DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN DAVID QUILINDO PALECHOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGIENERIA ELECTRONICA
POPAYAN
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN DAVID QUILINO PALECHOR

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGIENERIA ELECTRONICA
POPAYAN
2021

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

POPAYAN, 29 de noviembre de 2021

AGRADECIMIENTOS

Gracias a la Universidad Nacional Abierta y a Distancia (UNAD) por haberme permitido formarme y obtener nuevos conocimientos, gracias a todas las personas que fueron participes de estos procesos en especial el director de diplomado de profundización en CISCO Gerardo Granados Acuña y compañeros.

Agradezco de manera especial por el apoyo a la empresa donde trabajo en especial a mi jefe inmediato Hébert Macias, gracias a mis padres y mi pareja quienes fueron mis motivadores y gracias a Dios que fue mi principal apoyo y motivador para cada día continuar y no desfallecer.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Redes: conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc. Interfaces

Vlans: redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red físico.

Protocolo: Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router o switch cuando se comunica con otros router o switchs con el fin de compartir información de enrutamiento.

Packet Tracer: aplicación gratuita de Cisco la cual es una herramienta con la que es posible diseñar redes y realizar simulaciones sobre su uso.

Red ospf: (Open Shortest Path First ó en español, El Camino Más Corto Primero) es un protocolo de enrutamiento dinámico interior (IGP – Internal Gateway Protocol). Usa un algoritmo de tipo Estado de Enlace.

Switch: Un switch o conmutador es un dispositivo de interconexión utilizado para conectare quipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3)

RESUMEN

Este documento contiene la prueba de habilidades de una de las actividades que hacen parte del diplomado de profundización en CISCO-CCNP el cual se toma como opción de grado para la obtención de la titulación en ingeniería electrónica y que consta de una serie de ejercicios distribuidos en 6 partes Abordando los temas sobre networking CCNP de CISCO, donde se aplican todos los conceptos estudiados para la creación y enrutamiento de redes proporcionando conocimientos avanzados en el diseño de redes LAN, WAN. Para entender su funcionamiento se realiza a través de la práctica mediante entornos de simulación con el software GNS3, lo cual facilita el aprendizaje debido a lo complejo de tener todos los equipos en físico.

En cada parte de la actividad se aprenden los diferentes protocolos de comunicación y cómo se realizan las diferentes configuraciones de los equipos y dispositivos que intervienen en una red como: router, switch y terminales con sus diferentes periféricos. Todo esto se logra aprendiendo a utilizar los comandos que se requieren para el buen funcionamiento de los dispositivos, lo cual permite tener entornos más seguros, estables y con menor probabilidad de errores o conflictos.

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

ABSTRACT

This document contains the skills test of one of the activities that are part of the in-depth diploma at CISCO-CCNP, which is taken as a degree option to obtain the degree in electronic engineering and consists of a series of exercises distributed in 6 parts Addressing the topics on CISCO CCNP networking, where all the concepts studied for the creation and routing of networks are applied, providing advanced knowledge in the design of LAN and WAN networks. To understand its operation, it is done through practice using simulation environments with GNS3 software, which facilitates learning due to the complexity of having all the physical equipment.

In each part of the activity, the different communication protocols are learned and how the different configurations of the equipment and devices that intervene in a network are made, such as: router, switch and terminals with their different peripherals. All this is achieved by learning to use the commands that are required for the proper functioning of the devices, which allows to have more secure, stable environments and with less probability of errors or conflicts.

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

INTRODUCCIÓN

El siguiente documento contiene la prueba de habilidades correspondiente a una de las actividades que hace parte del diplomado de profundización en CISCO-CCNP el cual se toma como opción de grado para la obtención de la titulación en ingeniería electrónica, la cual consta de una serie de ejercicios distribuidos en 6 partes.

En las dos primeras partes se abordan temas relacionados a la Construcción de una red y configuración de los ajustes básicos de los dispositivos, el direccionamiento de las interfaces y Configurar la red de capa 2 y la compatibilidad con los hosts, posteriormente en una tercera y cuarta parte se aborda la configuración de protocolos de enrutamiento, los cuales administran la actividad de enrutamiento del sistema y se configura la redundancia del primer salto la cual evidencia la capacidad de una red para recuperarse dinámicamente de la falla de un dispositivo.

Por último, la Quinta y sexta parte se profundiza en la configuración de protocolos diseñados para proteger el acceso, el uso y la integridad de la red, seguido de la configuración de las funciones de administrativas de red donde se toman precauciones y se supervisa de la red, para mantener su funcionamiento eficiente espero que sea de su agrado.

DESARROLLO

Topología

Figura 1 Topología

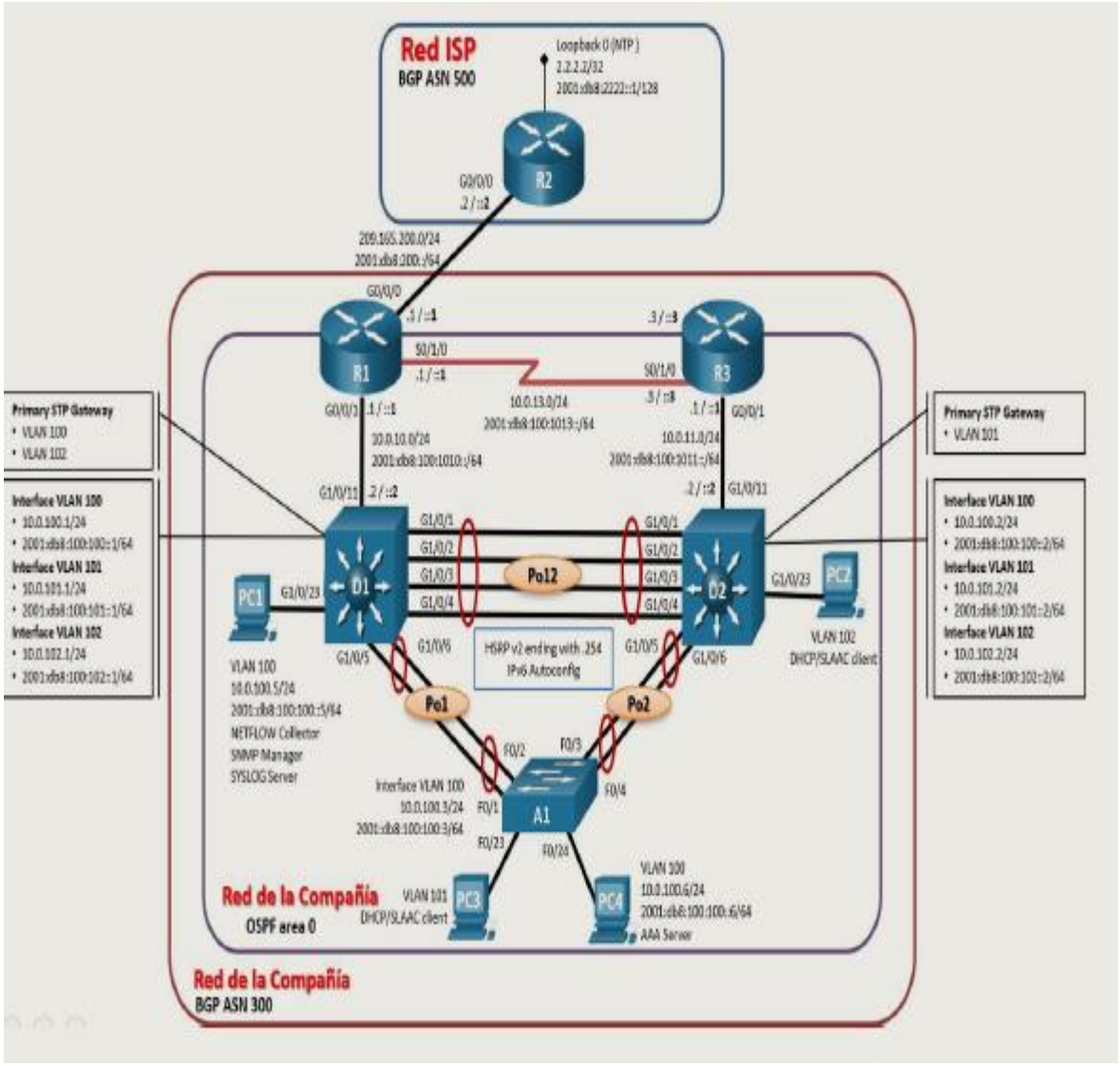
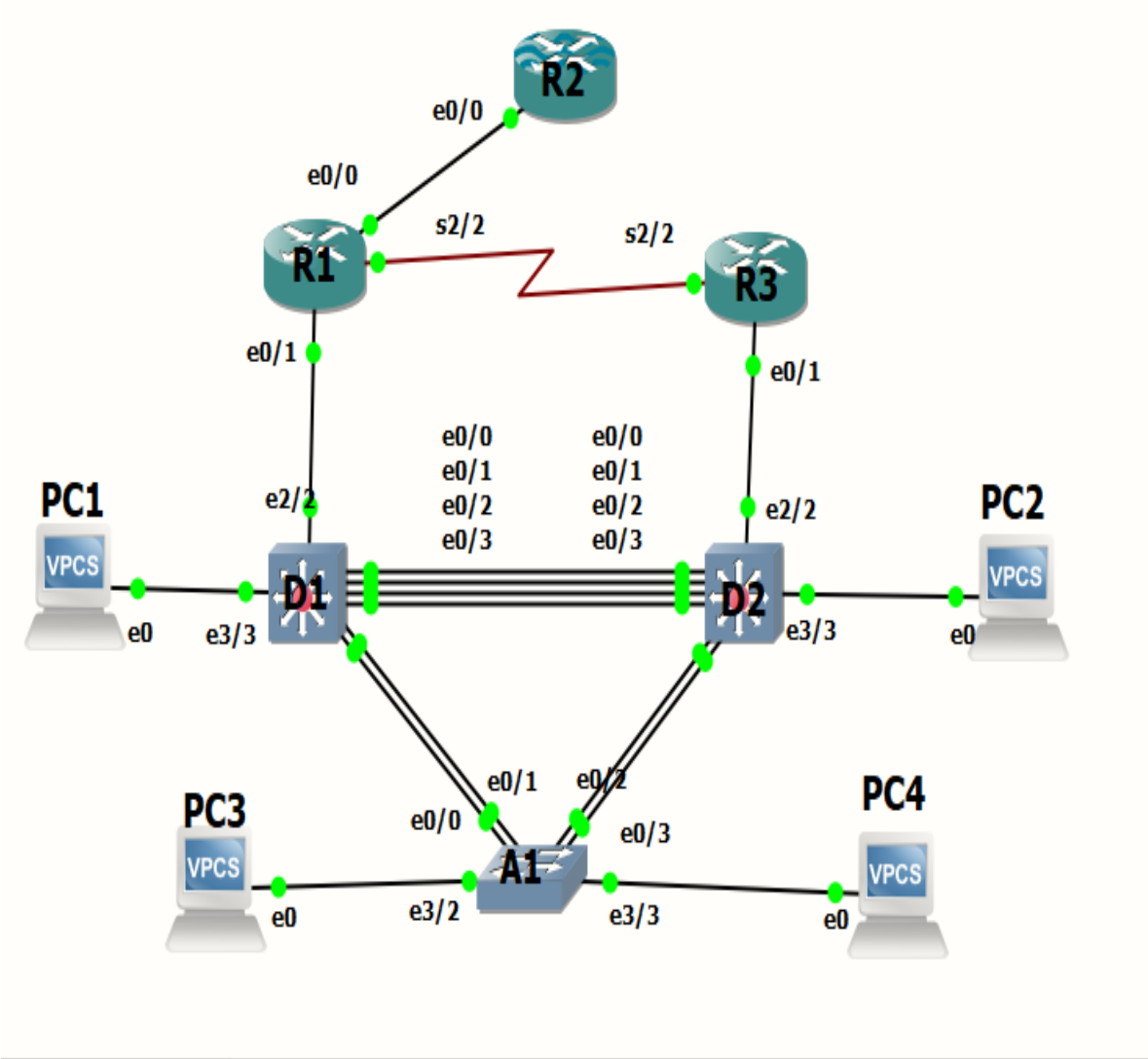


Figura 2 Simulación de Topología



Nota: para el desarrollo de esta actividad se toman como referencias las interfaces descritas en la simulación de la topología.

Tabla 1 Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	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	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Parte 1. Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

1.1 Configurar los parámetros básicos para cada dispositivo.

Para la configuración de los parámetros básicos de R1 se debe inicialmente asignar el nombre al router, seguido de la activación de protocolo ipv6 ,continuando con el apagado de la traducción de nombres a la dirección del dispositivo, posteriormente se crea un mensaje de aviso, luego se ingresa al modo de configuración de línea de consola, seguido se establece el tiempo de espera inactivo de la sesión remota donde una vez cumplido el tiempo cierra la sesión VTY, finalmente se emplea el comando logging synchronous para evitar que los mensajes inesperados nos desplacen los comandos escritos.

```
IOU1#
IOU1#confi ter
IOU1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
```

Configuración de la interfaz s3/3 se asignan la dirección ipv4, mascara de red y la dirección ipv6 con el fin de encaminar paquetes ip entre host .

```
R1(config)#inter e0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Configuración de la interfaz s3/3 se asignan la dirección ipv4, mascara de red y la dirección ipv6 con el fin de encaminar paquetes ip entre host.

```
R1(config)#inter e0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

Configuración de la interfaz s3/3 se asignan la dirección ipv4, mascara de red y la dirección ipv6 con el fin de encaminar paquetes ip entre host.

```
R1(config)#inter s3/3
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdow
```

Para la configuración de los parámetros básicos de R1 se debe inicialmente asignar el nombre al router, seguido de la activación de protocolo ipv6, continuando con el apagado de la traducción de nombres a la dirección del dispositivo, posteriormente se crea un mensaje de aviso, luego se ingresa al modo de configuración de línea de consola, finalmente se emplea el comando logging synchronous para evitar que los mensajes inesperados nos desplacen los comandos escritos.

```
IOU2#confi ter
IOU2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#logging synchronous
R2(config-line)#exi
```

Configuración de la interfaz e0/0 se asignan la dirección ipv4, mascara de red y la dirección ipv6 con el fin de encaminar paquetes ip entre host .

```
R2(config)#inter e0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

Configuración de la interfaz de red virtual donde se asigna la correspondiente ipv4, la máscara de red y la ipv6 con el fin de encaminar paquetes ip entre host.

```
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
```

Para la configuración de los parámetros básicos de R3 se debe inicialmente asignar el nombre al router, seguido de la activación de protocolo ipv6 ,continuando con el apagado de la traducción de nombres a la dirección del dispositivo, posteriormente se crea un mensaje de aviso, luego se ingresa al modo de configuración de línea de consola, seguido se establece el tiempo de espera inactivo de la sesión remota donde una vez cumplido el tiempo cierra la sesión VTY, finalmente se emplea el comando logging synchronous para evitar que los mensajes inesperados nos desplacen los comandos escritos.

```
IOU3#confi ter
Enter configuration commands, one per line.  End with CNTL/Z.
IOU3(config)#hostname R
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
```

Configuración de la interfaz e0/1se asignan la dirección ipv4, mascara de red y la dirección ipv6 con el fin de encaminar paquetes ip entre host.

```
R3(config)#inter e0/1
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#int
```

Configuración de la interfaz s3/3se asignan la dirección ipv4, mascara de red y la dirección ipv6 con el fin de encaminar paquetes ip entre host.

```
R3(config)#inter s3/3
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#end
```

Para la configuración de los parámetros básicos de D1 se debe inicialmente asignar el nombre al router, seguido de la activación de protocolo ipv6 ,continuando con el apagado de la traducción de nombres a la dirección del dispositivo, posteriormente se crea un mensaje de aviso, luego se ingresa al modo de configuración de línea de consola, seguido se establece el tiempo de espera inactivo de la sesión remota donde una vez cumplido el tiempo cierra la sesión VTY, finalmente se emplea el comando logging synchronous para evitar que los mensajes inesperados nos desplacen los comandos escritos.

```
IOU4#CONFI TER
Enter configuration commands, one per line.  End with CNTL/Z.
IOU4(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
```

Se crean las vlans 100,101,102 y 999 con el fin de crear redes lógicas independientes dentro de una misma física, seguido se les asigna nombre.

```
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
```

```
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
```

Se realiza la configuración de las interfaces e2/2 donde se asignan la dirección ipv4, seguido de la máscara de red, direccionamiento ipv6 link-local y ipv6.

```
D1(config)#interface e2/2
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdo
D1(config-if)#exit
D1(config)#
```

Se realiza la configuración de las interfaces vlans del switch D1 donde se asignan la dirección ipv4, seguido de la máscara de red, direccionamiento ipv6 link-local ipv6.

```
D1(config)#interface vlan 100
D1(config-if)#
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#
```

Se configura el switch D1 para asignación de direcciones IP de manera automática

Inicialmente con el fin de evitar conflictos de ip se excluyen las direcciones ip de las interfaces de las vlans, seguidamente se Define un pool para las vlans seguido del rango de direcciones ip tiene para asignar, finalmente se configura una ruta estática.

```
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
```

```
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit

D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#
D1(config)#interfa range e0/0-3,e1/0-1
D1(config-if-range)#shut
D1(config-if-range)#exit
```

Para la configuración de los parámetros básicos de D1 se debe inicialmente asignar el nombre al router, seguido de la activación de protocolo ipv6 ,continuando con el apagado de la traducción de nombres a la dirección del dispositivo, posteriormente se crea un mensaje de aviso, luego se ingresa al modo de configuración de línea de consola, seguido se establece el tiempo de espera inactivo de la sesión remota donde una vez cumplido el tiempo cierra la sesión VTY, finalmente se emplea el comando logging synchronous para evitar que los mensajes inesperados nos desplacen los comandos escritos.

```
IOU5#
IOU5#confi ter
Enter configuration commands, one per line.  End with CNTL/Z.
IOU5(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
```

Se crean las vlans 100,101,102 y 999 con el fin de crear redes lógicas independientes dentro de una misma física, seguido se les asigna nombre.

```
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exi
```

Ahora se realiza la configuración de la interfaz e2/2 donde inicialmente se desactiva la troncalización, luego se asigna la correspondiente ipv4, seguido de la máscara de red, el direccionamiento ipv6 link-local y ipv6

```
D2(config)#inter e2/2
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
```

Se realiza la configuración de las interfaces vlans del switch D2 donde se asignan la dirección ipv4, seguido de la máscara de red, direccionamiento ipv6 link-local ipv6.

```
D2(config)#interface vlan 100
D2(config-if)#
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 102
D2(config-if)#
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
```

Inicialmente con el fin de evitar conflictos de ip se excluyen las direcciones ip de las interfaces de las vlans, seguidamente se Define un pool para las vlans seguido del rango de direcciones ip tiene para asignar, finalmente se configura una ruta estática.

```
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
```

```
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interfa range e0/0-3,e1/0-1
D2(config-if-range)#shut
D2(config-if-range)#
D2(config-if-range)#exit
D2(config)#exit
```

Para la configuración de los parámetros básicos de A1 se debe inicialmente asignar el nombre al router, seguido de la activación de protocolo ipv6 ,continuando con el apagado de la traducción de nombres a la dirección del dispositivo, posteriormente se crea un mensaje de aviso, luego se ingresa al modo de configuración de línea de consola, seguido se establece el tiempo de espera inactivo de la sesión remota donde una vez cumplido el tiempo cierra la sesión VTY, finalmente se emplea el comando logging synchronous para evitar que los mensajes inesperados nos desplacen los comandos escritos.

```
IOU6(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
```

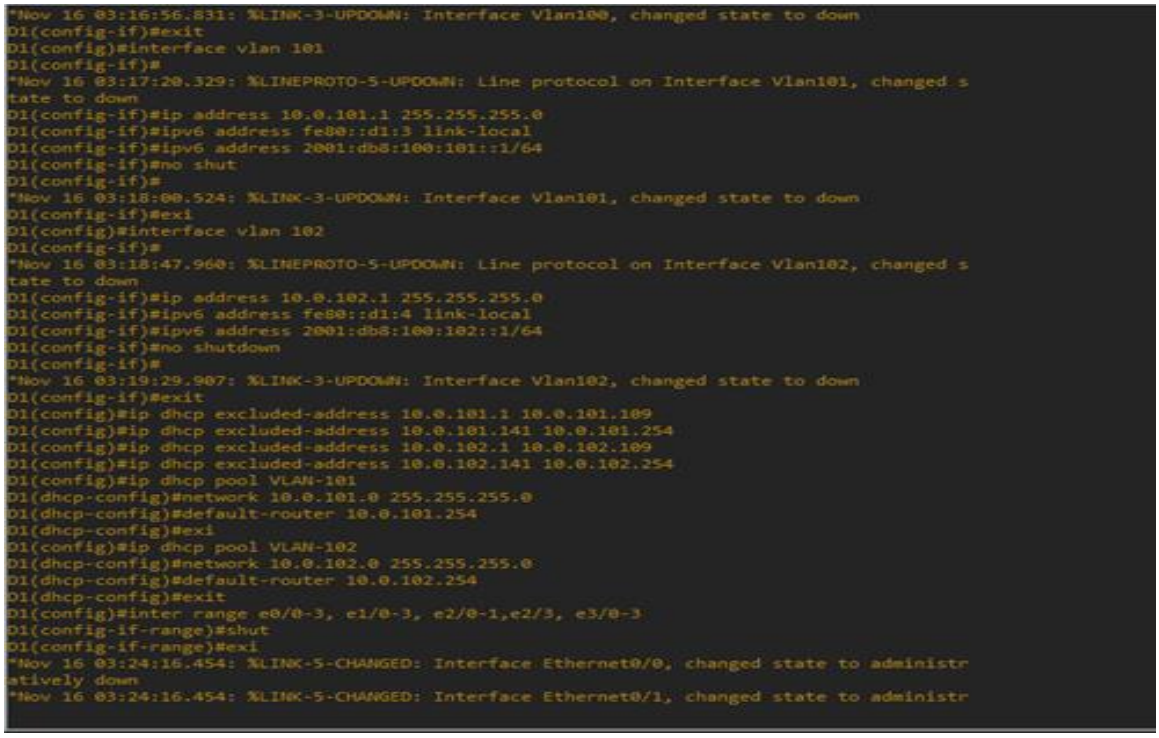
Se crean las vlans 100,101,102 y 999 con el fin de crear redes lógicas independientes dentro de una misma red física, seguido se les asigna nombre.

```
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exi
```

Se realiza la configuración de las interfaces vlans del switch D2 donde se asignan la dirección ipv4, seguido de la máscara de subred, direccionamiento ipv6 link-local ipv6.

```
A1(config)#interface vlan 100
A1(config-if)#
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#
A1(config)#inter range e0/0-3
A1(config-if-range)#shut
```

Figura 3 Configuración básica de dispositivos



1.2 Copie el archivo running-config al archivo startup-config en todos los dispositivos.

En este punto se ingresa al modo privilegiado, luego se utiliza el comando copy running-config startup-config con el fin de copiar la configuración activa de lo router o de los switches de la RAM a la NVRAM.

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

R2>
R2>enable
R2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

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

```
D1>
D1>enable
D1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2397 bytes to 1362 bytes[OK]

D2>
D2>enable
D2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2397 bytes to 1362 bytes[OK]

A1>
A1>enable
A1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2397 bytes to 1362 bytes[OK]
```

1.3 Se configura el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

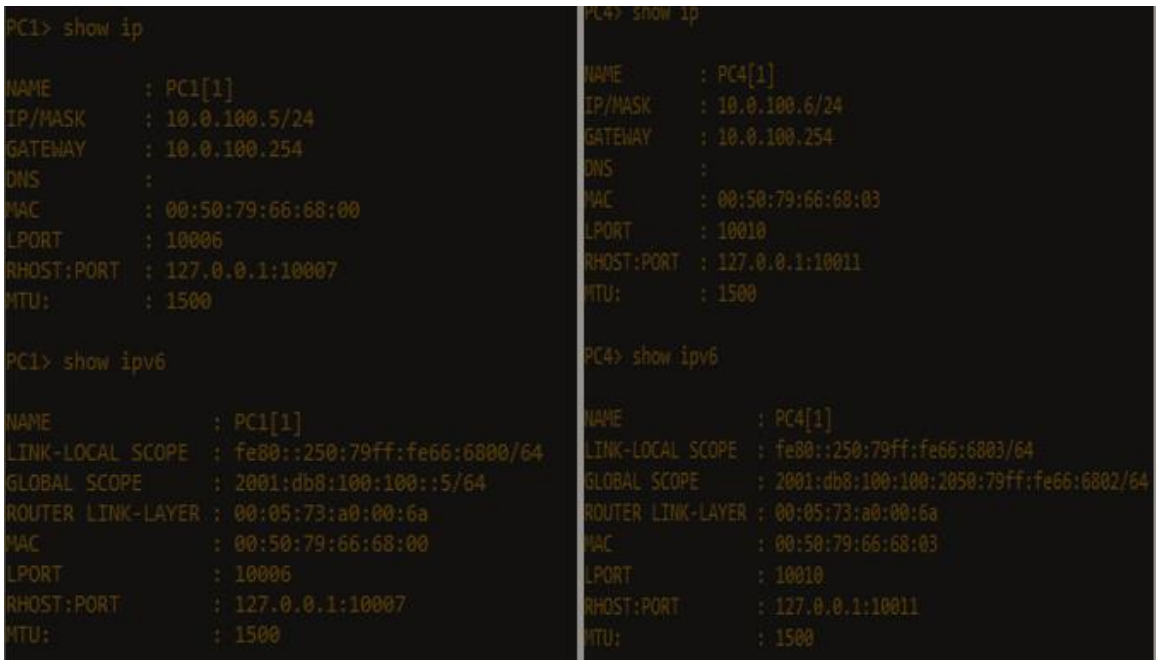
Se asigna la dirección ipv4 10.0.100.5, la máscara de red 255.255.255.0 y la puerta de enlace predeterminada 10.0.100.254 y ipv6 2001:db8:100:100::5/64/eui-64 en PC1

```
PC1> ip 10.0.100.5 255.255.255.0 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
PC1> ip 2001:db8:100:100::5/64/eui-64
PC1 : 2001:db8:100:100::5/64
PC1> save
Saving startup configuration to startup.vpc
 Done
```

Se asigna la dirección ipv4 10.0.100.6, la máscara de red 255.255.255.0 y la puerta de enlace predeterminada 10.0.100.254 y ipv6 2001:db8:100:100::6/64/eui-64 en PC4

```
PC4> ip 10.0.100.6 255.255.255.0 10.0.100.254
Checking for duplicate address...
PC4> ip 2001:db8:100:100::6/64/eui-64
PC1 : 2001:db8:100:100:2050:79ff:fe66:6802/64 eui-64
PC4> save
Saving startup configuration to startup.vpc
Done
```

Figura 4 Comprobación de direccionamiento pc1 y pc4



Parte 2. Configurar la capa 2 de la red y el soporte de host

Tabla 2 Tareas de configuración parte 2

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).

Tarea #	Tarea	Especificación
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Para la configuración de una vlan nativa se selecciona el rango de las interfaces en D1 e0/0-3, e1/0-1, en D2 e0/0-3, e1/0-1 Y en A1 e0/0-3, luego se activa el protocolo dot1q para que el switch posea enlaces troncales, seguido se activa el modo de enlace troncal permanente y finalmente se debe especificar las vlans que se permitirán el enlace troncal

```
D1(config)#inter range  e0/0-3,e1/0-1
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport  trunk allowed vlan 100,101,102,999
```

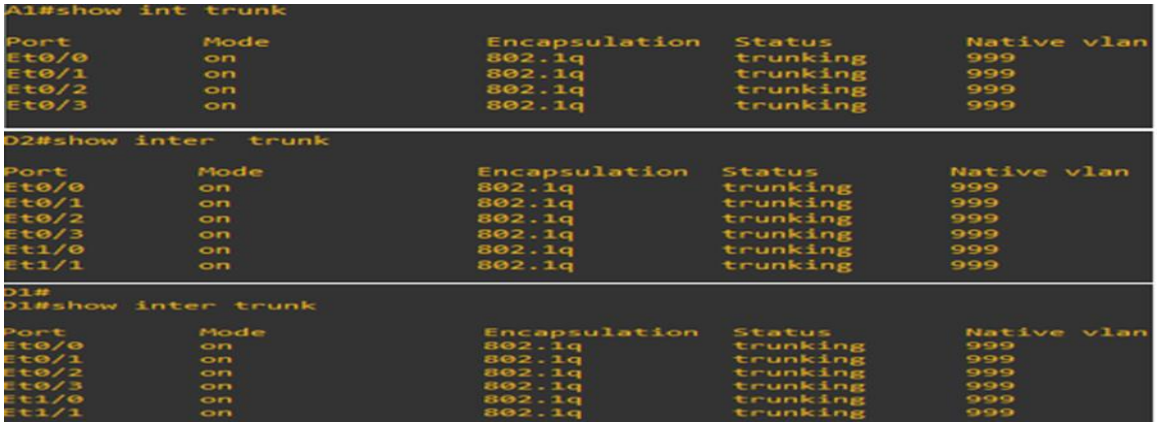
```
D1(config-if-range)#end


D2#confi ter
D2(config)#inter range  e0/0-3,e1/0-1
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport  trunk allowed vlan 100,101,102,999
D2(config-if-range)#end


A1#confi ter
A1(config)#inter range  e0/0-3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport  trunk allowed vlan 100,101,102,999
A1(config-if-range)#end
```

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

Para la configuración de una vlan nativa se selecciona el rango de las interfaces en D1 e0/0-3, e1/0-1, en D2 e0/0-3, e1/0-1 Y en A1 e0/0-3, luego se activa el modo de enlace troncal permanente, seguido se añaden las vlan de los enlaces troncales y finalmente se especifican las vlans que se permitirán en los enlaces troncales.

```
D1#
D1(config)#
D1(config)#inter range e0/0-3, e1/0-1
D1(config-if-range)#
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk NATIVE vlan 999
D1(config-if-range)# switchport  trunk allowed vlan 100,101,102,999
D1(config-if-range)#exi
D2#
D2(config)#
D2(config)#inter range e0/0-3, e1/0-1
D2(config-if-range)#
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk NATIVE vlan 999
D2(config-if-range)# switchport  trunk allowed vlan 100,101,102,999
D1(config-if-range)#exi
A1(config)#
A1(config)#inte range e0/0-3
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk NATIVE vlan 999
A1(config-if-range)# switchport  trunk allowed vlan 100,101,102,999
A1(config)#exit
```

Figura 5 Comprobación de enlaces troncales y vlan nativa



2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

Configura el modo de árbol de expansión PVST+ rápido

D1#confi ter
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#spanning-tree mode rapid-pvst
D1(config)#exit

D2#confi ter
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#spanning-tree mode rapid-pvst
D2(config)#exit

A1#confi ter
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#spanning-tree mode rapid-pvst
A1(config)#exit

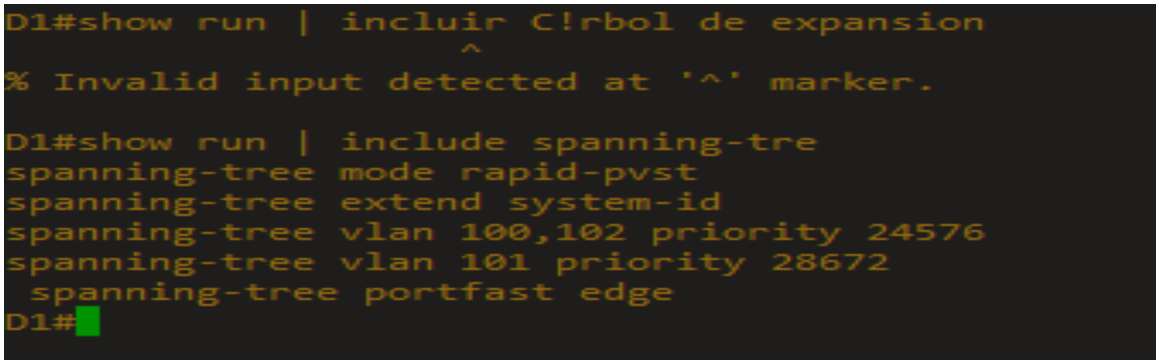
2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge)

spanning-tree vlan # root primary la prioridad para el conmutador se establece en el valor predefinido de 24.576 o en el múltiplo más alto de 4096 menos que la prioridad de puente más baja detectada en la red.

spanning-tree vlan # root secondary establece la prioridad para el interruptor en el valor predefinido 28,672. Esto asegura que el conmutador alternativo se convierta en el puente raíz si falla el puente raíz principal

D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#exi
D1(config)#end
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#end

Figura 6 Comprobación del puente raíz y el protocolo RSTP



2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología

Para la configuración EtherneChannels LACP se selecciona el rango de las interfaces en D1 e0/0-3, e1/0-1, en D2 e0/0-3, e1/0-1 Y en A1 e0/0-3 donde se activa el modo de enlace troncal permanente, seguido se añaden las vlan nativa a enlaces troncales de las interfaces y finalmente se configuran los grupos de enlaces dados por Po 12, Po1, Po2.

D1-D2
D1(config)#inter range e0/0-3
D1(config-if-range)#switchport mode trunk
D1(config-if-range)# switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#no shut
D1(config-if-range)#exit

inter range e0/0-3
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shut
D2(config-if-range)#end
D2#

D1-A1
D1(config)#inter range e1/0-1
D1(config-if-range)#switchport mode trunk
D1(config-if-range)# switchport trunk native vlan 999
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#no shut
D1(config-if-range)#end
D1#
A1(config)#inter range e0/0-1
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

```
A1(config-if-range)#no shu
A1(config-if-range)#exi
A1(config)#end
A1#
```

D2-A1

```
A1(config)#inter range e0/2-3
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
A1(config-if-range)#no shu
A1(config-if-range)#no shu
A1(config-if-range)#exi
A1(config)#end
A1#
D2(config)#inter rang e1/0-1
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
D2(config-if-range)#no shut
D2(config-if-range)#end
D2#
```

2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

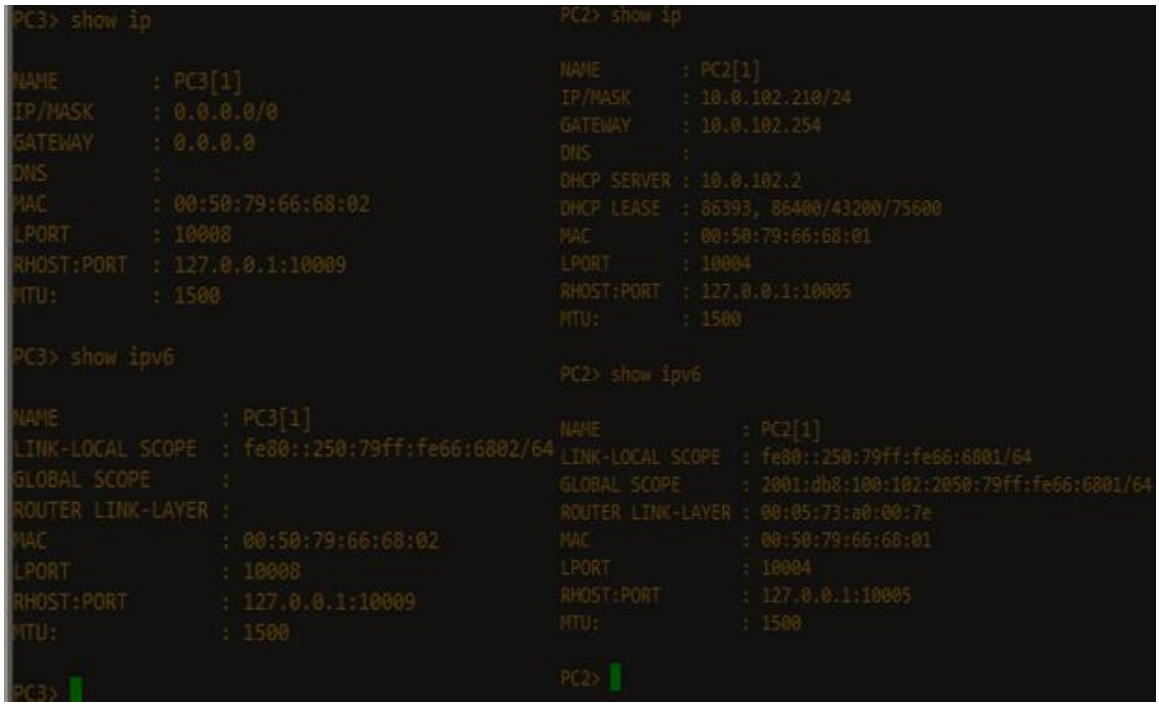
Se establecen los puertos e3/3, e3/3 y e3/2 correspondientes a los switch D1, D2 y A1 en modo de acceso, seguidamente se asigna los puertos a vlans permitiendo a las estaciones de usuarios finales obtener acceso inmediato a la red de capa 2.

```
D1(config)#inte e3/3
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
D1(config-if)#no shut
D1(config-if)#exit
D1(config)#end
D1#
D2#confi ter
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#inter e3/3
D2(config-if)#no shut
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)#no shut
D2(config-if)#exit
D2(config)#end
```

```
A1(config-if)#inter e3/2
A1(config-if)#no shutd
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#no shut
A1(config-if)#en
A1(config-if)#inter e3/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shut
A1(config-if)#exit
A1(config)#end
A1#
```

2.7 Verifique los servicios DHCP IPv4.

Figura 7 Verificación de servicios dhcp



2.8 Verifique la conectividad de la LAN local

Figura 8 Uso de comando ping para verificar la conectividad de la LAN local

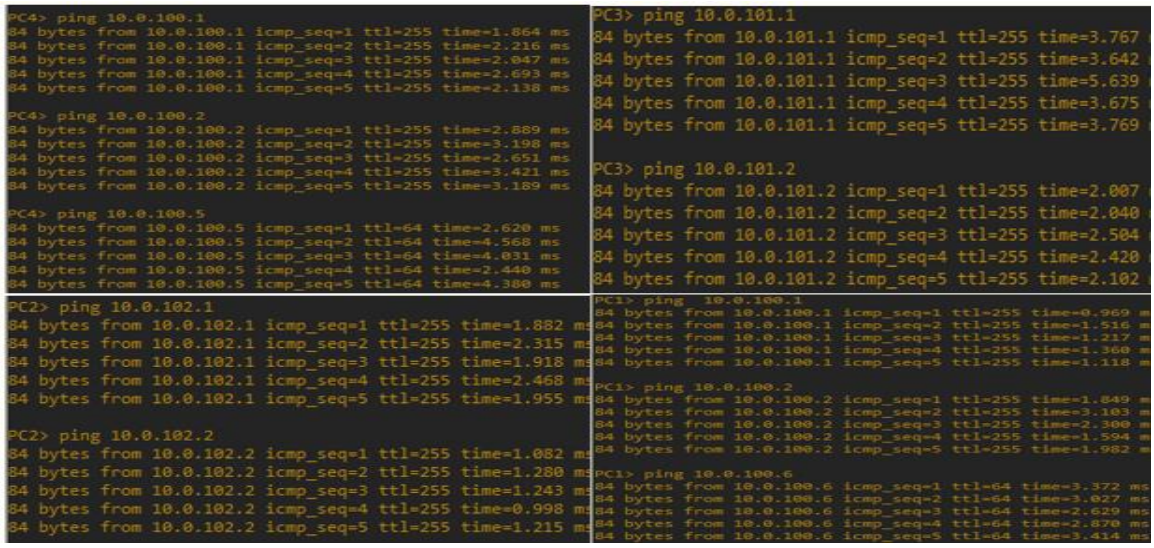
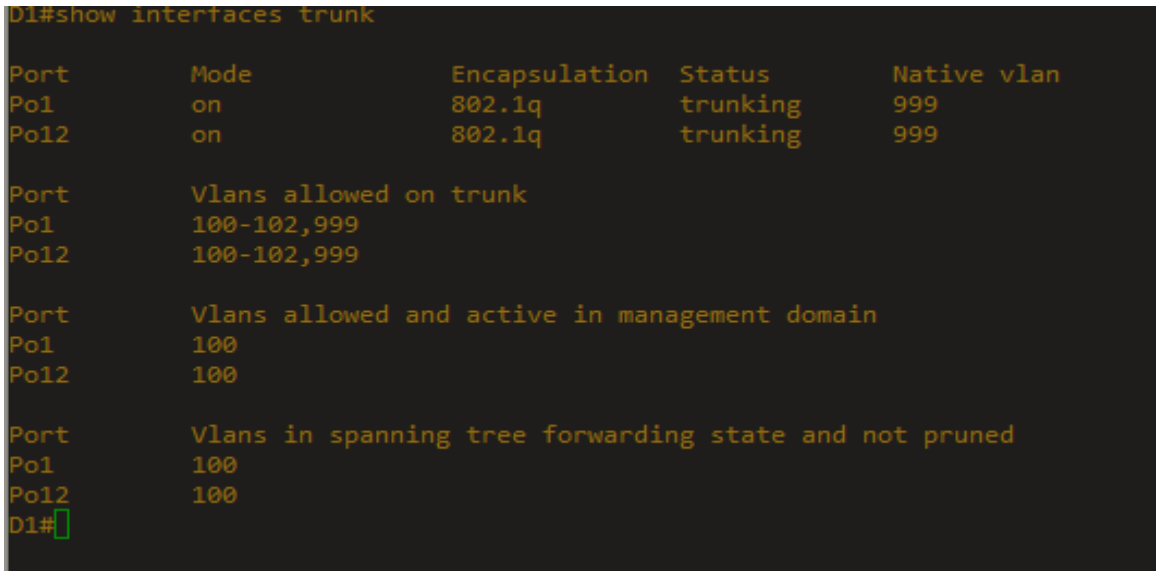


Figura 9Verificación de los puntos 2.1, 2.2 y 2.5 en switch D1



Parte 3. Configurar Los Protocolos De Enrutamiento

Tabla 3 Tareas de configuración parte 3

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

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

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-área OSPFv2 en área 0

Para el router R1 Inicialmente se habilita el enrutamiento por medio del OSPF en el proceso 4 seguido de la identificación del router ID OSPF, luego se signa las redes que serán la ruta del área 0, posteriormente se configura una ruta predeterminada en el áreay finalmente salimos de la configuración.

```
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)# default-information originate
R1(config-router)# exit
```

Para el router R3 Inicialmente se habilita el enrutamiento por medio del OSPF en el proceso 4 seguido de la identificación del router ID OSPF, luego se asignan las redes red serán ruta del área 0, luego se asigna la red que será ruta del área 0 y finalmente Salir de la configuración.

```
R3(config)#router ospf 4
R3(config-router)# router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
 R3(config-router)#exit
```

Para el switch D1 y D2 Primero se debe habilitar el enrutamiento por medio del OSPF en el proceso 4, seguido se asignan las redes que serán rutas del área 0, luego se activa el OSPFv2 todas las interfaces y por último no se deshabilitan las publicaciones de la interfaz Etherne2/2.

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-inter e2/2
D1(config-router)#exit
```

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-inter e2/2
D2(config-router)#exit
```

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.

Se habilita el protocolo OSPFv3 para R1, R3, D1 y D2.

Inicialmente se ingresa a la interface e0/1, seguido Se habilita el OSPF en el proceso 6 área 0 para publicar rutas, luego salimos de la interfaz e0/1, continuando en modo configuración global se ingresa en la interfaz S3/3 habilitando el OSPF en el proceso 6 área 0 para publicar rutas, luego salimos de la interfaz S3/3, posteriormente Se configura la tabla de rutas en la que se indica que la Ip Route 10.0.0.0 con Sub mascara 255.0.0.0 apunta a la interfaz null0 la cual es una interfaz virtual por ultimo Configuración ruta estática a la interfaz Null 0 para IPv6.

```
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)# default-information originate
R1(config-rtr)#inte e0/1
R1(config-if)#
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#inte s3/3
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
```

Ahora ingreso a la interface e0/1, seguido se habilita el OSPF en el proceso 6 área 0 para publicar rutas, luego salimos de la interfaz e0/1, continuando en modo configuración global se ingresa en la interfaz S3/3 habilitando el OSPF en el proceso 6 área 0 para publicar rutas, luego salimos de la interfaz S3/3

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#
R3(config)#inter e0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#
R3(config-if)#exit
R3(config)#interface s3/3
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#end
```

Para los switch D1 Y D2 Inicialmente se debe habilitar el enrutamiento por medio del OSPF en el proceso 6. Seguido se habilita el enrutamiento por medio del OSPF en el proceso 6, posteriormente deshabilito las publicaciones OSPFv3 en todas las interfaces, finamente no se deshabilitan publicaciones de la interfaz e2/2.

```
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 e2/2
D1(config-rtr)#exit

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-inte e2/2
D2(config-rtr)#exit
D2(config)#inter e2/2
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit

Figura 10 Configuración de protocolo ospfv2 y ospfv3 en router R3

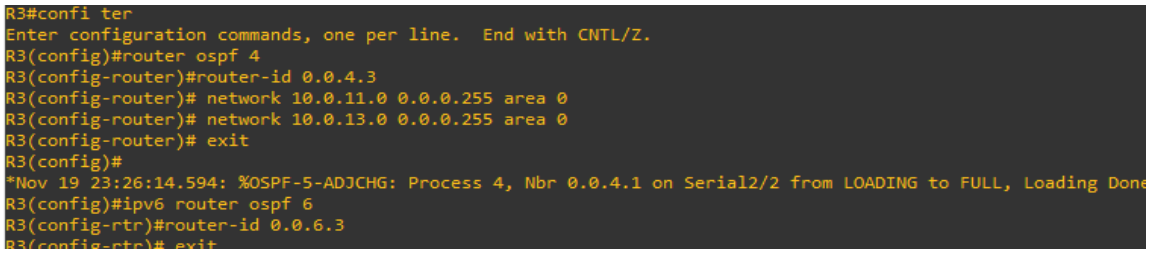


Figura 11 Configuración de protocolo ospfv2 y ospfv3 en router *D1*

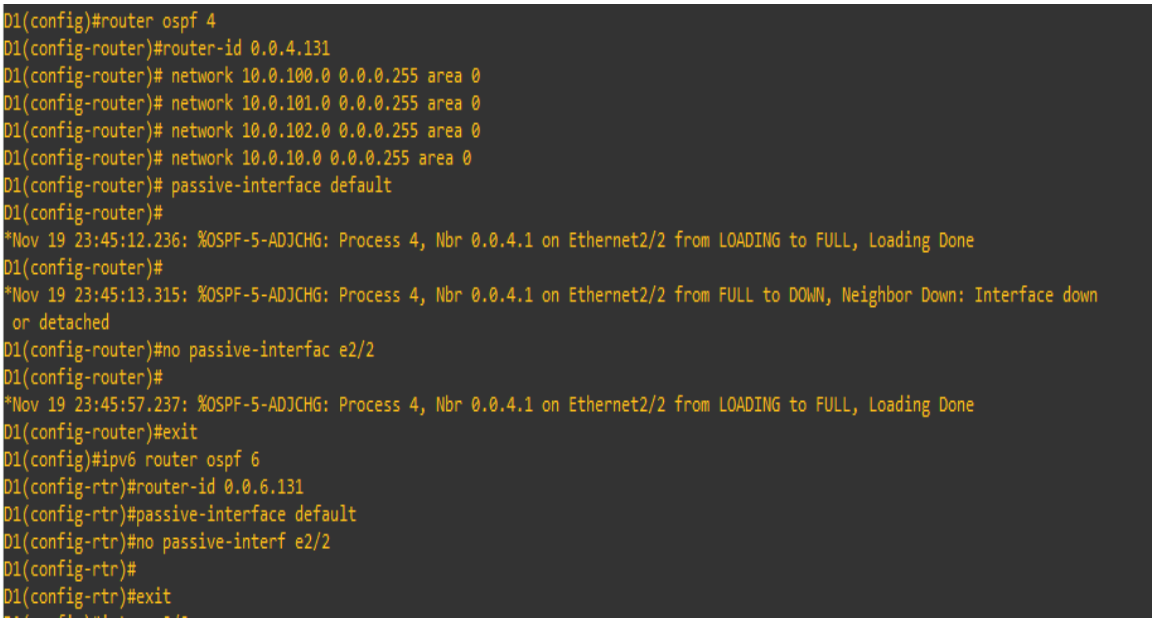
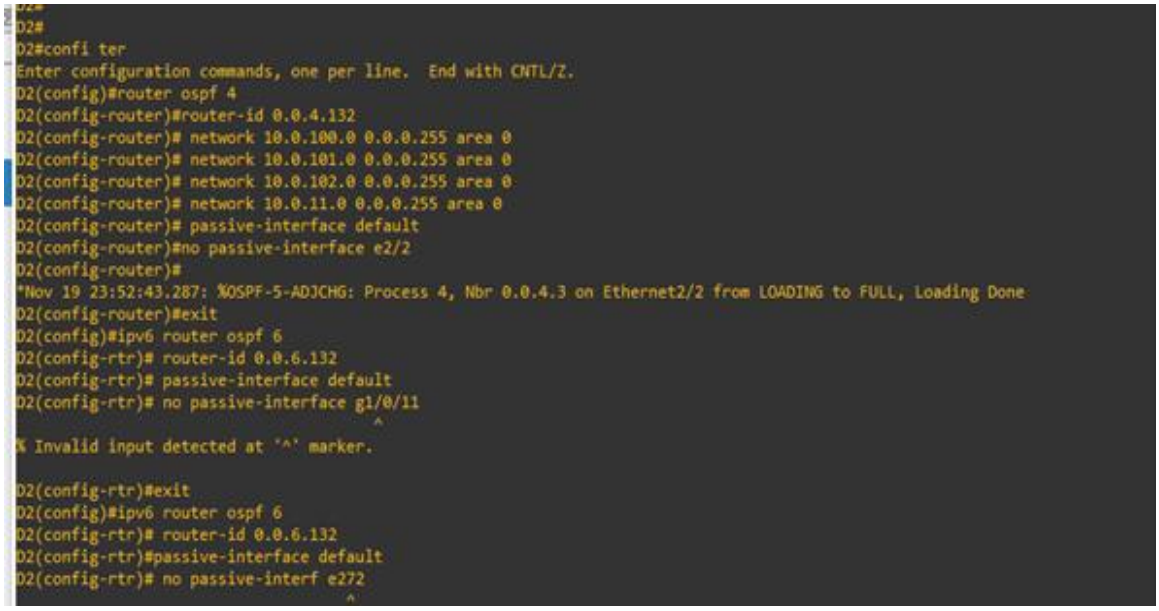


Figura 12 Configuración de protocolo ospfv2 y ospfv3 en router D2



3.3 En R2 en la “Red ISP”, configure MP-BGP.

inicialmente se configurar la rutas estáticas de la interfaz Loopback 0 para IPV4 con ruta por defecto (0.0.0.0/0), seguido se debe configurar las rutas estáticas de la interfaz Loopback 0 para IPV6 con ruta por defecto (::/0), posteriormente se usa BGP ASN 500, luego se usa BGP ASN 500 router-id 2.2.2.2, continuando se habilita una relación de vecindad IPv4 con R1 en ASN 300 , seguidamente se habilita una relación de vecindad IPv6 con R1 en ASN 300.

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)#
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

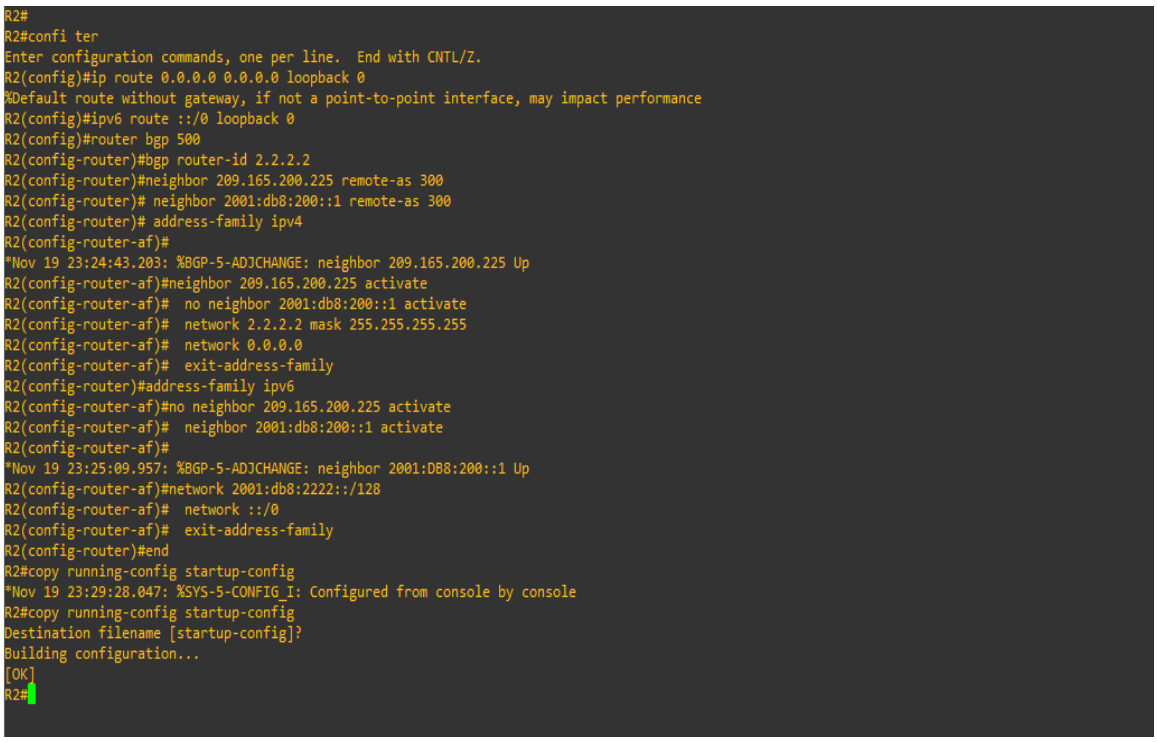
Ahora se habilita una relación de vecindad IPv4 con R1 en ASN 300 con dirección de familia, continuando con la activación de la dirección de vecindad en IPv4, luego se excluye la dirección de vecino de IPv6 en IPv4, continuado se asigna Router-id 2.2.2.2.a una Ruta por defecto (0.0.0.0/0). Se sale de la sub interfaz de direcciones vecino IPv4.

R2(config-router)# address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family

Ingreso a la sub interfaz de direcciones de vecindad IPv6, posteriormente se excluye la dirección de vecino de IPv4 en IPv6 continuado con la activación de la dirección de vecindad en IPv6, luego se ingresa Dirección de la red Loopback (/128) con Ruta por defecto (::/0), finalmente se debe salir de la sub interfaz de direcciones vecino IPv6R2.

R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family

Figura 13 Códigos para R2 en la "Red ISP", configure MP-BGP



En R1 en la "Red ISP", configure MP-BGP.

En este punto se debe configurar la tabla de rutas en la que se indica que la Ip Route 10.0.0.0 con Submask 255.0.0.0 la cual apunta a la interfaz null0 que es una interfaz virtual, continuando se configura la ruta estática a la interfaz Null 0 para IPv6, luego se usa BGP ASN 300, seguido de la configuración del ID del router en BGP, posteriormente se habilita una relación de vecindad IPv4 con R2 en ASN 500, del mismo modo se habilita una relación de vecindad IPv6 con R2 en ASN 500, seguidamente se especifica la familia de direcciones y se evita intercambio de direcciones IPv4 unicast de forma predeterminada, después se activa la dirección de vecindad en IPv4, luego se excluye la dirección de vecino de IPv6 en IPv4, así mismo como el anunciado de la red 10.0.0.0/8. En IPv6 address family, finalmente salimos de la sub interfaz de direcciones vecino IPv4.

```
R1(config)#
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)#no neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit-address-family
```

Ahora ingresamos sub interfaz de direcciones vecino IPv6 donde se excluye la dirección de vecindad de IPv4 en IPv6, luego se activa de la dirección de vecindad en IPv6, continuando se ingresa la Dirección de la red Loopback (/48), finalmente se debe salir de la sub interfaz de direcciones vecino IPv6.

```
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226
R1(config-router-af)#neighbor 2001:db8:200::2
R1(config-router-af)# network 2001:db8:100::/48
R1(config-router-af)# exit-address-family
R1(config-router)#
```

Figura 14 Códigos de configuración de protocolo de enrutamiento en router R1

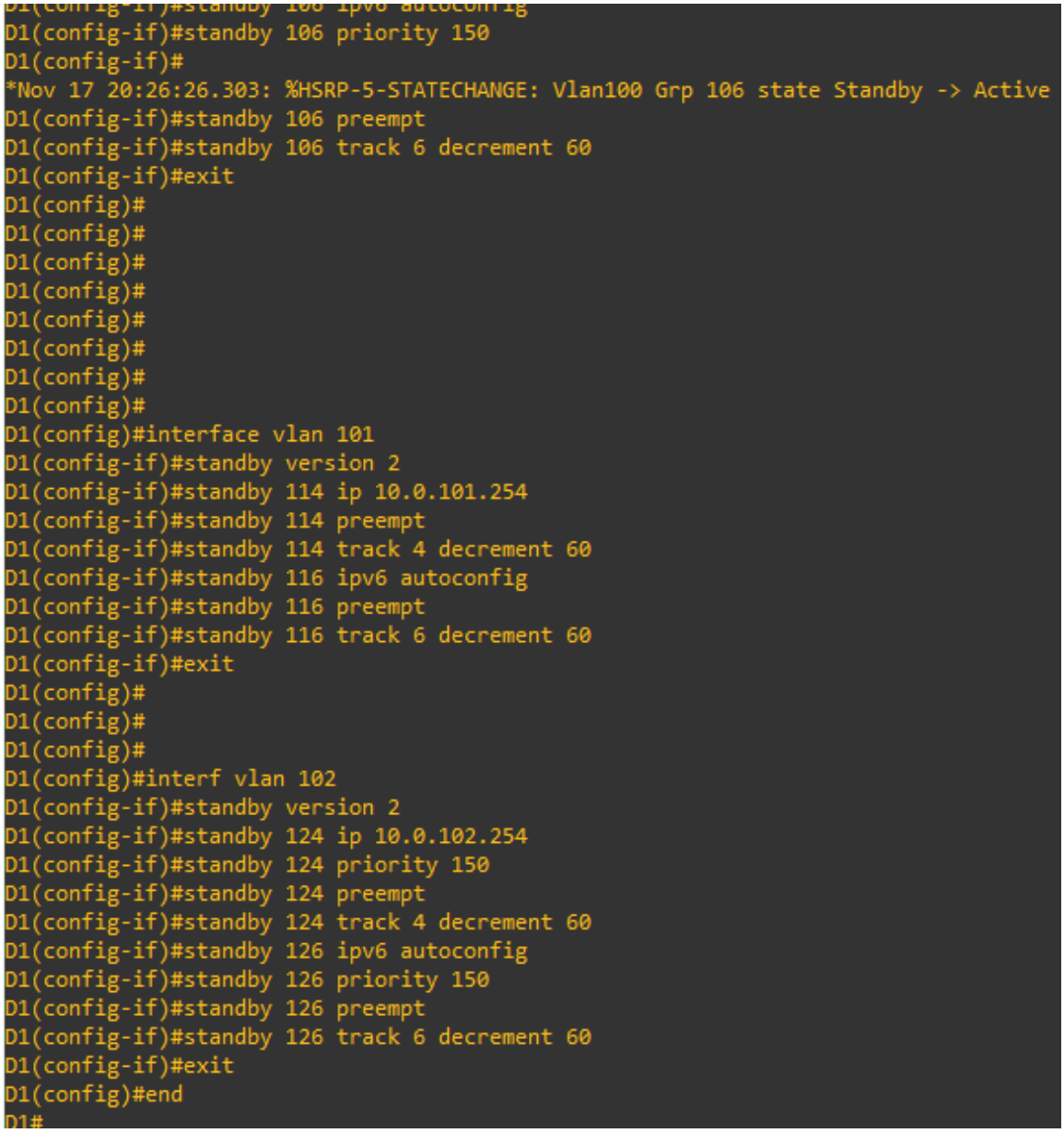
Figura 15 Códigos de configuración de protocolo de enrutamiento en router R2

```
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
*Nov 18 02:03:36.952: %BGP-5-ADJCHANGE: neighbor 209.165.200.225 Up
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)# network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-famil
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#
*Nov 18 02:05:54.107: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::1 Up
R2(config-router-af)# network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#exit
R2(config)#
```

Figura 16 Códigos de configuración de protocolo de enrutamiento en router R3

```
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#
*Nov 18 02:30:08.199: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.132 on Ethernet0/1 from LOADING to FULL, Loadi
ng Done
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)#exit
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#
R3(config)#inter e0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#
*Nov 18 02:31:12.485: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.132 on Ethernet0/1 from LOADING to FULL, Loa
ding Done
R3(config-if)#exit
R3(config)#interface s3/3
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#end
```

Figura 17 Códigos de configuración de protocolo de enrutamiento en switch D1



```
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#
*Nov 17 20:26:26.303: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#
D1(config)#
D1(config)#
D1(config)#
D1(config)#
D1(config)#
D1(config)#
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
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)#
D1(config)#
D1(config)#interf vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254
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(config)#end
D1#
```

Figura 18 Códigos de configuración de protocolo de enrutamiento en switch D2

```
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#
D2(config)#
D2(config)#
D2(config)#
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)#
D2(config)#
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#
D2(config)#
D2(config)#track 6 ip sla 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#
D2(config)#
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
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)#
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
```

Parte 4 . Configurar La Redundancia Del Primer Salto (First Hop Redundancy)

Tabla 4 Tareas de configuración parte 4

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLA que prueben la accesibilidad de la interfaz R1 G0 / 0/1.	Cree dos SLA de IP. ▪ Utilice el SLA número **4** para IPv4. ▪ Utilice el SLA número **6** para IPv6. Los IP SLA probarán la disponibilidad de la interfaz R1 G0 / 0/1 cada 5 segundos. Programe el SLA para una implementación inmediata sin hora de finalización. Cree un objeto IP SLA para IP SLA 4 y uno para IP SLA 6. ▪ Utilice la pista número **4** para IP SLA 4. ▪ Utilice la pista número **6** para IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de abajo a arriba después de 10 segundos, o de arriba a abajo después de 15 segundos.
4.2	En D2, cree IP SLA que prueben la accesibilidad de la interfaz R3 G0 / 0/1.	Cree dos SLA de IP. ▪ Utilice el SLA número **4** para IPv4. ▪ Utilice el SLA número **6** para IPv6. Los IP SLA probarán la disponibilidad de la interfaz R3 G0 / 0/1 cada 5 segundos. Programe el SLA para una implementación inmediata sin hora de finalización. Cree un objeto IP SLA para IP SLA 4 y uno para IP SLA 6. ▪ Utilice la pista número **4** para IP SLA 4. ▪ Utilice la pista número **6** para IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de abajo a arriba después de 10 segundos, o de arriba a abajo después de 15 segundos.
4.3	En D1, configure HSRPv2.	D1 es el enrutador principal para las VLAN 100 y 102; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP versión 2.

		Configure IPv4 HSRP group **104** para VLAN 100: ▪ Asigne la dirección IP virtual **10.0.100.254** . ▪ Establezca la prioridad de grupo en **150** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 4 y disminuir en 60. Configure el grupo IPv4 HSRP **114** para VLAN 101: ▪ Asigne la dirección IP virtual **10.0.101.254** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 4 para disminuir en 60. Configure el grupo **124 de** IPv4 HSRP para la VLAN 102: ▪ Asigne la dirección IP virtual **10.0.102.254** . ▪ Establezca la prioridad de grupo en **150** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 4 para disminuir en 60. Configure el grupo **106 de** IPv6 HSRP para VLAN 100: ▪ Asigne la dirección IP virtual usando **ipv6 autoconfig** . ▪ Establezca la prioridad de grupo en **150** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 6 y disminuir en 60. Configure el grupo **116 de** IPv6 HSRP para VLAN 101: ▪ Asigne la dirección IP virtual usando **ipv6 autoconfig** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 6 y disminuir en 60. Configure el grupo **126 de** IPv6 HSRP para la VLAN 102: ▪ Asigne la dirección IP virtual usando **ipv6 autoconfig** . ▪ Establezca la prioridad de grupo en **150** . ▪ Habilite la preferencia.

		▪ Seguimiento del objeto 6 y disminuir en 60.
	En D2, configure HSRPv2.	D2 es el enrutador principal para VLAN 101; por lo tanto, la prioridad también se cambiará a 150. Configure HSRP versión 2. Configure IPv4 HSRP group **104** para VLAN 100: ▪ Asigne la dirección IP virtual **10.0.100.254** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 4 y disminuir en 60. Configure el grupo IPv4 HSRP **114** para VLAN 101: ▪ Asigne la dirección IP virtual **10.0.101.254** . ▪ Establezca la prioridad de grupo en **150** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 4 para disminuir en 60. Configure el grupo **124 de** IPv4 HSRP para la VLAN 102: ▪ Asigne la dirección IP virtual **10.0.102.254** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 4 para disminuir en 60. Configure el grupo **106 de** IPv6 HSRP para VLAN 100: ▪ Asigne la dirección IP virtual usando **ipv6 autoconfig** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 6 y disminuir en 60. Configure el grupo **116 de** IPv6 HSRP para VLAN 101: ▪ Asigne la dirección IP virtual usando **ipv6 autoconfig** . ▪ Establezca la prioridad de grupo en 150. ▪ Habilite la preferencia. ▪ Seguimiento del objeto 6 y disminuir en 60. Configure el grupo **126 de** IPv6 HSRP para la VLAN 102:

		▪ Asigne la dirección IP virtual usando **ipv6 autoconfig** . ▪ Habilite la preferencia. ▪ Seguimiento del objeto 6 y disminuir en 60.

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 e0/1.

Inicialmente se crea SLA número 4 para IPv4, seguido se verifica la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV4, luego IP SLAs probarán la disponibilidad de la interfaz R1 e0/1 cada 5 segundos, finalmente se debe salir de la configuración

ip sla 4.D1(config)#ip sla 4
D1(config-ip-sla)#icmp-echo 10.0.10.1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#

Ahora se debe crear la SLA número 4 para IPv6, seguido se Verifica la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV6, IP SLAs probarán la disponibilidad de la interfaz R1 e0/1 cada 5 segundos, finalmente se debe salir de la configuración IP sla 6.

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)#
D1(config)#
D1(config)#exit

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 e/0/1.

Inicialmente se crea SLA número 4 para IPv4, seguido se verifica la conectividad de extremo a extremo entre dispositivos a través de la red (D2 a R3) en IPV4, luego IP SLAs probarán la disponibilidad de la interfaz R3 e0/1 cada 5 segundos, finalmente se debe salir de la configuración

D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#

Ahora se debe crear la SLA número 4 para IPv6, seguido se Verifica la conectividad de extremo a extremo entre dispositivos a través de la red (D2 a R3) en IPV6, IP SLAs probarán la disponibilidad de la interfaz R3 e0/1 cada 5 segundos, finalmente se debe salir de la configuración IP sla 6.

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)#
```

4.3 En D1 configure HSRPv2

Primero se debe ingresar a la interfaz Vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106, seguido de la configuración de HSRP versión 2, continuando con la asignación de dirección IP virtual 10.0.100.254 en IPv4 HSRP grupo 104, seguido se establece la prioridad del grupo en 150 y Se habilita la preferencia.

```
D1(config)#inter vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
```

Ahora se rastrea el objeto 4 y decremente en 60, seguido de la dirección IP virtual como automática y prioridad del grupo en 150.

```
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)#
```

Finamente se habilita la preferencia y se rastrea el objeto 6 decremente en 60, luego salimos de la configuración Vlan 100.

```
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#
D1(config)#
```

4.4 En D2, configure HSRPv2

Inicialmente se debe ingresar a la interfaz Vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106, seguido de la configuración de HSRP versión 2, continuando se establece la prioridad del grupo en 150 y Se habilita la preferencia.

```
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt
```

Inicialmente se debe ingresar a la interfaz vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106, seguido de la configuración de HSRP versión 2, continuando se establece la prioridad del grupo en 150 y Se habilita la preferencia.

```
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)#
```

Inicialmente se debe ingresar a la interfaz Vlan 101, IPv4 HSRP grupo 114 e IPV6 HSRP grupo 116, seguido de la configuración del protocolo Configuración de HSRP versión 2, continuando se asigna dirección IP virtual 10.0.101.254 en IPv4 HSRP grupo 114 con prioridad del grupo en 150.

```
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
```

Seguido se habilita la preferencia, seguido Rastrea el objeto 6 y decremente en 60, luego se configura la dirección IP virtual como automática y se da Prioridad del grupo en 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
```

Ahora se habilita la preferencia, seguido del rastreo del objeto 6 y decremente en 60 y finalmente salimos de la configuración Vlan 101.

```
D2(config-if)#standby 116 preempt
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#
```

Inicialmente se ingresa a la interfaz Vlan 102, para después configurar IPv4 HSRP grupo 124 así como la IPV6 HSRP grupo 126, luego se habilita la configuración de HSRP versión 2, continuando con la asignación de dirección IP virtual 10.0.102.254 en IPv4 HSRP grupo 124 y se habilita la preferencia.

```
D2(config)#interf vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
```

Ahora se rastrea el objeto 4 y decremente en 60, seguido de configura la dirección IP virtual como automática, luego se habilita la preferencia y se Rastrea el objeto 6 y decremente en 60, finalmente salimos de la configuración Vlan 102

```
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)#
```

Parte 5 Seguridad

Tabla 5 Tareas de configuración parte 5

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado mediante el algoritmo de cifrado SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un localizador y asegúrelo con el algoritmo de cifrado SCRYPT.	Detalles de la cuenta cifrada SCRYPT: ▪ Nombre de usuario local: **sadmin** ▪ Nivel de privilegio **15** ▪ Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS: ▪ La dirección IP del servidor RADIUS es 10.0.100.6. ▪ Puertos 1812 y 1813 del servidor RADIUS UDP. ▪ Contraseña: **$ trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.	Especificaciones de autenticación AAA: ▪ Usar la lista de métodos predeterminados ▪ Validar con el grupo de servidores RADIUS ▪ De lo contrario, use la base de datos local.
5,6	Verifique el servicio AAA en todos los dispositivos (excepto R2).	**Cierre** sesión e inicie sesión en todos los dispositivos (excepto R2) utilizando el nombre de usuario **raduser** y la contraseña **upass123** . Deberías tener éxito.

Para el desarrollo del este punto el cual se incluyen todos los dispositivos inicialmente se utiliza el del algoritmo de encriptación SCRYPT, luego Se habilita Autenticación, autorización, contabilidad (AAA)que permite el acceso a solo autorizados, posteriormente se debe ingresa a la interfaz del servidor Radius ,continuando se asignando IP del servidor Radius y los puertos UPD, seguido se Asigna la contraseña, finalmente salimos de la interfaz del servidor Radius y Se realiza autenticación por defecto

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT**.**

D1(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D2(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R1(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R3(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

5.3 En todos los dispositivos (excepto R2), habilite AAA.

R1(config)#AAA new-model

R3(config)#AAA new-model

D1(config)#AAA new-model

D2(config)#AAA new-model

A1(config)#AAA new-model

5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

R1(config)#radius server RADIUS
R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $trongPass
R1(config-radius-server)#exit
R3(config)#radius server RADIUS

R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass
R3(config-radius-server)#exit

D1(config)#radius server RADIUS
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $trongPass
D1(config-radius-server)#exit

D2(config)#radius server RADIUS
D2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)# key $trongPass
D2(config-radius-server)#exit

A1(config)#radius server RADIUS
A1(config-radius-server)#sv4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)#exit

En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

R1(config)#aaa authentication login default group radius local

R3(config)#aaa authentication login default group radius local

D1(config)#aaa authentication login default group radius local

D2(config)#aaa authentication login default group radius local

A1(config)#aaa authentication login default group radius local

Verifique el servicio AAA en todos los dispositivos (except R2).

Figura 19 Solicitud de autenticación router R1

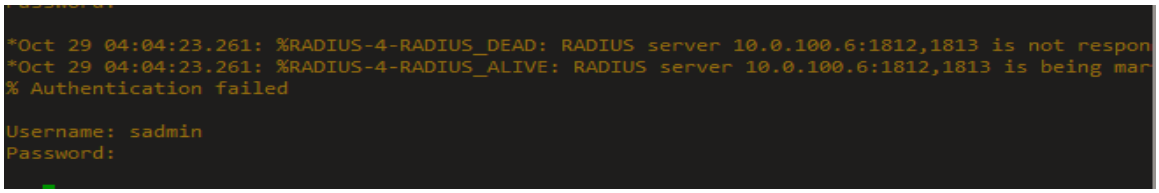


Figura 20 Solicitud de autenticación router R3

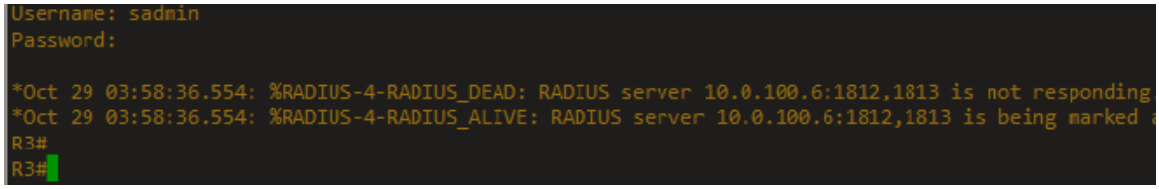


Figura 21 Solicitud de autenticación switch D1

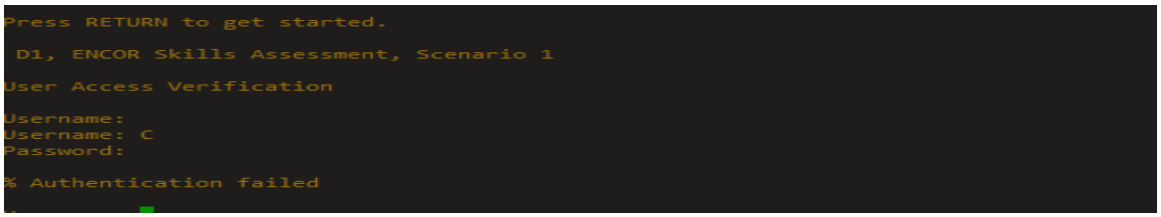


Figura 22 Solicitud de autenticación switch D2

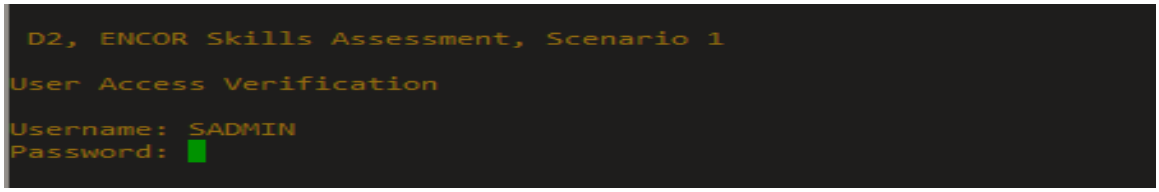
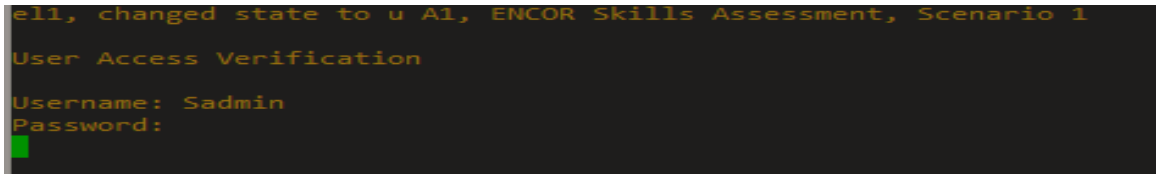


Figura 23 Solicitud de autenticación switch A1



Parte 6. Configure Las Funciones De Administración De Red

Tabla 6 Tareas de configuración parte 6

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.

6.2	Configure R2 como maestro NTP.	Configure R2 como maestro NTP en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2 y A1.	Configure NTP de la siguiente manera: ▪ R1 debe sincronizarse con R2. ▪ R3, D1 y A1 para sincronizar la hora con R1. ▪ D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2.	Los registros del sistema deben enviarse a la PC1 en 10.0.100.5 en el nivel de ADVERTENCIA.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2.	Especificaciones de SNMPv2: ▪ Solo se utilizará SNMP de solo lectura. ▪ Limite el acceso SNMP a la dirección IP de la PC1. ▪ Configure el valor de contacto SNMP a su nombre. ▪ Establezca la cadena de comunidad en **ENCORSA** . ▪ En R3, D1 y D2, habilite el envío de trampas config y ospf. ▪ En R1, habilite el envío de trampas bgp, config y ospf. ▪ En A1, habilite el envío de la configuración de trampas.

6.1 Configure R2 como un NTP maestro.
En este punto se configura la Sincronización reloj por medio del enrutamiento.

```
R2(config)#ntp master 3
R2(config)#end
```

6.3 Configure NTP en R1, R3, D1, D2, y A1.
Sincronización de tiempo con el servidor 2.2.2.2

Se configura NTP para sincronizar con R2 por medio de Loopback 0 Seguido se configura Syslog en nivel WARNING, finalizando se configuar Syslog a la PC1 10.0.100.5.

```
R1(config)#ntp server 2.2.2.2
R1(config)# logging trap warning
R1(config)#logging host 10.0.100.5
R1(config)#logging on
R1(config)#
```

Se configura NTP para sincronizar hora con R1, a continuación, se configura Syslog en nivel WARNING, luego se configura Syslog a la PC1 10.0.100.5 finalmente se enciende configuración Syslog.

```
R3(config)# ntp server 10.0.10.1
R3(config)#logging trap warning
R3(config)#logging host 10.0.100.5
R3(config)#logging on
```

Se configura NTP para sincronizar hora con R1, a continuación, se configura Syslog en nivel WARNING, luego se configura Syslog a la PC1 10.0.100.5 finalmente se enciende configuración Syslog.

```
D1(config)# ntp server 10.0.10.1
D1(config)#logging trap warning
D1(config)#logging host 10.0.100.5
D1(config)# logging on
```

Se configura NTP para sincronizar hora con R1, a continuación, se configura Syslog en nivel WARNING, luego se configura Syslog a la PC1 10.0.100.5 finalmente se enciende configuración Syslog.

```
D2(config)# ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)# logging on
```

Se configura NTP para sincronizar hora con R1, a continuación, se configura Syslog en nivel WARNING, luego se configura Syslog a la PC1 10.0.100.5 finalmente se enciende configuración Syslog.

```
A1(config)# ntp server 10.0.10.1
A1(config)#logging trap warning
A1(config)#logging host 10.0.100.5
A1(config)# logging on
```

6.4 Configure Syslog en todos los dispositivos excepto R2

Para los dispositivos R1, R3, D1, D2, A1 se realiza la Configuración de SNMPv2c en modo estándar, luego se configura el límite de acceso SNMP a la PC1, finalmente salimos de la configuración SNMPv2c

```
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)#permit host 10.0.100.5
R1(config-std-nacl)#exit
```

```
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)# permit host 10.0.100.5
R3(config-std-nacl)#exit
```

```
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#EXIT

D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#EXIT

A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#EXIT
```

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Para los dispositivos R1, R3, D1, D2, A1 Se configura el valor de contacto SNMP con el nombre Cisco Student, luego se establece community string en ENCORSA, seguido del Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA, continuando la configuración donde se identifica cada interfaz para la identificación SNMP de la interfaz usada, posteriormente se Envían notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP) y se Envían notificaciones de configuración.

```
R1(config)#snmp-server contact Cisco Student
R1(config)#snmp-server community ENCORSA ro SNMP-NMS
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)#snmp-server ifindex persist
R1(config)#snmp-server enable traps bgp
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
R1(config)#exit
R1#

R3(config)#snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server ifindex persist
R3(config)# snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#exit
R3#

D1(config)#snmp-server contact Cisco Student
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps
D1(config)#snmp-server enable traps ospf
D1(config)#END
D1#
```

```
D2(config)#snmp-server contact Cisco Student
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server ifindex persist
D2(config)#snmp-server enable traps
D2(config)#snmp-server enable traps ospf
D2(config)#END
D2#

A1(config)#snmp-server contact Cisco Student
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server ifindex persist
A1(config)#snmp-server enable traps
A1(config)#snmp-server enable traps ospf
A1(config)#END
A1#
```

Figura 24 Códigos de configuración funciones de administración de red en ruoter R1

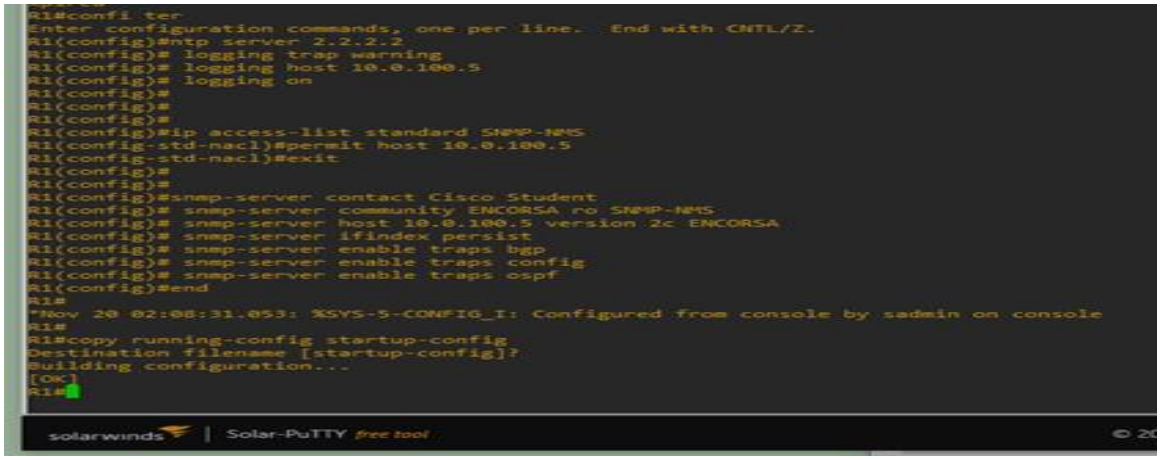


Figura 25 Códigos de configuración funciones de administración de red en ruoter R2

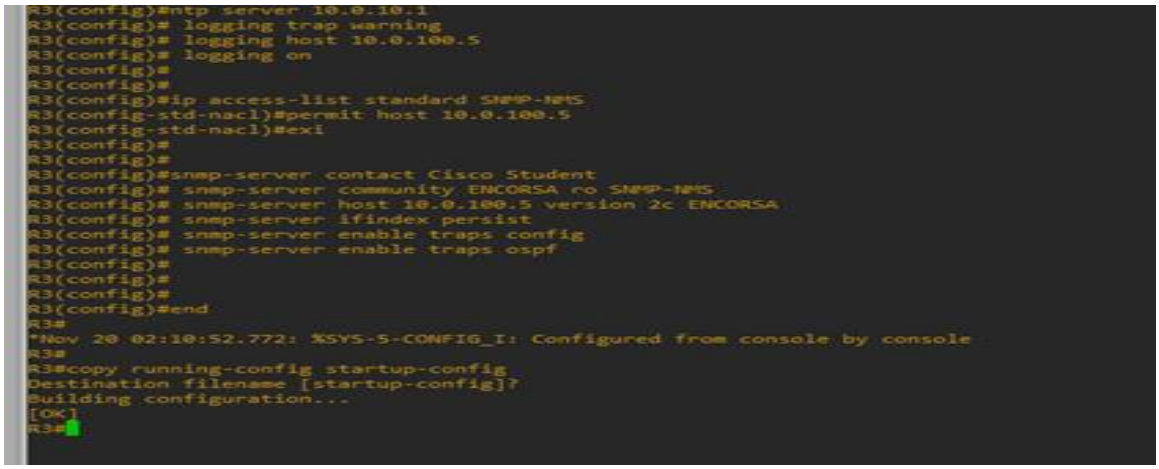
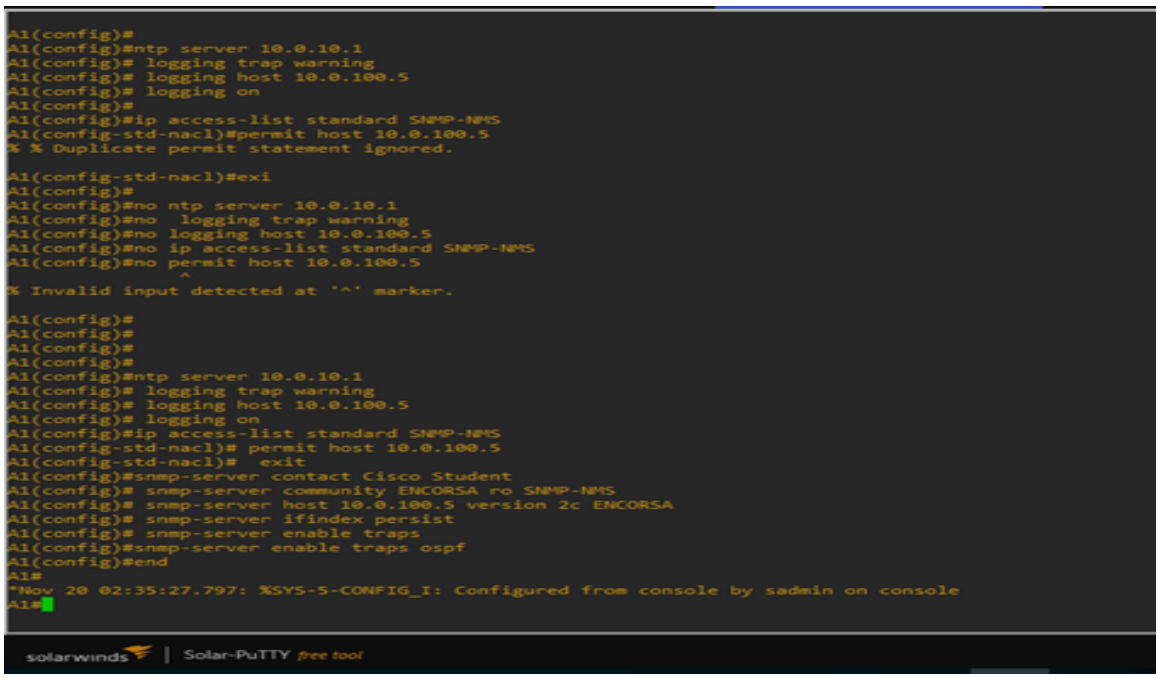


Figura 26 Códigos de configuración funciones de administración de red en switch D2

Figura 27 Códigos de configuración funciones de administración de red en switch A1



CONCLUSIONES

En esta actividad se logra poner en práctica los temas aprendidos durante el desarrollo del diplomado tales como la configuración básica de dispositivos expuestos en la topología, la configuración de una capa 2 de una red, la configuración de protocolos de enrutamiento, la configuración de la Redundancia del Primer Salto, la seguridad de una red y la configuración de las funciones de Administración de una red.

Para el desarrollo de la actividad hubo la necesidad de utilizar el programa gns3 dado que el programa Packet Tracer presenta características de simulación de redes limitadas y no me fue posible abordar la parte tres, cuatro, cinco y seis

Para el desarrollo de la actividad hubo la necesidad de investigar que archivos .bin funcionaban para el desarrollo de los puntos donde había la necesidad de utilizar los protocolo ipv6 y ospfv3.

El simulador GNS3 fue muy importante para el desarrollo de la actividad en donde se presentaron fallas al momento de configurar los Switchs dado a que no soportaba la capa 3 del modelo OSI; hubo la necesidad de descargar archivos Cisco IOU L2 Y Cisco IOU L3, así como utilizar herramientas de la máquina virtual y programas como PuTTY para configurar las actualizaciones para poder utilizar los switchs y Reuters adecuados.

BIBLIOGRAFÍA

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de: https://staticcourseassets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://staticcourseassets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de: https://staticcourseassets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static courseassets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1 Página 66 de 66

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1 45

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: https://static courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-courseassets.s3.amazonaws.coRSE50ES/module9/index.html#9.0.1

https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

http://www.ieslosviveros.es/alumnos/asig8/carpeta812/PROTOCOLOS_DE_ENRUTAMIENTO.pdf

https://www.ambit-bst.com/blog/todo-lo-que-debes-saber-de-cisco-packet-tracer
https://ccnadesdecero.com/curso/ospf/

http://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf

http://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf