DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDRÉS FELIPE ROMERO GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA ELECTRONICA
BOGOTA
2022

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDRÉS FELIPE ROMERO GARCIA

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

DIRECTOR:
JOHN HAROLD PÉREZ CALDERÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA ELECTRONICA
BOGOTA
2022

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 17 de noviembre de 2022

AGRADECIMIENTOS

En primera medida agradezco a la universidad UNAD por los conocimientos impartidos durante estos años de carrera, en los que me ayudaron a formarme profesionalmente y como persona, gracias a cada maestro que, con paciencia, me ayudaron en cada pequeño reto que representaba cada actividad y en los que me ayudaron a ver cómo me serviría en adelante durante toda mi formación.

Agradezco a los compañeros que apoyaron colaborativamente con sus conocimientos, compartiéndolos en los diferentes foros, web conferencias y demás medios por los que tuvimos contacto, ya que cada una de sus experiencias, las asumí como propias y me enriquecieron mucho como profesional.

Gracias también a mis seres queridos, que estuvieron allí para apoyarme y darme aliento durante estos años, que me ayudaron a no desfallecer en este camino y que, al final, ya se ven los resultados de este arduo camino.

CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

GLOSARIO

ACL: (Access Control List) Las listas de control de acceso son una colección secuencial de condiciones de permiso y denegación que se aplican a un paquete IP. El dispositivo de red prueba los paquetes contra las condiciones de la ACL uno a la vez. La primera coincidencia determina si el paquete se acepta o rechaza. Debido a que las ACL son secuenciales y se detiene la prueba de condiciones después de la primera coincidencia, el orden de las condiciones es crítico. Las ACL al final contienen una condición de denegación implícita, lo que indica que, si el paquete analizado no coincide con ninguna condición de la ACL, se deniega.

BANNER: Un banner es un mensaje personalizable que se muestra en un dispositivo de red cuando un administrador se conecta a este a través de la consola, SSH o telnet. Estos mensajes pueden ser informativos o de advertencia.

BGP: (Border Gateway Protocol) Es un protocolo de enrutamiento dinámico de puerta de enlace exterior (EGP) escalable, utilizado principalmente en redes de internet en el que se intercambia información de rutas en diferentes sistemas autónomos (AS).

DHCP: (Dynamic Host Configuration Protocol) Este protocolo permite a los hosts conectados a una red, obtener su configuración de red en forma automática, lo que facilita la administración de la red.

HSRP: (Hot Standby Router Protocol) Es un protocolo de capa 3, propietario de Cisco, que permite tener Gateway de red redundantes, proporcionando tolerancia a fallas de los dispositivos y eliminando puntos únicos de falla.

OSPF: (Open Shortest Path First) Es un protocolo de enrutamiento dinámico de estado de enlace, diseñado para compartir rutas entre diferentes router, calculando la ruta más corta entre 2 nodos.

SLAAC: (Stateless Address Autoconfiguration) Es un método en el cual un dispositivo conectado a una red con direccionamiento IPv6 puede obtener su configuración de red en forma automática, sin la necesidad de un servidor DHCPv6.

RESUMEN

A través de las prácticas realizadas en el diplomado de profundización CCNP de Cisco, se desarrollan habilidades para la implementación y administración de redes de comunicaciones empresariales, sobre las cuales se busca optimizar los recursos, obteniendo redes confiables, seguras, tolerantes a fallos y escalables, con el objetivo de lograr la mejor experiencia de usuario posible.

Durante el desarrollo de este diplomado se utilizó el software de simulación GNS3, sobre el cual se configuraron dispositivos de capa 2 y capa 3, simulando enlaces troncales con redundancia, diferentes subredes en los que se utilizaron diferentes métodos de enrutamiento estático y dinámico, y asignación de direccionamiento estático y dinámico por DHCP. Adicional se configuró redundancia de Gateway de red con el protocolo HSRP.

Palabras Clave: BGP, CISCO, CCNP, OSPF, HSRP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

Through the practices carried out in the Cisco CCNP deepening diploma, skills are developed for the implementation and administration of business communications networks, on which it is sought to optimize resources, obtaining reliable, secure, fault-tolerant and scalable networks, with the aim of achieving the best possible user experience.

During the development of this diploma, the GNS3 simulation software was used, on which layer 2 and layer 3 devices were configured, simulating trunk links with redundancy, different subnets in which different static and dynamic routing methods were used, and assignment static and dynamic addressing by DHCP. Additionally, network gateway redundancy was configured with the HSRP protocol.

Keywords: BGP, CISCO, CCNP, OSPF, HSRP, Routing, Switching, Networking, Electronics.

INTRODUCCION

En el presente trabajo se realiza la implementación de una red simulada en el software GNS3, en la que se requiere que se tenga accesibilidad completa de extremo a extremo, contiene direccionamiento IPv4 e IPv6 y se realiza en 2 escenarios. En el primero, se implementa la topología que contiene enlaces redundantes, en la que se utilizan puertos troncales y agregación de interfaces con protocolo LACP, se realiza la configuración básica de los dispositivos en los que se combina asignación de direccionamiento estático y dinámico (DHCP y SLAAC), se definen los parámetros del protocolo Spanning tree con RSTP y portfast. Como medida de seguridad en la red, se deshabilitan los puertos de switch que no están en uso.

En el segundo escenario se configuran los protocolos de enrutamiento dinámico OSPF y BGP en ambos tipos de direccionamiento, IPv4 e IPv6 y se genera la redundancia de Gateway por medio del protocolo propietario de Cisco HSRP. En el caso del protocolo OSPF se define la configuración single-area sobre el área de backbone 0. En el caso de BGP, se utiliza en la propagación de las redes entre el sistema autónomo de la empresa y el del ISP, realizando la propagación de la ruta default. Como medida adicional de seguridad, se deshabilita la propagación de rutas por los puertos que no lo requieren. HSRP se configura en modo preempt con SLA que hagan monitoreo de disponibilidad de los enlaces entre los router.

Durante toda la actividad se documentan los comandos ingresados y las diferentes pruebas de funcionamiento de la red.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología

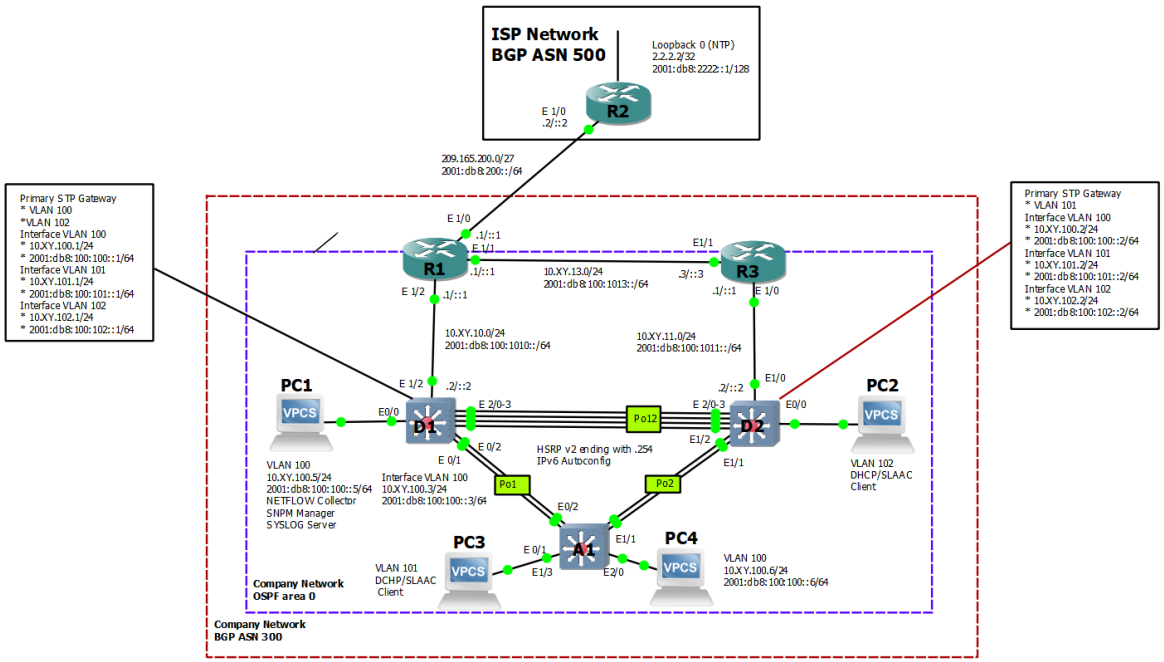


Tabla 1. Addressing Table

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

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
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
	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.XY.100.6/24	2001:db8:100:100::6/64	EUI-64

Objectives

Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing.

Part 2: Configure the Layer 2 Network and Host Support.

Part 3: Configure Routing Protocols.

Part 4: Configure First-Hop Redundancy.

Background / Scenario

In this skills assessment, you are responsible for completing the configuration of the network so there is full end-to-end reachability, so the hosts have reliable default gateway support, and so that management protocols are operational within the “Company Network” part of the topology. Be careful to verify that your configurations meet the provided specifications and that the devices perform as required.

Note: The routers used with CCNP hands-on labs are Cisco 7200 routers. The switches used in the labs are Cisco Catalyst L2 switches Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs.

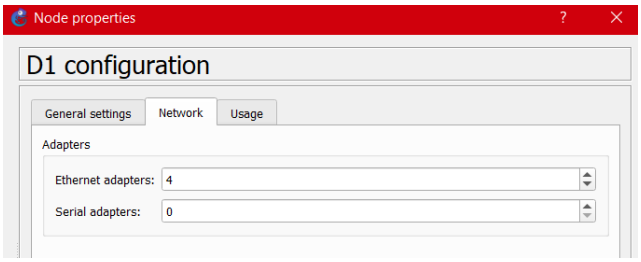
Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Note: The letters "X, Y" represent the last two digits of your ID number (cédula).

Required Resources

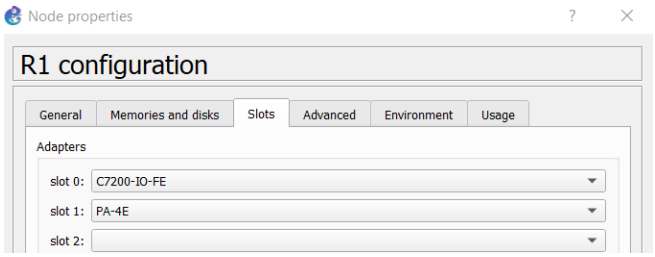
- 3 Routers (Cisco 7200). Click on the download link of the images for GNS3.
- 3 Switches (Cisco IOU L2). Click on the download link of the images for GNS3.
- 4 PCs (Use the GNS3’s VPCS)
- After the configuration of devices in GNS3, the Slots of the network adapters of the SW must be configured as follows:

Figura 2. Configuración adaptadores Sw



And of the Routers like this:

Figura 3. Configuración adaptadores Routers



Part 1: Build the Network and Configure Basic Device Settings and Interface Addressing

In Part 1, you will set up the network topology and configure basic settings and interface addressing.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for each device.

a. Console into each device, enter global configuration mode, and apply the basic settings. The startup configurations for each device are provided below.

Router R1

```
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 e1/2
 ip address 10.XY.10.1 255.255.255.0
 ipv6 address fe80::1:2 link-local
 ipv6 address 2001:db8:100:1010::1/64
 no shutdown
 exit
interface e1/1
 ip address 10.XY.13.1 255.255.255.0
 ipv6 address fe80::1:3 link-local
 ipv6 address 2001:db8:100:1013::1/64
 no shutdown
 exit
```

Router R2

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, 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
```

Router R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment#
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
interface e1/0
 ip address 10.XY.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.XY.13.3 255.255.255.0
 ipv6 address fe80::3:3 link-local
 ipv6 address 2001:db8:100:1010::2/64
 no shutdown
 exit
```

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.XY.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.XY.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.XY.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.XY.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.XY.101.1 10.XY.101.109
ip dhcp excluded-address 10.XY.101.141 10.XY.101.254
ip dhcp excluded-address 10.XY.102.1 10.XY.102.109
ip dhcp excluded-address 10.XY.102.141 10.XY.102.254
ip dhcp pool VLAN-101
 network 10.XY.101.0 255.255.255.0
 default-router 10.XY.101.254
 exit
ip dhcp pool VLAN-102
 network 10.XY.102.0 255.255.255.0
 default-router 10.XY.102.254
 exit
interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
 shutdown
 exit
```

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.XY.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.XY.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.XY.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.XY.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.XY.101.1 10.XY.101.209
ip dhcp excluded-address 10.XY.101.241 10.XY.101.254
ip dhcp excluded-address 10.XY.102.1 10.XY.102.209
ip dhcp excluded-address 10.XY.102.241 10.XY.102.254
ip dhcp pool VLAN-101
 network 10.XY.101.0 255.255.255.0
 default-router XY.0.101.254
 exit
ip dhcp pool VLAN-102
 network 10.XY.102.0 255.255.255.0
 default-router 10.XY.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
```

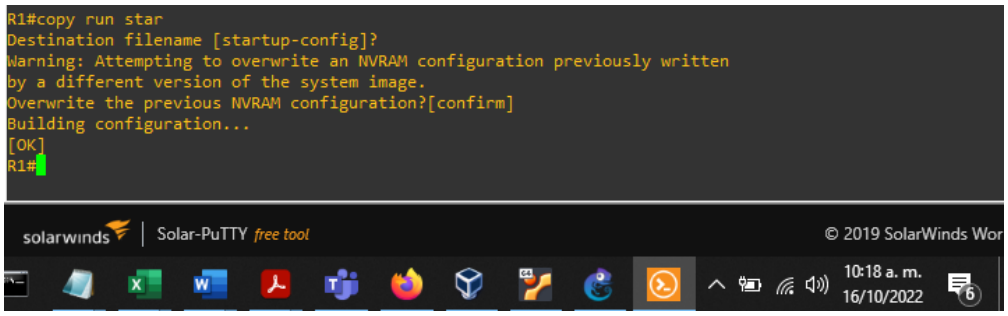
```
interface vlan 100
  ip address 10.XY.100.3 255.255.255.0
 ipv6 address fe80::a1:1 link-local
 ipv6 address 2001:db8:100:100::3/64
 no shutdown
 exit
interface range e0/0,e0/3,e1/0,e2/1-3,e3/0-3
 shutdown
 exit
```

b. Save the running configuration to startup-config on all devices.

R//:

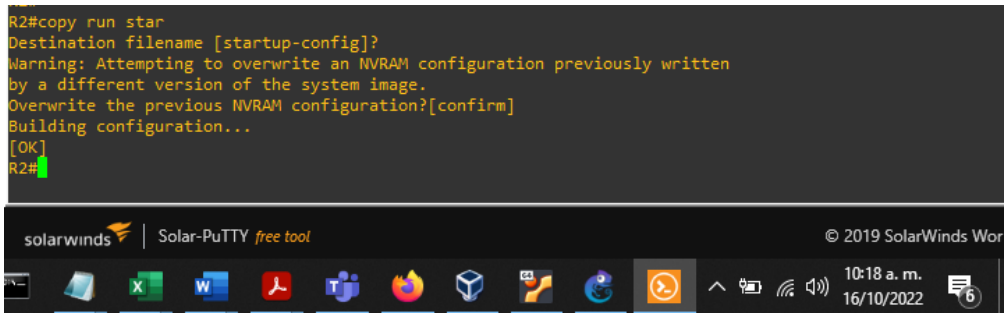
R1:

Figura 4. Guardado de config R1



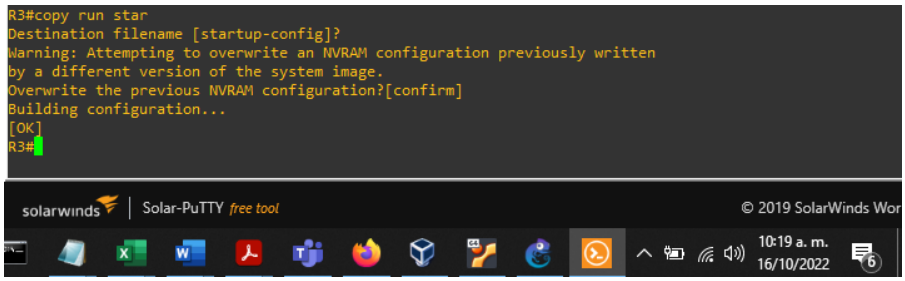
R2

Figura 5. Guardado de config R2



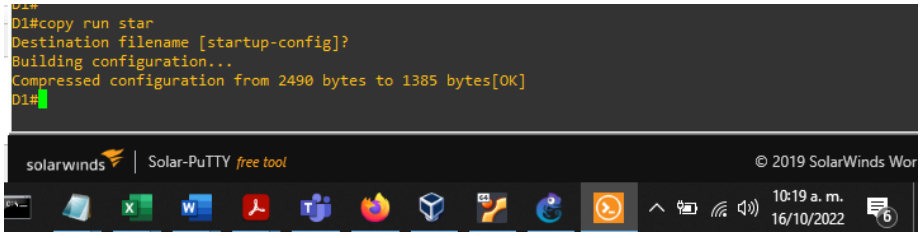
R3

Figura 6. Guardado de config R3



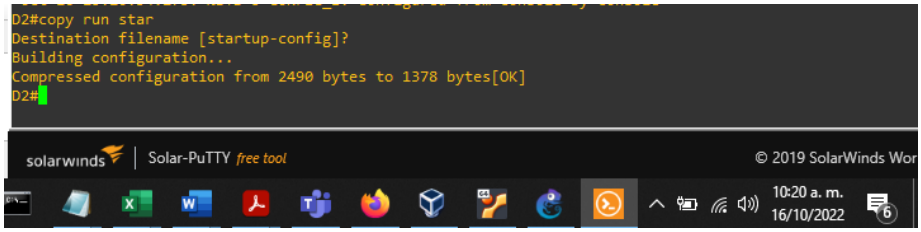
D1

Figura 7. Guardado de config D1



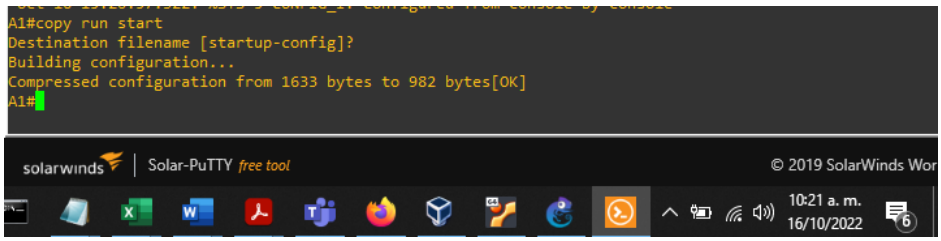
D2

Figura 8. Guardado de config D2



A1

Figura 9. Guardado de config A1

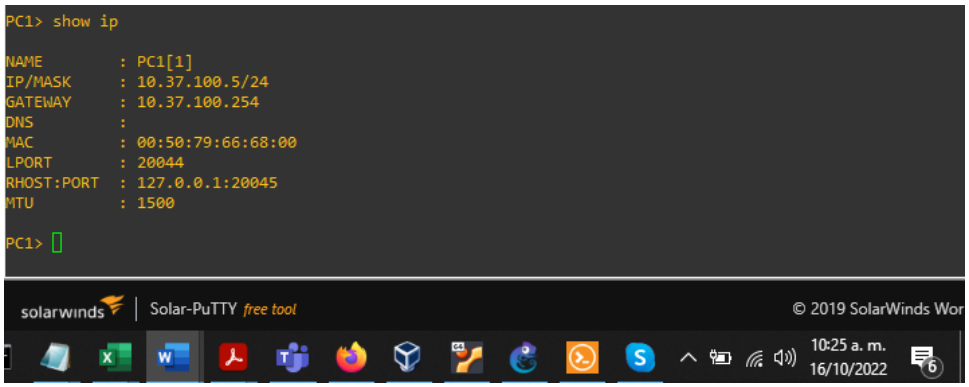


c. Configure PC 1 and PC 4 host addressing as shown in the addressing table. Assign a default gateway address of 10.XY.100.254 which will be the HSRP virtual IP address used in Part 4.

R//:

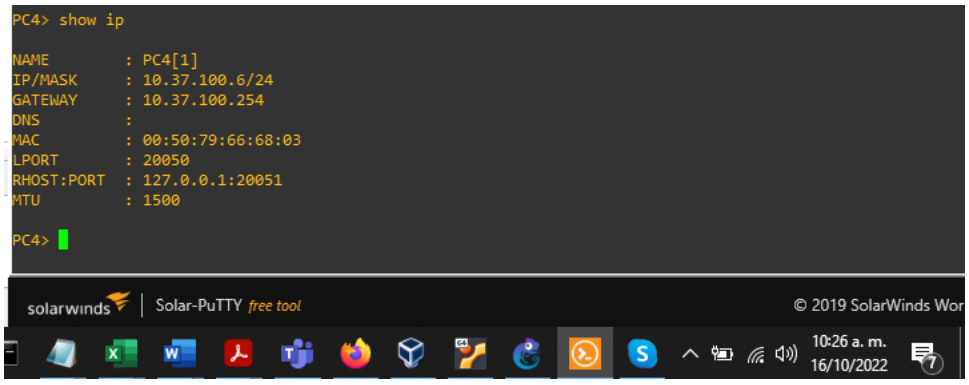
PC1:

Figura 10. Config IP PC1



PC4:

Figura 11. Config IP PC4



Part 2: Configure the Layer 2 Network and Host Support

In this part of the Skills Assessment, you will complete the Layer 2 network configuration and set up basic host support. At the end of this part, all the switches should be able to communicate. PC2 and PC3 should receive addressing from DHCP and SLAAC.

Your configuration tasks are as follows:

Tabla 2. Actividades 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: • D1 and D2 • D1 and A1 • D2 and A1	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: • D1 to D2 – Port channel 12 • D1 to A1 – Port channel 1 • D2 to A1 – Port channel 2	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

Task#	Task	Specification	Points
2.7	Verify IPv4 DHCP services.	PC2 and PC3 are DHCP clients and should be receiving valid IPv4 addresses.	1
2.8	Verify local LAN connectivity.	PC1 should successfully ping: • D1: 10.XY.100.1 • D2: 10.XY.100.2 • PC4: 10.XY.100.6 PC2 should successfully ping: • D1: 10.XY.102.1 • D2: 10.XY.102.2 PC3 should successfully ping: • D1: 10.XY.101.1 • D2: 10.XY.101.2 PC4 should successfully ping: • D1: 10.XY.100.1 • D2: 10.XY.100.2 • PC1: 10.XY.100.5	1

2.1: On all switches, configure IEEE 802.1Q trunk interfaces on interconnecting switch links:

R//:

D1:

D1(config)#inter range et0/1-2, et2/0-3

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

D1(config-if-range)#no shut

D2:

D2(config)#inter range et1/1-2, et2/0-3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#no shut

A1:
A1(config)#inter range et0/1-2, et1/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#no shut

2.2: On all switches, change the native VLAN on trunk links:

D1:
D1(config)#inter range et0/1-2, et2/0-3
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#

D2:
D2(config)#inter range et1/1-2, et2/0-3
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#

A1:
A1(config)#inter range et0/1-2, et1/1-2
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#

2.3: On all switches, enable the Rapid Spanning-Tree Protocol:

D1:

D1(config)#spanning-tree mode rapid-pvst

D1(config)#

D2:

D2(config)#spanning-tree mode rapid-pvst

D2(config)#

A1:

A1(config)#spanning-tree mode rapid-pvst

A1(config)#

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.:

D1:

D1(config)#spanning-tree vlan 100 root primary

D1(config)#spanning-tree vlan 101 root primary

D1(config)#spanning-tree vlan 102 root primary

D1(config)#spanning-tree vlan 999 root primary

D2:

D2(config)#spanning-tree vlan 100 root secondary

D2(config)#spanning-tree vlan 101 root secondary

D2(config)#spanning-tree vlan 102 root secondary

D2(config)#spanning-tree vlan 999 root secondary

2.5: On all switches, create LACP EtherChannels as shown in the topology diagram:

D1:

D1(config)#inter range et2/0-3
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#
D1(config-if-range)#inter range et0/1-2
D1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
D1(config-if-range)#

D2:
D2(config)#inter range et2/0-3
D2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12
D2(config-if-range)#
D2(config)# inter range et1/1-2
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)#

A1:
A1(config)#inter range et0/1-2
A1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
A1(config-if-range)#inter range et1/1-2
A1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
A1(config-if-range)#

2.6: On all switches, configure host access ports connecting to PC1, PC2, PC3, and PC4.:

D1:

D1(config)#inter e0/0
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast edge
D1(config-if)#no shut

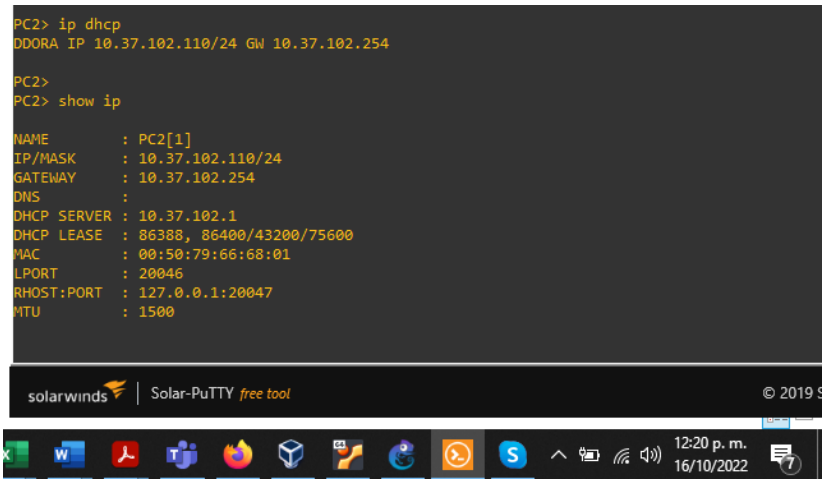
D2:
D2(config)#inter e0/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast edge
D2(config-if)#no shut

A1:
A1(config)#inter e1/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast edge
A1(config-if)#no shut
A1(config-if)#inter e2/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast edge
A1(config-if)#no shut

2.7: Verify IPv4 DHCP services:
R//:

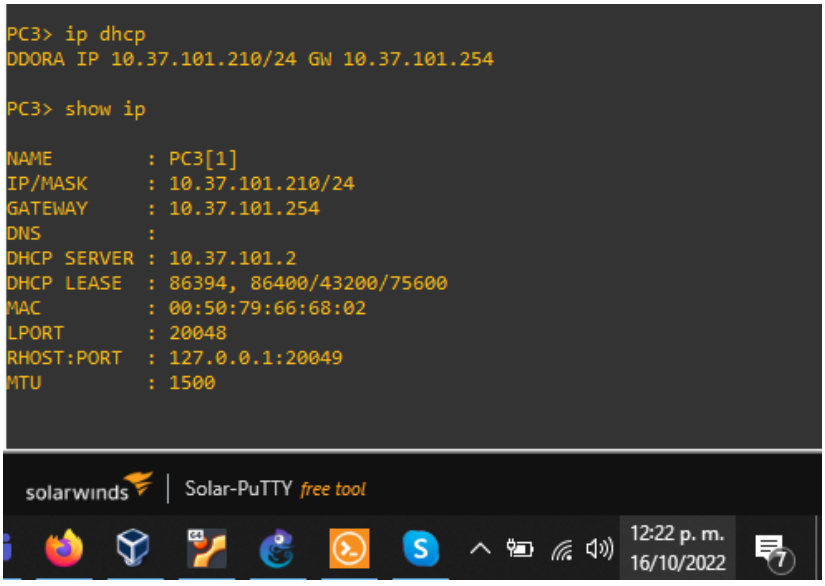
PC2:

Figura 12. Config IP DHCP PC2



PC3:

Figura 13. Config IP DHCP PC3



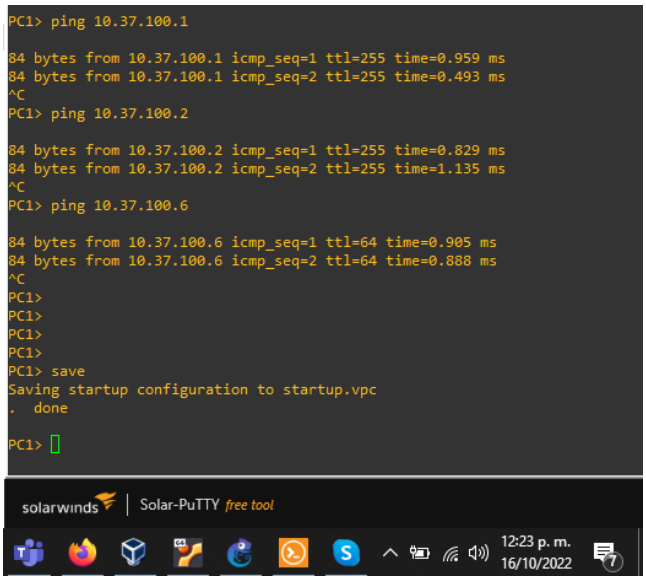
2.8: Verify local LAN connectivity

PC1 should successfully ping:

- D1: 10.XY.100.1
- D2: 10.XY.100.2
- PC4: 10.XY.100.6

R/::
PC1:

Figura 14. Pruebas ping PC1

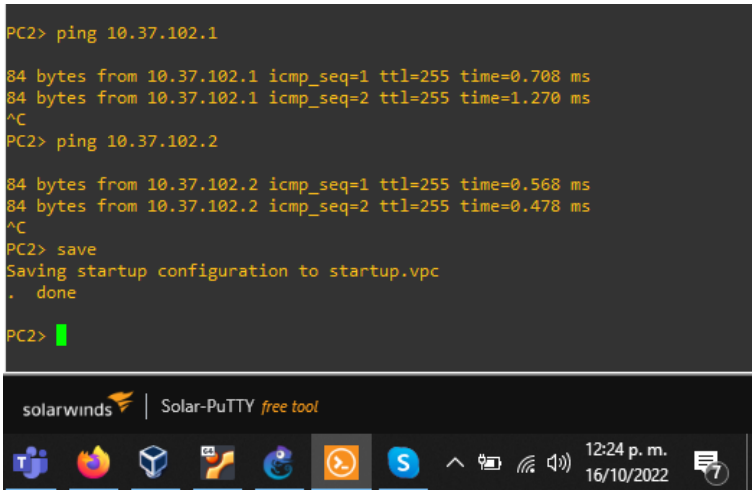


PC2 should successfully ping:

- D1: 10.XY.102.1
- D2: 10.XY.102.2

R//:
PC2:

Figura 15. Pruebas ping PC2

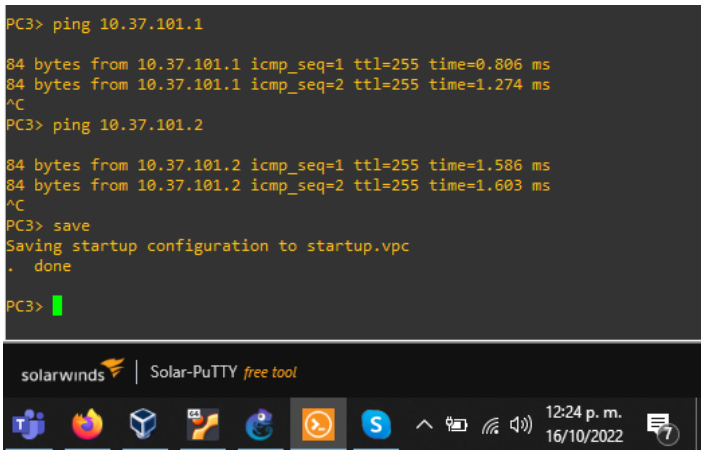


PC3 should successfully ping:

- D1: 10.XY.101.1
- D2: 10.XY.101.2

R//:
PC3:

Figura 16. Pruebas ping PC3

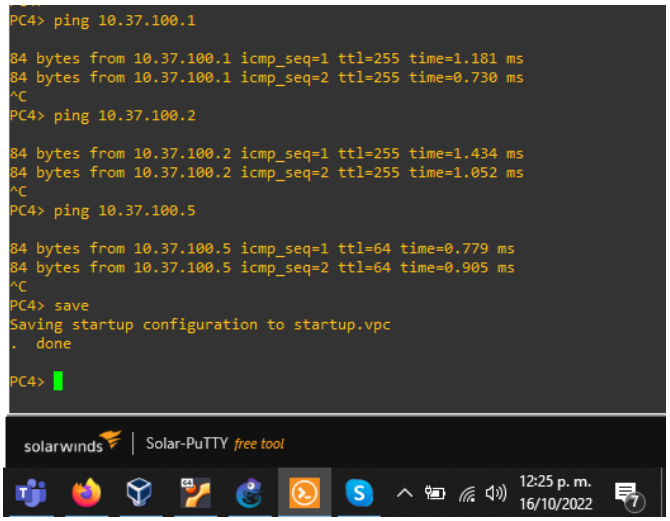


PC4 should successfully ping:

- D1: 10.XY.100.1
- D2: 10.XY.100.2
- PC1: 10.XY.100.5

R//:
PC4:

Figura 17. Pruebas ping PC4



2. ESCENARIO 2

ENCOR Skills Assessment (Scenario 2)

Part 3: 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. Actividades parte 3

Task#	Task	Specification	Points
3.1	On the “Company Network” (i.e., R1, R3, D1, and D2), configure single-area OSPFv2 in area 0.	Use OSPF Process ID **4** and assign the following router-IDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 On R1, R3, D1, and D2, advertise all directly connected networks / VLANs in Area 0. • On R1, do not advertise the R1 – R2 network. • On R1, propagate a default route. Note that the default route will be provided by BGP. Disable OSPFv2 advertisements on: • D1: All interfaces except E1/2 • D2: All interfaces except E1/0	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.	Use OSPF Process ID **6** and assign the following router-IDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 On R1, R3, D1, and D2, advertise all directly connected networks / VLANs in Area 0. • On R1, do not advertise the R1 – R2 network. • On R1, propagate a default route. Note that the default route will be provided by BGP. Disable OSPFv3 advertisements on: • D1: All interfaces except E1/2 • D2: All interfaces except E1/0	8
3.3	On R2 in the “ISP Network”, configure MP-BGP.	Configure two default static routes via interface Loopback 0: • An IPv4 default static route. • An IPv6 default static route. Configure R2 in BGP ASN **500** and use the router-id 2.2.2.2. Configure and enable an IPv4 and IPv6 neighbor relationship with R1 in ASN 300. In IPv4 address family, advertise: • The Loopback 0 IPv4 network (/32). • The default route (0.0.0.0/0). In IPv6 address family, advertise: • The Loopback 0 IPv4 network (/128). • The default route (::/0).	4

Task#	Task	Specification	Points
3.4	On R1 in the “ISP Network”, configure MP-BGP.	Configure two static summary routes to interface Null 0: • A summary IPv4 route for 10.XY.0.0/8. • A summary IPv6 route for 2001:db8:100::/48. Configure R1 in BGP ASN **300** and use the router-id 1.1.1.1. Configure an IPv4 and IPv6 neighbor relationship with R2 in ASN 500. In IPv4 address family: • Disable the IPv6 neighbor relationship. • Enable the IPv4 neighbor relationship. • Advertise the 10.XY.0.0/8 network. In IPv6 address family: • Disable the IPv4 neighbor relationship. • Enable the IPv6 neighbor relationship. • Advertise the 2001:db8:100::/48 network.	4

3.1: On the “Company Network” (i.e., R1, R3, D1, and D2), configure single-area OSPFv2 in area 0.

