DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

DANIELA PERILLA BARRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

DANIELA PERILLA BARRERA

Diplomado de opción de grado presentado para optar el título de
INGENIERIA DE TELECOMUNICACIONES

DIRECTOR:
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTÁ, 27 de noviembre 2022

AGRADECIMIENTOS

A mi esposo Edwin Navas y familia, tutores Gerardo Granados, director Juan Esteban Tapias quienes estuvieron en el transcurso de mi formación, con su constante apoyo, solidaridad acompañamiento y paciencia para culminar mi carrera de Ingeniería en Telecomunicaciones.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LACP: Forma parte de una especificación IEEE (802.3ad) también llamado llamadatrunking que permite agrupar varios puertos físicos para formar un único canal lógico. Un LACP permite que un Switch negocie un grupo automático mediante envió de paquetes.

Port Channel: Es un nombre propiedad de Cisco, construido de acuerdo con los estándares 802.3, permite la agrupación lógica de varios enlaces físicos, esta agrupación es tratada como un único enlace que permite sumar la velocidad nominal de cada puerto físico, usado así para obtener un enlace troncal de alta velocidad.

Rapid Spanning Tree: Es un Protocol de red de la segunda capa OSI que gestiona los enlaces redundantes, especificado en IEEE 802.1w. Cuando se configuran correctamente soluciona problemas de lentitud de STP

OSPF: Open Shortest Path First**,** es un protocolo de direccionamiento de tipo enlace-estado para encaminamiento jerárquico que usa el algoritmo Dijkstra, para calcular la ruta más corta entre los nodos, desarrollado para las redes IP**.**

BGP: Border Gateway Protocol, protocolo de puerta de enlace, es un protocolo que intercambia información escalable de dynamic routing usado en la internet por grupos enrutadores para compartir información de enrutamiento, BGP usa parámetros de ruta o atributos para definir políticas de enrutamiento y crear un entorno de enrutamiento estable

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 se utiliza en un grupo de routers para seleccionar un dispositivo activo y un dispositivo de reserva.

IP SLA: Es una tecnología de Cisco que monitorea activamente el tráfico para medir el desempeño de la red al medir parámetros críticos para el tráfico que pasa a través de los dispositivos con software Cisco IOS y otros servidores de aplicaciones de red. Al aprovechar Cisco IP SLA, es posible hacer que la red sea sensible a métricas críticas que afectan el rendimiento de la red y de sus aplicaciones asociadas.

RESUMEN

Las redes de telecomunicaciones se utilizan cada vez más para el intercambio de información dentro de las organizaciones y hacia internet. Es en estos entornos donde las tecnologías WAN y LAN tienen amplia cabida para implementar protocolos que conecten los dispositivos LAN hacia el exterior.

Este proyecto busca desarrollar una red corporativa compuesta por una switch multicapa con funcionalidades capa 2 y switches con funcionalidades capa 3 que serán los Gateway de la LAN para cada una de las VLANs y dos routers que proveen la salida a internet.

Se pondrán en práctica protocolos de capa 2 como LACP e Etherchannel para aumentar la capacidad de los enlaces y proveer mayor disponibilidad. Mediante el protocolo STP se garantiza una red libre de Loops capa 2.

Los protocolos de enrutamiento como OSPF y BGP se encargan del enrutamiento interno y hacia el exterior respectivamente para los segmentos de red IPv4 e IPv6. Esto combinado con HSRP y IP SLA complementan la disponibilidad de la red corporativa mediante la redundancia física de los Gateway de la LAN.

Esta prueba de habilidades abarca gran parte de los conceptos adquiridos durante todo el curso de CCNP y que son ampliamente utilizados en la vida profesional dentro del área de Networking IP.

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

ABSTRACT

Telecommunications networks are increasingly used for the exchange of information within organizations and to the Internet. It is in these environments where WAN and LAN technologies have ample room to implement protocols that connect LAN devices to the outside.

This project seeks to develop a corporate network made up of a multilayer switch with layer 2 functionalities and switches with layer 3 functionalities that will be the LAN Gateway for each of the VLANs and two routers that provide Internet access.

Layer 2 protocols such as LACP and EtherChannel will be put into practice to increase the capacity of the links and provide greater availability. Through the STP protocol, a loop-free layer 2 network is guaranteed.

Routing protocols such as OSPF and BGP handle internal and external routing respectively for IPv4 and IPv6 network segments. This combined with HSRP and IP SLA complement the availability of the corporate network through the physical redundancy of the LAN Gateways.

This skills test covers a large part of the concepts acquired throughout the CCNP course and that are widely used in professional life within the IP Networking area.

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

INTRODUCCIÓN

Durante el desarrollo de la guía podremos experimentar con protocolos capa dos como LACP sobre switches multicapa que además puede soportar funcionalidades de capa tres como DHCP y el direccionamiento para cada uno de los segmentos de la LAN.

Mediante el uso de GNS3 se implementará una red corporativa típica con dispositivos capa dos y capa tres haciendo uso de imágenes de sistema operativo funcionales sobre una máquina virtual.

La segunda parte de la prueba de habilidades comprende todo lo relacionado a protocolos de enrutamiento como OSPF, BGP y otras funcionalidades adicionales como HSRP e IP SLA para asegurar la redundancia y la alta disponibilidad de los servicios LAN.

DESARROLLO

1. ESCENARIO 1

ENCOR Skills Assessment (Scenario 1)

Topology

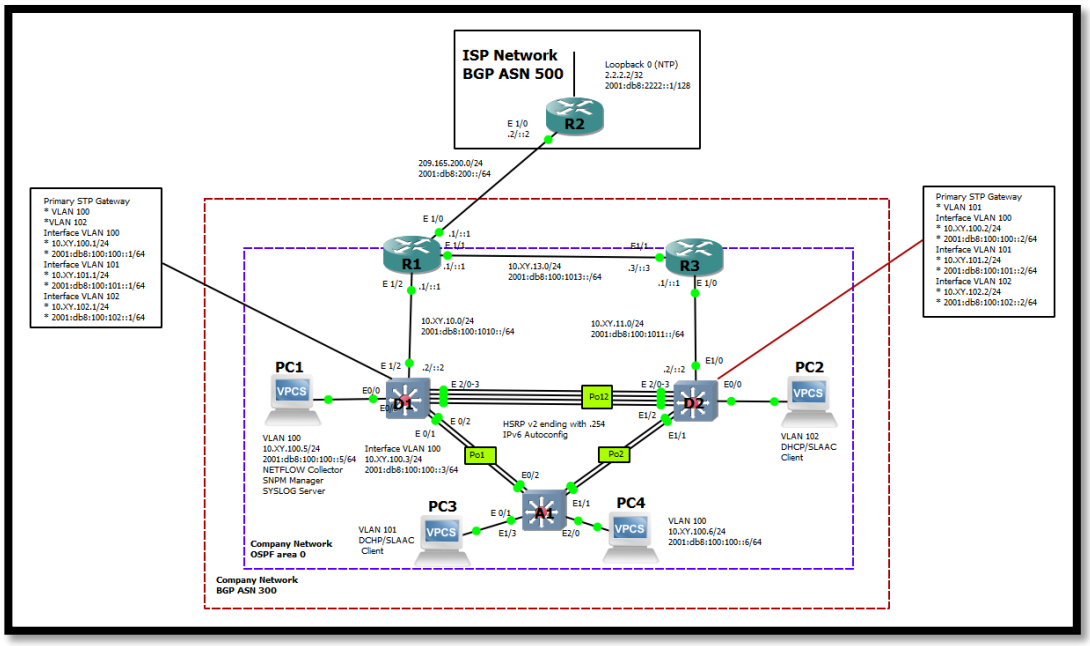

Figura 1. Topologia Escenario 1

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	10.30.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10. 30.13.1/24	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. 30.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10. 30.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10. 30.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
	VLAN 100	10. 30.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.30.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.30.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.30.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.30.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.30.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.30.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.30.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.30.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.30.100.6/24	2001:db8:100:100::6/64	EUI-64

Tabla 1. Tabla de direccionamiento

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:

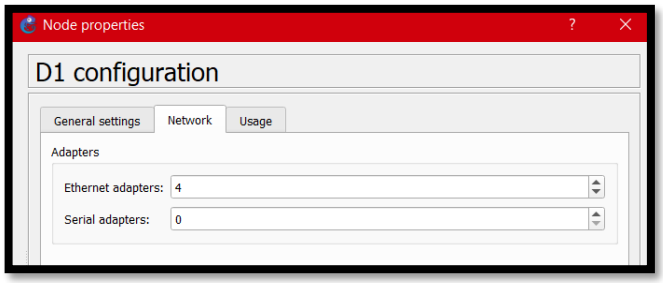

Figura 2. Plantilla Configuración fisica – Switch

And of the Routers like this:

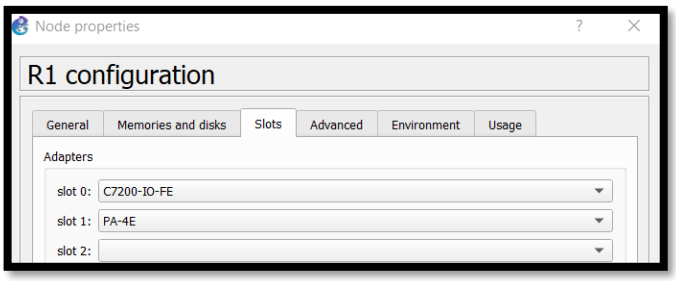

Figura 3. Plantilla Configuración física – Router

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

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.

Se realizo la configuración de acuerdo con la tabla de direccionamiento y la plantilla disponible en la guía

- *En los routers configuramos el direccionamiento IPv4 y IPv6*
- *En los switches multicapa definimos el direccionamiento IPv4 y IPv6 de las interfaces VLAN de la LAN que serán objeto los próximos pasos de configuración.*

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 10.30.10.1 255.255.255.0
 ipv6 address fe80::1:2 link-local
 ipv6 address 2001:db8:100:1010::1/64
 no shutdown
 exit
interface e1/1
 ip address 10.30.13.1 255.255.255.0
 ipv6 address fe80::1:3 link-local
 ipv6 address 2001:db8:100:1013::1/64
 no shutdown
 exit
```

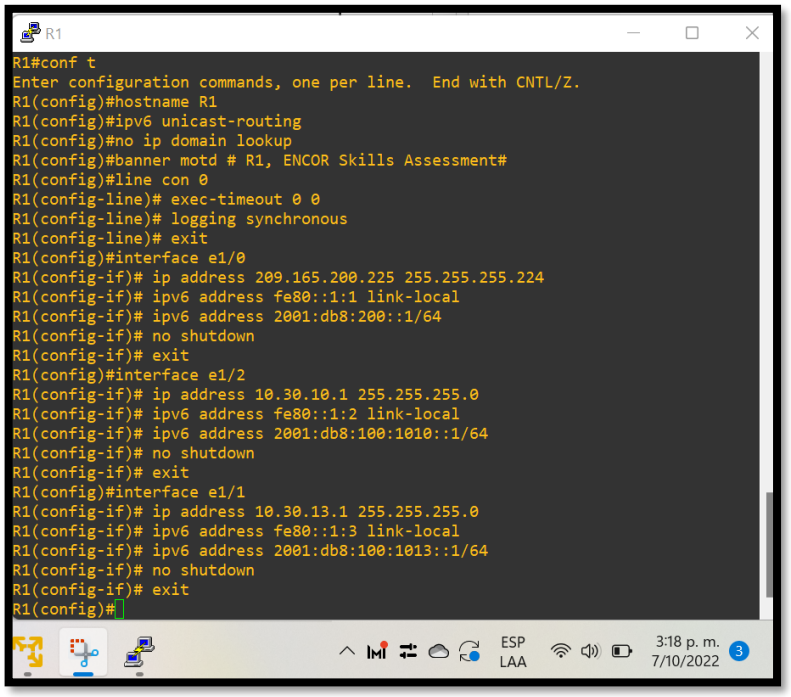

Figura 4. Configuración de direccionamiento - R1

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
```

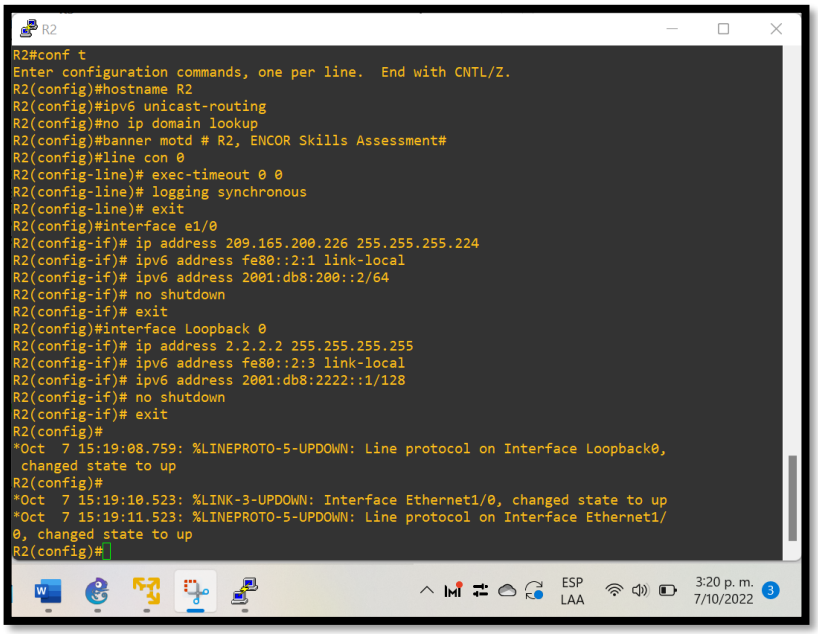

Figura 5. Configuración de Direccionamiento - R2

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 10.30.11.1 255.255.255.0
 ipv6 address fe80::3:2 link-local
 ipv6 address 2001:db8:100:1011::1/64
 no shutdown
 exit
interface e1/1
 ip address 10.30.13.3 255.255.255.0
 ipv6 address fe80::3:3 link-local
 ipv6 address 2001:db8:100:1010::2/64
 no shutdown
 exit
```

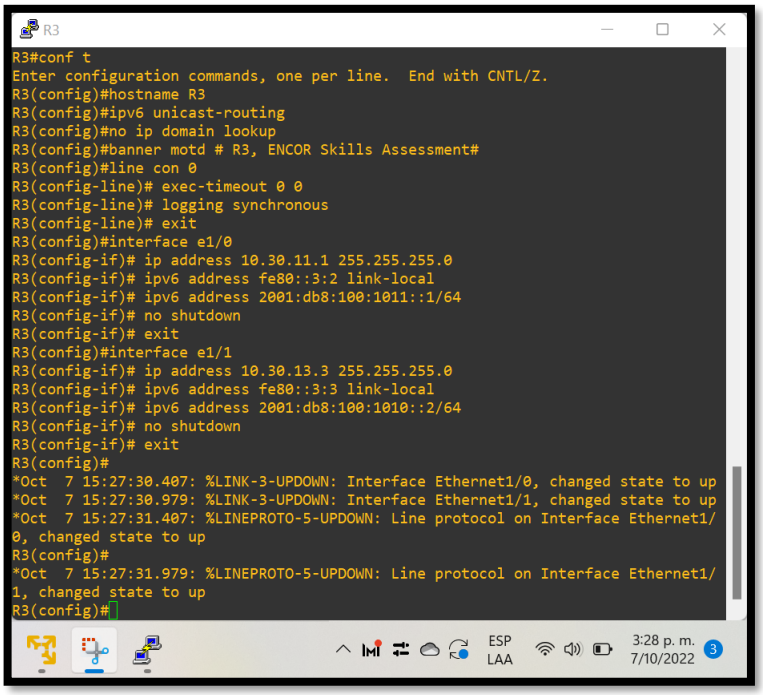

Figura 6. Configuración de Direccionamiento - R3

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 Gi1/2
```

```
 no switchport
 ip address 10.30.10.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:100:1010::2/64
 no shutdown
 exit
interface vlan 100
 ip address 10.30.100.1 255.255.255.0
 ipv6 address fe80::d1:2 link-local
 ipv6 address 2001:db8:100:100::1/64
 no shutdown
 exit
interface vlan 101
 ip address 10.30.101.1 255.255.255.0
 ipv6 address fe80::d1:3 link-local
 ipv6 address 2001:db8:100:101::1/64
 no shutdown
 exit
interface vlan 102
 ip address 10.30.102.1 255.255.255.0
 ipv6 address fe80::d1:4 link-local
 ipv6 address 2001:db8:100:102::1/64
 no shutdown
 exit
ip dhcp excluded-address 10.30.101.1 10.30.101.109
ip dhcp excluded-address 10.30.101.141 10.30.101.254
ip dhcp excluded-address 10.30.102.1 10.30.102.109
ip dhcp excluded-address 10.30.102.141 10.30.102.254
ip dhcp pool VLAN-101
 network 10.30.101.0 255.255.255.0
 default-router 10.30.101.254
 exit
ip dhcp pool VLAN-102
 network 10.30.102.0 255.255.255.0
 default-router 10.30.102.254
 exit
interface range Gi0/0-3,Gi1/0-1,Gi1/3,Gi2/0-3,Gi3/0-3
 shutdown
 exit
```

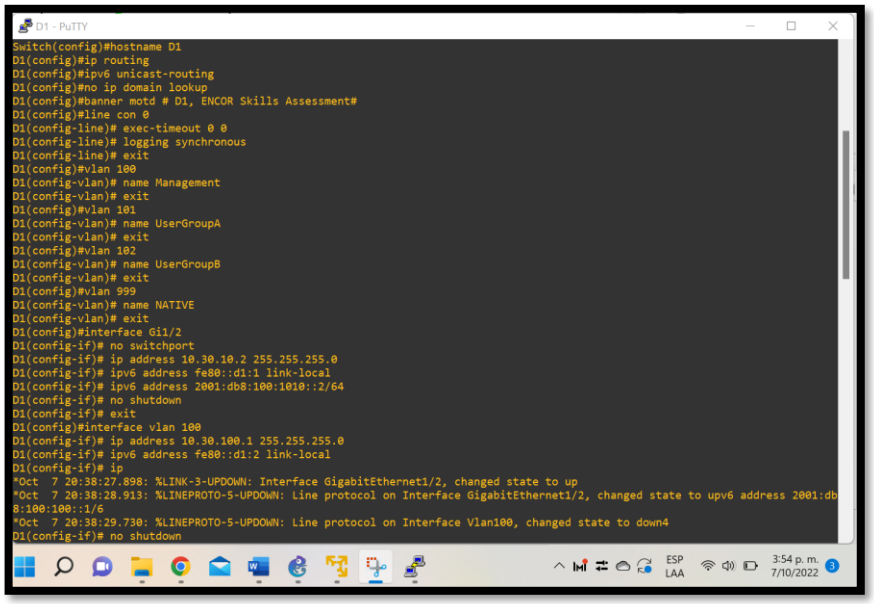

Figura 7. Configuración básica Switch D1

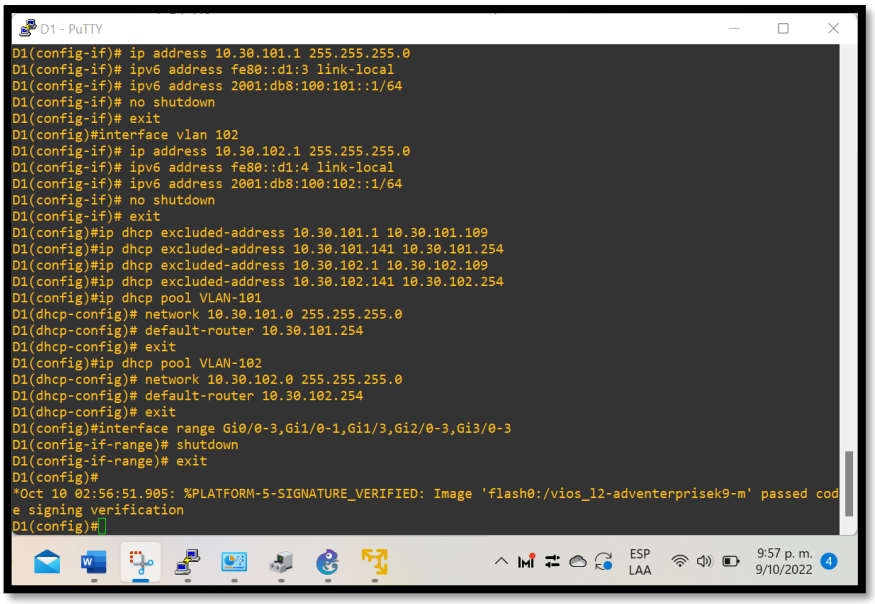

Figura 8 Configuración básica Capa 3 Switch D1

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 Gi1/0
 no switchport
 ip address 10.30.11.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:100:1011::2/64
 no shutdown
 exit
interface vlan 100
 ip address 10.30.100.2 255.255.255.0
 ipv6 address fe80::d2:2 link-local
 ipv6 address 2001:db8:100:100::2/64
 no shutdown
 exit
interface vlan 101
 ip address 10.30.101.2 255.255.255.0
 ipv6 address fe80::d2:3 link-local
 ipv6 address 2001:db8:100:101::2/64
 no shutdown
 exit
interface vlan 102
 ip address 10.30.102.2 255.255.255.0
 ipv6 address fe80::d2:4 link-local
 ipv6 address 2001:db8:100:102::2/64
 no shutdown
 exit
ip dhcp excluded-address 10.30.101.1 10.30.101.209
ip dhcp excluded-address 10.30.101.241 10.30.101.254
ip dhcp excluded-address 10.30.102.1 10.30.102.209
```

```
ip dhcp excluded-address 10.30.102.241 10.30.102.254
ip dhcp pool VLAN-101
 network 10.30.101.0 255.255.255.0
 default-router 10.30.101.254
 exit
ip dhcp pool VLAN-102
 network 10.30.102.0 255.255.255.0
 default-router 10.30.102.254
 exit
interface range Gi0/0-3,Gi1/1-3,Gi2/0-3,Gi3/0-3
 shutdown
 exit
```

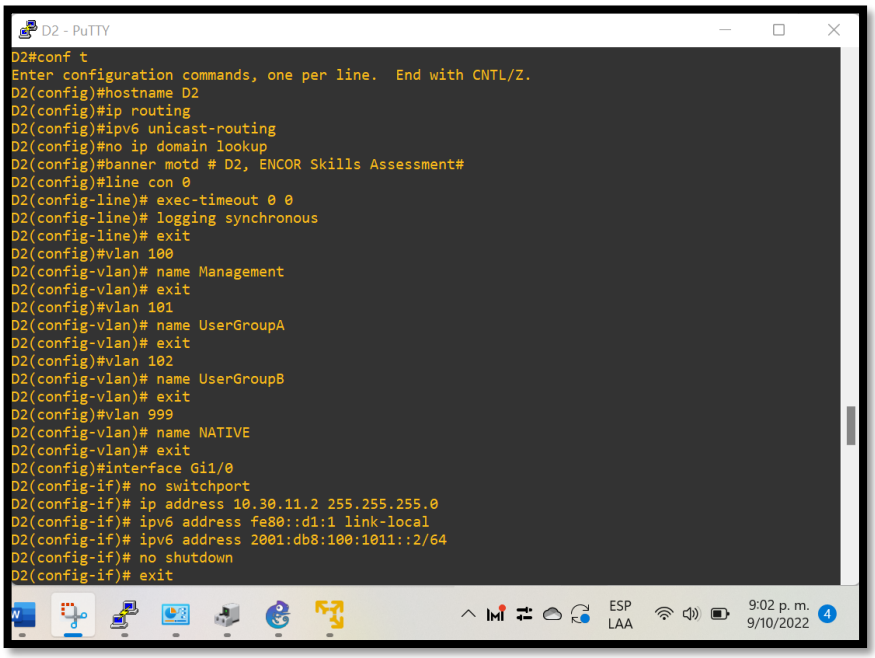

Figura 9. Configuración básica Switch D2

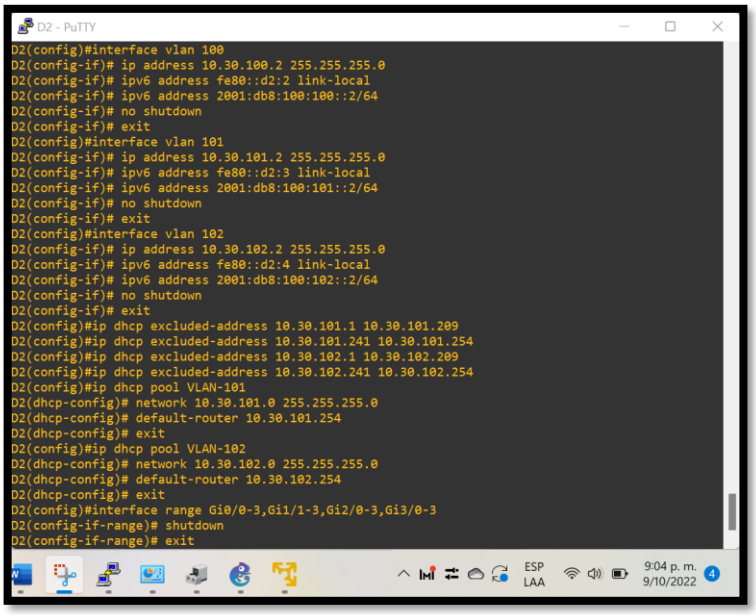

Figura 10. Configuración básica Capa 3 Switch D2

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 10.30.100.3 255.255.255.0
 ipv6 address fe80::a1:1 link-local
 ipv6 address 2001:db8:100:100::3/64
 no shutdown
```

```
 exit
interface range Gi0/0,Gi0/3,Gi1/0,Gi2/1-3,Gi3/0-3
 shutdown
 exit
```

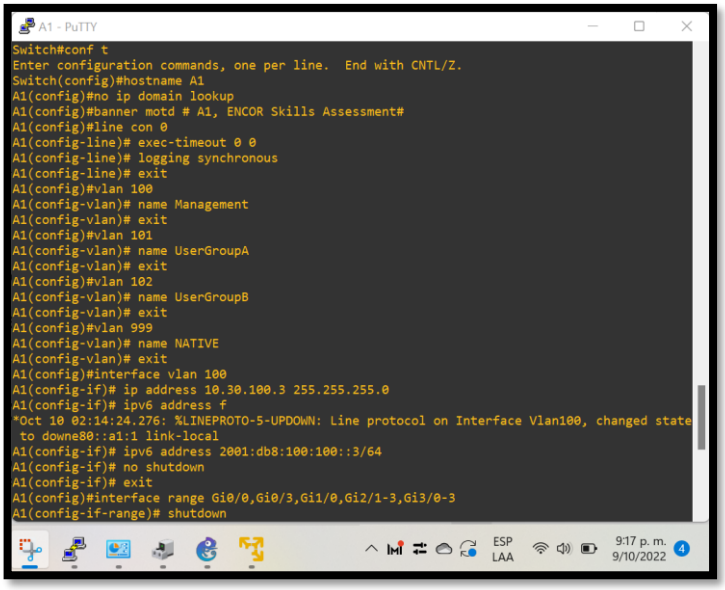

Figura 11. Configuración básica Switch A1

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

c. Configure PC 1 and PC 4 host addressing as shown in the addressing table. Assign a default gateway address of 10.30.100.254 which will be the HSRP virtual IP address used in Part 4.

```
PC1> ip 10.30.100.4/24 10.30.100.254
```

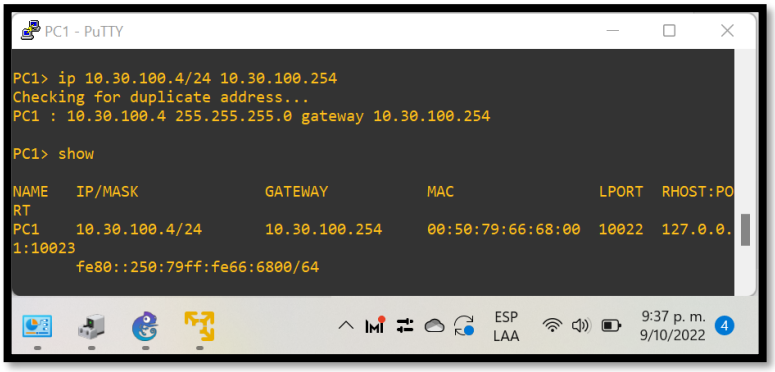

Figura 12. Configuración PC1

```
PC4> ip 10.30.100.6/24 10.30.100.254
```

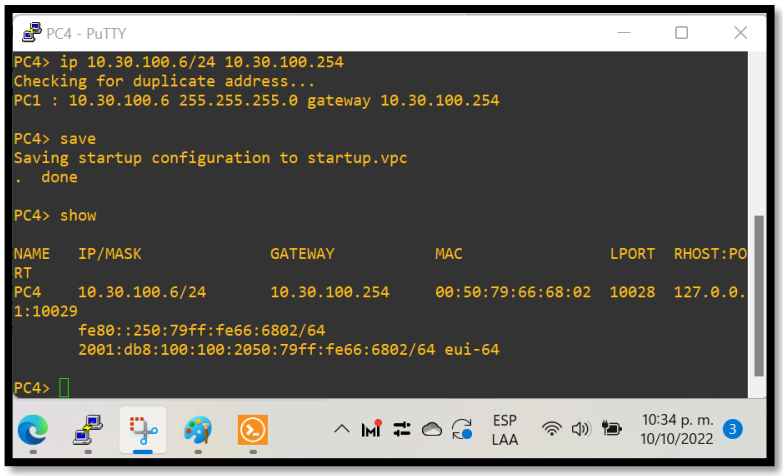

Figura 13. Configuración PC 4

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:

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

Task#	Task	Specification	Points
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
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: 10.30.100.1 • D2: 10.30.100.2 • PC4: 10.30.100.6 PC2 should successfully ping: • D1: 10.30.102.1 • D2: 10.30.102.2 PC3 should successfully ping: • D1: 10.30.101.1 • D2: 10.30.101.2 PC4 should successfully ping: • D1: 10.30.100.1 • D2: 10.30.100.2 • PC1: 10.30.100.5	1

Tabla 2. Tabla de Configuración

Configuración de Equipos

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

Switch D1

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
```

```
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
```

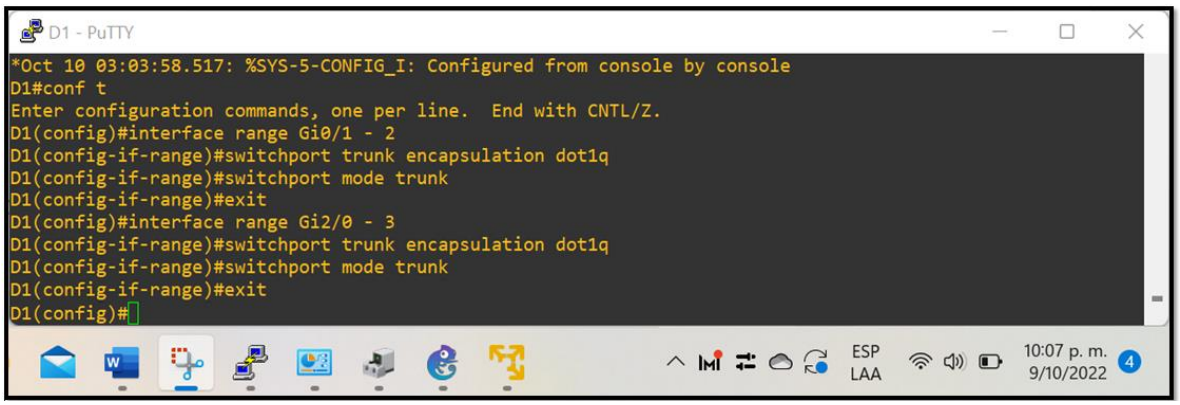

Figura 14. Configuración 802.1q Switch D1

Switch D2

```
interface GigabitEthernet1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet1/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet2/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
```

```
interface GigabitEthernet2/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
```

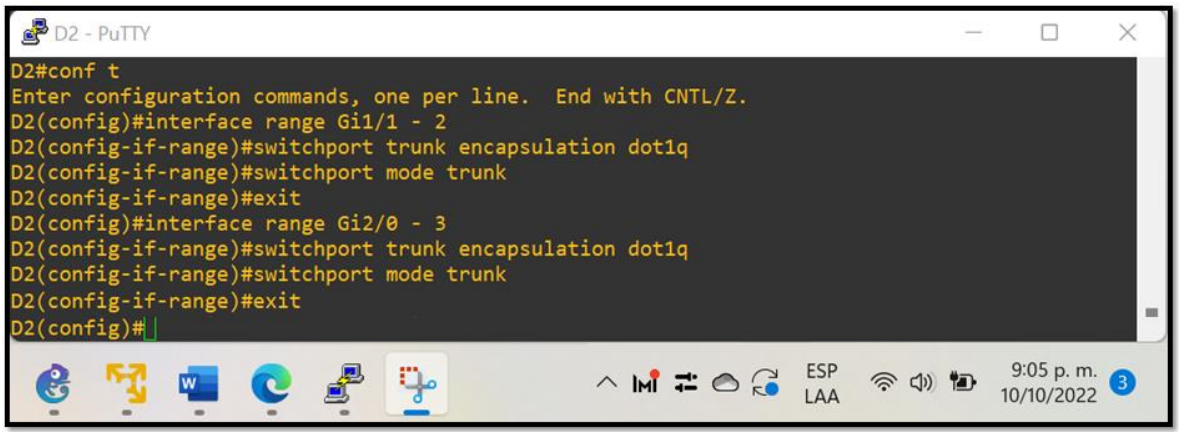

Figura 15. Configuración 802.1q Switch D2

Switch A1

```
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
negotiation auto
!
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
switchport mode trunk
negotiation auto
!
interface GigabitEthernet1/1
switchport trunk encapsulation dot1q
switchport mode trunk
negotiation auto
!
interface GigabitEthernet1/2
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
negotiation auto
!
```

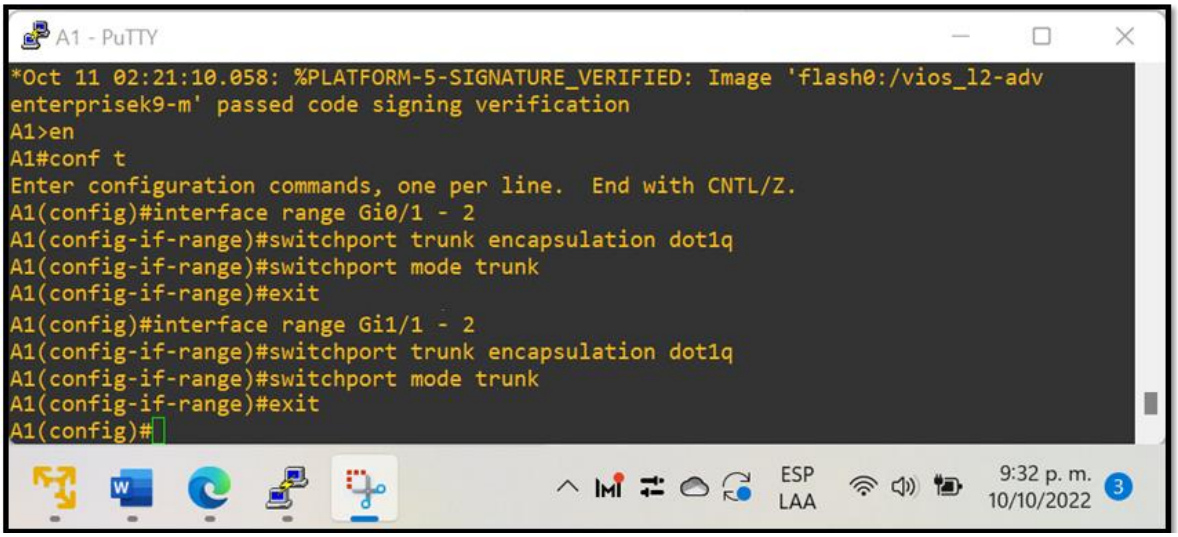

Figura 16. Configuración 802.1q Switch A1

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

Switch D1

```
interface GigabitEthernet0/1
 switchport trunk native vlan 999
!
interface GigabitEthernet0/2
 switchport trunk native vlan 999
!
interface GigabitEthernet2/0
 switchport trunk native vlan 999
!
interface GigabitEthernet2/1
 switchport trunk native vlan 999
!
interface GigabitEthernet2/2
 switchport trunk native vlan 999
!
```

```
interface GigabitEthernet2/3
 switchport trunk native vlan 999
!
```

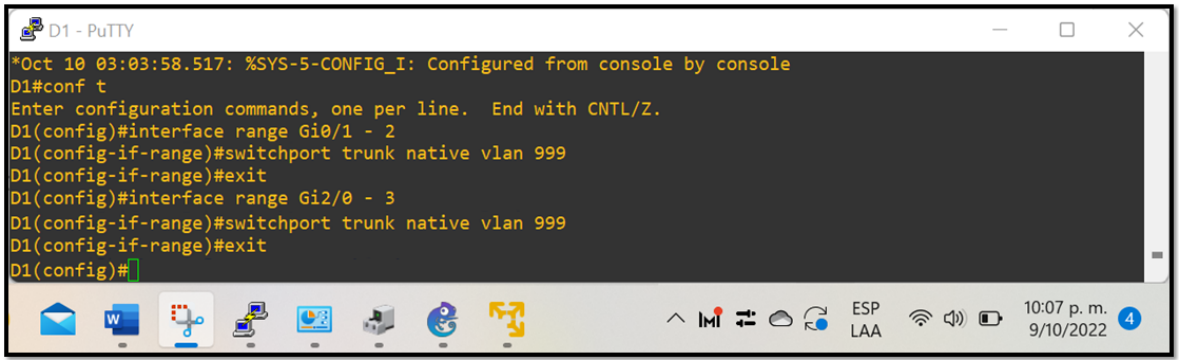

Figura 17. Configuración VLAN Nativa Switch D1

Switch D2

```
interface GigabitEthernet1/1
 switchport trunk native vlan 999
!
interface GigabitEthernet1/2
 switchport trunk native vlan 999
!
interface GigabitEthernet2/0
 switchport trunk native vlan 999
!
interface GigabitEthernet2/1
 switchport trunk native vlan 999
!
interface GigabitEthernet2/2
 switchport trunk native vlan 999
!
interface GigabitEthernet2/3
 switchport trunk native vlan 999
!
```

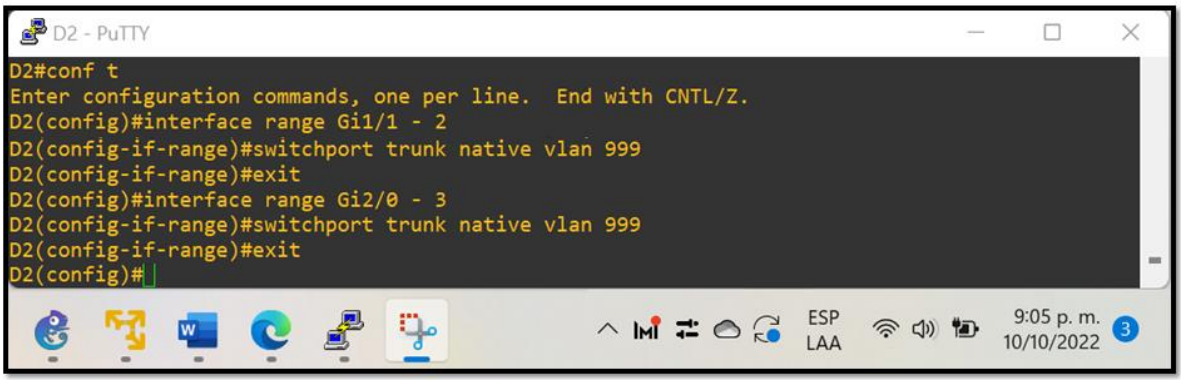

Figura 18. Configuración VLAN Nativa Switch D2

Switch A1

```
interface GigabitEthernet0/1
switchport trunk native vlan 999
!
interface GigabitEthernet0/2
switchport trunk native vlan 999
!
interface GigabitEthernet1/1
switchport trunk native vlan 999
!
interface GigabitEthernet1/2
switchport trunk native vlan 999
!
```

Figura 19. Configuración VLAN Nativa Switch D2

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

Switch D1

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

Figura 20. Habilitación de protocolo Spanning-Tree Switch D1

Switch D2

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

Figura 21. Habilitación de protocolo Spanning-Tree Switch D2

Switch A1

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

Figura 22. Habilitación de protocolo Spanning-Tree Protocol Switch A1

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.

Switch D1

```
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
```

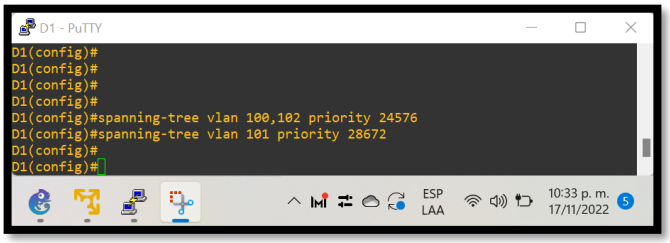

Figura 23. Configuración root bridge – Switch D1

Switch D2

```
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
```

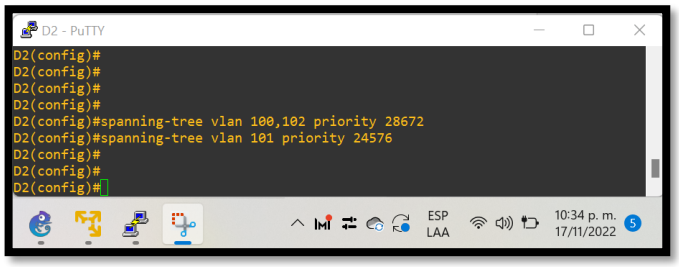

Figura 24. Configuración root bridge – Switch D2

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

Switch D1

```
interface GigabitEthernet0/1
channel-group 1 mode active
!
interface GigabitEthernet0/2
channel-group 1 mode active
!
interface GigabitEthernet2/0
channel-group 12 mode active
!
interface GigabitEthernet2/1
```

```
channel-group 12 mode active
!
interface GigabitEthernet2/2
channel-group 12 mode active
!
interface GigabitEthernet2/3
channel-group 12 mode active
!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
!
interface Port-channel12
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport mode trunk
```

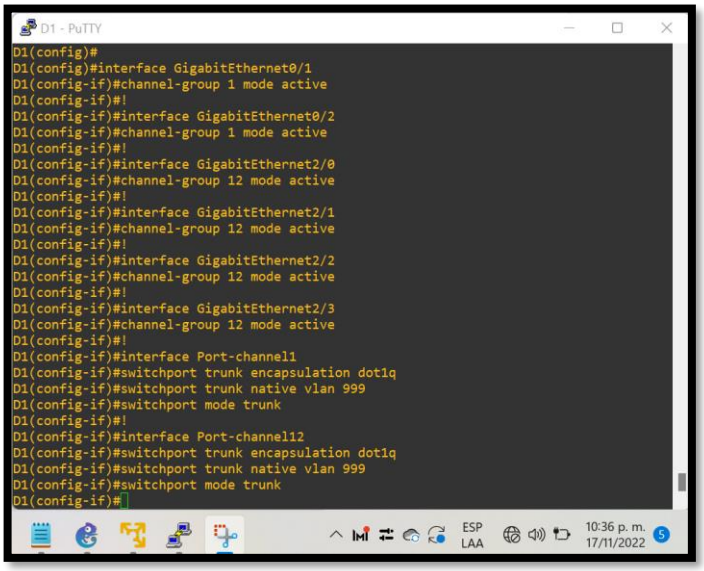

Figura 25. Creación LACP EtherChannels – Switch D1

Switch D2

```
interface GigabitEthernet1/1
 channel-group 2 mode active
```

```
!
interface GigabitEthernet1/2
 channel-group 2 mode active
!
interface GigabitEthernet2/0
 channel-group 12 mode active
!
interface GigabitEthernet2/1
 channel-group 12 mode active
!
interface GigabitEthernet2/2
 channel-group 12 mode active
!
interface GigabitEthernet2/3
 channel-group 12 mode active
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Port-channel12
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
```

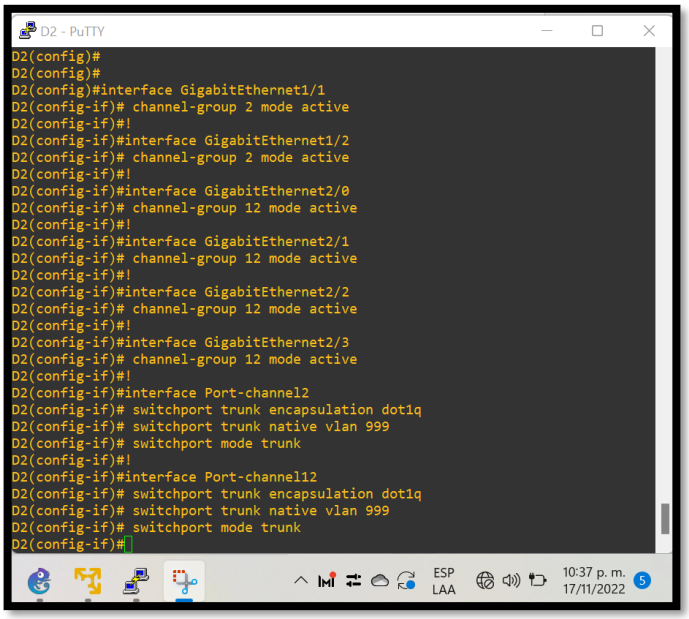

Figura 26. Creación LACP EtherChannels – Switch D2

Switch A1

```
interface GigabitEthernet0/1
channel-group 1 mode active
!
interface GigabitEthernet0/2
channel-group 1 mode active
!
interface GigabitEthernet1/1
channel-group 2 mode active
!
interface GigabitEthernet1/2
 channel-group 2 mode active
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
```

```
switchport mode trunk
```

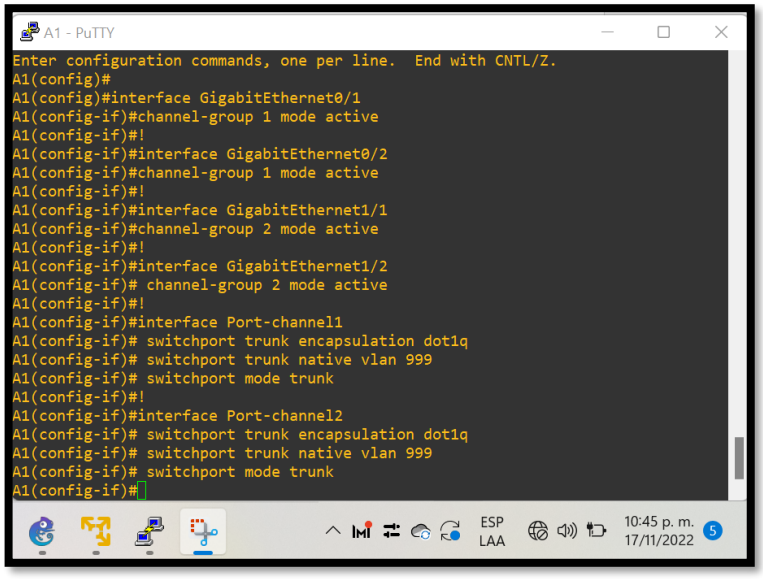

Figura 27. Creación LACP EtherChannels – Switch A1

Se procede a encender los puertos troncales que conectan los switches y verificar el estado de cada PortChannel

Switch D1

```
D1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG
```

```
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------------
----------

1      Po1(SU)          LACP      Gi0/1(P)    Gi0/2(P)
12     Po12(SU)         LACP      Gi2/0(P)    Gi2/1(P)    Gi2/2(P)
                                  Gi2/3(P)
```

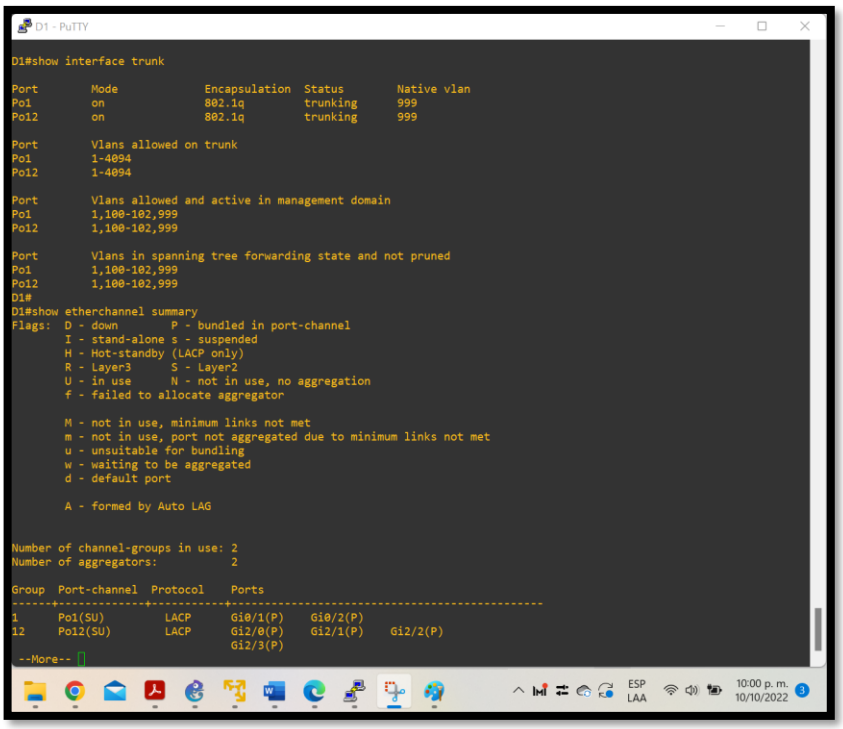

Figura 28. Verificación de estado de cada PortChannel – Switch D1

Switch D2

```
D2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
```

```
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------------
----------
2      Po2(SU)         LACP      Gi1/1(P)    Gi1/2(P)
12     Po12(SU)        LACP      Gi2/0(P)    Gi2/1(P)    Gi2/2(P)
                                 Gi2/3(P)
```

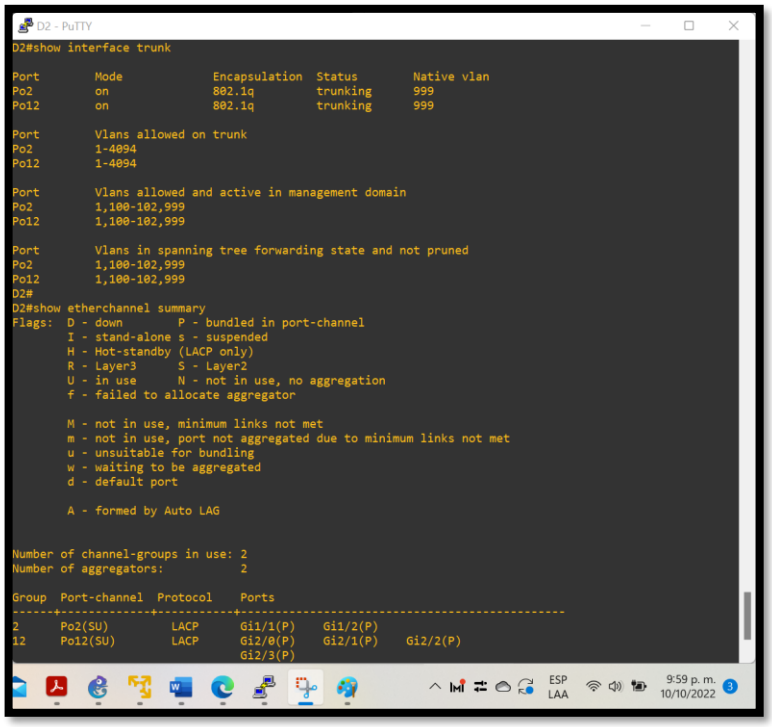

Figura 29. Verificación de estado de cada PortChannel – Switch D2

Switch A1

```
A1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG
```

```
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
----------
1      Po1(SU)          LACP       Gi0/1(P)     Gi0/2(P)
2      Po2(SU)          LACP       Gi1/1(P)     Gi1/2(P)
```

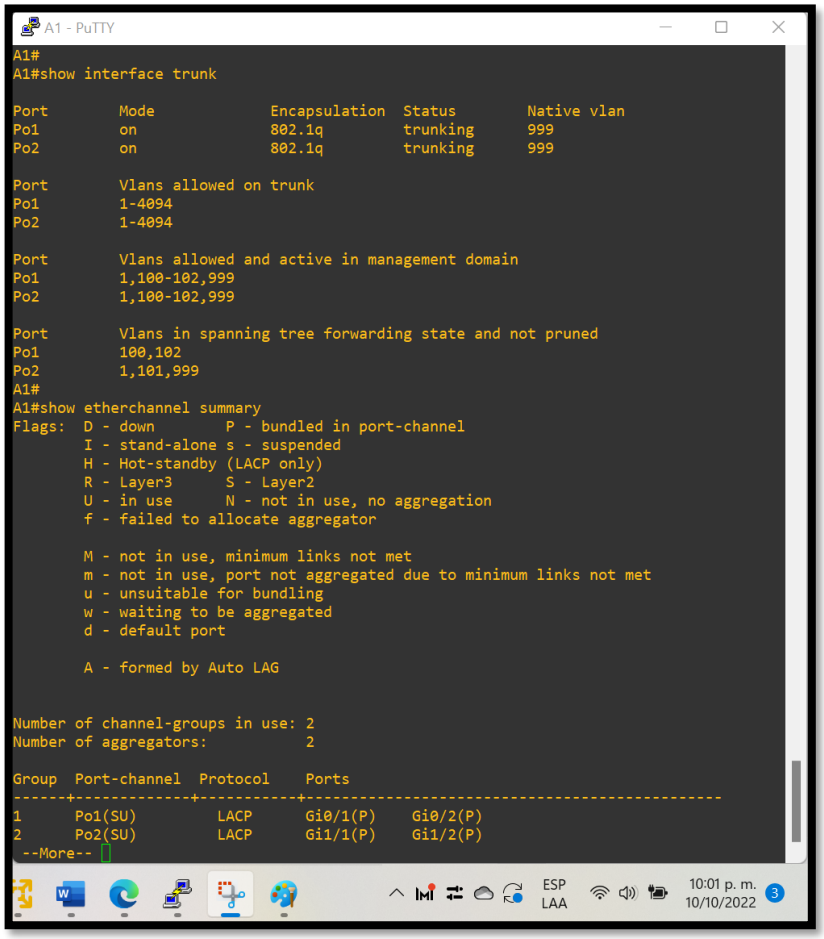

Figura 30. Verificación de estado de cada PortChannel – Switch A1

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

Switch D1

```
interface GigabitEthernet0/0
switchport access vlan 100
switchport mode access
negotiation auto
spanning-tree portfast edge
```

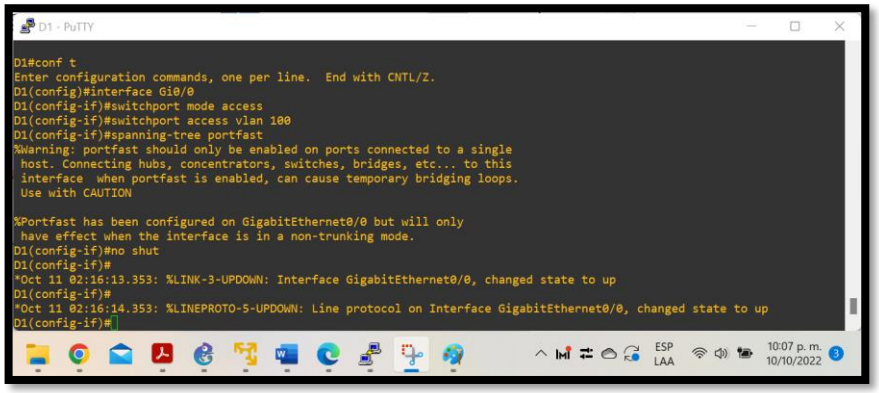

Figura 31. Configuración puertos de Acceso – Switch D1

Switch D2

```
interface GigabitEthernet0/0
switchport access vlan 102
switchport mode access
negotiation auto
spanning-tree portfast edge
```

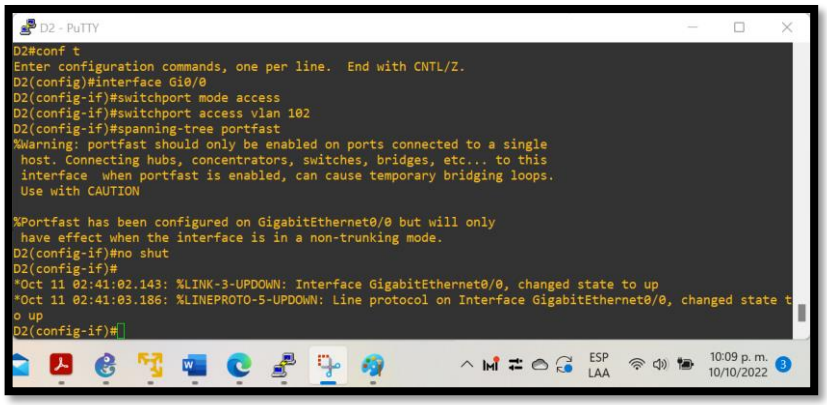

Figura 32. Configuración puertos de Acceso – Switch D2

Switch A1

```
interface GigabitEthernet1/3
switchport access vlan 101
switchport mode access
negotiation auto
panning-tree portfast edge
!
interface GigabitEthernet2/0
switchport access vlan 100
switchport mode access
negotiation auto
spanning-tree portfast edge
```

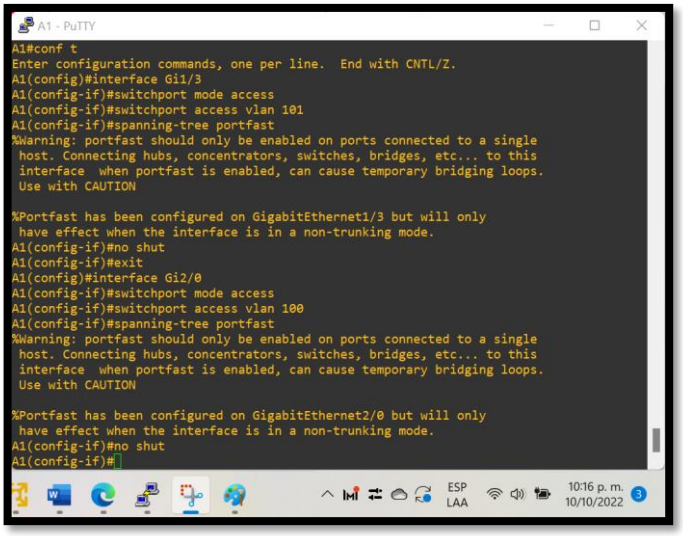

Figura 33. Configuración puertos de Acceso – Switch A1

2.7 Verify IPv4 DHCP services: PC2 and PC3 are DHCP clients and should be receiving valid IPv4 addresses.

Se habilita DHCP en los PC2 y PC3 y verifico que hayan tomado el direccionamiento definido en el pool

```
PC3> ip dhcp
DORA IP 10.30.101.110/24 GW 10.30.101.254
```

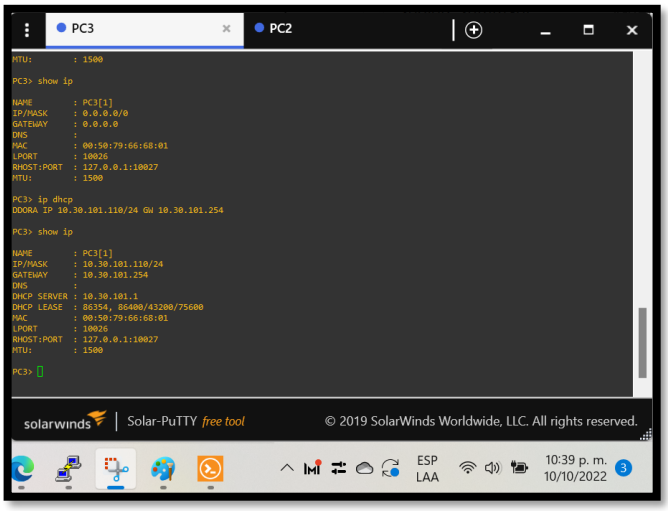

Figura 34. Habilitación DHCP – PC3

IP: 10.30.101.110/24

GW: 10.30.101.254

```
PC2> ip dhcp
DORA IP 10.30.102.110/24 GW 10.30.102.254
```

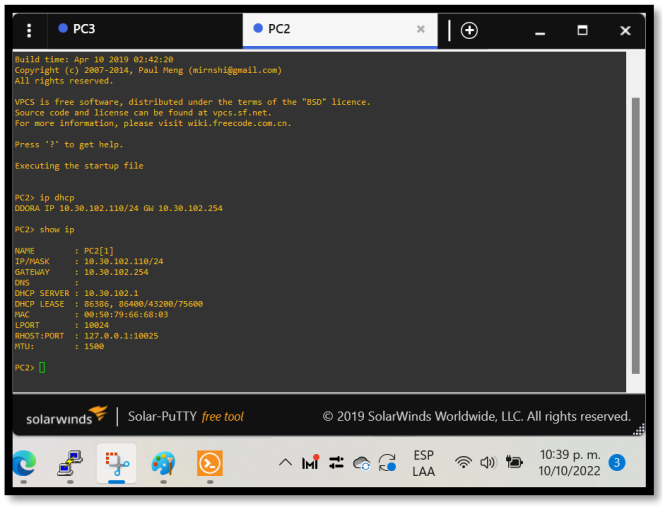

Figura 35. Habilitación DHCP – PC2

IP: 10.30.102.110/24

GW: 10.30.102.254

2.8 Verify local LAN connectivity

PC1 should successfully ping:

D1: 10.30.100.1
D2: 10.30.100.2
PC4: 10.30.100.6

```
PC1> ping 10.30.100.1
84 bytes from 10.30.100.1 icmp_seq=1 ttl=255 time=751.055 ms
84 bytes from 10.30.100.1 icmp_seq=2 ttl=255 time=329.231 ms
84 bytes from 10.30.100.1 icmp_seq=3 ttl=255 time=138.079 ms
84 bytes from 10.30.100.1 icmp_seq=4 ttl=255 time=187.044 ms
84 bytes from 10.30.100.1 icmp_seq=5 ttl=255 time=322.783 ms

PC1> ping 10.30.100.2
84 bytes from 10.30.100.2 icmp_seq=1 ttl=255 time=687.229 ms
84 bytes from 10.30.100.2 icmp_seq=2 ttl=255 time=245.189 ms
84 bytes from 10.30.100.2 icmp_seq=3 ttl=255 time=202.603 ms
84 bytes from 10.30.100.2 icmp_seq=4 ttl=255 time=125.198 ms
84 bytes from 10.30.100.2 icmp_seq=5 ttl=255 time=222.155 ms

PC1> ping 10.30.100.6
84 bytes from 10.30.100.6 icmp_seq=1 ttl=64 time=68.988 ms
84 bytes from 10.30.100.6 icmp_seq=2 ttl=64 time=59.965 ms
84 bytes from 10.30.100.6 icmp_seq=3 ttl=64 time=62.004 ms
84 bytes from 10.30.100.6 icmp_seq=4 ttl=64 time=78.488 ms
84 bytes from 10.30.100.6 icmp_seq=5 ttl=64 time=86.583 ms
```

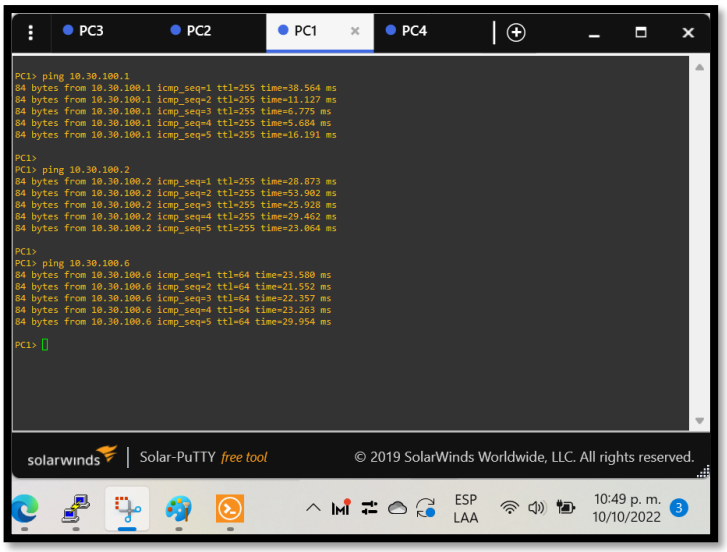

Figura 36. Verificación de conectividad – PC1

PC2 should successfully ping:

D1: 10.30.102.1
D2: 10.30.102.2

```
PC2> ping 10.30.102.1
84 bytes from 10.30.102.1 icmp_seq=1 ttl=255 time=295.471 ms
84 bytes from 10.30.102.1 icmp_seq=2 ttl=255 time=211.317 ms
84 bytes from 10.30.102.1 icmp_seq=3 ttl=255 time=455.042 ms
84 bytes from 10.30.102.1 icmp_seq=4 ttl=255 time=352.197 ms
84 bytes from 10.30.102.1 icmp_seq=5 ttl=255 time=174.158 ms

PC2> ping 10.30.102.2
84 bytes from 10.30.102.2 icmp_seq=1 ttl=255 time=484.156 ms
84 bytes from 10.30.102.2 icmp_seq=2 ttl=255 time=402.490 ms
84 bytes from 10.30.102.2 icmp_seq=3 ttl=255 time=423.457 ms
84 bytes from 10.30.102.2 icmp_seq=4 ttl=255 time=127.473 ms
84 bytes from 10.30.102.2 icmp_seq=5 ttl=255 time=152.528 ms
```

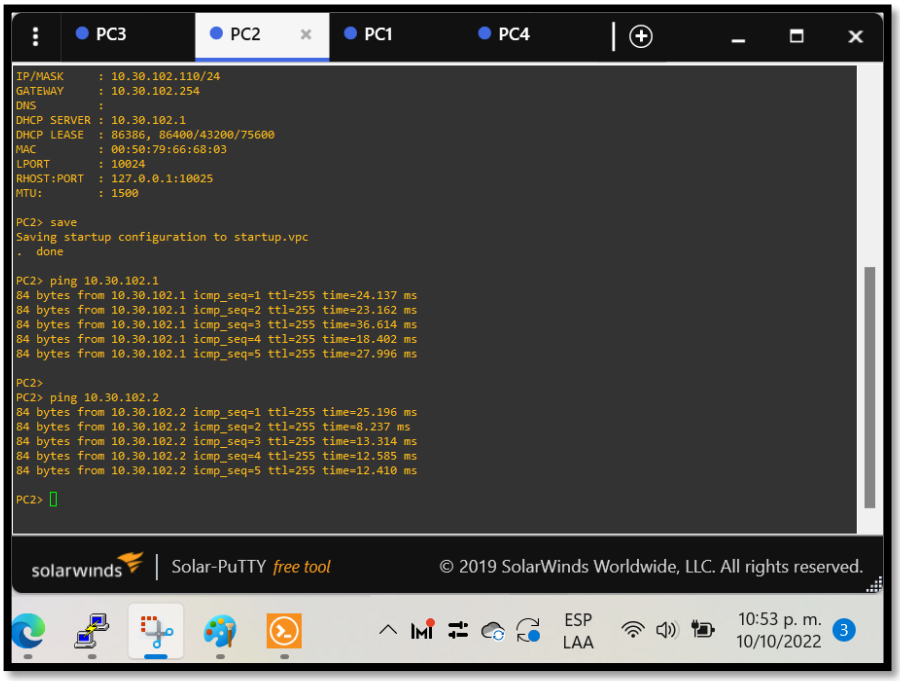

Figura 37. Verificación de conectividad – PC2

PC3 should successfully ping:

D1: 10.30.101.1
D2: 10.30.101.2

```
PC3> ping 10.30.101.1
84 bytes from 10.30.101.1 icmp_seq=1 ttl=255 time=210.094 ms
84 bytes from 10.30.101.1 icmp_seq=2 ttl=255 time=196.762 ms
84 bytes from 10.30.101.1 icmp_seq=3 ttl=255 time=250.798 ms
84 bytes from 10.30.101.1 icmp_seq=4 ttl=255 time=209.900 ms
84 bytes from 10.30.101.1 icmp_seq=5 ttl=255 time=263.184 ms

PC3>
PC3> ping 10.30.101.2
84 bytes from 10.30.101.2 icmp_seq=1 ttl=255 time=128.004 ms
```

```
84 bytes from 10.30.101.2 icmp_seq=2 ttl=255 time=140.095 ms
84 bytes from 10.30.101.2 icmp_seq=3 ttl=255 time=104.391 ms
84 bytes from 10.30.101.2 icmp_seq=4 ttl=255 time=243.363 ms
84 bytes from 10.30.101.2 icmp_seq=5 ttl=255 time=78.466 ms
```

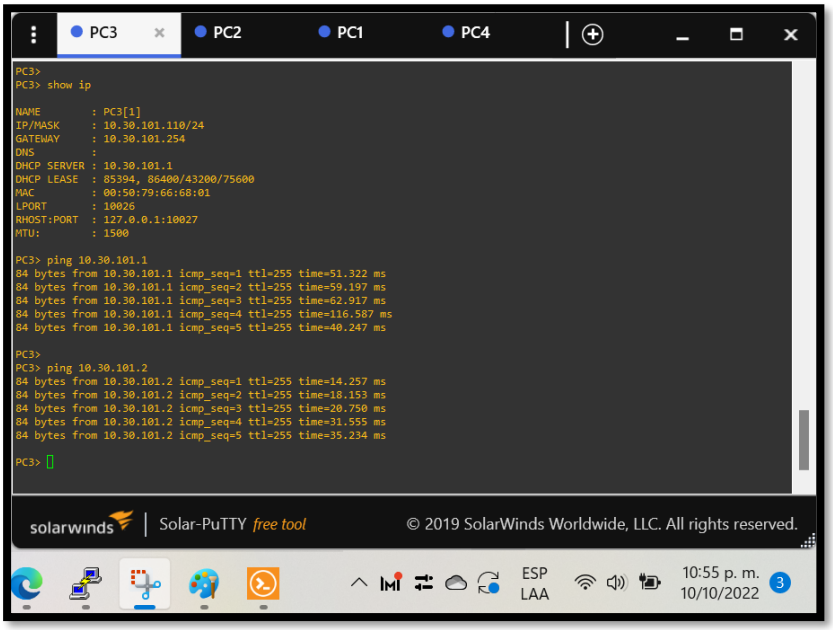

Figura 38. Verificación de conectividad – PC3

PC4 should successfully ping:

D1: 10.30.100.1
D2: 10.30.100.2
PC1: 10.30.100.5

```
PC4> ping 10.30.100.1
84 bytes from 10.30.100.1 icmp_seq=1 ttl=255 time=260.253 ms
84 bytes from 10.30.100.1 icmp_seq=2 ttl=255 time=386.472 ms
84 bytes from 10.30.100.1 icmp_seq=3 ttl=255 time=290.373 ms
84 bytes from 10.30.100.1 icmp_seq=4 ttl=255 time=274.351 ms
84 bytes from 10.30.100.1 icmp_seq=5 ttl=255 time=361.987 ms

PC4> ping 10.30.100.2
84 bytes from 10.30.100.2 icmp_seq=1 ttl=255 time=302.379 ms
84 bytes from 10.30.100.2 icmp_seq=2 ttl=255 time=298.774 ms
84 bytes from 10.30.100.2 icmp_seq=3 ttl=255 time=126.132 ms
84 bytes from 10.30.100.2 icmp_seq=4 ttl=255 time=365.701 ms
84 bytes from 10.30.100.2 icmp_seq=5 ttl=255 time=227.042 ms

PC4> ping 10.30.100.5
84 bytes from 10.30.100.5 icmp_seq=1 ttl=64 time=30.633 ms
84 bytes from 10.30.100.5 icmp_seq=2 ttl=64 time=84.990 ms
84 bytes from 10.30.100.5 icmp_seq=3 ttl=64 time=82.448 ms
84 bytes from 10.30.100.5 icmp_seq=4 ttl=64 time=92.217 ms
```

```
84 bytes from 10.30.100.5 icmp_seq=5 ttl=64 time=94.666 ms
```

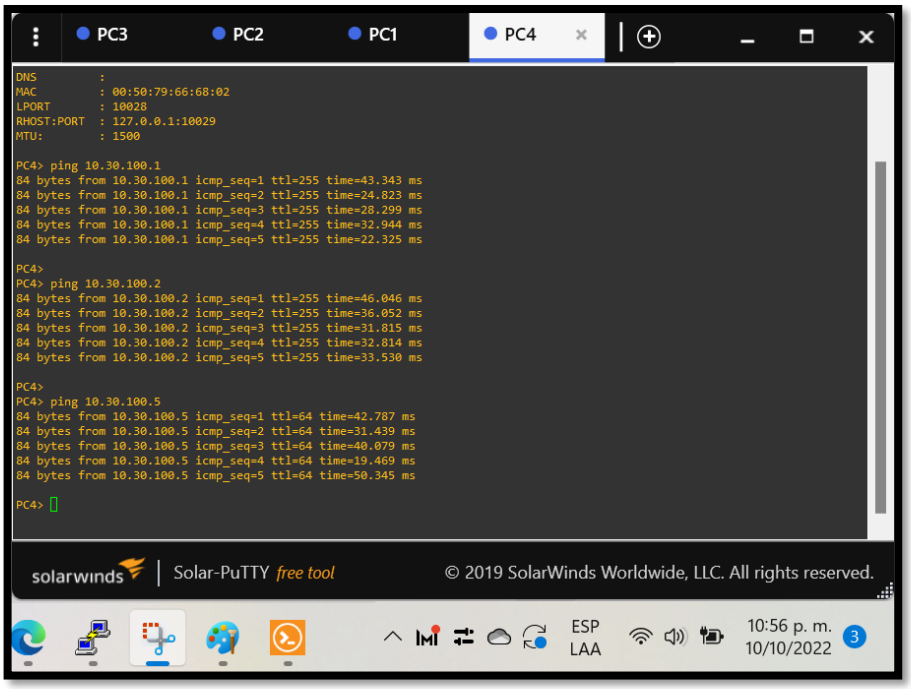

Figura 39. Verificación de conectividad – PC4

2. ESCENARIO 2

ENCOR Skills Assessment (Scenario 2)

Continuation of the Scenario 1

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:

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 Gi1/2 • D2: All interfaces except Gi1/0	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 Gi1/2 • D2: All interfaces except Gi1/0	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 10.30.0.0/8. • 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 10.30.0.0/8 network. In IPv6 address family: • Disable the IPv4 neighbor relationship. • Enable the IPv6 neighbor relationship. • Advertise the 2001:db8:100::/48 network.	4

Tabla 3. Tabla de configuraciones Routing Protocol

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:

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

Task#	Task	Specification	Points
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 **10.30.100.254**. • 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 **10.30.101.254**. • Enable preemption. • Track object 4 to decrement by 60. Configure IPv4 HSRP group **124** for VLAN 102: • Assign the virtual IP address **10.30.102.254**. • 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: • Assign the virtual IP address using **ipv6 autoconfig**. • Set the group priority to **150**. • Enable preemption. • Track object 6 and decrement by 60.	8

Task#	Task	Specification	Points
	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 **10.30.100.254**. • Enable preemption. • Track object 4 and decrement by 60. Configure IPv4 HSRP group **114** for VLAN 101: • Assign the virtual IP address **10.30.101.254**. • 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 **10.30.102.254**. • 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**. • Enable preemption. • Track object 6 and decrement by 60.	

Tabla 4. Tabla de configuraciones first hop redundancy

Configure Routing Protocols

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 Gi1/2
- D2: All interfaces except Gi1/0

Router R1

```
router ospf 4
 router-id 0.0.4.1
 network 10.30.10.0 0.0.0.255 area 0
 network 10.30.13.0 0.0.0.255 area 0
 default-information originate
```

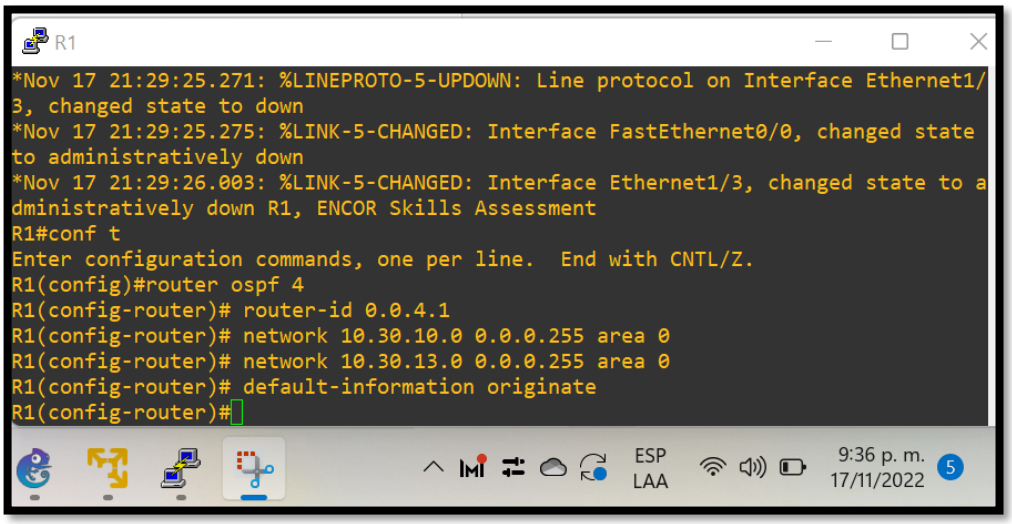

Figura 40. Configuración de OSPF v2 – Router R1

Router R3

```
router ospf 4
 router-id 0.0.4.3
 network 10.30.11.0 0.0.0.255 area 0
 network 10.30.13.0 0.0.0.255 area 0
```

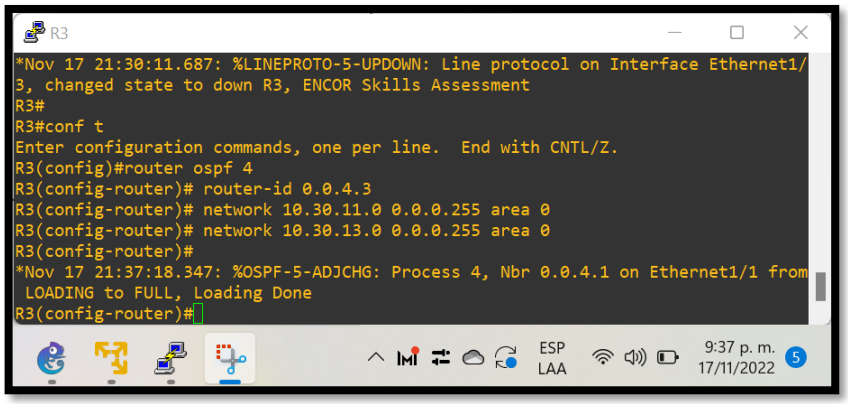

Figura 41. Configuración de OSPF v2 – Router R3

Switch D1

```
router ospf 4
 router-id 0.0.4.131
 passive-interface default
 no passive-interface GigabitEthernet1/2
 network 10.30.10.0 0.0.0.255 area 0
 network 10.30.100.0 0.0.0.255 area 0
 network 10.30.101.0 0.0.0.255 area 0
 network 10.30.102.0 0.0.0.255 area 0
```

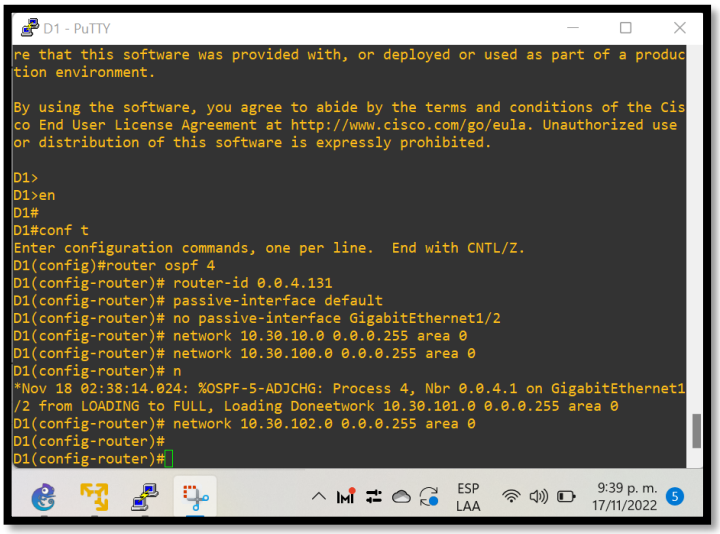

Figura 42. Configuración de OSPF v2– Switch D1

Switch D2

```
router ospf 4
 router-id 0.0.4.132
 passive-interface default
 no passive-interface GigabitEthernet1/0
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.101.0 0.0.0.255 area 0
 network 10.0.102.0 0.0.0.255 area 0
```

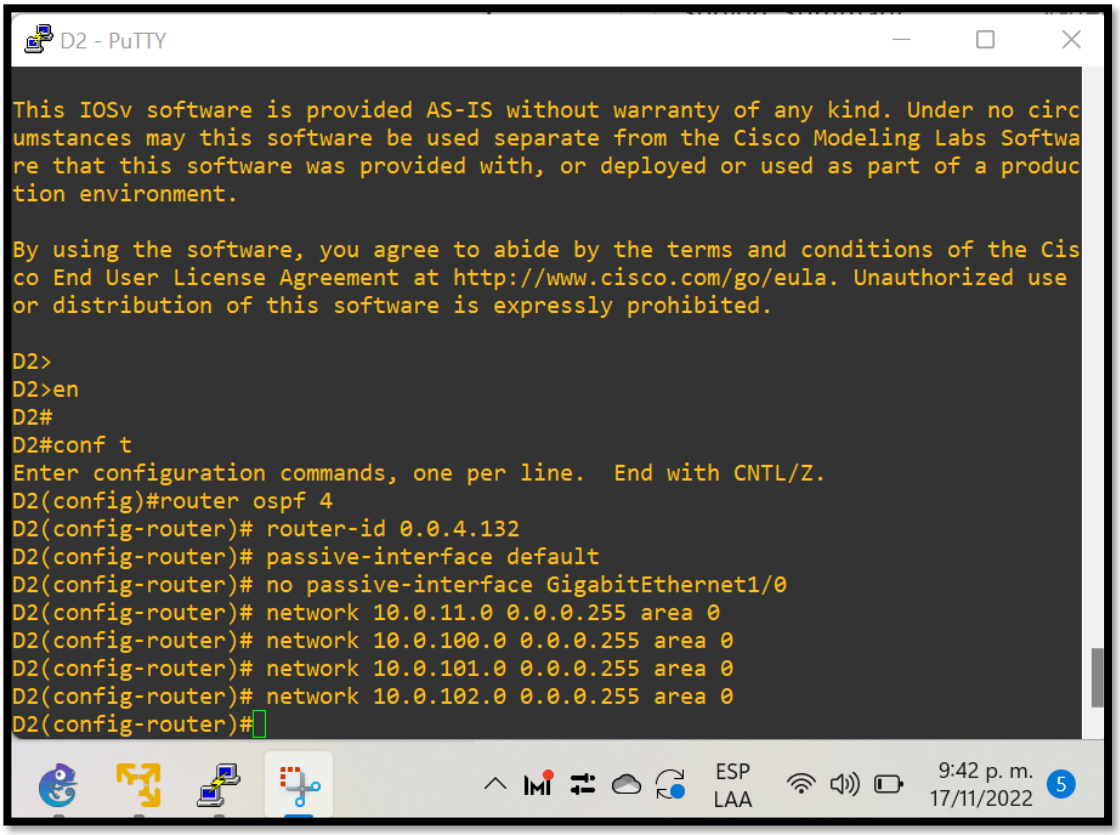

Figura 43. Configuración de OSPF v2 – Switch D2

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 Gi1/2

  D2: All interfaces except Gi1/0

Router R1

```
ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate
 exit
interface Eth1/1
 ipv6 ospf 6 area 0
 exit
interface Eth1/2
 ipv6 ospf 6 area 0
 exit
```

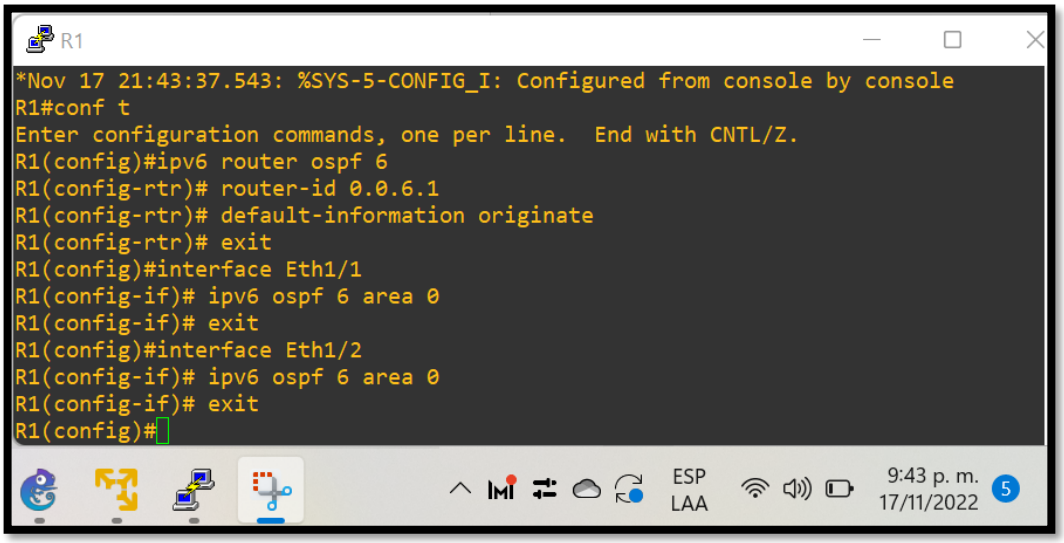

Figura 44. Configuración de OSPF v3 – Router R1

Router R3

```
ipv6 router ospf 6
 router-id 0.0.6.3
 exit
interface Eth1/0
 ipv6 ospf 6 area 0
 exit
interface Eth1/1
 ipv6 ospf 6 area 0
 exit
```

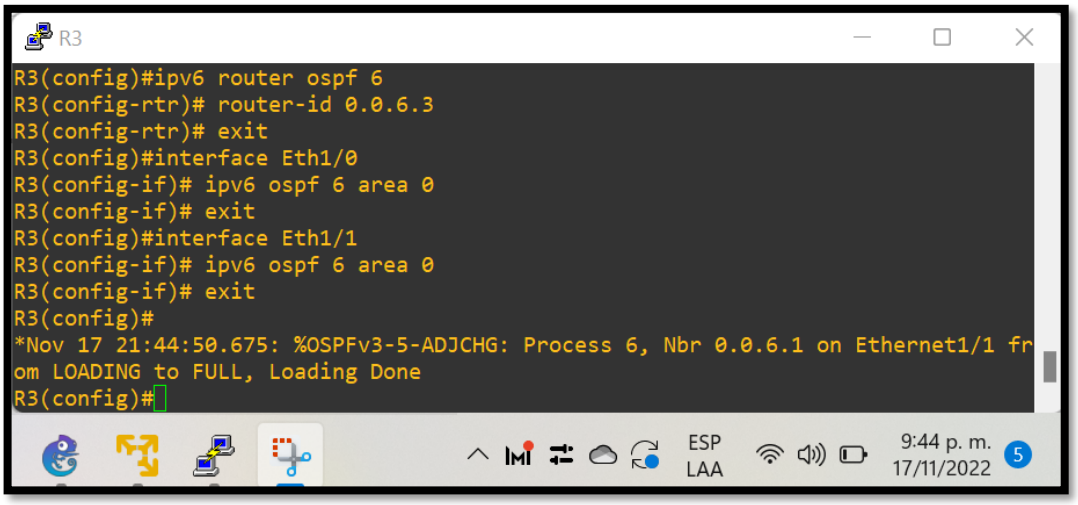

Figura 45. Configuración de OSPF v3 – Router R3

Switch D1

```
ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
 no passive-interface Gi1/2
 exit
interface Gi1/2
 ipv6 ospf 6 area 0
 exit
interface vlan 100
 ipv6 ospf 6 area 0
 exit
interface vlan 101
 ipv6 ospf 6 area 0
 exit
interface vlan 102
 ipv6 ospf 6 area 0
 exit
```

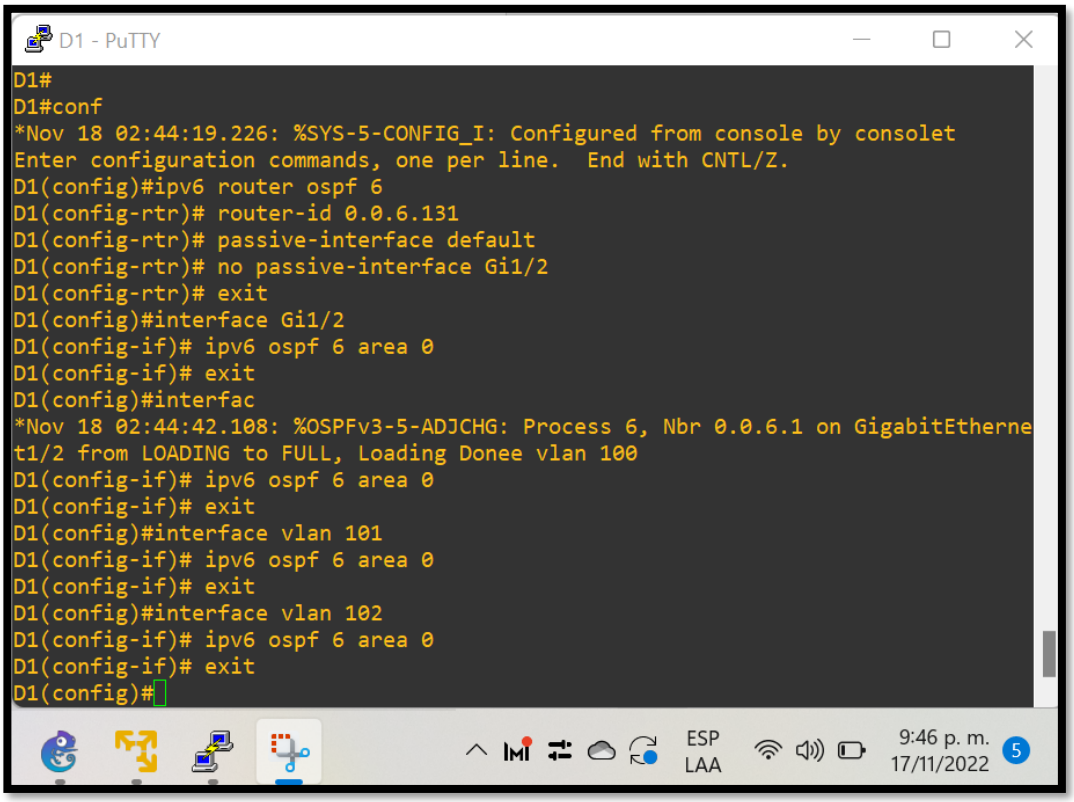

Figura 46. Configuración de OSPF v3 – Switch D1

Switch D2

```
ipv6 router ospf 6
 router-id 0.0.6.132
 passive-interface default
 no passive-interface Gi1/0
 exit
interface Gi1/0
 ipv6 ospf 6 area 0
 exit
interface vlan 100
 ipv6 ospf 6 area 0
 exit
interface vlan 101
 ipv6 ospf 6 area 0
 exit
interface vlan 102
 ipv6 ospf 6 area 0
 exit
```

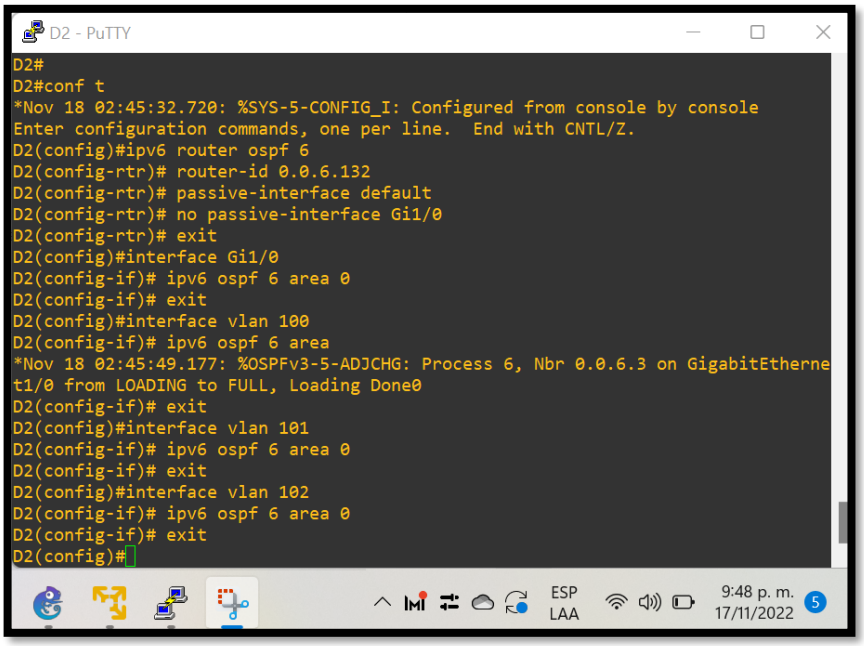

Figura 47. Configuración de OSPF v3 – Switch D2

3.3 On R2 in the "ISP Network", configure MP-BGP.

Router R2

Configure two default static routes via interface Loopback 0:

- An IPv4 default static route.
- An IPv6 default static route.

```
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
```

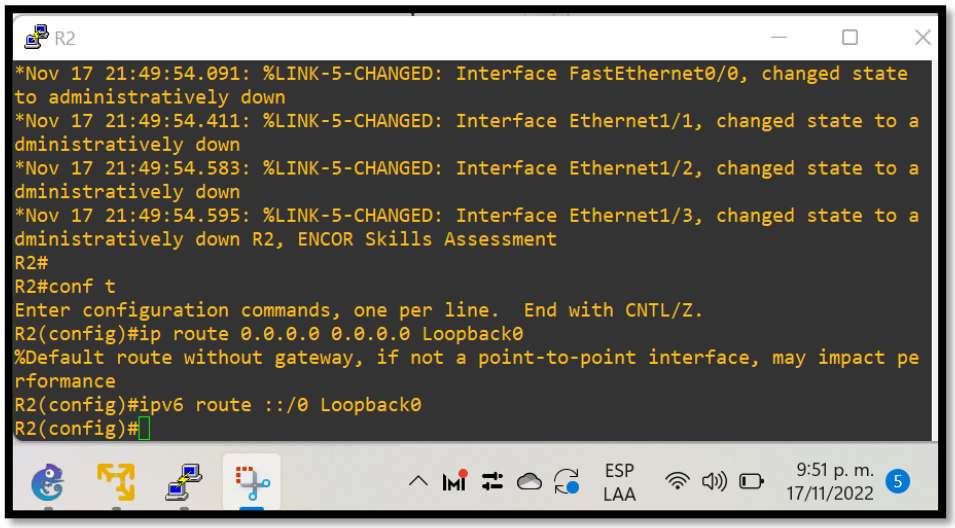

Figura 48. Configuración ruta estatica – Router R2

Configure R2 in BGP ASN **500** and use the router-id 2.2.2.2.

```
router bgp 500
 bgp router-id 2.2.2.2
```

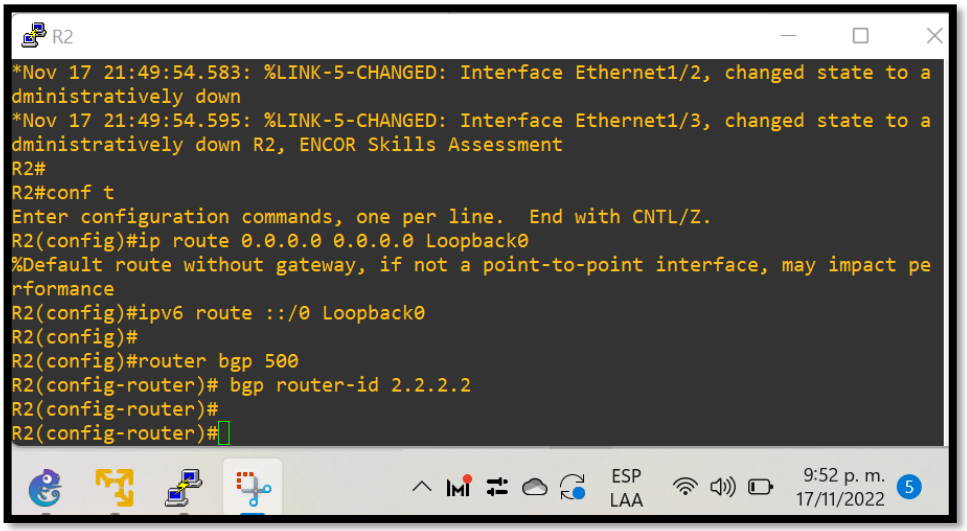

Figura 49. Configuración router ID – Router R2

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).

```
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
  network 0.0.0.0
  network 2.2.2.2 mask 255.255.255.255
  no neighbor 2001:DB8:200::1 activate
  neighbor 209.165.200.225 activate
 exit-address-family
 !
 address-family ipv6
  network ::/0
  network 2001:DB8:2222::/128
```

```
 neighbor 2001:DB8:200::1 activate
exit-address-family
```

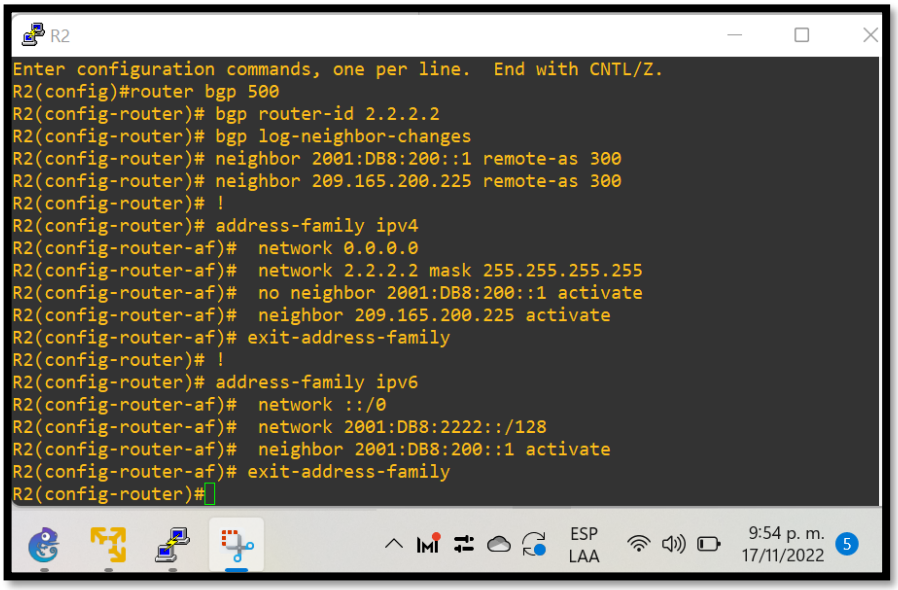

Figura 50. Configuración BGP – Router R2

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

Router R1

Configure two static summary routes to interface Null 0:

- A summary IPv4 route for 10.30.0.0/8.
- A summary IPv6 route for 2001:db8:100::/48.

```
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
```

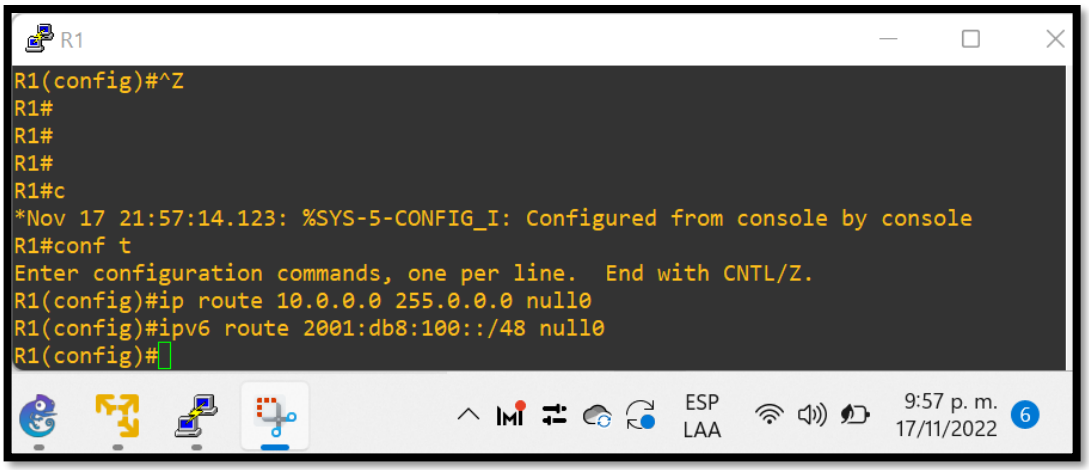

Figura 51. Configuración ruta estatica - Router R1

Configure R1 in BGP ASN **300** and use the router-id 1.1.1.1.

```
router bgp 300
 bgp router-id 1.1.1.1
```

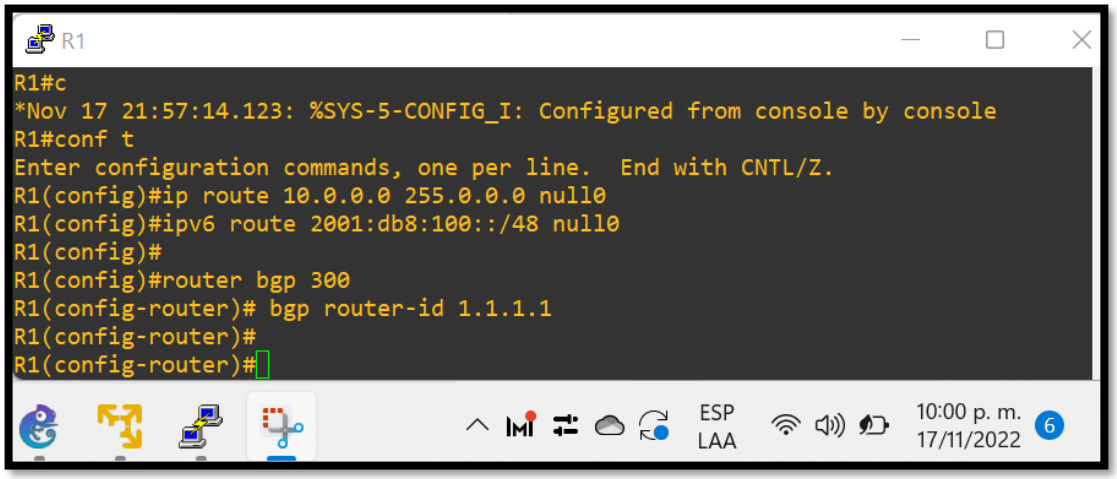

Figura 52. Configuración router ID - Router R1

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 10.30.0.0/8 network.

In IPv6 address family:

- Disable the IPv4 neighbor relationship.
- Enable the IPv6 neighbor relationship.

  Advertise the 2001:db8:100::/48 network.

```
router bgp 300
 bgp router-id 1.1.1.1
 neighbor 209.165.200.226 remote-as 500
 neighbor 2001:db8:200::2 remote-as 500
 address-family ipv4 unicast
  neighbor 209.165.200.226 activate
  no neighbor 2001:db8:200::2 activate
  network 10.0.0.0 mask 255.0.0.0
  exit-address-family
 address-family ipv6 unicast
```

```
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family
```

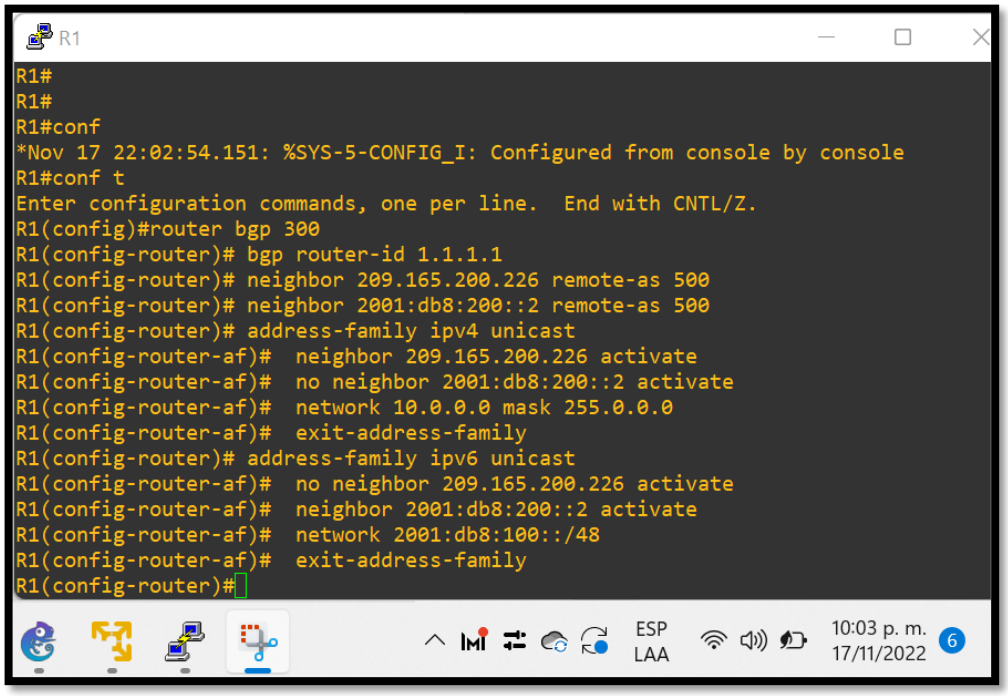

Figura 53. Configuración BGP - Router R1

Part 4: Configure First-Hop Redundancy

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

Switch D1

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.

```
ip sla 4
 icmp-echo 10.30.10.1
 frequency 5
 exit
ip sla 6
 icmp-echo 2001:db8:100:1010::1
 frequency 5
```

```
 exit


ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
```

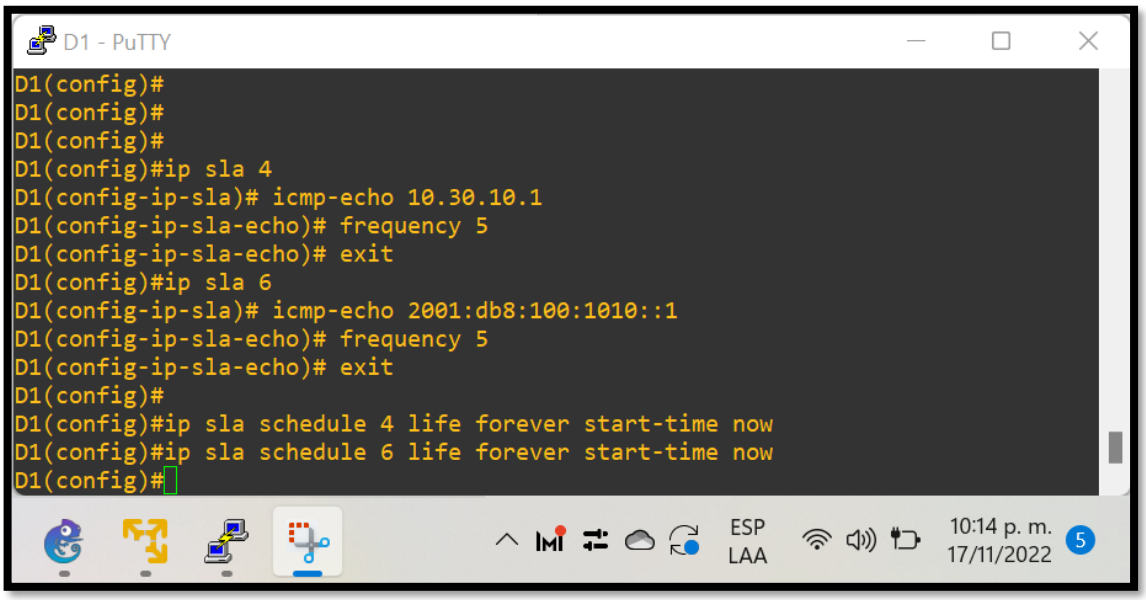

Figura 54. Configuración IP SLA – Switch D1

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.

```
track 4 ip sla 4
 delay down 10 up 15
 exit
track 6 ip sla 6
 delay down 10 up 15
 exit
```

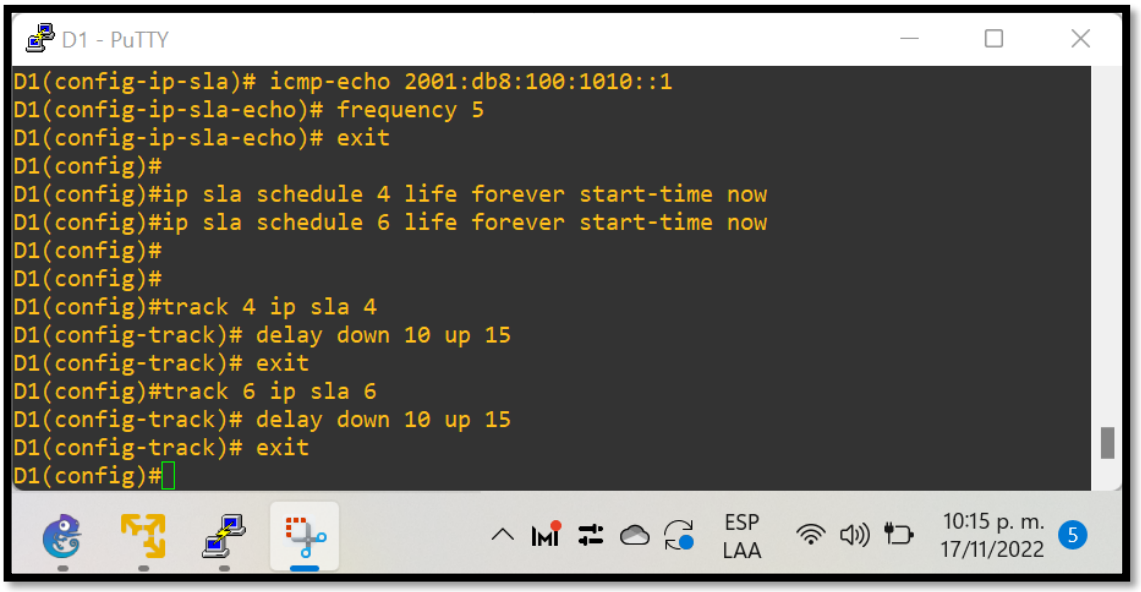

Figura 55. Configuración track number – Switch D1

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.

Switch D2

```
ip sla 4
 icmp-echo 10.30.11.1
 frequency 5

ip sla 6
 icmp-echo 2001:DB8:100:1011::1
 frequency 5

ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
```

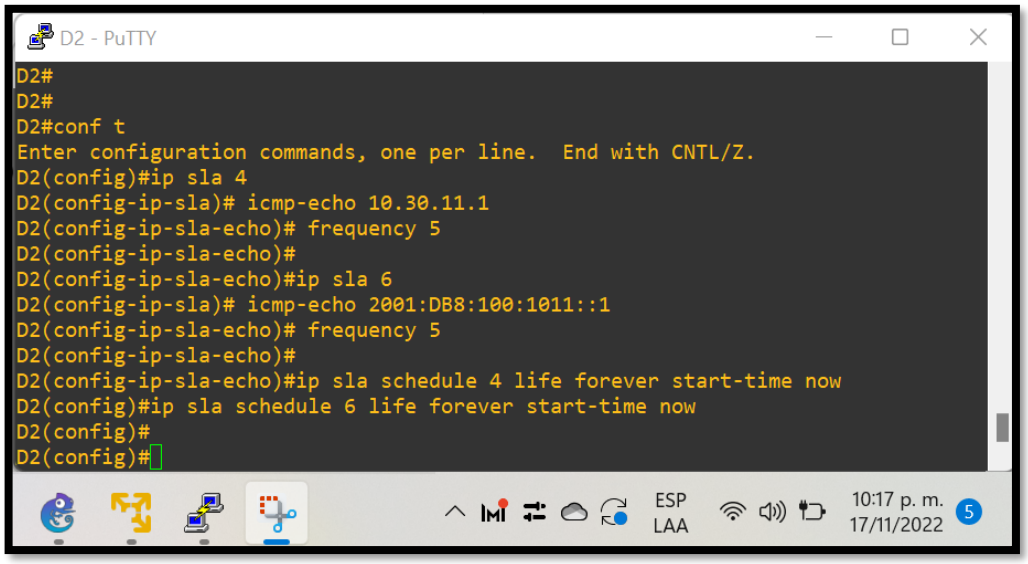

Figura 56. Configuración IP SLA – Switch D2

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.

```
track 4 ip sla 4
 delay down 10 up 15
track 6 ip sla 6
 delay down 10 up 15
```

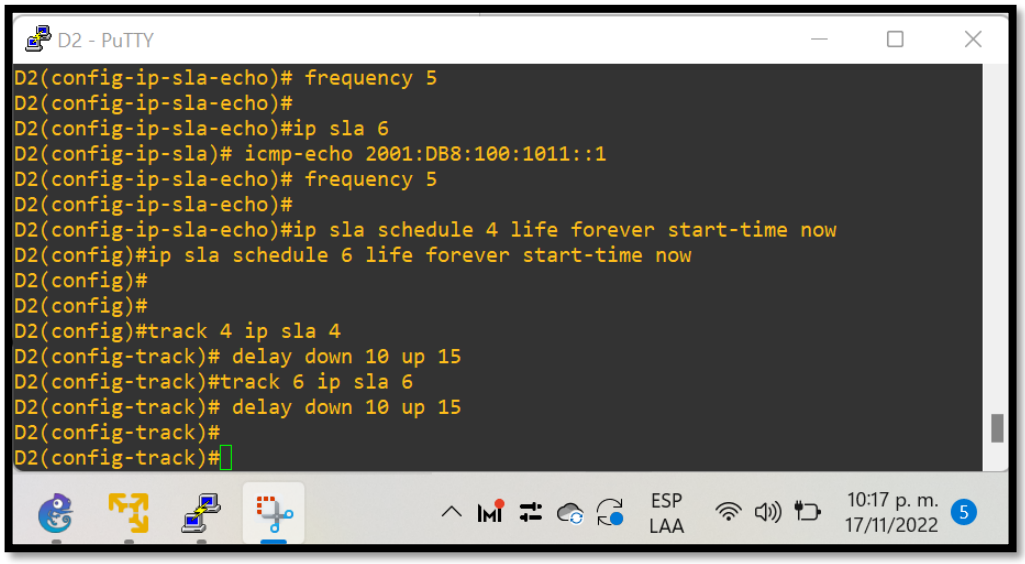

Figura 57. Configuración track number – Switch D2

4.3 On D1, configure HSRPv2.

Switch D1

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 **10.30.100.254**.
- Set the group priority to **150**.
- Enable preemption.
- Track object 4 and decrement by 60.

```
interface vlan 100
 standby version 2
 standby 104 ip 10.30.100.254
 standby 104 priority 150
 standby 104 preempt
 standby 104 track 4 decrement 60
```

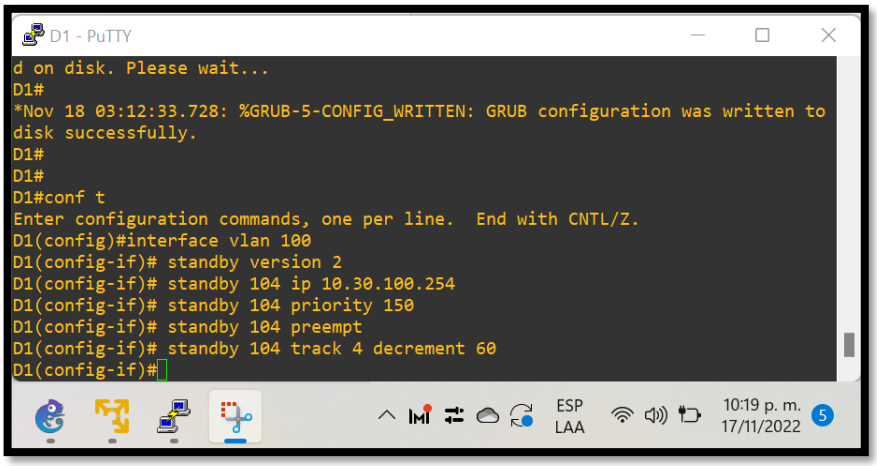

Figura 58. Configuración HSRP VLAN 100 – Switch D1

Configure IPv4 HSRP group **114** for VLAN 101:

- Assign the virtual IP address **10.30.101.254**.
- Enable preemption.
- Track object 4 to decrement by 60.

```
interface vlan 101
 standby version 2
 standby 114 ip 10.30.101.254
 standby 114 preempt
 standby 114 track 4 decrement 60
```

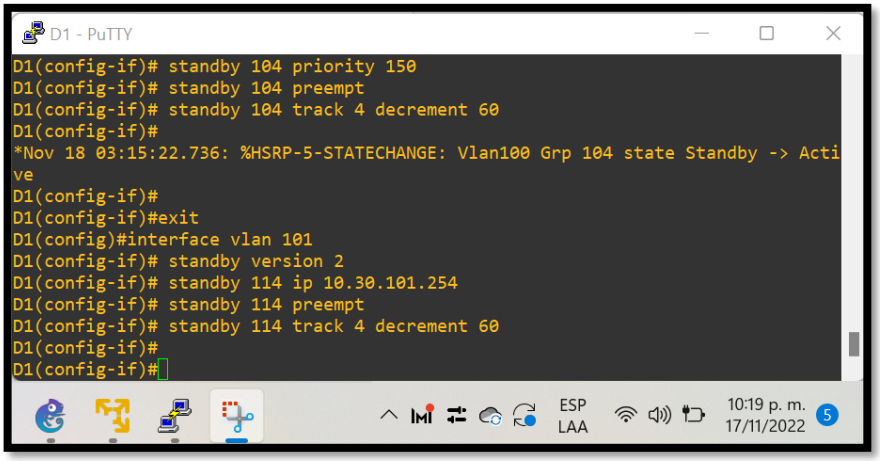

Figura 59. Configuración HSRP VLAN 101 – Switch D1

Configure IPv4 HSRP group **124** for VLAN 102:

- Assign the virtual IP address **10.30.102.254**.
- Set the group priority to **150**.
- Enable preemption.
- Track object 4 to decrement by 60.

```
interface vlan 102
```

```
standby version 2
standby 124 ip 10.30.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
```

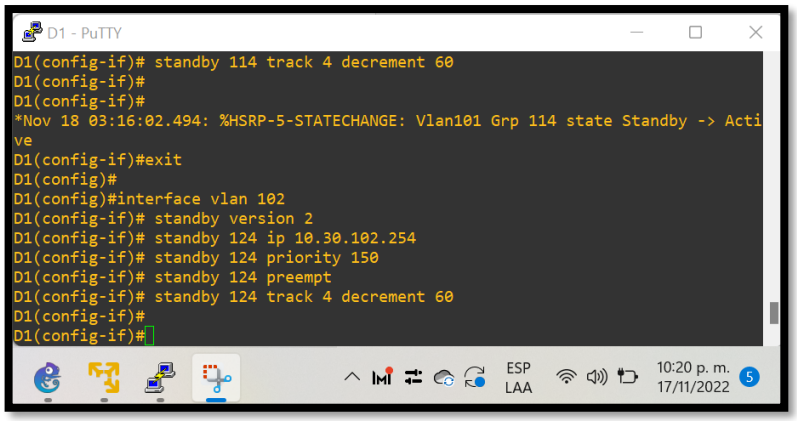

Figura 60. Configuración HSRP VLAN 102 – Switch D1

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.

```
interface vlan 100
 standby 106 ipv6 autoconfig
 standby 106 priority 150
 standby 106 preempt
 standby 106 track 6 decrement 60
 exit
```

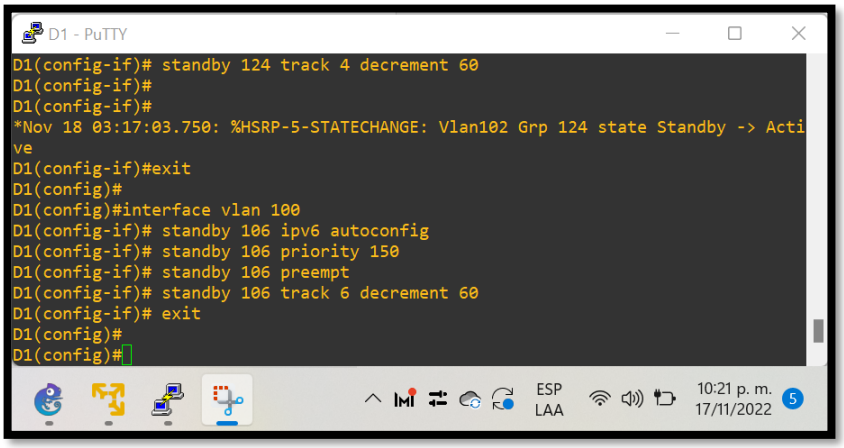

Figura 61. Configuración HSRP IPv6 VLAN 100 – Switch D1

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.

```
interface vlan 101
 standby 116 ipv6 autoconfig
 standby 116 preempt
 standby 116 track 6 decrement 60
 exit
```

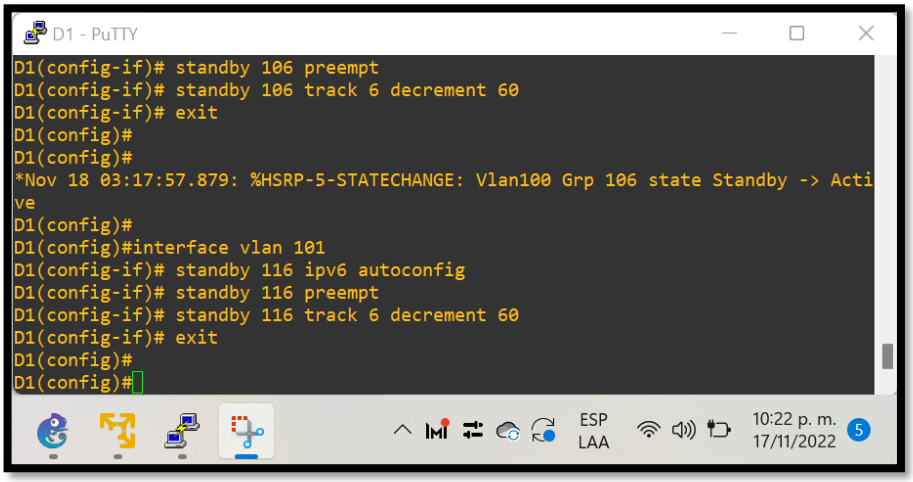

Figura 62. Configuración HSRP IPv6 VLAN 101 – Switch D1

Configure IPv6 HSRP group **126** for VLAN 102:

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

```
interface vlan 102
 standby 126 ipv6 autoconfig
 standby 126 priority 150
 standby 126 preempt
 standby 126 track 6 decrement 60
 exit
```

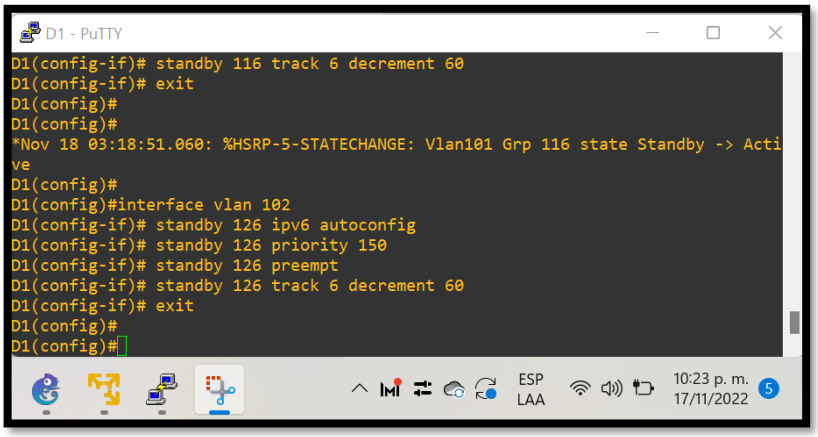

Figura 63. Configuración HSRP IPv6 VLAN 102 – Switch D1

On D2, configure HSRPv2.

Switch D2

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 **10.30.100.254**.
- Enable preemption.
- Track object 4 and decrement by 60.

```
interface vlan 100
 standby version 2
 standby 104 ip 10.30.100.254
 standby 104 preempt
 standby 104 track 4 decrement 60
 exit
```

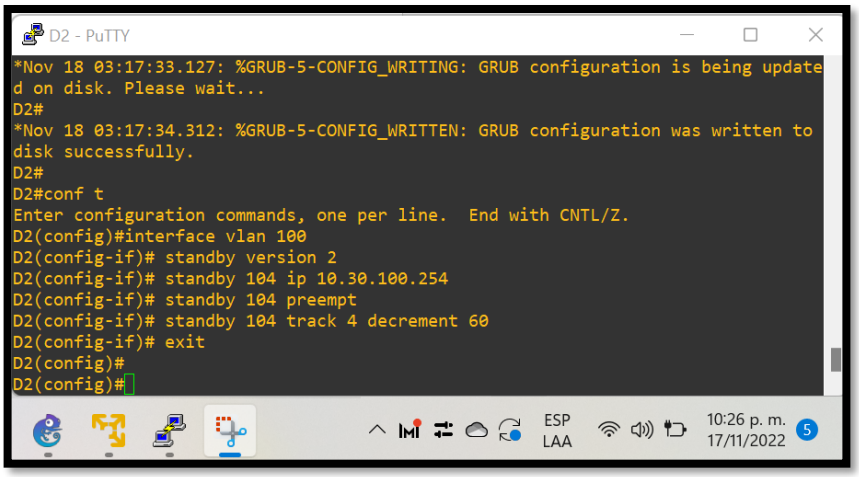

Figura 64. Configuración HSRP VLAN 100 – Switch D2

Configure IPv4 HSRP group **114** for VLAN 101:

- Assign the virtual IP address **10.30.101.254**.
- Set the group priority to **150**.
- Enable preemption.
- Track object 4 to decrement by 60.

```
interface vlan 101
 standby version 2
 standby 114 ip 10.30.101.254
 standby 114 priority 150
 standby 114 preempt
 standby 114 track 4 decrement 60
 exit
```

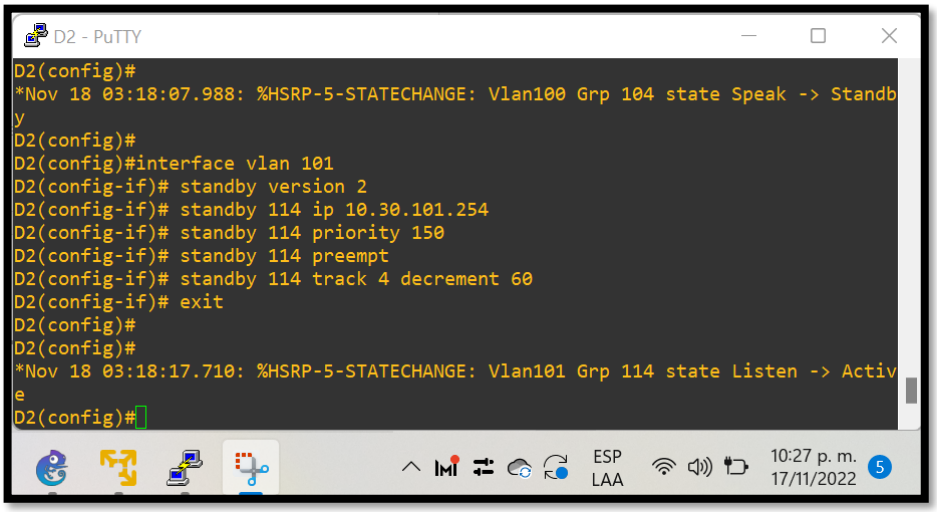

Figura 65. Configuración HSRP VLAN 100 – Switch D2

Configure IPv4 HSRP group **124** for VLAN 102:

- Assign the virtual IP address **10.30.102.254**.
- Enable preemption.
- Track object 4 to decrement by 60.

```
interface vlan 102
 standby version 2
 standby 124 ip 10.30.102.254
 standby 124 preempt
 standby 124 track 4 decrement 60
 exit
```

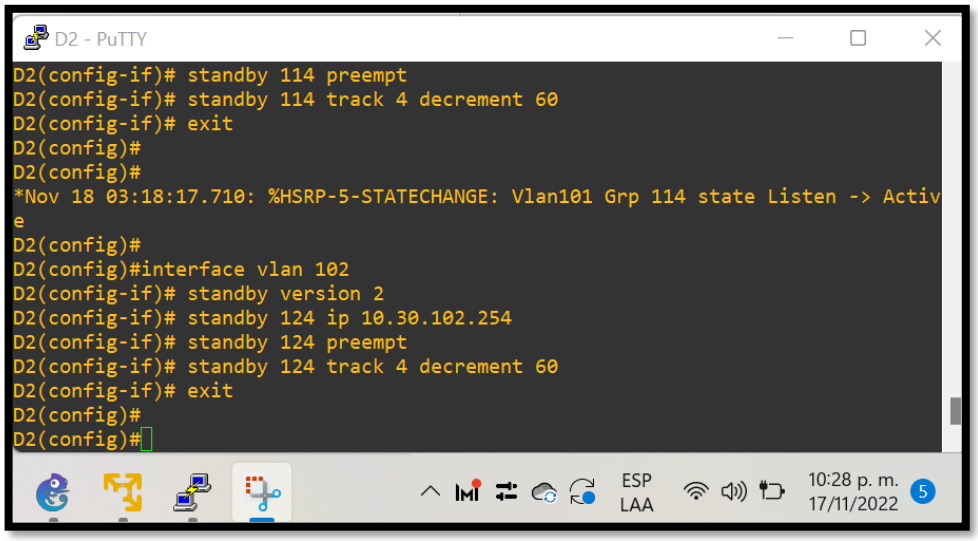

Figura 66. Configuración HSRP VLAN 102 – Switch D2

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.

```
interface vlan 100
 standby 106 ipv6 autoconfig
 standby 106 preempt
 standby 106 track 6 decrement 60
 exit
```

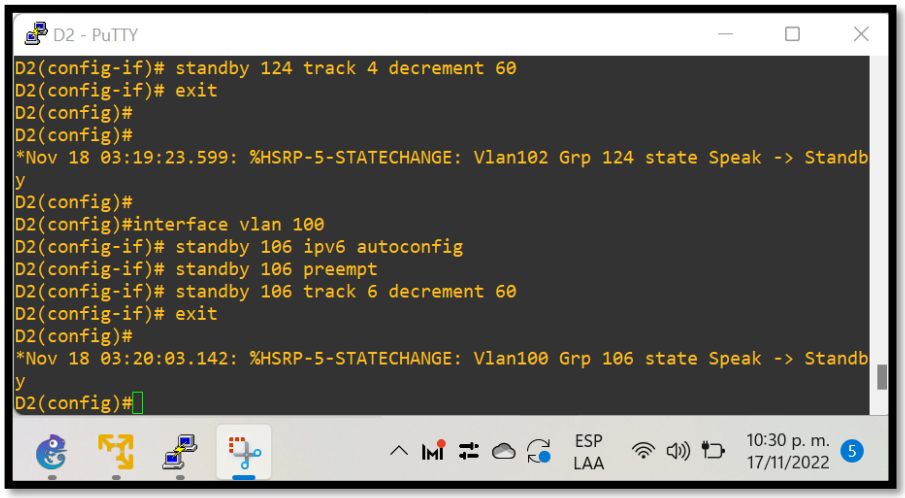

Figura 67. Configuración HSRP IPv6 VLAN 100 – Switch D2

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.

```
interface vlan 101
 standby 116 ipv6 autoconfig
 standby 116 priority 150
 standby 116 preempt
 standby 116 track 6 decrement 60
 exit
```

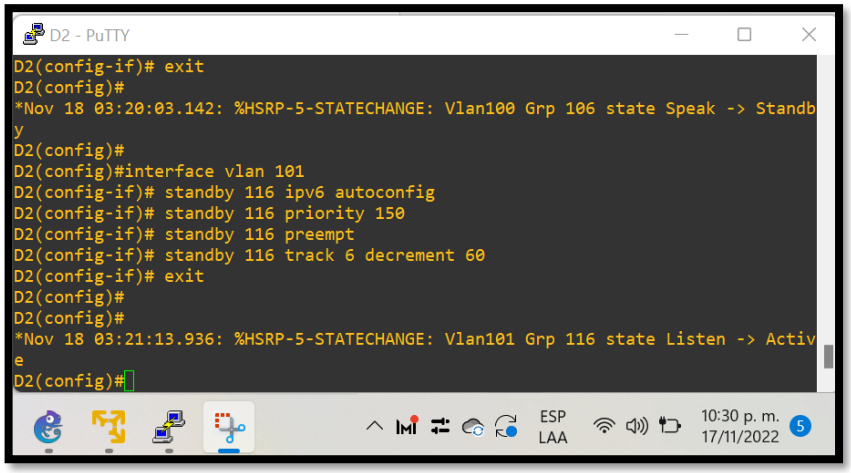

Figura 68. Configuración HSRP IPv6 VLAN 101 – Switch D2

Configure IPv6 HSRP group **126** for VLAN 102:

- Assign the virtual IP address using **ipv6 autoconfig**.
- Enable preemption.
  Track object 6 and decrement by 60.

```
interface vlan 102
 standby 126 ipv6 autoconfig
 standby 126 preempt
 standby 126 track 6 decrement 60
 exit
```

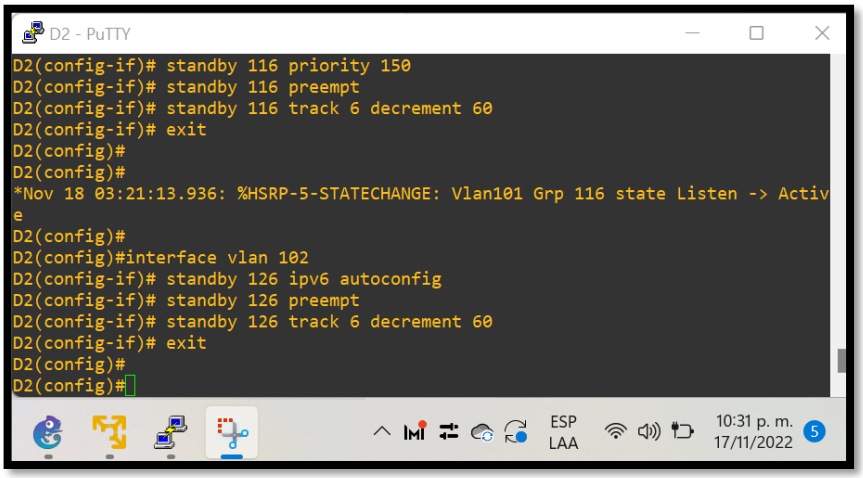

Figura 69. Configuración HSRP IPv6 VLAN 102 – Switch D2

CONCLUSIONES

La simulación del escenario típico de red corporativa mediante GNS3 me permitió investigar acerca de los APPLIANCE de red que no habían sido utilizados en cursos anteriores como el CISCO IOSvL2 con imagen de extensión QCOW2 las cuales requieren de una máquina virtual GNS3 VM o Virtual VOX para su funcionamiento.

Mediante comandos de verificación se pudo validar la operación de los EtherChannel configurados y la conectividad entre dispositivos dentro del mismo segmento de red. Hasta este punto no hace falta un default valido ni protocolo de enrutamiento porque las pruebas fueron ejecutadas sobre segmentos de red directamente conectados.

Las funcionalidades del servidor DHCP en la switch multicapa o router facilitan las labores de despliegue de red y reduce los costos asociados a servidores de propósitos específico

La configuración de EtherChannel mejora la disponibilidad de la red, al mismo tiempo que aumenta el ancho de banda mediante la agrupación lógica de enlaces sin riesgo a Loops en capa dos siempre y cuando se definan correctamente las instancias de Spanning Tree

Esta guía me permitió poner en práctica los conceptos de enrutamiento vistos durante el curso mediante la configuración de OSPFv2 y OSPFv3 para la propagación de rutas IPv4 e IPv6, así como la aplicación de interfaces pasivas para evitar que se intercambien mensajes de OSPF sobre las interfaces LAN

Mediante la configuración de MP-BGP se puso en práctica la implementación del protocolo de Gateway exterior eBGP requerido para intercambio de rutas entre sistemas autónomos externos para la familia ipv4 e ipv6 además de la sumarización de prefijos

El protocolo IP SLA nos permite censar los enlaces WAN y generar acciones mediante tracks para provocar la conmutacion de tráfico en combinación con el protocolo HSRP propietario de CISCO

Con el fin de tener redundancia de hardware en el Gateway de la LAN, se aplicó el protocolo HSRP que nos permite proteger los entornos LAN mediante la definición de una IP virtual como Gateway en dos Routers o switches multicapa. Esta funcionalidad es útil cuando se realizan labores de mantenimiento en los routers de la LAN y no queremos que se presente afectación de servicio

BIBLIOGRAFIA

Cisco. (s/f). Netacad.com. Recuperado el 31 de agosto de 2022, de https://www.netacad.com/portal/learning

(N.d.-c). Upw.Io. Retrieved October 12, 2022, from https://upw.io/4yu/vios_l2-adventerprisek9-m.ssa.high_iron_20200929.qcow2

(N.d.-d). Gns3.com. Retrieved October 12, 2022, from https://gns3.com/