DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS FERNANDO JIMÉNEZ BARRETO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS FERNANDO JIMÉNEZ BARRETO

Diplomado de opción de grado presentado para optar el título de Ingeniero de Telecomunicaciones

TUTOR:
Mag. JOHN HAROLD PÉREZ CALDERÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 17 de NOVIEMBRE de 2022

AGRADECIMIENTOS

Inicialmente quiero agradecer a Dios porque es quien concede la fuerza y las oportunidades para poder alcanzar las metas personales. Seguido quiero agradecer a mi familia a quienes sin duda alguna han sido pacientes y me han apoyado incondicionalmente, pues a lo largo de este proceso he sacrificado tiempo de calidad con ellos, para poder estar a la altura y exigencia de este diplomado y cumplir así de forma satisfactoria los objetivos. A mi madre, quiero hacer una mención especial porque fue quien me brindó los cimientos en una educación llena de valores y principios los cuales son la base fundamental de todos mis logros. A mis compañeros a quienes les debo su colaboración en la resolución de inquietudes y a cada uno de los docentes quienes me guiaron en este hermoso proceso de aprendizaje.

TABLA DE CONTENIDO

LISTA DE TABLAS

TABLA DE ILUSTRACIONES

GLOSARIO

CCNP: es el nivel intermedio de certificación de la compañía. En donde se deben superarvarias etapas y exámenes.

EtherChannel: tecnología que permite unir varios enlaces físicos en un solo enlace lógico proporcionando mayor ancho de banda, redundancia a fallos, uso compartido de carga.

GNS3: simulador usado para emular, probar, configurar y solucionar problemas enambientes virtuales reales.

Router: dispositivo que proporciona conectividad a nivel de red bajo el modelo OSI, en donde su función principal consiste en encaminar o enviar paquetes de datos de una red a otra, interconectando Subredes.

Switch: Dispositivo lógico de interconexión de equipos que opera bajo el modelo OSI. Interconecta dos o más host a los puentes de red, pasando datos de un segmento a otro dependiendo de la dirección MAC de destino de las tramas en la red.

VLAN: Red de area local virtual, lo que permite crear redes de area local independientes dentro de una red física, lo que facilita la administración y seguridad.

RESUMEN

El presente trabajo tiene como fin demostrar las habilidades prácticas adquiridas en el diplomado de profundización CCNP como opción de grado al título de ingeniero en telecomunicaciones de la universidad Nacional Abierta y a Distancia UNAD.

En este documento se evidencia el desarrollo de una red para una compañía la cual de acuerdo a sus necesidades debe cumplir unos parámetros de configuración y seguridad, permitiendo de esta forma realizar la práctica de cada uno de los temas y protocolos vistos en los diferentes módulos del presente diplomado.

Es así como se podrá observar en el desarrollo del proyecto, gracias a la herramienta de software GNS3 la cual fue usada para poder llevar a cabo el diseño y simulación de la red de datos empresarial, la cual se efectuó en 4 partes principalmente, donde se explica la configuración paso a paso de cada uno de los protocolos que en esta red se usaron con el fin de dar una solución óptima. Los protocolos usados fueron: *spanning-tree, etherchannels*, DHCP, OSPFv2, OSPFV3, BGP, se dispone HSRPv2 para proveer redundancia.

Palabras Clave: CISCO, CCNP, ENRUTAMIENTO, CONMUTACIÓN, BGP, *ETHERCHANNEL*, REDES, HSRPv2, OSPFV3.

ABTRACT

The purpose of this work is to demonstrate the practical skills acquired in the CCNP deepening diploma as a degree option for the degree of telecommunications engineer of the Universidad Nacional Abierta y a Distancia UNAD.

This document shows the development of a network for a company which, according to its needs, must comply with some configuration and security parameters, thus allowing the practice of each of the topics and protocols seen in the different modules of this diploma course.

This is how it can be seen in the development of the project, thanks to the software tool GNS3 which was used to carry out the design and simulation of the enterprise data network, which was carried out in 4 parts mainly, where the configuration is explained step by step of each of the protocols that were used in this network in order to provide an optimal solution. The protocols used were: spanning-tree, etherchannels, DHCP, OSPFv2, OSPFV3, BGP, and HSRPv2 to provide redundancy.

Key Words: CISCO, CCNP, ENRUTAMIENTO, CONMUTACIÓN, BGP, ETHERCHANNEL, REDES, HSRPv2, OSPFV3.

CAPÍTULO I
INTRODUCCIÓN

El presente documento es la evidencia de habilidades prácticas para el diplomado de profundización CCNP, para optar al título de ingeniero en telecomunicaciones de la Universidad Nacional Abierta y a Distancia UNAD, en el cual se plantea diseñar y configurar dos escenarios para una red empresarial. Donde se pretende aplicar los conocimientos adquiridos durante el desarrollo del evento académico.

Dando una solución a los dos escenarios de red planteados para una compañía en este trabajo, se busca afianzar y profundizar en esos conceptos y protocolos de conmutación y enrutamiento que se aprendieron en el proceso de cada actividad y laboratorio efectuado en los diferentes módulos del diplomado CCNP.

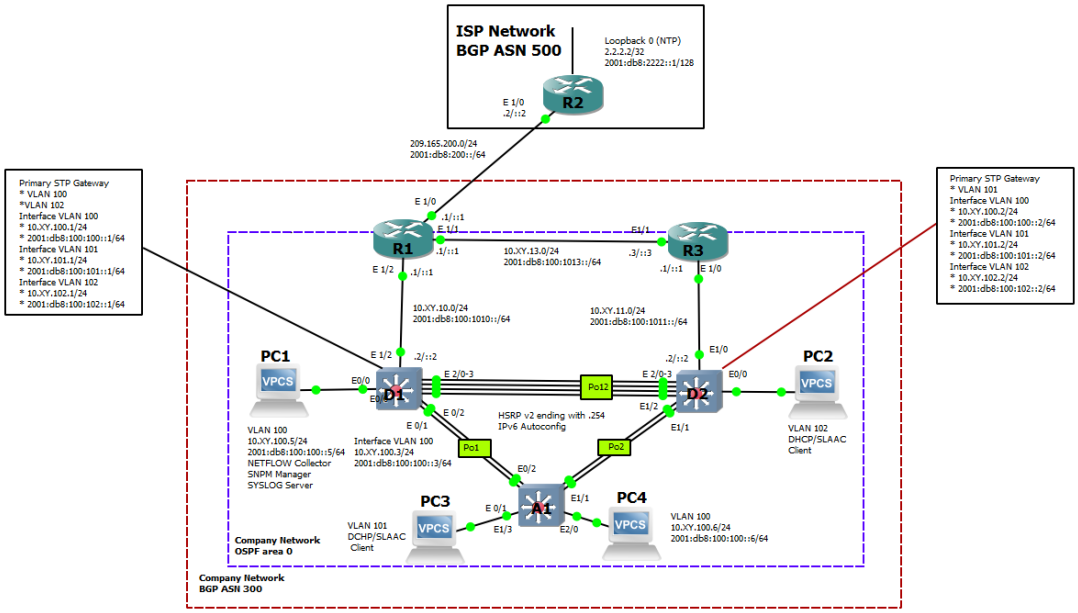
Este trabajo será la evidencia de que todo el conocimiento adquirido en el presente diplomado y durante todo el proceso en las diferentes materias que tienen que ver con redes de datos, permiten desarrollar competencias y ajustar los perfiles para llevarlo a la aplicación en la vida real, en los diferentes entornos que afronte un ingeniero en telecomunicaciones.

Es así como se logra realizar el diseño y configuración para la compañía de una red convergente, gracias al software GNS3 el cual permite simular de manera casi real estos escenarios, logrando interactuar con dispositivos activos de red, computadores, cableado, logrando así incorporar protocolos de enrutamiento y conmutación de la misma forma que si se realizara en un escenario real.

CAPÍTULO II
DESARROLLO

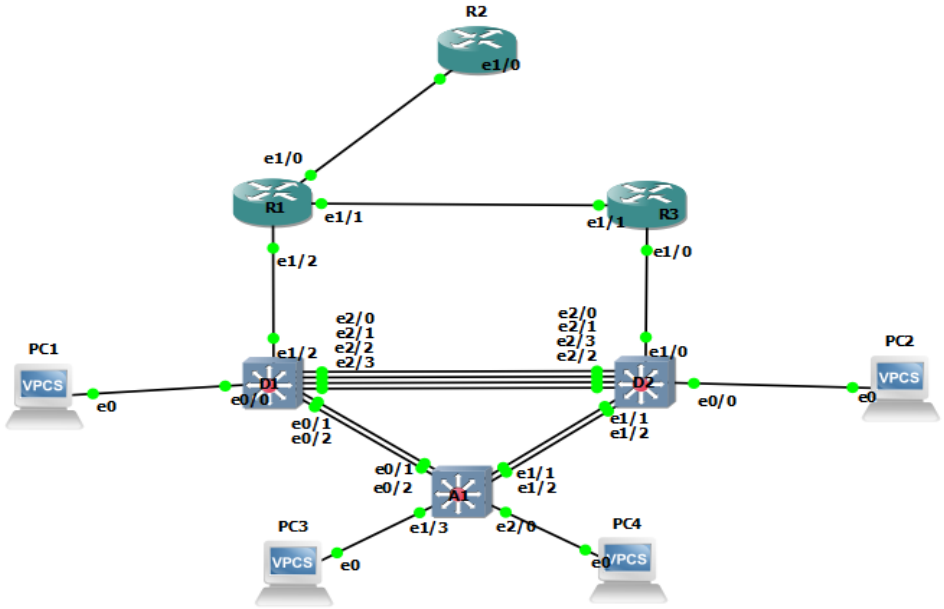
II.I ESCENARIO 1

Ilustración 1. Escenario propuesto



Fuente: UNAD

Ilustración 2. Diseño realizado.



Fuente: Propia.

Tabla 1. Direccionamiento

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.51.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10. 51.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10. 51.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10. 51.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10. 51.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10. 51.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10. 51.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10. 51.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10. 51.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10. 51.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10. 51.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10. 51.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10. 51.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10. 51.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente. UNAD

II.I.I Construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz.

En la Parte 1, establecerá la topología de la red y configurará los ajustes básicos y el direccionamiento de las interfaces.

a) Cablear la red como se muestra en la topología.

Se realizó la construcción de la topología según la ilustración 1 Seguido por las conexiones a las Ethernet disponibles en cada dispositivo.

b) Configurar los ajustes básicos para cada dispositivo.

Se realiza la configuración básica en cada elemento siguiendo los pasos y los comandosmencionados en la guía de trabajo

Router R1

```
configure terminal
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
 ip address 209.165.200.225 255.255.255.224
 ipv6 address fe80::1:1 link-local
 ipv6 address 2001:db8:200::1/64
 no shutdown
 exit
interface e1/1
 ip address 10.51.13.1 255.255.255.0
 ipv6 address fe80::1:3 link-local
 ipv6 address 2001:db8:100:1013::1/64
 no shutdown
 exit
interface e1/2
 ip address 10.51.10.1 255.255.255.0
 ipv6 address fe80::1:2 link-local
 ipv6 address 2001:db8:100:1010::1/64
 no shutdown
 exit
copy running-config startup-config
```

Descripción de cada comando ejecutado:

! Permite entrar al modo de configuración Global
! Se asigna nombre al router
! Habilitamos el direccionamiento IPv6 en el dispositivo
! Desactivar la búsqueda DNS
! Mensaje de aviso
! Ingresar al modo de configuración de línea de la consola
! Establece el tiempo de espera inactivo de la sesión remota
! Define el nivel de severidad de los mensajes de eventos que el sistema envía al puerto consola.
! Salir de la configuración global

! Configuración de interfaz Ethernet 1/0
! Asignamos la dirección Ipv4 de la interfaz y especificamos la máscara de subred
! Asignamos ipv6 link-local
! Asignamos la dirección ipv6 de la interfaz
! Encendemos el puerto de la interfaz.
! Salimos de la configuración de la interfaz.
! Copiar la configuración en ejecución al archivo de configuración de inicio

Se repite el procedimiento de configuración para las interfaces Ethernet 1/1-2

Router R2

```
configure terminal
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
 ip address 209.165.200.226 255.255.255.224
 ipv6 address fe80::2:1 link-local
 ipv6 address 2001:db8:200::2/64
 no shutdown
 exit
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
 ipv6 address fe80::2:3 link-local
 ipv6 address 2001:db8:2222::1/128
 no shutdown
 exit
copy running-config startup-config
```

Descripción de cada comando ejecutado:

! Permite entrar al modo de configuración Global
! Se asigna nombre al router
! Habilitamos el direccionamiento IPv6 en el dispositivo
! Desactivar la búsqueda DNS
! Mensaje de aviso
! Ingresar al modo de configuración de línea de la consola
! Establece el tiempo de espera inactivo de la sesión remota
! Define el nivel de severidad de los mensajes de eventos que el sistema envía al puerto consola.
! Salir de la configuración global
! Configuración de interfaz Ethernet 1/0
! Asignamos la dirección Ipv4 de la interfaz y especificamos la máscara de subred
! Asignamos ipv6 link-local
! Asignamos la dirección ipv6 de la interfaz
! Habilitamos la interfaz
! Salimos de la configuración de la interfaz.
! Ingresamos a la interfaz loopback 0 es una interfaz lógica que asegura que por lo menos una interfaz esté siempre disponible

! Asignamos la dirección Ipv4 de la interfaz y especificamos la máscara de subred
! Asignamos la dirección Ipv4 de la interfaz y especificamos la máscara de subred
! Salimos de la configuración de la interfaz
! Copiar la configuración en ejecución al archivo de configuración de inicio.