R//:

R1:

R1(config)#router ospf 4

R1(config-router)#router-id 0.0.4.1

R1(config-router)#network 10.37.10.0 0.0.0.255 area 0

R1(config-router)#network 10.37.13.0 0.0.0.255 area 0

R1(config-router)#default-information originate

R1(config-router)#

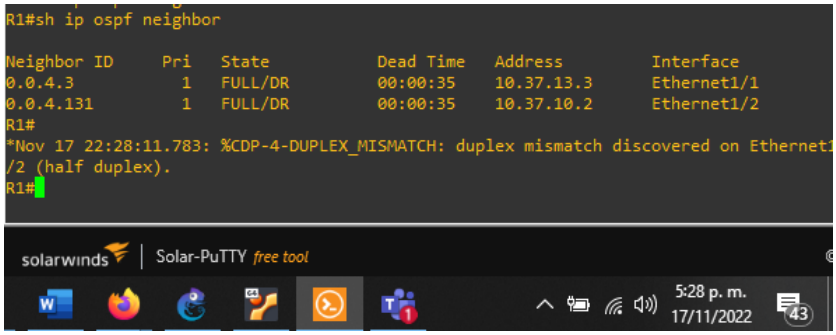
R3:
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.37.11.0 0.0.0.255 area 0
R3(config-router)#network 10.37.13.0 0.0.0.255 area 0
R3(config-router)#

D1:
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.37.10.0 0.0.0.255 area 0
D1(config-router)#network 10.37.100.0 0.0.0.255 area 0
D1(config-router)#network 10.37.101.0 0.0.0.255 area 0
D1(config-router)#network 10.37.102.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface e1/2

D2:
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.37.11.0 0.0.0.255 area 0
D2(config-router)#network 10.37.100.0 0.0.0.255 area 0
D2(config-router)#network 10.37.101.0 0.0.0.255 area 0
D2(config-router)#network 10.37.102.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface e1/0

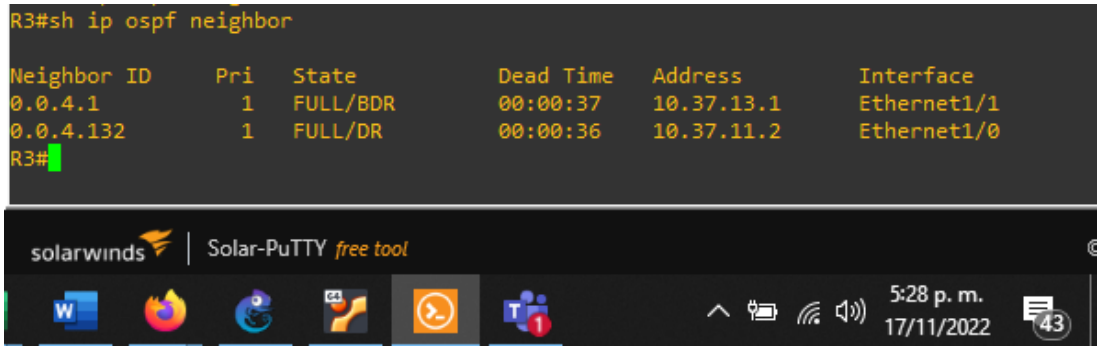
R1:

Figura 18. Verificación vecinos OSPF R1



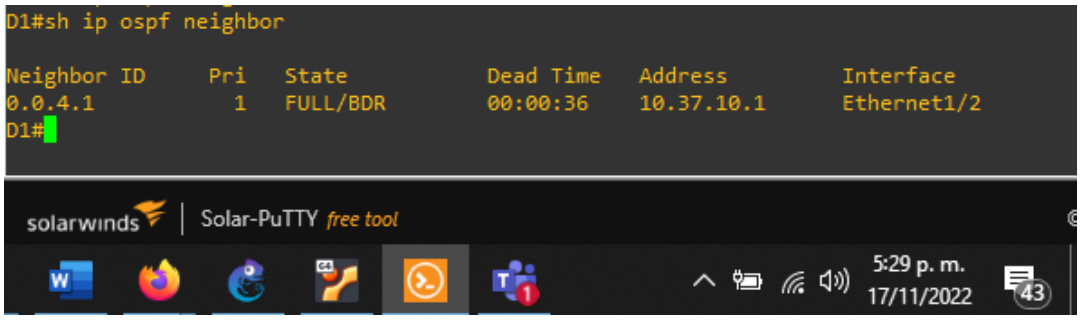
R3:

Figura 19. Verificación vecinos OSPF R3



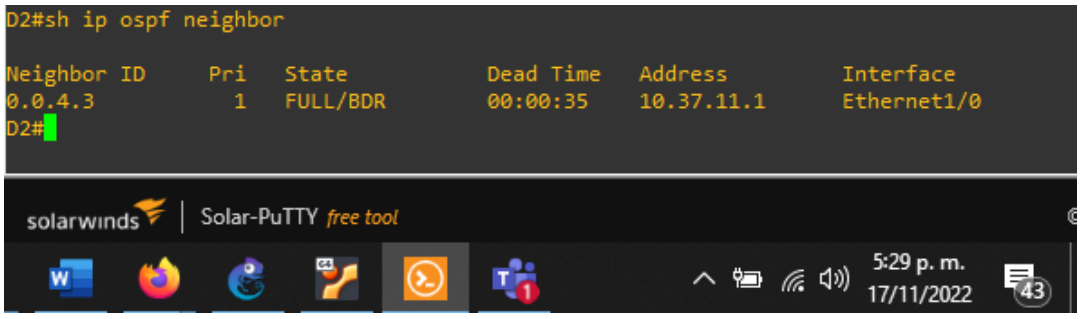
D1:

Figura 20. Verificación vecinos OSPF D1



D2:

Figura 21. Verificación vecinos OSPF D2



3.2: On the “Company Network” (i.e., R1, R3, D1, and D2), configure classic single-area OSPFv3 in area 0.

R//:
R1:
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)#int e1/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#int e1/2
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit

R3:
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#int e1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#int e1/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit

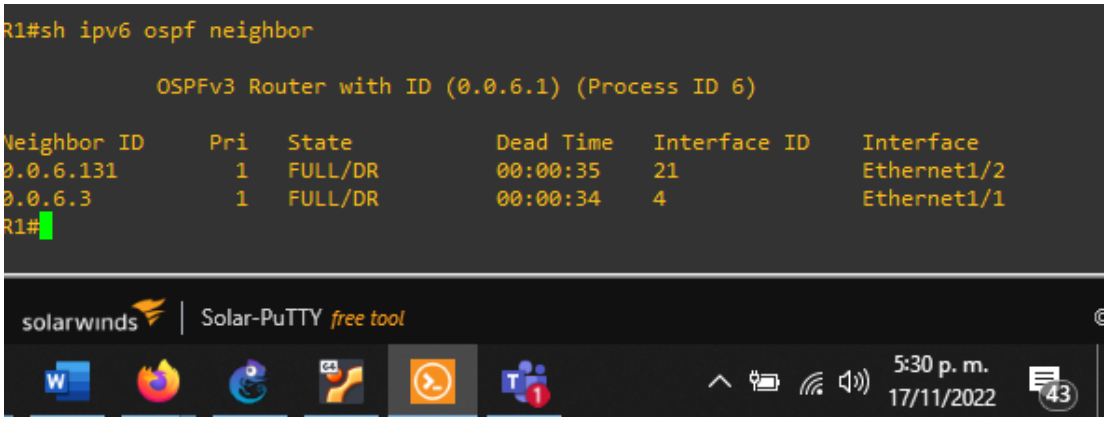
D1:
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface e1/2
D1(config-rtr)#exit
D1(config)#int e1/2
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int vlan 101

D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit

D2:
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface e1/0
D2(config-rtr)#exit
D2(config)#int e1/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#int vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#int vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#int vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit

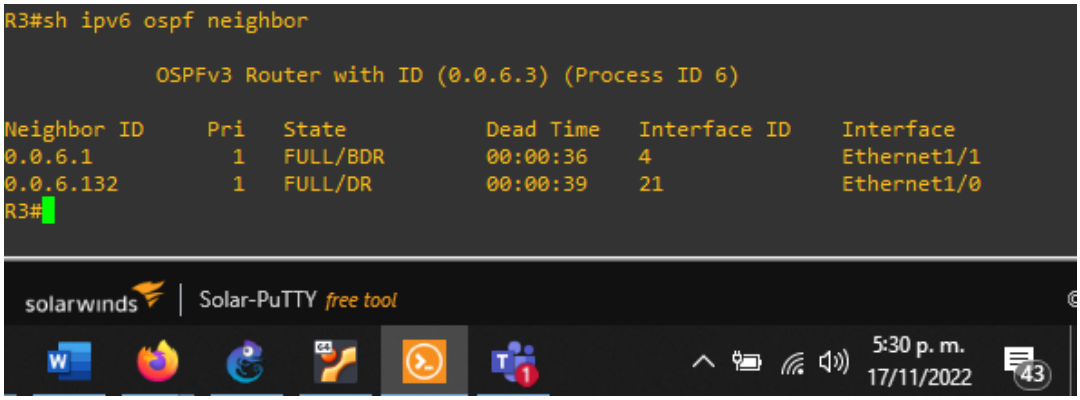
R1:

Figura 22. Verificación vecinos OSPFv3 R1



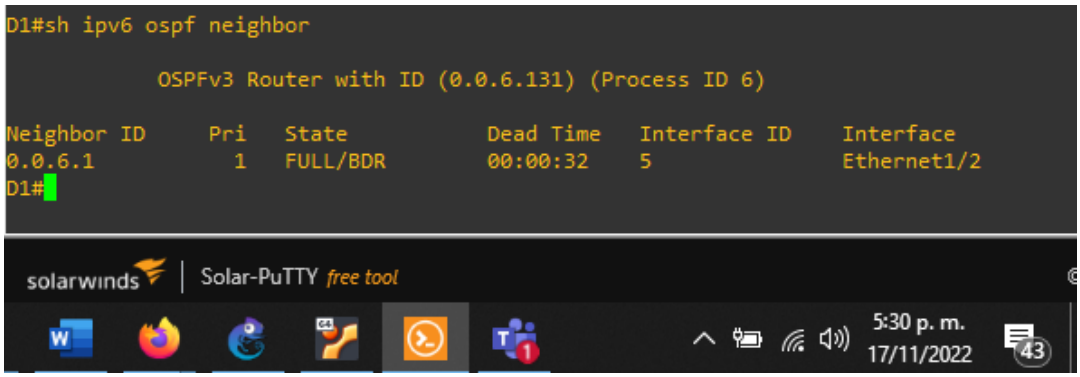
R3:

Figura 23. Verificación vecinos OSPFv3 R3



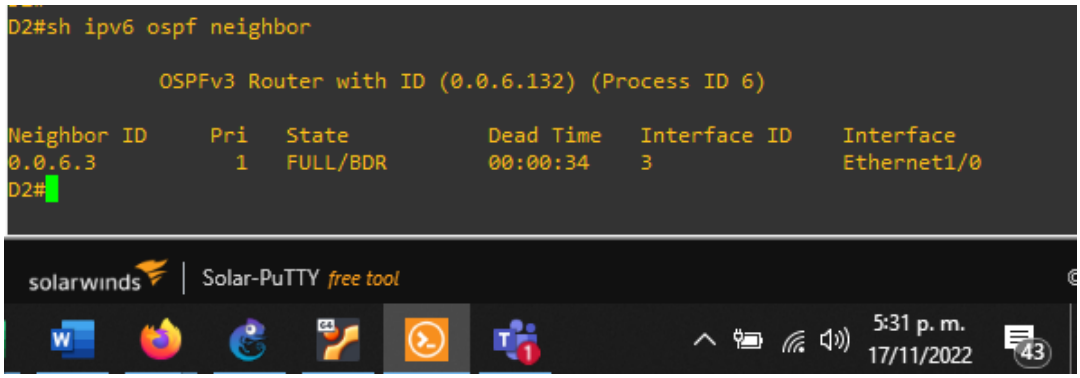
D1:

Figura 24. Verificación vecinos OSPFv3 D1



D2:

Figura 25. Verificación vecinos OSPFv3 D2



3.3: On R2 in the “ISP Network”, configure MP-BGP:

R//:

R2:

R2(config)#ip route 0.0.0.0 0.0.0.0 lo0

%Default route without gateway, if not a point-to-point interface, may impact performance

R2(config)#ipv6 route ::/0 lo0

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)#address-family ipv6

R2(config-router-af)#neighbor 2001:DB8:200::1 activate

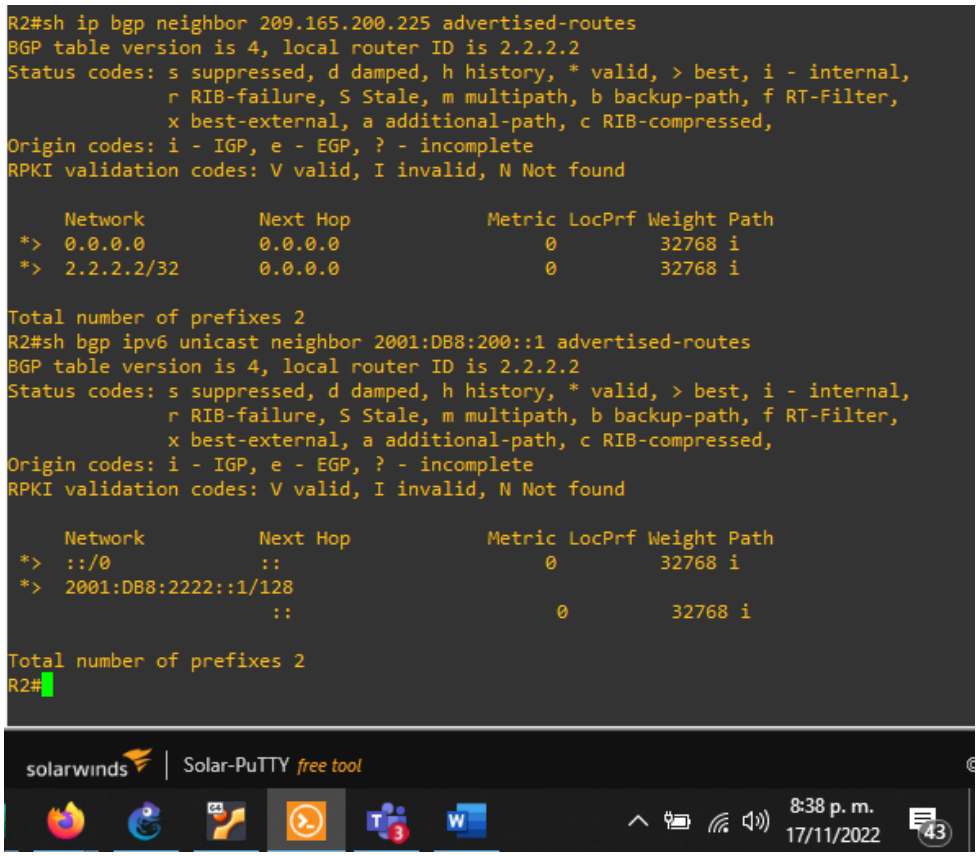
R2(config-router-af)#no neighbor 209.165.200.225 activate

R2(config-router-af)#network 2001:DB8:2222::1/128

R2(config-router-af)#network ::/0

R2:

Figura 26. Verificación rutas anunciadas BGP R2



3.4: On R1 in the “ISP Network”, configure MP-BGP:

R//:

R1:

R1(config)#ip route 10.37.0.0 255.0.0.0 null0

%Inconsistent address and mask

R1(config)#ip route 10.0.0.0 255.0.0.0 null0

R1(config)#ipv6 route 2001:db8:100::/48 null0

R1(config)#router bgp 300

R1(config-router)#bgp router-id 1.1.1.1

R1(config-router)#neighbor 209.165.200.226 remote-as 500

R1(config-router)#neighbor 2001:DB8:200::2 remote-as 500

R1(config-router)#address-family ipv4

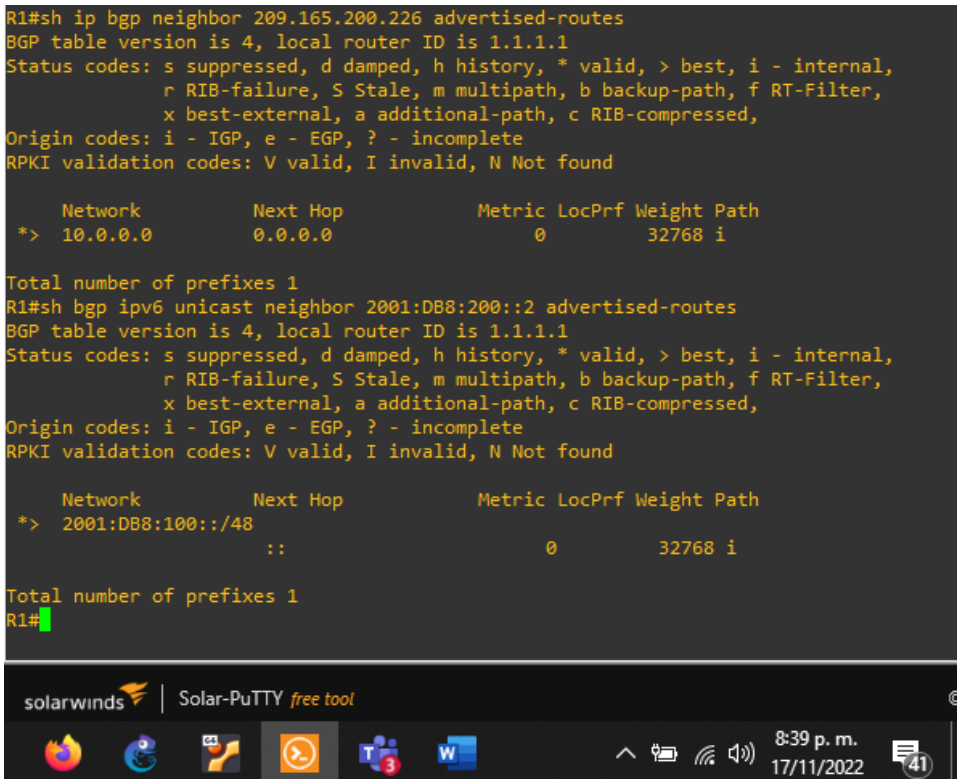
R1(config-router-af)#neighbor 209.165.200.226 activate

R1(config-router-af)#no neighbor 2001:DB8:200::2 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#address-family ipv6
R1(config-router-af)#neighbor 2001:DB8:200::2 activate
R1(config-router-af)#no neighbor 209.165.200.226 activate
R1(config-router-af)#network 2001:DB8:100::/48

Nota: para mi caso la ruta IPv4 sumarizada sería 10.37.0.0/8, pero esta no la recibe el router, ya que genera inconsistencia entre dirección y mascara, por lo que configure la 10.0.0.0/8.

R1:

Figura 27. Verificación rutas anunciadas BGP R1



Part 4: 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. Actividades parte 4

Task#	Task	Specification	Points
4.1	On D1, create IP SLAs that test the reachability of R1 interface E1/2.	Create two IP SLAs. • Use SLA number **4** for IPv4. • Use SLA number **6** for IPv6. The IP SLAs will test availability of R1 E1/2 interface every 5 seconds. Schedule the SLA for immediate implementation with no end time. Create an IP SLA object for IP SLA 4 and one for IP SLA 6. • Use track number **4** for IP SLA 4. • Use track number **6** for IP SLA 6. 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.	2
4.2	On D2, create IP SLAs that test the reachability of R3 interface E1/0.	Create two IP SLAs. • Use SLA number **4** for IPv4. • Use SLA number **6** for IPv6. The IP SLAs will test availability of R3 E1/0 interface every 5 seconds. Schedule the SLA for immediate implementation with no end time. Create an IP SLA object for IP SLA 4 and one for IP SLA 6. • Use track number **4** for IP SLA 4. • Use track number **6** for IP SLA 6. 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.	2

4.3	On D1, configure HSRPv2.	D1 is the primary router for VLANs 100 and 102; therefore, their priority will also be changed to 150. Configure HSRP version 2. Configure IPv4 HSRP group **104** for VLAN 100: • Assign the virtual IP address **10.XY.100.254**. • Set the group priority to **150**. • Enable preemption. • Track object 4 and decrement by 60. Configure IPv4 HSRP group **114** for VLAN 101: • Assign the virtual IP address **10.XY.101.254**. • Enable preemption. • Track object 4 to decrement by 60. Configure IPv4 HSRP group **124** for VLAN 102: • Assign the virtual IP address **10.XY.102.254**. • Set the group priority to **150**. • Enable preemption. • Track object 4 to decrement by 60. Configure IPv6 HSRP group **106** for VLAN 100: • Assign the virtual IP address using **ipv6 autoconfig**. • Set the group priority to **150**. • Enable preemption. • Track object 6 and decrement by 60. Configure IPv6 HSRP group **116** for VLAN 101: • Assign the virtual IP address using **ipv6 autoconfig**. • Enable preemption. • Track object 6 and decrement by 60. Configure IPv6 HSRP group **126** for VLAN 102:	8

Task#	Task	Specification	Points
		• Assign the virtual IP address using **ipv6 autoconfig**. • Set the group priority to **150**. • Enable preemption. • Track object 6 and decrement by 60.	

4.4	On D2, configure HSRPv2.	D2 is the primary router for VLAN 101; therefore, the priority will also be changed to 150. Configure HSRP version 2. Configure IPv4 HSRP group **104** for VLAN 100: • Assign the virtual IP address **10.XY.100.254**. • Enable preemption. • Track object 4 and decrement by 60. Configure IPv4 HSRP group **114** for VLAN 101: • Assign the virtual IP address **10.XY.101.254**. • Set the group priority to **150**. • Enable preemption. • Track object 4 to decrement by 60. Configure IPv4 HSRP group **124** for VLAN 102: • Assign the virtual IP address **10.XY.102.254**. • Enable preemption. • Track object 4 to decrement by 60. Configure IPv6 HSRP group **106** for VLAN 100: • Assign the virtual IP address using **ipv6 autoconfig**. • Enable preemption. • Track object 6 and decrement by 60. Configure IPv6 HSRP group **116** for VLAN 101: • Assign the virtual IP address using **ipv6 autoconfig**. • Set the group priority to **150**. • Enable preemption. • Track object 6 and decrement by 60. Configure IPv6 HSRP group **126** for VLAN 102: • Assign the virtual IP address using **ipv6 autoconfig**.	

Task#	Task	Specification	Points
		• Enable preemption. • Track object 6 and decrement by 60.	

4.1: On D1, create IP SLAs that test the reachability of R1 interface E1/2:

R//:

D1:

D1(config)#ip sla 4

D1(config-ip-sla)#icmp-echo 10.37.10.1

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 4 ip sla 4

D1(config-track)#delay up 10 down 15

D1(config-track)#exit

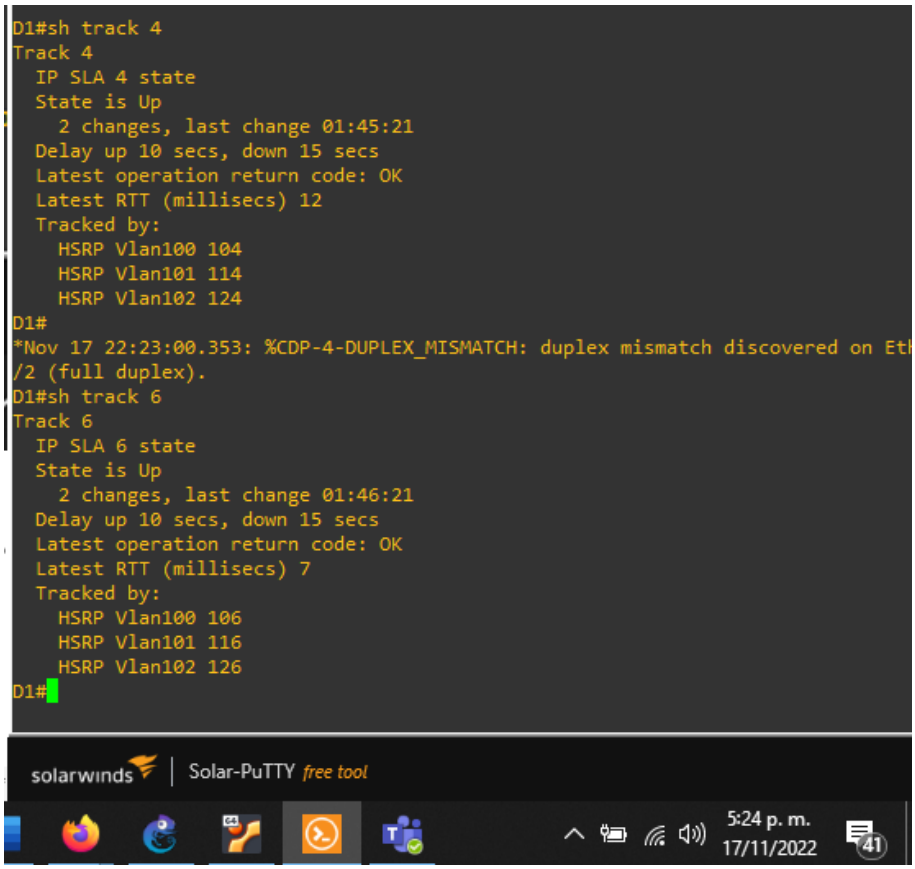
D1(config)#track 6 ip sla 6

D1(config-track)#delay up 10 down 15

D1(config-track)#exit

D1:

Figura 28. Verificación tracks D1



4.2: On D2, create IP SLAs that test the reachability of R3 interface E1/0:

R//:

D2:

D2(config)#ip sla 4

D2(config-ip-sla)#icmp-echo 10.37.11.1

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 up 10 down 15

D2(config-track)#exit

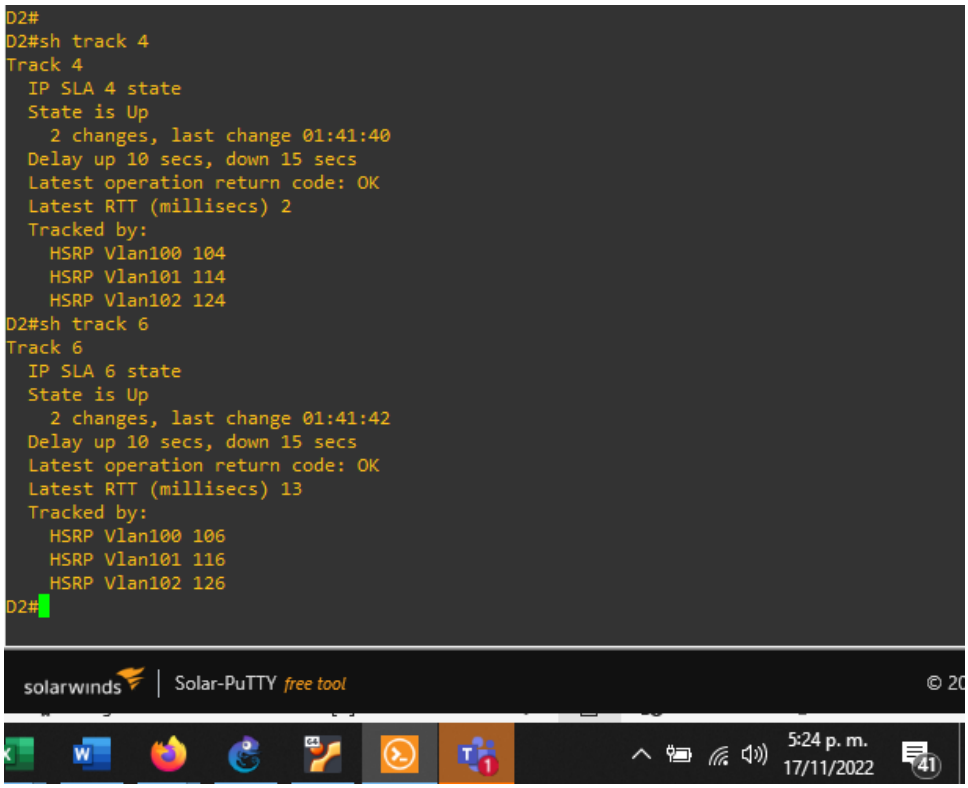
D2(config)#track 6 ip sla 6

D2(config-track)#delay up 10 down 15

D2(config-track)#exit

D2:

Figura 29. Verificación tracks D2



4.3: On D1, configure HSRPv2:

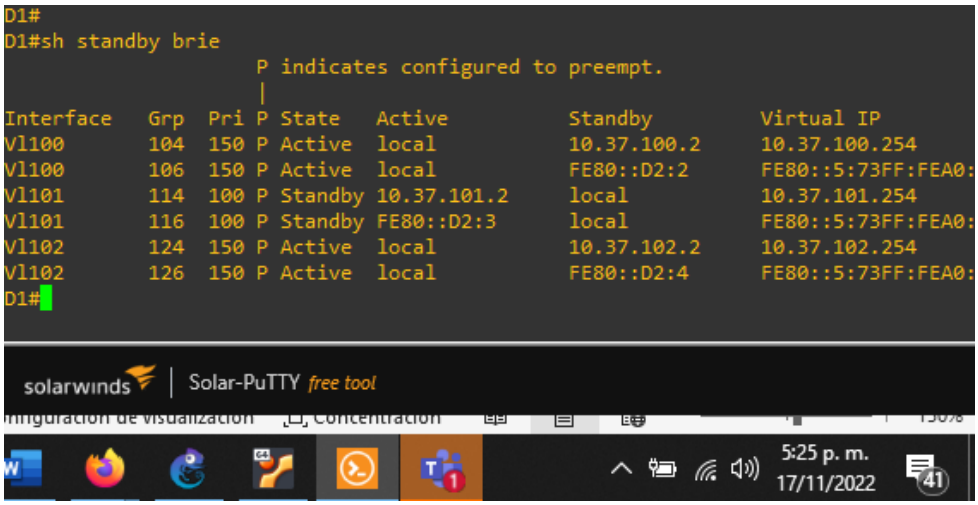
R//:

D1:

```
D1(config)#int vlan 100
D1(config-if)#standby ver 2
D1(config-if)#standby 104 ip 10.37.100.254
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)#
D1(config)#int vlan 101
D1(config-if)#standby ver 2
D1(config-if)#standby 114 ip 10.37.101.254
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)#
D1(config)#int vlan 102
D1(config-if)#standby ver 2
D1(config-if)#standby 124 ip 10.37.102.254
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 126 track 6 decrement 60
D1(config-if)#exit
```

D1:

Figura 30. Verificación estado HSRP D1



4.4: On D2, configure HSRPv2:

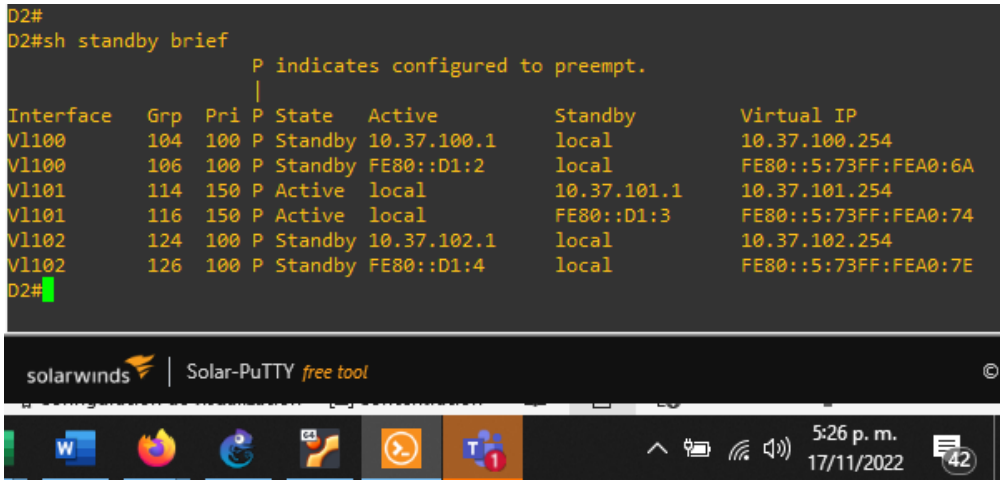
D2:

```
D2(config)#int vlan 100
D2(config-if)#standby ver 2
D2(config-if)#standby 104 ip 10.37.100.254
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)#
D2(config)#int vlan 101
D2(config-if)#standby ver 2
D2(config-if)#standby 114 ip 10.37.101.254
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)#
D2(config)#int vlan 102
D2(config-if)#standby ver 2
D2(config-if)#standby 124 ip 10.37.102.254
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

D2:

Figura 31. Verificación estado HSRP D2



CONCLUSIONES

Durante el desarrollo de estas prácticas de laboratorio se encontraron algunos puntos importantes para la implementación de redes empresariales, en las que es importante tener bien documentada la topología, ya que, por la cantidad de conexiones, se pueden confundir los puertos, las direcciones IP y sus configuraciones.

Dentro de esta documentación se debe tener claro los modos de configuración de los protocolos, ya que, por ejemplo, en LACP solo negocia correctamente en las configuraciones activo-activo o activo-pasivo, y si se configura indebidamente, no se construyen los etherchannel exitosamente, generando problemas en la comunicación y reduciendo el troughput esperado. También se debe tener especial cuidado en este protocolo que todos los puertos miembros del etherchannel tengan una configuración homogénea, ya que si no están iguales en velocidad, dúplex y modo (acceso o troncal), no se agregan como miembros.

En la topología de este laboratorio se evidenció que, por buenas prácticas de seguridad, se recomienda en OSPF evitar el anuncio de las rutas por interfaces que no se requieren, es decir, por puertos donde no estén conectados router que requieran la información de OSPF, ya que esto genera una vulnerabilidad a ataques de inyección de rutas al protocolo; y en temas de Switching deshabilitar los puertos que no se estén usando, para así evitar la creación de troncales, en los que se pueden llegar a inyectar información de VLANs por el protocolo VTP o generar ataques de VLAN Hopping.

Este diplomado de CCNP de Cisco nos aporto bastante conocimiento que podemos aplicar en las diferentes redes empresariales en la vida real y, por medio de estas simulaciones, nos da un avance en la experiencia de algunos problemas que podemos llegar a presentar en un entorno real.

REFERENCIAS BIBLIOGRÁFICAS

EDGEWORTH, Bradley, GARZA RIOS, Ramiro, GOOLEY, Jason, HUCABY, David. (2020). CISCO Press (Ed.). Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCORE 350-401 Official Cert Guide. Cisco Systems, Inc.

EDGEWORTH, Bradley, GARZA RIOS, Ramiro, GOOLEY, Jason, HUCABY, David. (2020). CISCO Press (Ed.). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCORE 350-401 Official Cert Guide. Cisco Systems, Inc.

EDGEWORTH, Bradley, GARZA RIOS, Ramiro, GOOLEY, Jason, HUCABY, David. (2020). CISCO Press (Ed.). Advanced OSPF. CCNP and CCIE Enterprise Core ENCORE 350-401 Official Cert Guide. Cisco Systems, Inc.

EDGEWORTH, Bradley, GARZA RIOS, Ramiro, GOOLEY, Jason, HUCABY, David. (2020). CISCO Press (Ed.). Advanced BGP. CCNP and CCIE Enterprise Core ENCORE 350-401 Official Cert Guide. Cisco Systems, Inc.

EDGEWORTH, Bradley, GARZA RIOS, Ramiro, GOOLEY, Jason, HUCABY, David. (2020). CISCO Press (Ed.). IP Services. CCNP and CCIE Enterprise Core ENCORE 350-401 Official Cert Guide. Cisco Systems, Inc.