DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

WILMER ESTEBAN CALDERÓN MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA TELECOMUNICACIONES
BOGOTÁ D.C.
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

WILMER ESTEBAN CALDERÓN MUÑOZ

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

DIRECTOR
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA TELECOMUNICACIONES
BOGOTÁ D.C.
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTÁ D.C., 28 de noviembre de 2021

AGRADECIMIENTOS

Quiero agradecer a Dios por brindarme la oportunidad de crecer profesionalmente, a mi familia por ser el motor que me impulsa para cumplir mis metas, a mis padres porque son las personas que me inculcaron desde pequeño valores y principios, especialmente el apoyarme para tener una mejor educación y así mismo forjarme para tener un mejor bienestar personal y laboral.

Especialmente quiero agradecerle a mi esposa Edna Jimena Garcia Perez, por ser mi compañera de vida y brindarme su apoyo incondicional en este crecimiento profesional, a mi hijo Emmanuel Calderón Garcia quien es mi mayor motivación para continuar formándome profesional y laboralmente, porque quiero ser su ejemplo a seguir para que en un futuro sea un gran profesional con valores y principios.

Y finalizo mis agradecimientos al tutor Gerardo Granados Acuña, por su guía y acompañamiento durante el desarrollo de este diplomado y por facilitar la metodología desarrollada en esta monografía.

CONTENIDO

AGRADECIMIENTOS 4
CONTENIDO 5
LISTA DE TABLAS 6
LISTA DE ILUSTRACIONES 7
GLOSARIO 8
RESUMEN 9
ABSTRACT 9
INTRODUCCIÓN 10
DESARROLLO 11
CONCLUSIONES 49
BIBLIOGRÁFIA 50

LISTA DE TABLAS

Tabla 1 Configuración inicial R1 13
Tabla 2 Configuración inicial R2 13
Tabla 3 Configuración inicial R3 14
Tabla 4 Configuración inicial D1 15
Tabla 5 Configuración inicial D2 16
Tabla 6 Configuración inicial A1 16
Tabla 7 Tareas parte 2 19
Tabla 8 Configuración Capa 2 en D1 20
Tabla 9 Configuración Capa 2 en D2 21
Tabla 10 Configuración Capa 2 en A1 23
Tabla 11 Tareas parte 3 26
Tabla 12 Configuración enrutamiento R1 27
Tabla 13 Configuración enrutamiento R2 29
Tabla 14 Configuración enrutamiento R3 30
Tabla 15 Configuración enrutamiento D1 32
Tabla 16 Configuración enrutamiento D2 33
Tabla 17 Tareas parte 4 35
Tabla 18 Tareas parte 4-1 38
Tabla 19 Configuración redundancia en D1 39
Tabla 20 Configuración redundancia en D2 41
Tabla 21 Tareas parte 5 43
Tabla 22 Configuración de seguridad ALL Devices 43
Tabla 23 Tareas parte 6 45
Tabla 24 Administración de red R1 46
Tabla 25 Administración de red R3 46
Tabla 26 Administración de red D1 - A1 46
Tabla 27 Administración de red D2 47
Tabla 28 Network Time Protoco R2 48

LISTA DE ILUSTRACIONES

Ilustración 1. Topología Escenario propuesto 11
Ilustración 2. Simulación GNS3 12
Ilustración 3. Direccionamiento en PC1 17
Ilustración 4. Direccionamiento en PC4 18
Ilustración 5. Consulta protocolo RSTP en D1 24
Ilustración 6. Consulta protocolo RSTP en D2 24
Ilustración 7. Validación Show Run A1 24
Ilustración 8. Configuración enrutamiento R1 29
Ilustración 9. Configuración enrutamiento R2 30
Ilustración 10. Configuración enrutamiento R3 31
Ilustración 11. Configuración enrutamiento D1 33
Ilustración 12. Configuración enrutamiento D2 34
Ilustración 13 IP SLA en D1 40
Ilustración 14 IP SLA en D2 42
Ilustración 15 Show run contraseña 43
Ilustración 16 Server RADIUS 44
Ilustración 17 Show run AAA 44
Ilustración 18 Consulta clock 47
Ilustración 19 Configuración UTC R2 48

GLOSARIO

CCNP: Son las siglas de Cisco Certified Networking Professional. Es decir, un certificado de networking y telecomunicaciones, como veíamos antes con la CCNA, solo que esta vez hay un elemento decisivo que lo diferencia y separa ambas categorías. Este elemento es la P de las siglas, la palabra proffesional o, dicho en castellano, profesional.

HOST: También conocido como hosting, hospedaje o anfitrión, es cualquier computadora o máquina conectada a una red mediante un número de IP definido y un dominio, que ofrece recursos, información y servicios a sus usuarios.

LAN: Local Area Network. Denomina redes con extensión física limitada. La mayoría de las redes LAN se usan en hogares privados o en empresas, para instalar redes de hogar o de empresa. De este modo, distintos dispositivos pueden comunicarse entre ellos.

LOOPBACK: es una dirección ip (también conocida como localhost) reservada específicamente para probar el funcionamiento de TCP/IP en un dispositivo. La dirección reservada del espacio de direccionamiento IPv4 es el que corresponde al segmento 127.0.0.0/8. La dirección reservada del espacio de direccionamiento IPv6 es solamente una IP::1

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

ROUTER: Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.

VLAN: (Virtual LAN), o también conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física.

RESUMEN

El presente trabajo evidencia el desarrollo practico de las temáticas trabajadas en las unidades del Diplomado de profundización CISCO CCNP, donde se manejan protocolos de enrutamiento como lo son la versión 4 (IPv4) e IP versión 6 (IPv6) y el Protocolo de enrutamiento de Gateway interior mejorado (EIGRP) – CCNP ROUTE y donde el CCNP SWITCH se establecen los fundamentos de conmutación y se comprenden las arquitecturas de red, además de enrutamientos de VLANs y tecnologías de conmutación y aseguramiento.

Los módulos mencionados con anterioridad que se desarrollan por medio del presente trabajo resultado final bajo dos escenarios prácticos, con instrucciones para el desarrollo de los mismos e implementándolos con el software de desarrollo practico Packet Tracer o GNS3 como modelo de aprendizaje eficaz en la carrera de ingeniería electrónica y en fortalecimiento de habilidades necesarias para la implementación de redes con diferentes protocolos.

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

ABSTRACT

This work shows the practical development of the topics worked in the units of the CISCO CCNP in-depth Diploma, where routing protocols such as version 4 (IPv4) and IP version 6 (IPv6) and the Gateway Routing Protocol are handled. Enhanced Interior (EIGRP) - CCNP ROUTE and where the CCNP SWITCH lays the basics of switching and understands network architectures, as well as VLAN routing and switching and assurance technologies.

The aforementioned modules that are developed through this work, final result under two practical scenarios, with instructions for their development and implementing them with the practical development software Packet Tracer or GNS3 as an effective learning model in the engineering career electronics and in strengthening the skills necessary for the implementation of networks with different protocols.

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

INTRODUCCIÓN

Para un ingeniero de telecomunicaciones es vital obtener conocimientos, habilidades y acertado desempeño en el campo de las redes de comunicación como sistema eficaz para diferentes aplicaciones actuales en las industrias.

A través del desarrollo del diplomado de CCNP de CICSO se obtendrán conocimientos en el área de enrutamiento de protocolos tales como el OSPF, BGP, IPV4, IPV6, AAA, NTP, entre otros. Además del enrutamiento de VLANs y el aseguramiento de la plataforma de comunicación. La estrategia del diplomado está compuesta de dos escenarios y radica en la solución de ejercicios donde se aplicará los conocimientos de enrutamiento por medio de herramientas de simulación como Packet Tracer, GNS3 o smartlab. Su objetivo es comprender la arquitectura y el control de la red de rango medio y enfatizar en el Protocolo de enrutamiento y su optimización mediante configuración. Esto lo permitirá el desarrollo y conocimientos adquiridos en el curso de profundización en dos etapas CCNP route y CCNP Switch, así como las destrezas obtenidas durante el desarrollo del programa de pregrado.

DESARROLLO

Parte 1 cableado de red según topología

1. Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

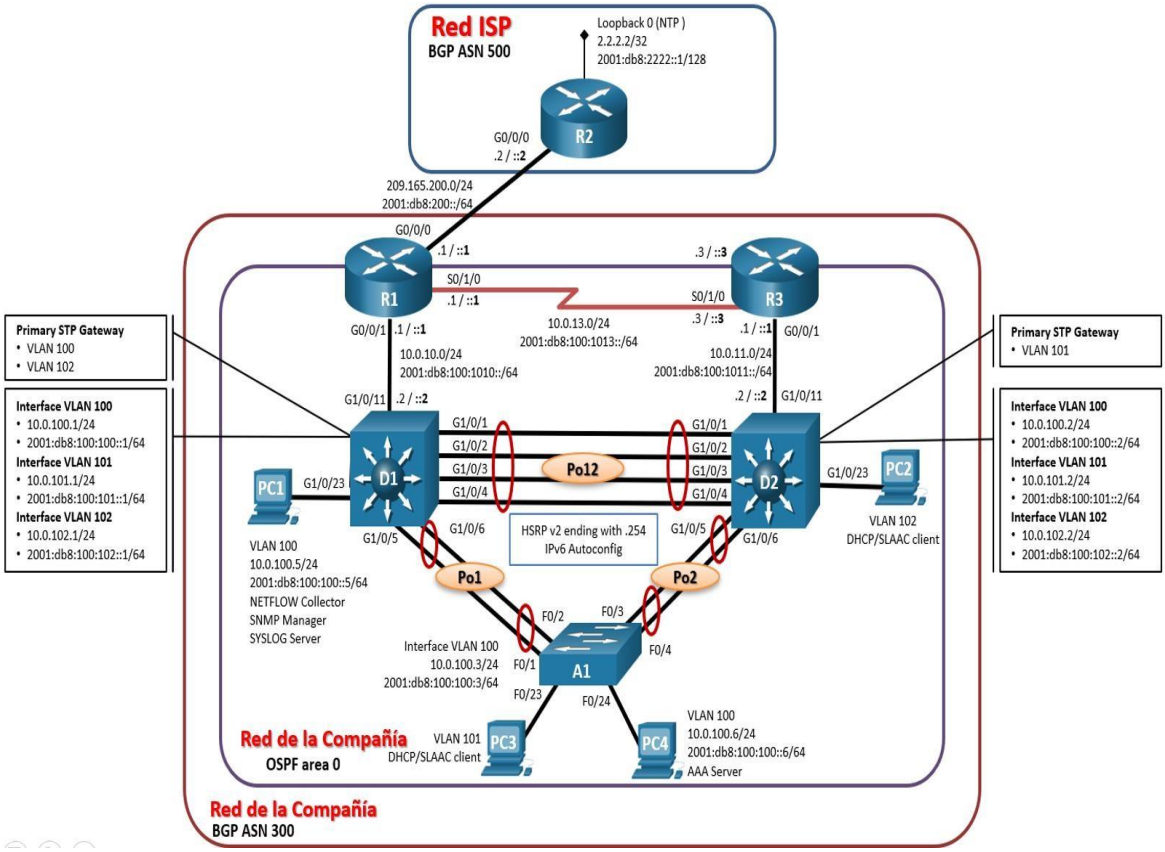

Ilustración 1. Topología Escenario propuesto

Se realiza construcción en GNS3 de escenario propuesto con dispositivos de similares características, para llevar a cabo la topología conformada por 3 routers, 3 Switches y 4 dispositivos PC, como se muestra a continuación.

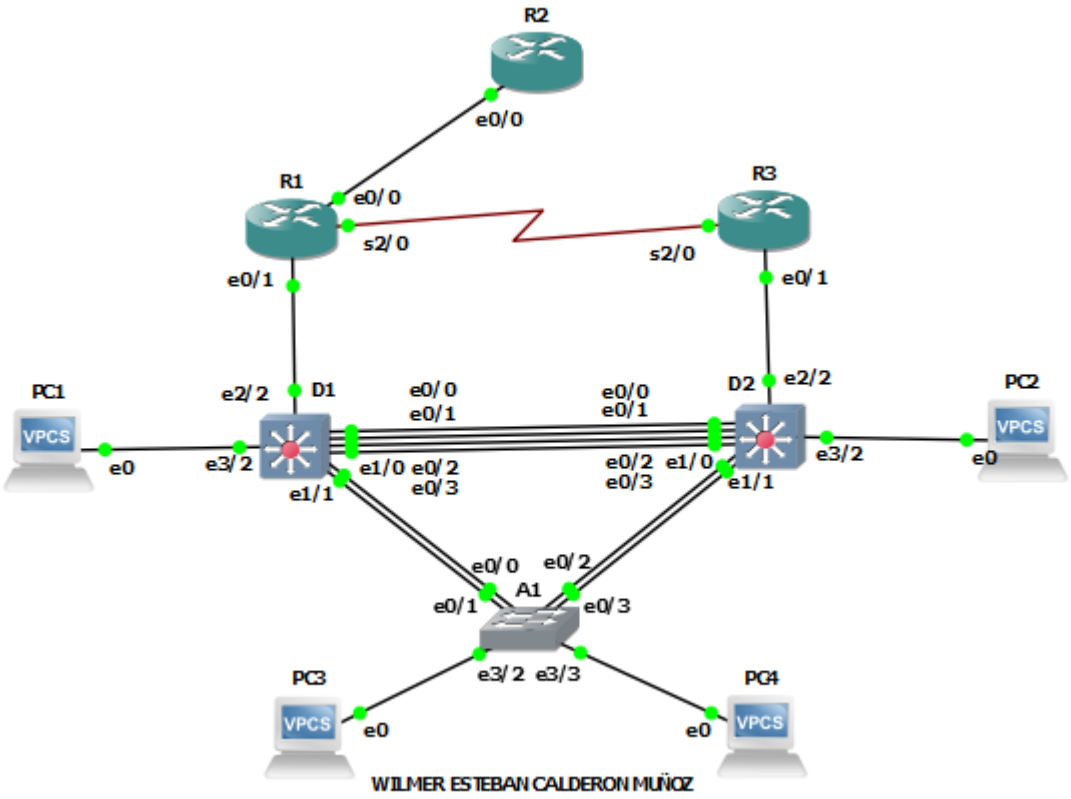

Ilustración 2. Simulación GNS3

2. Configuración los parámetros básicos para cada dispositivo.

a. Procedemos a realizar las configuraciones iniciales cada uno de los dispositivos requeridos para llevar a cabo la construcción de la topología planteada, donde por modo configuración de terminal, asignamos nombre, habilitamos traducción de nombre a dirección, Routing para IPV6, configuramos mensajes personalizados mediante comando “baner motd”, predeterminamos el ingreso a modo consola y configuramos en cero el tiempo de espera para la sesión remota por consola, entre otras configuraciones se establece el direccionamiento en base a la tabla planteada inicialmente, en los dispositivos tipo Switch determinamos las VLAN redes lógicas independientes

Router R1	
Enable	no shutdown
Conf t	exit

Hostname R1	interface e0/1
ipv6 unicast-routing	ip address 10.0.10.1 255.255.255.0
no ip domain lookup	ipv6 address fe80::1:2 link-local
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	ipv6 address 2001:db8:100:1010::1/64
line con 0	no shutdown
exec-timeout 0 0	exit
logging synchronous	interface s2/0
exit	ip address 10.0.13.1 255.255.255.0
interface e0/0	ipv6 address fe80::1:3 link-local
ip address 209.165.200.225 255.255.255.224	ipv6 address 2001:db8:100:1013::1/64
ipv6 address fe80::1:1 link-local	no shutdown
ipv6 address 2001:db8:200::1/64	exit

Tabla 1 Configuración inicial R1

Router R2	
Enable	ip address 209.165.200.226 255.255.255.224
Conf t	ipv6 address fe80::2:1 link-local
hostname R2	ipv6 address 2001:db8:200::2/64
ipv6 unicast-routing	no shutdown
no ip domain lookup	exit
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	interface Loopback 0
line con 0	ip address 2.2.2.2 255.255.255.255
exec-timeout 0 0	ipv6 address fe80::2:3 link-local
logging synchronous	ipv6 address 2001:db8:2222::1/128
exit	no shutdown
interface e0/0	exit

Tabla 2 Configuración inicial R2

Router R3	
Enable	ip address 10.0.11.1 255.255.255.0
Conf t	ipv6 address fe80::3:2 link-local

hostname R3	ipv6 address 2001:db8:100:1011::1/64
ipv6 unicast-routing	no shutdown
no ip domain lookup	exit
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	interface s2/0
line con 0	ip address 10.0.13.3 255.255.255.0
exec-timeout 0 0	ipv6 address fe80::3:3 link-local
logging synchronous	ipv6 address 2001:db8:100:1010::2/64
exit	no shutdown
interface e0/1	exit