Router R3
configure terminal
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
ip address 10.51.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface e1/1
ip address 10.51.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
copy running-config startup-config

Switch D1
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit

```
interface e1/2
 no switchport
 ip address 10.51.10.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:100:1010::2/64
 no shutdown
 exit
interface vlan 100
 ip address 10.51.100.1 255.255.255.0
 ipv6 address fe80::d1:2 link-local
 ipv6 address 2001:db8:100:100::1/64
 no shutdown
 exit
interface vlan 101
 ip address 10.51.101.1 255.255.255.0
 ipv6 address fe80::d1:3 link-local
 ipv6 address 2001:db8:100:101::1/64
 no shutdown
 exit
interface vlan 102
 ip address 10.51.102.1 255.255.255.0
 ipv6 address fe80::d1:4 link-local
 ipv6 address 2001:db8:100:102::1/64
 no shutdown
 exit
ip dhcp excluded-address 10.51.101.1 10.51.101.109
ip dhcp excluded-address 10.51.101.141 10.51.101.254
ip dhcp excluded-address 10.51.102.1 10.51.102.109
ip dhcp excluded-address 10.51.102.141 10.51.102.254
ip dhcp pool VLAN-101
network 10.51.101.0 255.255.255.0
default-router 10.51.101.254
exit
ip dhcp pool VLAN-102
network 10.51.102.0 255.255.255.0
default-router 10.51.102.254
 exit
interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
 shutdown
 exit
```

Descripción de cada comando ejecutado:

! Permite entrar al modo de configuración Global
! Configura el nombre del dispositivo.
! Habilitamos el direccionamiento IPv6 en el dispositivo
! Desactivar la búsqueda DNS
! ¡Mensaje de aviso! Ingresar al modo de configuración de línea de la consola
! Establece el tiempo de espera inactivo de la sesión remota
! Define el nivel de severidad de los mensajes de eventos que el sistema envía al puerto consola.
! Modo de configuración *vlan* 100

! Nombre grupo de usuarios de la vlan 100
! Modo de configuración vlan 101
! Nombre grupo de usuarios de la vlan 101
! Modo de configuración vlan 102
! Nombre grupo de usuarios de la vlan 102
! Modo de configuración vlan 999
! Nombre grupo de usuarios de la vlan 999 NATIVE
! Entramos al modo de configuración de la interfaz Ethernet 1/2.
! Este comando evita que la interfaz genere tramas DTP
! Asignación de dirección ipv4 y mascara de subred
! Asignación de dirección ipv6 link local
! Asignación de dirección ipv6 de la subinterfaz
! Se activa la interfaz
! Ingresamos al modo de Configuración vlan 100
! Asignación de dirección ipv4 y mascara de subred
! Asignación de dirección ipv6 link local
! Asignación de dirección ipv6 de la subinterfaz
! Se habilita la interfaz.
! Se repite la configuración para las vlan 101 y 102 teniendo en cuenta la tabla de direccionamiento.
! Se excluye el rango de direcciones
! Se excluye el rango de direcciones
! Se excluye el rango de direcciones
! Se excluye el rango de direcciones
! Configuración DHCP pool vlan 101
! Asignamos direccionamiento ipv4 al servicio DHCP
! Habilitamos router por defecto a la vlan y asignamos la puerta de enlace.
! configuración DHCP pool vlan 102
! Asignamos direccionamiento ipv4 al servicio DHCP
! Habilitamos router por defecto a la vlan y asignamos la puerta de enlace
! Ingresamos a la configuración del rango de interfaces e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
! Apagamos o deshabilitamos los puertos de las interfaces
! Finaliza la configuración y nos saca de modo global
! Guarda la configuración del dispositivo.

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment#
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
vlan 100
 name Management
 exit
vlan 101
```

```
 name UserGroupA
 exit
vlan 102
 name UserGroupB
 exit
vlan 999
 name NATIVE
 exit
interface e1/0
 no switchport
 ip address 10.51.11.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:100:1011::2/64
 no shutdown
 exit
interface vlan 100
 ip address 10.51.100.2 255.255.255.0
 ipv6 address fe80::d2:2 link-local
 ipv6 address 2001:db8:100:100::2/64
 no shutdown
 exit
interface vlan 101
 ip address 10.51.101.2 255.255.255.0
 ipv6 address fe80::d2:3 link-local
 ipv6 address 2001:db8:100:101::2/64
 no shutdown
 exit
interface vlan 102
 ip address 10.51.102.2 255.255.255.0
 ipv6 address fe80::d2:4 link-local
 ipv6 address 2001:db8:100:102::2/64
 no shutdown
 exit
ip dhcp excluded-address 10.51.101.1 10.51.101.209
ip dhcp excluded-address 10.51.101.241 10.51.101.254
ip dhcp excluded-address 10.51.102.1 10.51.102.209
ip dhcp excluded-address 10.51.102.241 10.51.102.254
dhcp pool VLAN-101
 network 10.51.101.0 255.255.255.0
 default-router 10.51.101.254
 exit
ip dhcp pool VLAN-102
 network 10.51.102.0 255.255.255.0
 default-router 10.51.102.254
 exit
interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
 shutdown
 exit
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment#
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
vlan 100
 name Management
 exit
vlan 101
 name UserGroupA
 exit
vlan 102
 name UserGroupB
 exit
vlan 999
 name NATIVE
 exit
interface vlan 100
 ip address 10.51.100.3 255.255.255.0
 ipv6 address fe80::a1:1 link-local
 ipv6 address 2001:db8:100:100::3/64
 no shutdown
 exit
interface range e0/0,e0/3,e1/0,e2/1-3,e3/0-3
 shutdown
 exit
```

Ilustración 3. Configuración PC1

```
PC1> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    10.51.100.5/24       10.51.100.254     00:50:79:66:68:01  20032  127.0.0.1:20033
       fe80::250:79ff:fe66:6801/64
       2001:db8:100:100:2050:79ff:fe66:6801/64 eui-64
```

Fuente: Propia.

Ilustración 4. Configuración PC4

