

**DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

**JORGE CAMILO AREVALO RAMOS**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
VALLEDUPAR  
2022**

**DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

**JORGE CAMILO AREVALO RAMOS**

**Diplomado de opción de grado presentado para optar el título de INGENIERO  
ELECTRONICO**

**DIRECTOR:**

**Ing. JUAN ESTEBAN TAPIAS**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
VALLEDUPAR  
2022**

## NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

VALLEDUPAR, 30 de Septiembre del 2022

## **AGRADECIMIENTOS**

A DIOS primeramente autor de todas las cosas que me ha permitido llegar donde estoy sin él no somos nada Gracias Dios por permitirme llegar hasta donde tú me tienes ahora.

A mis queridos padres que con su amor y sacrificio me heredaron la mejor educación y me supieron guiar por el camino correcto, a mi familia que día a día nos apoyan y siempre están junto a nosotros, y a nuestros amigos por su amistad y empuje.

A la Universidad Nacional Abierta y a Distancia y su cuerpo de docentes, por todos los conocimientos adquiridos a lo largo de esta hermosa carrera.

## Tabla de contenido

AGRADECIMIENTOS .....	4
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	8
RESUMEN .....	10
ABSTRACT .....	11
INTRODUCCION .....	12
ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES .....	13
ESCENARIO 1 .....	13
1.1 Parte 1: Construcción de la red y configuración básica de dispositivos y el direccionamiento de la interfaz .....	14
1.1.1 Paso 1: Cableado de la topología .....	14
1.1.2 Paso 2: Configuración de los ajustes básicos para cada dispositivo .	15
1.2 Parte 2: Configurar la red de capa 2 y la compatibilidad con el host .....	23
ESCENARIO 2 .....	34
1.3 Part 1: Configure Routing Protocols .....	34
1.4 Part 2: Configure First Hop Redundancy .....	46
CONCLUSIONES .....	54
BIBLIOGRAFIA .....	55

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento Escenario 1 .....	13
Tabla 2. Tareas de configuración - Parte 2 .....	23
Tabla 3. Tareas de configuración Escenario 2 - Parte 1 .....	34
Tabla 4. Tareas de configuración Escenario 2 - Parte 2 .....	46

## LISTA DE FIGURAS

Figura 1. Conexión de la topología del Escenario 1 en GNS3 .....	15
Figura 2. Configuración guardada en los dispositivos .....	21
Figura 3. Configuración IP del PC1 y PC4 .....	22
Figura 4. Verificación de la IP de PC1 y PC4 .....	22
Figura 5. Verificación de las interfaces troncales y la VLAN nativa en D1 y D2 .....	27
Figura 6. Verificación de la creación de los LACP EtherChannel .....	28
Figura 7. Verificación del RSTP en D1 y D2 .....	29
Figura 8. Configuración adecuada de la VLAN en los 3 switches .....	30
Figura 9. PC2 y PC3 recibiendo direccionamiento a través de DHCP .....	30
Figura 10. Ping desde PC1 hacia D1, D2 y PC4 .....	31
Figura 11. Ping desde PC2 hacia D1 y D2 .....	31
Figura 12. Ping desde PC3 hacia D1 y D2 .....	32
Figura 13. Ping desde PC4 hacia D1, D2 y PC1 .....	32
Figura 14. Verificación de la configuración OSPFv2 en R1, R3, D1 y D2 .....	40
Figura 15. Verificación de la configuración OSPFv3 en R1, R3, D1 y D2 .....	41
Figura 16. Verificación del MP-BGP en R2 y las rutas estáticas predeterminadas ....	42
Figura 17. Verificación del MP-BGP en R1 y las rutas estáticas predeterminadas ....	43
Figura 18. Tabla de enrutamiento en R1 .....	43
Figura 19. Verificación que OSPFv3 para IPv6 funciona correctamente en R1 .....	44
Figura 20. Verificación que OSPF para IPv4 funciona correctamente en R3 .....	44
Figura 21. Verificación que OSPFv3 para IPv6 funciona correctamente en R3 .....	45
Figura 22. Verificación de la configuración IP SLA en D1 y D2 .....	51
Figura 23. D1 como enrutador principal para las VLAN 100 y 102 .....	52
Figura 24. D2 como enrutador principal para la VLAN 101 .....	53

## GLOSARIO

**DHCP:** Es un protocolo de configuración dinámica de host, el cual permite configurar los parámetros de TCP/IP como la asignación automática de direcciones IP, gateways predeterminadas, así como otros parámetros de red que necesiten los clientes. El sistema DHCP envía automáticamente todos los parámetros para que los clientes se comuniquen sin problema dentro de la red.

**SLAAC:** es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP.

**HSRP:** es un protocolo exclusivo de Cisco diseñado para permitir la conmutación por falla transparente de un dispositivo IPv4 de primer salto. HSRP proporciona una alta disponibilidad de red, ya que proporciona redundancia de routing de primer salto para los hosts IPv4 en las redes configuradas con una dirección IPv4 de gateway predeterminado. HSRP utiliza una IP y MAC virtual, que es la misma para todos los routers de un mismo grupo.

**RSTP:** es el protocolo que previene **loops** en una red de switches, es una evolución del árbol de expansión que proporciona una convergencia más rápida que la implementación original de 802.1D. Esta versión resuelve varios problemas de convergencia, pero dado que aún proporciona una única instancia de STP, no resuelve los problemas de flujo de tráfico poco óptimo.

**LACP EtherChannel:** Los EtherChannels son una opción de configuración que permite agrupar lógicamente múltiples interfaces físicas para proporcionar redundancia y rendimiento de enlace adicionales. LACP es un protocolo estándar que los dispositivos de red pueden utilizar para negociar un enlace Etherchannel.



LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al peer.

**IEEE 802.1Q:** El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking) o enlace troncal. Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales.

**OSPF:** es un protocolo de enrutamiento abierto del tipo Estado de Enlace (*Link State*). Los protocolos de enrutamiento *Link State*, a diferencia de los protocolos *Distance Vector*, no intercambian tablas de enrutamiento en intervalos específicos de tiempo, sino que las rutas son actualizadas cuando hay un cambio en la topología de la red.

**MP-BGP:** es un BGP extendido que permite que BGP lleve información de ruteo para múltiples protocolos de capa de red IPv6, VPNv4 y otros. MP-BGP le permite tener una topología de ruteo unicast diferente de una topología de ruteo multicast, que ayuda a controlar la red y los recursos.

## RESUMEN

El presente proyecto de grado se fundamenta en el desarrollo de 2 escenarios de configuración de redes VLAN y la implementación de los protocolos MP-BGP, HSRP, OSPF y RSTP donde se aplican los conocimientos adquiridos a lo largo del curso. Para el desarrollo del ESCENARIO 1 se implementan las configuraciones básicas en cada dispositivo de la topología, como las interfaces y direcciones IPv4 e IPv6, la configuración de las VLANs y la distribución de direcciones IP pertenecientes a cada switch, los nombres de host, etc. También se realizará la configuración de interfaces troncales en todos los conmutadores, usando la VLAN 999 como VLAN nativa. De igual manera se habilitará el protocolo Rapid Spanning-Tree configurando los puentes raíz apropiados, al igual que la creación de LACP EtherChannels según la información del diagrama de topología. Para el desarrollo del ESCENARIO 2, se configurará los protocolos de enrutamiento IPv4 e IPv6, haciendo uso del protocolo OSPFv2 y OSPFv3 de área única. De igual forma, se anunciarán todas las redes VLAN conectadas directamente en el Área 0 y pertenecientes a cada dispositivo. Por otro lado, se configurarán dos rutas estáticas predeterminadas a través de la interfaz Loopback 0 en el Router R2, al igual que la creación de SLA de IP en D1 tanto para IPv4 como para IPv6, haciendo el mismo procedimiento en D2, teniendo en cuenta que se debe configurar el protocolo HSRPv2 en D1 y D2, donde inicialmente D1 será el enrutador principal para las VLAN 100 y 102, luego, D2 será configurado como el enrutador principal para la VLAN 101.

**Palabras Clave:** Enrutamiento, Redundancia, Protocolos, Direccionamiento, CCNP, Interfaces, Configuración.

## ABSTRACT

This degree project is based on the development of 2 VLAN network configuration scenarios and the implementation of the MP-BGP, HSRP, OSPF and RSTP protocols where the knowledge acquired throughout the course is applied. For the development of SCENARIO 1, the basic configurations are implemented in each device of the topology, such as the interfaces and IPv4 and IPv6 addresses, the configuration of the VLANs and the distribution of IP addresses belonging to each switch, the host names, etc. Trunk interfaces will also be configured on all switches, using VLAN 999 as the native VLAN. In the same way, the Rapid Spanning-Tree protocol will be enabled by configuring the appropriate root bridges, as well as the creation of LACP EtherChannels according to the information in the topology diagram. For the development of SCENARIO 2, the IPv4 and IPv6 routing protocols will be configured, making use of the OPSFv2 and OSPFv3 single-area protocols. In the same way, all the VLAN networks directly connected in Area 0 and belonging to each device will be announced. On the other hand, two default static routes will be configured through the Loopback 0 interface on Router R2, as well as the creation of IP SLAs in D1 for both IPv4 and IPv6, doing the same procedure in D2, taking into account that the HSRPv2 protocol should be configured on D1 and D2, where initially D1 will be the primary router for VLANs 100 and 102, then D2 will be configured as the primary router for VLAN 101.

**Keywords:** Routing, Redundancy, Protocols, Addressing, CCNP, Interfaces, Configuration.

## INTRODUCCION

El desarrollo del diplomado de profundización CISCO CCNP tiene como objetivo fortalecer la importancia de establecer niveles de seguridad básicos, mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de red, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación mejorados tales como: VLAN, Protocolo de enlace troncal de VLAN (VTP), Protocolo rápido de árbol de expansión (Rapid Spanning Tree Protocol - RSTP), Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP) y encapsulamiento por 802.1q para mejorar los flujos de tráfico de datos, seguridad, redundancia y rendimiento de LANs de campus o WANs basadas en routers y switches, así como acceso remoto a redes.

En el desarrollo del ESCENARIO 1, se implementan las configuraciones básicas en cada dispositivo de la topología, como las interfaces y direcciones IPv4 e IPv6 asociadas a cada uno. De igual manera se realiza la configuración de interfaces troncales en todos los conmutadores, teniendo en cuenta que se debe usar la VLAN 999 como VLAN nativa. Por otro lado, se realizara la habilitación del protocolo Rapid Spanning-Tree (RSTP), donde se realiza la configuración del puente raíz apropiado en cada conmutador, teniendo en cuenta que los switches D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz. Como parte final, se verifica la conectividad de la red LAN local a través de ping entre los dispositivos.

Para el desarrollo del ESCENARIO 2, se realiza la configuración de protocolos de enrutamiento IPv4 e IPv6 y redundancia del primer salto, teniendo en cuenta que este último proporciona la capacidad que tiene una red para recuperarse dinámicamente de la falla de un dispositivo que funciona como gateway predeterminado. En los routers R1 y R3, y en los switches D1 y D2 se realiza la configuración del protocolo OSPFv2 y OSPFv3 de área única. El enrutamiento OSPF necesita un proceso ID y un ID de área, los cuales son suministrados por la guía práctica, además, se anuncian todas las redes VLAN conectadas directamente en el Área 0.

# ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

## ESCENARIO 1

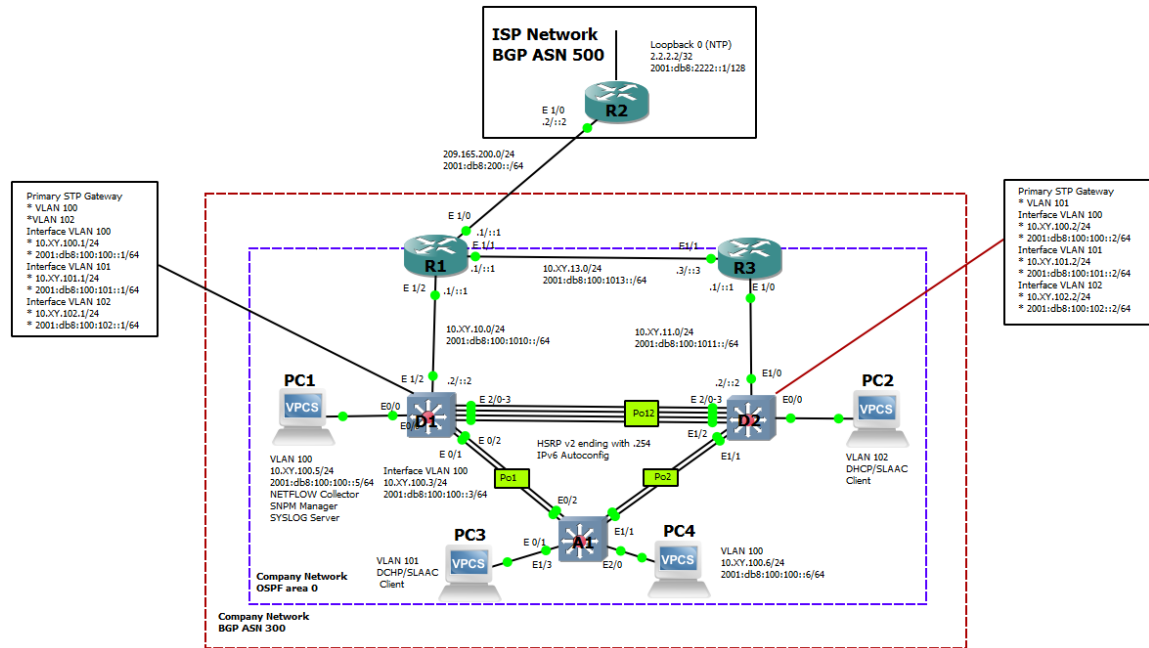


Tabla de direccionamiento:

**Tabla 1.** Tabla de direccionamiento Escenario 1

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.XY.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10.XY.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.XY.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.XY.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10.XY.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.XY.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.XY.101.1/24	2001:db8:100:101::1/64	fe80::d1:3

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
	VLAN 102	10.XY.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.XY.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.XY.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.XY.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.XY.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.XY.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.XY.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

## 1.1 Parte 1: Construcción de la red y configuración básica de dispositivos y el direccionamiento de la interfaz

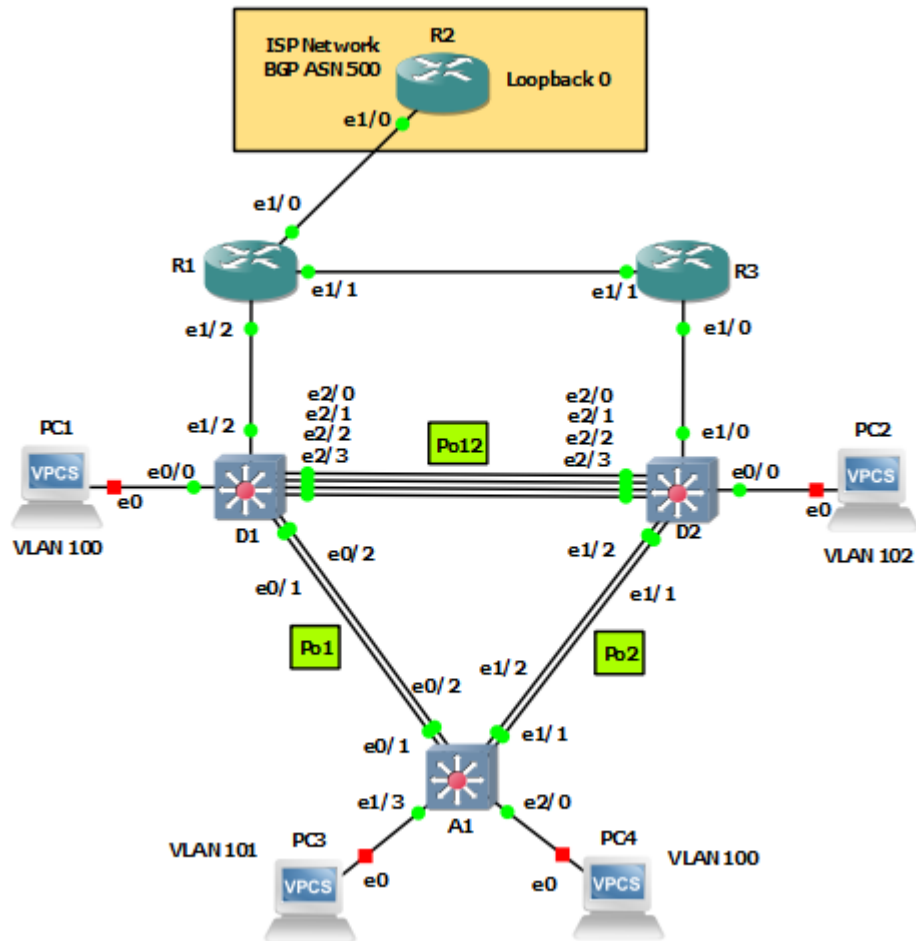
En la Parte 1, configurará la topología de la red y configurará los ajustes básicos y el direccionamiento de la interfaz.

### 1.1.1 Paso 1: Cableado de la topología

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

Se procede a realizar las respectivas conexiones entre los routers, los switches, los PCs y sus interfaces en el simulador GNS3, como se ilustra en la figura 1.

Figura 1. Conexión de la topología del Escenario 1 en GNS3



Fuente: Propia

### 1.1.2 Paso 2: Configuración de los ajustes básicos para cada dispositivo

- a. Ingrese al modo de configuración global y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.
- b. Guarde la configuración en ejecución en **startup-config** en todos los dispositivos.

En primer lugar, se aplicarán las configuraciones básicas de cada dispositivo tales como: nombre del host, las interfaces Ethernet y Loopback asociada a cada router y switch, la configuración de las direcciones IPv4 e IPv6, y posteriormente se procede a guardar la configuración de los dispositivos:

```
R1#configure terminal
R1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment#
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface e1/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface e1/2
R1(config-if)#ip address 10.07.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface e1/1
R1(config-if)#ip address 10.07.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#copy running-config startup-config
```

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



```
R2(config-if)# ipv6 address 2001:db8:2222::1/128
R2(config-if)# no shutdown
R2(config-if)#exit
R2(config)# exit
R2# copy running-config startup-config
```

```
R3#configure terminal
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment#
R3(config)# line con 0
R3(config-line)# exec-timeout 0 0
R3(config-line)# logging synchronous
R3(config-line)#exit
R3(config)# interface e1/0
R3(config-if)# ip address 10.07.11.1 255.255.255.0
R3(config-if)# ipv6 address fe80::3:2 link-local
R3(config-if)# ipv6 address 2001:db8:100:1011::1/64
R3(config-if)# no shutdown
R3(config-if)#exit
R3(config)# interface e1/1
R3(config-if)# ip address 10.07.13.3 255.255.255.0
R3(config-if)# ipv6 address fe80::3:3 link-local
R3(config-if)# ipv6 address 2001:db8:100:1010::2/64
R3(config-if)# no shutdown
R3(config-if)#exit
R3(config)# exit
R3# copy running-config startup-config
```

```
D1#configure terminal
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment#
D1(config)# line con 0
D1(config-line)# exec-timeout 0 0
D1(config-line)# logging synchronous
D1(config-line)#exit
D1(config)# vlan 100
D1(config-vlan)# name Management
D1(config-vlan)# exit
D1(config)# vlan 101
D1(config-vlan)# name UserGroupA
D1(config-vlan)#exit
D1(config)# vlan 102
```

```

D1(config-vlan)# name UserGroupB
D1(config-vlan)# exit
D1(config)# vlan 999
D1(config-vlan)# name NATIVE
D1(config-vlan)#exit
D1(config)# interface e1/2
D1(config-if)# no switchport
D1(config-if)# ip address 10.07.10.2 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:1 link-local
D1(config-if)# ipv6 address 2001:db8:100:1010::2/64
D1(config-if)# no shutdown
D1(config-if)#exit
D1(config)# interface vlan 100
D1(config-if)# ip address 10.07.100.1 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:2 link-local
D1(config-if)# ipv6 address 2001:db8:100:100::1/64
D1(config-if)# no shutdown
D1(config-if)#exit
D1(config)# interface vlan 101
D1(config-if)# ip address 10.07.101.1 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:3 link-local
D1(config-if)# ipv6 address 2001:db8:100:101::1/64
D1(config-if)# no shutdown
D1(config-if)#exit
D1(config)# interface vlan 102
D1(config-if)# ip address 10.07.102.1 255.255.255.0
D1(config-if)# ipv6 address fe80::d1:4 link-local
D1(config-if)# ipv6 address 2001:db8:100:102::1/64
D1(config-if)# no shutdown
D1(config-if)#exit
D1(config)# ip dhcp excluded-address 10.07.101.1 10.07.101.109
D1(config)# ip dhcp excluded-address 10.07.101.141 10.07.101.254
D1(config)# ip dhcp excluded-address 10.07.102.1 10.07.102.109
D1(config)# ip dhcp excluded-address 10.07.102.141 10.07.102.254
D1(config)# ip dhcp pool VLAN-101
D1(dhcp-config)# network 10.07.101.0 255.255.255.0
D1(dhcp-config)# default-router 10.07.101.254
D1(dhcp-config)# exit
D1(config)# ip dhcp pool VLAN-102
D1(dhcp-config)# network 10.07.102.0 255.255.255.0
D1(dhcp-config)# default-router 10.07.102.254
D1(dhcp-config)# exit
D1(config)# interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
D1(config-if-range)# shutdown
D1(config-if-range)# exit
D1(config)# exit
D1# copy running-config startup-config

```

```
D2#configure terminal
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment#
D2(config)# line con 0
D2(config-line)# exec-timeout 0 0
D2(config-line)# logging synchronous
D2(config-line)#exit
D2(config)# vlan 100
D2(config-vlan)# name Management
D2(config-vlan)# exit
D2(config)# vlan 101
D2(config-vlan)# name UserGroupA
D2(config-vlan)#exit
D2(config)# vlan 102
D2(config-vlan)# name UserGroupB
D2(config-vlan)# exit
D2(config)# vlan 999
D2(config-vlan)# name NATIVE
D2(config-vlan)#exit
D2(config)# interface e1/0
D2(config-if)# no switchport
D2(config-if)# ip address 10.07.11.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d1:1 link-local
D2(config-if)# ipv6 address 2001:db8:100:1011::2/64
D2(config-if)# no shutdown
D2(config-if)#exit
D2(config)# interface vlan 100
D2(config-if)# ip address 10.07.100.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d2:2 link-local
D2(config-if)# ipv6 address 2001:db8:100:100::2/64
D2(config-if)# no shutdown
D2(config-if)#exit
D2(config)# interface vlan 101
D2(config-if)# ip address 10.07.101.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d2:3 link-local
D2(config-if)# ipv6 address 2001:db8:100:101::2/64
D2(config-if)# no shutdown
D2(config-if)#exit
D2(config)# interface vlan 102
D2(config-if)# ip address 10.07.102.2 255.255.255.0
D2(config-if)# ipv6 address fe80::d2:4 link-local
D2(config-if)# ipv6 address 2001:db8:100:102::2/64
D2(config-if)# no shutdown
D2(config-if)#exit
D2(config)# ip dhcp excluded-address 10.07.101.1 10.07.101.209
D2(config)# ip dhcp excluded-address 10.07.101.241 10.07.101.254
```

```
D2(config)# ip dhcp excluded-address 10.07.102.1 10.07.102.209
D2(config)# ip dhcp excluded-address 10.07.102.241 10.07.102.254
D2(config)# ip dhcp pool VLAN-101
D2(dhcp-config)# network 10.07.101.0 255.255.255.0
D2(dhcp-config)# default-router 07.0.101.254
D2(dhcp-config)# exit
D2(config)# ip dhcp pool VLAN-102
D2(dhcp-config)# network 10.07.102.0 255.255.255.0
D2(dhcp-config)# default-router 10.07.102.254
D2(dhcp-config)# exit
D2(config)# interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
D2(config-if-range)# shutdown
D2(config-if-range)# exit
D2(config)# exit
D2# copy running-config startup-config
```

```
A1#configure terminal
A1(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment#
A1(config)# line con 0
A1(config-line)# exec-timeout 0 0
A1(config-line)# logging synchronous
A1(config-line)#exit
A1(config)# vlan 100
A1(config-vlan)# name Management
A1(config-vlan)# exit
A1(config)# vlan 101
A1(config-vlan)# name UserGroupA
A1(config-vlan)#exit
A1(config)# vlan 102
A1(config-vlan)# name UserGroupB
A1(config-vlan)# exit
A1(config)# vlan 999
A1(config-vlan)# name NATIVE
A1(config-vlan)#exit
A1(config)# interface vlan 100
A1(config-if)# ip address 10.07.100.3 255.255.255.0
A1(config-if)# ipv6 address fe80::a1:1 link-local
A1(config-if)# ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)# interface range e0/0,e0/3,e1/0,e1/3,e2/0-3,e3/0-3
A1(config-if-range)# shutdown
A1(config-if-range)# exit
A1(config)# exit
A1# copy running-config startup-config
```

El siguiente paso es guardar la configuración en cada dispositivo mediante el comando `copy running-config startup-config` como se observa en la figura 2:

**Figura 2.** Configuración guardada en los dispositivos

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

```
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 3556 bytes to 1813 bytes[OK]
```

```
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 3555 bytes to 1820 bytes[OK]
```

```
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2509 bytes to 1358 bytes[OK]
```

**Fuente:** Propia

- c. Configure el direccionamiento de host de PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.XY.100.254, que será la dirección IP virtual de HSRP utilizada en la Parte 4.

Se procede a configurar las direcciones IPv4 e IPv6 en PC1 y PC4 así como el gateway predeterminado, para ello se emplea la tabla 1 de direccionamiento dada anteriormente como se muestra en la figura 3:

**Figura 3.** Configuración IP del PC1 y PC4

```
PC1> ip 10.07.100.5/24 10.07.100.254
Checking for duplicate address...
PC1 : 10.7.100.5 255.255.255.0 gateway 10.7.100.254

PC1> ip 2001:db8:100:100::5/64
PC1 : 2001:db8:100:100::5/64

PC1> save
Saving startup configuration to startup.vpc
. done
```

```
PC4> ip 10.07.100.5/24 10.07.100.254
Checking for duplicate address...
PC1 : 10.7.100.5 255.255.255.0 gateway 10.7.100.254

PC4> ip 2001:db8:100:100::5/64
PC1 : 2001:db8:100:100::5/64

PC4> save
Saving startup configuration to startup.vpc
. done
```

**Fuente:** Propia

Ahora se realiza la verificación de la configuración de los PCs:

**Figura 4.** Verificación de la IP de PC1 y PC4

```
PC1> show

NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
RT
PC1      10.7.100.5/24    10.7.100.254     00:50:79:66:68:00 10004  127.0.0.1:10005
          fe80::250:79ff:fe66:6800/64
          2001:db8:100:100::5/64
```

```
PC4> show

NAME      IP/MASK          GATEWAY          MAC              LPORT  RHOST:PORT
RT
PC4      10.7.100.6/24    10.7.100.254     00:50:79:66:68:03 10006  127.0.0.1:10007
          fe80::250:79ff:fe66:6803/64
          2001:db8:100:100::6/64
```

**Fuente:** Propia

## 1.2 Parte 2: Configurar la red de capa 2 y la compatibilidad con el host

En esta parte de la evaluación de habilidades, completará la configuración de la red de capa 2 y configurará el soporte de host básico. Al final de esta parte, todos los interruptores deberían poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC:

**Tabla 2.** Tareas de configuración - Parte 2

Task#	Task	Specification	Points
2.1	On all switches, configure IEEE 802.1Q trunk interfaces on interconnecting switch links	Enable 802.1Q trunk links between: <ul style="list-style-type: none"> <li>• D1 and D2</li> <li>• D1 and A1</li> <li>• D2 and A1</li> </ul>	6
2.2	On all switches, change the native VLAN on trunk links.	Use VLAN 999 as the native VLAN.	6
2.3	On all switches, enable the Rapid Spanning-Tree Protocol.	Use Rapid Spanning Tree.	3
2.4	On D1 and D2, configure the appropriate RSTP root bridges based on the information in the topology diagram.  D1 and D2 must provide backup in case of root bridge failure.	Configure D1 and D2 as root for the appropriate VLANs with mutually supporting priorities in case of switch failure.	2
2.5	On all switches, create LACP EtherChannels as shown in the topology diagram.	Use the following channel numbers: <ul style="list-style-type: none"> <li>• D1 to D2 – Port channel 12</li> <li>• D1 to A1 – Port channel 1</li> <li>• D2 to A1 – Port channel 2</li> </ul>	3
2.6	On all switches, configure host access ports connecting to PC1, PC2, PC3, and PC4.	Configure access ports with appropriate VLAN settings as shown in the topology diagram.  Host ports should transition immediately to forwarding state.	4
2.7	Verify IPv4 DHCP services.	PC2 and PC3 are DHCP clients and should be receiving valid IPv4 addresses.	1

Task#	Task	Specification	Points
2.8	Verify local LAN connectivity.	PC1 should successfully ping: <ul style="list-style-type: none"> <li>• D1: 10.XY.100.1</li> <li>• D2: 10.XY.100.2</li> <li>• PC4: 10.XY.100.6</li> </ul> PC2 should successfully ping: <ul style="list-style-type: none"> <li>• D1: 10.XY.102.1</li> <li>• D2: 10.XY.102.2</li> </ul> PC3 should successfully ping: <ul style="list-style-type: none"> <li>• D1: 10.XY.101.1</li> <li>• D2: 10.XY.101.2</li> </ul> PC4 should successfully ping: <ul style="list-style-type: none"> <li>• D1: 10.XY.100.1</li> <li>• D2: 10.XY.100.2</li> <li>• PC1: 10.XY.100.5</li> </ul>	1

En las tareas 2.1 y 2.2 se realizan las configuraciones de las interfaces troncales IEEE 802.1Q en todos los switches, teniendo en cuenta que se debe cambiar la VLAN nativa en estos enlaces troncales. En las tareas 2.3 y 2.4 se habilitara el protocolo Rapid Spanning-Tree (RSTP) en todos los switches, además, en los switches D1 y D2 se debe configurar los puentes raíz RSTP apropiados según la información del diagrama de topología, teniendo en cuenta que estos deben proporcionar respaldo en caso de falla del puente raíz. En las tareas 2.5 y 2.6 se deben crear LACP EtherChannels en todos los switches, como se muestra en el diagrama de topología, teniendo en cuenta que se deben especificar los números de canal de la siguiente manera: D1 a D2 debe usar el Port channel 12, D1 a A1 debe usar el Port channel 1, D2 a A1 debe usar el Port channel 2. Por otro lado, en todos los switches se deben configurar los puertos de acceso de host que se conectan a PC1, PC2, PC3 y PC4 con la configuración de VLAN adecuada, como se muestra en el diagrama de topología, donde se debe evidenciar que los puertos de host deben pasar inmediatamente al estado de reenvío.

Finalmente, para las tareas 2.7 y 2.8 se debe verificar los servicios DHCP IPv4, teniendo en cuenta que PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas, realizando la verificación de la conectividad de la LAN haciendo ping entre los PCs y los switches. A continuación se anexan las líneas de configuración de los dispositivos para dar cumplimiento con estas tareas:



```
D1#configure terminal
D1(config)#interface range e2/0-3
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface range e0/1-2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1((config-if-range)#channel-group 1 mode active
D1(config-if-range)#no shutdown
D1(config)#exit
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface e0/0
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#exit
D1#copy running-config startup-config
```

```
D2#configure terminal
D2(config)#interface range e2/0-3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface range e1/1-2
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
```

```
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#interface e0/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#exit
D2#copy running-config startup-config
```

```
A1#configure terminal
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e0/1-2
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface range e1/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface e1/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface e2/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#exit
A1#copy running-config startup-config
```

Una vez realizada las configuraciones en los dispositivos, el siguiente paso es verificar la configuración de la interfaz troncal y la VLAN nativa en D1 y D2 como se ilustra en la figura 5:

**Figura 5.** Verificación de las interfaces troncales y la VLAN nativa en D1 y D2

```
D1#show interfaces trunk

Port      Mode          Encapsulation  Status        Native vlan
Po1       on            802.1q         trunking     999
Po12      on            802.1q         trunking     999

Port      Vlans allowed on trunk
Po1       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
Po1       1,100-102,999
Po12      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,100-102,999
Po12      1,100-102,999

D2#show interfaces trunk

Port      Mode          Encapsulation  Status        Native vlan
Po2       on            802.1q         trunking     999
Po12      on            802.1q         trunking     999

Port      Vlans allowed on trunk
Po2       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
Po2       1,100-102,999
Po12      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,100-102,999
Po12      1,100-102,999
```

**Fuente:** Propia

Un aspecto que es necesario a tener en cuenta es que el enlace troncal que se configuro en los puertos del switch permite el paso del tráfico de la VLAN que hemos configurado. Hay que comprender que sin un enlace troncal, el hecho de querer presentar dos o más VLAN a dos o más switches, necesitaría un enlace de cada VLAN en cada switch a la misma VLAN en todos los demás switches que participan en dicha VLAN. Por otro lado, en la figura 5 se puede ver a simple vista que el puerto está formando un canal de forma eficaz, además de que los canales

LACP en los switches están en el modo activo y fueron configurados según la tabla 1 de direccionamiento como se observa en la figura 6.

**Figura 6.** Verificación de la creación de los LACP EtherChannel

```
D1#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:

Port      Flags      LACP port      Admin Oper   Port  Port
      Priority Dev ID          key  Key   Number State
Et0/1     SA        32768 aabb.cc80.0300 12s  0x0  0x1  0x2  0x3D
Et0/2     SA        32768 aabb.cc80.0300 7s   0x0  0x1  0x3  0x3D

Channel group 12 neighbors

Partner's information:

Port      Flags      LACP port      Admin Oper   Port  Port
      Priority Dev ID          key  Key   Number State
Et2/0     SA        32768 aabb.cc80.0200 1s   0x0  0xC  0x201 0x3D
Et2/1     SA        32768 aabb.cc80.0200 24s  0x0  0xC  0x202 0x3D
Et2/2     SA        32768 aabb.cc80.0200 1s   0x0  0xC  0x203 0x3D
Et2/3     SA        32768 aabb.cc80.0200 26s  0x0  0xC  0x204 0x3D
```

```
D2#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 2 neighbors

Partner's information:

Port      Flags      LACP port      Admin Oper   Port  Port
      Priority Dev ID          key  Key   Number State
Et1/1     SA        32768 aabb.cc80.0300 14s  0x0  0x2  0x102 0x3D
Et1/2     SA        32768 aabb.cc80.0300 24s  0x0  0x2  0x103 0x3D

Channel group 12 neighbors

Partner's information:

Port      Flags      LACP port      Admin Oper   Port  Port
      Priority Dev ID          key  Key   Number State
Et2/0     SA        32768 aabb.cc80.0100 17s  0x0  0xC  0x201 0x3D
Et2/1     SA        32768 aabb.cc80.0100 4s   0x0  0xC  0x202 0x3D
Et2/2     SA        32768 aabb.cc80.0100 14s  0x0  0xC  0x203 0x3D
Et2/3     SA        32768 aabb.cc80.0100 9s   0x0  0xC  0x204 0x3D
```

```

A1#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:

Port      Flags      LACP port
Priority  Dev ID      Age      Admin  Oper  Port  Port
Et0/1     SA         32768    aabb.cc80.0100 26s     0x0   0x1   0x2   0x3D
Et0/2     SA         32768    aabb.cc80.0100 17s     0x0   0x1   0x3   0x3D

Channel group 2 neighbors

Partner's information:

Port      Flags      LACP port
Priority  Dev ID      Age      Admin  Oper  Port  Port
Et1/1     SA         32768    aabb.cc80.0200 5s       0x0   0x2   0x102 0x3D
Et1/2     SA         32768    aabb.cc80.0200 1s       0x0   0x2   0x103 0x3D

```

**Fuente:** Propia

Ahora se verifica la configuración del protocolo Rapid Spanning-Tree (RSTP) en todos los switches, al igual que la configuración del puente raíz RSTP en los switches D1 y D2 como se observa en la figura 7.

**Figura 7.** Verificación del RSTP en D1 y D2

```

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 edge

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
spanning-tree portfast edge

```

**Fuente:** Propia

En la figura 8 se observa la configuración adecuada de la VLAN en los tres switches teniendo en cuenta el diagrama de topología.

**Figura 8.** Configuración adecuada de la VLAN en los 3 switches

```
D1#show run interface e0/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet0/0
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
```

```
D2#show run interface e0/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet0/0
 switchport access vlan 102
 switchport mode access
 spanning-tree portfast edge
end
```

```
A1#show run interface e1/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet1/3
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
end
```

```
A1#show run interface e2/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/0
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
```

**Fuente:** Propia

Finalmente, se debe verificar los servicios DHCP IPv4 teniendo en cuenta que PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas como se observa en la figura 9, por otro lado, también se verifica la conectividad de la LAN haciendo ping entre los PCs y los switches D1 y D2. Para comprobar la conectividad entre los PCs, se ejecuta un **ping** desde cada PC a los demás. Ejecutamos ping desde el PC1 hacia D1, D2 y PC4 como se observa en la figura 10:

**Figura 9.** PC2 y PC3 recibiendo direccionamiento a través de DHCP

```
PC2> show

NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PORT
RT
PC2      10.7.102.210/24  10.7.102.254  00:50:79:66:68:01  10008  127.0.0.1:10009
          fe80::250:79ff:fe66:6801/64
          2001:db8:100:102:2050:79ff:fe66:6801/64  eui-64
```

```
PC3> show
NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PO
RT
PC3      10.7.101.110/24      10.7.101.254      00:50:79:66:68:02      10010  127.0.0.
1:10011
fe80::250:79ff:fe66:6802/64
2001:db8:100:101:2050:79ff:fe66:6802/64 eui-64
```

**Fuente:** Propia

**Figura 10.** Ping desde PC1 hacia D1, D2 y PC4

```
PC1> ping 10.07.100.1
84 bytes from 10.7.100.1 icmp_seq=1 ttl=255 time=10.382 ms
84 bytes from 10.7.100.1 icmp_seq=2 ttl=255 time=1.058 ms
84 bytes from 10.7.100.1 icmp_seq=3 ttl=255 time=1.184 ms
84 bytes from 10.7.100.1 icmp_seq=4 ttl=255 time=1.607 ms
84 bytes from 10.7.100.1 icmp_seq=5 ttl=255 time=1.365 ms

PC1> ping 10.07.100.2
84 bytes from 10.7.100.2 icmp_seq=1 ttl=255 time=3.677 ms
84 bytes from 10.7.100.2 icmp_seq=2 ttl=255 time=1.701 ms
84 bytes from 10.7.100.2 icmp_seq=3 ttl=255 time=2.233 ms
84 bytes from 10.7.100.2 icmp_seq=4 ttl=255 time=2.566 ms
84 bytes from 10.7.100.2 icmp_seq=5 ttl=255 time=1.709 ms

PC1> ping 10.07.100.6
84 bytes from 10.7.100.6 icmp_seq=1 ttl=64 time=2.436 ms
84 bytes from 10.7.100.6 icmp_seq=2 ttl=64 time=3.415 ms
84 bytes from 10.7.100.6 icmp_seq=3 ttl=64 time=3.017 ms
84 bytes from 10.7.100.6 icmp_seq=4 ttl=64 time=1.949 ms
84 bytes from 10.7.100.6 icmp_seq=5 ttl=64 time=17.814 ms
```

**Fuente:** Propia

Ejecutamos ping desde el PC2 hacia D1 y D2 como se muestra en la figura 11:

**Figura 11.** Ping desde PC2 hacia D1 y D2

```
PC2> ping 10.07.102.1
84 bytes from 10.7.102.1 icmp_seq=1 ttl=255 time=1.661 ms
84 bytes from 10.7.102.1 icmp_seq=2 ttl=255 time=2.486 ms
84 bytes from 10.7.102.1 icmp_seq=3 ttl=255 time=1.672 ms
84 bytes from 10.7.102.1 icmp_seq=4 ttl=255 time=1.686 ms
84 bytes from 10.7.102.1 icmp_seq=5 ttl=255 time=1.563 ms

PC2> ping 10.07.102.2
84 bytes from 10.7.102.2 icmp_seq=1 ttl=255 time=2.889 ms
84 bytes from 10.7.102.2 icmp_seq=2 ttl=255 time=2.090 ms
84 bytes from 10.7.102.2 icmp_seq=3 ttl=255 time=4.446 ms
84 bytes from 10.7.102.2 icmp_seq=4 ttl=255 time=1.634 ms
84 bytes from 10.7.102.2 icmp_seq=5 ttl=255 time=1.022 ms
```

**Fuente:** Propia

Ejecutamos ping desde el PC3 hacia D1 y D2 como se muestra en la figura 12:

**Figura 12.** Ping desde PC3 hacia D1 y D2

```
PC3> ping 10.07.101.1
84 bytes from 10.7.101.1 icmp_seq=1 ttl=255 time=2.208 ms
84 bytes from 10.7.101.1 icmp_seq=2 ttl=255 time=2.966 ms
84 bytes from 10.7.101.1 icmp_seq=3 ttl=255 time=3.552 ms
84 bytes from 10.7.101.1 icmp_seq=4 ttl=255 time=3.219 ms
84 bytes from 10.7.101.1 icmp_seq=5 ttl=255 time=2.478 ms

PC3> ping 10.07.101.2
84 bytes from 10.7.101.2 icmp_seq=1 ttl=255 time=1.596 ms
84 bytes from 10.7.101.2 icmp_seq=2 ttl=255 time=1.598 ms
84 bytes from 10.7.101.2 icmp_seq=3 ttl=255 time=1.673 ms
84 bytes from 10.7.101.2 icmp_seq=4 ttl=255 time=1.851 ms
84 bytes from 10.7.101.2 icmp_seq=5 ttl=255 time=1.600 ms
```

**Fuente:** Propia

Finalmente hacemos ping desde el PC4 hacia D1, D2 y PC1 como se muestra en la figura 13:

**Figura 13.** Ping desde PC4 hacia D1, D2 y PC1

```
PC4> ping 10.07.100.1
84 bytes from 10.7.100.1 icmp_seq=1 ttl=255 time=2.261 ms
84 bytes from 10.7.100.1 icmp_seq=2 ttl=255 time=2.144 ms
84 bytes from 10.7.100.1 icmp_seq=3 ttl=255 time=2.458 ms
84 bytes from 10.7.100.1 icmp_seq=4 ttl=255 time=2.162 ms
84 bytes from 10.7.100.1 icmp_seq=5 ttl=255 time=1.475 ms

PC4> ping 10.07.100.2
84 bytes from 10.7.100.2 icmp_seq=1 ttl=255 time=2.721 ms
84 bytes from 10.7.100.2 icmp_seq=2 ttl=255 time=2.201 ms
84 bytes from 10.7.100.2 icmp_seq=3 ttl=255 time=3.468 ms
84 bytes from 10.7.100.2 icmp_seq=4 ttl=255 time=1.895 ms
84 bytes from 10.7.100.2 icmp_seq=5 ttl=255 time=2.394 ms

PC4> ping 10.07.100.5
84 bytes from 10.7.100.5 icmp_seq=1 ttl=64 time=2.714 ms
84 bytes from 10.7.100.5 icmp_seq=2 ttl=64 time=2.103 ms
84 bytes from 10.7.100.5 icmp_seq=3 ttl=64 time=3.294 ms
84 bytes from 10.7.100.5 icmp_seq=4 ttl=64 time=2.729 ms
84 bytes from 10.7.100.5 icmp_seq=5 ttl=64 time=3.135 ms
```

**Fuente:** Propia

En las figuras 10, 11, 12 y 13 se observa que en este caso el ping ha sido satisfactorio, los cinco paquetes de prueba han llegado correctamente, esto se



debe a que los 3 switches se encuentran configurados dentro de la misma VLAN, en este caso la vlan 999, que les permite cambiar información entre ellos mediante los enlaces troncales que fueron configurados inicialmente.

## ESCENARIO 2

### 1.3 Part 1: Configure Routing Protocols

In this part, you will configure IPv4 and IPv6 routing protocols. At the end of this part, the network should be fully converged. IPv4 and IPv6 pings to the Loopback 0 interface from D1 and D2 should be successful.

Note: Pings from the hosts will not be successful because their default gateways are pointing to the HSRP address which will be enabled in Part 4.

