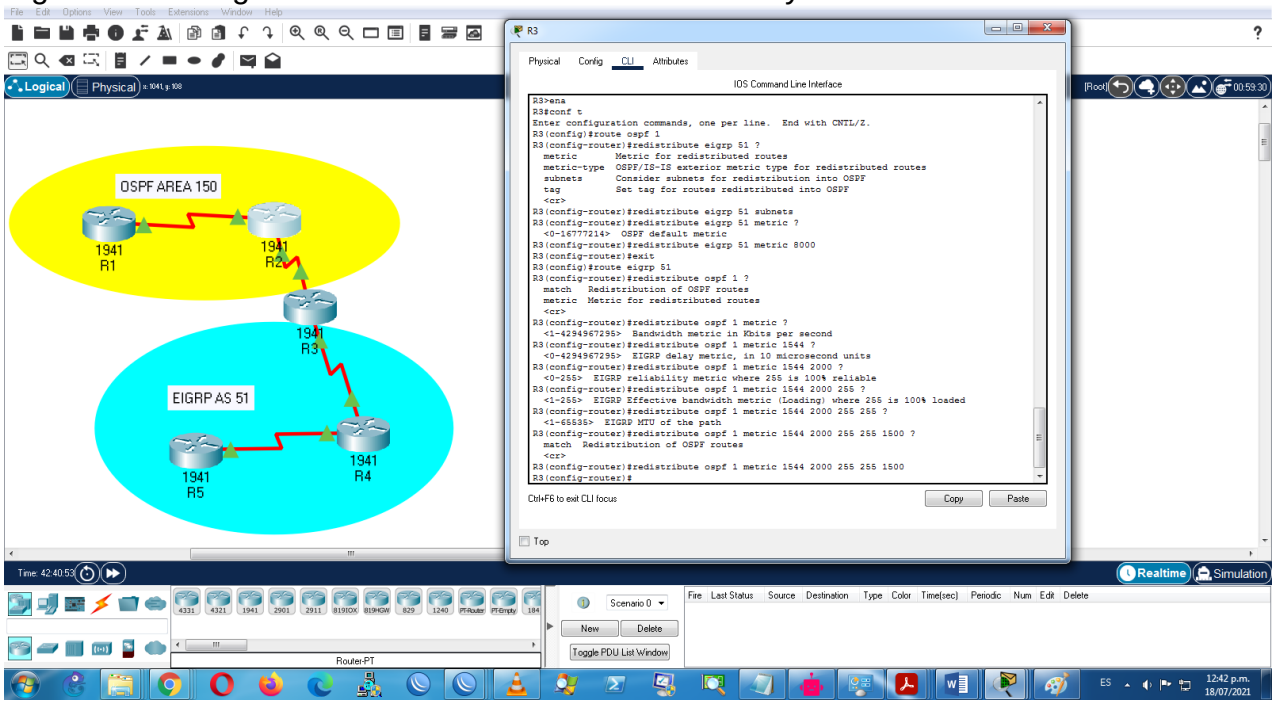
Para configurar la redistribución de rutas OSPF en EIGRP se definen los dos valores principales de la métrica EIGRP: ancho de banda en kbps donde T1 equivale a 1544 kbps y tiempo de retardo de 2000 ajustado en unidades de 10 microsegundos, otros valores secundarios asignados son: confiabilidad, MTU y ancho de banda efectiva

Como se observa en la Figura 1.4 con ayuda contextual se validan opciones soportadas de configuración de redistribución para ambos protocolos en R3

Configuración R3

route ospf 1	(cambia a modo router OSPF ID 1)
redistribute eigrp 51 subnets	(redistribuye sin sumarización por defecto EIGRP)
redistribute eigrp 51 metric 80000 subnets	(redistribuye rutas EIGRP con ajuste de parámetros)
route eigrp 51	(cambia a modo router EIGRP AS 51)
redistribute ospf 1 metric 1544 2000 255 255 1500	(redistribuye rutas OSPF con ajuste de parámetros)

Figura 1.4 Configuración de redistribución entre OSPF y EIGRP



Fuente: Autor

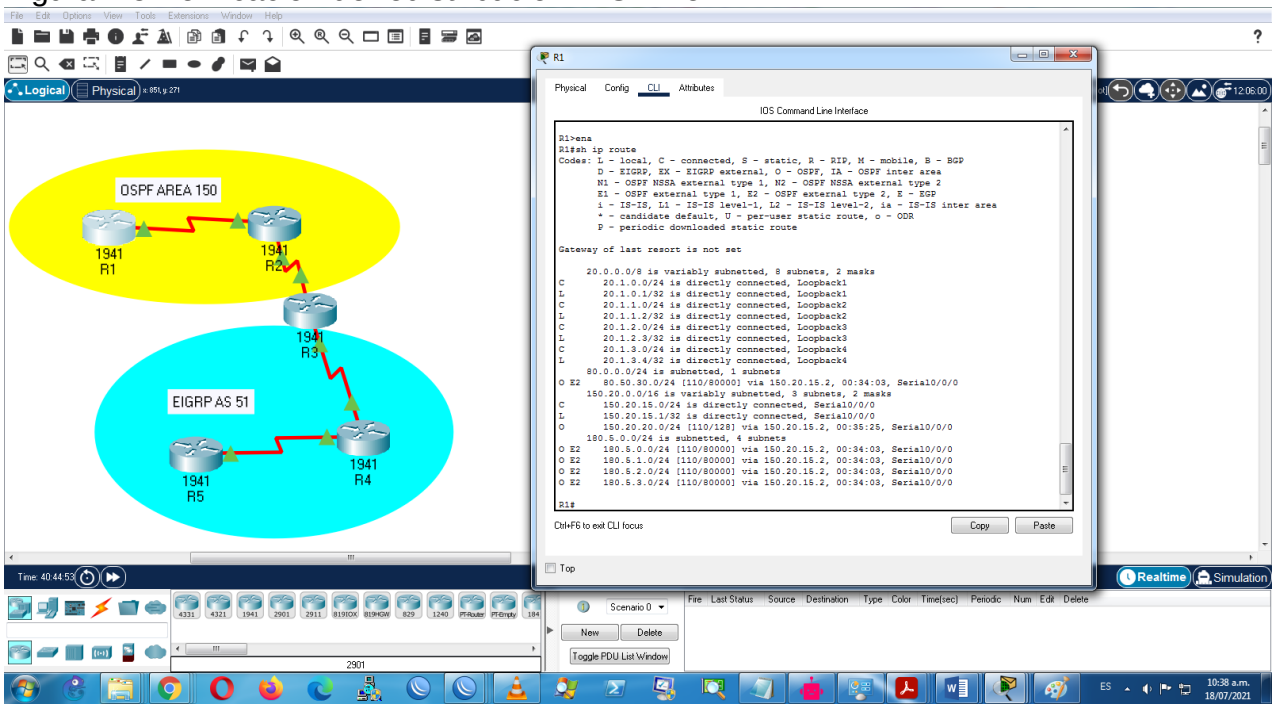
1.6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando show ip route.

Las rutas desde AS opuestos efectivamente son aprendidas desde R1 y R5 como se aprecia en la Figura 1.5 y Figura 1.6.

En R1 se aprenden las redes provenientes del dominio de EIGRP y se marcan “O E2”, es decir aprendidas mediante OSPF pero existentes en un dominio de enrutamiento externo y diferente de OSPF

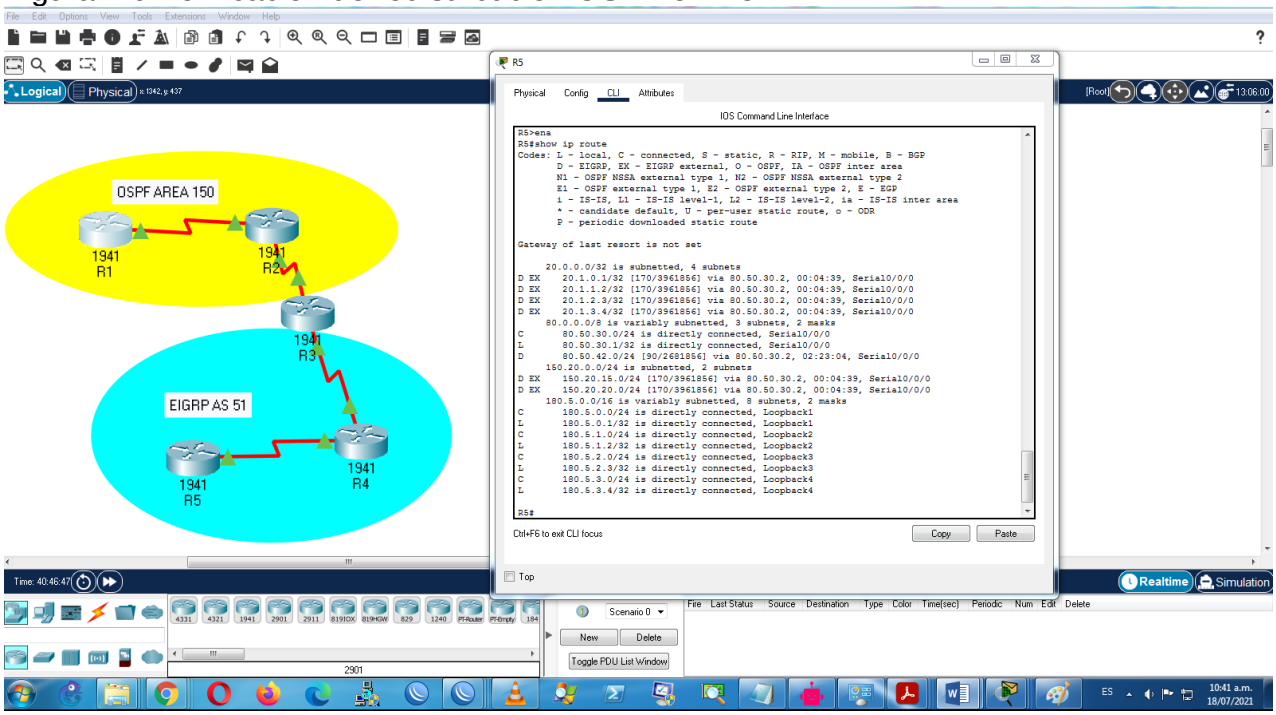
En R5 se aprenden las redes provenientes del dominio de OSPF y se marcan “D EX”, es decir aprendidas mediante EIGRP pero existentes en un dominio de enrutamiento externo

Figura 1.5 Verificación de redistribución EIGRP en R1



Fuente: Autor

Figura 1.6 Verificación de redistribución OSPF en R5

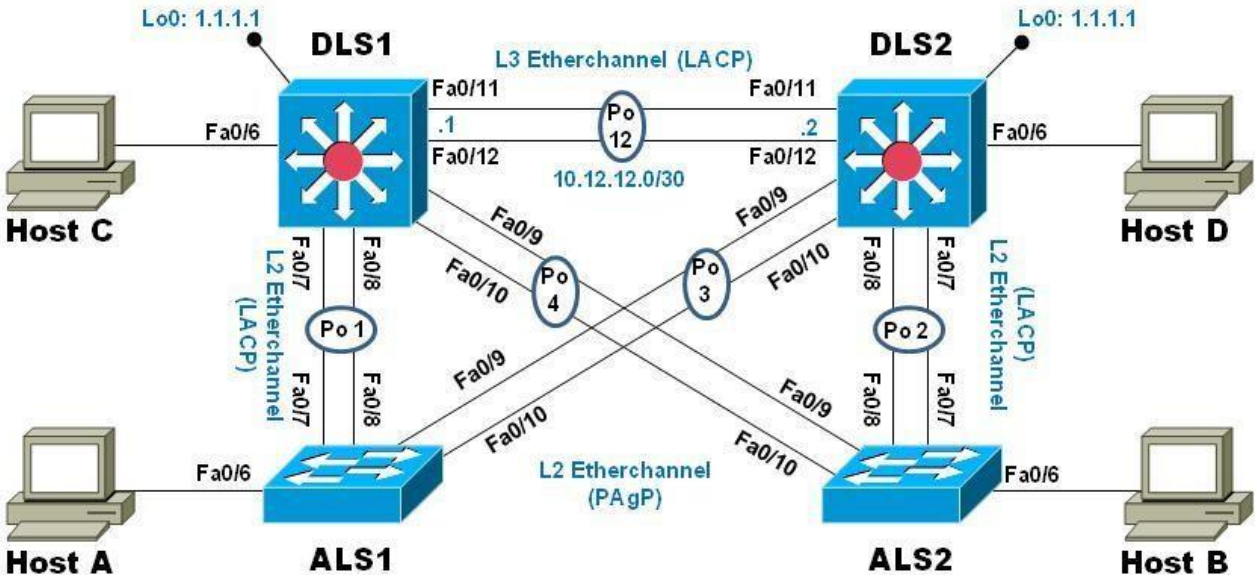


Fuente: Autor

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 en la Figura 2.1.

Figura 2.1 Topología de red de escenario 2



Fuente: UNAD

Simulación en Packet Tracer

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

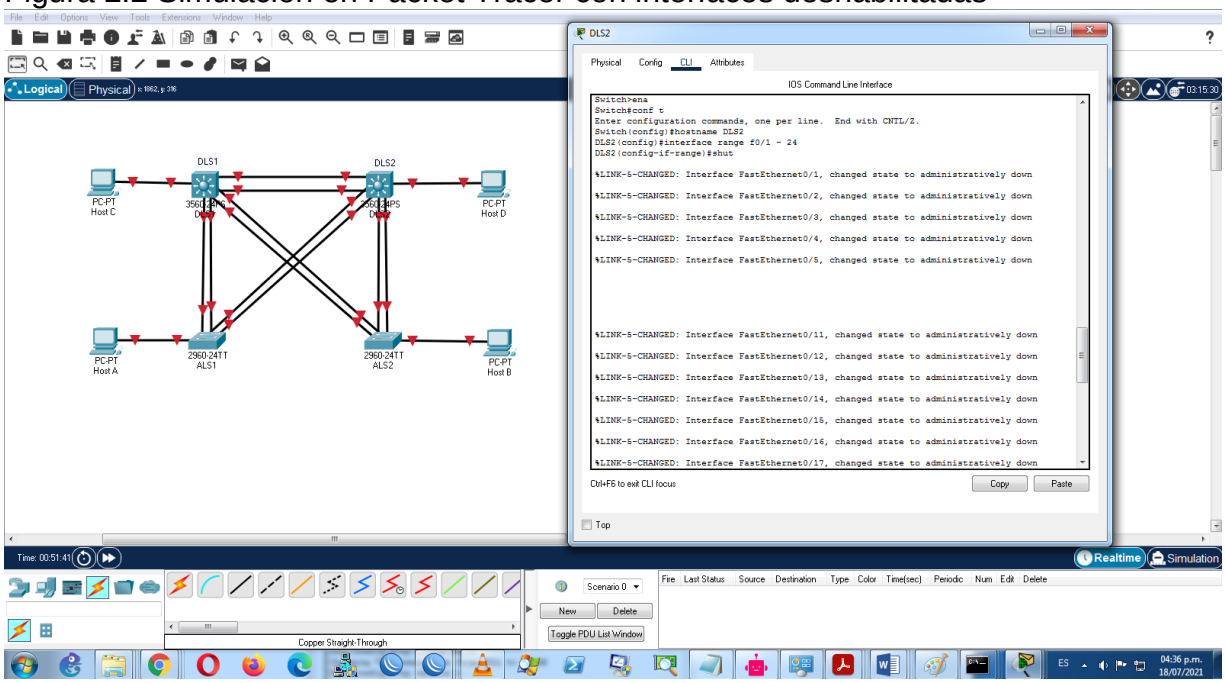
a. Apagar todas las interfaces en cada switch.

Configuración global en los 4 Switch en modo configuración global:

```
interface range f0/1-24          (cambia a modo rango de interfaces)
    shutdown                     (deshabilita las interfaces del rango)
```

En la Figura 2.2 vemos la simulación en Packet Tracer con todas las interfaces conectadas deshabilitadas inicialmente para evitar inconsistencias o loops durante la configuración de redundancia

Figura 2.2 Simulación en Packet Tracer con interfaces deshabilitadas



Fuente: Autor

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

Configuración global en Switch DLS1:

Hostname DLS1 (asigna nombre DLS1, modo configuración global)

Configuración global en Switch DLS2:

Hostname DLS2 (asigna nombre DLS2, modo configuración global)

Configuración global en Switch ALS1:

Hostname ALS1 (asigna nombre ALS3, modo configuración global)

Configuración global en Switch ALS2:

Hostname ALS2 (asigna nombre ALS4, modo configuración global)

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

1) La conexión entre DLS1 y DLS2 será un EtherChannel capa-3 de LACP. Para DLS1 se utilizará la dirección IP 10.20.20.1/30 y para DLS2 utilizará 10.20.20.2/30.

Configuración de interfaz L3 Port-Channel 12 en DLS1

```
interface range f0/11-12                    (cambia a modo rango de interfaces f0/11-12)
      channel-group 12 mode active          (crea etherchannel 12 LACP activo y asocia interfaces)
interface Port-channel12                    (cambia a modo interfaz port-channel 12)
      no switchport                         (deshabilita funcionalidad switching y habilita routing)
      ip address 10.20.20.1 255.255.255.252 (asigna dirección IP y mascara de subred)
```

Configuración de interfaz L3 Port-Channel 12 en DLS2

```
interface range f0/11-12                    (cambia a modo rango de interfaces f0/11-12)
      channel-group 12 mode active          (crea etherchannel 12 LACP activo y asocia interfaces)
interface Port-channel12                    (cambia a modo interfaz port-channel 12)
      no switchport                         (deshabilita funcionalidad switching y habilita routing)
      ip address 10.20.20.2 255.255.255.252 (asigna dirección IP y mascara de subred)
```

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

Configuración de interfaz L2 Port-Channel 1 en DLS1 y ALS1

```
interface range f0/7-8                      (cambia a modo rango de interfaces f0/7-8)
      channel-group 1 mode active           (crea etherchannel 1 LACP activo y asocia interfaces)
interface Port-channel1                     (cambia a modo interfaz port-channel 1)
      switchport trunk encapsulation dot1q  (asigna la encapsulación DOT1Q en modo troncal)
      switchport mode trunk                 (habilita switching en modo troncal)
```

Configuración de interfaz L2 Port-Channel 2 en DLS2 y ALS2

```
interface range f0/7-8                      (cambia a modo rango de interfaces)
      channel-group 2 mode active           (crea etherchannel 2 LACP activo y asocia interfaces)
interface Port-channel2                     (cambia a modo interfaz port-channel 2)
      switchport trunk encapsulation dot1q  (asigna la encapsulación DOT1Q en modo troncal)
      switchport mode trunk                 (habilita switching en modo troncal)
```

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

Configuración de interfaz L2 Port-Channel 3 en DLS2 y ALS1

```
interface range f0/9-10                     (cambia a modo rango de interfaces)
      channel-group 3 mode desirable        (crea etherchannel 3 PAGP desirable y asocia rango)
interface Port-channel3                     (cambia a modo interfaz port-channel 3)
      switchport trunk encapsulation dot1q  (asigna la encapsulación DOT1Q en modo troncal)
      switchport mode trunk                 (habilita switching en modo troncal)
```

Configuración de interfaz L2 Port-Channel 4 en DLS1 y ALS2

```
interface range f0/9-10                     (cambia a modo rango de interfaces)
      channel-group 4 mode desirable        (crea etherchannel 4 PAGP desirable y asocia rango)
interface Port-channel4                     (cambia a modo interfaz port-channel 4)
      switchport trunk encapsulation dot1q  (asigna la encapsulación DOT1Q en modo troncal)
      switchport mode trunk                 (habilita switching en modo troncal)
```

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

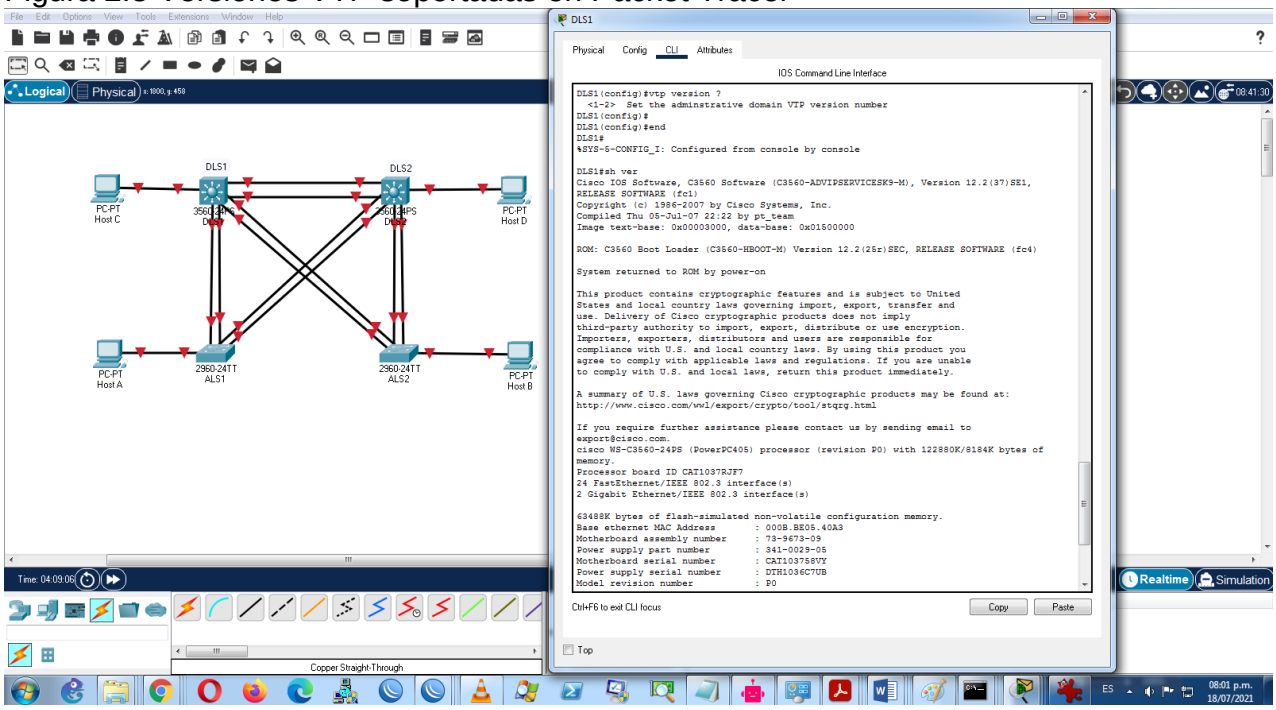
Configuración en cada interfaz L2 Port-Channel de los 4 Switch

switchport trunk native vlan 500 (asigna vlan nativa en modo interfaz Port-Channel)

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

Como se observa en la Figura 2.3 Packet Tracer no soporta VTP versión 3 por lo que se configura versión 2:

Figura 2.3 Versiones VTP soportadas en Packet Tracer



Fuente: Autor

1) Utilizar el nombre de dominio CISCO con la contraseña ccnp321
2) Configurar DLS1 como servidor principal para las VLAN.
3) Configurar ALS1 y ALS2 como clientes VTP.

Configuración de servidor VTP en DLS1

vtp version 2 (asigna última version disponible VTP de 2)
vtp domain CISCO (asigna nombre de dominio VTP)
vtp password ccnp321 (asigna contraseña VTP)
vtp mode server (asigna rol servidor VTP)

Configuración de clientes VTP en ALS1 y ALS2

```
vtp version 2                  (asigna última version disponible VTP de 2)
vtp domain CISCO               (asigna nombre de dominio VTP)
vtp password ccnp321           (asigna contraseña VTP)
vtp mode client                (asigna rol cliente VTP)
```

e. Configurar en el servidor principal las siguientes VLAN:

Tabla 2.1 VLANs por departamento

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
600	**NATIVA**	420	**PROVEEDORES**
15	**ADMON**	100	**SEGUROS**
240	**CLIENTES**	1050	**VENTAS**
1112	**MULTIMEDIA**	3550	**PERSONAL**

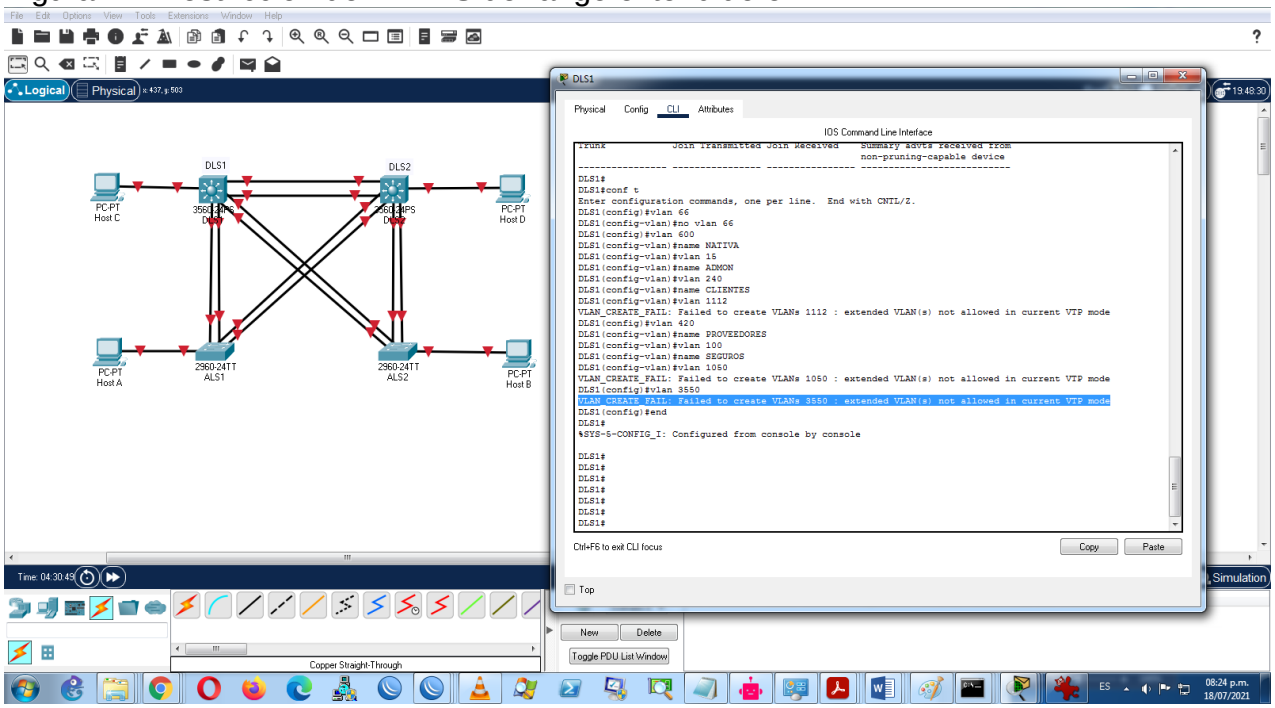
Fuente: UNAD

Configuración de las VLAN en servidor VTP DLS1 (se asigna la vlan 500 como la nativa debido a que esta se asignó como nativa en el paso c-4:

```
vlan 500                       (crea vlan 500 en modo configuración global)
    name NATIVA                (asigna nombre NATIVA en modo vlan 500)
vlan 15                        (crea vlan 15 en modo configuración global)
    name ADMON                 (asigna nombre ADMON en modo vlan 15)
vlan 240                       (crea vlan 240 en modo configuración global)
    name CLIENTES              (asigna nombre CLIENTES en modo vlan 240)
vlan 1112                      (crea vlan 1112 en modo configuración global)
    name MULTIMEDIA            (asigna nombre MULTIMEDIA en modo vlan 1112)
vlan 420                       (crea vlan 420 en modo configuración global)
    name PROVEEDORES           (asigna nombre PROVEEDORES en modo vlan 420)
vlan 100                       (crea vlan 100 en modo configuración global)
    name SEGUROS               (asigna nombre SEGUROS en modo vlan 100)
vlan 1050                      (crea vlan 1050 en modo configuración global)
    name VENTAS                (asigna nombre VENTAS en modo vlan 1050)
vlan 3550                      (crea vlan 3550 en modo configuración global)
    name PERSONAL              (asigna nombre PERSONAL en modo vlan 3550)
```

Debido a que Packet Tracer no soporta VTP versión 3 tampoco permite crear 3 VLANS de la lista por ser de rango extendido, como puede verse en la Figura 2.4.

Figura 2.4 Restricción de VLANS de rango extendido en VTP v2



Fuente: Autor

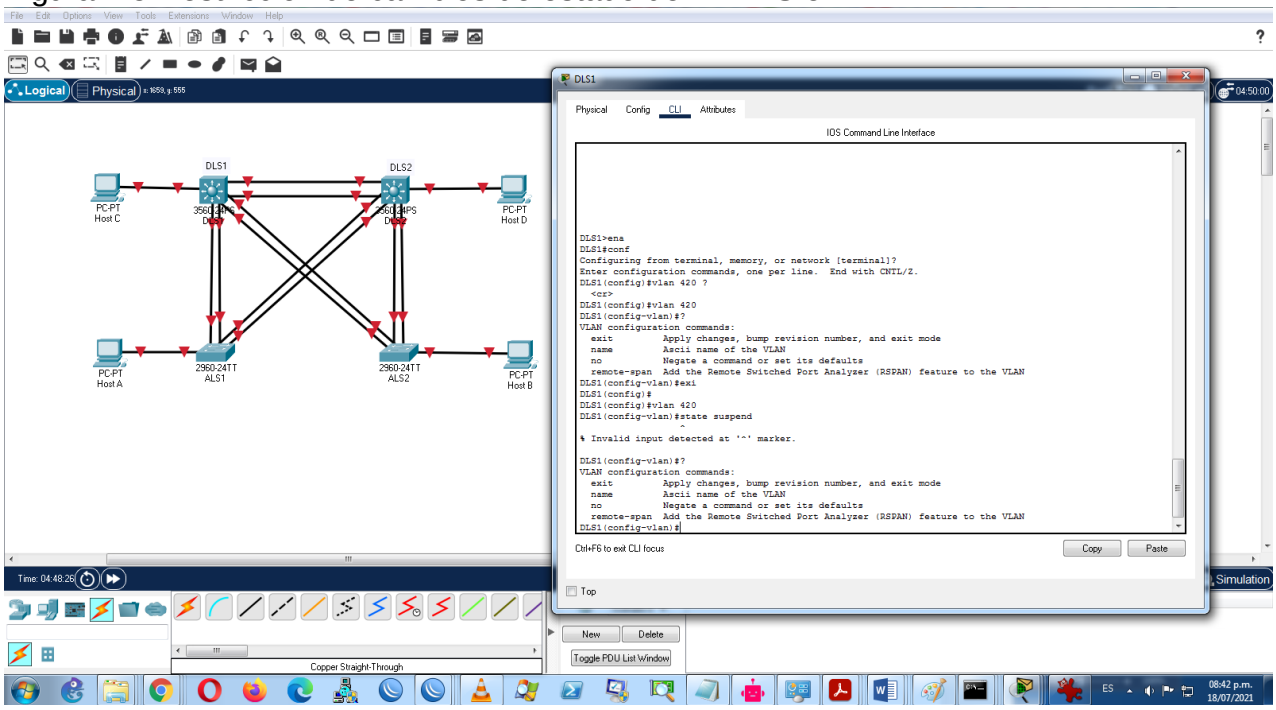
f. En DLS1, suspender la VLAN 420.

Suspensión de VLAN 420 en servidor VTP DLS1

```
vlan 420                    (cambia a modo vlan 420)
    state suspend           (pone la VLAN en estado suspendido)
```

Packet Tracer tampoco permite cambiar de estado administrativamente una VLAN como vemos en la Figura 2.5

Figura 2.5 Restricción de cambios de estado de VLANS en VTP v2



Fuente: Autor

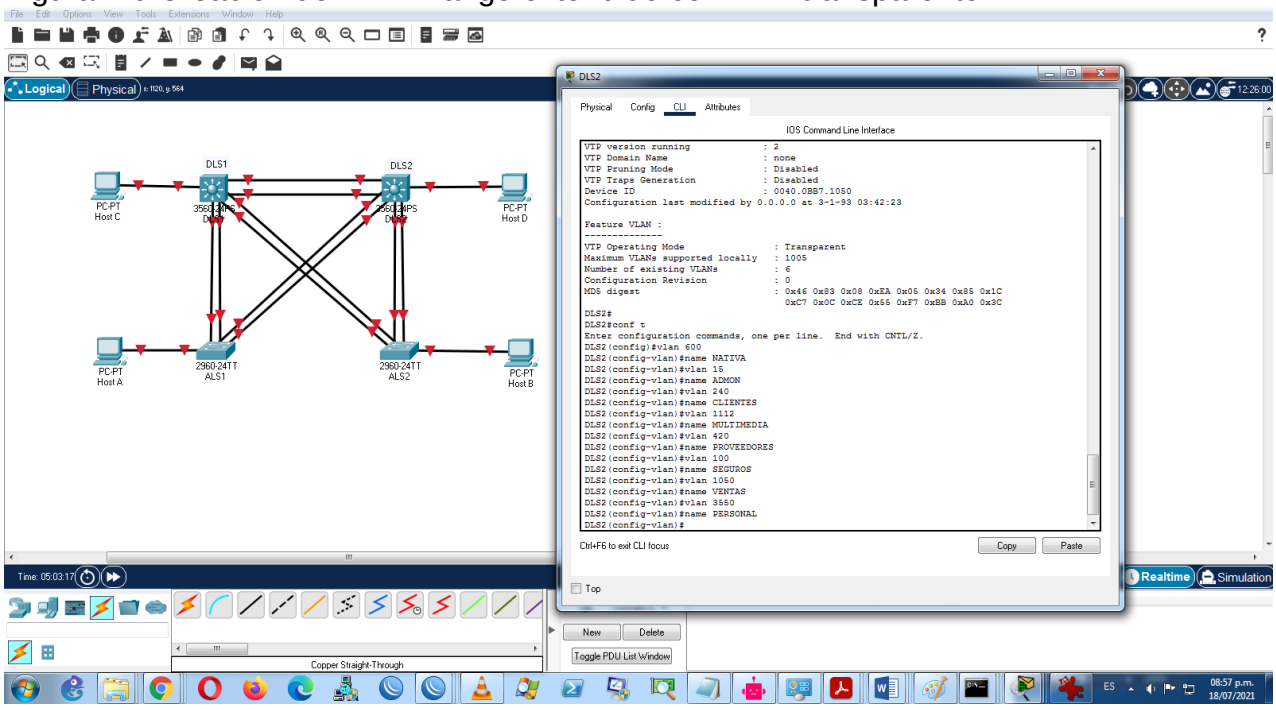
g. Configurar DLS2 en modo VTP transparente VTP utilizando VTP versión 2, y configurar en DLS2 las mismas VLAN que en DLS1.

Configuración de DLS1 en modo VTP transparente

vtp version 2	(asigna última version disponible VTP de 2)
vtp domain CISCO	(asigna nombre de dominio VTP)
vtp password ccnp321	(asigna contraseña VTP)
vtp mode transparent	(asigna modo VTP transparente)

La configuración de las VLAN en DLS2 se realiza con los mismos comandos para configurar las VLAN en DLS1 del paso 1e, pero a diferencia de DLS1 en DLS2 si es posible configurar VLAN de rango extendido como se confirma en la Figura 2.6 debido a que VTP no limita las VLAN disponibles en modo VTP transparente incluso teniendo la misma versión 2 de VTP

Figura 2.6 Creación de VLAN rango extendido con VTP transparente



Fuente: Autor

h. Suspender VLAN 420 en DLS2.

Como se evidencio en el paso 1f Packet Tracer no soporta el cambio de estado de una VLAN incluso si el modo VTP del switch es transparente

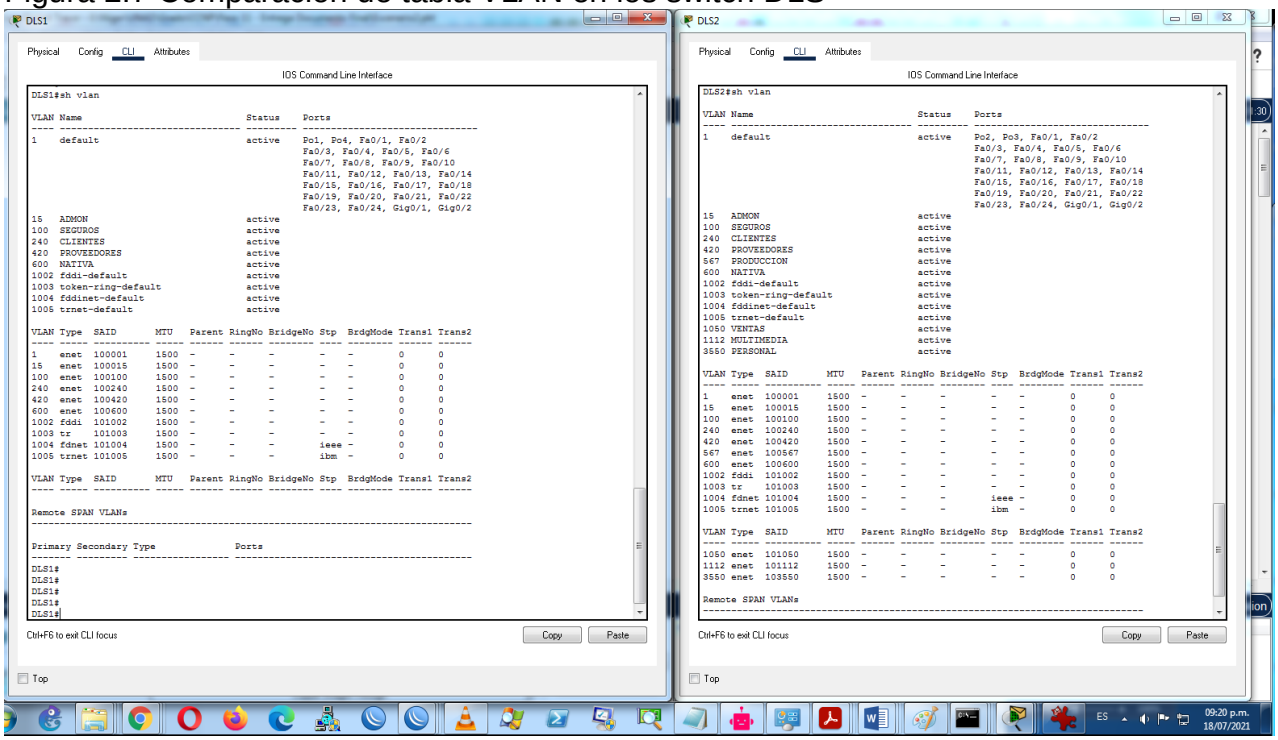
i. En DLS2, crear VLAN 567 con el nombre de PRODUCCION. La VLAN de PRODUCCION no podrá estar disponible en cualquier otro Switch de la red.

Configuración de VLAN en DLS2 en modo VTP transparente

```
vlan 567                                  (crea vlan 567 en modo privilegiado)
    name PRODUCCION                       (asigna nombre PRODUCCION en modo vlan 567)
```

En la Figura 2.7 vemos una comparación de tabla de VLANs en DLS1 vs DLS2 donde se observa que efectivamente la VLAN 567 solo queda creada en DLS2 donde además si quedan las VLAN de rango extendido

Figura 2.7 Comparación de tabla VLAN en los switch DLS



Fuente: Autor

j. Configurar DLS1 como Spanning tree root para las VLANs 1, 12, 420, 600, 1050, 1112 y 3550 y como raíz secundaria para las VLAN 100 y 240.

Configuración de prioridades STP en DLS1 en modo privilegiado

spanning-tree vlan 1,12,420,600,1050,1112,3550 root primary	(asigna VLANs para raíz primaria)
spanning-tree vlan 100,240 root secondary	(asigna VLANs para raíz secundaria)

k. Configurar DLS2 como Spanning tree root para las VLAN 100 y 240 y como una raíz secundaria para las VLAN 15, 420, 600, 1050, 1112 y 3550.

Configuración de prioridades STP en DLS2 en modo privilegiado

spanning-tree vlan 100,240 root primary	(asigna VLANs para raíz primaria)
spanning-tree vlan 15,420,600,1050,1112,3550 root secondary	(asigna VLANs para raíz secundaria)

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

Configuración en los 4 switch de las VLAN habilitadas en los enlaces troncales:

DLS1

```
interface Port-channel1                                          (modo interfaz Port-channel1)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel4                                          (modo interfaz Port-channel4)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

DLS2

```
interface Port-channel2                                          (modo interfaz Port-channel2)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel3                                          (modo interfaz Port-channel3)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

ALS1

```
interface Port-channel1                                          (modo interfaz Port-channel1)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel3                                          (modo interfaz Port-channel3)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

ALS2

```
interface Port-channel2                                          (modo interfaz Port-channel2)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel4                                          (modo interfaz Port-channel4)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

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

Tabla 2.2 Asignación de VLANs en puertos de acceso

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3550	15, 1050	100, 1050	240
Interfaz Fa0/15	1112	1112	1112	1112
Interfaces F0 /16-18		567		

Fuente: Autor

Solo se permite configurar una VLAN en modo acceso por puerto ya que el tráfico fluye sin etiqueta alguna de VLAN, por ello se realiza la configuración de esta manera:

Configuración de interfaces en modo acceso en DLS1

```
interface f0/6                          (cambia a modo interfaz f0/6)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 3550         (asigna VLAN 3550 en modo acceso)
interface f0/15                         (cambia a modo interfaz f0/15)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112         (asigna VLAN 1112 en modo acceso)
```

Configuración de interfaces en modo acceso en DLS2

```
interface f0/6                          (cambia a modo interfaz f0/6)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 15           (asigna VLAN 15 en modo acceso)
interface f0/15                         (cambia a modo interfaz f0/15)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112         (asigna VLAN 1112 en modo acceso)
interface range f0/16-18                (cambia a modo rango de interfaz f0/16-18)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 567          (asigna VLAN 567 en modo acceso)
```

Configuración de interfaces en modo acceso en ALS1

```
interface f0/6                          (cambia a modo interfaz f0/6)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 100          (asigna VLAN 100 en modo acceso)
interface f0/15                         (cambia a modo interfaz f0/15)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112         (asigna VLAN 1112 en modo acceso)
```

Configuración de interfaces en modo acceso en ALS2

```
interface range f0/6                    (cambia a modo rango de interfaz f0/6)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 240          (asigna VLAN 240 en modo acceso)
interface range f0/15                   (cambia a modo rango de interfaz f0/15)
    switchport mode access              (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112         (asigna VLAN 1112 en modo acceso)
```

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

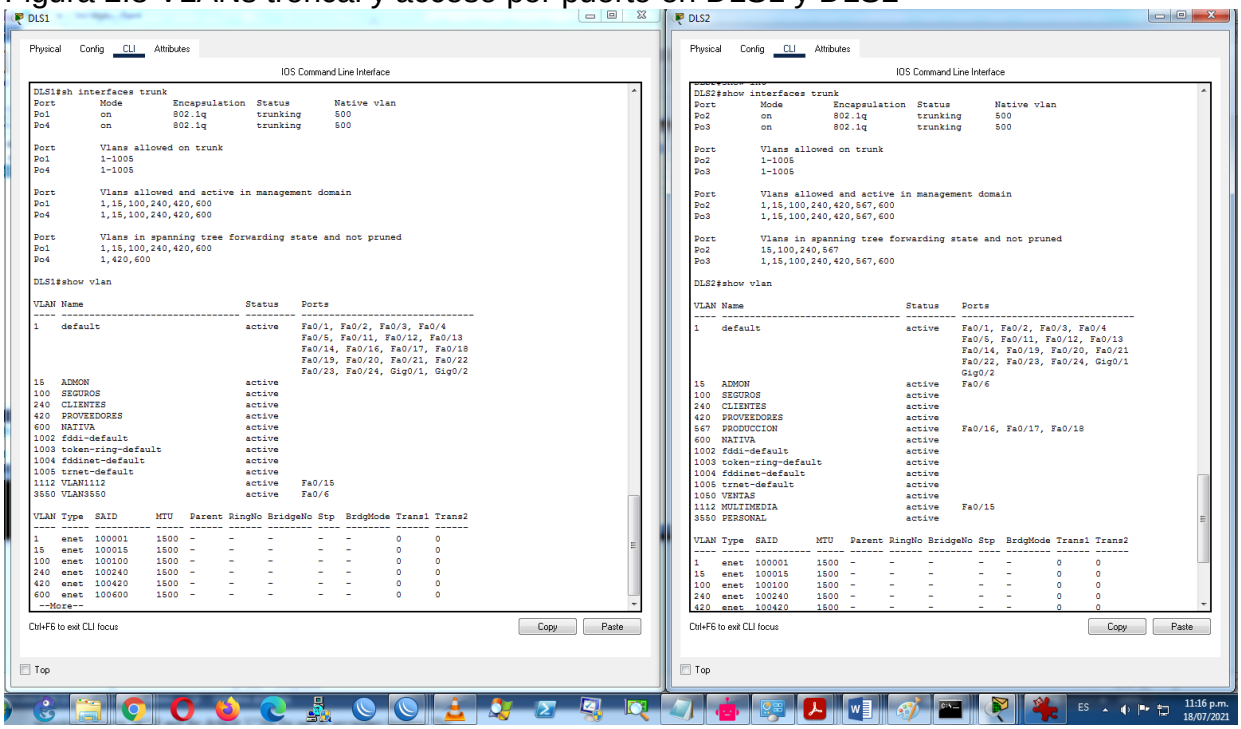
a. Verificar la existencia de las VLAN correctas en todos los switches y la asignación de puertos troncales y de acceso

En los 4 Switch se habilitan las interfaces deshabilitadas en el paso 1a:

```
interface range f0/1-24                 (cambia a modo rango de interfaces f0/1-24)
    no shutdown                         (deshabilita las interfaces del rango)
```

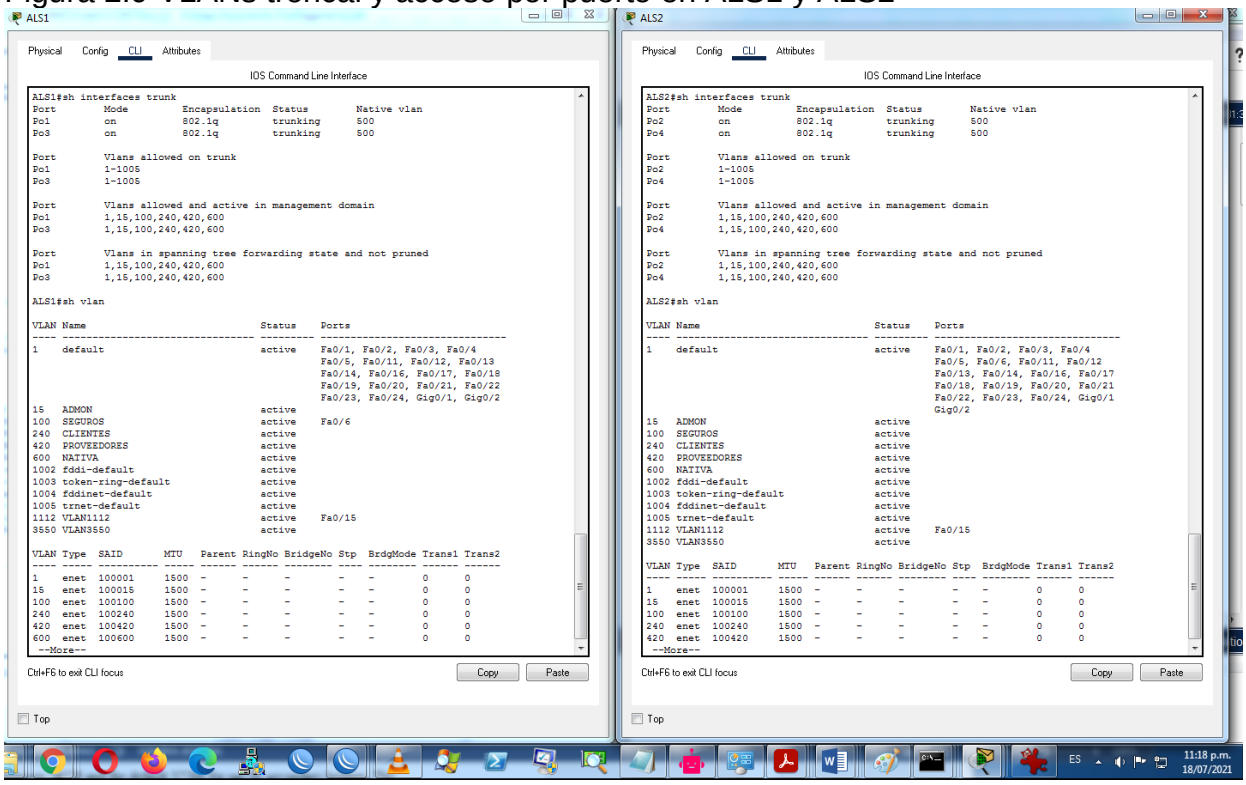
Después de habilitar administrativamente las interfaces verificamos en la Figura 2.8 y 2.9 ejecutando show interfaces trunk que las interfaces troncales quedaron creadas y agrupadas satisfactoriamente en interfaces Port-channel en DLS1 y ALS1 de acuerdo a las VLAN asignada, mientras que con show vlan verificamos que la configuración manual de VLAN del servidor VTP DLS1 se configura automáticamente en los clientes ALS sin que tengan en cuenta la configuración manual del switch transparente DLS2, por ejemplo crean la VLAN 567 de DLS2.

Figura 2.8 VLANs troncal y acceso por puerto en DLS1 y DLS2



Fuente: Autor

Figura 2.9 VLANs troncal y acceso por puerto en ALS1 y ALS2

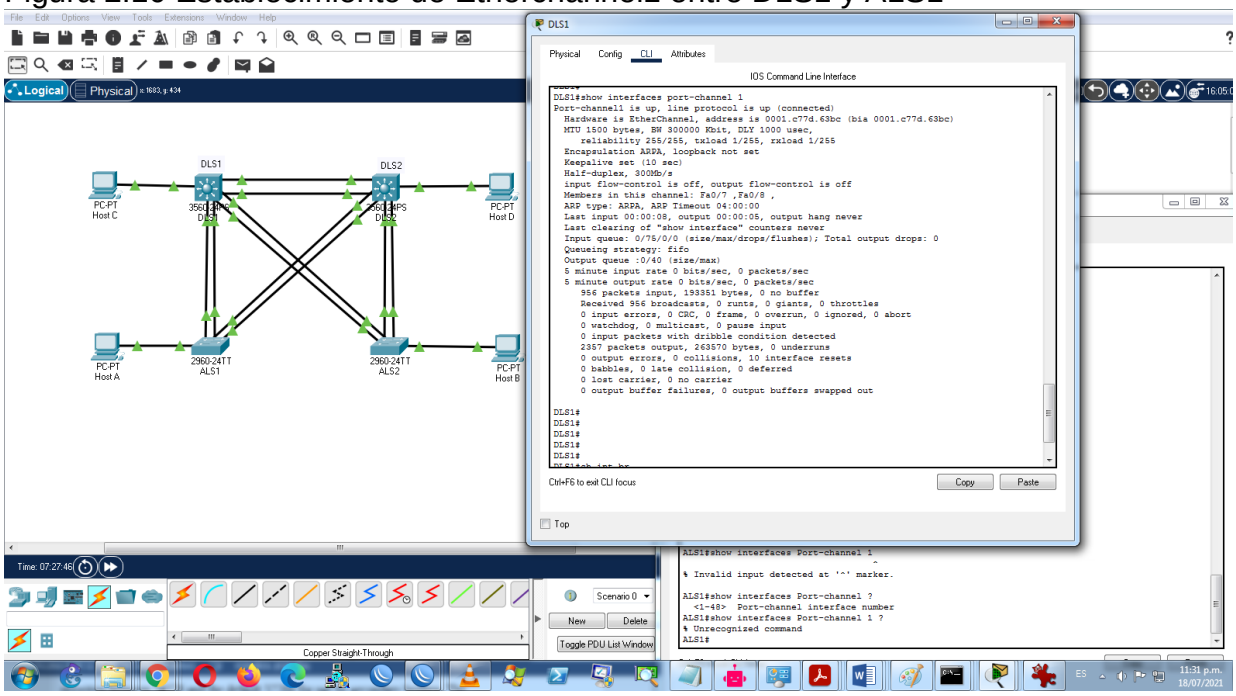


Fuente: Autor

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

Ejecutando show interface port-channel 1 en DLS1 o en ALS1 verificamos el estado up-up lo que indica que la interfaz ya está habilitada física y lógicamente, además vemos conteo de paquetes transmitidos y recibidos confirmando así su funcionalidad entre ambos extremos, tal como se observa en la Figura 2.10:

Figura 2.10 Establecimiento de Etherchannel1 entre DLS1 y ALS1

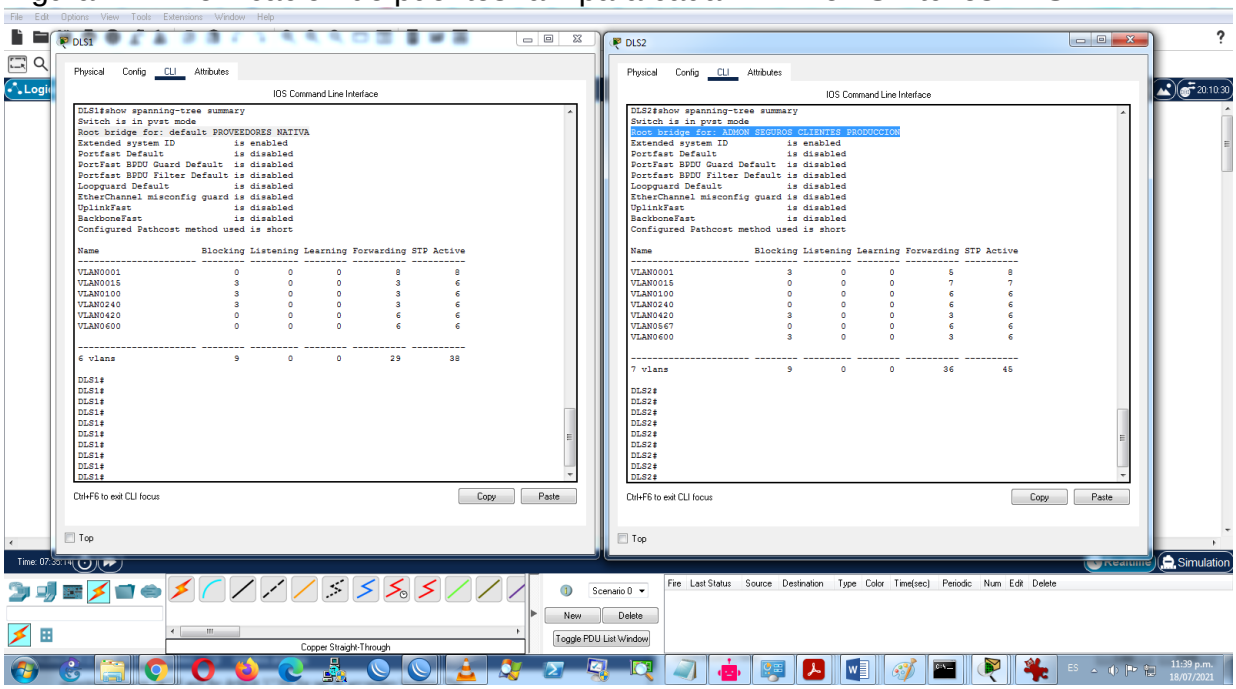


Fuente: Autor

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

La asignación de VLAN de Spanning tree entre DLS1 y DLS2 se verifica en cada switch con show spanning-tree summary como vemos en la Figura 2.11, en la segunda línea resaltada de resultado vemos la asignación del puente raíz

Figura 2.11 Verificación de puentes raíz para cada VLAN en Switches DLS



Fuente: Autor

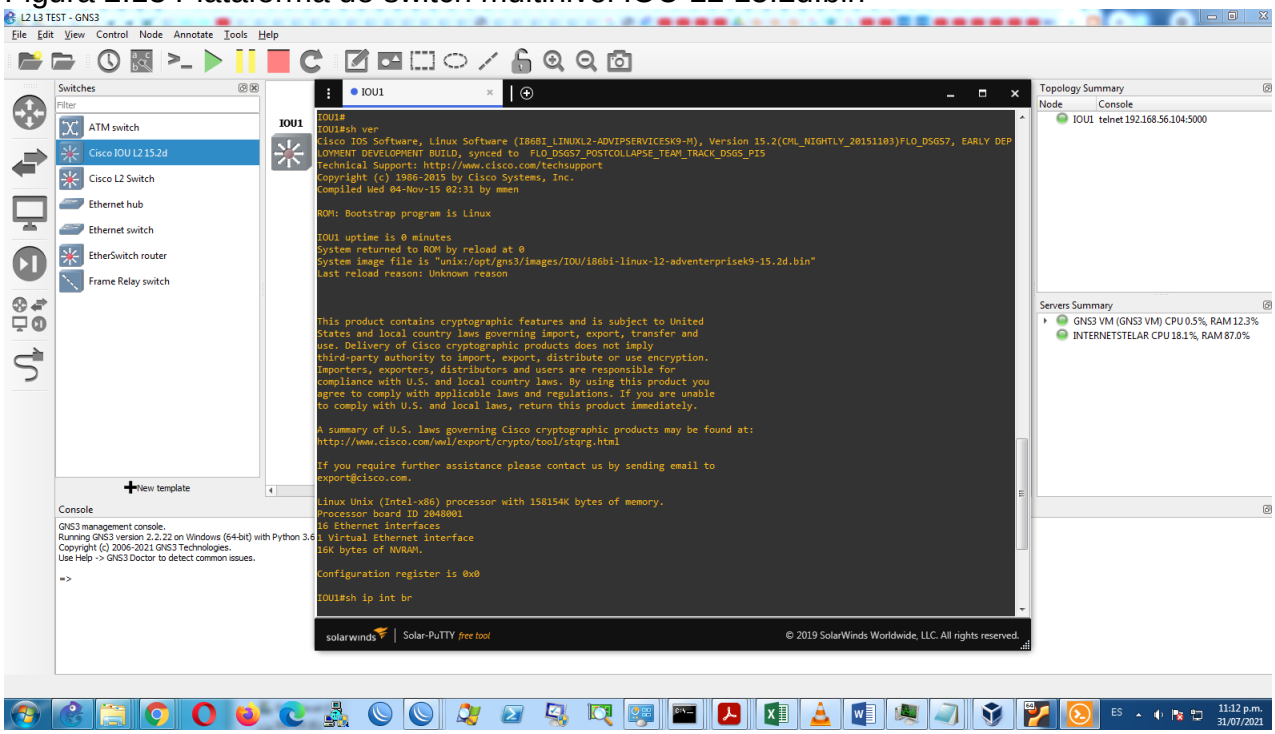
Simulación en GNS3

Esta simulación es relativamente más difícil de implementar pero más funcional, se simulan 4 switch L2 mediante máquina virtual Virtualbox 2.2.22 y plataforma de switch multinivel IOU L2 15.2d.bin, como se aprecia en la Figura 2.12 y Figura 2.13

Figura 2.12 Virtualización en GNS3 mediante VM Virtualbox 2.2.22

Fuente: Autor

Figura 2.13 Plataforma de switch multinivel IOU L2 15.2d.bin



Fuente: Autor

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

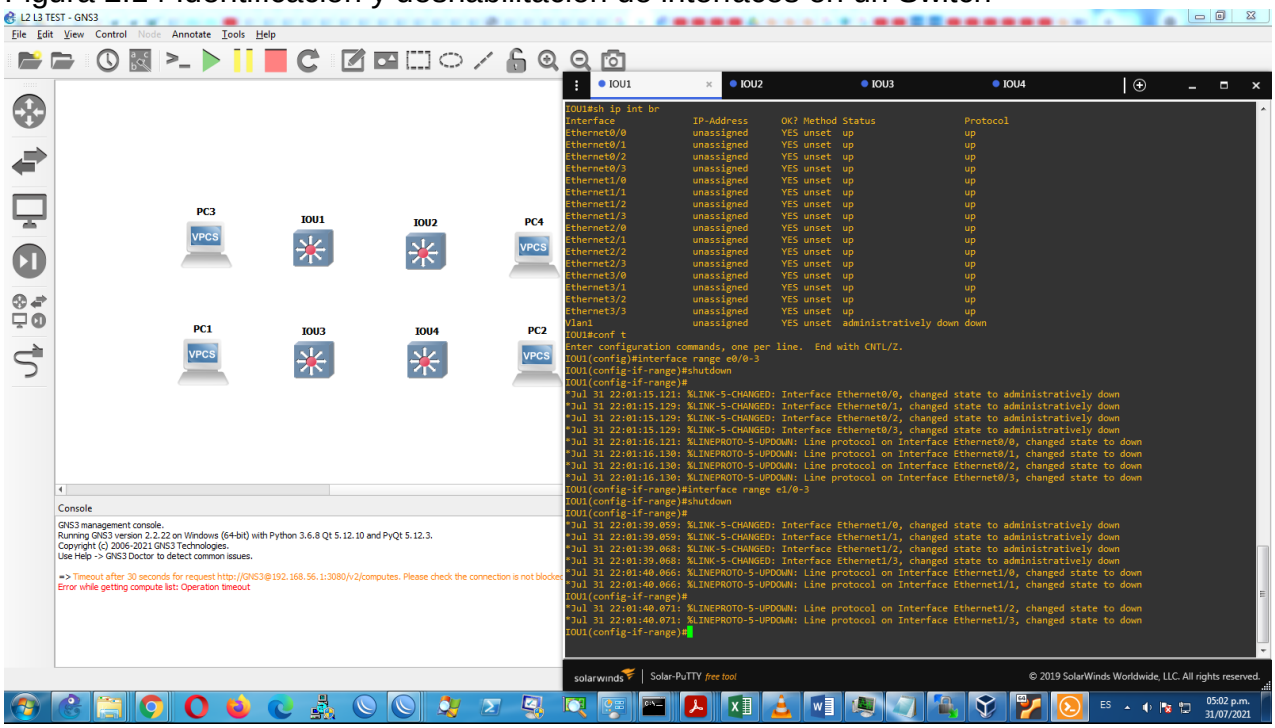
a. Apagar todas las interfaces en cada switch.

Primero se identifican las interfaces presentes en los Switch mediante el comando show ip interfaces brief, para después deshabilitarlas manualmente como se ve a continuación y en el ejemplo de la Figura 2.14:

Configuración global en los 4 Switch en modo global:

```
interface range e0/0-3          (cambia a modo rango de interfaces Ethernet 0/0-3)
    shutdown                    (deshabilita las interfaces del rango)
interface range e1/0-3          (cambia a modo rango de interfaces Ethernet 1/0-3)
    shutdown                    (deshabilita las interfaces del rango)
interface range e2/0-3          (cambia a modo rango de interfaces Ethernet 2/0-3)
    shutdown                    (deshabilita las interfaces del rango)
interface range e3/0-3          (cambia a modo rango de interfaces Ethernet 3/0-3)
    shutdown                    (deshabilita las interfaces del rango)
```

Figura 2.14 Identificación y deshabilitación de interfaces en un Switch



Fuente: Autor

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

Configuración global en Switch DLS1:

Hostname DLS1 (asigna nombre DLS1, modo configuración global)

Configuración global en Switch DLS2:

Hostname DLS2 (asigna nombre DLS2, modo configuración global)

Configuración global en Switch ALS1:

Hostname ALS1 (asigna nombre ALS3, modo configuración global)

Configuración global en Switch ALS2:

Hostname ALS2 (asigna nombre ALS4, modo configuración global)

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

1) La conexión entre DLS1 y DLS2 será un EtherChannel capa-3 de LACP. Para DLS1 se utilizará la dirección IP 10.20.20.1/30 y para DLS2 utilizará 10.20.20.2/30.

Configuración de interfaz L3 Port-Channel 12 en DLS1

```
interface range E2/0-1                          (cambia a modo rango de interfaces E2/0-1)
      no switchport                             (deshabilita funcionalidad switching y habilita routing)
      channel-group 12 mode active              (crea etherchannel 12 LACP activo y asocia interfaces)
interface Port-channel12                        (cambia a modo interfaz port-channel 12)
      no switchport                             (deshabilita funcionalidad switching y habilita routing)
      ip address 10.20.20.1 255.255.255.252     (asigna dirección IP y mascara de subred)
```

Configuración de interfaz L3 Port-Channel 12 en DLS2

```
interface range E2/0-1                      (cambia a modo rango de interfaces E2/0-1)
    no switchport                           (deshabilita funcionalidad switching y habilita routing)
    channel-group 12 mode active            (crea etherchannel 12 LACP activo y asocia interfaces)
interface Port-channel12                    (cambia a modo interfaz port-channel 12)
    no switchport                           (deshabilita funcionalidad switching y habilita routing)
    ip address 10.20.20.2 255.255.255.252   (asigna dirección IP y mascara de subred)
```

2) Los Port-channels en las interfaces E1/0 y E1/1 utilizarán LACP.

Configuración de interfaz L2 Port-Channel 1 en DLS1 y ALS1:

```
interface range E1/0-1                      (cambia a modo rango de interfaces E1/0-1)
    switchport mode trunk                   (habilita switching en modo troncal)
    channel-group 1 mode active             (crea etherchannel 1 LACP activo y asocia interfaces)
interface Port-channel1                     (cambia a modo interfaz port-channel 1)
    switchport mode trunk                   (habilita switching en modo troncal)
    switchport trunk encapsulation dot1q    (asigna la encapsulación DOT1Q en modo troncal)
```

Configuración de interfaz L2 Port-Channel 2 en DLS2 y ALS2:

```
interface range E1/0-1                      (cambia a modo rango de interfaces E1/0-1)
    switchport mode trunk                   (habilita switching en modo troncal)
    channel-group 2 mode active             (crea etherchannel 2 LACP activo y asocia interfaces)
interface Port-channel2                     (cambia a modo interfaz port-channel 2)
    switchport mode trunk                   (habilita switching en modo troncal)
    switchport trunk encapsulation dot1q    (asigna la encapsulación DOT1Q en modo troncal)
```

3) Los Port-channels en las interfaces E1/2 y E1/3 utilizará PAgP.

Configuración de interfaz L2 Port-Channel 3 en DLS2 y ALS1:

```
interface range E1/2-3                      (cambia a modo rango de interfaces E1/2-3)
    switchport mode trunk                   (habilita switching en modo troncal)
    channel-group 3 mode desirable          (crea etherchannel 3 PAGP desirable y asocia rango)
interface Port-channel3                     (cambia a modo interfaz port-channel 3)
    switchport mode trunk                   (habilita switching en modo troncal)
    switchport trunk encapsulation dot1q    (asigna la encapsulación DOT1Q en modo troncal)
```

Configuración de interfaz L2 Port-Channel 4 en DLS1 y ALS2:

```
interface range E1/2-3                      (cambia a modo rango de interfaces E1/2-3)
    switchport mode trunk                   (habilita switching en modo troncal)
    channel-group 4 mode desirable          (crea etherchannel 4 PAGP desirable y asocia rango)
interface Port-channel4                     (cambia a modo interfaz port-channel 4)
    switchport mode trunk                   (habilita switching en modo troncal)
    switchport trunk encapsulation dot1q    (asigna la encapsulación DOT1Q en modo troncal)
```

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

Configuración de VLAN nativa en cada interfaz Port-Channel L2 de los 4 Switch y sus rangos de interfaces físicas asociadas

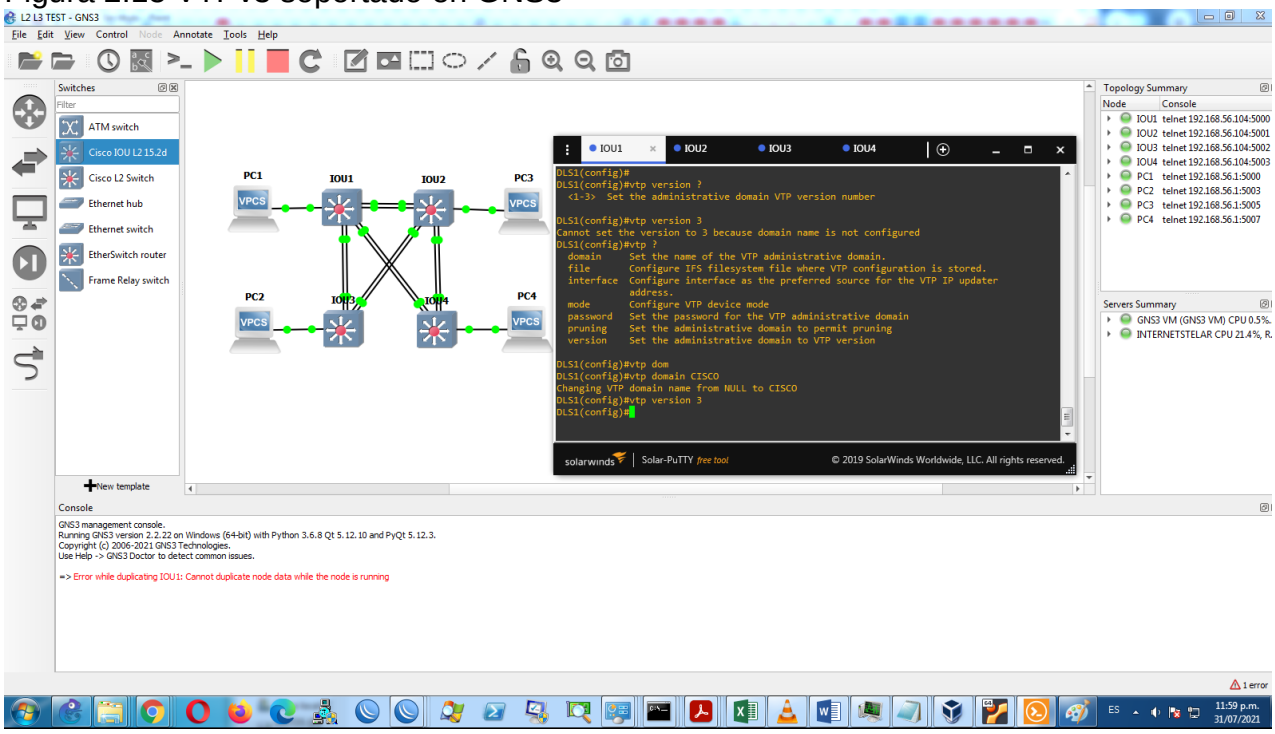
switchport trunk native vlan 500 (asigna vlan nativa en modo interfaz)

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

Como se observa en la Figura 2.15 GNS3 a diferencia de Packet Tracer si soporta VTP versión 3 por lo que se configura versión 3 en los 3 switch DLS1, ALS1, y ALS2, no sin antes configurar el dominio VTP exigido previamente por el IOS:

vtp domain CISCO (asigna dominio VTP en modo global)
vtp versión 3 (asigna version VTP 3 en modo global)

Figura 2.15 VTPv3 soportado en GNS3



Fuente: Autor

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

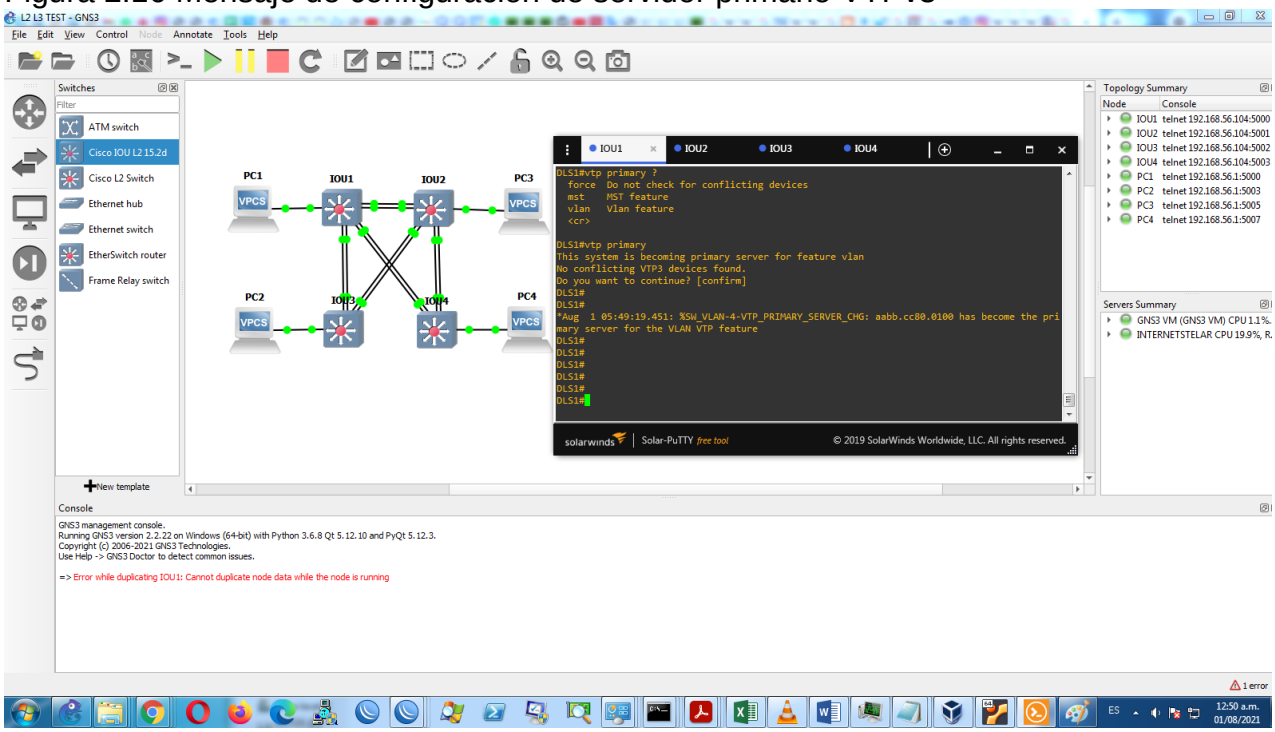
vtp password ccnp321 (asigna password VTP ccnp321 en modo global)

2) Configurar DLS1 como servidor principal para las VLAN.

Solo en VTPv3 se admite la configuración de servidor VTP primario, al ejecutarse aparece un mensaje confirmando que no se produzcan conflictos y la MAC asignada al servidor primario, como se observa en la Figura 2.16.

vtp primary	(asigna rol de servidor VTP primario en modo global)

Figura 2.16 Mensaje de configuración de servidor primario VTPv3



Fuente: Autor

3) Configurar ALS1 y ALS2 como clientes VTP.

Configuración de clientes VTP en ALS1 y ALS2

vtp domain CISCO	(asigna nombre de dominio VTP)
vtp password ccnp321	(asigna contraseña VTP)
vtp mode client	(asigna rol cliente VTP)

e. Configurar en el servidor principal las siguientes VLAN:

Tabla 2.3 VLANs por departamento

Número de VLAN	Nombre de VLAN	Número de VLAN	Nombre de VLAN
600	**NATIVA**	420	**PROVEEDORES**
15	**ADMON**	100	**SEGUROS**
240	**CLIENTES**	1050	**VENTAS**
1112	**MULTIMEDIA**	3550	**PERSONAL**

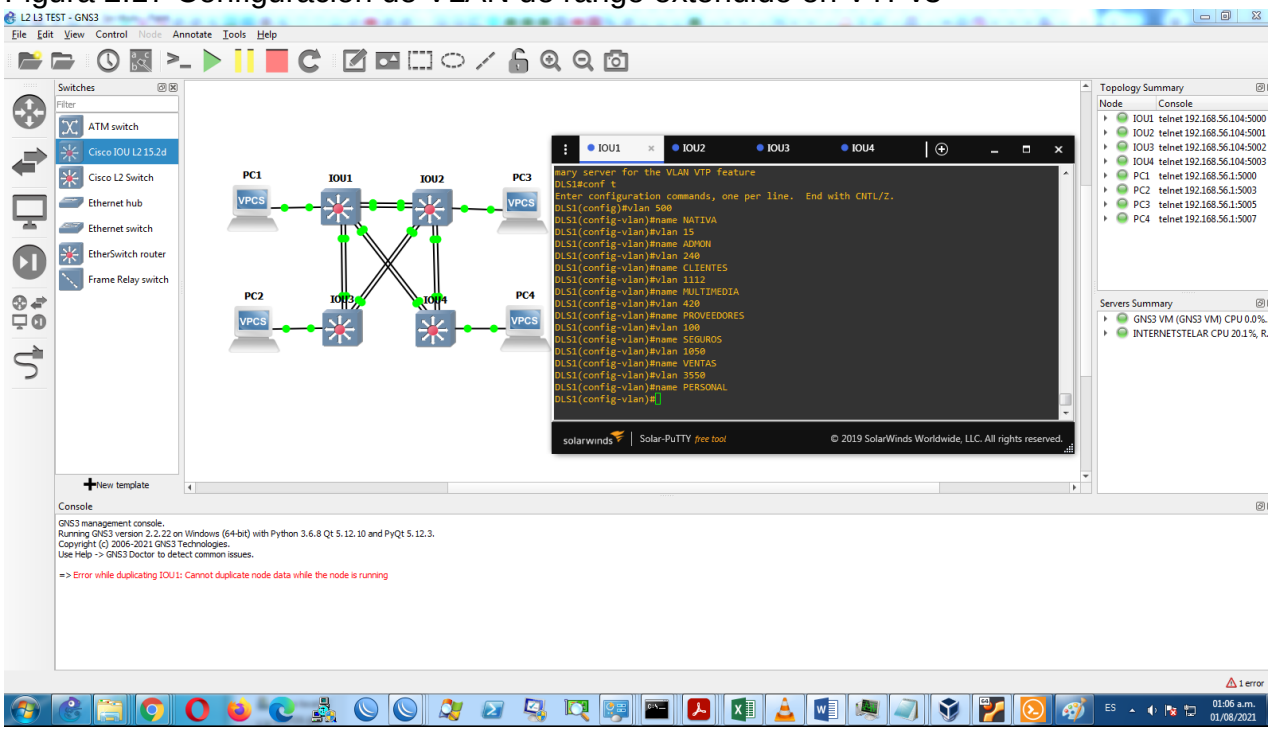
Fuente: UNAD

Configuración de las VLAN en servidor VTP DLS1 (se asigna la vlan 500 como la nativa debido a que esta se asignó como nativa en el paso c-4.

```
vlan 500                          (crea vlan 500 en modo privilegiado)
    name NATIVA                   (asigna nombre NATIVA en modo vlan 500)
vlan 15                           (crea vlan 15 en modo privilegiado)
    name ADMON                    (asigna nombre ADMON en modo vlan 15)
vlan 240                          (crea vlan 240 en modo privilegiado)
    name CLIENTES                 (asigna nombre CLIENTES en modo vlan 240)
vlan 1112                         (crea vlan 1112 en modo privilegiado)
    name MULTIMEDIA               (asigna nombre MULTIMEDIA en modo vlan 1112)
vlan 420                          (crea vlan 420 en modo privilegiado)
    name PROVEEDORES              (asigna nombre PROVEEDORES en modo vlan 420)
vlan 100                          (crea vlan 100 en modo privilegiado)
    name SEGUROS                  (asigna nombre SEGUROS en modo vlan 100)
vlan 1050                         (crea vlan 1050 en modo privilegiado)
    name VENTAS                   (asigna nombre VENTAS en modo vlan 1050)
vlan 3550                         (crea vlan 3550 en modo privilegiado)
    name PERSONAL                 (asigna nombre PERSONAL en modo vlan 3550)
```

Debido a que a diferencia de Packet Tracer, GNS3 si soporta VTP versión 3 permite crear también VLANS de rango extendido, como puede verse en la Figura 2.17.

Figura 2.17 Configuración de VLAN de rango extendido en VTPv3



Fuente: Autor

f. En DLS1, suspender la VLAN 420.

Suspensión de VLAN 420 en servidor VTP DLS1

A diferencia de Packet Tracer, GNS3 sí reconoce el comando para cambiar de estado administrativamente una VLAN:

```
vlan 420                    (cambia a modo vlan 420)
    state suspend           (pone la VLAN en estado suspendido)
```

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

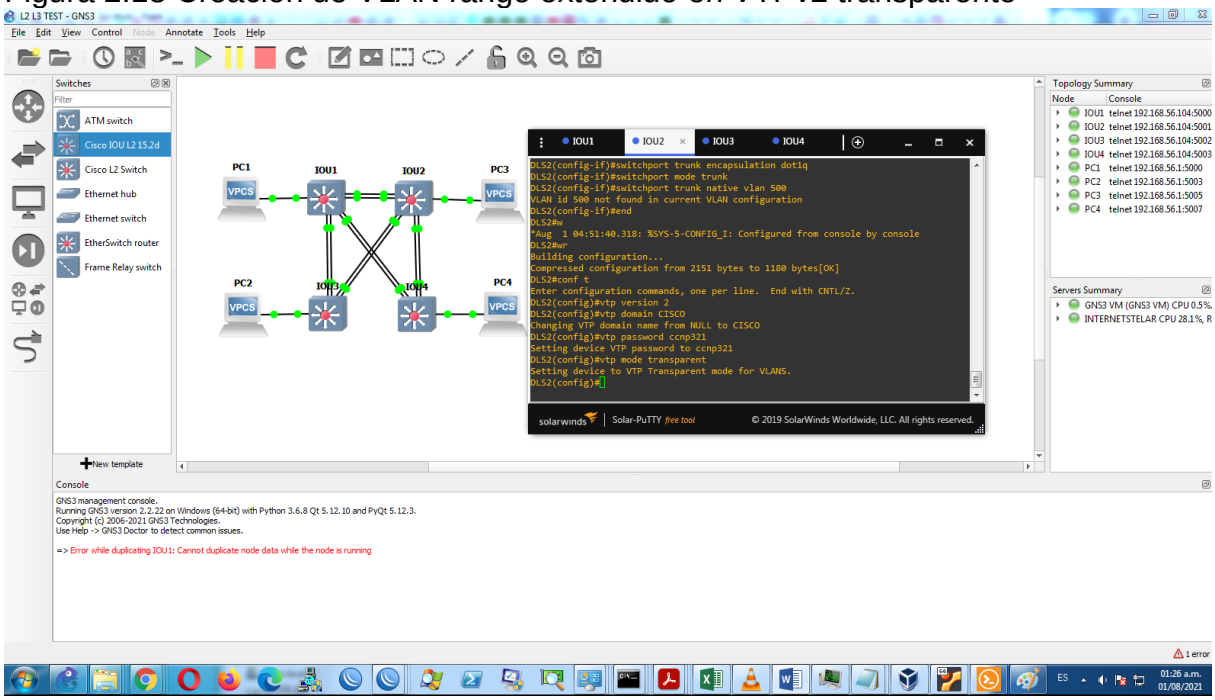
Configuración de DLS2 en VTP versión 2 y modo VTP transparente

```
vtp version 2               (asigna última version disponible VTP de 2)
vtp domain CISCO            (asigna nombre de dominio VTP)
vtp password ccnp321        (asigna contraseña VTP)
vtp mode transparent        (asigna modo VTP transparente)
```

La configuración de las VLAN en DLS2 se realiza con los mismos comandos para configurar las VLAN en DLS1 del paso 1e, a pesar de que en DLS2 no es posible

que las VLAN de rango extendido participen de VTP version 2, es viable configurar estas al asignar el modo de VTP en transparente como se confirma en la Figura 2.18.

Figura 2.18 Creación de VLAN rango extendido en VTPv2 transparente



Fuente: Autor

h. Suspender VLAN 420 en DLS2.

```
vlan 420                          (cambia a modo vlan 420)
    state suspend                 (pone la VLAN en estado suspendido)
```

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.

Configuración de VLAN en DLS2 en modo VTP transparente

```
vlan 567                          (crea vlan 567 en modo privilegiado)
  name PRODUCCION                 (asigna nombre PRODUCCION en modo vlan 567)
```

j. Configurar DLS1 como Spanning tree root para las VLANs 1, 12, 420, 500, 1050, 1112 y 3550 y como raíz secundaria para las VLAN 100 y 240.

Configuración de prioridades STP en DLS1 en modo global

```
spanning-tree vlan 1,12,420,500,1050,1112,3550 root primary     (asigna VLANs para raíz primaria)
spanning-tree vlan 100,240 root secondary                       (asigna VLANs para raíz secundaria)
```

k. Configurar DLS2 como Spanning tree root para las VLAN 100 y 240 y como una raíz secundaria para las VLAN 15, 420, 500, 1050, 1112 y 3550.

Configuración de prioridades STP en DLS2 en modo global

```
spanning-tree vlan 100,240 root primary                         (asigna VLANs para raíz primaria)
spanning-tree vlan 15,420,500,1050,1112,3550 root secondary     (asigna VLANs para raíz secundaria)
```

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

Configuración en los 4 switch de las VLAN habilitadas en los enlaces troncales:

DLS1

```
interface Port-channel1                                         (modo interfaz Port-channel1)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel4                                         (modo interfaz Port-channel4)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

DLS2

```
interface Port-channel2                                         (modo interfaz Port-channel2)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel3                                         (modo interfaz Port-channel3)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

ALS1

```
interface Port-channel1                                         (modo interfaz Port-channel1)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel3                                         (modo interfaz Port-channel3)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

ALS2

```
interface Port-channel2                                         (modo interfaz Port-channel2)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
interface Port-channel4                                         (modo interfaz Port-channel4)
    switchport trunk allowed vlan 15,100,240,420,500,1050,1112,3550   (lista VLAN habilitadas en troncal)
```

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

Tabla 2.4 Asignación de VLANs en puertos de acceso

Interfaz	DLS1	DLS2	ALS1	ALS2
Interfaz Fa0/6	3550	15, 1050	100, 1050	240
Interfaz Fa0/15	1112	1112	1112	1112
Interfaces F0 /16-18		567		

Fuente: UNAD

Solo se permite configurar una VLAN en modo acceso por puerto ya que el tráfico fluye sin etiqueta alguna de VLAN, adicionalmente dado que los switch simulados en GNS3 tienen otra nomenclatura se realiza la configuración de esta manera:

Configuración de interfaces en modo acceso en DLS1

```
interface E0/0                      (cambia a modo interfaz E0/0)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 3550     (asigna VLAN 3550 en modo acceso)
interface E3/0                      (cambia a modo interfaz E3/0)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112     (asigna VLAN 1112 en modo acceso)
```

Configuración de interfaces en modo acceso en DLS2

```
interface E0/0                      (cambia a modo interfaz E0/0)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1050     (asigna VLAN 1050 en modo acceso)
interface E3/0                      (cambia a modo interfaz E3/0)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112     (asigna VLAN 1112 en modo acceso)
interface range E3/0-3              (cambia a modo rango de interfaces E3/0-3)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 567      (asigna VLAN 567 en modo acceso)
```

Configuración de interfaces en modo acceso en ALS1

```
interface E0/0                      (cambia a modo interfaz E0/0)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1050     (asigna VLAN 1050 en modo acceso)
interface E3/0                      (cambia a modo interfaz E3/0)
    switchport mode access          (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112     (asigna VLAN 1112 en modo acceso)
```

Configuración de interfaces en modo acceso en ALS2

```
interface E0/0                  (cambia a modo interfaz E0/0)
    switchport mode access      (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 240  (asigna VLAN 240 en modo acceso)
interface E3/0                  (cambia a modo interfaz E3/0)
    switchport mode access      (asigna modo acceso en puerto con funcionalidad switching)
    switchport access vlan 1112 (asigna VLAN 1112 en modo acceso)
```

Parte 2: Verificar la red de acuerdo con las especificaciones.

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

En los 4 Switch se habilitan las interfaces deshabilitadas en el paso 1a:

```
interface range e0/0-3          (cambia a modo rango de interfaces Ethernet 0/0-3)
    no shutdown                 (deshabilita las interfaces del rango)
interface range e1/0-3          (cambia a modo rango de interfaces Ethernet 1/0-3)
    no shutdown                 (deshabilita las interfaces del rango)
interface range e2/0-3          (cambia a modo rango de interfaces Ethernet 2/0-3)
    no shutdown                 (deshabilita las interfaces del rango)
interface range e3/0-3          (cambia a modo rango de interfaces Ethernet 3/0-3)
    no shutdown                 (deshabilita las interfaces del rango)
```

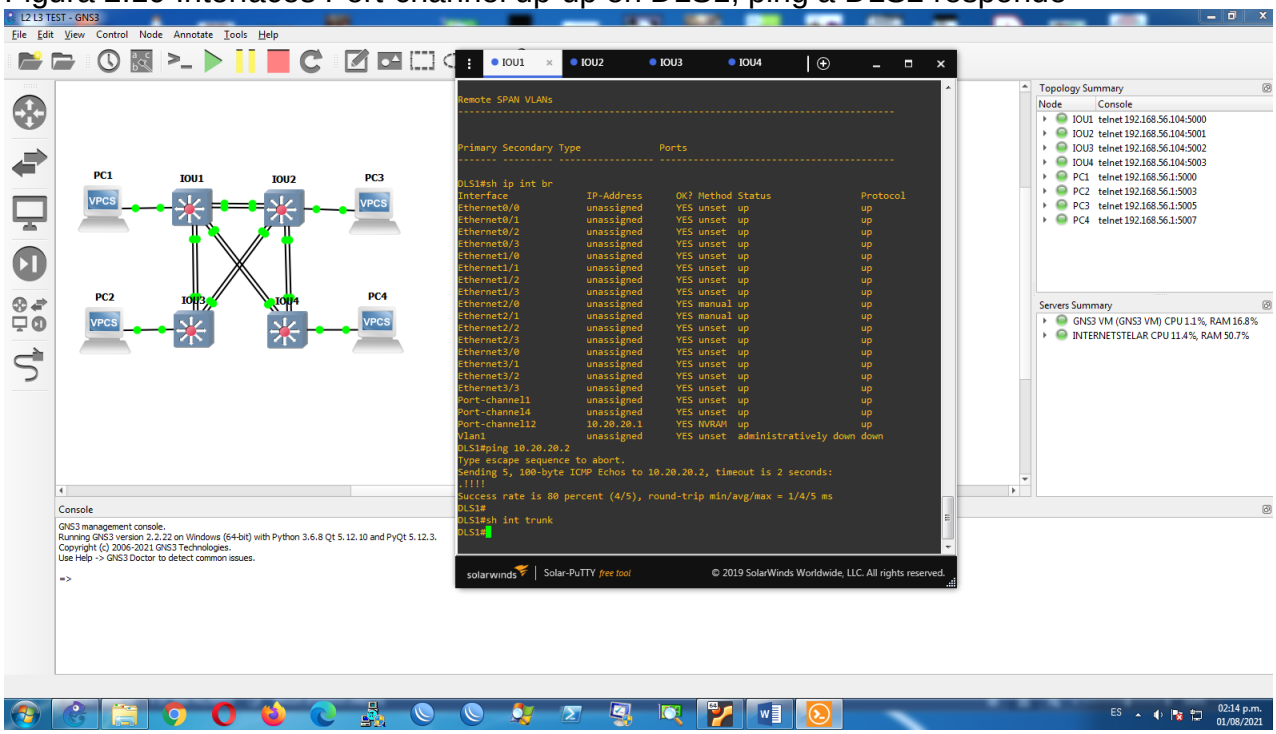
Después de habilitar administrativamente las interfaces verificamos lo siguiente:

En la Figura 2.19 vemos que las interfaces portchannel quedan habilitadas también operativamente en estado up-up de acuerdo a la verificación mediante comando show ip interfaces brief, de tal forma que responde ping entre las IP de los switch conectados en interfaz Portchannel12 L3

En la Figura 2.20 vemos ejecutando show vlan que la configuración manual de VLAN del switch servidor primario DLS1 se configura automáticamente en los clientes ALS, no se tiene en cuenta la configuración manual del switch transparente DLS2 porque por ejemplo no se crea la VLAN 567 creada en DLS2

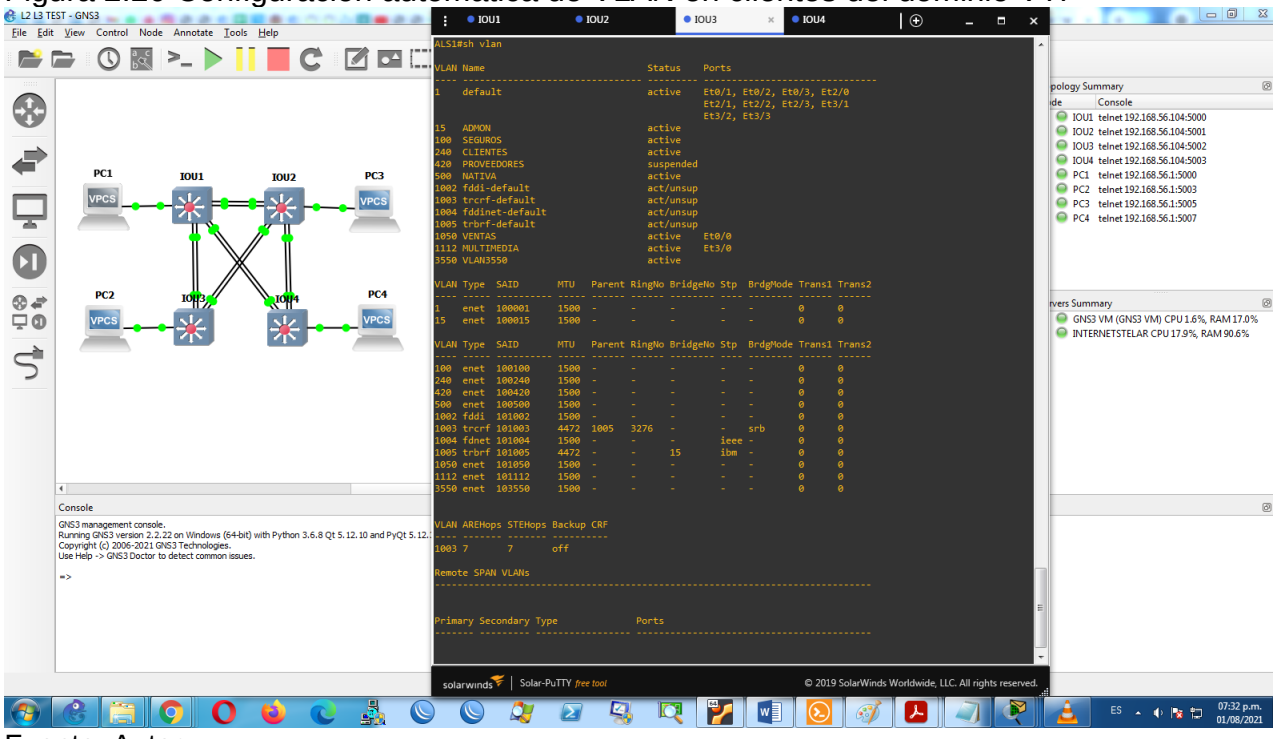
En la Figura 2.21 y Figura 2.22 vemos con show interfaces trunk que las interfaces troncales quedaron creadas y agrupadas satisfactoriamente en interfaces Port-channel en DLS1 y ALS1 de acuerdo a las VLAN asignadas

Figura 2.19 Interfaces Port-channel up-up en DLS1, ping a DLS2 responde



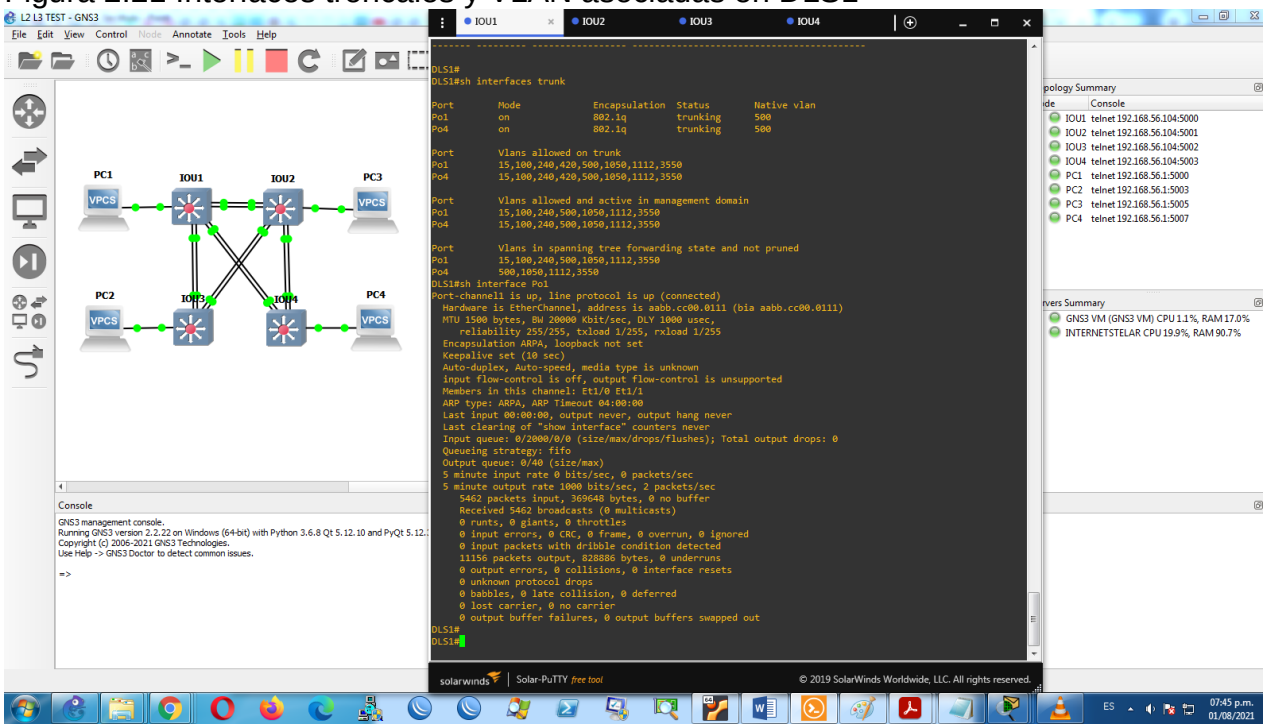
Fuente: Autor

Figura 2.20 Configuración automática de VLAN en clientes del dominio VTP



Fuente: Autor

Figura 2.21 Interfaces troncales y VLAN asociadas en DLS1

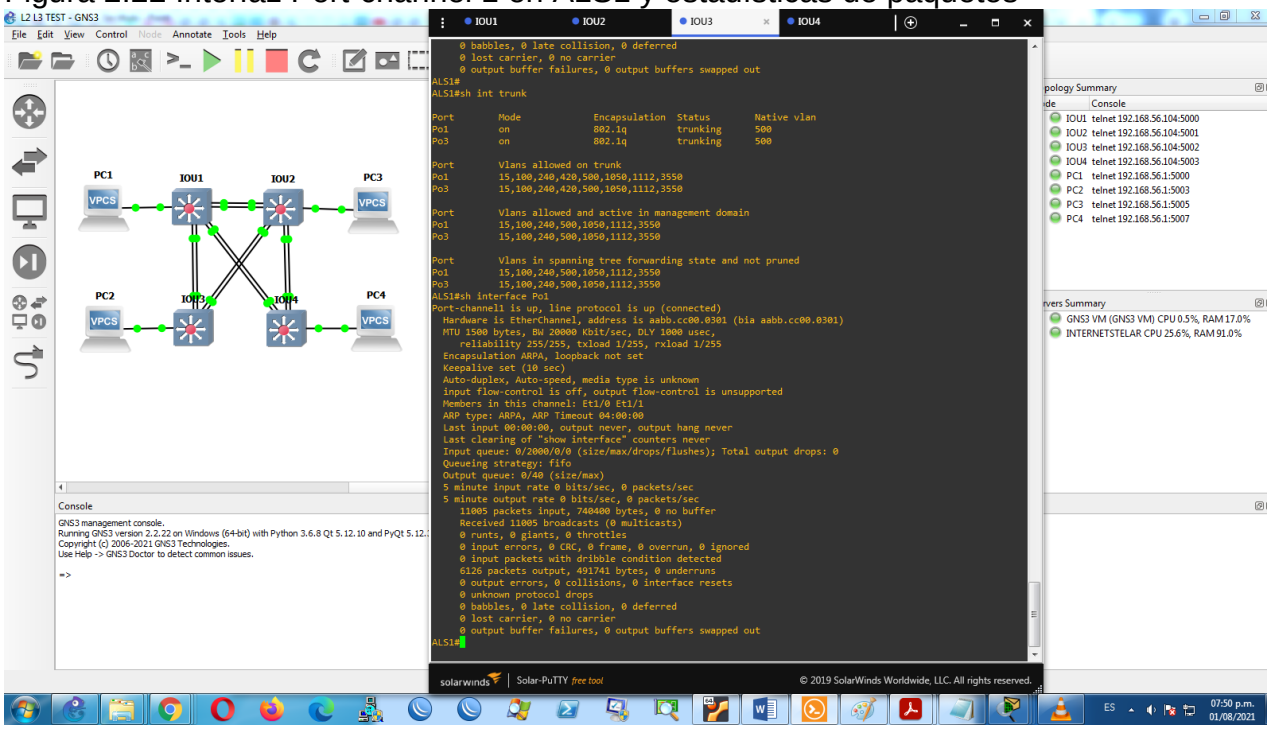


Fuente: Autor

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

El EtherChannel entre DLS1 y ALS1 se verifica en cada switch con show interface port-channel 1, vemos en la figura 2.20 que para DLS1 la interfaz port-channel 1 ya presenta el estado conectado y en sus estadísticas hay paquetes transmitidos y recibidos sin errores, de la misma forma esto se observa en el otro extremo del EtherChannel en ALS1 como se observa en la Figura 2.22

Figura 2.22 Interfaz Port-channel 1 en ALS1 y estadísticas de paquetes

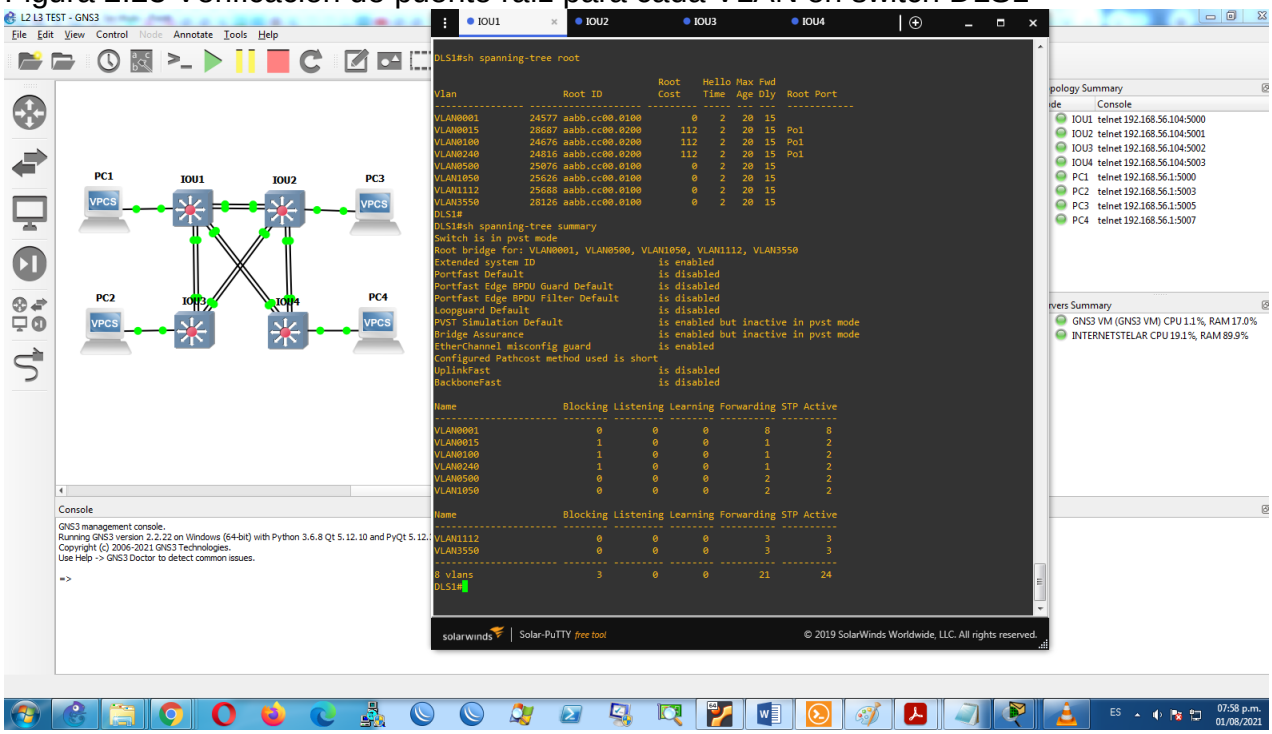


Fuente: Autor

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

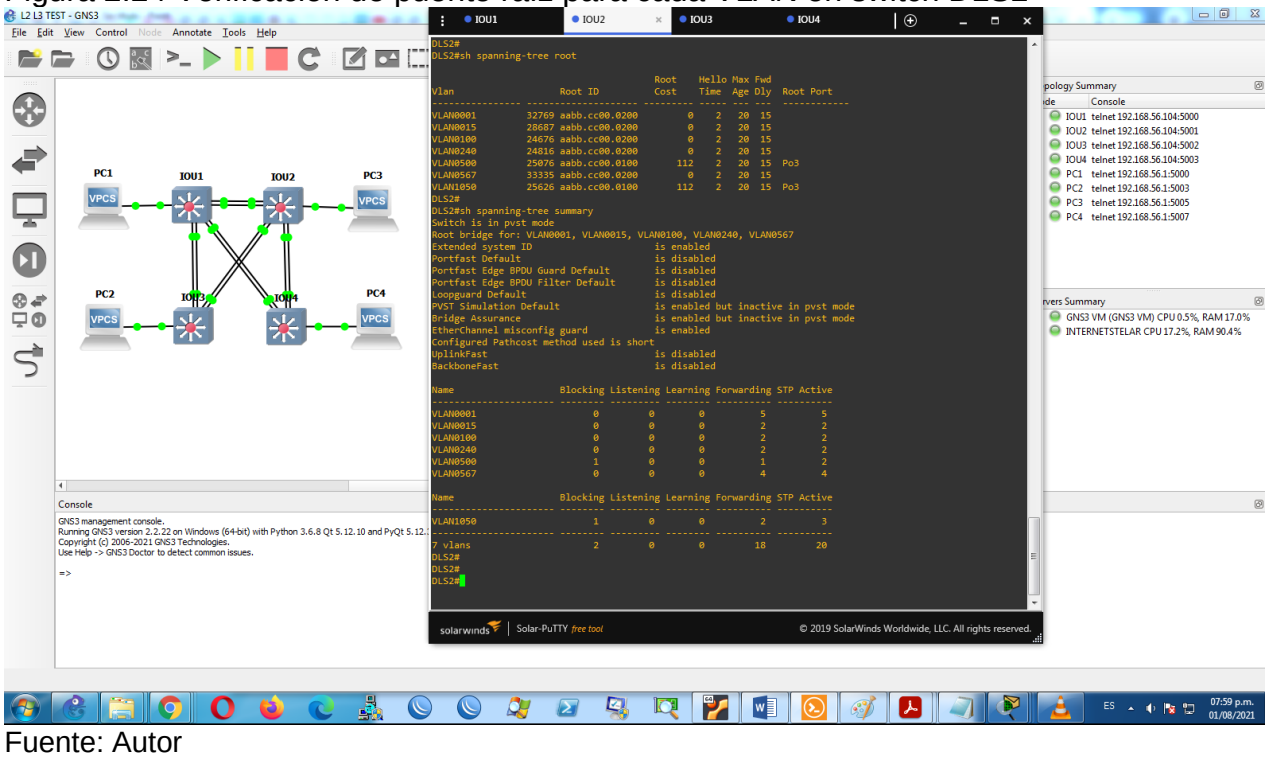
El puente raíz y la asignación de VLAN de Spanning tree entre DLS1 y DLS2 se verifica en cada switch con show spanning-tree root y show spanning-tree summary como vemos en la Figura 2.23 y Figura 2.24

Figura 2.23 Verificación de puente raíz para cada VLAN en switch DLS1



Fuente: Autor

Figura 2.24 Verificación de puente raíz para cada VLAN en switch DLS2



Fuente: Autor

CONCLUSIONES

Se corrobora la relevancia de los conocimientos adquiridos en el programa CCNP de CISCO, la amplia disponibilidad de comandos y funcionalidades aprendidas reúne un set de herramientas prácticas muy poderoso para llevar a la realidad complejas topologías y dar solución a diversidad de problemas en el área de Networking.

Los protocolos de enrutamiento dinamice OSPF y EIGRP funcionan con lógicas y métricas diferentes pero permiten integrarse fácilmente y funcionar de manera flexible y eficiente mediante la técnica de redistribución de rutas en escenarios que requieran la coexistencia entre estos y otros protocolos, se observa una mayor versatilidad de configuración en EIGRP.

Las técnicas de agregación de enlaces y control de redundancia de capa 2 son relativamente complejos de implementar dado que se deben controlar diversas variables entre los distintos puertos y equipos que participan en asociaciones de varios enlaces redundantes, se debe tener especial cuidado en asegurar la compatibilidad de parámetros entre switches capa 2 y switches multinivel, en general se requiere garantizar una completa coherencia de parámetros de switchport no solo para el establecimiento de agrupaciones en interfaces físicas en EtherChannel L2 y L3, sino para que además resulte optimo y lógico el control de loop mediante la configuración de puentes raíz de Spanning-tree, pero esto no es mayor problema si se cuenta con un adecuado entrenamiento en técnicas de troubleshooting que identifiquen un potencial problema y logren obtener como resultado redes con muy buenas prestaciones.

Mediante la simulación con GNS3 se logra cumplir efectivamente con los objetivos que quedan pendientes en la simulación de Packet Tracer, su mayor complejidad de implementación que requiere de máquina virtual y un IOS virtualizado sobre UNIX (IOU) se ve claramente compensada al soportar la implementación virtualizada de un switch multinivel con IOS v15, el cual soporta la última versión del protocolo VTPv3 de manejo centralizado de VLAN en enlaces troncales permitiendo así apreciar su mayor cantidad de opciones y escalabilidad que nos da este protocolo principalmente por la inclusión del rango extendido de VLAN y un control más seguro y sencillo con servidor primario.

BIBLIOGRAFIA

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-NT1IlnWR0hoMxgBNv1CJ

Romero, C., (2019) Establecer IOU L2 e IOU L3 en GNS3. Recuperado de https://www.youtube.com/watch?v=ZXfseiLKIgI

Sagar, Azeem, A. (2020) CCNP ENTERPRISE 2020. ENCOR 350-401 ENARSI 300-410 For enrolling in Online “CCNP Enterprise” batch. Recuperado de http://www.networkjourney.com/wp-content/uploads/2020/04/ccnpenterpriseworkbookv1-200418043231.pdf

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

ANEXO

Se anexa link en Drive de carpeta compartida con los siguientes elementos:

Una copia del presente trabajo en formato .pdf

Dos archivos ejecutables .pkt a de las dos simulaciones en Packet Tracer para el primer y segundo escenarios

Un archivo ejecutable .gns3 de la simulación en GNS3 para el segundo escenario

Una carpeta comprimida .zip con los archivos necesarios para implementar la imagen Cisco IOU L2, la cual se montó en máquina virtual oficial GNS3 sobre VirtualBox, necesaria en la simulación de GNS3 de acuerdo a procedimiento indicado en video-tutorial de referencia

Un block de notas con el link del video de sustentación en youtube

https://drive.google.com/drive/folders/1C0oH0wrjBzt-5WkQvWYpZL3LCUNDTVT-?usp=sharing