```
PC4> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    10.51.100.6/24       10.51.100.254     00:50:79:66:68:03  20028  127.0.0.1:20029
       fe80::250:79ff:fe66:6803/64
       2001:db8:100:100:2050:79ff:fe66:6803/64 eui-64
```

Fuente: Propia.

II.I.II Configurar la capa 2 de la red y el soporte de Host

En esta parte de la evaluación de habilidades, se completa la configuración de la red de Capa 2 y se establece el soporte básico del host. Al final de esta parte, todos los conmutadores deben ser capaces de comunicarse. El PC2 y el PC3 deben recibir direcciones desde DHCP y SLAAC.

a) Habilite enlaces *trunk* 802.1Q.

Procedemos a crear el protocolo VRF en cada dispositivo con los comandos:

Switch D1 and D2

D1

confgure terminal	// ingreso configuración global
interface range Ethernet 2/0-3	// Ingresamos al rango de interfaces Ethernet 2/0-3
switchport trunk encapsulation dot1q	// Habilitamos el modo troncal de las interfaces.
switchport mode trunk	// ponemos el modo troncal a las interfaces
switchport trunk allowed vlan 100,101,102	// permite el paso de VLANs de un enlace troncal
end	// finalizamos la configuración global
wr	// guardamos la configuración del dispositvo.

D2

enable
configure terminal
interface range Ethernet 2/0-3
switchport trunk encapsulation dot1q
switch mode trunk
switchport trunk allowed vlan 100,101,102

Switch D1 and A1

D1

enable
configure terminal
interface range Ethernet 0/1-2
switchport trunk encapsulation dot1q
switch mode trunk
switchport trunk allowed vlan 100,101,102
end

A1
interface range Ethernet 0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 100,101,102
end

D2 and A1

D2
configure terminal
interface range Ethernet 1/1-2
switchport trunk encapsulation dot1q
switch mode trunk
switchport trunk allowed vlan 100,101,102

A1
configure terminal
interface range Ethernet 1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
switchport trunk allowed vlan 100,101,102
end end
wr

b) Use *VLAN* 999 Como la *VLAN native*.

D1
confgure terminal
interface range Ethernet 2/0-3
switchport trunk native vlan 999
exit
interface range Ethernet 0/1-2
switchport trunk native vlan 999
exit

D2
configure terminal
interface range Ethernet 2/0-3
switchport trunk native vlan 999
exit
interface range Ethernet 1/1-2
switchport trunk native vlan 999

A1
confgure terminal
interface range Ethernet 0/1-2
switchport trunk native vlan 999
exit
interface range Ethernet 1/1-2

switchport trunk native vlan 999

c) Use *Rapid Spanning Tree* (RSPT).

Router R1

D1

enable
configure terminal //ingreso configuración global
spanning-tree mode raapid-pvst //configuración RSPT

D2

enable
configure terminal //ingreso configuración global
spanning-tree mode raapid-pvst //configuración RSPT

A1

enable
configure terminal //ingreso configuración *global spanning-tree mode raapid-pvst* //configuración RSPT

d) Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

Se configura D1 con spannin-tree las vlan 100 y 102 como raíz primaria y 101 como raíz secundaria, así mismo el D2 con las vlan 100, 102 como raíz secundaria y 101 como raíz primaria

Switch D1

configure terminal // configuración global
spanning-tree vlan 100 *root primary* // pone la vlan 100 como primaria
spanning-tree vlan 101 root secondary // pone la vlan 101 como secundaria
spanning-tree vlan 102 root primary // pone la vlan 102 como primaria

Switch D2

configure terminal // configuración global
spanning-tree vlan 100 root primary // pone la vlan 100 como secundaria
spanning-tree vlan 101 root secondary // pone la vlan 101 como primaria
spanning-tree vlan 102 root primary // pone la vlan 102 como secundaria

e) En todos los switches, cree *EtherChannels* LACP como se muestra en el diagrama de topología. Se configura *port channel* entre cada dispositivo

D1 a D2 – *Port channel* 12

D1

confi ter	//ingreso configuración globa
interface range e2/0-3	//selección de rango interfaz
CHANNEL-GROUP 12 mode active	//asignación *port channel*

D2

confi ter	//ingreso configuración global
interface range e2/0-3	//selección de rango interfaz
CHANNEL-GROUP 12 mode *active*	//asignación *port channel*

D1 a A1 – *Port channel* 1

D1

Configure terminal	//ingreso configuración global
interface range Ethernet 0/1-2	//selección de rango interfaz
CHANNEL-GROUP 1 *mode active*	//asignacion *port channel*

A1

Configure terminal	//ingreso configuración global
interface range Ethernet 0/1-2	//selección de rango interfaz
CHANNEL-GROUP 1 *mode active*	//asignación *port channel*

D2 a A1 – *Port channel* 2

D2

conf terminal	//ingreso configuración global
interface range e1/1-2	//selección de rango interfaz
CHANNEL-GROUP 2 *mode active*	//asignación *port channel*

A1

conf terminal	// ingreso configuración global
interface range e1/1-2	// selection de Rango interfaz
CHANNEL-GROUP 2 *mode active*	// asignación *port channel*

f) Tarea 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.

Acceso pc 1

configure terminal //acceso modo global
Interface e0/0 //selección interfaz
switchport mode access //configuración modo *access vlan* 100
switch access vlan 100

Acceso pc 2

configure terminal //acceso modo global
interface e0/0 //selección interfaz
switchport mode access //configuración modo *access vlan* 102
switch acces vlan 102

Acceso a pc3

configure terminal //acceso modo global
interfaz e1/3 //selección interfaz
switchport mode access //configuración modo *access vlan* 101
switch access vlan 101

Acceso a pc4

configure terminal //acceso modo global
interface e2/0 //selección interfaz
switchport mode access //configuración modo *access vlan* 101
switch access vlan 100

g) Tarea 2.7: Verifique los servicios DHCP IPv4

Ilustración 5 Verificación direccionamiento DHCP para el pc 2

```
PC2> ip dhcp
DORA IP 10.51.102.210/24 GW 10.51.102.254

PC2>
PC2>
PC2> ip dhcp
DORA IP 10.51.102.210/24 GW 10.51.102.254

PC2>
```

Fuente. Propia

Ilustración 6 Verificación direccionamiento DHCP para el pc 3

```
NAME   IP/MASK              GATEWAY           MAC                  DNS
PC3    10.51.101.112/24     51.0.101.254      00:50:79:66:68:02

PC3> ip dhcp
DORA IP 10.51.101.212/24 GW 51.0.101.254

PC3> ip dhcp
DORA IP 10.51.101.212/24 GW 10.51.101.254
```

Fuente. Propia

h) Tarea 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

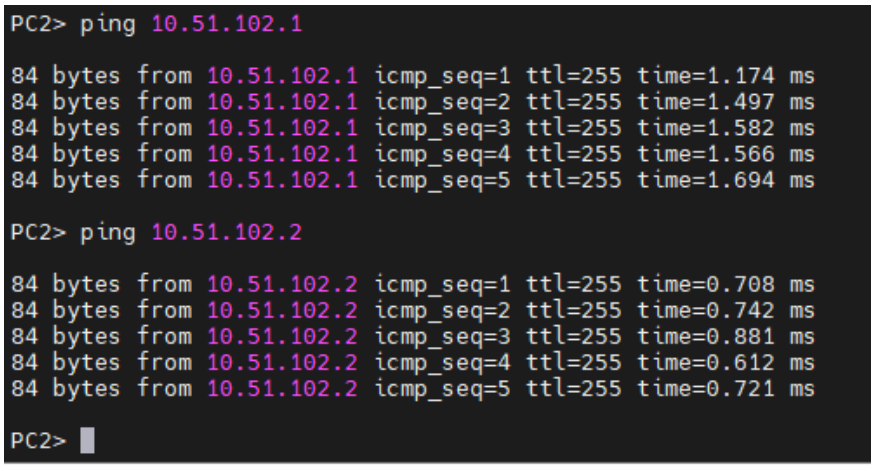
Ilustración 7 Verificación ping desde el pc1

```
PC1> ping 10.51.100.1

84 bytes from 10.51.100.1 icmp_seq=1 ttl=255 time=0.600 ms
84 bytes from 10.51.100.1 icmp_seq=2 ttl=255 time=0.981 ms
84 bytes from 10.51.100.1 icmp_seq=3 ttl=255 time=0.776 ms
84 bytes from 10.51.100.1 icmp_seq=4 ttl=255 time=1.243 ms
84 bytes from 10.51.100.1 icmp_seq=5 ttl=255 time=0.759 ms

PC1> ping 10.51.100.2

84 bytes from 10.51.100.2 icmp_seq=1 ttl=255 time=1.313 ms
84 bytes from 10.51.100.2 icmp_seq=2 ttl=255 time=1.582 ms
84 bytes from 10.51.100.2 icmp_seq=3 ttl=255 time=2.747 ms
84 bytes from 10.51.100.2 icmp_seq=4 ttl=255 time=2.025 ms
84 bytes from 10.51.100.2 icmp_seq=5 ttl=255 time=1.764 ms

PC1> ping 10.51.100.6

84 bytes from 10.51.100.6 icmp_seq=1 ttl=64 time=1.467 ms
84 bytes from 10.51.100.6 icmp_seq=2 ttl=64 time=1.756 ms
84 bytes from 10.51.100.6 icmp_seq=3 ttl=64 time=1.733 ms
84 bytes from 10.51.100.6 icmp_seq=4 ttl=64 time=2.161 ms
84 bytes from 10.51.100.6 icmp_seq=5 ttl=64 time=1.589 ms

PC1>
```

Fuente propia

PC2 debería hacer ping con éxito a:
D1: 10.0.102.1
D2: 10.0.102.2

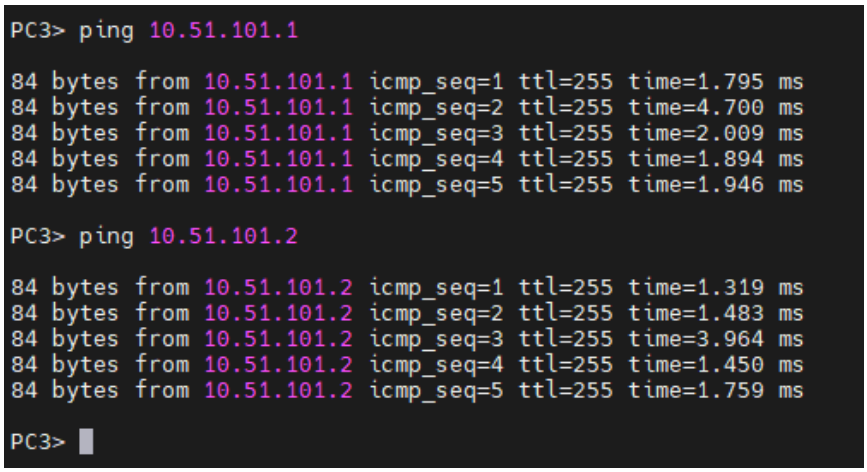
Ilustración 8 Verificación ping desde el pc2



Fuente propia.

PC3 debería hacer ping con éxito a:
D1: 10.0.101.1
D2: 10.0.101.2

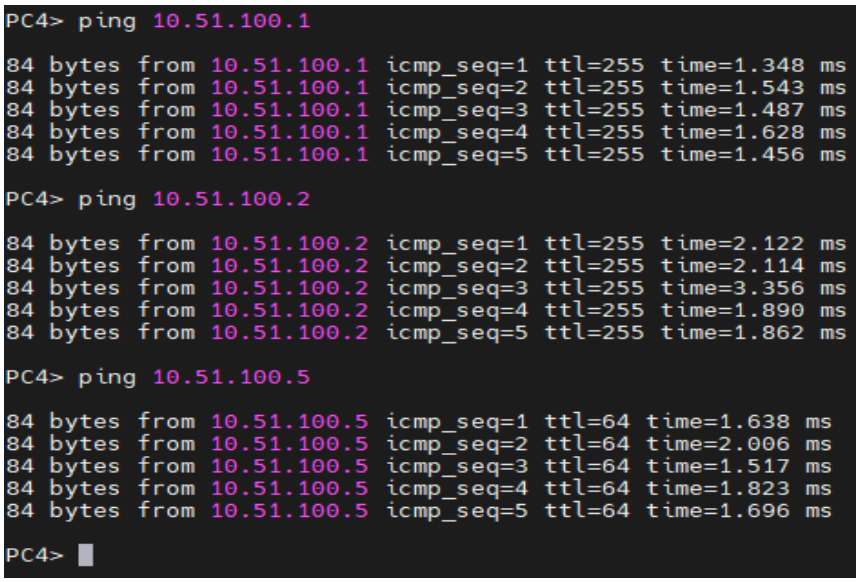
Ilustración 9 Verificación ping desde el pc3



Fuente propia

PC4 debería hacer ping con éxito a:
D1: 10.0.100.1
D2: 10.0.100.2
PC1: 10.0.100.5

Ilustración 10 Verificación ping desde el pc4



II.II ESCENARIO 2

II.II.I Configurar los protocolos de enrutamiento

En esta parte,se procede a configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los *pings* de IPv4 e IPv6 a la *interfaz Loopback* 0 desde D1 y D2 deberían ser exitosos.

Nota: Los *pings* desde los *hosts* no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

a) En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure *single-area* OSPFv2 en area 0.

Al Router **R1** le asignamos el ID 0.0.4.1

Configure terminal // configuración global
router ospf 4 // configuración OSPF *Process ID* 4
router-id 0.0.4.1 // asignación de ID

- Al Router **R3** le asignamos el ID 0.0.4.3

Configure terminal // configuración global
router ospf 4 // configuración OSPF *Process ID* 4
router-id 0.0.4.3 // asignación de ID

- Al switch **D1** le asignamos el ID 0.0.4.131

Configure terminal // configuración global
router ospf 4 // configuración OSPF *Process ID* 4
router-id 0.0.4.131 // asignación de ID

- Al switch **D2** le asignamos el ID: 0.0.4.132

Configure terminal // configuración global
router ospf 4 // configuración OSPF *Process ID* 4
router-id 0.0.4.132 // asignación de ID

✓ En R1, R3, D1, y D2, se anuncian todas las redes directamente conectadas y también las *VLANs* en Area 0.

- En R1, no se publica la red R1 que conecta con R2.

R1
network 10.51.10.0 0.0.0.255 area 0 // anuncio de redes R1 en area 0
network 10.51.13.0 0.0.0.255 area 0 // anuncio de redes R1 en area 0
passive-interface Ethernet 1/2 // Evita actualizaciones innecesarias

R3
network 10.51.11.0 0.0.0.255 area 0 // anuncio de la red R3-D2 en área 0
network 10.51.13.0 0.0.0.255 area 0 // anuncio de la red R3-R1 en área 0
passive-interface Ethenet 1/0 // Evita actualizaciones innecesarias

D1
do show ip route connected
network 10.51.10.0 0.0.0.255 area 0 // anuncio de las redes de D1 en área 0
network 10.51.100.0 0.0.0.255 area 0
network 10.51.101.0 0.0.0.255 area 0
network 10.51.102.0 0.0.0.255 area 0

D2
network 10.51.11.0 0.0.0.255 area 0 // anuncio de redes D2 en area 0
network 10.51.100.0 0.0.0.255 area 0
network 10.51.101.0 0.0.0.255 area 0
network 10.51.102.0 0.0.0.255 area 0

- En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Configure terminal	// entrar a la configuración global
ipv6 router ospf 4	// Ingresa al router ospf 6.
router-id 0.0.4.1	// Asignación id 0.0.4.1.
default-information originate	// asignación ruta predeterminada

✓ Se deshabilitan las publicaciones OSPFv2 en D1 y D2 exceptuando en la interfaz e1/2 y 1/0 respectivamente.

- D1: todas las interfaces excepto Ethernet 1/2

passive-interface Ethernet 0/0 //deshabilitar publicaciones OSPFv2 en D1 para la interfaz
passive-interface Ethernet 0/1
passive-interface Ethernet 0/2
passive-interface Ethernet 2/0
passive-interface Ethernet 2/1
passive-interface Ethernet 2/2
passive-interface Ethernet 2/3

- D2: todas las interfaces excepto Ethernet 1/0

Passive-interface Ethernet 0/0
passive-interface Ethernet 1/1
passive-interface Ethernet 1/2
passive-interface Ethernet 2/0
passive-interface Ethernet 2/1
passive-interface Ethernet 2/2
passive-interface Ethernet 2/3

b) En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure classic *single-area* OSPFv3 en area 0.

✓ Se configura OSPFv3 usando OSPF *Process* ID 6 y se asignan los siguientes *router*-IDs.

- **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, se debe anunciar todas las redes directamente conectadas y también las *VLANs* en Area 0.

- En R1, no publique la red R1 que se conecta con R2.
- Se propaga una ruta por defecto provista por BGP.

R1: 0.0.6.1

```
ipv6 router ospf 6                  // Ingresa al router ospf 6.
router-id 0.0.6.1                   // Asigna el id 0.0.6.1
interface Ethernet 1/1              // ingreso a interfaz
ipv6 ospf 6 area 0                  // ingreso ipv6 ospf 6 area 0
exit                                // salida
interface Ethernet 1/2              // ingreso interfaz G1/0
Ripv6 ospf 6 area 0                 // ingreso ipv6 ospf 6 area 0
exit
```

R3: 0.0.6.3

```
ipv6 router ospf 6                  // ingreso ipv6 ospf 6 area 0
router-id 0.0.6.3                   // asignación id 0.0.6.3
interface Ethernet 1/1              // ingreso interfaz s6/0
ipv6 ospf 6 area 0                  // habilitar OSPFv3 en interfaz
exit                                // salida
interface Ethernet 1/0              // ingreso interfaz G1/0
ipv6 ospf 6 area 0                  // habilitar OSPFv3 en interfaz
```

D1: 0.0.6.131

```
ipv6 router ospf 6                  // Habilita OSPFv3
router-id 0.0.6.131                 // asignación id 0.0.6.131
interface Ethernet 1/2              // ingreso interfaz
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface vlan 100                  // ingreso interfaz vlan 100
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface vlan 101                  // ingreso interfaz vlan 101
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface vlan 102                  // ingreso interfaz vlan 102
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface e3/3                      // ingreso interfaz e3/3
```

D2: 0.0.6.132

```
ipv6 router ospf 6                  // Habilita OSPFv3
router-id 0.0.6.132                 // asignación id 0.0.6.132
interface Ethernet 1/0              // ingreso interfaz e0/0
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface vlan 100                  // ingreso interfaz vlan 100
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface vlan 101                  // ingreso interfaz vlan 101
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
interface vlan 102                  // ingreso interfaz vlan 102
ipv6 ospf 6 area 0                  // Habilita OSPFv3 en interfaz
```

- ✓ Se deshabilitan publicaciones de OSPFv3 en D1 y D2 excepto en la interfaz Ethernet 1/2 y *Ethernet* 1/0 respectivamente.

  - D1: todas las interfaces excepto *Ethernet* 1/2.

```
ipv6 router ospf 6                    //deshabilita publicaciones OSPFv3 en D1
passive-interface vlan 100
passive-interface vlan 101
passive-interface vlan 102
```

  - D2: todas las interfaces excepto Ethernet 1/0

```
ipv6 router ospf 6                    // deshabilita publicaciones  OSPFv3 enD2
passive-interface vlan 100
passive-interface vlan 101
passive-interface vlan 102
```

c) Configuración de MP-BGP En el Router R2, en la "Red ISP"

- ✓ Se configuran dos rutas estáticas predeterminadas a través de la interfaz *Loopback* 0, para IPV4 e IPV6.
- ✓ Se configura R2 en BGP ASN 500 y se usa el *router*-id 2.2.2.2.
- ✓ Se configura y habilita una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

Router R2

```
Configure terminal                                  // ingresamos configuración global.
ip route 0.0.0.0 0.0.0.0 loopback 0                 // ruta estatica ipv4 con loopback 0
ipv6 route ::/0 loopback 0                          // ruta estatica ipv6 con loopback 0
router bgp 500                                      // Se Crea proceso BGP dentro del router
bgp router-id 2.2.2.2                               // identificador de R2 en BGP
neighbor 209.165.200.225 remote-as 300              // establecer vecinos de conexión ASN300 ipv4
neighbor 2001:db8:200::1 remote-as 300              // establecer vecinos de conexión ASN300 ipv6
address-family ipv4                                 // configuración Familia ipv4
209.165.200.225 activate                            // relación router vecino
no neighbor 2001:db8:200::1 activate                // Deshabilite la relación de vecino IPv6 con R1
network 2.2.2.2 mask 255.255.255.255                // anuncio de red por BGP
network 0.0.0.0                                     // ruta estática
exit-address-family                                 // salir de Familia ipv4
address-family ipv6                                 // entrar en configuración Familia IPV6
no neighbor 209.165.200.225 activate                // Deshabilite la relación de vecino ipv4 con R1
neighbor 2001:db8:200::1 activate                   // relación router vecino
network 2001:db8:2222::/128                         // anuncie la red . 2001:db8:2222::/128
network ::/0                                        // se configura el enrutamiento por defecto
exit-address-family                                 // salir de la configuración familia ipv6
```

d) En R1 en la “Red ISP”, configure MP-BGP

✓ Se configuran dos rutas resumen estáticas a la interfaz *Null* 0:

- Una ruta resumen IPv4 para 10.51.0.0/8.

```
Cofigure terminal                       // configuración global
Ip route 10.51.0.0 255.0.0.0 null0      // configuración ruta resumen IPV4
```

- Una ruta resumen IPv6 para 2001:db8:100::/48.

```
Configure terminal                      // configuración global
ipv6 route 2001:db8:100::/48 null0      // configuración ruta resumen IPV6
```

✓ Configure R1 en BGP ASN 300 y use el *router-id* 1.1.1.1
✓ Configuración de una relación vecino IPv4 e IPv6 con R2 en ASN 500

- En IPv4 *address family*, se deshabilitan la relación de vecino ipv6, habilite las relaciones de vecino en ipv4 y anuncie la red 10.51.0.0/8.

```
Configure terminal                      // configuración global
Rouer bgp 300                           // configuración de router BGP 300
bgp router-id 1.1.1.1                   // identificador de R1 en BGP 300
neighbor 209.165.200.226 remote-as 500  // establecer vecinos de conexión ASN500 ipv4
neighbor 2001:db8:200::2 remote-as 500  // establecer vecinos de conexión ASN500 ipv6
address-family ipv4                     // configuración de familia direcciones IPV4 R1
neighbor 209.165.200.226 activate       // Habilita relación vecino IPv4.
no neighbor 2001:db8:200::2 activate    // Deshabilita relación vecino IPv6.
network 10.51.0.0 mask 255.0.0.0        // Anuncia la red 10.51.0.0/8
network 0.0.0.0                         // se configura el enrutamiento por defecto
exit-address-family                     // salir de configuración de familia ipv4
```

- En IPv6 *address family*, deshabilite la relación de vecino ipv4, habilite las relaciones de vecino en ipv4 y anuncie la red 10.51.0.0/8.

Estando en la configuración de router BGP 300 se procede a configurar *address-family ipv6*

```
address-family ipv6                     // configura familia direcciones IPV6
no neighbor 209.165.200.226 activate    // Deshabilita relación vecina IPv4
neighbor 2001:db8:200::2 activate       // habilita relación vecino IPv6.
network 2001:db8:100::/48               // Anuncie la red 2001:db8:100::/48
network ::/0                            // se configura el enrutamiento por defecto
exit-address-family                     // salir de configuración de familia ipv6
```

II.II.II Configuración de la Redundancia del Primer Salto (*First Hop Redundancy)*

En esta parte, se configura HSRP versión 2 para proveer redundancia de primer salto en los hosts en la “Red de la Compañía”.

a) En D1, se crea IP SLAs que comprueben la accesibilidad de la interfaz R1 G1/0.

Se crea en en el *swtich* D1 IP SLAs , usando el número 4 para IPV4 y el número 6 para IPV6, estas IP SLAs comprobarán la disponibilidad de la interfaz R1 *Ethernet* 1/2 cada 5 segundos y se programa la SLA para una implementación inmediata sin tiempo de finalización.

- Use la SLA número 4 para IPv4.

***Switch* D1**

```
Configure terminal                    // configuración global
ip sla 4                              // definir # de IP SLA  IPV4
icmp-echo 10.51.10.1                  // tipo mensaje, IP, origen
frequency 5                           // frecuencia de monitoreo
exit                                  // salida ip-sla
```

- Use la SLA número 6 para IPv6.

```
Configure terminal                    // configuración global
ip sla 6                              // definir # de IP SLA  IPV6
icmp-echo 2001:db8:100:1010::1        // se configura el mesaje de control ipv6
frequency 5                           // se configura la frecuencia de monitoreo
exit                                  // salida ip-sla
ip sla schedule 4 life forever start-time now   // se inicia o activa el monitoreo ipv4
ip sla schedule 6 life forever start-time now   // se inicia o activa el monitoreo ipv6
```

Se crea una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6, los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de *down* y a *up* después de 10 segundos o de *up* a *down* después de 15 segundos.

- Se usa el número de rastreo 4 para la IP SLA 4.

```
track 4 ip sla 4                      //definicion # rastreo ip sla 4
delay down 15 up 10 //down 15” y up 10”
exit
```

- Se usa el número de rastreo 6 para la IP SLA 6.

```
track 6 ip sla 6                    // definición # rastreo ip sla 4
delay down 15 up 10                 // down 15" y up 10"
exit                                // salida
```

b) En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.

- ✓ Se crean IP SLAs en D2 usando la SLA número 4 para IPv4 y la SLA número 6 para IPv6, las cuales comprobarán la disponibilidad de la interfaz de R3 *Ethernet* 1/0 cada 5 segundos, así mismo se programa la SLA para una implementación inmediata sin tiempo de finalización

```
ip sla 4                                    // definir # de IP SLA  IPV4
icmp-echo 10.0.11.1                         // tipo mensaje, IP, origen mensaje
frequency 5                                 // frecuencia de monitoreo
exit                                        // salida
ip sla 6                                    // definir # de IP SLA  IPV4
icmp-echo 2001:db8:100:1011::1              // mensaje, IP, origen IPV6
frequency 5                                 // frecuencia de monitoreo
exit                                        // salida
ip sla schedule 4 life forever start-time now   // Habilita IP SLA ahora y siempre
ip sla schedule 6 life forever start-time now   // Habilita IP SLA ahora y siempre
```

- ✓ Se crea una IP SLA objeto para la IP SLA 4 y una IP SLA 6, usando el número de rastreo 4 para la IP SLA 4 y el número de rastreo 6 para la SLA 6, estos 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.

```
track 4 ip sla 4                    // Crea id objeto 4 y lo asocia con IP SLA4
delay down 15 up 10                 // retraso de tiempo para  down y up
exit                                // salida
track 6 ip sla 6                    // Crea id objeto  6 y lo socia con IP SLA6
delay down 15 up 10                 // retraso de tiempo para down y up
exit                                // salida
```

c) En D1 configure HSRPv2.

- ✓ Se cambia la prioridad a 150 de D1 siendo el *router* primario para las *VLAN*s 100 y 102 Se configure HSRP version 2, y IPv4 HSRP grupo 104 para la VLAN 100

```
Configure terminal                  // configuración global
interface vlan 100                  // interfaz vlan 100
standby version 2                   // version 2
```

standby 104 ip 10.0.100.254 // Asigne la dirección IP virtual
standby 104 priority 150 // prioridad del grupo en 150
standby 104 preempt // Habilite la preferencia
standby 104 track 4 decrement 60 // Rastree el objeto 4 y decremente en 60
exit

- Se configure IPv4 HSRP grupo 114 para la VLAN 101

interface vlan 101 // interfaz vlan 101
standby version 2 // version 2
standby 114 ip 10.0.101.254 // Asigne la dirección IP virtual
standby 114 preempt // Habilita la preferencia
standby 114 track 4 decrement 60 // Rastree el objeto 4 y decremente 60
exit // salida

- Se configure IPv4 HSRP grupo 124 para la VLAN 102

interface vlan 102 // interfaz vlan 102
standby version 2 // version 2
standby 124 ip 10.0.102.254 // Asigne la dirección IP virtual
standby 124 priority 150 // prioridad del grupo en 150
standby 104 preempt // Habilite la preferencia
standby 104 track 4 decrement 60 // Rastree el objeto 4 y decrementa 60
exit

- Se configure IPv6 HSRP grupo 106 para la VLAN 100

interface vlan 100 // interfaz vlan 100
standby version 2 // version 2
standby 106 ipv6 autoconfig // Asigne la dirección IP virtual
standby 106 priority 150 // prioridad del grupo en 150
standby 106 preempt // Habilite la preferencia
standby 106 track 4 decrement 60 //Rastree el objeto 4 y decrementa 60
exit

- Configure IPv6 HSRP grupo 116 para la VLAN 101

interface vlan 101 // interfaz vlan 101
standby version 2 // version 2
standby 116 ipv6 autoconfig // Asigne la dirección IP virtual
standby 116 preempt // Habilita la preferencia
standby 116 track 4 decrement 60 // Rastree el objeto 4 y decrementa 60
exit

- Configure IPv6 HSRP grupo 126 para la VLAN 102

interface vlan 102 // interfaz vlan 102
standby 126 ipv6 autoconfig // Asigne la dirección IP virtual
standby 126 priority 150 // prioridad del grupo en 150
standby 126 preempt // Habilite la preferencia
standby 126 track 4 decrement 60 // Rastree el objeto 4 ydecremeta 60
exit

CAPÍTULO III
CONCLUSIONES

Se logra el diseño y configuración de la red cumpliendo con los parámetros exigidos, implementando protocolos como *Etherchannel*, OSPFv2, OSPFv3, BGP, entre otros, los cuales permitieron lograr una red convergente, operativa segura.

La implementación de protocolos de enrutamiento como OSPF permite que la red sea más operativa y eficiente, pues este protocolo ayuda a calcular las rutas a gran velocidad determinado su métrica, ofreciendo rendimiento a las redes, dinamismo en su forma de actualizar las tablas de enrutamiento con los siguientes saltos.

Las SLAs es una tecnología fundamental que se debe configurar en las redes que se administran, ya que esta permite que se pueda hacer un seguimiento del comportamiento de la red, realizar métricas y tomar decisiones que permitan mitigar cualquier impacto negativo.

En el desarrollo del proyecto se presentaron errores de configuración, así como de diseño los cuales pudieron ser superados a satisfacción con la asesoría de los docentes y la documentación entregada por parte de los mismos, los que permitió afianzar los conceptos de redes, aprendidos durante el evento académico.

El software GNS3 utilizado para la simulación de la red empresarial cumplió con las expectativas de funcionamiento, pues el entorno de trabajo es casi real, lo cual permitió desarrollar competencias en el diseño y configuración de dispositivos activos de red

BIBLIOGRAFÍA

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

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

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

universidad complutense. (s.f.). universidad complutense. Recuperado el 27 de 11 de 2021, de https://www.ucm.es/pimcd2014-free-software/gns3

ccna-learner.com. (27 de 12 de 2020). *ccna-learner.com*. Recuperado el 26 de 11 de 2021, de https://www.ccna-learner.com/2020/12/27/radius-configuration-on-cisco-routerlab-radius-configure-and-improve-your-ski/

CAPÍTULO IV
ANEXOS 1

Ilustración 11. Show ip sla summary Switch D1

```
D1#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
---------------------------------------------------------------------
*4           icmp-echo   10.51.10.1        RTT=4       OK          4 seconds ago



*6           icmp-echo   2001:DB8:100:1010 RTT=3       OK          4 seconds ago
                         ::1
```

Fuente. Propia

Ilustración 12Show ip SLA summary Switch D2.

```
D2#Show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
---------------------------------------------------------------------
*4           icmp-echo   10.51.11.1        RTT=5       OK          3 seconds ago



*6           icmp-echo   2001:DB8:100:1011 RTT=4       OK          3 seconds ago
                         ::1
```

Fuente. Propia

Ilustración 13. Show standby brief D1

```
D1#show standby brief
D1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       104  150 P Active  local           unknown         10.51.100.254
Vl100       106  150 P Active  local           unknown         FE80::5:73FF:FEA0:6A
Vl101       114  100 P Active  local           unknown         10.51.101.254
Vl101       116  100 P Active  local           unknown         FE80::5:73FF:FEA0:74
Vl102       124  150   Active  local           unknown         10.51.102.254
Vl102       126  150 P Active  local           unknown         FE80::5:73FF:FEA0:7E
D1#
```

Fuente. Propia