Tabla 3 Configuración inicial R3

Switch D1	
Enable	ipv6 address fe80::d1:2 link-local
Conf t	ipv6 address 2001:db8:100:100::1/64
hostname D1	no shutdown
ip routing	exit
ipv6 unicast-routing	interface vlan 101
no ip domain lookup	ip address 10.0.101.1 255.255.255.0
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	ipv6 address fe80::d1:3 link-local
line con 0	ipv6 address 2001:db8:100:101::1/64
exec-timeout 0 0	no shutdown
logging synchronous	exit
exit	interface vlan 102
vlan 100	ip address 10.0.102.1 255.255.255.0
name Management	ipv6 address fe80::d1:4 link-local
exit	ipv6 address 2001:db8:100:102::1/64
vlan 101	no shutdown
name UserGroupA	exit
exit	ip dhcp excluded-address 10.0.101.1 10.0.101.109
vlan 102	ip dhcp excluded-address 10.0.101.141 10.0.101.254
name UserGroupB	ip dhcp excluded-address 10.0.102.1 10.0.102.109
exit	ip dhcp excluded-address 10.0.102.141 10.0.102.254

vlan 999	ip dhcp pool VLAN-101
name NATIVE	network 10.0.101.0 255.255.255.0
exit	default-router 10.0.101.254
interface e2/2	exit
no switchport	ip dhcp pool VLAN-102
ip address 10.0.10.2 255.255.255.0	network 10.0.102.0 255.255.255.0
ipv6 address fe80::d1:1 link-local	default-router 10.0.102.254
ipv6 address 2001:db8:100:1010::2/64	exit
no shutdown	interface range e0/0-3, e1/0-3, e2/0-1, e2/3, e3/0-3
exit	shutdown
interface vlan 100	exit
ip address 10.0.100.1 255.255.255.0	

Tabla 4 Configuración inicial D1

Switch D2	
Enable	ipv6 address fe80::d2:2 link-local
Conf t	ipv6 address 2001:db8:100:100::2/64
hostname D2	no shutdown
ip routing	exit
ipv6 unicast-routing	interface vlan 101
no ip domain lookup	ip address 10.0.101.2 255.255.255.0
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	ipv6 address fe80::d2:3 link-local
line con 0	ipv6 address 2001:db8:100:101::2/64
exec-timeout 0 0	no shutdown
logging synchronous	exit
exit	interface vlan 102
vlan 100	ip address 10.0.102.2 255.255.255.0
name Management	ipv6 address fe80::d2:4 link-local
exit	ipv6 address 2001:db8:100:102::2/64
vlan 101	no shutdown
name UserGroupA	exit
exit	ip dhcp excluded-address 10.0.101.1 10.0.101.209
vlan 102	ip dhcp excluded-address 10.0.101.241 10.0.101.254
name UserGroupB	ip dhcp excluded-address 10.0.102.1 10.0.102.209
exit	ip dhcp excluded-address 10.0.102.241 10.0.102.254

vlan 999	ip dhcp pool VLAN-101
name NATIVE	network 10.0.101.0 255.255.255.0
exit	default-router 10.0.101.254
interface e2/2	exit
no switchport	ip dhcp pool VLAN-102
ip address 10.0.11.2 255.255.255.0	network 10.0.102.0 255.255.255.0
ipv6 address fe80::d1:1 link-local	default-router 10.0.102.254
ipv6 address 2001:db8:100:1011::2/64	exit
no shutdown	interface range e0/0-3, e1/0-3, e2/0-1, e2/3, e3/0-3
exit	shutdown
interface vlan 100	exit
ip address 10.0.100.2 255.255.255.0	

Tabla 5 Configuración inicial D2

Switch A1	
Enable	vlan 102
Conf t	name UserGroupB
hostname A1	exit
no ip domain lookup	vlan 999
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	name NATIVE
line con 0	exit
exec-timeout 0 0	interface vlan 100
logging synchronous	ip address 10.0.100.3 255.255.255.0
exit	ipv6 address fe80::a1:1 link-local
vlan 100	ipv6 address 2001:db8:100:100::3/64
name Management	no shutdown
exit	exit
vlan 101	interface range e1/0-3,e2/0-3,e3/0-1
name UserGroupA	shutdown
exit	exit

Tabla 6 Configuración inicial A1

b. Realizamos copia de seguridad de ingresando en modo configuración seguido del comando copy running-config startup-config para almacenar la configuración de todos los dispositivos recién creada lo cual permitirá copiar la configuración activa de la RAM a la NVRAM.

show running-config
copy running-config startup-config

c. En los equipos tipo PC 1 y 4 realizamos configuración de su direccionamiento de acuerdo con lo estipulado en la tabla

Host PC1

ip 10.0.100.5/24 10.0.100.254
ip 2001:db8:100:100::5/64 auto
show ip /all
show ipv6 /all

```
PC1> show ip /all

NAME   IP/MASK              GATEWAY           MAC                DNS
PC1    10.0.100.5/24        10.0.100.254      00:50:79:66:68:00

PC1> show ipv6 /all

NAME   IP/MASK                 ROUTER LINK-LAYER  MTU
PC1    fe80::250:79ff:fe66:6800/64
       2001:db8:100:100::5/64                     1500

PC1>
```

Ilustración 3. Direccionamiento en PC1

Host PC4

ip 10.0.100.6/24 100.0.10.254
ip 2001:db8:100:100::6/64 auto
show ip /all
show ipv6 /all

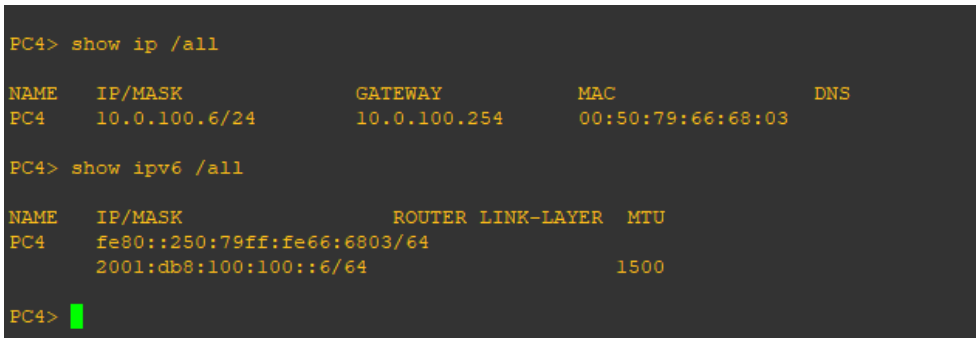

Ilustración 4. Direccionamiento en PC4

Parte 2 Configuración la capa 2 de la red y el soporte de Host

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
Tarea#	**Tarea**	**Especificación**
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2

2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Tabla 7 Tareas parte 2

En esta parte realizamos procedimientos de configuración de los equipos correspondientes a la capa 2 de nuestra topología, donde configuramos los puertos para permitir el paso de trafico de las diferentes VLAN utilizando el comando (switchport trunk encapsulation dot1q y switchport mode trunk), mediante (channel-group mode active) activamos canales y grupos para balancear el tráfico entre los diferentes puertos permitiendo aumentar el ancho de banda y la redundancia, definimos la VLAN activas en cada Switch con Spanning-tree. Y validamos conectividad entre dispositivos.

Comandos de configuración ingresados en cada dispositivo.

Switch D1	
Enable	channel-group 1 mode active

Conf t	no shutdown
interface range e0/0-3	exit
switchport trunk encapsulation dot1q	spanning-tree mode rapid-pvst
switchport mode trunk	spanning-tree vlan 100,102 root primary
switchport trunk native vlan 999	spanning-tree vlan 101 root secondary
channel-group 12 mode active	interface e3/2
no shutdown	switchport mode access
exit	switchport access vlan 100
interface range e1/0-1	spanning-tree portfast
switchport trunk encapsulation dot1q	no shutdown
switchport mode trunk	exit
switchport trunk native vlan 999	end

Tabla 8 Configuración Capa 2 en D1

Pasos para la configuración en D1

- Ingresamos en modo configuración (configuración terminal).
- Elegimos el rango de interfaces de 0/0 a la 0/3 para aplicar en estas las siguientes configuraciones.
- Con el comando (switchport trunk encapsulation dot1q) damos vida al enlace troncal basado en el estándar IEEE 802.1Q para permitir el paso del tráfico de las distintas VLANs que hemos configurado en el paso 1.
- Con (switchport mode trunk) hacemos que la interfaz quede en trunking permanentemente, y negocia convertir el enlace en enlace troncal para la interfaz previamente seleccionada.
- Especificamos la VLAN 999 mediante (switchport trunk native) para los enlaces troncales sin etiquetar.
- Activamos con (channel-group 12 mode active) un grupo de interfaz asociadas a un numero de grupo en este caso el 1 y el 12 para asociarlas al canal de los dispositivos a comunicar según interface de entrada.
- Con (no shutdown) aplicamos los cambios realizados sobre las interfaces seleccionadas, y podemos salir nuevamente a modo configuración para trabajar sobre otra interfaz.
- Tomamos otro rango de interfaces 1/0 a la 1/1.
- Igualmente, con el comando (switchport trunk encapsulation dot1q) damos vida al enlace troncal basado en el estándar IEEE 802.1Q para permitir el paso del tráfico de las distintas VLANs que hemos configurado en pasos anteriores.

- Y seguido de esto usamos comandos (switchport mode trunk, switchport trunk native vlan 999) para habilitar y permitir el trafico de enlaces sin etiquetar en esta interfaz.
- Aplicamos cambios nuevamente con (no shutdown) y salimos (exit) para retornar al modo de configuración.
- Con el nombramiento del protocolo (Rapid Spanning-Tree) buscamos permitir a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión.
- Nombrando las VLAN 100 y 102 como primarias y la 101 como secundaria.
- En la interfaz 3/2 habilitamos (switchport mode Access) para dejarla en modo permanente nontrunking y permitirle que negocie convertir el enlace en no troncal para la VLAN 100.
- Habilitamos a los usuarios con el (spanning-tree portfast) para que las estaciones finales puedan obtener acceso inmediato a la red.
- Aplicamos cambios en esta interfaz con (no shutdown) y salimos del modo configuración.

Switch D2	
Enable	channel-group 2 mode active
Conf t	no shutdown
interface range e0/0-3	exit
switchport trunk encapsulation dot1q	spanning-tree mode rapid-pvst
switchport mode trunk	spanning-tree vlan 101 root primary
switchport trunk native vlan 999	spanning-tree vlan 100,102 root secondary
channel-group 12 mode active	interface e3/2
no shutdown	switchport mode access
exit	switchport access vlan 102
interface range e1/0-1	spanning-tree portfast
switchport trunk encapsulation dot1q	no shutdown
switchport mode trunk	exit
switchport trunk native vlan 999	end

Tabla 9 Configuración Capa 2 en D2

Pasos para la configuración en D2

Repetimos los pasos ejecutados en D1 teniendo presente la nomenclatura que se tenga para cada una de las interfaces con su respectivo rango, donde debemos aplicar las respectivas configuraciones.

- Con el comando (switchport trunk encapsulation dot1q) damos vida al enlace troncal basado en el estándar IEEE 802.1Q para permitir el paso del tráfico de las distintas VLANs que hemos configurado en el paso 1.
- Con (switchport mode trunk) hacemos que la interfaz quede en trunking permanentemente, y negocia convertir el enlace en enlace troncal para la interfaz previamente seleccionada.
- Especificamos la VLAN 999 mediante (switchport trunk native) para los enlaces troncales sin etiquetar.
- Activamos con (channel-group 12 mode active) un grupo de interfaz asociadas a un numero de grupo en este caso el 2 y el para asociarlas al canal de los dispositivos a comunicar según interfaz de entrada.
- Con (no shutdown) aplicamos los cambios realizados sobre las interfaces seleccionadas, y podemos salir nuevamente a modo configuración para trabajar sobre otra interfaz.
- Tomamos otro rango de interfaces 1/0 a la 1/1.
- Igualmente, con el comando (switchport trunk encapsulation dot1q) damos vida al enlace troncal basado en el estándar IEEE 802.1Q para permitir el paso del tráfico de las distintas VLANs que hemos configurado en pasos anteriores.
- Y seguido de esto usamos comandos (switchport mode trunk, switchport trunk native vlan 999) para habilitar y permitir el tráfico de enlaces sin etiquetar en esta interfaz.
- Aplicamos cambios nuevamente con (no shutdown) y salimos (exit) para retornar al modo de configuración.
- Con el nombramiento del protocolo (Rapid Spanning-Tree) buscamos permitir a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión.
- Nombrando en este caso las VLAN 100 y 102 como secundarias y la 101 como primaria.
- En la interfaz 3/2 habilitamos (switchport mode Access) para dejarla en modo permanente nontrunking y permitirle que negocie convertir el enlace en no troncal para la VLAN 100.
- Habilitamos a los usuarios con el (spanning-tree portfast) para que las estaciones finales puedan obtener acceso inmediato a la red.
- Aplicamos cambios en esta interfaz con (no shutdown) y salimos del modo configuración.

Switch A1	
Enable	no shutdown
Conf t	exit
spanning-tree mode rapid-pvst	interface e3/2
interface range e1/0-1	switchport mode access
switchport trunk encapsulation dot1q	switchport access vlan 101
switchport mode trunk	spanning-tree portfast
switchport trunk native vlan 999	no shutdown
channel-group 1 mode active	exit
no shutdown	interface e3/3
exit	switchport mode access
interface range e1/2-3	switchport access vlan 100
switchport trunk encapsulation dot1q	spanning-tree portfast
switchport mode trunk	no shutdown
switchport trunk native vlan 999	exit
channel-group 2 mode active	end

Tabla 10 Configuración Capa 2 en A1

Pasos para la configuración en A1

- Ingresamos en modo configuración (configuración terminal).
- Enunciando (spanning-tree mode rapid-pvst) Configuramos el modo de árbol de expansión PVST rápido.
- Elegimos el rango de interfaces de 1/0 a la 1/1 para aplicar en estas las próximas configuraciones.
- Usando (switchport trunk encapsulation dot1q) damos vida en este rango de INT al enlace troncal basado en el estándar IEEE 802.1Q para permitir el paso del tráfico de las distintas VLANs que hemos configurado en el paso 1.
- Con (switchport mode trunk) hacemos que la interfaz quede en trunking permanentemente, y negocia convertir el enlace en enlace troncal para la interfaz previamente seleccionada.
- Especificamos la VLAN 999 mediante (switchport trunk native) para los enlaces troncales sin etiquetar.
- Activamos con (channel-group 1 mode active) un grupo de interfaz asociadas a un numero de grupo en este caso el 1 y 2 para asociarlas al canal de los dispositivos a comunicar según interfaz de entrada.
- Con (no shutdown) aplicamos los cambios realizados sobre las interfaces seleccionadas, y podemos salir nuevamente a modo configuración para trabajar sobre otra interfaz.

- En la interfaz 3/2 habilitamos (switchport mode Access) para dejarla en modo permanente nontrunking y permitirle que negocie convertir el enlace en no troncal para la VLAN 101.
- Con (no shutdown) aplicamos los cambios realizados sobre las interfaces seleccionadas, y podemos salir nuevamente a modo configuración para trabajar sobre otra interfaz.
- En la interfaz 3/3 habilitamos (switchport mode Access) para dejarla en modo permanente nontrunking y permitirle que negocie convertir el enlace en no troncal para la VLAN 100.
- Habilitamos a los usuarios con el (spanning-tree portfast) para que las estaciones finales puedan obtener acceso inmediato a la red.
- Aplicamos cambios en esta interfaz con (no shutdown) y salimos del modo configuración finalizando el proceso con comando END.

Validaciones realizadas en los dispositivos

```
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
 spanning-tree portfast
```

Ilustración 5. Consulta protocolo RSTP en D1

```
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
```

Ilustración 6. Consulta protocolo RSTP en D2

```
A1#show run interface e3/2
Building configuration...

Current configuration : 118 bytes
!
interface Ethernet3/2
 switchport access vlan 101
 switchport mode access
 duplex auto
 spanning-tree portfast
end

A1#show run interface e3/3
Building configuration...

Current configuration : 118 bytes
!
interface Ethernet3/3
 switchport access vlan 100
 switchport mode access
 duplex auto
 spanning-tree portfast
end
```

Ilustración 7. Validación Show Run A1

Parte 3 Configuración protocolos de enrutamiento.

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en area 0.	Use OSPF Process ID **4** y asigne los siguientes routerIDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID **6** y asigne los siguientes routerIDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
Tarea#	**Tarea**	**Especificación**

3.3	En R2 en la “Red ISP”, configure MPBGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MPBGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

Tabla 11 Tareas parte 3

Se realiza configuración de protocolos multi área con OSPF V2 y 3 respectivamente para direccionamiento IPV4 e IPV6 con lo cual podemos determinar el mejor camino a utilizar al realizar un envió de un paquete atreves de la red. Anunciando las rutas de red directamente conectadas a los dispositivos que tendrán función de

enrutadores. Igualmente, en estos dispositivos por medio de protocolo BGP (Border Gateway Protocol) definimos las políticas de enrutamiento que nos periten crear entornos de enrutamiento más estables configurando también direccionamiento por familias identificadas bajo los diferentes segmentos de red.

Comandos de configuración aplicados en cada dispositivo

Router R1	
Enable	exit
Conf t	ip route 10.0.0.0 255.0.0.0 null0
router ospf 4	ipv6 route 2001:db8:100::/48 null0
router-id 0.0.4.1	router bgp 300
network 10.0.10.0 0.0.0.255 area 0	bgp router-id 1.1.1.1
network 10.0.13.0 0.0.0.255 area 0	neighbor 209.165.200.226 remote-as 500
default-information originate	neighbor 2001:db8:200::2 remote-as 500
exit	address-family ipv4 unicast
ipv6 unicast-routing	neighbor 209.165.200.226 activate
ipv6 router ospf 6	no neighbor 2001:db8:200::2 activate
router-id 0.0.6.1	network 10.0.0.0 mask 255.0.0.0
default-information originate	exit-address-family
exit	address-family ipv6 unicast
interface e0/1	no neighbor 209.165.200.226 activate
ipv6 ospf 6 area 0	neighbor 2001:db8:200::2 activate
exit	network 2001:db8:100::/48
interface s2/0	exit-address-family
ipv6 ospf 6 area 0	

Tabla 12 Configuración enrutamiento R1

Pasos para la configuración en R1

- Ingresamos en modo configuración (configuración terminal).
- Con el comando (router ospf 4) Open Shortest Pacth First para IP V4 donde el ID asignado al proceso correspondiente al número 4 con el cual buscamos segmentar y determinar los mejores caminos de comunicación.
- Con (router-id 0.0.4.1) determinamos el parámetro de OSPF con el cual podremos identificar el dispositivo que origina y procesa información del protocolo.

- Habilitamos enrutamiento de las redes 10.0.10.0 0.0.0.255 y 10.0.13.0 0.0.0.255 definiendo una rota entre áreas para este caso nombrada bajo área 0 con lo cual empezamos a nombrar o sectorizar el mapa de nuestra topología.
- Con la línea (default-information originate) mediante proceso RIP anunciamos dinámicamente la ruta determinada para los demás enrutadores.
- Damos exit para finalizar los procesos sobre las interfaces seleccionadas.
- Habilitamos con (ipv6 unicast-routing) el protocolo IPV6 en el Router.
- (ipv6 router ospf 6) Inicia el proceso de redirección OSPF para IPv6 y del mismo modo induce al modo de configuración para el proceso de redirección.
- En esta ocasión con (router-id 0.0.6.1) determinamos el parámetro determinado de OSPF con el cual podremos identificar el dispositivo que origina o procesa información del protocolo en consecuencia en esta ocasión para IPV6.
- Luego de anunciar para IPV6 la ruta dinámica, con Exit cerramos la configuración sobre estos protocolos y procedemos con configuración de las interfaces.
- Tanto para interfaz Ethernet 0/1 como para Serial 2/0 habilitamos direccionamiento Ipv6, protocolo Open Shortest Pacth First bajo V6 y asociamos en el mapa de topología bajo el área 0 correspondiente para todas las redes directamente conectadas.
- Configuramos las rutas estáticas de la interfaz NULL 0 designadas para IPV4 y 6.
- Habilitamos BGP para definir políticas de enrutamiento en la red ISP y establecemos el número de sistema autónomo (300).
- (bgp router-id 1.1.1.1) se determina el ID para la ruta que se estableció previamente en los protocolos tanto IPv4 y 6 con BGP Border Gateway Protocol.
- Configuramos con (neighbor IPv4 y IPV6 remote-as 500) la ruta del dispositivo remoto R2 para los dos protocolos, estableciendo el número de sistema autónomo con (500).
- Se habilita (address-family ipv4 unicast) con el fin de configurar una variedad de opciones de enrutamiento unidifusión del Protocolo de puerta de enlace vecina con versión V4 (habilitamos relación de confianza entre vecinos.) R2 y R3.
- Luego de realizar los ajustes donde definimos los direccionamientos entre familias para los protocolos V4 y V6 salimos fara finalizar (exit-address-family).

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interface e0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#interface s2/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)#no neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226 activate
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#exit-address-family
R1(config-router)#
```

Ilustración 8. Configuración enrutamiento R1

Router R2	
Enable	no neighbor 2001:db8:200::1 activate
Conf T	network 2.2.2.2 mask 255.255.255.255
interface Loopback 0	network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 loopback 0	exit-address-family
ipv6 route ::/0 loopback 0	address-family ipv6 unicast
router bgp 500	no neighbor 209.165.200.225 activate
bgp router-id 2.2.2.2	neighbor 2001:db8:200::1 activate
neighbor 209.165.200.225 remote-as 300	network 2001:db8:2222::/128
neighbor 2001:db8:200::1 remote-as 300	network ::/0
address-family ipv4	exit-address-family
neighbor 209.165.200.225 activate	

Tabla 13 Configuración enrutamiento R2

Pasos para la configuración en R2

- Ingresamos en modo configuración (configuración terminal).
- Habilitamos la interfaz virtual Loopback 0 (interfaz Loopback 0) la cual en mapa de ruteo es otra entrada de R2 para ISP.

- Se configura la ruta estática para interfaz loopback 0 (ip route 0.0.0.0 0.0.0.0 loopback 0).
- Habilitamos BGP para definir políticas de enrutamiento en la red ISP y establecemos el número de sistema autónomo (500).
- Designamos el ID (bgp router-id 2.2.2.2) para determinar bajo el ID 2.2.2.2 la ruta que se estableció previamente en los protocolos tanto IPv4 y 6 con BGP Border Gateway Protocol según corresponda.
- Con (neighbor 209.165.200.225 remote-as 300 y neighbor 2001:db8:200::1 remote-as 300) se habilitan y configuran la relación de vecinos desde R2 con R1 estableciendo el número de sistema autónomo en (300).
- Aplicando los anteriores comandos se hace lo mismo para configurar las familias vecinas que presentan entrada por Loopback 0.

```
R2(config)#interface Loopback 0
R2(config-if)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6 unicast
R2(config-router-af)#no neighbor 209.165.200.225 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#
```

Ilustración 9. Configuración enrutamiento R2

Router R3	
Enable	router-id 0.0.6.3
Conf T	exit
router ospf 4	interface e0/1
router-id 0.0.4.3	ipv6 ospf 6 area 0
network 10.0.11.0 0.0.0.255 area 0	exit
network 10.0.13.0 0.0.0.255 area 0	interface s2/0
exit	ipv6 ospf 6 area 0
ipv6 unicast-routing	exit
ipv6 router ospf 6	end

Tabla 14 Configuración enrutamiento R3

Pasos para la configuración en R3

- Ingresamos en modo configuración (configuración terminal).

- Por medio de (router ospf 4) Open Shortest Pacth First para IP V4 donde el ID asignado al proceso correspondiente al número 4 con el cual buscamos segmentar y determinar los mejores caminos de comunicación.
- Con (router-id 0.0.4.3) determinamos el parámetro de OSPF con el cual podremos identificar el dispositivo que origina y procesa información del protocolo de principio a fin.
- Construimos mapa de red con (network 10.0.11.0 0.0.0.255 area 0) que se forma entre D2 con R3 y lo mismo para (network 10.0.13.0 0.0.0.255 area 0) red formada entre R1 con R3.
- Antes de enunciar algún comando que requiera Ipv6 lo habilitamos con (ipv6 unicast-routing) el protocolo IPV6 en el Router R3.
- Esta vez con (router-id) 0.0.6.3 determinamos el parámetro de OSPF con el cual podremos identificar el dispositivo que origina y procesa información del protocolo de principio a fin.
- Ingresamos en la configuración de interfaz e0/1 y s2/0 para definir en IPV6 el área o la ruta más corta en la subred que se conforma desde R3.

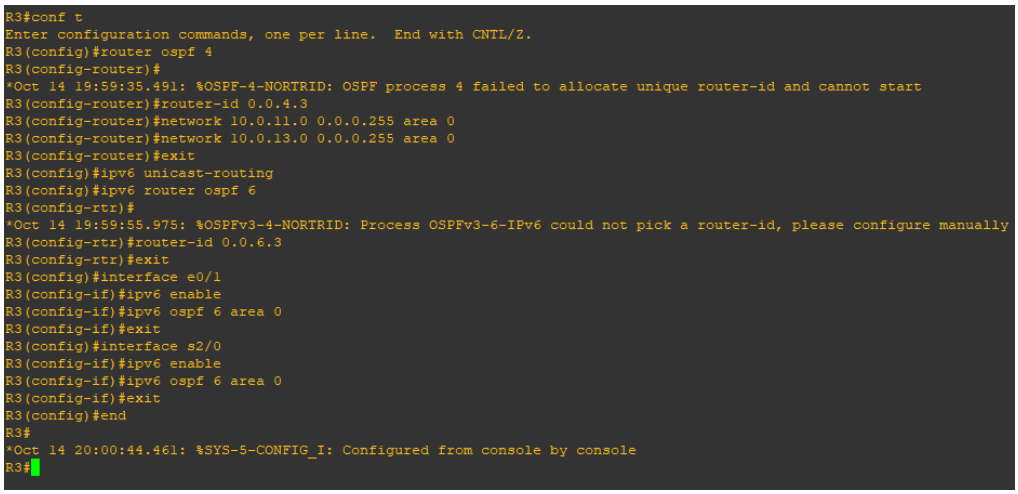

Ilustración 10. Configuración enrutamiento R3

Switch D1	
Enable	exit
Conf T	interface e2/2
router ospf 4	ipv6 ospf 6 area 0
router-id 0.0.4.131	exit
network 10.0.100.0 0.0.0.255 area 0	interface vlan 100
network 10.0.101.0 0.0.0.255 area 0	ipv6 ospf 6 area 0

network 10.0.102.0 0.0.0.255 area 0	exit
network 10.0.10.0 0.0.0.255 area 0	interface vlan 101
passive-interface default	ipv6 ospf 6 area 0
no passive-interface e2/2	exit
exit	interface vlan 102
ipv6 router ospf 6	ipv6 ospf 6 area 0
router-id 0.0.6.131	exit
passive-interface default	end
no passive-interface e2/2	

Tabla 15 Configuración enrutamiento D1

Pasos para la configuración en D1

- Luego de ingresar en modo configuración de terminal y habilitar por medio de (router ospf 4) se asigna el Router id (0.0.4.131) para la red que se conforma desde D1 con D2 y A1.
- La anterior configuración se asigna bajo nomenclatura de área 0 para las redes conformadas por las VLANs 100, 101 y 102.
- Con (passive-interface default) a modo de elevar la seguridad lo ejecutamos para que estas interfaces “anunciadas” no reciban actualizaciones de enrutamiento y tampoco formen adyacencias vecinas.
- En la interfaz e2/2 con (no passive-interface) excepcionamos para estas interfaces él envió de actualizaciones previamente y adyacencia de vecinos establecido.
- Tomamos una a una las VLAN 100,101 y 102 y con el uso de (ipv6 ospf 6 área 0) las asociamos al área 0 para definir el grupo de routers que comparten la misma información de estado de enlace.

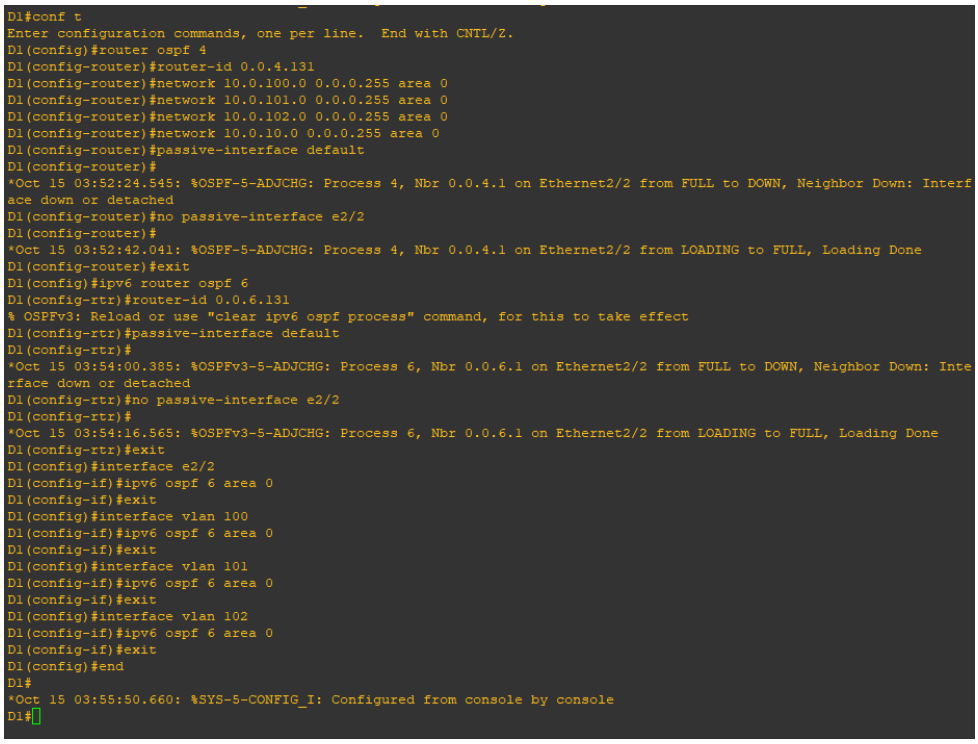

Ilustración 11. Configuración enrutamiento D1

Switch D2	
Enable	exit
Conf T	interface e2/2
router ospf 4	ipv6 ospf 6 area 0
router-id 0.0.4.132	exit
network 10.0.100.0 0.0.0.255 area 0	interface vlan 100
network 10.0.101.0 0.0.0.255 area 0	ipv6 ospf 6 area 0
network 10.0.102.0 0.0.0.255 area 0	exit
network 10.0.11.0 0.0.0.255 area 0	interface vlan 101
passive-interface default	ipv6 ospf 6 area 0
no passive-interface e2/2	exit
exit	interface vlan 102
ipv6 router ospf 6	ipv6 ospf 6 area 0
router-id 0.0.6.132	exit
passive-interface default	end
no passive-interface e2/2	

Tabla 16 Configuración enrutamiento D2

Pasos para la configuración en D2:

- Luego de ingresar en modo configuración de terminal y habilitar por medio de (router ospf 4) se asigna el Router id (0.0.4.132) para la red que se conforma desde D2 con D1 y A1.
- La anterior configuración se asigna bajo nomenclatura de área 0 para las redes conformadas por las VLANs 100, 101 y 102.
- Con (passive-interface default) a modo de elevar la seguridad lo ejecutamos para que estas interfaces “anunciadas” no reciban actualizaciones de enrutamiento y tampoco formen adyacencias vecinas.
- En la interfaz e2/2 con (no passive-interface) excepcionamos para estas interfaces él envió de actualizaciones previamente y adyacencia de vecinos establecido.
- Tomamos una a una las VLAN 100,101 y 102 y con el uso de (ipv6 ospf 6 área 0) las asociamos al área 0 para definir el grupo de routers que comparten la misma información de estado de enlace.

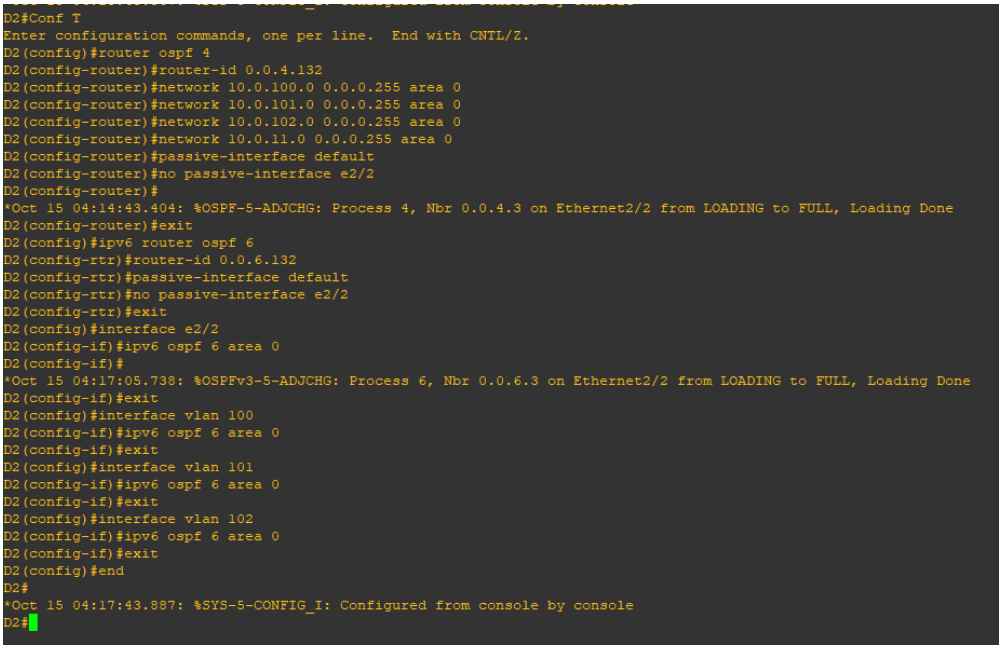

Ilustración 12. Configuración enrutamiento D2

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. • Use la SLA número **4** para IPv4. • Use la SLA número **6** para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. • Use la SLA número **4** para IPv4. • Use la SLA número **6** para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Tabla 17 Tareas parte 4

Tarea#	Tarea	Especificación
4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60.

		Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.
Tarea#	**Tarea**	**Especificación**
	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101:

		• Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

Tabla 18 Tareas parte 4-1

En esta parte utilizamos tecnologías IP SLA con la cual los enrutadores pueden realizar diversas pruebas de red mediante el intercambio de datos, para recopilar información sobre el rendimiento de la red, adicionalmente nos ayuda para administrar los niveles de calidad del servicio, también es una herramienta que nos permite validar la raíz de problemas que se puedan presentar y comprometan los niveles de rendimiento.

También involucramos el protocolo HSRPv2 el cual ya interviene principalmente en la capa 3, este ese encargara de administrar las direcciones virtuales que identifican cada enrutador.

Comandos de configuración aplicados en cada dispositivo

Switch D1	
ip sla 4	standby 106 preempt
icmp-echo 10.0.10.1	standby 106 track 6 decrement 60
frequency 5	exit
exit	interface vlan 101
ip sla 6	standby version 2
icmp-echo 2001:db8:100:1010::1	standby 114 ip 10.0.101.254
frequency 5	standby 114 preempt
exit	standby 114 track 4 decrement 60
ip sla schedule 4 life forever start-time now	standby 116 ipv6 autoconfig
ip sla schedule 6 life forever start-time now	standby 116 preempt

track 4 ip sla 4	standby 116 track 6 decrement 60
delay down 10 up 15	exit
exit	interface vlan 102
track 6 ip sla 6	standby version 2
delay down 10 up 15	standby 124 ip 10.0.102.254
exit	standby 124 priority 150
interface vlan 100	standby 124 preempt
standby version 2	standby 124 track 4 decrement 60
standby 104 ip 10.0.100.254	standby 126 ipv6 autoconfig
standby 104 priority 150	standby 126 priority 150
standby 104 preempt	standby 126 preempt
standby 104 track 4 decrement 60	standby 126 track 6 decrement 60
standby 106 ipv6 autoconfig	exit
standby 106 priority 150	end

Tabla 19 Configuración redundancia en D1

Pasos para la configuración en D1

- Configuramos tecnología SLA para IPv4 (ip sla 4) para la interfaz que se comunica con R1 por medio de la IP 10.0.10.1, con el cual se busca que cada 5 segundos (frequency 5) probara disponibilidad de esta interfaz.
- Del mismo modo se configura tecnología SLA para IPv6 para la interfaz que hace comunicación con R1 con dirección (2001:db8:100:1010::1) acorde al protocolo, la cual el mismo modo cada 5 segundos (frequency 5) probara disponibilidad o comunicación con esta interfaz en R1.
- Programamos que las indicaciones programadas sean ejecutadas indefinidamente por medio del comando (ip sla schedule 4 life forever start-time now y ip sla schedule 6 life forever start-time now) propiamnete para IPv4 e Ipv6.
- Anunciando cada uno de los protocolos con el comando (delay down 10 up 15) definimos deben notificar a D1 cuando el estado de IP SLA cambie de inactivo a activo después de 10 segundos o viceversa después de 15 segundos.
- En D1 establecemos su prioridad cambie a 150 configurando los grupos de HSRP para administrar direcciones virtuales donde definimos los grupos 104, 114 y 124 para las VLANs 100, 101 y 102 asignando la IP Virtual 10.0.100.254 habilitando preferencia (preemption), con esta última se garantiza que el dispositivo que ingrese a estado activo se base en la

prioridad establecida (150), finalmente se indica que rastree el objeto 4 para su seguimiento.

- Configuramos ahora IPv6 HSRP con los grupos 106 116 y 126 para las VLANs 100, 101 y 102, en este caso asignamos a IP virtual por DHCP con el comando ipv6 autoconfig igual que en el paso anterior para v4 habilitamos preferencia (preemption), para garantizar que el dispositivo que llegue a ingresar mantenga la misma prioridad (150) y se indica rastrear el objeto 6.
- Con lo anterior se definen las políticas con las que deben entrar los nuevos elementos en estas redes.

```
D1#show run | section ip sla
track 4 ip sla 4
 delay down 10 up 15
track 6 ip sla 6
 delay down 10 up 15
ip sla 4
 icmp-echo 10.0.10.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1010::1
 frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

Ilustración 13 IP SLA en D1

Switch D2	
ip sla 4	standby 106 track 6 decrement 60
icmp-echo 10.0.11.1	exit
frequency 5	interface vlan 101
exit	standby version 2
ip sla 6	standby 114 ip 10.0.101.254
icmp-echo 2001:db8:100:1011::1	standby 114 priority 150
frequency 5	standby 114 preempt
exit	standby 114 track 4 decrement 60
ip sla schedule 4 life forever start-time now	standby 116 ipv6 autoconfig
ip sla schedule 6 life forever start-time now	standby 116 priority 150
track 4 ip sla 4	standby 116 preempt
delay down 10 up 15	standby 116 track 6 decrement 60
exit	exit
track 6 ip sla 6	interface vlan 102
delay down 10 up 15	standby version 2
exit	standby 124 ip 10.0.102.254
interface vlan 100	standby 124 preempt
standby version 2	standby 124 track 4 decrement 60
standby 104 ip 10.0.100.254	standby 126 ipv6 autoconfig

standby 104 preempt	standby 126 preempt
standby 104 track 4 decrement 60	standby 126 track 6 decrement 60
standby 106 ipv6 autoconfig	exit
standby 106 preempt	end

Tabla 20 Configuración redundancia en D2

Pasos para la configuración en D2

- Configuramos tecnología SLA para IPv4 (ip sla 4) para la interfaz que se comunica con R3 por medio de la IP 10.0.11.1, con el cual se busca que cada 5 segundos (frequency 5) probara disponibilidad de esta interfaz.
- Del mismo modo se configura tecnología SLA para IPv6 para la interfaz que hace comunicación con R3 con dirección (2001:db8:100:1011::1) acorde al protocolo, la cual el mismo modo cada 5 segundos (frequency 5) probara disponibilidad o comunicación con esta interfaz en R3.
- Programamos que las indicaciones programadas sean ejecutadas indefinidamente por medio del comando (ip sla schedule 4 life forever start-time now y ip sla schedule 6 life forever start-time now) propiamnete para IPv4 e Ipv6.
- Anunciando cada uno de los protocolos con el comando (delay down 10 up 15) definimos deben notificar a D1 cuando el estado de IP SLA cambie de inactivo a activo después de 10 segundos o viceversa después de 15 segundos.
- En D2 establecemos su prioridad cambie a 150 configurando los grupos de HSRP para administrar direcciones virtuales donde definimos los grupos 104, 114 y 124 para las VLANs 100, 101 y 102 asignando la IP Virtual 10.0.102.254 habilitando preferencia (preemption), con esta última se garantiza que el dispositivo que ingrese a estado activo se base en la prioridad establecida (150) al igual que en D1.
- Configuramos ahora IPv6 HSRP con los grupos 106 116 y 126 para las VLANs 100, 101 y 102, en este caso asignamos a IP virtual por DHCP con el comando ipv6 autoconfig igual que en el paso anterior para v4 habilitamos preferencia (preemption), para garantizar que el dispositivo que llegue a ingresar mantenga la misma prioridad (150) y se indica rastrear el objeto 6.
- Con lo anterior se definen las políticas con las que deben entrar los nuevos elementos en estas redes.

```
D2#show run | section ip sla
track 4 ip sla 4
 delay down 10 up 15
track 6 ip sla 6
 delay down 10 up 15
ip sla 4
 icmp-echo 10.0.11.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1011::1
 frequency 5
ip sla schedule 6 life forever start-time now
D2#
```

Ilustración 14 IP SLA en D2

Parte 5: Seguridad

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.

5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **raduser** y la contraseña: **upass123**.

Tabla 21 Tareas parte 5

En el paso 5 realizamos configuraciones de seguridad donde procedemos a configurar el modo EXEC protegido.

- Ingresando en modo configuración de consola realizamos asignación de contraseña **cisco12345cisco.**
- Seguido creamos el usuario local **SADMIN.**
- Asignando nivel de privilegios 15 el cual permitirá acceso completo a todos los comandos.
- Finalmente copiamos estas configuraciones en la NVRAM usando el comando (copy running-config startup-config).

Todos los dispositivos
Conf t
enable algorithm-type SCRYPT secret cisco12345cisco
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
exit

Tabla 22 Configuración de seguridad ALL Devices

```
R1#en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable algorithm-type SCRYPT secret ciscol2345cisco
R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret ciscol234$
R1(config)#exit
R1#
*Nov  4 04:17:28.170: %SYS-5-CONFIG_I: Configured from console by console
R1#en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#exit
R1#
*Nov  4 04:18:35.569: %SYS-5-CONFIG_I: Configured from console by console
R1#show run | include secret
enable secret 9 $9$.aOKsQPrHcC/CX$.5mG0G5214mOb32Vs311mCy8dYMmnBjnRobUOVvJZMY
username sadmin privilege 15 secret 9 $9$wH6JNQoR.i3rbX$j6Xjku.2haBrfBne8cBfPSy9yMWlA0su8Xq9EB.yOZ2
R1#
```

Ilustración 15 Show run contraseña

Dispositivos R1, R3, D1, D2 y A1
aaa new-model
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
exit

aaa authentication login default group radius local
end

Ilustración 16 Server RADIUS

- Con la configuración realizada anteriormente en todos los dispositivos a excepción de R2 habilitamos en primera instancia el protocolo **AAA** el cual se encarga de realizar 3 funciones (Authentication, Authorization and Accounting) que en otras palabras es una lista de métodos de autenticación.
- Configuramos el servidor RADIUS con dirección IP 10.0.100.6 con los puertos 1812 que se asignara para los mensajes de autenticación y 1813 para los mensajes de contabilización.
- Seguido configuramos la autenticación AAA para los dispositivos de manera predeterminada con el comando (aaa authentication login default group radius local) donde la lista nombrada es predeterminada y se incluyen 2 métodos de autenticación (radio de grupo y local).

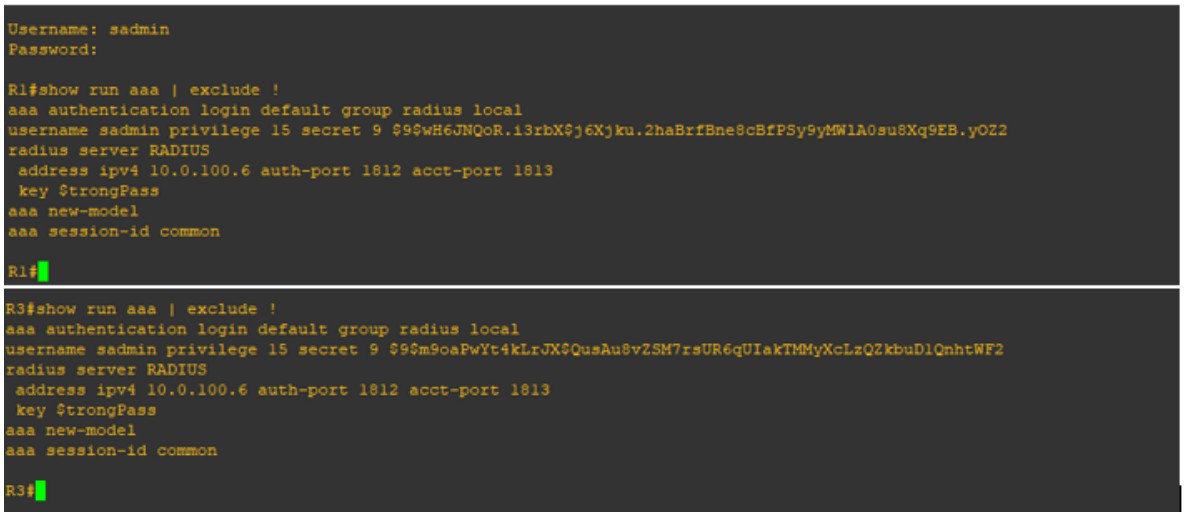

Ilustración 17 Show run AAA

Parte 6: Configure las funciones de Administración de Red

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
Tarea#	**Tarea**	**Especificación**

6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *traps config* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

Tabla 23 Tareas parte 6

Para el paso 6 configuramos inicialmente en R2 el protocolo NTP (Network Time Protocol) y lo determinamos como maestro, y para los demás dispositivos configuramos UTC (Universal Time Coordinated), con lo que buscamos tomen la configuración local definida desde R2 para los equipos de la red.

Router R1	
Conf t	snmp-server contact Cisco Student
ntp server 2.2.2.2	snmp-server community ENCORSA ro SNMP-NMS
logging trap warning	snmp-server host 10.0.100.5 version 2c ENCORSA
logging host 10.0.100.5	snmp-server ifindex persist
logging on	snmp-server enable traps bgp
ip access-list standard SNMP-NMS	snmp-server enable traps config
permit host 10.0.100.5	snmp-server enable traps ospf
exit	end

Tabla 24 Administración de red R1

Router R3	
ntp server 10.0.10.1	snmp-server contact Cisco Student
logging trap warning	snmp-server community ENCORSA ro SNMP-NMS
logging host 10.0.100.5	snmp-server host 10.0.100.5 version 2c ENCORSA
logging on	snmp-server ifindex persist
ip access-list standard SNMP-NMS	snmp-server enable traps config
permit host 10.0.100.5	snmp-server enable traps ospf
exit	end

Tabla 25 Administración de red R3

Switch D1 - A1	
ntp server 10.0.10.1	snmp-server contact Cisco Student
logging trap warning	snmp-server community ENCORSA ro SNMP-NMS
logging host 10.0.100.5	snmp-server host 10.0.100.5 version 2c ENCORSA
logging on	snmp-server ifindex persist
ip access-list standard SNMP-NMS	snmp-server enable traps config
permit host 10.0.100.5	snmp-server enable traps ospf
exit	end

Tabla 26 Administración de red D1 - A1

Switch D2	
Conf t	exit
ntp server 10.0.10.1	snmp-server contact Cisco Student

logging trap warning	snmp-server community ENCORSA ro SNMP-NMS
logging host 10.0.100.5	snmp-server host 10.0.100.5 version 2c ENCORSA
logging on	snmp-server enable traps config
ip access-list standard SNMP-NMS	snmp-server enable traps ospf
permit host 10.0.100.5	end

Tabla 27 Administración de red D2

- ➔ Configuramos protocolo NTP el cual lo tomará del dispositivo definido como servidor o maestro y tendrá salida por 10.0.10.1 partiendo de su condición al tener comunicación directa con R2.
- ➔ Por medio del comando (logging trap warning) enrutado para que cargue la información en 10.0.100.5, siendo PC1 donde se almacenaran para los análisis respectivos los mensajes que se envíen al servidor NTP maestro.
- ➔ Con (ip access-list standard SNMP-NMS) configuramos los dispositivos como agentes (Simple Network Management Protocol) que corresponde a un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de la topología. Permitiendo el tráfico en la red con destino a 10.0.100.5 PC1 determinado anteriormente como fuente de almacenamiento.
- ➔ Finalmente habilitamos él envió de información de los diferentes protocolos con los que se cuentan en la red que serán almacenados en PC1.

Ilustración 18 Consulta clock

Router R2	
ntp master 3	end

Tabla 28 Network Time Protoco R2

Estando en modo de configuración ingresamos el comando (NTP master) con el cual habilitamos la sincronización de relojes y así mismo definimos como maestro, incluimos el numero 3 haciendo referencia a la condición jerarquía o estrato que se aplicara.

Ilustración 19 Configuración UTC R2

CONCLUSIONES

Por medio de este trabajo se evidencia la ejecución y aplicación de los conocimientos adquiridos durante cada una de las unidades del Diplomado de profundización CISCO CCNP, al poner este aprendizaje en práctica mediante los escenarios desarrollados se está obteniendo como resultado tener una mayor competencia en el ámbito de las redes de comunicaciones, sus configuraciones y su aplicación.

Mediante desarrollo practico de los escenarios o ejercicios propuestos y realizados en los entornos y software de desarrollo como GNS3, se obtienen habilidades para la correcta configuración de equipos de enrutamiento utilizando protocolos como el OSPF y EIGRP los cuales se implementaron en el desarrollo propuesto del escenario 1

La implementación de protocolos como Spanning Tree permiten una mejor optimización de los recursos de nuestra red, puesto que evitan él envió desproporcionado de paquetes entre equipos y garantizan una convergencia de red ágil.

Durante la presente actividad se pusieron en marcha los conocimientos previamente adquiridos durante el presente semestre, principalmente relacionados con la configuración de dispositivos emulados virtuales L3 y L2 utilizando protocolos basados en VLANs.

CNNP brinda todos los conocimientos que permiten reforzar nuestras capacidades y habilidades necesarias para la implementación de estructuras de red integradas.

Mediante conocimientos adquiridos en OSPF denominada multi área nos brinda destrezas que podemos llevar a la practica en redes de mayor tamaño o gruesa arquitectura, ya que reduce las cargas de almacenamiento y procesamiento, OSPF se utiliza para calcular las mejores rudas reduciendo redundancia en la comunicación entre dispositivos de red, ya que coloca las rutas aprendidas en bases de datos utilizadas para crear la tabla de routing.

BIBLIOGRÁFIA

CISCO. (s.f.). Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-does-a-router-work

Cursos y Master en Madrid – Formatalent. (s.f.). Obtenido de https://formatalent.com/diferencias-entre-ccna-y-ccnp/

De luz, S. (12 de Agosto de 2021). redeszone.net. Obtenido de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Digital Guide IONOS. (02 de Marzo de 2020). Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/lan/

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Overlay Tunnels**.** CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF v3**.** CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Gerometta, O. (17 de Febrero de 2019). Mis Libros de Networking. Obtenido de http://librosnetworking.blogspot.com/2019/02/la-direccion-de-loopback.html

IBM. (s.f.). Obtenido de https://www.ibm.com/docs/es/i/7.1?topic=routing-open-shortest-path-first

Rockcontent. (4 de Septiembre de 2020). Obtenido de https://rockcontent.com/es/blog/que-es-un-host/

UNAD (2017). Configuración de Switches y Routers [OVA]**.** Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC