DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JONATAN DAMIAN CHONA BASTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA ELECTRONICA
CUCUTA
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO CCNP
PRUEBA DE HABILIDADES PRACTICAS CCNP

JONATAN DAMIAN CHONA BASTO

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 BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA ELECTRONICA
CUCUTA
2021

NOTA DE ACEPTACION

_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

CUCUTA, 29 de noviembre del 2021

AGRADECIMIENTOS

En primer lugar, agradecer a mi familia porque de una u otra manera estuvieron siempre apoyándome para poder seguir con mis estudios, aun cuando mis ánimos decaían, mi hermana que en todo momento decía sentirse orgulloso de mi por luchar por mis objetivos y servirle como ejemplo a seguir.

También al instructor Gerardo Granados Acuña, quien con sus conocimientos nos guio y oriento en cada una de las etapas del proceso que se desarrollo en el proyecto para lograr los objetivos previstos.

Y por último a la UNAD por brindarme los recursos, herramientas y plataformas necesarias para poder conseguir una carrera profesional siendo lideres en estrategias virtuales para que muchos podamos alcanzar.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Topologia:
En primera instancia se tiene la presentación del elemento que conforma todo el trabajo que se está desarrollando actualmente, dado que este aspecto hace referencia directa a una parte importante en la rama de las ciencias matemáticas, pero en este caso se sabe que este apartado se encuentra completamente dedicado al estudio de todas las propiedades pertenecientes a los cuerpos geométricos que actualmente se encuentran inalterados por una serie de transformaciones continuas.

Red:
En segunda instancia es importante mencionar un elemento que rige por completo el espectro de trabajo que se tiene en una topología en particular, dado que este hace referencia a todo conjunto de nodos y elementos digitales que previamente han sido conectados entre sí, todo esto mediante la implementación especifica de dispositivos de índole físico, y que estos a su vez tienen la función de realizar el intercambio de datos entre usuarios conectados a la misma.

Sistemas:
Posterior a lo anteriormente mencionado en este documento se tiene un aspecto que influye en todo el estudio realizado en este proyecto, dado que los sistemas son básicamente una serie de objetos que poseen un funcionamiento complejo, y que estos a su vez se encuentran entrelazados con al menos un componente de todo el campo de trabajo actualmente disponible. Todo esto siendo una especificación de índole conceptual o material.

Protocolo:
Por otra parte, se tiene el proceso mediante el cual se pueden ejecutar todas las tareas relacionadas con el intercambio de datos entre usuarios, dado que un protocolo se puede definir como un sistema de reglas y condiciones que permiten que dos o más entidades propias de un sistema tengan la capacidad de comunicarse exitosamente entre ellas, siendo que luego de esto será posible transmitir sin ningún problema la información deseada.

Direccion IP:
Por último, se tiene el componente encargado de identificar cada elemento ubicado al interior de una topología en especial, siendo que para este caso se puede decir que la dirección IP es simplemente un conjunto de números, los cuales pueden identificar fácilmente un componente de una red de telecomunicaciones, siendo que esto se hace de manera lógica y jerárquica, y hacia una interfaz especifica perteneciente a la red que posee un dispositivo en particular

RESUMEN

En este proyecto de investigación estará enfocado en el análisis y control de un sistema topológico el cual permitirá realizar el intercambio de datos entre una amplia cantidad de usuarios de una manera eficiente y ordenada, este sistema cuenta con la presencia de tres router, 3 switches y por ultimo 3 ordenadores, los cuales tendrán la capacidad de recibir y enviar información sin ningún tipo de inconveniente, dado que cada uno de ellos estará configurado adecuadamente mediante el proceso de configuración respectivo de cada componente en particular, dado que en este caso se especificaran sus direcciones IP y máscaras de subred, cabe recalcar que para el desarrollo de este proyecto será necesario conocer el modo el en cual son utilizados los comandos CLI de cada componentes presente en la topología.

Palabras claves: CISCO, CCNP, Redes, Conmutación,

ABSTRACT

This research project will focus on the analysis and control of a topological system which will allow the exchange of data between a large number of users in an efficient and orderly manner, this system has the presence of three routers, 3 switches and finally 3 computers, which will have the ability to receive and send information without any inconvenience, since each of them will be configured properly through the respective configuration process of each particular component, since in this case their IP addresses and subnet masks, it should be noted that for the development of this project it will be necessary to know the way in which the CLI commands of each component present in the topology are used.

Keywords: router, switch, computer, ethernet, cli, topology, network.

INTRODUCCION

Para el desarrollo de este proyecto de investigación será importante conocer la forma en la cual trabaja una topología de red en particular, dado que para realizar múltiples conexiones y que estas a su vez puedan compartir información, es necesario conocer inicialmente sus métodos de conexión, al igual que la forma en la cual se configuran, dado que para solventar esta problemática se debe tener un conocimiento básico en cuanto a los comandos, siendo que por este medio será posible establecer prioridades, otorgar permisos, definir máscaras de subred, realizar configuraciones de redes LAN, entre otros.

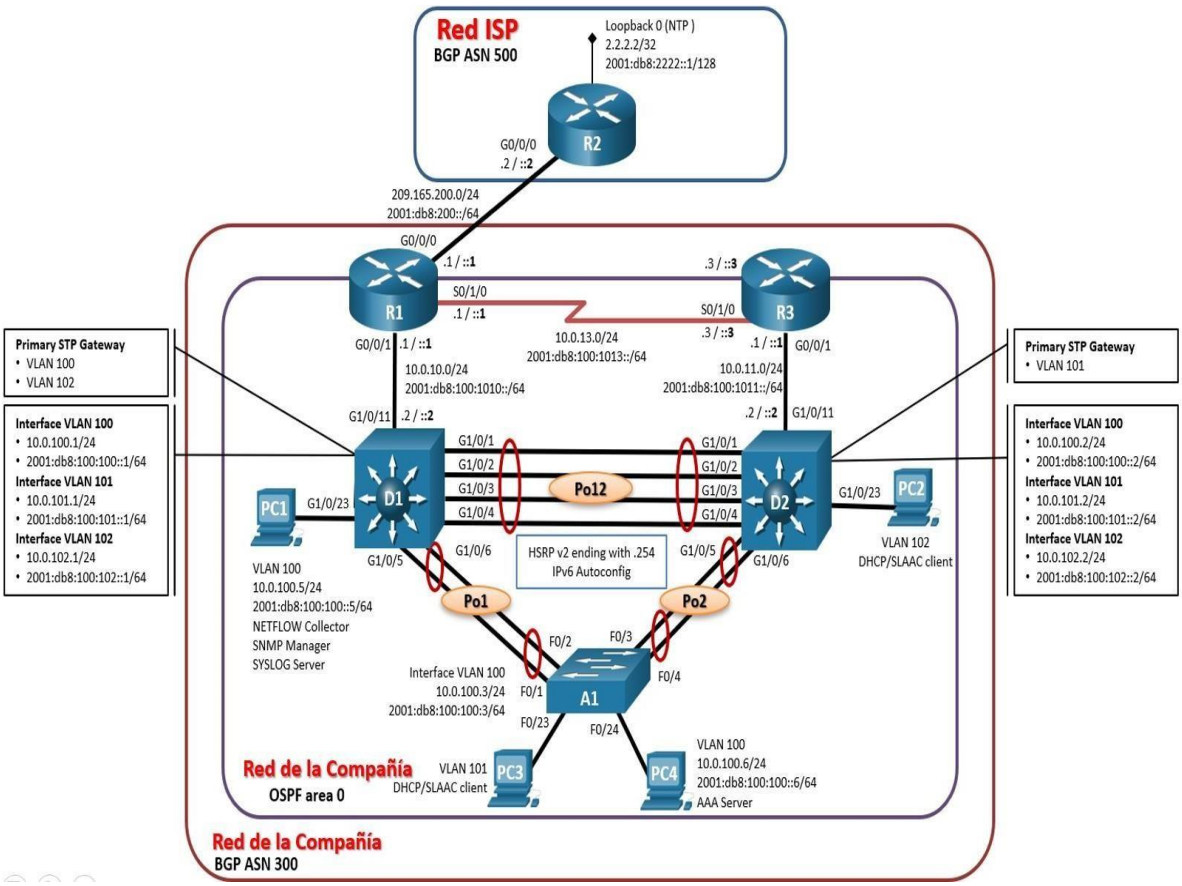
El desarrollo de la topología de red de la compañía propuesta es bastante compleja compuesta por 3 router, 3 switches y 4 PCs donde deberá haber una accesibilidad completa de entre toda la red, de un extremo a otro y garantizarles a los usuarios un soporte confiable.

Para eso se desarrollará las respectivas configuraciones en cada uno de los equipos que componen la red para que los servicios sean operativos y todos los protocolos cumplan con lo establecido dentro de la red de la compañía y para ello se verificara cada configuración para garantizar que cumplan y los dispositivos funcionen

DESARROLLO

ESCENARIO PROPUESTO

Figura 1: Topología del Escenario propuesto



Fuente: Autor

TABLA DE DIRECCIONAMIENTO

Tabla 1: Tabla de 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

Fuente: Autor

Objetivos

Parte 1: construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
Parte 2: configurar la capa dos de la red y el soporte de voz
Parte 3: configurar los protocolos de enrutamiento
Parte 4: configurar la redundancia del primer salto.
Parte 5: configurar la seguridad.
Parte 6: Configurar las características de administración de red.

Escenario

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "**Red de laCompañía**" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Nota: Los routers usados son Cisco 4221 con CISCO IOS XE versión 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco

IOS XE versión 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS versión 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variarde lo que se muestra en las prácticas de laboratorio.

Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tenganconfiguraciones de inicio.

Nota: La plantilla de Switch Data base Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soportaIPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global **sdm prefer dual-ipv4-and-ipv6 default**. Cambiar la plantilla requerirá el reinicio del switch.

Recursos necesarios

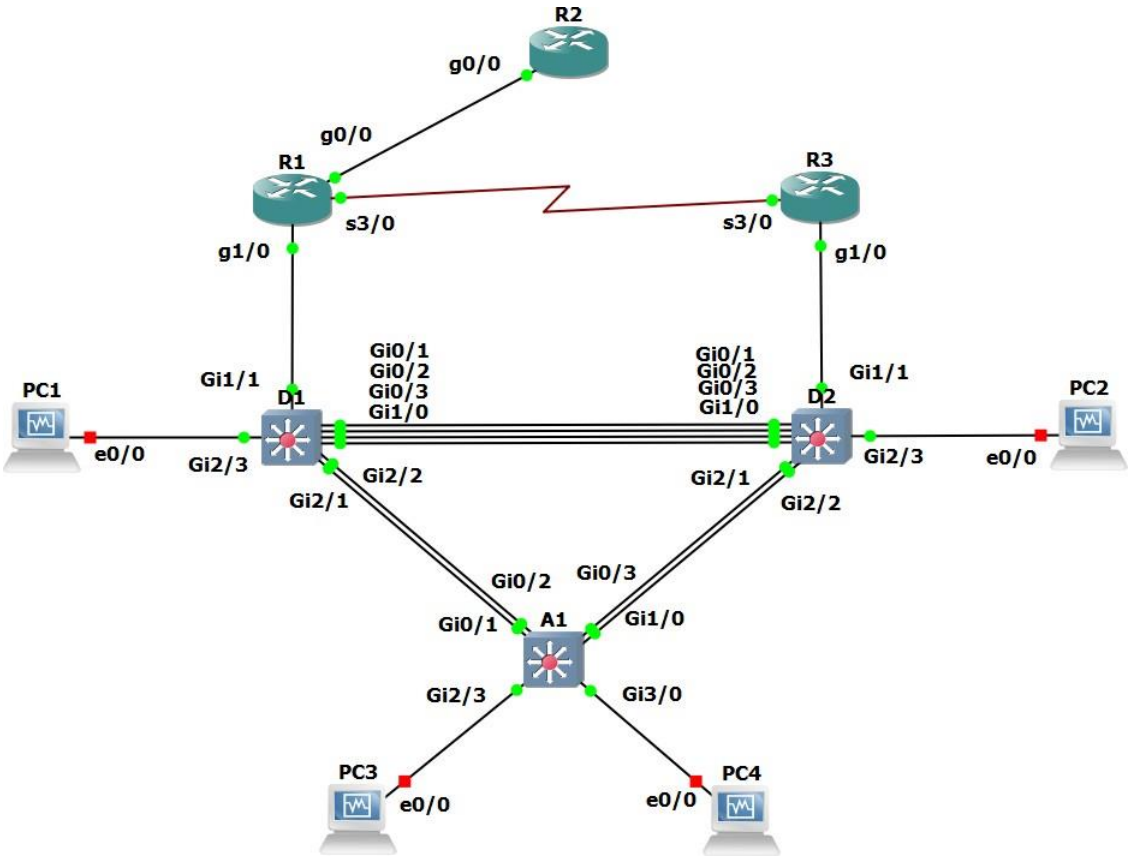
- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 2 switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 1 switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
- 4 PC (utilice el programa de emulación de terminal)
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
- Los cables Ethernet y seriales van como se muestra en la topología.

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

Paso 1: Cablear la red como se muestra en la topología.

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

Figura 2: Montaje de Topología de Red



Fuente: Autor

Paso 2: Configurar los parámetros básicos para cada dispositivo.

a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

Router R1

hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous

```
exit
interface g0/0
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 g1/0
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s3/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
```

Router R2

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

Router R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g1/0
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s3/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

Switch D1

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
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 g1/1
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g0/0-3,g1/0,g1/2-3,g2/0-3,g3/0-3
shutdown
exit
```

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
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 g1/1
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
```

```
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g0/0-3,g1/0,g1/2-3,g2/0-3,g3/0-3
shutdown
exit
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
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 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
```

```
exit
interface range g1/1-3,g2/0-3,g3/0-3
shutdown
exit
```

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

c. Configure 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.

Parte 2: Configurar la capa 2 de la red y el soporte de Host

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibirdireccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:
Figura 3: Interface troncal

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.

Switch D1

```
interface range g0/1-3,g1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
 no shutdown
 exit
interface range g2/1-2
 switchport trunk encapsulation dot1q
```

switchport mode trunk
switchport trunk native vlan 999
no shutdown
exit

Switch D2

interface range g0/1-3,g1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
exit
interface range g2/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
exit

Switch A1

interface range g0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
exit
interface range g0/3,g1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
no shutdown
exit

2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
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	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

	respaldo en caso de falla del puente raíz (root bridge).	

Switch D1

```
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
```

Switch D2

```
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
```

Switch A1

```
spanning-tree mode rapid-pvst
```

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

Switch D1

```
interface range g0/1-3,g1/0
 channel-group 12 mode active
 exit
interface range g2/1-2
 channel-group 1 mode active
 exit
```

Switch D2

```
interface range g0/1-3,g1/0
 channel-group 12 mode active
 exit
interface range g2/1-2
 channel-group 2 mode active
 exit
```

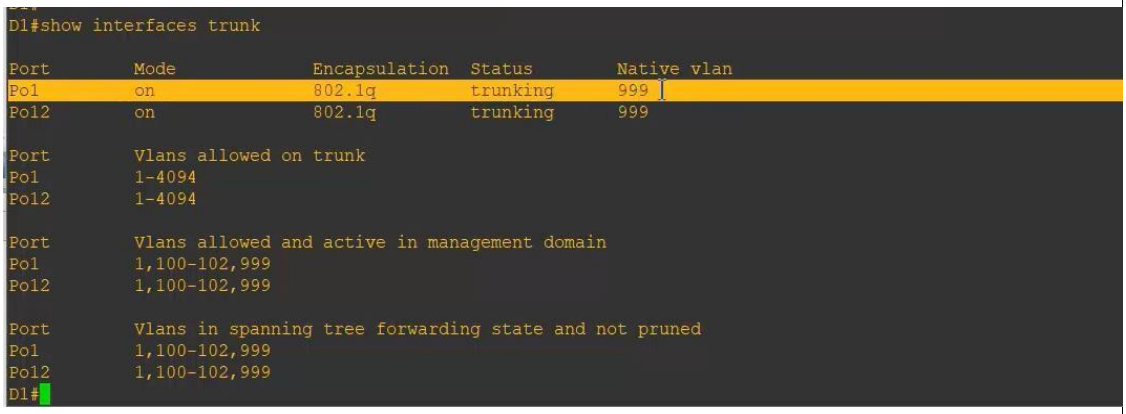
<table>
<tr><td colspan="3">Switch A1

interface range g0/1-2
channel-group 1 mode active
exit
interface range g0/3,g1/0
channel-group 2 mode active
exit</td></tr>
<tr><td>2.6</td><td>En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.</td><td>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).</td></tr>
<tr><td colspan="3">Switch D1
interface g2/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit

Switch D2
interface g2/3
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit

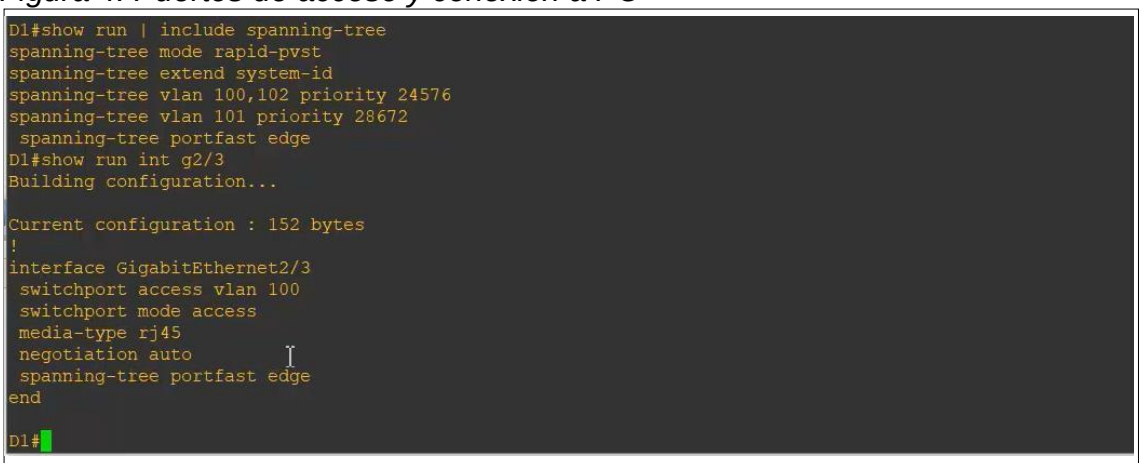
Switch A1
interface g2/3
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface g3/0
switchport mode access
switchport access vlan 100</td></tr>
</table>

spanning-tree portfast no shutdown exit		
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



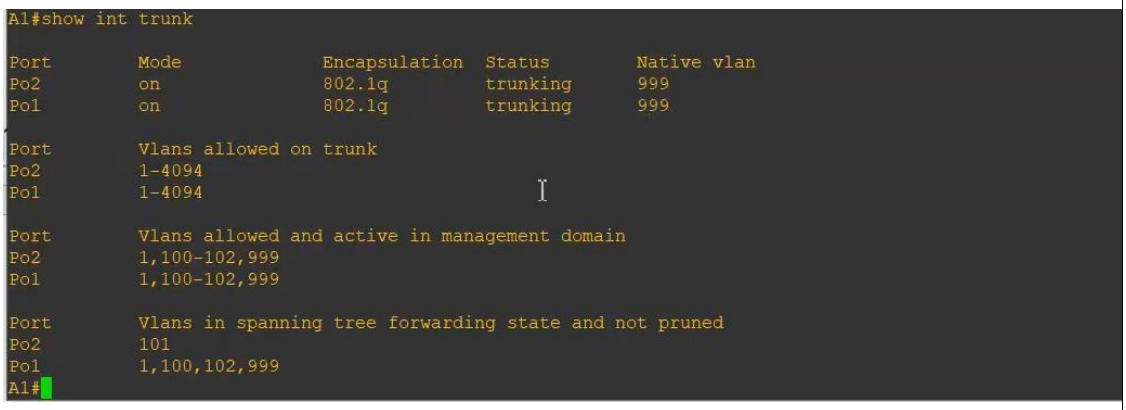
Fuente: Autor

Figura 4: Puertos de acceso y conexión a PC



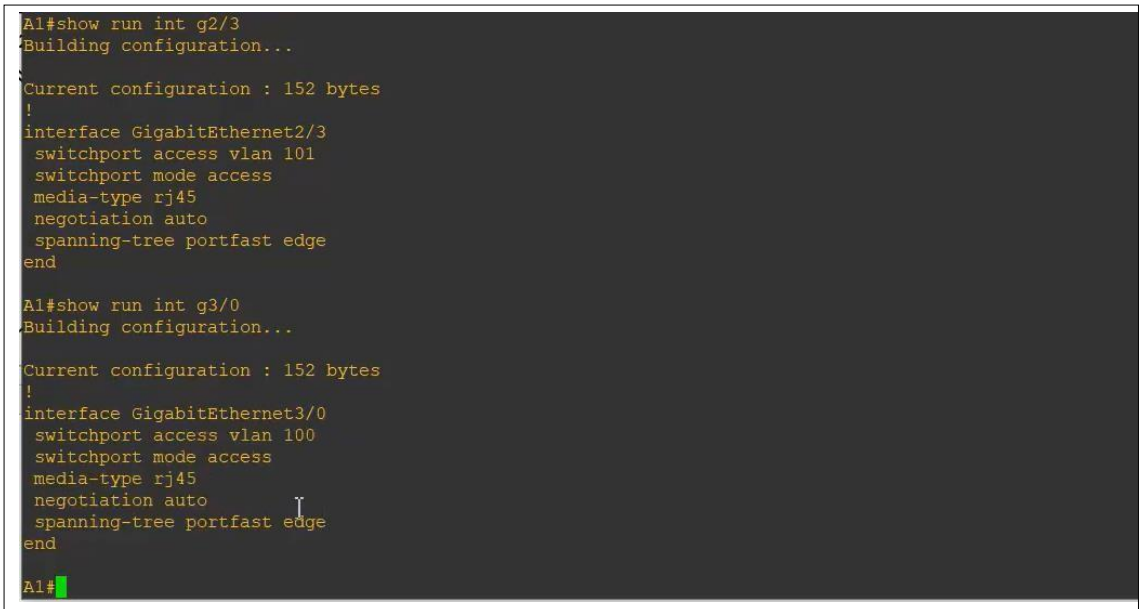
Fuente: Autor

Figura 5: verificacion en A1 de conexión a D1 y D2



Fuente: Autor

Figura 6: Puertos de acceso en A1



```
A1#show run int g2/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet2/3
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

A1#show run int g3/0
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet3/0
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

A1#
```

Fuente: Autor

Parte 3: configurar los protocolos de enrutamiento

En esta en esta parte debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta etapa la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz look back 0 desde D1 y D2 deberían ser exitosos.

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

Las tareas de configuración son las siguientes:

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

Router R1

```
router ospf 4
 router-id 0.0.4.1
 network 10.0.10.0 0.0.0.255 area 0
 network 10.0.13.0 0.0.0.255 area 0
 default-information originate
 exit
```

Router R3

```
router ospf 4
 router-id 0.0.4.3
 network 10.0.11.0 0.0.0.255 area 0
 network 10.0.13.0 0.0.0.255 area 0
 exit
```

Switch D1

```
router ospf 4
 router-id 0.0.4.131
 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
 network 10.0.10.0 0.0.0.255 area 0
```

<table>
<tr><td colspan="3">passive-interface default
no passive-interface g1/1
exit

Switch D2

router ospf 4
router-id 0.0.4.132
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
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface g1/1
exit</td></tr>
<tr><td>3.2</td><td>En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.</td><td>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 Área 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</td></tr>
</table>

```
Router R1

ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate
 exit
interface g1/0
 ipv6 ospf 6 area 0
 exit
interface s3/0
 ipv6 ospf 6 area 0
 exit

Router R3

ipv6 router ospf 6
 router-id 0.0.6.3
 exit
interface g1/0
 ipv6 ospf 6 area 0
 exit
interface s3/0
 ipv6 ospf 6 area 0
 exit

Switch D1

ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
 no passive-interface g1/1
 exit
interface g1/1
 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
```

<table>
<tr><td colspan="3">Switch D2

ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g1/1
exit
interface g1/1
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</td></tr>
<tr><td>3.3</td><td>En R2 en la “Red ISP”, configure MP- BGP.</td><td>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).</td></tr>
</table>

<table>
<tr><td colspan="3">Router R2

ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family</td></tr>
<tr><td>3.4</td><td>En R1 en la “Red ISP”, configure MP- BGP.</td><td>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.</td></tr>
</table>

Router R1

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

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 7: OSPF en R1

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.4.3           0   FULL/  -        00:00:38    10.0.13.3       Serial3/0
0.0.4.131         1   FULL/BDR        00:00:38    10.0.10.2       GigabitEthernet1/0
R1#
```

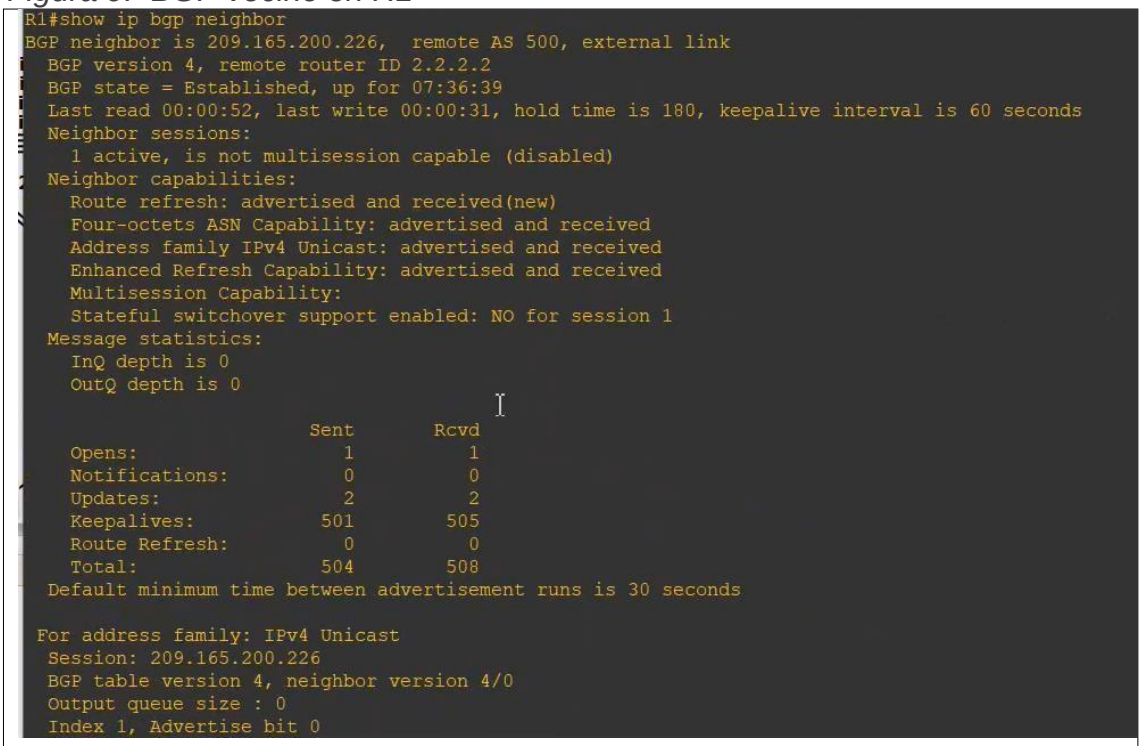
Figura 8: OSPF en D2

```
D2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
0.0.4.3           1   FULL/DR         00:00:38    10.0.11.1       GigabitEthernet1/1
D2#
```

Fuente: Autor

Figura 9: BGP vecino en R1



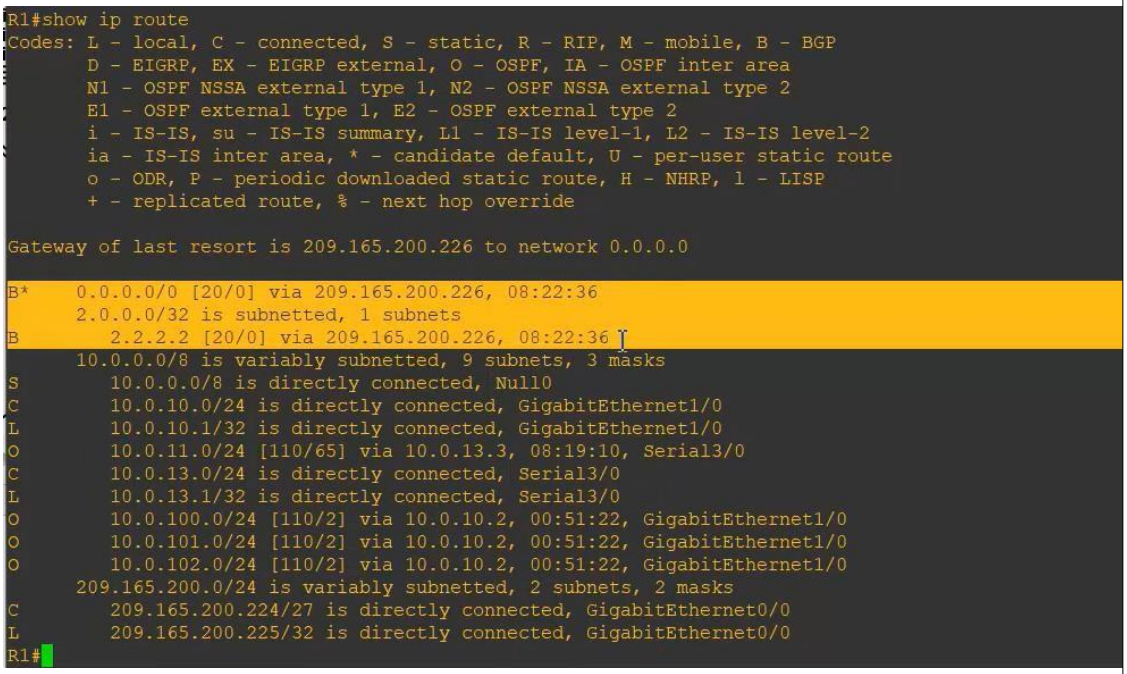
```
R1#show ip bgp neighbor
BGP neighbor is 209.165.200.226,  remote AS 500, external link
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 07:36:39
  Last read 00:00:52, last write 00:00:31, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                2          2
    Keepalives:           501        505
    Route Refresh:          0          0
    Total:                504        508
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  Session: 209.165.200.226
  BGP table version 4, neighbor version 4/0
  Output queue size : 0
  Index 1, Advertise bit 0
```

Fuente: Autor

Figura 10: Redes estáticas, rutas OSPF en R1



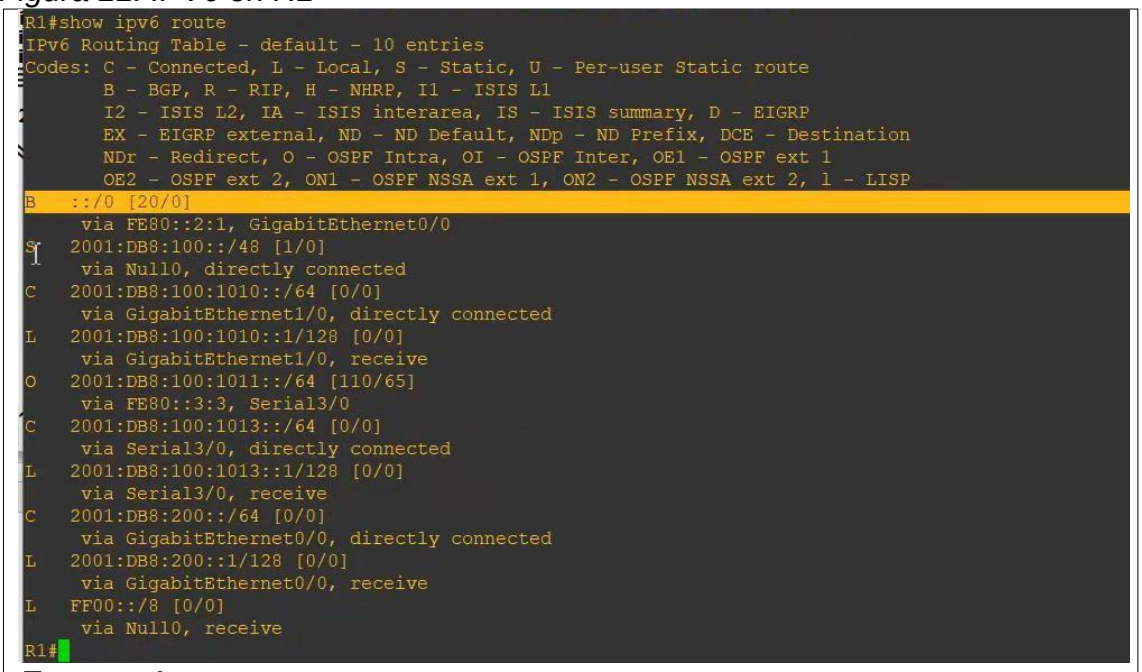
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.165.200.226, 08:22:36
      2.0.0.0/32 is subnetted, 1 subnets
B        2.2.2.2 [20/0] via 209.165.200.226, 08:22:36
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Null0
C        10.0.10.0/24 is directly connected, GigabitEthernet1/0
L        10.0.10.1/32 is directly connected, GigabitEthernet1/0
O        10.0.11.0/24 [110/65] via 10.0.13.3, 08:19:10, Serial3/0
C        10.0.13.0/24 is directly connected, Serial3/0
L        10.0.13.1/32 is directly connected, Serial3/0
O        10.0.100.0/24 [110/2] via 10.0.10.2, 00:51:22, GigabitEthernet1/0
O        10.0.101.0/24 [110/2] via 10.0.10.2, 00:51:22, GigabitEthernet1/0
O        10.0.102.0/24 [110/2] via 10.0.10.2, 00:51:22, GigabitEthernet1/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, GigabitEthernet0/0
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0
R1#
```

Fuente: Autor

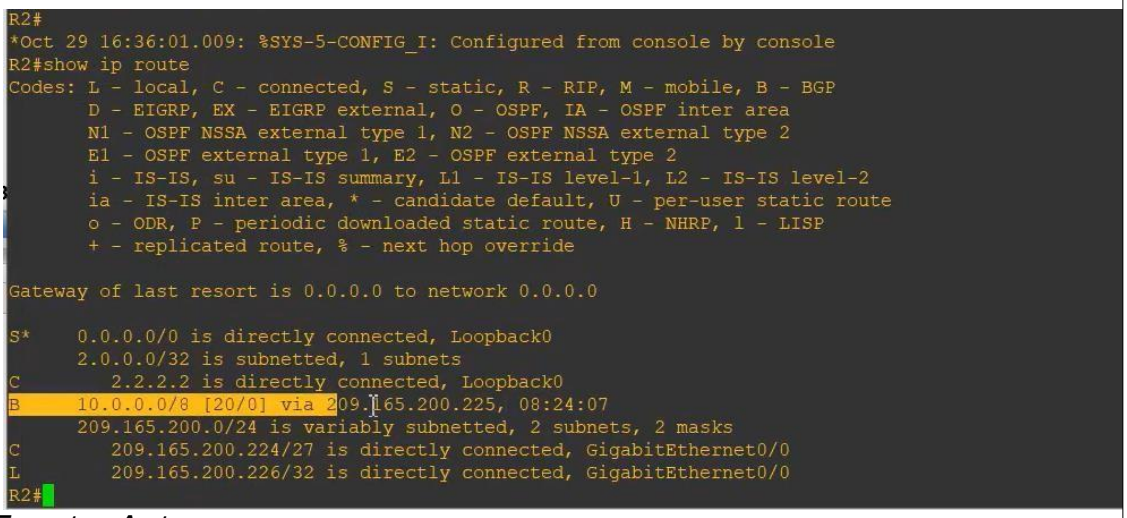
Figura 11: IPV6 en R1



```
R1#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
B   ::/0 [20/0]
     via FE80::2:1, GigabitEthernet0/0
S   2001:DB8:100::/48 [1/0]
     via Null0, directly connected
C   2001:DB8:100:1010::/64 [0/0]
     via GigabitEthernet1/0, directly connected
L   2001:DB8:100:1010::1/128 [0/0]
     via GigabitEthernet1/0, receive
O   2001:DB8:100:1011::/64 [110/65]
     via FE80::3:3, Serial3/0
C   2001:DB8:100:1013::/64 [0/0]
     via Serial3/0, directly connected
L   2001:DB8:100:1013::1/128 [0/0]
     via Serial3/0, receive
C   2001:DB8:200::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:200::1/128 [0/0]
     via GigabitEthernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Fuente: Autor

Figura 12: Ruta estática, BGP en R2



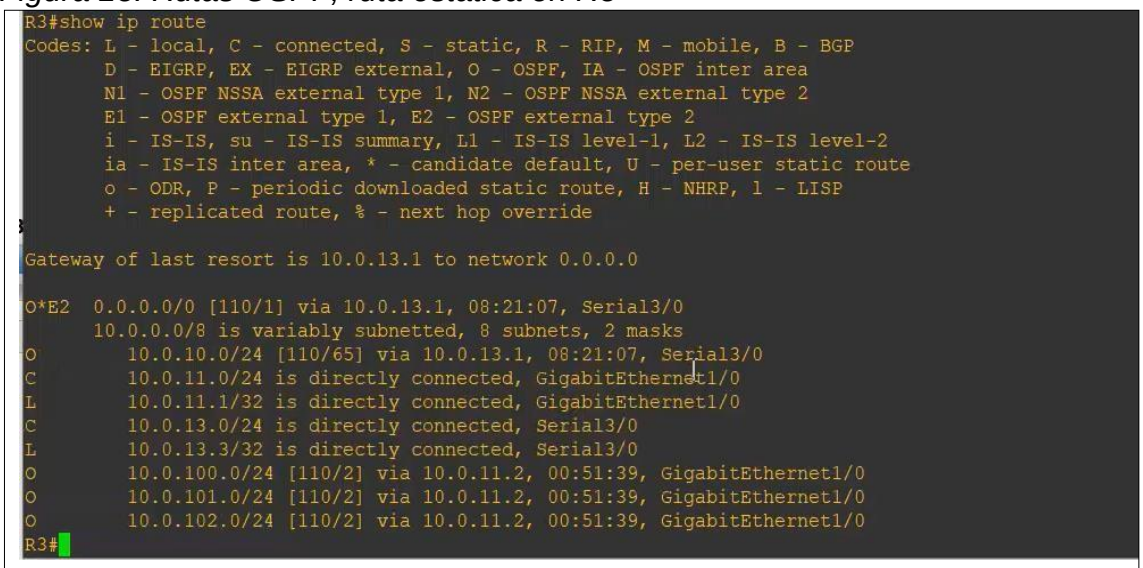
```
R2#
*Oct 29 16:36:01.009: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
B     10.0.0.0/8 [20/0] via 209.165.200.225, 08:24:07
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, GigabitEthernet0/0
L        209.165.200.226/32 is directly connected, GigabitEthernet0/0
R2#
```

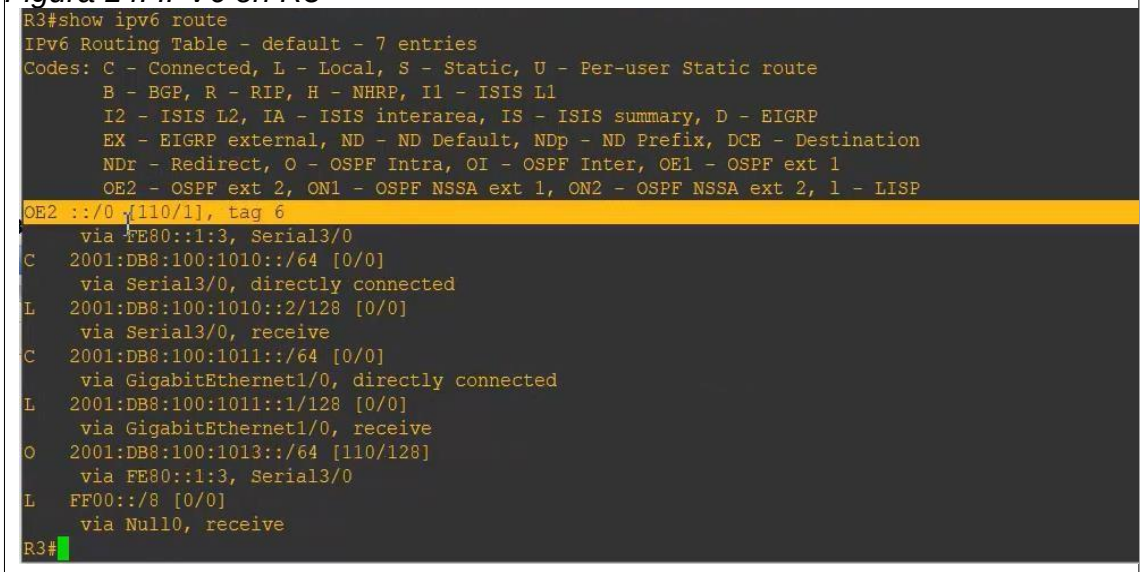
Fuente: Autor

Figura 13: Rutas OSPF, ruta estática en R3



Fuente: Autor

Figura 14: IPV6 en R3



Fuente: Autor

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

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

Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. • Use la SLA número **4** para IPv4. • Use la SLA número **6** para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

<table>
<tr><td colspan="3">Switch D1

ip sla 4
icmp-echo 10.0.10.1
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
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit</td></tr>
<tr><td>4.2</td><td>En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.</td><td>Cree IP SLAs.
Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6.
Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.
Programe la SLA para una implementación inmediata sin tiempo de finalización.
Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la SLA 6.
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</td></tr>
</table>

<table>
<tr><td colspan="3">Switch D2

ip sla 4
icmp-echo 10.0.11.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit</td></tr>
<tr><td>4.3</td><td>En D1 configure HSRPv2.</td><td>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:
• Asigne la dirección IP virtual 10.0.100.254.
• Establezca la prioridad del grupo en 150.
• Habilite la preferencia (preemption).
• Rastree el objeto 4 y decremente en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:
• Asigne la dirección IP virtual 10.0.101.254.
• Habilite la preferencia (preemption).
• Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:
• Asigne la dirección IP virtual 10.0.102.254.
• Establezca la prioridad del grupo en 150.</td></tr>
</table>

		• Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). Rastree el objeto 6 y decremente en 60.

Fuente: Autor

Switch D1

```
interface vlan 100
 standby version 2
 standby 104 ip 10.0.100.254
 standby 104 priority 150
 standby 104 preempt
 standby 104 track 4 decrement 60
 standby 106 ipv6 autoconfig
 standby 106 priority 150
 standby 106 preempt
 standby 106 track 6 decrement 60
 exit
interface vlan 101
```

```
 standby version 2
 standby 114 ip 10.0.101.254
 standby 114 preempt
 standby 114 track 4 decrement 60
 standby 116 ipv6 autoconfig
 standby 116 preempt
 standby 116 track 6 decrement 60
 exit
interface vlan 102
 standby version 2
 standby 124 ip 10.0.102.254
 standby 124 priority 150
 standby 124 preempt
 standby 124 track 4 decrement 60
 standby 126 ipv6 autoconfig
 standby 126 priority 150
 standby 126 preempt
 standby 126 track 6 decrement 60
 exit
```

	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60.

		Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). Rastree el objeto 6 para disminuir en 60.

Fuente: Autor

Switch D2

```
interface vlan 100
 standby version 2
 standby 104 ip 10.0.100.254
 standby 104 preempt
 standby 104 track 4 decrement 60
 standby 106 ipv6 autoconfig
 standby 106 preempt
 standby 106 track 6 decrement 60
 exit
interface vlan 101
 standby version 2
 standby 114 ip 10.0.101.254
 standby 114 priority 150
 standby 114 preempt
 standby 114 track 4 decrement 60
 standby 116 ipv6 autoconfig
 standby 116 priority 150
 standby 116 preempt
 standby 116 track 6 decrement 60
exit
```

```
 interface vlan 102
 standby version 2
 standby 124 ip 10.0.102.254
 standby 124 preempt
 standby 124 track 4 decrement 60
 standby 126 ipv6 autoconfig
 standby 126 preempt
 standby 126 track 6 decrement 60
exit
```

Figura 15: Informe de Vlan, IPV4 y IPV6 en D1

```
D1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       104  150 P Active  local           10.0.100.2      10.0.100.254
Vl100       106  150 P Active  local           FE80::D2:2      FE80::5:73FF:FEA0:6A
Vl101       114  100 P Standby 10.0.101.2      local           10.0.101.254
Vl101       116  100 P Standby FE80::D2:3      local           FE80::5:73FF:FEA0:74
Vl102       124  150 P Active  local           10.0.102.2      10.0.102.254
Vl102       126  150 P Active  local           FE80::D2:4      FE80::5:73FF:FEA0:7E
D1#
```

Fuente: Autor

Figura 16: Informe de Vlans activas y en espera de D2

```
D2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl100       104  100 P Standby 10.0.100.1      local           10.0.100.254
Vl100       106  100 P Standby FE80::D1:2      local           FE80::5:73FF:FEA0:6A
Vl101       114  150 P Active  local           10.0.101.1      10.0.101.254
Vl101       116  150 P Active  local           FE80::D1:3      FE80::5:73FF:FEA0:74
Vl102       124  100 P Standby 10.0.102.1      local           10.0.102.254
Vl102       126  100 P Standby FE80::D1:4      local           FE80::5:73FF:FEA0:7E
D2#
```

Fuente: Autor

Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
Router R1, Router R2, Router R3, Switch D1, Switch D2, Switch A1 enable algorithm-type SCRYPT secret cisco12345cisco username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Alternativo enable secret cisco12345cisco username sadmin privilege 15 secret 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.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**

<table>
<tr><td colspan="3">Router R1, Router R3, Switch D1, Switch D2, Switch A1

aaa new-model
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
exit</td></tr>
<tr><td>5.5</td><td>En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA</td><td>Especificaciones de autenticación AAA:
Use la lista de métodos por defecto
Valide contra el grupo de servidores RADIUS
De lo contrario, utilice la base de datos local.</td></tr>
<tr><td colspan="3">Router R1, Router R3, Switch D1, Switch D2, Switch A1

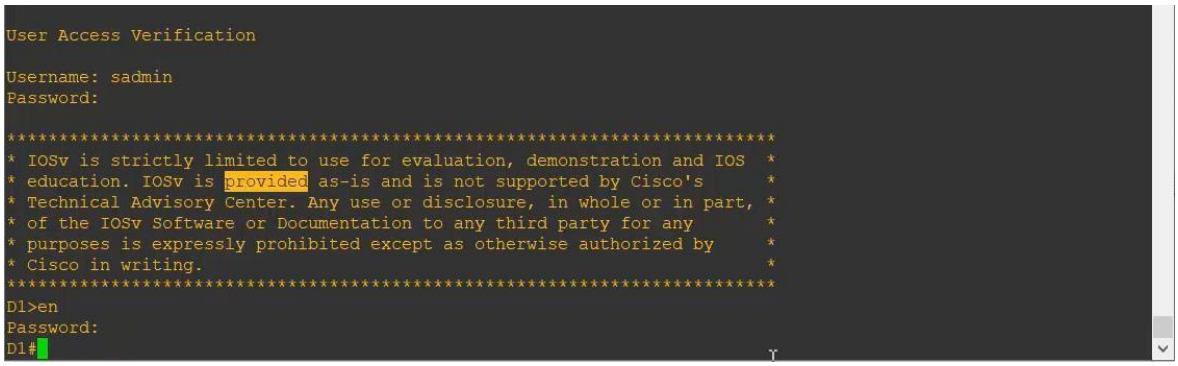
aaa authentication login default group radius local</td></tr>
<tr><td>5.6</td><td>Verifique el servicio AAA en todos los dispositivos (except R2).</td><td>Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.</td></tr>
</table>

Fuente: Autor

Figura 17: Modo seguro en R1

Fuente: Autor

Figura 18: verificación de seguridad en D1



Fuente: Autor

Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

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.
Router R1, Router R2, Router R3, Switch D1, Switch D2, Switch A1 clock set 13:00:00 20 November 2021		
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
Router R2 ntp master 3		
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.

<table>
<tr><td colspan="3">Router R1

ntp server 2.2.2.2

Router R3, Switch D1, Switch A1

ntp server 10.0.10.1

Switch D2

ntp server 10.0.11.1</td></tr>
<tr><td>6.4</td><td>Configure Syslog en todos los dispositivos excepto R2</td><td>Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.</td></tr>
<tr><td colspan="3">Router R1, Router R3, Switch D1, Switch D2, Switch A1

logging trap warning
logging host 10.0.100.5
logging on</td></tr>
<tr><td>6.5</td><td>Configure SNMPv2c en todos los dispositivos excepto R2</td><td>Especificaciones de SNMPv2:
Unicamente se usará SNMP en modo lectura (Read-Only).
Limite el acceso SNMP a la dirección IP de la PC1.
Configure el valor de contacto SNMP con su nombre.
Establezca el community string en ENCORSA.
En R3, D1, y D2, habilite el envío de traps config y ospf.
En R1, habilite el envío de traps bgp, config, y ospf.
En A1, habilite el envío de traps config.</td></tr>
</table>

Fuente: Autor

Router R1

```
ip access-list standard SNMP-NMS
  permit host 10.0.100.5
  exit
 snmp-server contact Cisco Student
 snmp-server community ENCORSA ro SNMP-NMS
 snmp-server host 10.0.100.5 version 2c ENCORSA
 snmp-server ifindex persist
 snmp-server enable traps bgp
 snmp-server enable traps config
 snmp-server enable traps ospf
```

Router R3, Switch D1, Switch D2

```
ip access-list standard SNMP-NMS
  permit host 10.0.100.5
  exit
 snmp-server contact Cisco Student
 snmp-server community ENCORSA ro SNMP-NMS
 snmp-server host 10.0.100.5 version 2c ENCORSA
 snmp-server ifindex persist
 snmp-server enable traps config
 snmp-server enable traps ospf
```

Switch A1

```
ip access-list standard SNMP-NMS
  permit host 10.0.100.5
  exit
 snmp-server contact Cisco Student
 snmp-server community ENCORSA ro SNMP-NMS
 snmp-server host 10.0.100.5 version 2c ENCORSA
 snmp-server ifindex persist
snmp-server enable traps config
  exit.
```

Figura 19: Configuración SNMP en R1

```
R1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
R1#
```

Fuente: Autor

Figura 20: Configuración SNMP en D1

```
D1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
D1#
```

Fuente: Autor

CONCLUSIONES

Durante todo el proceso de este proyecto de investigación fue posible evidenciar que para realizar subredes anidadas a un router en específico es importante que cada uno de ellos posea una puerta de enlace predeterminada, mediante la cual sea posible establecer la conexión encargada del intercambio de datos entre componentes de un mismo sistema en particular.

Por otra parte, es indispensable tener conocimientos básicos en cuanto a la implementación de comandos en el CLI propio de componentes configurables, tales como routers y switches, dado que mediante este tipo de códigos es posible realizar ajustes avanzados en la topología.

Con el uso de herramientas virtuales de simulación se permitió realizar el análisis de la topología de red para dicha empresa y poder hacer un análisis sobre el comportamiento de los protocolos y enrutamientos necesarios para su funcionamiento

El uso de las VLAN es de gran ayuda a la seguridad cuando se tienen datos sensibles o confidenciales dentro de la empresa ya que los separa del resto de la red para evitar que ocurran violaciones de información, y ofreciendo un mejor rendimiento en redes de capa 2 reduciendo el tráfico innecesario en la red y posteriormente un mejor rendimiento

BIBLIOGRAFIAS

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

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

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

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

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

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

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

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

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