

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

Diego Alexander Figueroa Villarreal

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

Informe de avance – Prueba de habilidades práctica

Diego Alexander Figueroa Villarreal

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

DIRECTOR:
JOHN HAROLD PEREZ CALDERON

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del jurado

Firma del jurado

Bogotá, 20 de noviembre de 2022

AGRADECIMIENTOS

En primera medida agradezco la finalización de este trabajo a Dios todo poderoso por darme la vida y darme también la posibilidad de cumplir mis sueños, a mi familia quienes han sido un pilar fundamental para el crecimiento como persona y el cumplimiento de mis proyectos.

A la Universidad Nacional Abierta y a Distancia, por brindarme la oportunidad de pertenecer a esta institución y por permitirme mejorar mis competencias como futuro Ingeniero de Telecomunicaciones, al cuerpo de Docentes que con su compromiso y dedicación permitieron que se logra el desarrollo del presente trabajo.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO	5
LISTA DE FIGURAS	6
GLOSARIO	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCIÓN	11
ESCENARIO 1.....	12
PARTE 1: CREE LA RED Y CONFIGURE LOS AJUSTES BÁSICOS DEL DISPOSITIVO Y EL DIRECCIONAMIENTO DE LA INTERFAZ.....	12
PASO 1: CABLEE LA RED COMO SE MUESTRA EN LA TOPOLOGÍA.	12
.....	12
PARTE 2: CONFIGURAR LA COMPATIBILIDAD DE RED Y HOST DE CAPA 2	22
ESCENARIO 2.....	31
PART 1: CONFIGURAR PROTOCOLOS DE ENRUTAMIENTO	31
3.1 En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv2 de área única en el área 0	31
3.2 En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv3 clásico de área única en el área 0.	35
3.3 En R2 en la "Red ISP", configure MP-BGP.....	39
3.4 En R1 en la "Red ISP", configure MP-BGP.....	41
PART 2: CONFIGURAR REDUNDANCIA DE PRIMER SALTO	43
4.1 En D1, cree IP SLA que prueben la accesibilidad de la interfaz E1/2 de R1.	43
4.2 En D2, cree IP SLA que prueben la accesibilidad de la interfaz E1/0 de R3	44
4.3 En D1, configure HSRPv2.....	46
CONCLUSIONES	51
BIBLIOGRAFÍA.....	52

LISTA DE FIGURAS

	Pág
Figura 1. Configuración Topología de Red	12
Figura 2. Configuración comando startup-config en R1	20
Figura 3. Configuración comando startup-config en R2.....	20
Figura 4. Configuración comando startup-config en R3.....	20
Figura 5. Configuración comando startup-config en D1	21
Figura 6. Configuración comando startup-config en D2.....	21
Figura 7. Configuración comando startup-config en A1	21
Figura 8. Dirección IP del PC1	22
Figura 9. Dirección IP del PC4.....	22
Figura 10. Verificación Enlace troncal en D1	22
Figura 11. Verificación Enlace troncal en D2	23
Figura 12. Verificación Enlace troncal en A1	23
Figura 13. Verificación VLAN 999 Native en D1	23
Figura 14. Verificación VLAN 999 Native en D2	23
Figura 15. Verificación VLAN 999 Native en A1.....	24
Figura 16. Verificación Árbol de expansión en D1	24
Figura 17. Verificación Árbol de expansión en D2	24
Figura 18. Verificación Árbol de expansión en A1	24
Figura 19. Verificación del puente raíz en D1	25
Figura 20. Verificación del puente raíz en D2	25
Figura 21. Verificación EtherChannel en D1	25
Figura 22. Verificación EtherChannel en D2.....	26
Figura 23. Verificación EtherChannel en A1	26
Figura 24. Verificación Puertos de Acceso PC1	26
Figura 25. Verificación Puertos de Acceso PC2	27
Figura 26. Verificación Puertos de Acceso PC3	27
Figura 27. Verificación Puertos de Acceso PC4	28
Figura 28. Verificación DHCP en PC2	28
Figura 29. Verificación DHCP en PC3	28
Figura 30. Verificación Comando Ping PC1.....	29
Figura 31. Verificación Comando Ping PC2.....	29
Figura 32. Verificación Comando Ping PC3.....	30
Figura 33. Verificación Comando Ping en PC4.....	30
Figura 34. configuración OSPFV2 en R1	33
Figura 35. configuración OSPFV2 en R3.....	33
Figura 36. configuración OSPFV2 en D2.....	34
Figura 37. configuración OSPFV2 en D1	34
Figura 38. Configuración OSPFv3 en R1.....	37
Figura 39. Configuración OSPFv3 en R3.....	38
Figura 40. Configuración OSPFv3 en D1.....	38

Figura 41. Configuración OSPFv3 en D2.....	39
Figura 42. Configuración MP-BGP en R2.....	41
Figura 43. Configuración MP-BGP en la red ISP R1	42
Figura 44. Configuración Ip Sla Para El Acceso A La Interfaz E1/2 De R1	44
Figura 45. Configuración Ip Sla Para El Acceso A La Interfaz E1/0 De R3	45
Figura 46. Verificación Ip Interfaz E1/0 De R3.....	46
Figura 47. configuración HSRPv2 en D1	48
Figura 48. verificación HSRPv2 en D1.....	49
Figura 49. configuración HSRPv2 en D2	50
Figura 50. verificación HSRPv2 en D2.....	50

LISTA DE TABLA

	Pág.
Tabla 1 Direcciones IP de Equipos	13

GLOSARIO

DHCP: Protocolo de asignación automática de direcciones IP.

SWITCH: Dispositivo que permite la conexión equipos en una red.

HOST: Dispositivo electrónico que permite la conexión a la red de internet.

CCNP: Certificación Cisco Certified Network Professional.

LAN: Red de área local, que permite la comunicación entre equipos activos en una red.

PROTOCOLO: Conjunto de reglas o estándares que contienen procedimientos, restricciones que permiten el intercambio de paquetes de información.

ROUTER: Equipo electrónico que permite interconectar distintas redes y establecer la mejor ruta de un equipo a otro.

RESUMEN

El desarrollo de este trabajo contiene las competencias del Diplomado de Profundización Cisco CCNP, el cual permite la construcción de redes conmutadas (LAN y WAN), utilizando los diferentes protocolos de comunicaciones para el paso de paquetes entre los diferentes equipos activos en la topología como los son Switch y Router, logrando que los Host de la red se comuniquen garantizando la seguridad de la red, todo esto mediante el uso de software de simulación (GN3), que permite la ejecución de cada uno de los comando planteados en el trabajo.

Palabras claves: DHCP, SWITCH, HOST, CCNP, LAN, PROTOCOLO

ABSTRACT

The development of this work contains the skills of the Cisco CCNP Deepening Diploma, which allows the construction of switched networks (LAN and WAN), using the different communication protocols for the passage of packets between the different active equipment in the topology such as They are Switch and Router, making the Hosts of the network communicate, guaranteeing the security of the network, all this through the use of simulation software (GN3), which allows the execution of each of the commands proposed in the work.

Keywords: DHCP, SWITCH, HOST, CCNP, LAN, PROTOCOL

INTRODUCCIÓN

En el desarrollo del *Diplomado de Profundización Cisco CCNP*, se busca planificar, diseñe, estructure y realizar la simulación de redes jerárquicas convergentes, escalables y seguras para empresas locales y de área específica. En donde se cuenta con el apropiamiento de los conocimientos básicos de redes empresariales, en temas como calidad de servicio, escalabilidad y seguridad entre otros.

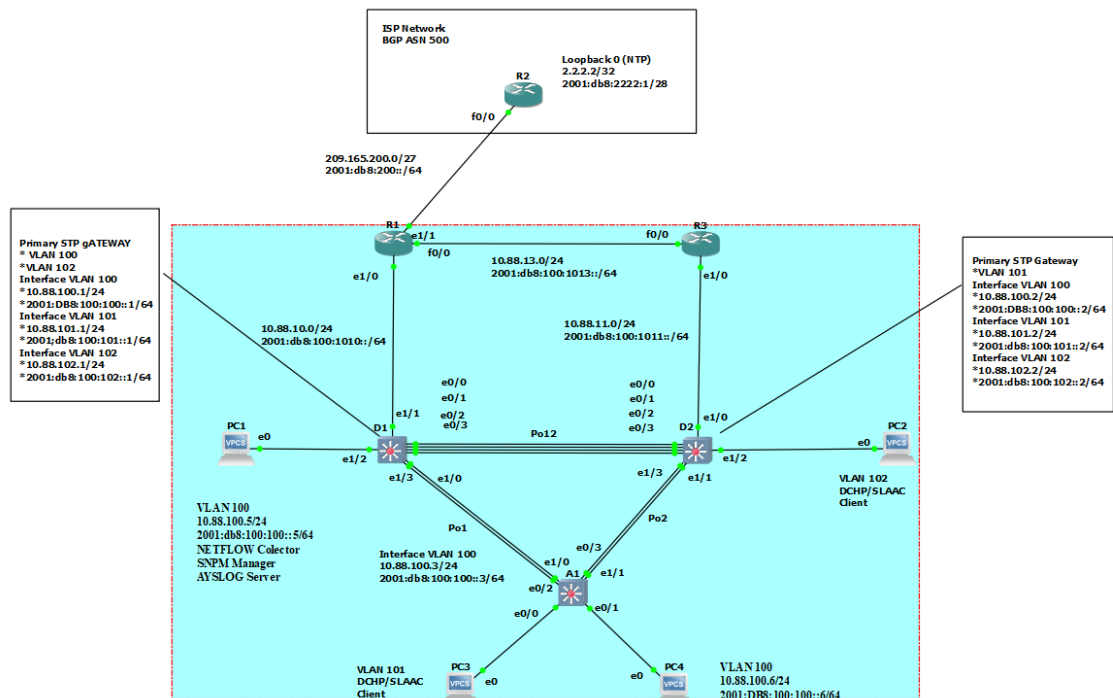
Es así como se logra a través de escenarios de simulación la creación de una red con equipos activos y con la implementación de protocolos como DHCP, STP, IPV4, IPV6 y OSPF que permiten acceso seguro a través de la automatización y virtualización, logrando solucionar problemas presentado en el simulador GN3.

ESCENARIO 1

PARTE 1: CREACION DE LA RED Y CONFIGURACION DE LOS AJUSTES BÁSICOS DEL DISPOSITIVO Y EL DIRECCIONAMIENTO DE LA INTERFAZ

PASO 1: CABLEAR LA RED COMO SE MUESTRA EN LA TOPOLOGÍA.

Figura 1. Configuración Topología de Red



Fuente: propia

Tabla 1 Direcciones IP de Equipos

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R1	E1/1	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/0	10.88.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	F0/0	10.88.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	F0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Bucle invertido0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10.88.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	F0/0	10.88.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/1	10.88.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	vlan 100	10.88.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	vlan 101	10.88.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	vlan 102	10.88.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.88.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	vlan 100	10.88.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	vlan 101	10.88.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	vlan 102	10.88.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	vlan 100	10.88.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	Nada	10.88.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	Nada	DHCP	SLAAC	EUI-64
PC3	Nada	DHCP	SLAAC	EUI-64
PC4	Nada	10.88.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente: propia

PASO 2: CONFIGURACION DE LOS AJUSTES BÁSICOS PARA CADA DISPOSITIVO.

Router R1

```
Enable
configure terminal
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR SKills Assessment#
line console 0
exec-time 0 0
logging synchronous
exit
interface e1/1
ip address 209.165.200.255 255.255.255.224
ipv6 address 2001:db8:200::1/64
ipv6 address fe80::1:1 link-local
no shutdown
exit
interface F0/0
ip address 10.88.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
interface ethernet 1/0
ip address 10.88.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
```

Router R2

```
enable
configure terminal
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR SKills Assessment#
line console 0
exec-time 0 0
logging synchronous
exit
interface f0/0
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
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

```
enable
configure terminal
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR SKills Assessment#
line console 0
exec-time 0 0
logging synchronous
exit
interface f0/0
ip address 10.88.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2011:db8:100:1013::3/64
```

```
no shutdown
exit
interface e1/0
ip address 10.88.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2011:db8:100:1011::1/64
no shutdown
```

Switch D1

```
enable
configure terminal
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1,ENCOR SKILLS Assessment#
line console 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e1/1
no switchport
ip address 10.88.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
```



```
ip address 10.88.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.88.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.88.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.88.101.1 10.88.101.109
ip dhcp excluded-address 10.88.101.141 10.88.101.254
ip dhcp excluded-address 10.88.102.1 10.88.102.109
ip dhcp excluded-address 10.88.102.141 10.88.102.254
ip dhcp pool VLAN-101
network 10.88.101.0 255.255.255.0
default-router 10.88.101.254
exit
ip dhcp pool VLAN-102
network 10.88.102.0 255.255.255.0
default-router 10.88.102.254
interface range e2/0-3, e3/0-3
shutdown
exit
```

Switch D2

```
Enable
configure terminal
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motf # D2, ENCOR Skills Assessment#
line console 0
```

```
exec-time 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e1/0
no switchport
ip address 10.88.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.88.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.88.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.88.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.88.101.1 10.88.101.209
```

```
ip dhcp excluded-address 10.88.101.241 10.88.101.254
ip dhcp excluded-address 10.88.102.1 10.88.102.209
ip dhcp excluded-address 10.88.102.241 10.88.102.254
ip dhcp pool VLAN-101
network 10.88.101.0 255.255.255.0
default-router 88.0.101.254
exit
ip dhcp pool VLAN-102
network 10.88.102.0 255.255.255.0
default-router 10.88.102.254
exit
interface range e2/0-3, e3/0-3
shutdown
exit
```

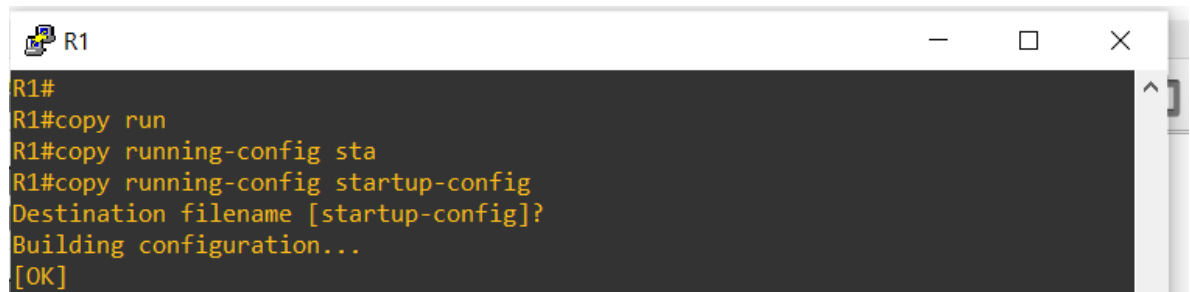
SWITCH A1

```
enable
configure terminal
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment#
line console 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 10.88.100.3 255.255.254.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no sh
```

interface range e1/2-3, e2/0-3, e3/0-3
shutdown

b. Guardar la configuración en ejecución en startup-config en todos los dispositivos.

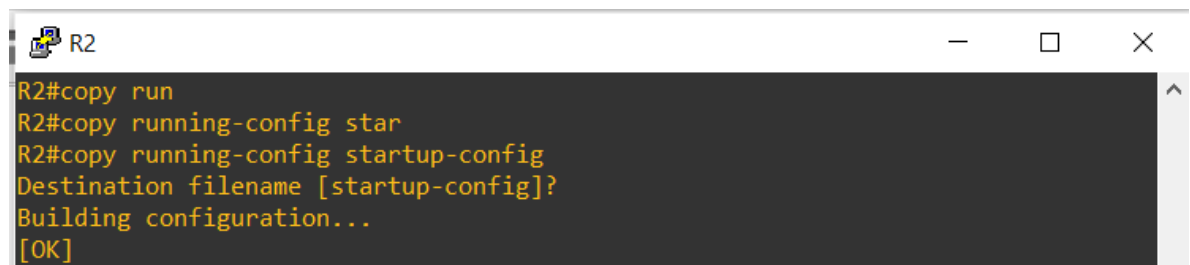
Figura 2. Configuración comando startup-config en R1



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

Fuente: propia

Figura 3. Configuración comando startup-config en R2



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

Fuente: propia

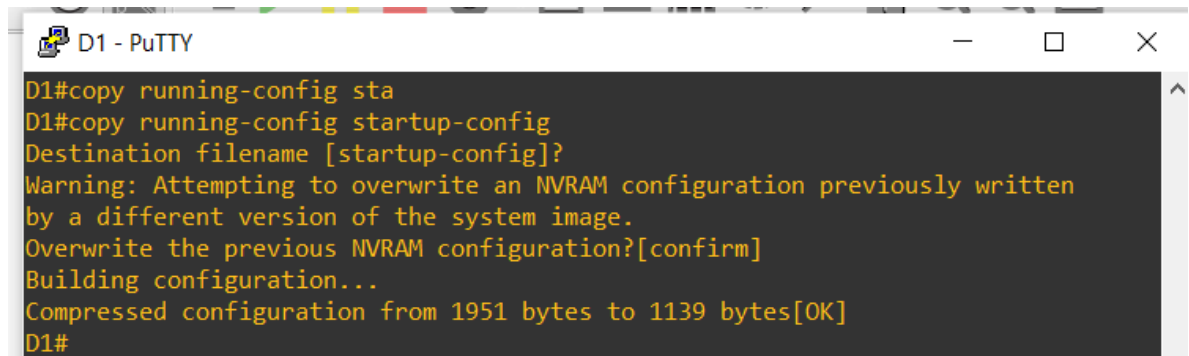
Figura 4. Configuración comando startup-config en R3



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

Fuente: propia

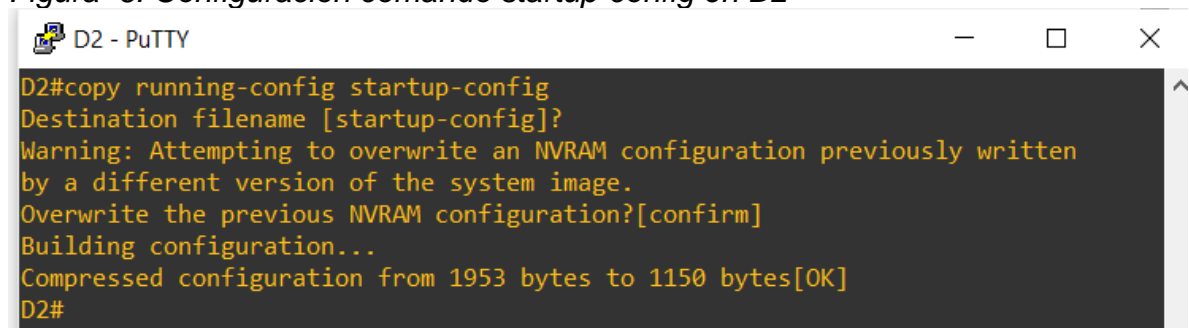
Figura 5. Configuración comando startup-config en D1



```
D1#copy running-config sta
D1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1951 bytes to 1139 bytes[OK]
D1#
```

Fuente: propia

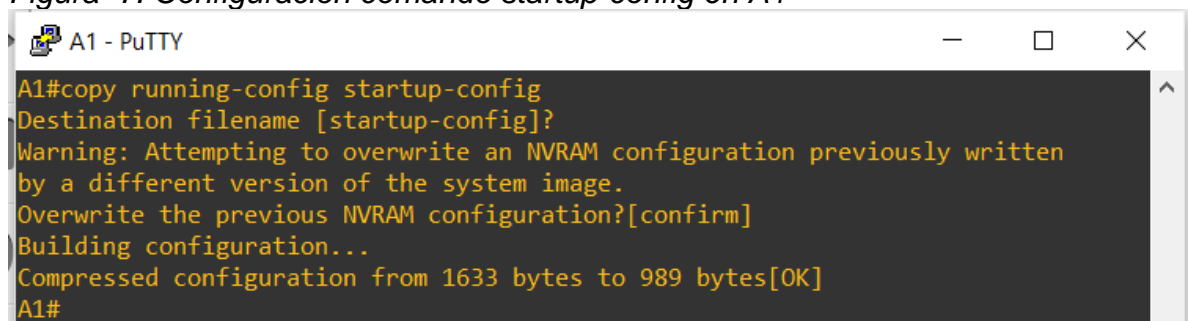
Figura 6. Configuración comando startup-config en D2



```
D2#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1953 bytes to 1150 bytes[OK]
D2#
```

Fuente: propia

Figura 7. Configuración comando startup-config en A1

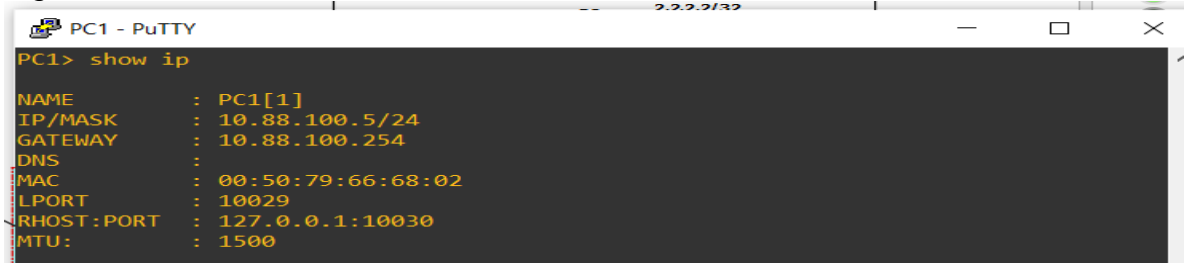


```
A1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1633 bytes to 989 bytes[OK]
A1#
```

Fuente: propia

c. Configurar el direccionamiento de Host de PC 1 y PC 4 como se muestra en la tabla de direcciones. Asignar una dirección de puerta de enlace predeterminada de 10.XY.100.254, que será la dirección IP virtual HSRP utilizada en la Parte 4.

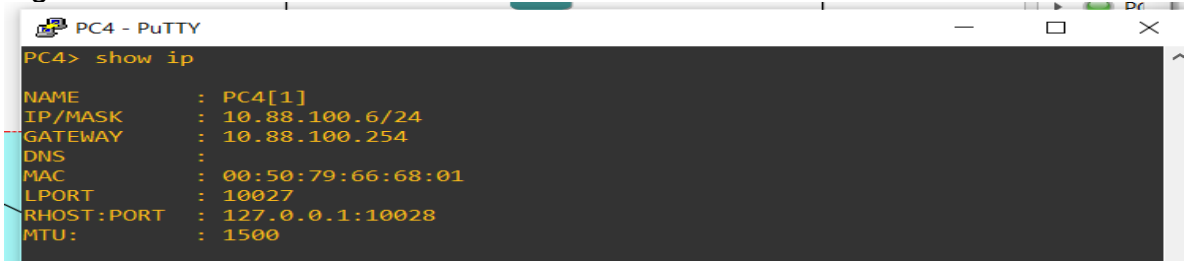
Figura 8. Dirección IP del PC1



```
PC1 - PuTTY
PC1> show ip
NAME       : PC1[1]
IP/MASK    : 10.88.100.5/24
GATEWAY    : 10.88.100.254
DNS        :
MAC        : 00:50:79:66:68:02
LPORT     : 10029
RHOST:PORT : 127.0.0.1:10030
MTU        : 1500
```

Fuente: propia

Figura 9. Dirección IP del PC4



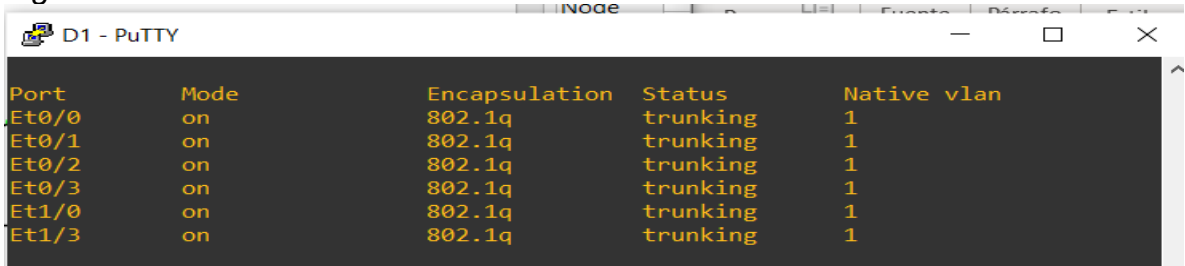
```
PC4 - PuTTY
PC4> show ip
NAME       : PC4[1]
IP/MASK    : 10.88.100.6/24
GATEWAY    : 10.88.100.254
DNS        :
MAC        : 00:50:79:66:68:01
LPORT     : 10027
RHOST:PORT : 127.0.0.1:10028
MTU        : 1500
```

Fuente: propia

PARTE 2: CONFIGURAR LA COMPATIBILIDAD DE RED Y HOST DE CAPA 2

2.1 En todos los conmutadores, configurar las interfaces troncales IEEE 802.1Q en los enlaces de conmutación interconectados.

Figura 10. Verificación Enlace troncal en D1



```
D1 - PuTTY
Port      Mode      Encapsulation  Status      Native vlan
Et0/0     on        802.1q         trunking    1
Et0/1     on        802.1q         trunking    1
Et0/2     on        802.1q         trunking    1
Et0/3     on        802.1q         trunking    1
Et1/0     on        802.1q         trunking    1
Et1/3     on        802.1q         trunking    1
```

Fuente: propia

Figura 11. Verificación Enlace troncal en D2

```
D2 - PuTTY
Port      Mode      Encapsulation  Status      Native vlan
Et0/0     on        802.1q         trunking    1
Et0/1     on        802.1q         trunking    1
Et0/2     on        802.1q         trunking    1
Et0/3     on        802.1q         trunking    1
Et1/1     on        802.1q         trunking    1
Et1/3     on        802.1q         trunking    1
```

Fuente: propia

Figura 12. Verificación Enlace troncal en A1

```
A1 - PuTTY
Port      Mode      Encapsulation  Status      Native vlan
Et0/2     on        802.1q         trunking    1
Et0/3     on        802.1q         trunking    1
Et1/0     on        802.1q         trunking    1
Et1/1     on        802.1q         trunking    1
```

Fuente: propia

2.2 En todos los conmutadores, cambie la VLAN nativa de los enlaces troncales.

Figura 13. Verificación VLAN 999 Native en D1

```
D1 - PuTTY
D1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Et0/0     on        802.1q         trunking    999
Et0/1     on        802.1q         trunking    999
Et0/2     on        802.1q         trunking    999
Et0/3     on        802.1q         trunking    999
Et1/0     on        802.1q         trunking    999
Et1/3     on        802.1q         trunking    999
```

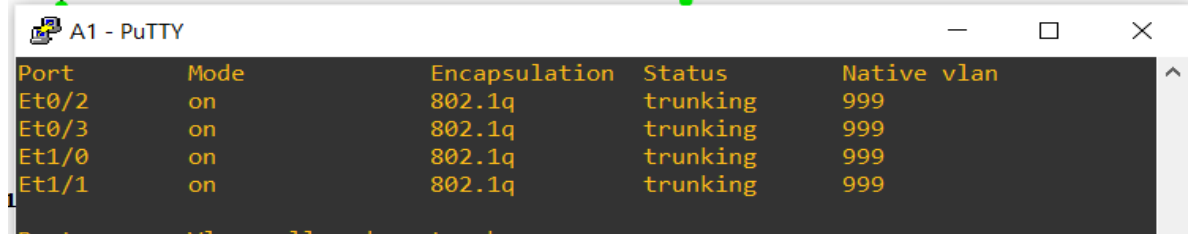
Fuente: propia

Figura 14. Verificación VLAN 999 Native en D2

```
D2 - PuTTY
Port      Mode      Encapsulation  Status      Native vlan
Et0/0     on        802.1q         trunking    999
Et0/1     on        802.1q         trunking    999
Et0/2     on        802.1q         trunking    999
Et0/3     on        802.1q         trunking    999
Et1/1     on        802.1q         trunking    999
Et1/3     on        802.1q         trunking    999
```

Fuente: propia

Figura 15. Verificación VLAN 999 Native en A1

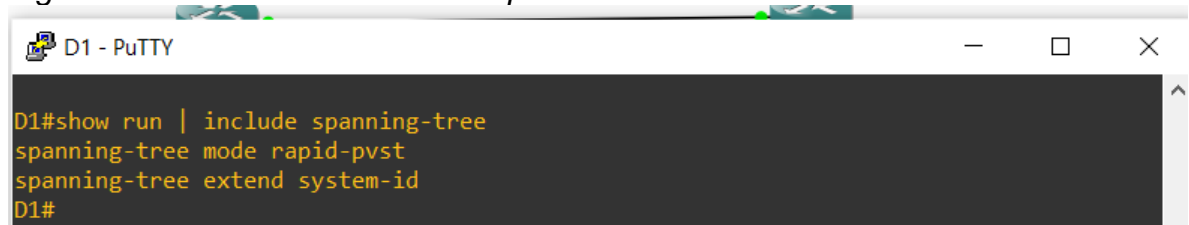


```
A1 - PuTTY
Port      Mode      Encapsulation  Status      Native vlan
Et0/2     on        802.1q         trunking    999
Et0/3     on        802.1q         trunking    999
Et1/0     on        802.1q         trunking    999
Et1/1     on        802.1q         trunking    999
```

Fuente: propia

2.3 En todos los conmutadores, se habilita el protocolo de árbol de expansión rápida.

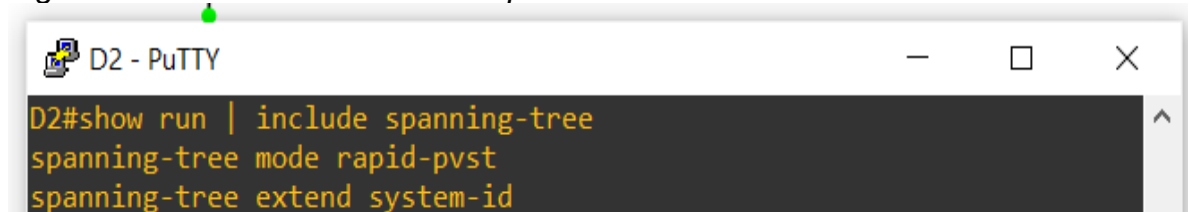
Figura 16. Verificación Árbol de expansión en D1



```
D1 - PuTTY
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
D1#
```

Fuente: propia

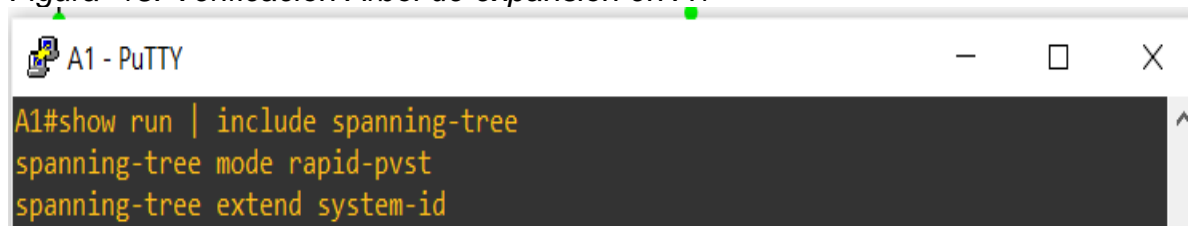
Figura 17. Verificación Árbol de expansión en D2



```
D2 - PuTTY
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

Fuente: propia

Figura 18. Verificación Árbol de expansión en A1

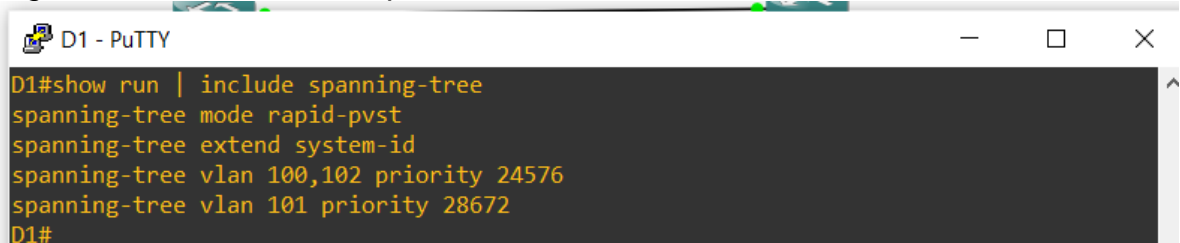


```
A1 - PuTTY
A1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
```

Fuente: propia

2.4 En D1 y D2, configurar los puentes raíz RSTP adecuados en función de la información del diagrama de topología. Así mismo D1 y D2 deben proporcionar copia de seguridad en caso de fallo del puente raíz.

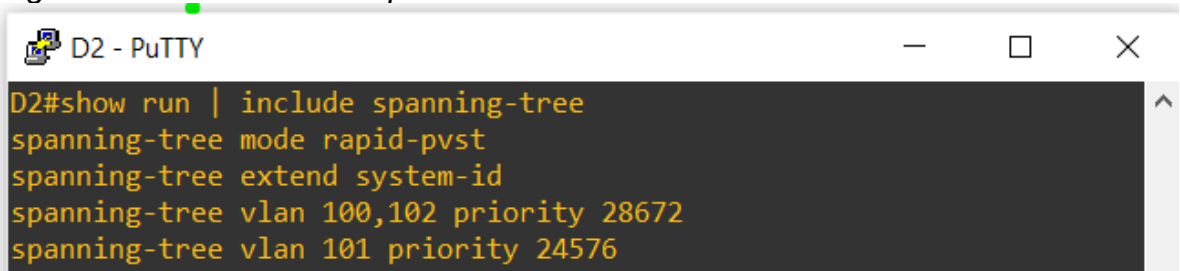
Figura 19. Verificación del puente raíz en D1



```
D1 - PuTTY
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
D1#
```

Fuente: propia

Figura 20. Verificación del puente raíz en D2

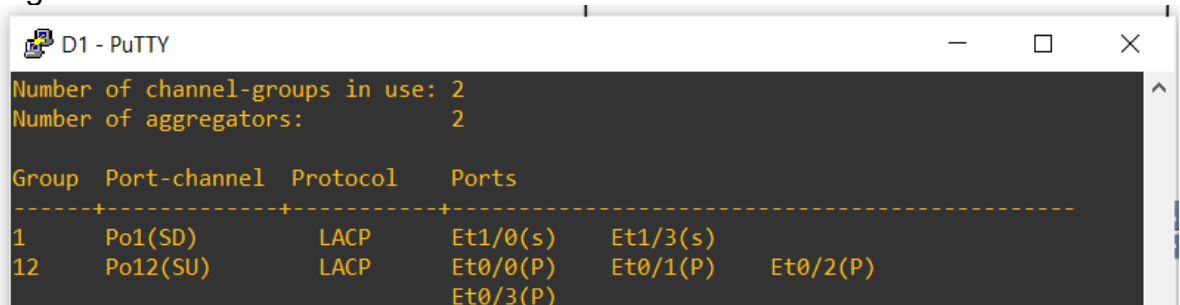


```
D2 - PuTTY
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
spanning-tree vlan 101 priority 24576
```

Fuente: propia

2.5 En todos los Switches, crear LACP EtherChannel como se muestra en el diagrama de topología.

Figura 21. Verificación EtherChannel en D1



```
D1 - PuTTY
Number of channel-groups in use: 2
Number of aggregators: 2

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SD)        LACP      Et1/0(s)  Et1/3(s)
12     Po12(SU)       LACP      Et0/0(P)  Et0/1(P)  Et0/2(P)
                               Et0/3(P)
```

Fuente: propia

Figura 22. Verificación EtherChannel en D2

```

D2 - PuTTY
Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2(SD)        LACP      Et1/1(s)  Et1/3(s)
12     Po12(SU)       LACP      Et0/0(P)  Et0/1(P)  Et0/2(P)
                                         Et0/3(P)
    
```

Fuente: propia

Figura 23. Verificación EtherChannel en A1

```

A1 - PuTTY
Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1(SU)        LACP      Et0/2(P)  Et1/0(P)
2      Po2(SU)        LACP      Et0/3(P)  Et1/1(P)
    
```

Fuente: propia

2.6 En todos los conmutadores, configurar los puertos de acceso al host que se conectan a PC1, PC2, PC3 y PC4.

Figura 24. Verificación Puertos de Acceso PC1

```

D1 - PuTTY
D1#show spanning-tree vlan 100

VLAN0100
  Spanning tree enabled protocol rstp
  Root ID    Priority    24676
             Address    aabb.cc00.0100
             This bridge is the root
             Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    24676 (priority 24576 sys-id-ext 100)
             Address    aabb.cc00.0100
             Hello Time  2 sec    Max Age 20 sec    Forward Delay 15 sec
             Aging Time  300 sec

Interface    Role Sts Cost      Prio.Nbr Type
-----+-----+-----+-----+-----+-----
Et1/2        Desg FWD 100      128.7   Shr Edge
Po12         Desg FWD 41       128.65  Shr
Po1          Desg FWD 56       128.66  Shr
    
```

Fuente: propia

Figura 25. Verificación Puertos de Acceso PC2

```

D2#show spanning-tree vlan 102

VLAN0102
  Spanning tree enabled protocol rstp
  Root ID    Priority    24678
            Address    aabb.cc00.0100
            Cost      41
            Port      65 (Port-channel12)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28774 (priority 28672 sys-id-ext 102)
            Address    aabb.cc00.0200
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Et1/2                    Desg FWD 100      128.7   Shr Edge
Po12                     Root FWD 41       128.65  Shr
Po2                      Desg FWD 56       128.66  Shr
  
```

Fuente: propia

Figura 26. Verificación Puertos de Acceso PC3

```

A1#show spanning-tree vlan 101

VLAN0101
  Spanning tree enabled protocol rstp
  Root ID    Priority    24677
            Address    aabb.cc00.0200
            Cost      56
            Port      66 (Port-channel2)
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32869 (priority 32768 sys-id-ext 101)
            Address    aabb.cc00.0300
            Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Et0/0                    Desg FWD 100      128.1   Shr Edge
Po1                      Altn BLK 56       128.65  Shr
Po2                      Root FWD 56       128.66  Shr
  
```

Fuente: propia

Figura 27. Verificación Puertos de Acceso PC4

```
A1#show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol rstp
  Root ID    Priority    24676
             Address    aabb.cc00.0100
             Cost      56
             Port      65 (Port-channel1)
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32868 (priority 32768 sys-id-ext 100)
             Address    aabb.cc00.0300
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Et0/1                    Desg FWD 100      128.2   Shr Edge
Po1                       Root FWD 56       128.65  Shr
Po2                       Altn BLK 56       128.66  Shr
```

Fuente: propia

2.7 Comprobación de los servicios DHCP IPv4.

Figura 28. Verificación DHCP en PC2

```
PC2> ip dhcp
DDORA IP 10.88.102.110/24 GW 10.88.102.254
```

Fuente: propia

Figura 29. Verificación DHCP en PC3

```
PC3> ip dhcp
DDORA IP 10.88.101.210/24 GW 88.0.101.254
```

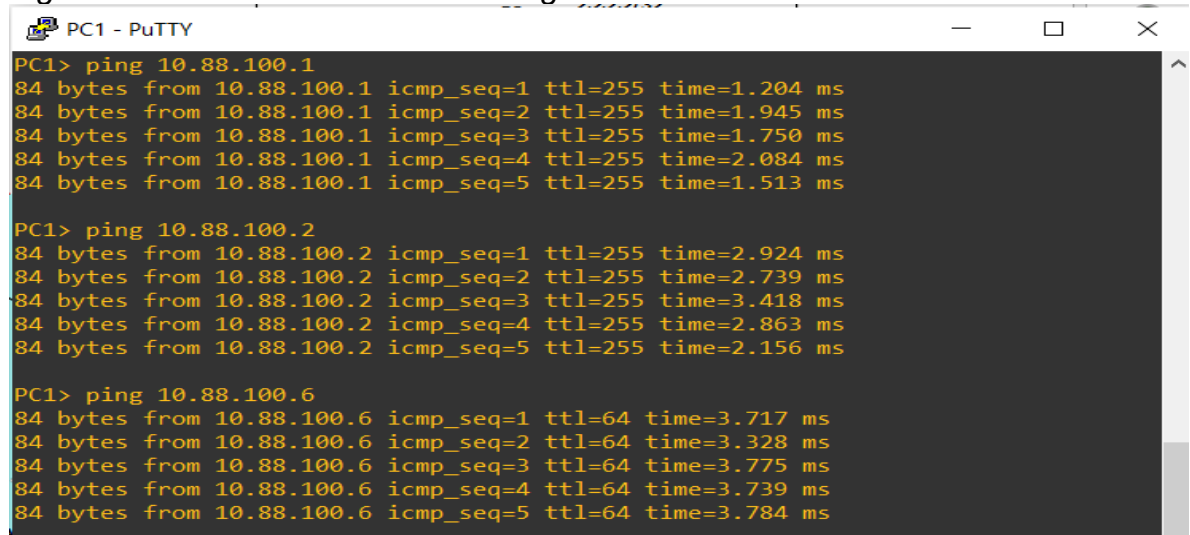
Fuente: propia

2.8 Comprobar la conectividad LAN local.

PC1 debería hacer ping con éxito:

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

Figura 30. Verificación Comando Ping PC1



```
PC1 - PuTTY
PC1> ping 10.88.100.1
84 bytes from 10.88.100.1 icmp_seq=1 ttl=255 time=1.204 ms
84 bytes from 10.88.100.1 icmp_seq=2 ttl=255 time=1.945 ms
84 bytes from 10.88.100.1 icmp_seq=3 ttl=255 time=1.750 ms
84 bytes from 10.88.100.1 icmp_seq=4 ttl=255 time=2.084 ms
84 bytes from 10.88.100.1 icmp_seq=5 ttl=255 time=1.513 ms

PC1> ping 10.88.100.2
84 bytes from 10.88.100.2 icmp_seq=1 ttl=255 time=2.924 ms
84 bytes from 10.88.100.2 icmp_seq=2 ttl=255 time=2.739 ms
84 bytes from 10.88.100.2 icmp_seq=3 ttl=255 time=3.418 ms
84 bytes from 10.88.100.2 icmp_seq=4 ttl=255 time=2.863 ms
84 bytes from 10.88.100.2 icmp_seq=5 ttl=255 time=2.156 ms

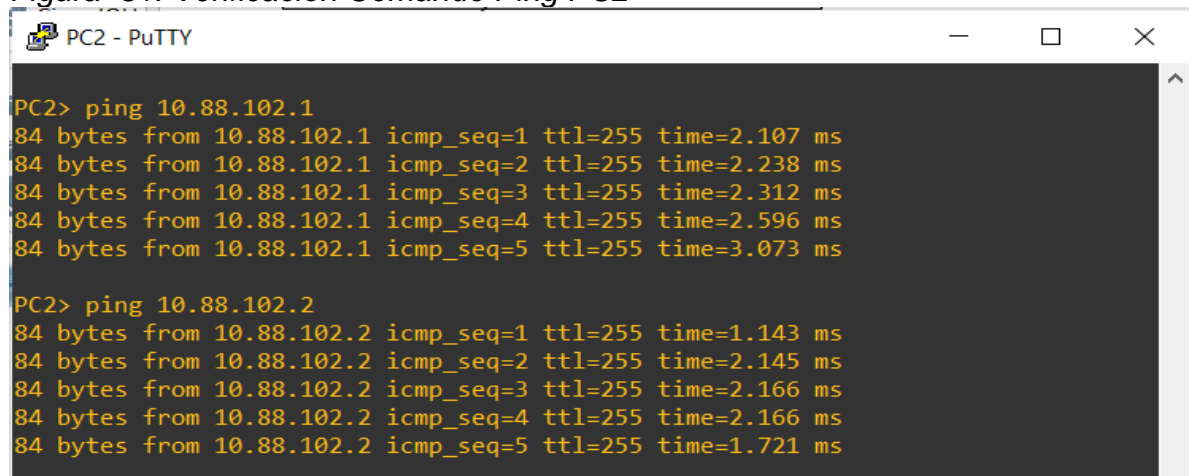
PC1> ping 10.88.100.6
84 bytes from 10.88.100.6 icmp_seq=1 ttl=64 time=3.717 ms
84 bytes from 10.88.100.6 icmp_seq=2 ttl=64 time=3.328 ms
84 bytes from 10.88.100.6 icmp_seq=3 ttl=64 time=3.775 ms
84 bytes from 10.88.100.6 icmp_seq=4 ttl=64 time=3.739 ms
84 bytes from 10.88.100.6 icmp_seq=5 ttl=64 time=3.784 ms
```

Fuente: propia

PC2 debería hacer ping correctamente:

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

Figura 31. Verificación Comando Ping PC2



```
PC2 - PuTTY
PC2> ping 10.88.102.1
84 bytes from 10.88.102.1 icmp_seq=1 ttl=255 time=2.107 ms
84 bytes from 10.88.102.1 icmp_seq=2 ttl=255 time=2.238 ms
84 bytes from 10.88.102.1 icmp_seq=3 ttl=255 time=2.312 ms
84 bytes from 10.88.102.1 icmp_seq=4 ttl=255 time=2.596 ms
84 bytes from 10.88.102.1 icmp_seq=5 ttl=255 time=3.073 ms

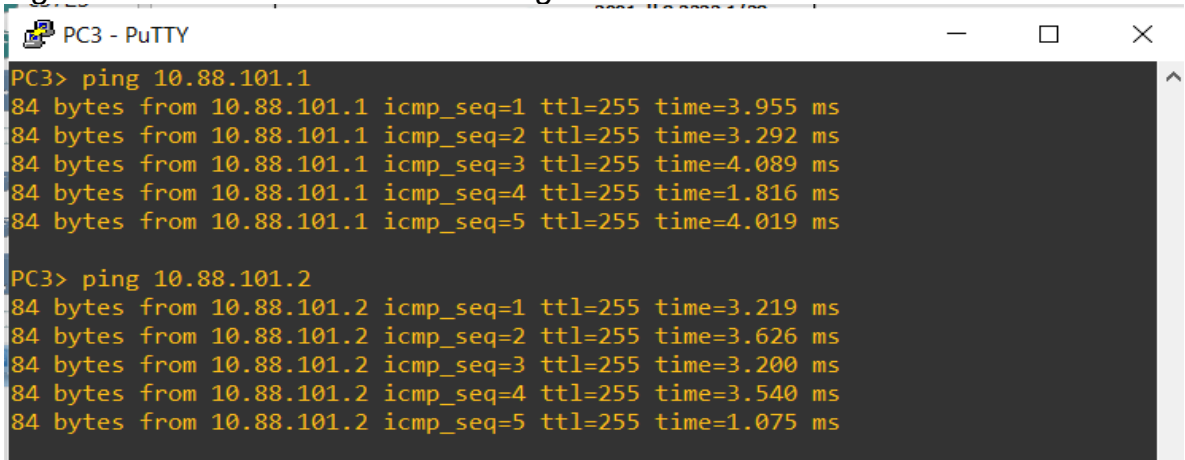
PC2> ping 10.88.102.2
84 bytes from 10.88.102.2 icmp_seq=1 ttl=255 time=1.143 ms
84 bytes from 10.88.102.2 icmp_seq=2 ttl=255 time=2.145 ms
84 bytes from 10.88.102.2 icmp_seq=3 ttl=255 time=2.166 ms
84 bytes from 10.88.102.2 icmp_seq=4 ttl=255 time=2.166 ms
84 bytes from 10.88.102.2 icmp_seq=5 ttl=255 time=1.721 ms
```

Fuente: propia

PC3 debería hacer ping correctamente:

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

Figura 32. Verificación Comando Ping PC3



```
PC3 - PuTTY
PC3> ping 10.88.101.1
84 bytes from 10.88.101.1 icmp_seq=1 ttl=255 time=3.955 ms
84 bytes from 10.88.101.1 icmp_seq=2 ttl=255 time=3.292 ms
84 bytes from 10.88.101.1 icmp_seq=3 ttl=255 time=4.089 ms
84 bytes from 10.88.101.1 icmp_seq=4 ttl=255 time=1.816 ms
84 bytes from 10.88.101.1 icmp_seq=5 ttl=255 time=4.019 ms

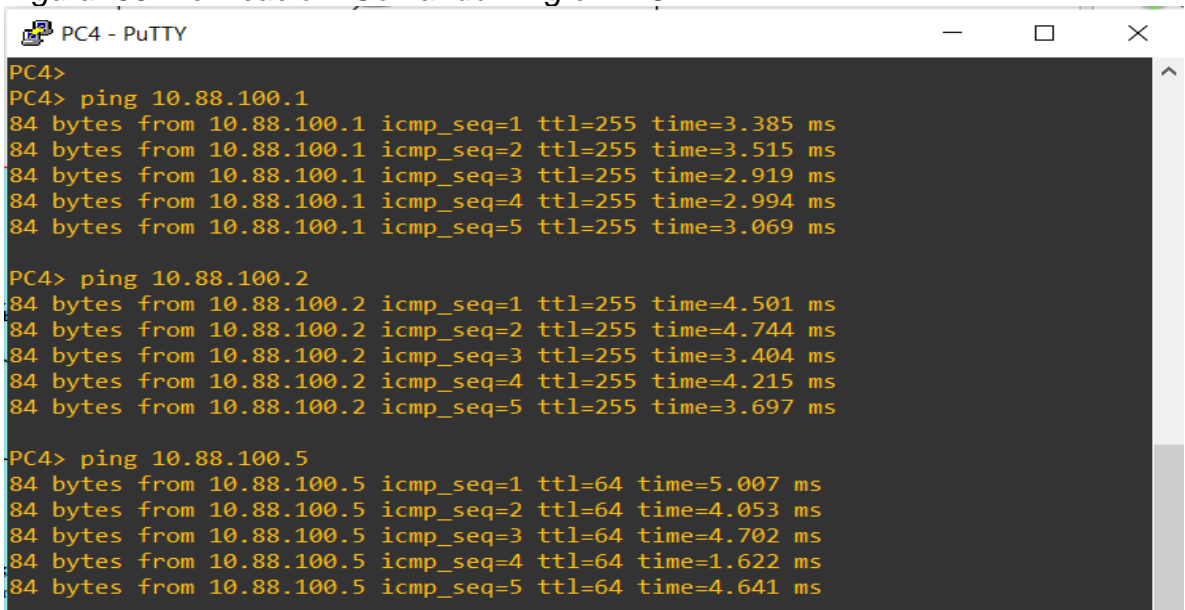
PC3> ping 10.88.101.2
84 bytes from 10.88.101.2 icmp_seq=1 ttl=255 time=3.219 ms
84 bytes from 10.88.101.2 icmp_seq=2 ttl=255 time=3.626 ms
84 bytes from 10.88.101.2 icmp_seq=3 ttl=255 time=3.200 ms
84 bytes from 10.88.101.2 icmp_seq=4 ttl=255 time=3.540 ms
84 bytes from 10.88.101.2 icmp_seq=5 ttl=255 time=1.075 ms
```

Fuente: propia

PC4 debería hacer ping correctamente:

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

Figura 33. Verificación Comando Ping en PC4



```
PC4 - PuTTY
PC4>
PC4> ping 10.88.100.1
84 bytes from 10.88.100.1 icmp_seq=1 ttl=255 time=3.385 ms
84 bytes from 10.88.100.1 icmp_seq=2 ttl=255 time=3.515 ms
84 bytes from 10.88.100.1 icmp_seq=3 ttl=255 time=2.919 ms
84 bytes from 10.88.100.1 icmp_seq=4 ttl=255 time=2.994 ms
84 bytes from 10.88.100.1 icmp_seq=5 ttl=255 time=3.069 ms

PC4> ping 10.88.100.2
84 bytes from 10.88.100.2 icmp_seq=1 ttl=255 time=4.501 ms
84 bytes from 10.88.100.2 icmp_seq=2 ttl=255 time=4.744 ms
84 bytes from 10.88.100.2 icmp_seq=3 ttl=255 time=3.404 ms
84 bytes from 10.88.100.2 icmp_seq=4 ttl=255 time=4.215 ms
84 bytes from 10.88.100.2 icmp_seq=5 ttl=255 time=3.697 ms

PC4> ping 10.88.100.5
84 bytes from 10.88.100.5 icmp_seq=1 ttl=64 time=5.007 ms
84 bytes from 10.88.100.5 icmp_seq=2 ttl=64 time=4.053 ms
84 bytes from 10.88.100.5 icmp_seq=3 ttl=64 time=4.702 ms
84 bytes from 10.88.100.5 icmp_seq=4 ttl=64 time=1.622 ms
84 bytes from 10.88.100.5 icmp_seq=5 ttl=64 time=4.641 ms
```

Fuente: propia

Escenario 2

PART 1: CONFIGURAR PROTOCOLOS DE ENRUTAMIENTO

3.1 En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv2 de área única en el área 0.

- Utilizando el ID de proceso OSPF 4 y asigne los siguientes ID de enrutador:
 - 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/VLAN conectadas directamente en el Área 0.
 - En R1, no anuncie la red R1 – R2.
 - En el R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada.

- Deshabilitar los anuncios OSPFv2 en:
 - D1: All interfaces except E1/2
 - D2: All interfaces except E1/0

Router R1:

```
enable
configure terminal
Router ospf 4
Router-id 0.0.4.1
network 10.88.10.0 0.0.0.255 area 0
network 10.88.13.0 0.0.0.255 area 0
default-information originate
exit
```

ROUTER 3

```
enable
configure terminal
router ospf 4
router-id 0.0.4.3
network 10.88.11.0 0.0.0.255 area 0
network 10.88.13.0 0.0.0.255 area 0
exit
```

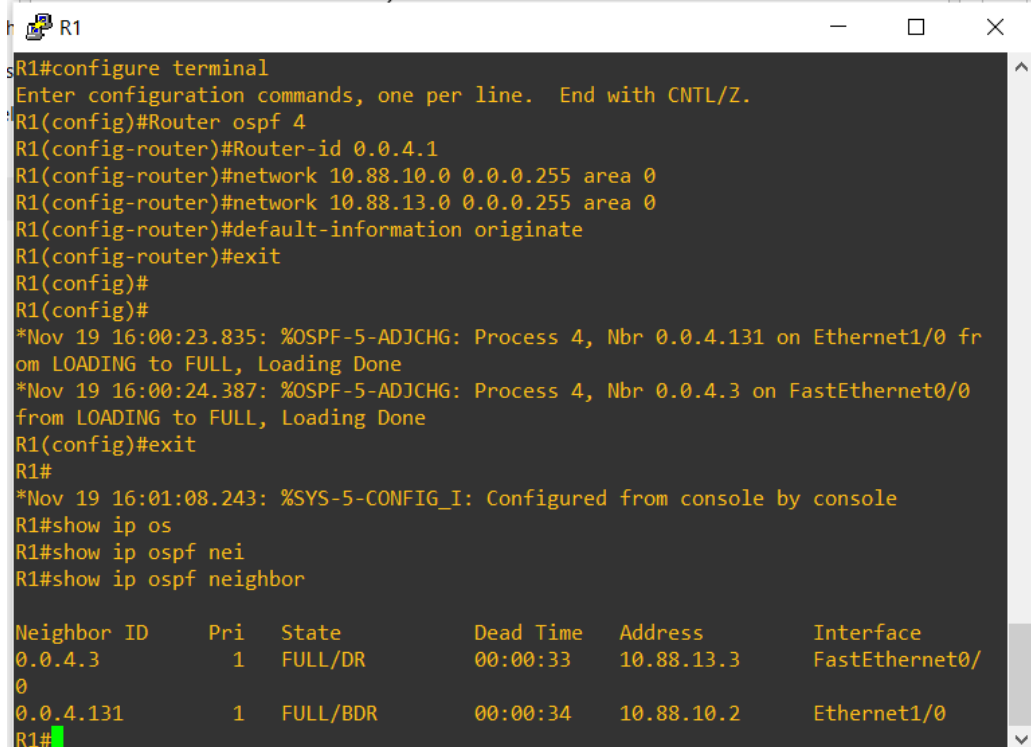
SWITCH D1

```
enable
configure terminal
router ospf 4
router-id 0.0.4.131
network 10.88.100.0 0.0.0.255 area 0
network 10.88.101.0 0.0.0.255 area 0
network 10.88.102.0 0.0.0.255 area 0
network 10.88.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/1
exit
```

SWITCH D2

```
enable
configure terminal
router ospf 4
router-id 0.0.4.132
network 10.88.100.0 0.0.0.255 area 0
network 10.88.101.0 0.0.0.255 area 0
network 10.88.102.0 0.0.0.255 area 0
network 10.88.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/0
exit
```


Figura 34. configuración OSPFV2 en R1



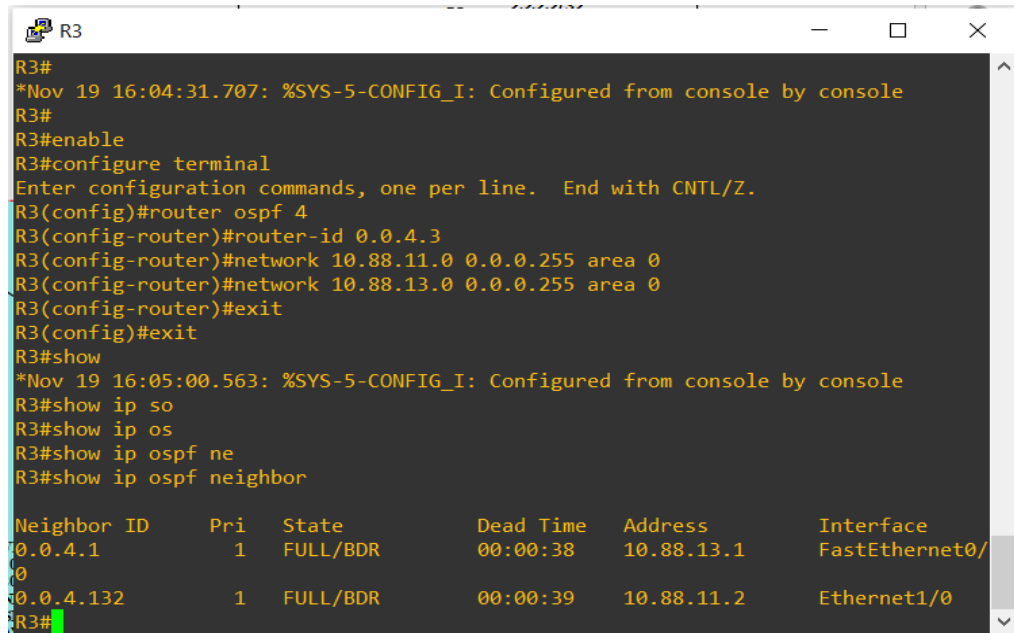
```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#Router ospf 4
R1(config-router)#Router-id 0.0.4.1
R1(config-router)#network 10.88.10.0 0.0.0.255 area 0
R1(config-router)#network 10.88.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#
R1(config)#
*Nov 19 16:00:23.835: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on Ethernet1/0 fr
om LOADING to FULL, Loading Done
*Nov 19 16:00:24.387: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on FastEthernet0/0
from LOADING to FULL, Loading Done
R1(config)#exit
R1#
R1#
*Nov 19 16:01:08.243: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip os
R1#show ip ospf nei
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.4.3	1	FULL/DR	00:00:33	10.88.13.3	FastEthernet0/0
0.0.4.131	1	FULL/BDR	00:00:34	10.88.10.2	Ethernet1/0

```
R1#
```

Fuente: propia

Figura 35. configuración OSPFV2 en R3



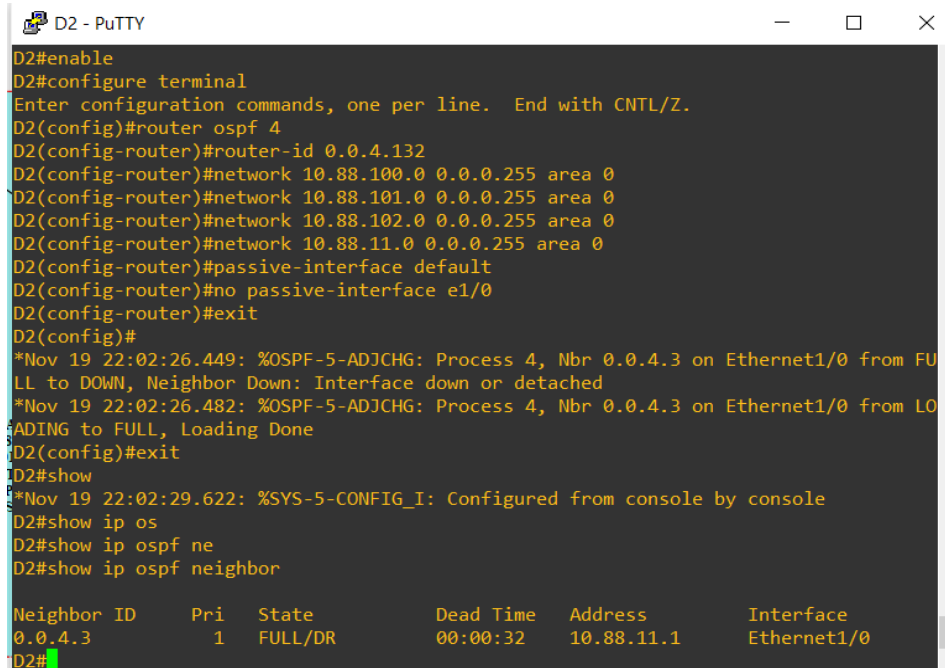
```
R3#
*Nov 19 16:04:31.707: %SYS-5-CONFIG_I: Configured from console by console
R3#
R3#enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.88.11.0 0.0.0.255 area 0
R3(config-router)#network 10.88.13.0 0.0.0.255 area 0
R3(config-router)#exit
R3(config)#exit
R3#show
*Nov 19 16:05:00.563: %SYS-5-CONFIG_I: Configured from console by console
R3#show ip so
R3#show ip os
R3#show ip ospf ne
R3#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.4.1	1	FULL/BDR	00:00:38	10.88.13.1	FastEthernet0/0
0.0.4.132	1	FULL/BDR	00:00:39	10.88.11.2	Ethernet1/0

```
R3#
```

Fuente: propia

Figura 36. configuración OSPFV2 en D2



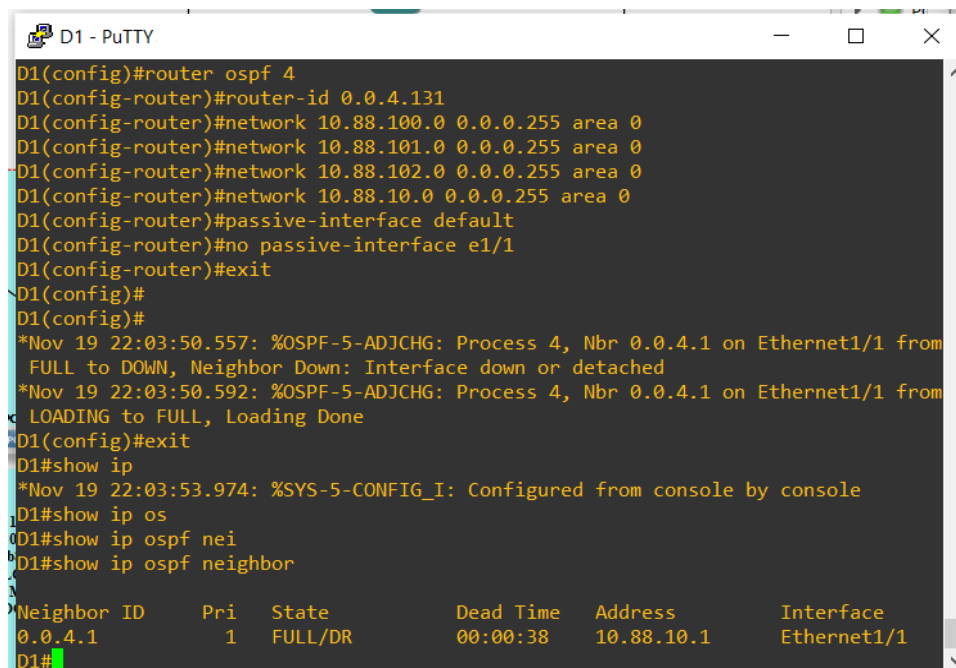
```
D2#enable
D2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.88.100.0 0.0.0.255 area 0
D2(config-router)#network 10.88.101.0 0.0.0.255 area 0
D2(config-router)#network 10.88.102.0 0.0.0.255 area 0
D2(config-router)#network 10.88.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface e1/0
D2(config-router)#exit
D2(config)#
*Nov 19 22:02:26.449: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on Ethernet1/0 from FULL to DOWN, Neighbor Down: Interface down or detached
*Nov 19 22:02:26.482: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on Ethernet1/0 from LOADING to FULL, Loading Done
D2(config)#exit
D2#show
*Nov 19 22:02:29.622: %SYS-5-CONFIG_I: Configured from console by console
D2#show ip os
D2#show ip ospf ne
D2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.4.3	1	FULL/DR	00:00:32	10.88.11.1	Ethernet1/0

```
D2#
```

Fuente: propia

Figura 37. configuración OSPFV2 en D1



```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.88.100.0 0.0.0.255 area 0
D1(config-router)#network 10.88.101.0 0.0.0.255 area 0
D1(config-router)#network 10.88.102.0 0.0.0.255 area 0
D1(config-router)#network 10.88.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface e1/1
D1(config-router)#exit
D1(config)#
D1(config)#
*Nov 19 22:03:50.557: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/1 from FULL to DOWN, Neighbor Down: Interface down or detached
*Nov 19 22:03:50.592: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/1 from LOADING to FULL, Loading Done
D1(config)#exit
D1#show ip
*Nov 19 22:03:53.974: %SYS-5-CONFIG_I: Configured from console by console
D1#show ip os
D1#show ip ospf nei
D1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.4.1	1	FULL/DR	00:00:38	10.88.10.1	Ethernet1/1

```
D1#
```

Fuente: propia

3.2 En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configurar OSPFv3 clásico de área única en el área 0.

➤ Utilizar el ID de proceso OSPF 6 para asignar los siguientes ID de enrutamiento:

- 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/VLAN conectadas directamente en el Área 0.

- En R1, no anuncie la red R1 – R2.
- En R1, propagar una ruta predeterminada, teniendo en cuenta que BGP proporcionará la ruta predeterminada.

➤ Deshabilitar los anuncios OSPFv3 en:

- D1: Todas las interfaces excepto E1/2
- D2: Todas las interfaces excepto E1/0

ROUTER R1:

```
enable
configure terminal
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface f0/0
ipv6 ospf 6 area 0
exit
```

ROUTER 3

```
enable
configure terminal
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface f0/0
ipv6 ospf 6 area 0
exit
end
```

SWITCH D1

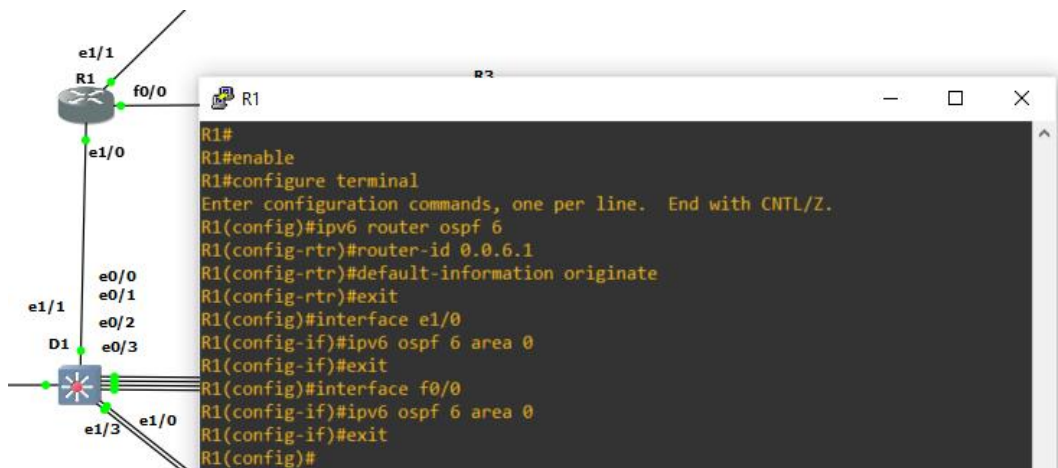
```
enable
configure terminal
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface e1/1
exit
interface e1/1
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

SWITCH D2

```
enable
configure terminal
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface e1/0
exit
```

```
interface e1/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

Figura 38. Configuración OSPFv3 en R1



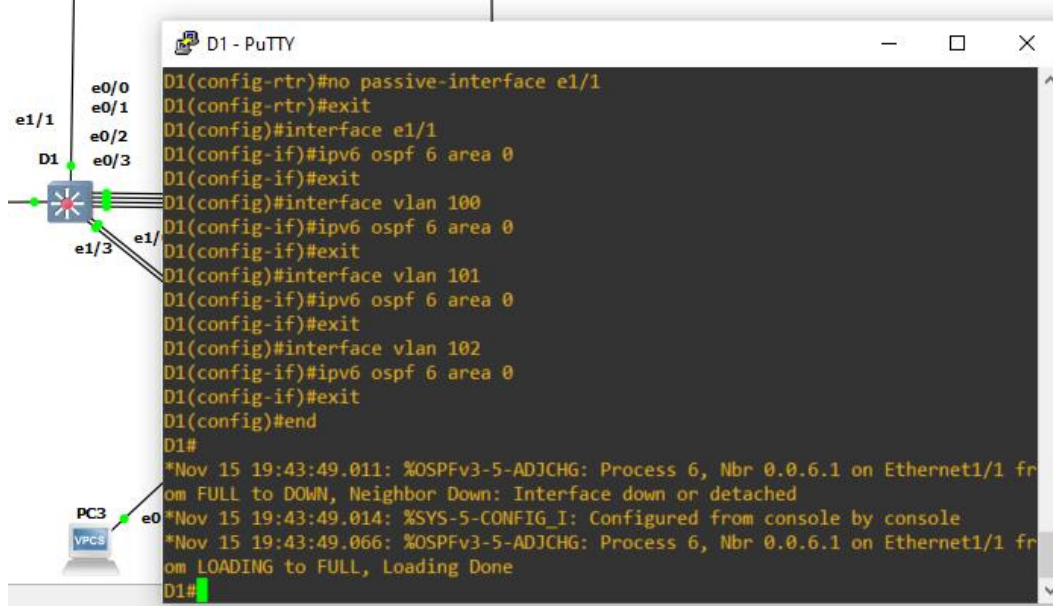
Fuente: propia

Figura 39. Configuración OSPFv3 en R3



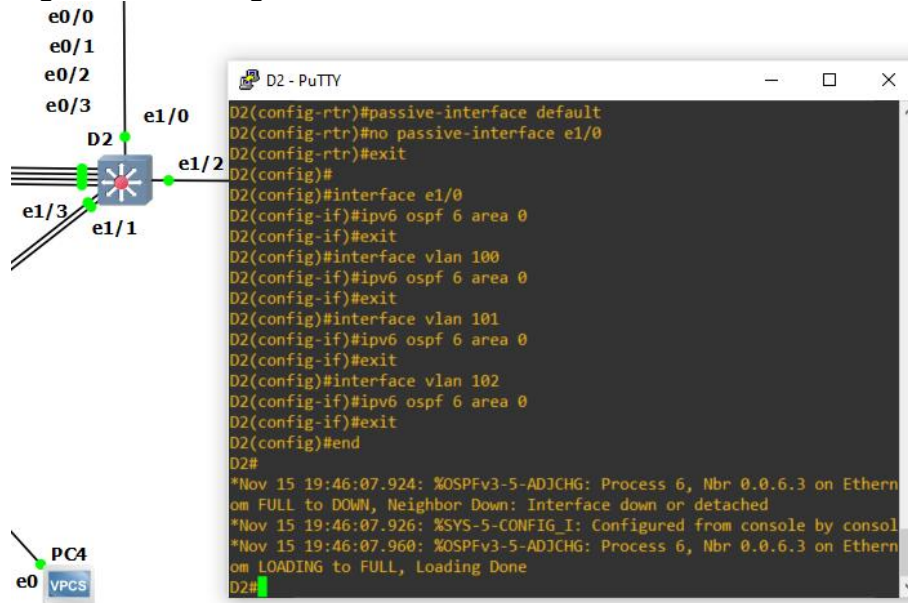
Fuente: propia

Figura 40. Configuración OSPFv3 en D1



Fuente: propia

Figura 41. Configuración OSPFv3 en D2



Fuente: propia

3.3 En R2 en la "Red ISP", configurar MP-BGP.

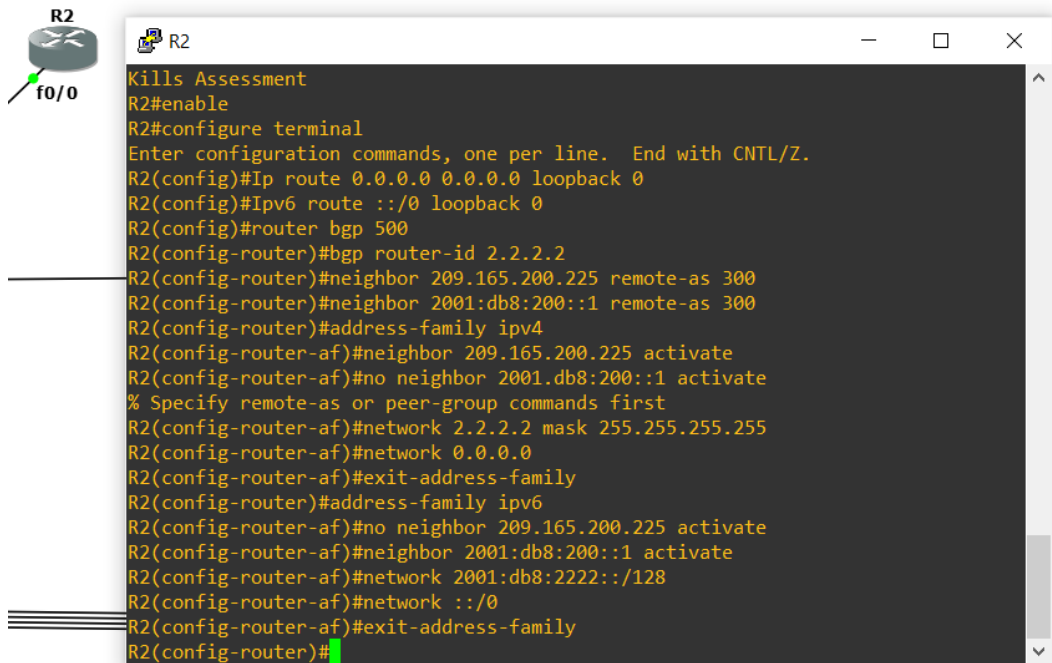
- Configurar dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:
 - Una ruta estática predeterminada IPv4.
 - Una ruta estática predeterminada IPv6.
- Configurar R2 en BGP ASN 500 y usar la identificación del enrutador 2.2.2.2.
- Configurar y habilitar una relación de vecino IPv4 e IPv6 con R1 en ASN 300.
- En la familia de direcciones IPv4, Undvertise:
 - La red IPv4 de bucle invertido 0 (/32).
 - La ruta predeterminada (0.0.0.0/0).
- En Familia de direcciones IPv6, anuncie:

- La red IPv4 de bucle invertido 0 (/128).
- La ruta predeterminada (::/0).

ROUTER R2:

```
enable
configure terminal
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
```


Figura 42. Configuración MP-BGP en R2



```
Kills Assessment
R2#enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#Ip route 0.0.0.0 0.0.0.0 loopback 0
R2(config)#Ipv6 route ::/0 loopback 0
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
% Specify remote-as or peer-group commands first
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#
```

Fuente: propia

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

- Configurar dos rutas resumidas estáticas a la interfaz NULL 0:
 - Una ruta IPv4 resumida para 10.91.0.0/8.
 - Una ruta IPv6 resumida para 2001:db8:100::/48.
- Configurar R1 en BGP ASN 300 y use la identificación del enrutador 1.1.1.1.
- Configurar una relación de vecino IPv4 e IPv6 con R2 en ASN 500.
- En la familia de direcciones IPv4:
 - Deshabilitar la relación de vecino IPv6.
 - Habilitar la relación de vecino IPv4.
 - Anunciar la red 10.91.0.0/8.

En la familia de direcciones IPv6:

- Deshabilitar la relación de vecino IPv4.
- Habilitar la relación de vecino IPv6.

- Anunciar la red 2001:db8:100::/48.

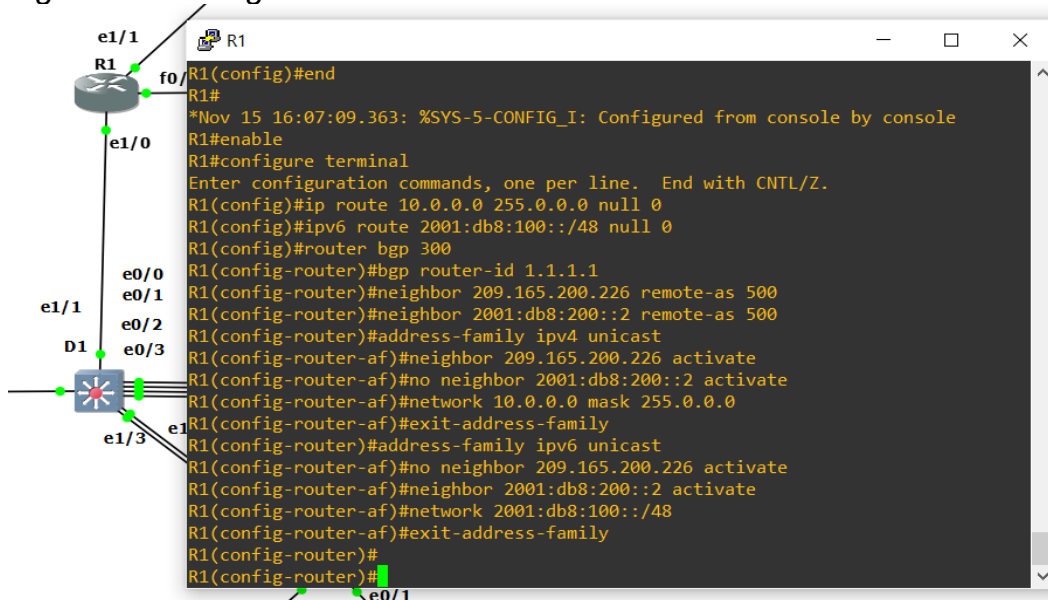
ROUTER 1

```

enable
configure terminal
ip route 10.0.0.0 255.0.0.0 null 0
ipv6 route 2001:db8:100::/48 null 0
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 43. Configuración MP-BGP en la red ISP R1



Fuente: propia

PART 2: CONFIGURAR REDUNDANCIA DE PRIMER SALTO

4.1 En D1, crear IP SLA que prueben la accesibilidad de la interfaz E1/2 de R1.

- Cree dos IP SLA.
 - Utilizar el SLA número 4 para IPv4.
 - Utilizar el SLA número 6 para IPv6.
- Las IP SLA probarán la disponibilidad de la interfaz R1 E1/2 cada 5 segundos.
- Programar el SLA para implementación inmediata sin tiempo de finalización.
- Crear un objeto IP SLA para IP SLA 4 y otro para IP SLA 6.
 - Usar la pista número 4 para IP SLA 4.
 - Usar la pista número 6 para IP SLA 6.

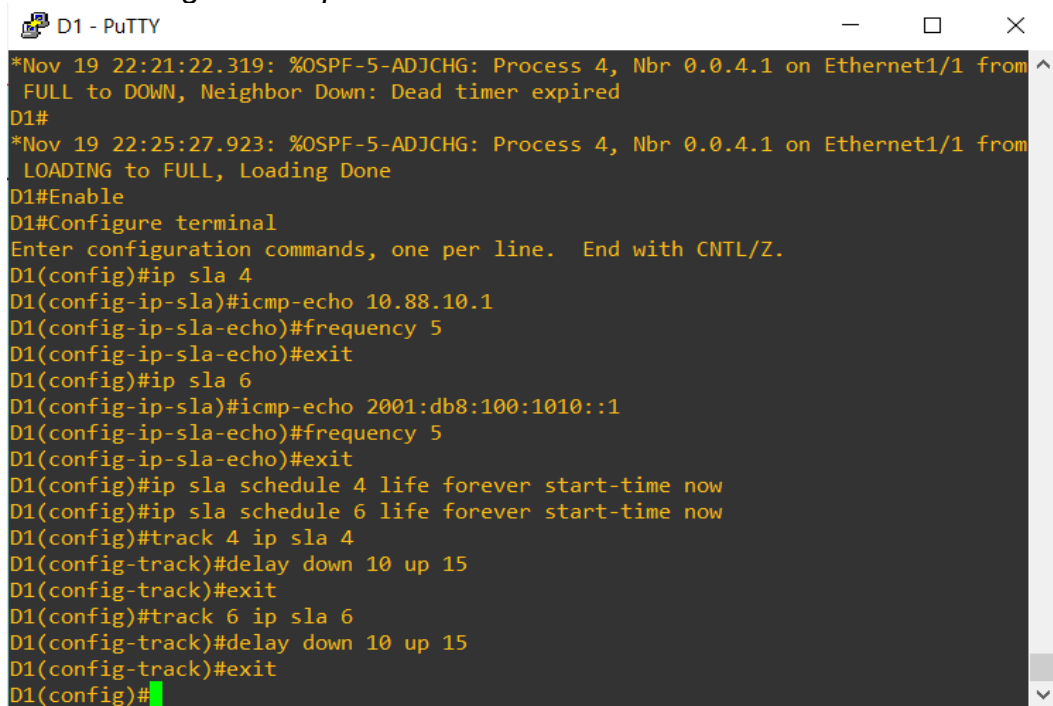
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de abajo a arriba después de 10 segundos, o de arriba a abajo después de 15 segundos.

SWITCH D1

```
Enable
Configure terminal
ip sla 4
icmp-echo 10.88.10.1
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
```

Figura 44. Configuración Ip Sla Para El Acceso A La Interfaz E1/2 De R1



```
D1 - PuTTY
*Nov 19 22:21:22.319: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/1 from
FULL to DOWN, Neighbor Down: Dead timer expired
D1#
*Nov 19 22:25:27.923: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/1 from
LOADING to FULL, Loading Done
D1#Enable
D1#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip sla 4
D1(config-ip-sla)#icmp-echo 10.88.10.1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#track 4 ip sla 4
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#
```

Fuente: propia

4.2 En D2, crear IP SLA que prueben la accesibilidad de la interfaz E1/0 de R3

- Crear dos IP SLA.
 - Utilizar el SLA número 4 para IPv4.
 - Utilizar el SLA número 6 para IPv6.
- Las SLA IP probarán la disponibilidad de la interfaz R3 E1/0 cada 5 segundos.
- Programar el SLA para implementación inmediata sin tiempo de finalización.
- Crear un objeto IP SLA para IP SLA 4 y otro para IP SLA 6.
 - Use la pista número 4 para IP SLA 4.

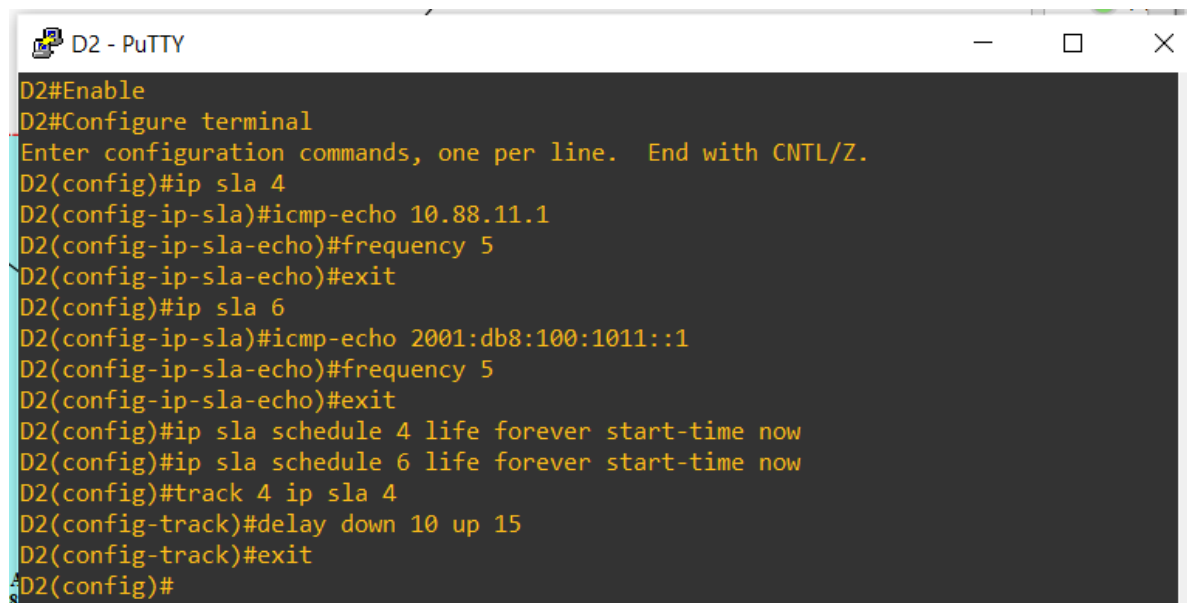
- Use la pista número 6 para IP SLA 6.

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.

SWITCH D2

```
Enable
Configure terminal
ip sla 4
icmp-echo 10.88.11.1
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
```

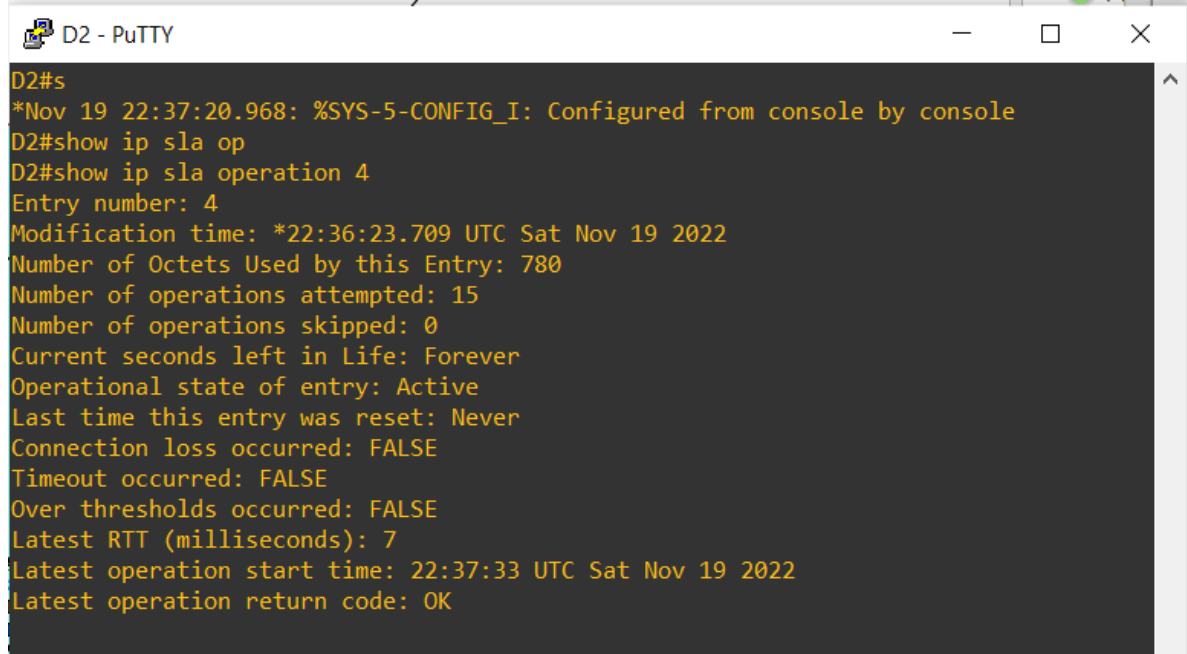
Figura 45. Configuración Ip Sla Para El Acceso A La Interfaz E1/0 De R3



```
D2 - PuTTY
D2#Enable
D2#Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.88.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#
```

Fuente: propia

Figura 46. Verificación Ip Interfaz E1/0 De R3



```
D2 - PuTTY
D2#s
*Nov 19 22:37:20.968: %SYS-5-CONFIG_I: Configured from console by console
D2#show ip sla op
D2#show ip sla operation 4
Entry number: 4
Modification time: *22:36:23.709 UTC Sat Nov 19 2022
Number of Octets Used by this Entry: 780
Number of operations attempted: 15
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 7
Latest operation start time: 22:37:33 UTC Sat Nov 19 2022
Latest operation return code: OK
```

Fuente: propia

4.3 En D1, configurar HSRPv2.

- D1 es el enrutador principal para la VLAN 100 y 102; por lo tanto, su prioridad también se cambiará a 150.
- Configurar la versión 2 de HSRP.
- Configurar el grupo 104 de HSRP de IPv4 para la VLAN 100:
 - Asignar la dirección IP virtual 10.91.100.254.
 - Establezca la prioridad del grupo en 150.
 - Habilitar preferencia.
 - Siga el objeto 4 y disminuya en 60.
- Configure el grupo 114 de HSRP de IPv4 para la VLAN 101:
 - Asigne la dirección IP virtual 10.91.101.254.
 - Habilitar preferencia.
 - Seguimiento del objeto 4 para disminuir en 60.
- Configure el grupo 124 de HSRP de IPv4 para la VLAN 102:

- Asignar la dirección IP virtual 10.91.102.254.
- Establezca la prioridad del grupo en 150.
- Habilitar preferencia.
- Seguimiento del objeto 4 para disminuir en 60.
 - Configurar el grupo 106 de HSRP de IPv6 para la VLAN 100:
- Asignar la dirección IP virtual mediante la configuración automática de ipv6.
- Establezca la prioridad del grupo en 150.
- Habilitar preferencia.
- Siga el objeto 6 y disminuya en 60.
 - Configurar el grupo 116 de HSRP de IPv6 para la VLAN 101:
 - Asignar la dirección IP virtual mediante la configuración automática de ipv6.
 - Habilitar preferencia.
 - Siga el objeto 6 y disminuya en 60.
 - Configurar el grupo 126 de HSRP de IPv6 para la VLAN 102:
- Asignar la dirección IP virtual mediante la configuración automática de ipv6.
- Establezca la prioridad del grupo en 150.
- Habilitar preferencia.
- Siga el objeto 6 y disminuya en 60.

SWITCH D1

```

enable
configure terminal
interface vlan 100
standby version 2
standby 104 ip 10.88.100.254
standby 104 priority 150
standby 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 104 ip 10.88.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.88.102.254
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
end

```

Figura 47. configuración HSRPv2 en D1

```

D1 - PuTTY
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.88.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.88.102.254
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#
*Nov 19 22:39:10.241: %SYS-5-CONFIG_I: Configured from console by console
D1#

```

Fuente: propia

Figura 48. verificación HSRPv2 en D1

```
D1 - PuTTY
D1#show standby brief
P indicates configured to preempt.
|
Interface   Grp  Pri  P State   Active      Standby      Virtual IP
Vl100       104  150  Active local    unknown     10.88.100.254
Vl100       106  150  P Active local    unknown     FE80::5:73FF:FEA0:6A
Vl101       104  100  Active local    unknown     10.88.101.254
Vl101       106  100  Active local    unknown     FE80::5:73FF:FEA0:6A
Vl102       124  150  P Active local    unknown     10.88.102.254
Vl102       126  150  P Active local    unknown     FE80::5:73FF:FEA0:7E
D1#
```

Fuente: propia

SWITCH D2

```
interface vlan 100
standby version 2
standby 104 ip 10.88.100.254
standby 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 104 ip 10.88.101.254
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 10.88.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
```

```
standby 126 track 6 decrement 60
exit
end
```

Figura 49. configuración HSRPv2 en D2

```
D2 - PuTTY
D2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#interface vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.88.100.254
D2(config-if)#standby 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-if)#exit
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.88.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.88.102.254
D2(config-if)#standby 124 preempt
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit
D2(config)# end
```

Fuente: propia

Figura 50. verificación HSRPv2 en D2

```
D2#show standby brief
P indicates configured to preempt.
|
Interface  Grp  Pri  P  State  Active  Standby  Virtual IP
Vl100      104  100  |  Standby  10.88.100.1  local    10.88.100.254
Vl100      106  100  P  Standby  FE80::D1:2  local    FE80::5:73FF:FEA0:6A
Vl101      104  100  |  Standby  10.88.101.1  local    10.88.101.254
Vl101      116  150  P  Active  local        unknown  FE80::5:73FF:FEA0:74
Vl102      124  100  P  Standby  10.88.102.1  local    10.88.102.254
Vl102      126  100  P  Standby  FE80::D1:4  local    FE80::5:73FF:FEA0:7E
D2#
```

Fuente: propia

CONCLUSIONES

El desarrollo del curso de *Diplomado de Profundización CISCO CCNP* permitió planificar, diseñar y simular redes empresariales locales de manera que sean escalables, de igual forma se logra comprender los conceptos técnicos de redes de telecomunicaciones, como calidad de servicio, seguridad, escalabilidad, que alberga el diplomado.

De igual forma se logra comprender el funcionamiento y manejo correcto de la herramienta de simulación GN3, el cual permite la simulación correcta del ejercicio planteado, con cada uno de los dispositivos activos en la red.

Es así como se puede ver que se logró la implementación de protocolos de enrutamiento, dentro de la red LAN, con el fin de garantizar la calidad de la infraestructura de red, calidad de servicio y automatización.

BIBLIOGRAFÍA

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPFv3. CCNP and CCIE Enterprise Core ENCOR 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>