Your configuration tasks are as follows:

**Tabla 3.** Tareas de configuración Escenario 2 - Parte 1

Task#	Task	Specification	Points
3.1	On the “Company Network” (i.e., R1, R3, D1, and D2), configure single-area OSPFv2 in area 0.	<p>Use OSPF Process ID 4 and assign the following router-IDs:</p> <ul style="list-style-type: none"><li>• R1: 0.0.4.1</li><li>• R3: 0.0.4.3</li><li>• D1: 0.0.4.131</li><li>• D2: 0.0.4.132</li></ul> <p>On R1, R3, D1, and D2, advertise all directly connected networks / VLANs in Area 0.</p> <ul style="list-style-type: none"><li>• On R1, do not advertise the R1 – R2 network.</li><li>• On R1, propagate a default route. Note that the default route will be provided by BGP.</li></ul> <p>Disable OSPFv2 advertisements on:</p> <ul style="list-style-type: none"><li>• D1: All interfaces except E1/2</li><li>• D2: All interfaces except E1/0</li></ul>	8

Task#	Task	Specification	Points
3.2	On the “Company Network” (i.e., R1, R3, D1, and D2), configure classic single-area OSPFv3 in area 0.	<p>Use OSPF Process ID <b>6</b> and assign the following router-IDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.6.1</li> <li>• R3: 0.0.6.3</li> <li>• D1: 0.0.6.131</li> <li>• D2: 0.0.6.132</li> </ul> <p>On R1, R3, D1, and D2, advertise all directly connected networks / VLANs in Area 0.</p> <ul style="list-style-type: none"> <li>• On R1, do not advertise the R1 – R2 network.</li> <li>• On R1, propagate a default route. Note that the default route will be provided by BGP.</li> </ul> <p>Disable OSPFv3 advertisements on:</p> <ul style="list-style-type: none"> <li>• D1: All interfaces except E1/2</li> <li>• D2: All interfaces except E1/0</li> </ul>	8
3.3	On R2 in the “ISP Network”, configure MP-BGP.	<p>Configure two default static routes via interface Loopback 0:</p> <ul style="list-style-type: none"> <li>• An IPv4 default static route.</li> <li>• An IPv6 default static route.</li> </ul> <p>Configure R2 in BGP ASN <b>500</b> and use the router-id 2.2.2.2.</p> <p>Configure and enable an IPv4 and IPv6 neighbor relationship with R1 in ASN 300.</p> <p>In IPv4 address family, advertise:</p> <ul style="list-style-type: none"> <li>• The Loopback 0 IPv4 network (/32).</li> <li>• The default route (0.0.0.0/0).</li> </ul> <p>In IPv6 address family, advertise:</p> <ul style="list-style-type: none"> <li>• The Loopback 0 IPv4 network (/128).</li> <li>• The default route (::/0).</li> </ul>	4

Task#	Task	Specification	Points
3.4	On R1 in the "ISP Network", configure MP-BGP.	<p>Configure two static summary routes to interface Null 0:</p> <ul style="list-style-type: none"> <li>• A summary IPv4 route for 10.XY.0.0/8.</li> <li>• A summary IPv6 route for 2001:db8:100::/48.</li> </ul> <p>Configure R1 in BGP ASN <b>300</b> and use the router-id 1.1.1.1.</p> <p>Configure an IPv4 and IPv6 neighbor relationship with R2 in ASN 500.</p> <p>In IPv4 address family:</p> <ul style="list-style-type: none"> <li>• Disable the IPv6 neighbor relationship.</li> <li>• Enable the IPv4 neighbor relationship.</li> <li>• Advertise the 10.XY.0.0/8 network.</li> </ul> <p>In IPv6 address family:</p> <ul style="list-style-type: none"> <li>• Disable the IPv4 neighbor relationship.</li> <li>• Enable the IPv6 neighbor relationship.</li> <li>• Advertise the 2001:db8:100::/48 network.</li> </ul>	4

En esta parte, se realizara la configuración de los protocolos de enrutamiento IPv4 e IPv6. En las tareas 3.1 y 3.2 se realizan las configuraciones del protocolo OSPFv2 y OSPFv3 de área única en el área 0 en R1, R3, D1 y D2 anunciando todas las redes/VLAN conectadas directamente en el Área 0. A continuación se anexan las líneas de configuración de los dispositivos para dar cumplimiento con estas tareas:

```

R1#configure terminal
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.07.10.0 0.0.0.255 area 0
R1(config-router)#network 10.07.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
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 e1/2
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#interface e1/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
```

```
R3#configure terminal
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.07.11.0 0.0.0.255 area 0
R3(config-router)#network 10.07.13.0 0.0.0.255 area 0
R3(config-router)#exit
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface e1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#interface e1/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#exit
```

```
D1#configure terminal
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.07.100.0 0.0.0.255 area 0
D1(config-router)#network 10.07.101.0 0.0.0.255 area 0
D1(config-router)#network 10.07.102.0 0.0.0.255 area 0
D1(config-router)#network 10.07.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface e1/2
D1(config-router)#exit
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface e1/2
D1(config-rtr)#exit
```

```
D1(config)#interface e1/2
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#exit
```

```
D2#configure terminal
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.07.100.0 0.0.0.255 area 0
D2(config-router)#network 10.07.101.0 0.0.0.255 area 0
D2(config-router)#network 10.07.102.0 0.0.0.255 area 0
D2(config-router)#network 10.07.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface e1/0
D2(config-router)#exit
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.131
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface e1/0
D2(config-rtr)#exit
D2(config)#interface e1/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#exit
```

En la tarea 3.3 se configurará el protocolo MP-BGP en R2 teniendo en cuenta que se deben configurar dos rutas estáticas predeterminadas en IPv4 e IPv6 a través de la interfaz Loopback 0. De igual manera se configurara el protocolo BGP en R2 usando la identificación del enrutador habilitando una relación de vecino IPv4 e IPv6 con R1. A continuación se anexan las líneas de configuración en R2 para dar cumplimiento con esta tarea:

```
R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
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
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)#exit
```

Al igual que en la tarea 3.3, en la tarea 3.4 se configurará el protocolo MP-BGP en R1 teniendo en cuenta que se deben configurar dos rutas resumidas estáticas IPv4 e IPV6 a la interfaz Null 0. De igual manera se configurara el protocolo BGP en R1 usando la identificación del enrutador habilitando una relación de vecino IPv4 e IPv6 con R2. A continuación se anexan las líneas de configuración en R1 para dar cumplimiento con esta tarea:

```
R1#configure terminal
R1(config)#ip route 10.07.0.0 255.0.0.0 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 10.07.0.0 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)#exit

```

Una vez realizada las configuraciones en los dispositivos, el siguiente paso es verificar la configuración del proceso OSPF 4, las ID asignadas y todas las redes VLAN conectadas directamente en el Área 0 anunciadas en cada dispositivo como se observa en la figura 14:

**Figura 14.** Verificación de la configuración OSPFv2 en R1, R3, D1 y D2

```

R1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.1
log-adjacency-changes
network 10.7.10.0 0.0.0.255 area 0
network 10.7.13.0 0.0.0.255 area 0
default-information originate

```

```

R3#show run | section ^router ospf
router ospf 4
router-id 0.0.4.3
log-adjacency-changes
network 10.7.11.0 0.0.0.255 area 0
network 10.7.13.0 0.0.0.255 area 0

```

```

D1#show run | section ^router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/2
network 10.7.10.0 0.0.0.255 area 0
network 10.7.100.0 0.0.0.255 area 0
network 10.7.101.0 0.0.0.255 area 0
network 10.7.102.0 0.0.0.255 area 0

```

```

D2#show run | section ^router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet1/0
network 10.7.11.0 0.0.0.255 area 0
network 10.7.100.0 0.0.0.255 area 0
network 10.7.101.0 0.0.0.255 area 0
network 10.7.102.0 0.0.0.255 area 0

```

**Fuente:** Propia

En la figura15 se observa la configuración OSPFv3, teniendo en cuenta que cada router debe conocer además la ruta hasta cada red LAN de destino. El router tiene ya información acerca de las redes que están conectadas directamente. Por tanto, deberá aprender las rutas a las redes que no están conectadas directamente. Debe existir una conexión física en el router para cada VLAN, o bien se debe habilitar la troncalidad en una conexión física individual, como se hizo anteriormente anunciando todas las redes VLAN conectadas directamente en el Área 0.



**Figura 15.** Verificación de la configuración OSPFv3 en R1, R3, D1 y D2

```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  log-adjacency-changes
  default-information originate
R1#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID    Cost  State Nbrs F/C
Et1/1     6   0             7          10   DR    1/1
Et1/2     6   0             8          10   DR    1/1
```

```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
  log-adjacency-changes
R3#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID    Cost  State Nbrs F/C
Et1/1     6   0             7          10   BDR   1/1
Et1/0     6   0             6          10   DR    1/1
```

```
D1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.131
  passive-interface default
  no passive-interface Ethernet1/2
D1#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID    Cost  State Nbrs F/C
Vl102     6   0             25         1    DR    0/0
Vl101     6   0             24         1    DR    0/0
Vl100     6   0             23         1    DR    0/0
Et1/2     6   0             21         10   BDR   1/1
```

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.131
  passive-interface default
  no passive-interface Ethernet1/0
D2#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID    Cost  State Nbrs F/C
Vl102     6   0             25         1    DR    0/0
Vl101     6   0             24         1    DR    0/0
Vl100     6   0             23         1    DR    0/0
Et1/0     6   0             21         10   BDR   1/1
```

**Fuente:** Propia

Las dos direcciones IP que utiliza en el comando neighbor de los routers deben poder alcanzarse entre sí. No es necesario que los routers BGP tengan conexión directa. Pero, debe haber algún IGP que se ejecute y permita que los dos vecinos se alcancen entre sí. Al no tener vínculos con los protocolos, las rutas estáticas no reciben actualizaciones, lo cual indica que el administrador debe reconfigurar

estas rutas nuevamente e incluir los cambios en la topología. En la figura 16 se observa el número de sistema autónomo (ASN) al que pertenece el router R1 y la vecindad que forma con R2 a través del anuncio de la ruta estática predeterminada de IPv4 e IPv6.

**Figura 16.** Verificación del MP-BGP en R2 y las rutas estáticas predeterminadas

```
R2#show run | section bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.225 remote-as 300
  !
  address-family ipv4
    no neighbor 2001:DB8:200::1 activate
    neighbor 209.165.200.225 activate
    no auto-summary
    no synchronization
    network 0.0.0.0
    network 2.2.2.2 mask 255.255.255.255
  exit-address-family
  !
  address-family ipv6
    neighbor 2001:DB8:200::1 activate
    network ::/0
    network 2001:DB8:2222::/128
  exit-address-family
```

```
R2#show run | include route
ip source-route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
```

**Fuente:** Propia

En la figura 17 se observa el estado BGP y el número de sistema autónomo (ASN) en R1, con las dos rutas resumidas estáticas a la interfaz Null 0, la ruta IPv4 resumida y la ruta IPv6 resumida. Además, se observa la configuración de vecindad que existe entre R1 y R2:

**Figura 17.** Verificación del MP-BGP en R1 y las rutas estáticas predeterminadas

```
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate
    no auto-summary
    no synchronization
  exit-address-family
  !
  address-family ipv6
    neighbor 2001:DB8:200::2 activate
    network 2001:DB8:100::/48
  exit-address-family
```

**Fuente:** Propia

Por otro lado, podemos verificar la tabla de enrutamiento en R1 para analizar si los protocolos OSPF y BGP para IPv4 están funcionando correctamente tal como se observa en la figura 18.

**Figura 18.** Tabla de enrutamiento en R1

```
R1#show ip route | include O|B
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       o - ODR, P - periodic downloaded static route
B       2.2.2.2 [20/0] via 209.165.200.226, 00:17:51
O       10.7.11.0 [110/20] via 10.7.13.3, 00:23:50, Ethernet1/1
O       10.7.101.0 [110/11] via 10.7.10.2, 00:23:08, Ethernet1/2
O       10.7.100.0 [110/11] via 10.7.10.2, 00:23:08, Ethernet1/2
O       10.7.102.0 [110/11] via 10.7.10.2, 00:23:08, Ethernet1/2
B*     0.0.0.0/0 [20/0] via 209.165.200.226, 00:17:52
```

**Fuente:** Propia

En R1, emitimos el comando **show ipv6 route** para verificar que OSPFv3 para IPv6 está funcionando correctamente como se observa en la figura 19.

Figura 19. Verificación que OSPFv3 para IPv6 funciona correctamente en R1

```
R1#show ipv6 route
IPv6 Routing Table - Default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   ::/0 [20/0]
    via FE80::2:1, Ethernet1/0
S   2001:DB8:100::/48 [1/0]
    via Null0, directly connected
O   2001:DB8:100:100::/64 [110/21]
    via FE80::3:3, Ethernet1/1
O   2001:DB8:100:101::/64 [110/21]
    via FE80::3:3, Ethernet1/1
O   2001:DB8:100:102::/64 [110/21]
    via FE80::3:3, Ethernet1/1
C   2001:DB8:100:1010::/64 [0/0]
    via Ethernet1/2, directly connected
L   2001:DB8:100:1010::1/128 [0/0]
    via Ethernet1/2, receive
O   2001:DB8:100:1011::/64 [110/20]
    via FE80::3:3, Ethernet1/1
C   2001:DB8:100:1013::/64 [0/0]
    via Ethernet1/1, directly connected
L   2001:DB8:100:1013::1/128 [0/0]
    via Ethernet1/1, receive
C   2001:DB8:200::/64 [0/0]
    via Ethernet1/0, directly connected
L   2001:DB8:200::1/128 [0/0]
    via Ethernet1/0, receive
L   FF00::/8 [0/0]
```

Fuente: Propia

En R3, emitimos el comando **show ip route ospf** para verificar que OSPF para IPv4 funciona correctamente, como se observa en la figura 20.

Figura 20. Verificación que OSPF para IPv4 funciona correctamente en R3

```
R3#show ip route ospf | begin Gateway
R3#show ip route ospf
 10.0.0.0/24 is subnetted, 6 subnets
O    10.7.10.0 [110/20] via 10.7.13.1, 00:27:09, Ethernet1/1
O    10.7.101.0 [110/11] via 10.7.11.2, 00:23:12, Ethernet1/0
O    10.7.100.0 [110/11] via 10.7.11.2, 00:23:12, Ethernet1/0
O    10.7.102.0 [110/11] via 10.7.11.2, 00:23:12, Ethernet1/0
O*E2 0.0.0.0/0 [110/1] via 10.7.13.1, 00:21:07, Ethernet1/1
```

Fuente: Propia

En R3 emitimos el comando **show ipv6 route ospf** para verificar que OSPFv3 para IPv6 funciona correctamente como se observa en la figura 21.

**Figura 21.** Verificación que OSPFv3 para IPv6 funciona correctamente en R3

```
R3#show ipv6 route ospf
IPv6 Routing Table - Default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OE2 ::/0 [110/1], tag 6
    via FE80::1:3, Ethernet1/1
O   2001:DB8:100:100::/64 [110/21]
    via FE80::1:3, Ethernet1/1
O   2001:DB8:100:101::/64 [110/21]
    via FE80::1:3, Ethernet1/1
O   2001:DB8:100:102::/64 [110/21]
    via FE80::1:3, Ethernet1/1
O   2001:DB8:100:1013::/64 [110/10]
    via Ethernet1/1, directly connected
```

**Fuente:** Propia

## 1.4 Part 2: Configure First Hop Redundancy

In this part, you will configure HSRP version 2 to provide first-hop redundancy for hosts in the “Company Network”.

Your configuration tasks are as follows:

**Tabla 4.** Tareas de configuración Escenario 2 - Parte 2

Task#	Task	Specification	Points
4.1	On D1, create IP SLAs that test the reachability of R1 interface E1/2.	<p>Create two IP SLAs.</p> <ul style="list-style-type: none"> <li>• Use SLA number <b>4</b> for IPv4.</li> <li>• Use SLA number <b>6</b> for IPv6.</li> </ul> <p>The IP SLAs will test availability of R1 E1/2 interface every 5 seconds.</p> <p>Schedule the SLA for immediate implementation with no end time.</p> <p>Create an IP SLA object for IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"> <li>• Use track number <b>4</b> for IP SLA 4.</li> <li>• Use track number <b>6</b> for IP SLA 6.</li> </ul> <p>The tracked objects should notify D1 if the IP SLA state changes from down to up after 10 seconds, or from up to down after 15 seconds.</p>	2
4.2	On D2, create IP SLAs that test the reachability of R3 interface E1/0.	<p>Create two IP SLAs.</p> <ul style="list-style-type: none"> <li>• Use SLA number <b>4</b> for IPv4.</li> <li>• Use SLA number <b>6</b> for IPv6.</li> </ul> <p>The IP SLAs will test availability of R3 E1/0 interface every 5 seconds.</p> <p>Schedule the SLA for immediate implementation with no end time.</p> <p>Create an IP SLA object for IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"> <li>• Use track number <b>4</b> for IP SLA 4.</li> <li>• Use track number <b>6</b> for IP SLA 6.</li> </ul> <p>The tracked objects should notify D1 if the IP SLA state changes from down to up after 10 seconds, or from up to down after 15 seconds.</p>	2

Task#	Task	Specification	Points
4.3	On D1, configure HSRPv2.	<p>D1 is the primary router for VLANs 100 and 102; therefore, their priority will also be changed to 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP group <b>104</b> for VLAN 100:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address <b>10.XY.100.254</b>.</li> <li>• Set the group priority to <b>150</b>.</li> <li>• Enable preemption.</li> <li>• Track object 4 and decrement by 60.</li> </ul> <p>Configure IPv4 HSRP group <b>114</b> for VLAN 101:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address <b>10.XY.101.254</b>.</li> <li>• Enable preemption.</li> <li>• Track object 4 to decrement by 60.</li> </ul> <p>Configure IPv4 HSRP group <b>124</b> for VLAN 102:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address <b>10.XY.102.254</b>.</li> <li>• Set the group priority to <b>150</b>.</li> <li>• Enable preemption.</li> <li>• Track object 4 to decrement by 60.</li> </ul> <p>Configure IPv6 HSRP group <b>106</b> for VLAN 100:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address using <b>ipv6 autoconfig</b>.</li> <li>• Set the group priority to <b>150</b>.</li> <li>• Enable preemption.</li> <li>• Track object 6 and decrement by 60.</li> </ul> <p>Configure IPv6 HSRP group <b>116</b> for VLAN 101:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address using <b>ipv6 autoconfig</b>.</li> <li>• Enable preemption.</li> <li>• Track object 6 and decrement by 60.</li> </ul> <p>Configure IPv6 HSRP group <b>126</b> for VLAN 102:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address using <b>ipv6 autoconfig</b>.</li> <li>• Set the group priority to <b>150</b>.</li> <li>• Enable preemption.</li> <li>• Track object 6 and decrement by 60.</li> </ul>	8

Task#	Task	Specification	Points
	On D2, configure HSRPv2.	<p>D2 is the primary router for VLAN 101; therefore, the priority will also be changed to 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP group <b>104</b> for VLAN 100:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address <b>10.XY.100.254</b>.</li> <li>• Enable preemption.</li> <li>• Track object 4 and decrement by 60.</li> </ul> <p>Configure IPv4 HSRP group <b>114</b> for VLAN 101:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address <b>10.XY.101.254</b>.</li> <li>• Set the group priority to <b>150</b>.</li> <li>• Enable preemption.</li> <li>• Track object 4 to decrement by 60.</li> </ul> <p>Configure IPv4 HSRP group <b>124</b> for VLAN 102:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address <b>10.XY.102.254</b>.</li> <li>• Enable preemption.</li> <li>• Track object 4 to decrement by 60.</li> </ul> <p>Configure IPv6 HSRP group <b>106</b> for VLAN 100:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address using <b>ipv6 autoconfig</b>.</li> <li>• Enable preemption.</li> <li>• Track object 6 and decrement by 60.</li> </ul> <p>Configure IPv6 HSRP group <b>116</b> for VLAN 101:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address using <b>ipv6 autoconfig</b>.</li> <li>• Set the group priority to <b>150</b>.</li> <li>• Enable preemption.</li> <li>• Track object 6 and decrement by 60.</li> </ul> <p>Configure IPv6 HSRP group <b>126</b> for VLAN 102:</p> <ul style="list-style-type: none"> <li>• Assign the virtual IP address using <b>ipv6 autoconfig</b>.</li> <li>• Enable preemption.</li> <li>• Track object 6 and decrement by 60.</li> </ul>	

Para la tarea 4.1 creamos SLA de IP en D1, una para IPv4 y otra para IPv6 para probar la accesibilidad de la interfaz E1/2 de R1, cuya función nos permite monitorear la conectividad por red de uno o múltiples nodos donde sea que estos se encuentren y sean alcanzables. Los objetos rastreados deben notificar a D1 si



el estado de IP SLA cambia de abajo a arriba después de 10 segundos, o de arriba a abajo después de 15 segundos.

En la tarea 4.2 creamos SLA de IP en D2, una para IPv4 y otra para IPv6 para probar la accesibilidad de la interfaz E1/2 de R3. En la tarea 4.3 configuramos el protocolo HSRPv2 en D1 y D2. Inicialmente, D1 será el enrutador principal para las VLAN 100 y 102, luego, D2 será configurado como el enrutador principal para la VLAN 101. A continuación se anexan las líneas de configuración de los dispositivos para dar cumplimiento con estas tareas:

```
D1#configure terminal
D1(config)#ip sla 4
D1(config-ip-sla)#icmp-echo 10.07.10.1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#ip sla schedule 6 life forever start-time now
D1(config-track)#track 4 ip sla 4
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.07.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.07.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
```

```
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.07.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 priority 150
D1(config-if)#standby 126 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#exit
```

```
D2#configure terminal
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.07.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#track 6 ip sla 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.07.100.254
D2(config-if)#standby 104 preempt
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 track 6 decrement 60
```

```

D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.07.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.07.102.254
D2(config-if)#standby 124 preempt
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit

```

Una vez realizada las configuraciones en los dispositivos, el siguiente paso es verificar la configuración IP SLA en D1 y D2 con un tiempo de bajada después de 10 segundos, o de subida después de 15 segundos con una frecuencia de 5 segundos, como se ilustra en la figura 22:

**Figura 22.** Verificación de la configuración IP SLA en D1 y D2

```

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 10.7.10.1
  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

```

```

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 10.7.11.1
  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

```

**Fuente:** Propia

En la figura 23 se observa que D1 es el enrutador principal para las VLAN 100 y 102 con la prioridad de 150, mientras que la VLAN 101 se encuentra en estado de espera o “Standby”, con una prioridad de 100.

**Figura 23.** D1 como enrutador principal para las VLAN 100 y 102

```

D1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Vl100     104  150 P Active local          10.7.100.2      10.7.100.254
Vl100     106  150 P Active local          FE80::D2:2      FE80::5:73FF:FEA0
:6A
Vl101     114  100 P Standby 10.7.101.2     local           10.7.101.254
Vl101     116  100 P Standby FE80::D2:3     local           FE80::5:73FF:FEA0
:74
Vl102     124  150 P Active local          10.7.102.2      10.7.102.254
Vl102     126  150 P Active local          FE80::D2:4      FE80::5:73FF:FEA0
:7E

```

**Fuente:** Propia

Ahora, si nos vamos a la figura 24, se puede observar que D2 es el enrutador principal para la VLAN 101 donde la prioridad pasa de 100 a 150, mientras que las VLAN 100 y 102 se encuentra en estado de espera o “Standby” pasando la prioridad de 150 a 100.

**Figura 24.** D2 como enrutador principal para la VLAN 101

```
D2#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State   Active           Standby           Virtual IP
Vl100          104 100 P Standby 10.7.100.1       local             10.7.100.254
Vl100          106 100 P Standby FE80::D1:2       local             FE80::5:73FF:FEA0
:6A
Vl101          114 150 P Active  local            10.7.101.1       10.7.101.254
Vl101          116 150 P Active  local            FE80::D1:3       FE80::5:73FF:FEA0
:74
Vl102          124 100 P Standby 10.7.102.1       local             10.7.102.254
Vl102          126 100 P Standby FE80::D1:4       local             FE80::5:73FF:FEA0
:7E
```

**Fuente:** Propia

## CONCLUSIONES

Una vez finalizada la configuración de los dispositivos en el escenario propuesto, se puede concluir que para proporcionar routing y conectividad a varias VLAN es necesario implementar un enlace troncal 802.1Q entre uno o más switches y una única interfaz del router, donde se pudo observar cómo se dividía la interfaz física del router en varias subinterfases que proporcionan rutas lógicas a todas las VLAN conectadas, además, se configuró el routing entre las VLANs basado en enlaces troncales, recordando que este enlace troncal de VLAN amplía las VLAN a través de toda la red. Las VLAN no serían muy útiles sin los enlaces troncales de VLAN. Por otro lado, los enlaces troncales de VLAN permitieron que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router. Al utilizar el protocolo 802.1Q hay siempre una VLAN nativa, y en este caso la VLAN nativa es la VLAN 999.

El uso de EtherChannel pudo proporcionar un mayor ancho de banda y redundancia, además de ser conveniente porque permitió ampliar el ancho de banda sin aumentar la complejidad del diseño, por otro lado, el árbol de expansión considera al agrupamiento de EtherChannel como un solo link, sin embargo, durante la configuración de los protocolos de ruteo se pudo observar que el EtherChannel era tratado como una única interfaz enrutada con una dirección IP común, además, se logró que hubiera un puerto que reemplaza al puerto raíz cuando el puerto raíz falle, gracias al uso del protocolo RSTP, que es básicamente un STP mejorado que permitió tener una red conmutada. Una manera de verificar que las configuraciones cumplieron su papel dentro de la red, fue mediante el comando **ping** entre los dispositivos para así verificar que se cumplía con el enrutamiento y la conexión exitosa, donde claramente se observó que todas las verificaciones fueron satisfactorias.

## BIBLIOGRAFIA

EDGEWORTH, Bradley, *et al.* (2020). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. CISCO Press. 2019. 1024p.

ARIGANELLO, Ernesto y SEVILLA BARRIENTOS, Enrique. Redes CISCO. CCNP a fondo. Guía de estudio para profesionales. Madrid. RA-MA, S.A. 2015. 915p.

TEARE, Diane. CCNP Routing and Switching. Foundation Learning Guide Library. CISCO Press. 2015. 2088p

EMPSON, Scott y GARGANO, Patrick. CCNP and CCIE Enterprise Core & CCNP Enterprise Advanced Routing Portable Command Guide. CISCO Press. 2020. 416p

ARIGANELLO, Ernesto .Técnicas de Configuración de Routers CISCO. Madrid. RA-MA, S.A. 2014. 255p.