

DIPLOMADO DE PROFUNDIZACIÓN CISCO
INFORME - PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE TITO CANAVAL JIMENEZ

UNIVERSIDA NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
CEAD DOSQUEBRADAS

2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE TITO CANAVAL JIMENEZ

Diplomado de opción de grado presentado para optar al título de
INGENIERO ELECTRÓNICO

DIRECTOR:
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
CEAD DOSQUEBRADAS
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

DOSQUEBRADAS, 27 de noviembre de 2022

CONTENIDO

Lista de figuras.....	5
Glosario	8
Resumen	9
Abstrac.....	9
Introducción	10
1. Parámetros de configuración	11
2. Tabla de direccionamiento	11
3. Escenario propuesto	12
3.1. Objetivos.....	12
3.2. Escenario.....	13
3.3. Dispositivos utilizados.....	13
4. Parte 1.	
Construir la red y configurar.....	13
4.1 Paso 1. Configure los ajustes básicos para cada dispositivo.....	13
4.2 Paso 2. Configure los ajustes básicos para cada dispositivo.....	14
5. Parte 2.	
Configurar la red de capa 2 y la compatibilidad con el host.....	22
5.1 Configuración de dispositivos parte 2.....	24
5.2 Conectividad interfaces trunk.....	27
5.3 Conectividad entre las PC's.....	29
6. Configurar protocolos de enrutamiento.....	34
6.1 Código en los diferentes dispositivos.....	36
6.2 Verificación de configuración.....	41
6.3 Verificación de configuración de la interfaz ipv6 OSPF.....	43
6.4 Configuración del protocolo BGP sistema autónomo 500	44
6.5 Configuración del protocolo BGP sistema autónomo 300.....	45
6.6 Tablas de enrutamiento en el router R1.....	45
6.7 Configuración del protocolo OSPF.....	46
6.8 Configuración del protocolo OSPF router R3.....	47
7. Configurar la redundancia del primer salto.....	47
7.1 Configuración de dispositivos con base en especificaciones.....	50
7.2 Verificación de la configuración de los dispositivos D1 y D2.....	53
Conclusiones.....	56
Bibliografía.....	57

LISTA DE FIGURAS

Figura 1. Parámetros de configuración de la topología.....	11
Figura 2. Conexión entre los diferentes dispositivos tomando como base las instrucciones dadas.....	13
Figura 3. Imagen de verificación de las interfaces en modo troncal en el switch D1.....	28
Figura 4. Imagen de verificación de las interfaces en modo troncal en el switch D2.....	28
Figura 5. Verificación de conexión de las VLAN 100 y 101 y sus respectivos puertos Ethernet.....	29
Figura 6. Conexión entre PC1 y D1.....	29
Figura 7. Conexión entre PC1 y D2.....	30
Figura 8. Conexión entre PC1 y PC4.....	30
Figura 9. Conexión entre PC2 y D1.....	31
Figura 10. Conexión entre PC2 y D2.....	31
Figura 11. Conexión entre PC3 y D1.....	32
Figura 12. Conexión entre PC3 y D2.....	32
Figura 13. Conexión entre PC4 y D1.....	33
Figura 14. Conexión entre PC4 y PC1.....	33
Figura 15. En la figura 15 se observa que el protocolo OSPF está correctamente configurado en el router R1.....	41
Figura 16. En la figura 16 se observa que el protocolo OSPF está correctamente configurado en el router R3.....	41
Figura 17. En la figura 17 se observa que el protocolo OSPF está correctamente configurado en el switch D1.....	42
Figura 18. En la figura 18 se observa que el protocolo OSPF está correctamente configurado en el switch D2.....	42
Figura 19. En la figura 19 se observa la interfaz ipv6 OSPF configurada en el router R1.....	43
Figura 20. En la figura 20 se observa la interfaz ipv6 OSPF configurada en el router R3.....	43
Figura 21. En la figura 21 se observa la interfaz ipv6 OSPF configurada en el switch D1.....	43
Figura 22. En la figura 22 se observa la interfaz ipv6 OSPF configurada en el switch D2.....	44

Figura 23. En las figuras 23 se observa la correcta configuración del protocolo BGP en el router R2.....	44
Figura 24. En las figuras 24 se observa la correcta configuración del protocolo BGP en el router R2.....	45
Figura 25. En la figura 25 se observa la correcta configuración en el router R1 del protocolo BGP.....	45
Figura 26. En la figura 26 se observa que OSPF y BGP trabajan correctamente para ipv4.....	46
Figura 27. En la figura 27 se observa la forma como está configurada la tabla de enrutamiento para ipv6 en el router R1.....	46
Figura 28. En la figura 28 se observa la forma como está configurada la tabla de enrutamiento para ipv6 en el router R3.....	47
Figura 29. En la figura 29 se observa la ejecución del comando show run section ip sla en el switch D1, el cual nos muestra el estado de configuración.....	54
Figura 30. En la figura 30 se observa la ejecución del comando show standby brief en el switch D1, el cual nos presenta la configuración de prioridades respecto al switch D1.....	54
Figura 31. En la figura 31 se observa la ejecución del comando show standby brief en el switch D1, el cual nos presenta la configuración de prioridades respecto al switch D2.....	55

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento.....	11
Tabla 2. Código router R1 parte 1.....	14
Tabla 3. Código router R2 parte 1.....	15
Tabla 4. Código router R3 parte 1.....	16
Tabla 5. Código switch D1 parte 1.....	17
Tabla 6. Código switch D2 parte 1.....	19
Tabla 7. Código switch A1 parte 1.....	21
Tabla 8. Parámetros de configuración de los dispositivos.....	22
Tabla 9. Código switch D1 parte 2.....	24
Tabla 10. Código switch D2 parte 2.....	25
Tabla 11. Código switch A1 parte 2.....	26
Tabla 12. Tareas de configuración.....	34
Tabla 13. Código configuración para el router R1.....	37
Tabla 14. Configuración para el sistema autónomo 500 en el router R2.....	38
Tabla 15. Configuración de OSPF para el router R3.....	39
Tabla 16. Configuración de OSPF para el switch D1.....	39
Tabla 17. Configuración de OSPF para el switch D2.....	40
Tabla 18. Tareas de configuración HSRP.....	48
Tabla 19. Configuración del ICMP en el switch D1.....	51
Tabla 20. Configuración del ICMP en el switch D2.....	53

GLOSARIO

Red: Es la conexión simultánea entre varios dispositivos informáticos con la finalidad de establecer una comunicación e intercambiar datos y otros servicios.

Red inalámbrica: Es un tipo de red que permite la comunicación entre dispositivos por medio ondas de radio.

Topología de red: La definición está dada por dos conceptos el primero el cual se refiere a la forma física como están dispuestas la conexiones entre los dispositivos y el segundo concepto se refiere a la forma en como los hosts tienen acceso a los medios para intercambiar la información.

Dirección IP: IP significa "Protocolo de Internet" y es una forma de identificar única e irrepitiblemente a un dispositivo que se encuentra dentro de una red global o local.

IPV4: Significa Protocolo de Internet versión 4 y es un protocolo para redes de datos el cual utiliza direcciones de 32 bits alcanzando su máximo posible en 4 294 967 296.

IPV6: Como el ipv4 este también es un protocolo, pero versión 6 y fue diseñado para reemplazar el actual ipv4.

Switch: Es un dispositivo que tiene como función poder conectar y controlar varios periféricos como PC's, impresoras y servidores entre otros, permitiendo así una comunicación.

Router: Es un dispositivo que tiene la finalidad de recibir, procesar y mover datos entre redes informáticas.

Puerto de acceso: Es la parte física en donde se realiza la conexión de un dispositivo o periférico como una PC o impresora.

Protocolo: Es un conjunto de normas y estándares los cuales rigen la forma y como se controla la interacción entre dispositivos en una red.

Red LAN: Es una red local la cual permite la comunicación entre dispositivos que están dentro del mismo edificio.

Red WAN: Es la unión de varias redes locales "LAN".

Red VLAN: Es una red virtual local la cual subsiste dentro de una misma red física.

Host: Representa a cualquier PC o dispositivo que esté conectado a una red.

Protocolo DHCP: Protocolo de configuración dinámica DHCP y es un protocolo cliente/servidor el cual proporciona automáticamente un host o IP asignando una configuración de subred y puerta de enlace.

Sistema autónomo AS: Es una red que se compone de un grupo de redes de tamaño considerable y que comparten una única forma de enrutamiento.

Protocolo BGP: Es un protocolo que permite la comunicación entre sistemas autónomos "AS".

Protocolo OSPF: Es un protocolo de enlace/estado el cual basa su funcionamiento en el algoritmo de la vía más corta.

Protocolo ICMP: Este protocolo define si el destino está activo y es alcanzable, también diagnostica problemas, sincroniza y obtiene las direcciones en la red.

RESUMEN

Este trabajo se desarrolla sobre la práctica en el software GNS3, en primera instancia en el punto 1 se establecen unas pautas de diseño, en el punto 2 se presenta la tabla de enrutamiento, en el punto 3 se establecen el escenario propuesto, los objetivos, los dispositivos necesarios para la red, en el punto 4 se diseña la red en GNS3 y se realiza una configuración básica de los dispositivos que componen la red, en el punto 5 se configura la red de capa 2 y la compatibilidad en el host, también se concentra la programación en los dispositivos D1, D2, A1 y se hace un test de prueba de funcionamiento en los dispositivos. En el punto 6 se configuran los protocolos de enrutamiento en los dispositivos R1, R2, R3, D1, D2, A1, además se realiza una prueba de funcionamiento de los protocolos configurados en cada uno de los dispositivos. En el punto 7 la programación se concentra en los dispositivos D1 y D2 en donde se configura la versión 2 del HSRP la cual proporcionará la redundancia de primer salto para los hosts en la red y finalmente se hace una prueba de la que la configuración en los dispositivos se haya realizado correctamente.

ABSTRAC

This work is developed on the practice in the GNS3 software, in the first instance in point 1 some design guidelines are based, in point 2 the routing table is presented, in point 3 the proposed scenario is based, the objectives, the necessary devices for the network, in point 4 the network is designed in GNS3 and a basic configuration of the devices that make up the network is carried out, in point 5 the layer 2 network is configured and the compatibility in the host, as well the programming is concentrated in the devices D1, D2, A1 and a functional test is carried out on the devices. In point 6, the routing protocols are configured in the devices R1, R2, R3, D1, D2, A1, in addition, a functional test of the protocols configured in each of the devices is carried out. In point 7, the programming is concentrated in the D1 and D2 devices where version 2 of the HSRP is configured, which achieves first hop redundancy for the hosts in the network and finally a test is made that the configuration in the devices is successful.

INTRODUCCIÓN

Desde que se inventó el telégrafo hasta la invención del satélite la sociedad no para de perfeccionar los medios y las formas transmitir información, pero estos inventos no serían útiles sin aplicación de los protocolos como el OSPF el cual utiliza un algoritmo para establecer la vía más corta para realizar la conexión, o el BGP el cual permite la comunicación entre sistemas autónomos. Este diplomado en redes CCNP se desarrolla sobre la aplicación de diferentes conceptos de protocolos, LAN's, WAN's, VLAN's, direccionamiento ipv4 e ipv6, sin los cuales esta red no podría funcionar apropiadamente.

De forma general el documento en primera instancia es un escenario propuesto en donde se presenta una red la cual se debe diseñar siguiendo unas especificaciones dadas en cuanto a los ajustes básicos en cada dispositivo y estableciendo un direccionamiento de las diferentes interfaces; configurar la capa 2 de la red del host, configurar los protocolos, configurar la redundancia del primer salto y configurar la seguridad.

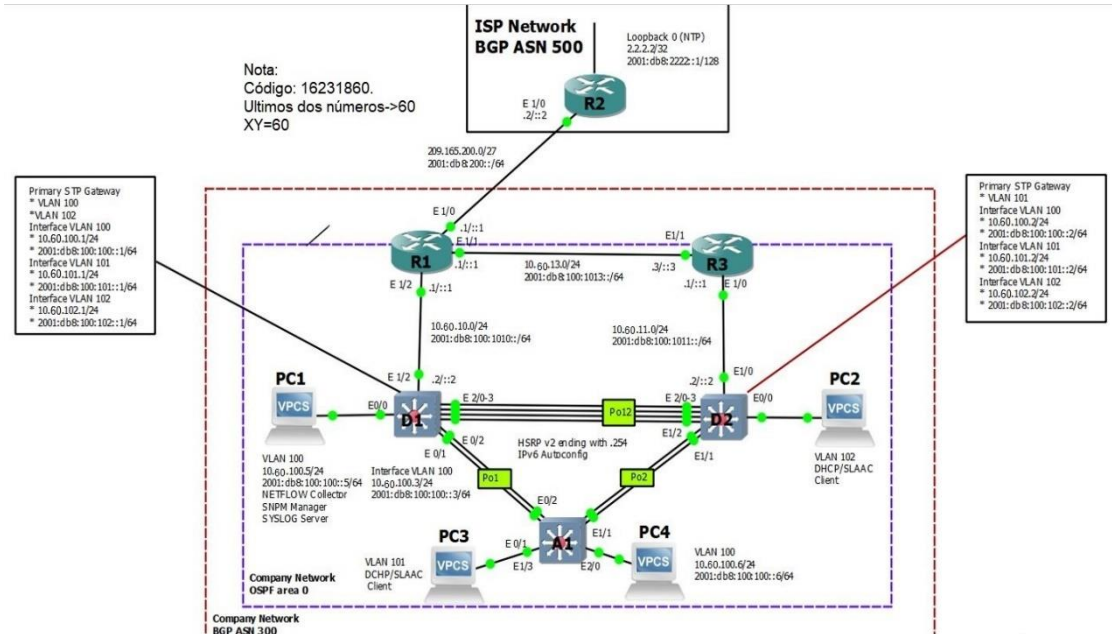
De forma más específica el documento se encuentra dividido en dos partes, la primera parte se compone desde los puntos 1, 2, 3 y 4 los cuales tratan sobre el diseño de la red y sigue una secuencia de configuración de todos los dispositivos que componen la red y la segunda parte se componen de los puntos 5, 6 y 7 y se enfocan en mayor parte en la configuración en los switches D1, D2 y A1 que están relacionados con las respectivas VLAN's, la configuración del protocolo BGP para el funcionamiento del sistema autónomo AS 500 y del sistema autónomo AS 300.

Esta red tendrá una accesibilidad de extremo a extremo, de modo que los hosts tengan soporte de puerta de enlace predeterminada confiable y para que los protocolos de administración estén operativos dentro de la red. Así mismo en el desarrollo de este trabajo se verá paso a paso con la aplicación de los diferentes comandos agrupados en tablas las cuales estarán debidamente identificadas para que dispositivo aplica y reiterando que estas configuraciones siguen las instrucciones dadas para que estos dispositivos funcionen como se requiere.

Prueba de habilidades práctica.

1. Parámetros de configuración para la topología de red establecida.

Figura 1. En la imagen se establecen los parámetros de diseño que se siguen para la conexión y configuración entre los dispositivos que conforman la red.



Nota: Para la siguiente configuración de red se utiliza el código: 16231860; de modo que los dos últimos números para XY=60

2. Tabla de direccionamiento.

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfac e	Dirección Ipv4	Dirección Ipv6	Ipv6 Link-Local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.60.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10.60.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1

Dispositivo	Interfaz	Dirección Ipv4	Dirección Ipv6	Ipv6 Link-Local
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10.60.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.60.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10.60.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.60.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.60.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.60.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.60.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.60.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.60.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.60.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.60.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.60.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.60.100.6/24	2001:db8:100:100::6/64	EUI-64

3. Escenario propuesto.

3.1 Objetivos.

- Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz.
- Parte 2: configurar la red de capa 2 y la compatibilidad con el host.
- Parte 3: configurar protocolos de enrutamiento.
- Parte 4: configurar la redundancia de primer salto.

3.2 Escenario.

En esta evaluación de habilidades, usted es responsable de completar la configuración de la red para que haya accesibilidad completa de extremo a extremo, para que los hosts tengan soporte de puerta de enlace predeterminada confiable y para que los protocolos de administración estén operativos dentro de la parte de "Red de la empresa" de la topología. Tenga cuidado de verificar que sus configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen según lo requerido.

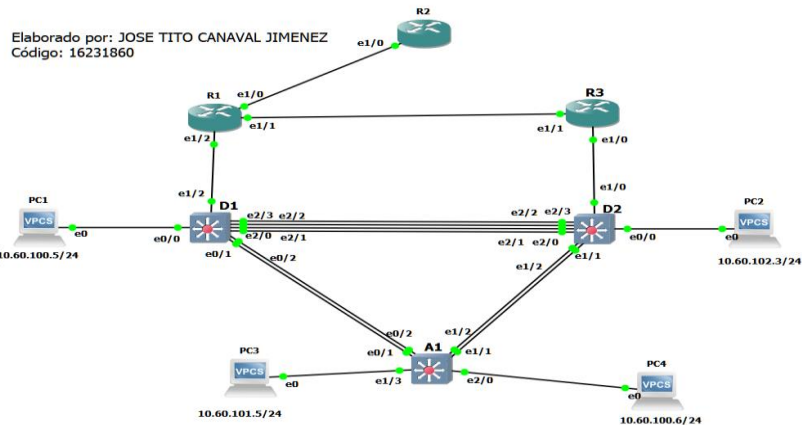
3.3 Dispositivos utilizados.

- 3 Routers (Cisco 7200).
- 3 Switches (Cisco IOU L2).
- 4 PCs (Use the GNS3's VPCS)

4. Parte 1: construir la red y configurar los ajustes básicos del dispositivo y el direccionamiento de la interfaz

4.1 Paso 1: conecte la red como se muestra en la topología.

Figura 2. Conexión entre los diferentes dispositivos tomando como base las instrucciones dadas.



4.2 Paso 2: Configure los ajustes básicos para cada dispositivo.

a. En el modo consola en cada dispositivo, ingrese al modo de configuración global y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.

Router R1.

En la tabla 2 se presenta el código de programación del router R1 en donde se cambia el nombre del dispositivo, las interfaces, las direcciones IP, entre otros.

Tabla 2. Código router R1 parte 1

```

Hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment#
line con 0
  exec-timeout 0 0
  logging synchronous
exit
interface e1/0
  ip address 209.165.200.225 255.255.255.224
  ipv6 address fe80::1:1 link-local
  ipv6 address 2001:db8:200::1/64
  no shutdown
exit
interface e1/2

```

```
ip address 10.60.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface e1/1
ip address 10.60.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
```

Router R2.

En la tabla 3 se presenta el código de programación del router R2 donde se cambia el nombre del dispositivo, las interfaces, las direcciones IP, entre otros.

Tabla 3. Código router R2 parte 1

```
Hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment#
line con 0
exec-timeout 0 0
logging synchronous
exit
interface e1/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
```

```
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

Router R3

En la tabla 4 se presenta el código de programación del router R3 donde se cambia el nombre del dispositivo, las interfaces, las direcciones IP, entre otros.

Tabla 4. Código router R3 parte 1

```
Hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment#
line con 0
  exec-timeout 0 0
  logging synchronous
exit
interface e1/0
  ip address 10.60.11.1 255.255.255.0
  ipv6 address fe80::3:2 link-local
  ipv6 address 2001:db8:100:1011::1/64
  no shutdown
exit
interface e1/1
  ip address 10.60.13.3 255.255.255.0
  ipv6 address fe80::3:3 link-local
  ipv6 address 2001:db8:100:1010::2/64
  no shutdown
exit
```

Switch D1

En la tabla 5 se presenta el código correspondiente a la programación del switch D1, en el cual se configura el nombre del dispositivo, el aviso de advertencia, el nombre de cada una de las VLAN, las direcciones IP, las interfaces Ethernet, entre otros.

Tabla 5. Código switch D1 parte 1

```
Hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment#
line con 0
  exec-timeout 0 0
  logging synchronous
exit
vlan 100
  name Management
exit
vlan 101
  name UserGroupA
exit
vlan 102
  name UserGroupB
exit
vlan 999
  name NATIVE
exit
interface e1/2
  no switchport
  ip address 10.60.10.2 255.255.255.0
  ipv6 address fe80::d1:1 link-local
  ipv6 address 2001:db8:100:1010::2/64
```

```
no shutdown
exit
interface vlan 100
ip address 10.60.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.60.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.60.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.60.101.1 10.60.101.109
ip dhcp excluded-address 10.60.101.141 10.60.101.254
ip dhcp excluded-address 10.60.102.1 10.60.102.109
ip dhcp excluded-address 10.60.102.141 10.60.102.254
ip dhcp pool VLAN-101
network 10.60.101.0 255.255.255.0
default-router 10.60.101.254
exit
ip dhcp pool VLAN-102
network 10.60.102.0 255.255.255.0
default-router 10.60.102.254
```

```
exit
interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
shutdown
exit
```

Switch D2

En la tabla 6 se presenta el código correspondiente a la programación del switch D2, en el cual se configura el nombre del dispositivo, el aviso de advertencia, el nombre de cada una de las VLAN, las direcciones IP, las interfaces Ethernet, entre otros.

Tabla 6. Código switch D2 parte 1.

```
Hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment#
line con 0
  exec-timeout 0 0
logging synchronous
exit
vlan 100
  name Management
exit
vlan 101
  name UserGroupA
exit
vlan 102
```

```
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e1/0
no switchport
ip address 10.60.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.60.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.60.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.60.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.60.101.1 10.60.101.209
```

```
ip dhcp excluded-address 10.60.101.241 10.60.101.254
ip dhcp excluded-address 10.60.102.1 10.60.102.209
ip dhcp excluded-address 10.60.102.241 10.60.102.254
ip dhcp pool VLAN-101
  network 10.60.101.0 255.255.255.0
  default-router 10.60.0.101.254
  exit
ip dhcp pool VLAN-102
  network 10.60.102.0 255.255.255.0
  default-router 10.60.102.254
  exit
interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
  shutdown
  exit
```

Switch A1

En la tabla 7 se presenta el código corresponde a la programación del switch A1, en el cual se configura el nombre del dispositivo, el aviso de advertencia, el nombre de cada una de las VLAN, las direcciones IP, las interfaces Ethernet, entre otros.

Tabla 7. Código switch A1 parte 1.

```
Hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment#
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
vlan 100
  name Management
  exit
vlan 101
```

```
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.60.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range e0/0,e0/3,e1/0,e2/1-3,e3/0-3
shutdown
exit
```

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

Mediante el comando *copy running-config startup-config* aplicado cada dispositivo se guarda la configuración.

c. Configure el direccionamiento de host de PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.60.100.254, que será la dirección IP virtual de HSRP utilizada en la Parte 4.

5. Parte 2: configurar la red de capa 2 y la compatibilidad con el host.

En esta parte de la evaluación de habilidades, completará la configuración de la red de capa 2 y configurará el soporte de host básico. Al final de esta parte, todos los interruptores deberían poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Sus tareas de configuración son las siguientes:

Tabla 8. Parámetros de configuración de los dispositivos.

Tarea #	Tarea	Especificaciones	Puntos
2.1	En todos los conmutadores, configure las interfaces troncales IEEE 802.1Q en los enlaces de conmutador de interconexión	Habilite enlaces troncales 802.1Q entre: <ul style="list-style-type: none"> • D1 y D2 • D1 y A1 • D2 y A1 	6
2.2	En todos los conmutadores, cambie la VLAN nativa en los enlaces troncales.	Utilice la VLAN 999 como la VLAN nativa.	6
2.3	En todos los conmutadores, habilite el protocolo Rapid Spanning-Tree.	Use Rapid Spanning Tree.	3
2.4	En D1 y D2, configure los puentes raíz RSTP apropiados según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz.	Configure D1 y D2 como raíz para las VLAN apropiadas con prioridades que se apoyen mutuamente en caso de falla del conmutador.	2
2.5	En todos los switches, cree LACP EtherChannels como se muestra en el diagrama de topología.	Utilice los siguientes números de canal: <ul style="list-style-type: none"> • D1 a D2: canal de puerto 12 • D1 a A1: canal de puerto 1 • D2 a A1: canal de puerto 2 	3

Tarea #	Tarea	Especificaciones	Puntos
2.6	En todos los conmutadores, configure los puertos de acceso de host que se conectan a PC1, PC2, PC3 y PC4.	<p>Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.</p> <p>Los puertos de host deben pasar inmediatamente al estado de reenvío.</p> <p>Abrir en Google Traductor</p> <ul style="list-style-type: none"> • <p>Comentarios</p>	4
2.7	Verificar los servicios Ipv4 DHCP.	PC2 y PC3 son clientes DHCP y deben recibir direcciones Ipv4 válidas.	1
2.8	Verificar la conectividad local LAN.	<p>PC1 debería hacer ping:</p> <ul style="list-style-type: none"> • D1: 10.60.100.1 • D2: 10.60.100.2 • PC4: 10.60.100.6 <p>PC2 debería hacer ping:</p> <ul style="list-style-type: none"> • D1: 10.60.102.1 • D2: 10.60.102.2 <p>PC3 debería hacer ping:</p> <ul style="list-style-type: none"> • D1: 10.60.101.1 • D2: 10.60.101.2 <p>PC4 debería hacer ping:</p> <ul style="list-style-type: none"> • D1: 10.60.100.1 • D2: 10.60.100.2 • PC1: 10.60.100.5 	1

5.1 Código en cada uno de los dispositivos con base en las especificaciones establecidas en la tabla 8.

Switch D1.

En la tabla 9 se presenta el código correspondiente a la programación del switch D1, en el cual se configuran los diferentes rangos de interfaces utilizados, el modo de encapsulamiento, el modo de operación Trunk, las VLAN prioritarias, entre otros.

Tabla 9. Código switch D1 parte 2.

```
Interface range e2/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit

interface range e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit

spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
interface e0/0
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
```

```
end
```

Switch D2.

En la tabla 10 se presenta el código correspondiente a la programación del switch D2, en el cual se configuran los diferentes rangos de interfaces utilizados, el modo de encapsulamiento, el modo de operación Trunk, las VLAN prioritarias, entre otros.

Tabla 10. Código switch D2 parte 2.

```
Interface range e2/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
interface e0/0
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
end
```

Switch A1.

En la tabla 11 se presenta el código correspondiente a la programación del switch A1, en el cual se configuran los diferentes rangos de interfaces utilizados, el modo de encapsulación, el modo de operación Trunk, las VLAN prioritarias, entre otros.

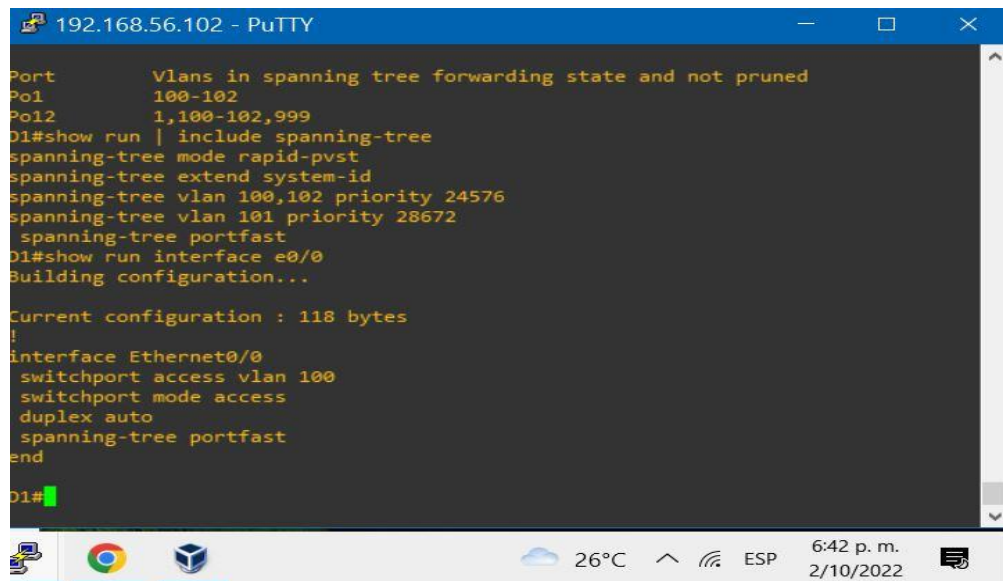
Tabla 11. Código switch A1 parte 2.

```
Spanning-tree mode rapid-pvst
interface range e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
interface range e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
interface e1/3
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface e2/0
switchport mode access
switchport access vlan 100
spanning-tree portfast
```

```
no shutdown
exit
end
```

5.2 Resultados de conexión entre interfaces trunk.

Figura 3. Imagen de verificación de las interfaces en modo troncal en el switch D1.

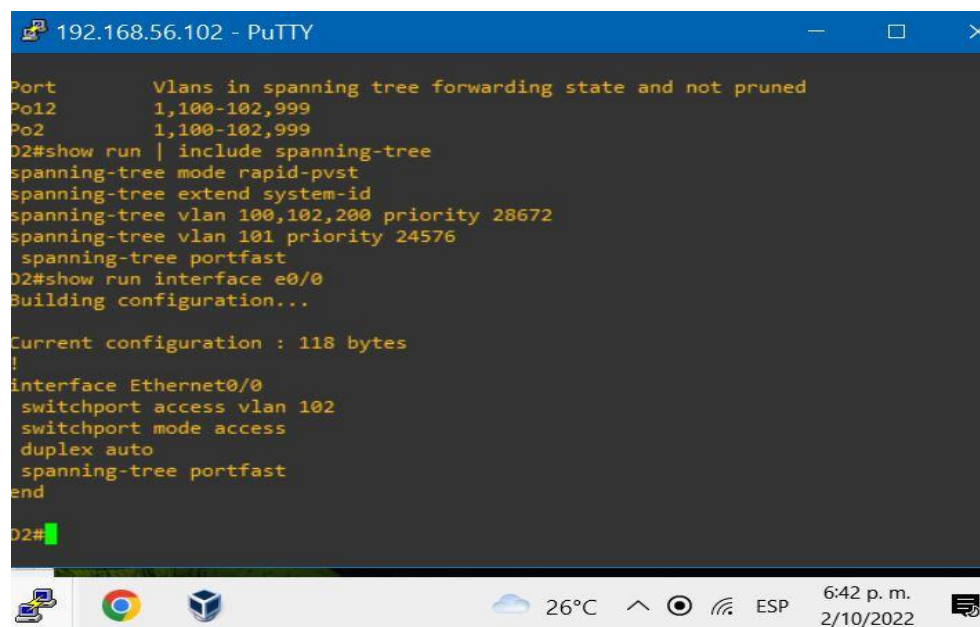


```
192.168.56.102 - PuTTY
Port      Vlans in spanning tree forwarding state and not pruned
Po1       100-102
Po12      1,100-102,999
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
spanning-tree portfast
D1#show run interface e0/0
Building configuration...

Current configuration : 118 bytes
!
interface Ethernet0/0
 switchport access vlan 100
 switchport mode access
 duplex auto
 spanning-tree portfast
end
D1#
```

Switch D2.

Figura 4. Imagen de verificación de las interfaces en modo troncal en el switch D2.

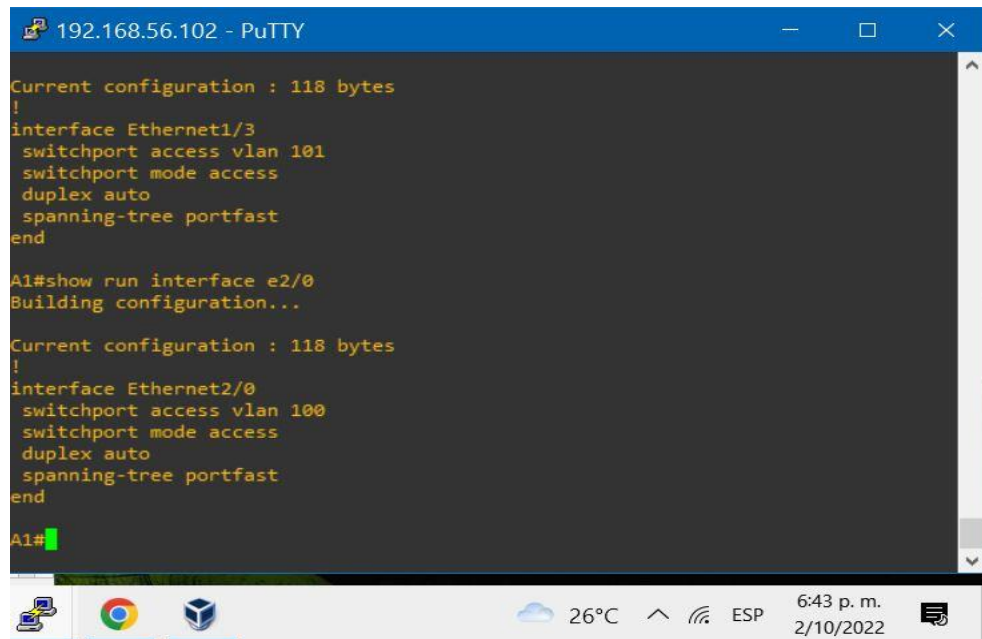


```
192.168.56.102 - PuTTY
Port      Vlans in spanning tree forwarding state and not pruned
Po12      1,100-102,999
Po2       1,100-102,999
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102,200 priority 28672
spanning-tree vlan 101 priority 24576
spanning-tree portfast
D2#show run interface e0/0
Building configuration...

Current configuration : 118 bytes
!
interface Ethernet0/0
 switchport access vlan 102
 switchport mode access
 duplex auto
 spanning-tree portfast
end
D2#
```

Switch A1.

Figura 5. Verificación de conexión de las VLAN 100 y 101 y sus respectivos puertos Ethernet.



```
192.168.56.102 - PuTTY
Current configuration : 118 bytes
!
interface Ethernet1/3
 switchport access vlan 101
 switchport mode access
 duplex auto
 spanning-tree portfast
end

A1#show run interface e2/0
Building configuration...

Current configuration : 118 bytes
!
interface Ethernet2/0
 switchport access vlan 100
 switchport mode access
 duplex auto
 spanning-tree portfast
end

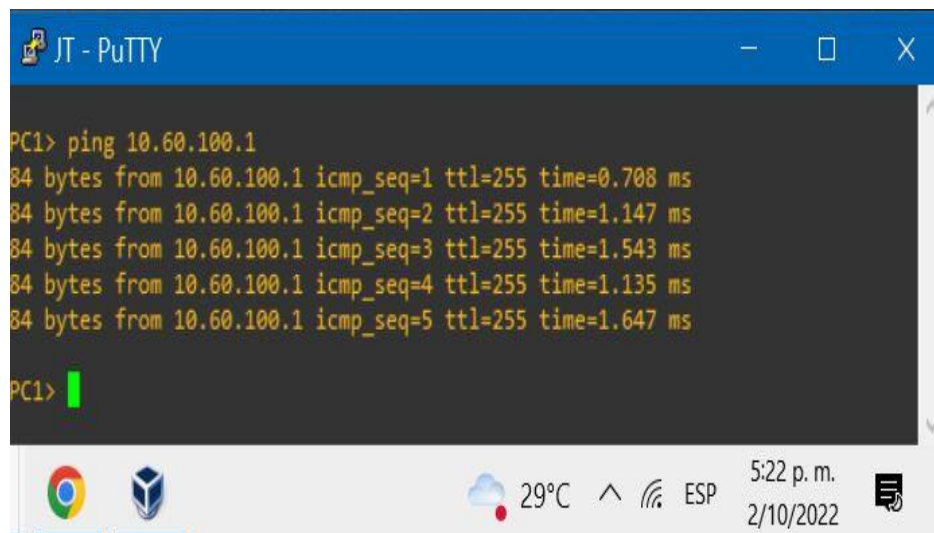
A1#
```

5.3 Resultados de conectividad entre las PC's.

PC1.

- D1: D1: 10.60.100.1

Figura 6. Las figuras 6, 7 y 8 muestran la evidencia de conexión entre el PC1 y los dispositivos D1, D2 y PC4 respectivamente.



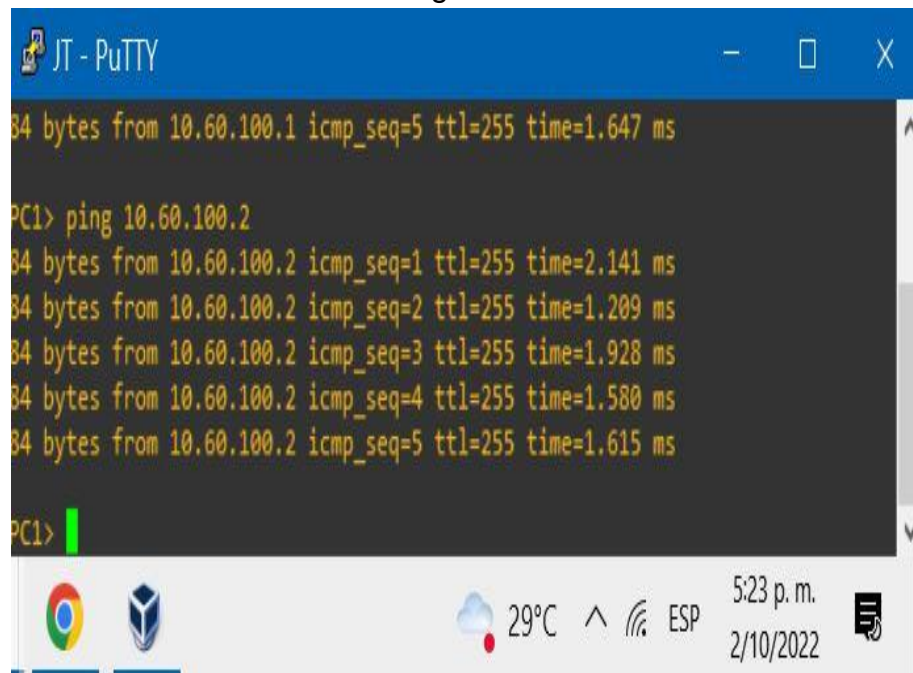
```
JT - PuTTY

PC1> ping 10.60.100.1
84 bytes from 10.60.100.1 icmp_seq=1 ttl=255 time=0.708 ms
84 bytes from 10.60.100.1 icmp_seq=2 ttl=255 time=1.147 ms
84 bytes from 10.60.100.1 icmp_seq=3 ttl=255 time=1.543 ms
84 bytes from 10.60.100.1 icmp_seq=4 ttl=255 time=1.135 ms
84 bytes from 10.60.100.1 icmp_seq=5 ttl=255 time=1.647 ms

PC1>
```

- D2: 10.60.100.2

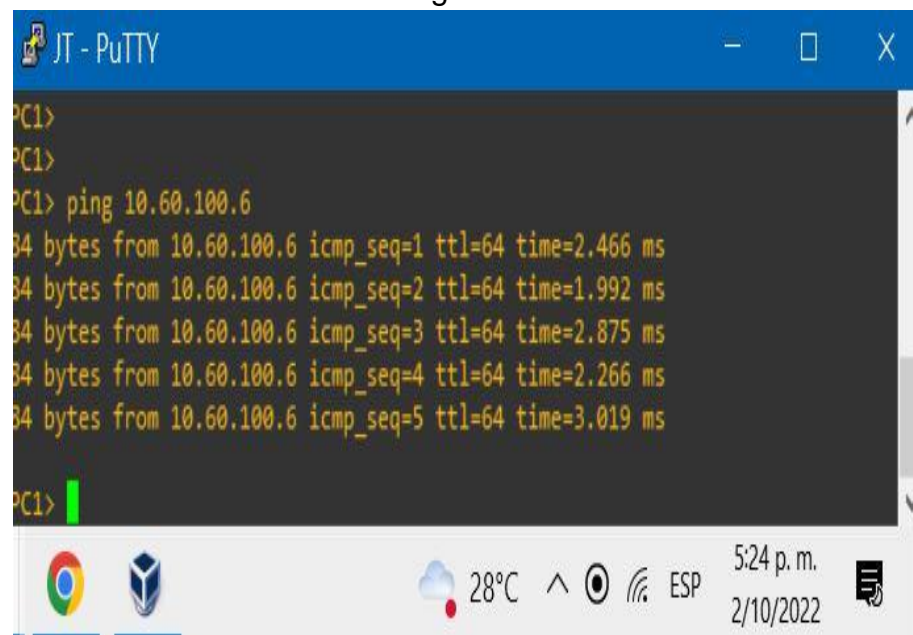
Figura 7.



```
JT - PuTTY  
84 bytes from 10.60.100.1 icmp_seq=5 ttl=255 time=1.647 ms  
PC1> ping 10.60.100.2  
84 bytes from 10.60.100.2 icmp_seq=1 ttl=255 time=2.141 ms  
84 bytes from 10.60.100.2 icmp_seq=2 ttl=255 time=1.209 ms  
84 bytes from 10.60.100.2 icmp_seq=3 ttl=255 time=1.928 ms  
84 bytes from 10.60.100.2 icmp_seq=4 ttl=255 time=1.580 ms  
84 bytes from 10.60.100.2 icmp_seq=5 ttl=255 time=1.615 ms  
PC1>
```

- PC1: 10.60.100.6

Figura 8.

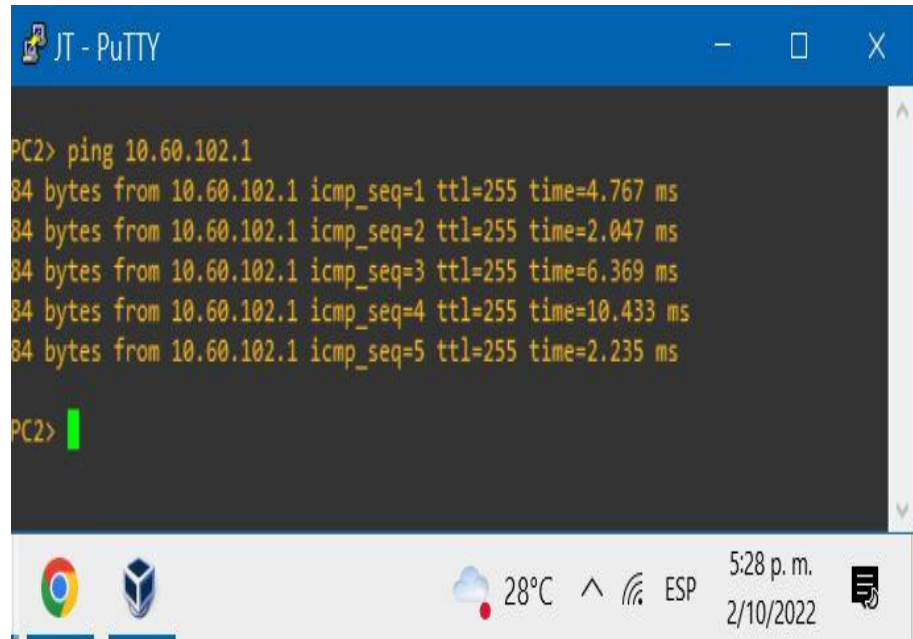


```
JT - PuTTY  
PC1>  
PC1>  
PC1> ping 10.60.100.6  
84 bytes from 10.60.100.6 icmp_seq=1 ttl=64 time=2.466 ms  
84 bytes from 10.60.100.6 icmp_seq=2 ttl=64 time=1.992 ms  
84 bytes from 10.60.100.6 icmp_seq=3 ttl=64 time=2.875 ms  
84 bytes from 10.60.100.6 icmp_seq=4 ttl=64 time=2.266 ms  
84 bytes from 10.60.100.6 icmp_seq=5 ttl=64 time=3.019 ms  
PC1>
```

PC2.

- D1: 10.60.102.1

Figura 9. Las figuras 9 y 10 muestran la evidencia de conexión entre la PC2 y los dispositivos D1, D2 respectivamente.

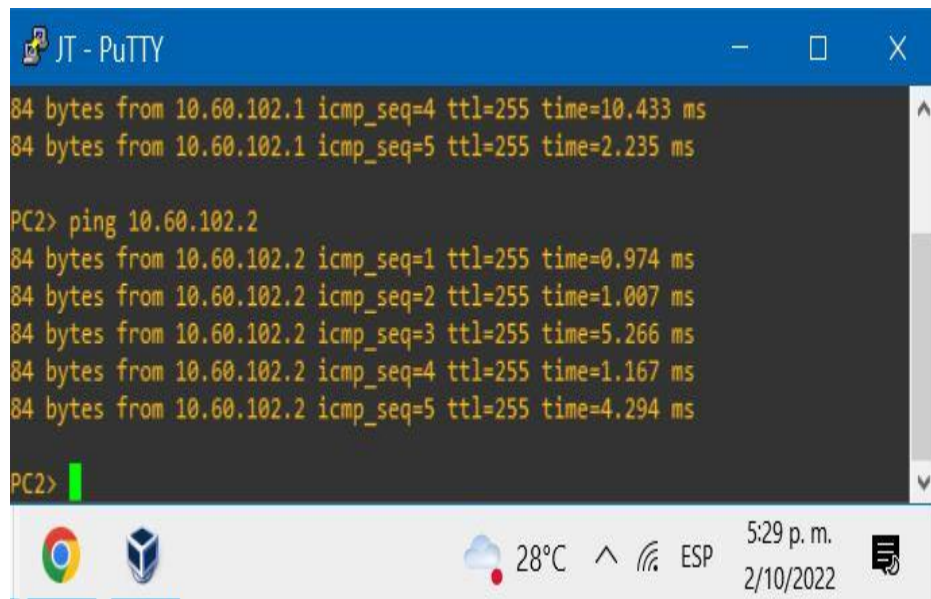


```
JT - PuTTY
PC2> ping 10.60.102.1
84 bytes from 10.60.102.1 icmp_seq=1 ttl=255 time=4.767 ms
84 bytes from 10.60.102.1 icmp_seq=2 ttl=255 time=2.047 ms
84 bytes from 10.60.102.1 icmp_seq=3 ttl=255 time=6.369 ms
84 bytes from 10.60.102.1 icmp_seq=4 ttl=255 time=10.433 ms
84 bytes from 10.60.102.1 icmp_seq=5 ttl=255 time=2.235 ms

PC2> |
```

- D2: 10.60.102.2

Figura 10.



```
JT - PuTTY
84 bytes from 10.60.102.1 icmp_seq=4 ttl=255 time=10.433 ms
84 bytes from 10.60.102.1 icmp_seq=5 ttl=255 time=2.235 ms

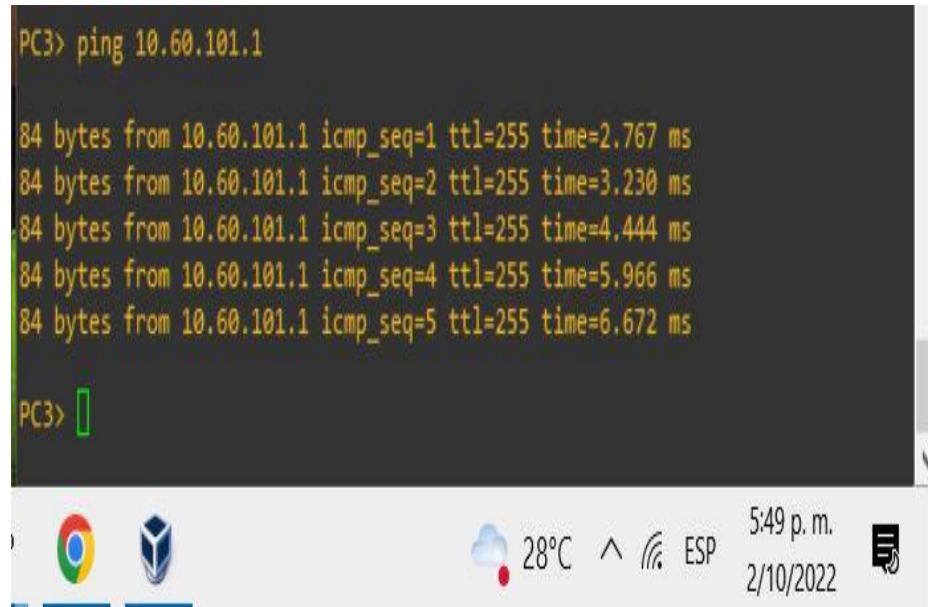
PC2> ping 10.60.102.2
84 bytes from 10.60.102.2 icmp_seq=1 ttl=255 time=0.974 ms
84 bytes from 10.60.102.2 icmp_seq=2 ttl=255 time=1.007 ms
84 bytes from 10.60.102.2 icmp_seq=3 ttl=255 time=5.266 ms
84 bytes from 10.60.102.2 icmp_seq=4 ttl=255 time=1.167 ms
84 bytes from 10.60.102.2 icmp_seq=5 ttl=255 time=4.294 ms

PC2> |
```

PC3.

- D1: 10.60.101.1

Figura 11. Las figuras 11 y 12 muestran la evidencia de conexión entre PC3 y los dispositivos D1, D2 respectivamente.



```
PC3> ping 10.60.101.1

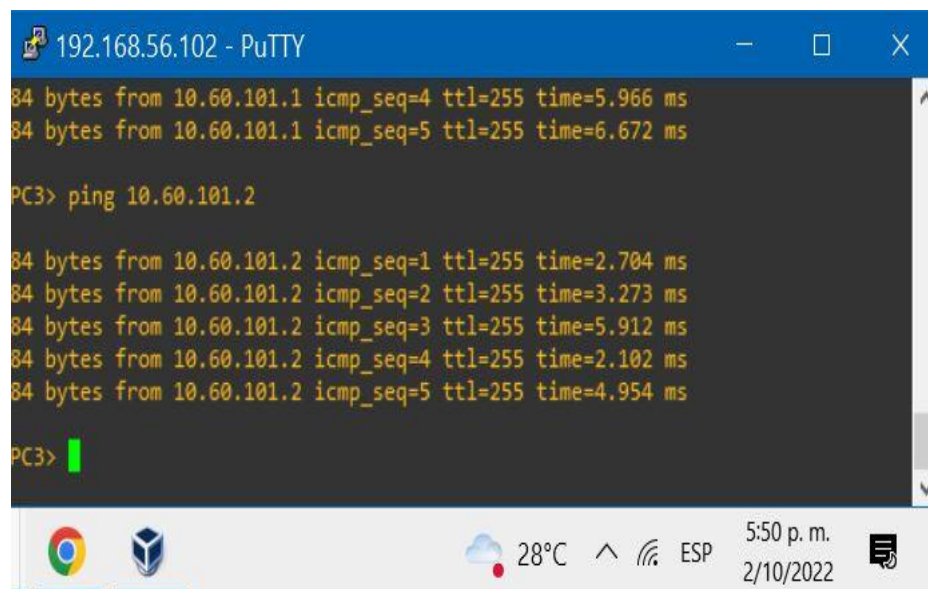
84 bytes from 10.60.101.1 icmp_seq=1 ttl=255 time=2.767 ms
84 bytes from 10.60.101.1 icmp_seq=2 ttl=255 time=3.230 ms
84 bytes from 10.60.101.1 icmp_seq=3 ttl=255 time=4.444 ms
84 bytes from 10.60.101.1 icmp_seq=4 ttl=255 time=5.966 ms
84 bytes from 10.60.101.1 icmp_seq=5 ttl=255 time=6.672 ms

PC3> |
```

The screenshot shows a terminal window with a dark background and yellow text. The command 'ping 10.60.101.1' has been executed, resulting in five successful replies. Each reply line shows '84 bytes from 10.60.101.1 icmp_seq=[number] ttl=255 time=[time] ms'. The times are 2.767, 3.230, 4.444, 5.966, and 6.672 ms. The prompt 'PC3>' is visible at the top and bottom of the terminal area. The Windows taskbar at the bottom shows the time as 5:49 p.m. on 2/10/2022, along with weather and network icons.

- D2: 10.60.101.2

Figura 12.



```
192.168.56.102 - PuTTY

84 bytes from 10.60.101.1 icmp_seq=4 ttl=255 time=5.966 ms
84 bytes from 10.60.101.1 icmp_seq=5 ttl=255 time=6.672 ms

PC3> ping 10.60.101.2

84 bytes from 10.60.101.2 icmp_seq=1 ttl=255 time=2.704 ms
84 bytes from 10.60.101.2 icmp_seq=2 ttl=255 time=3.273 ms
84 bytes from 10.60.101.2 icmp_seq=3 ttl=255 time=5.912 ms
84 bytes from 10.60.101.2 icmp_seq=4 ttl=255 time=2.102 ms
84 bytes from 10.60.101.2 icmp_seq=5 ttl=255 time=4.954 ms

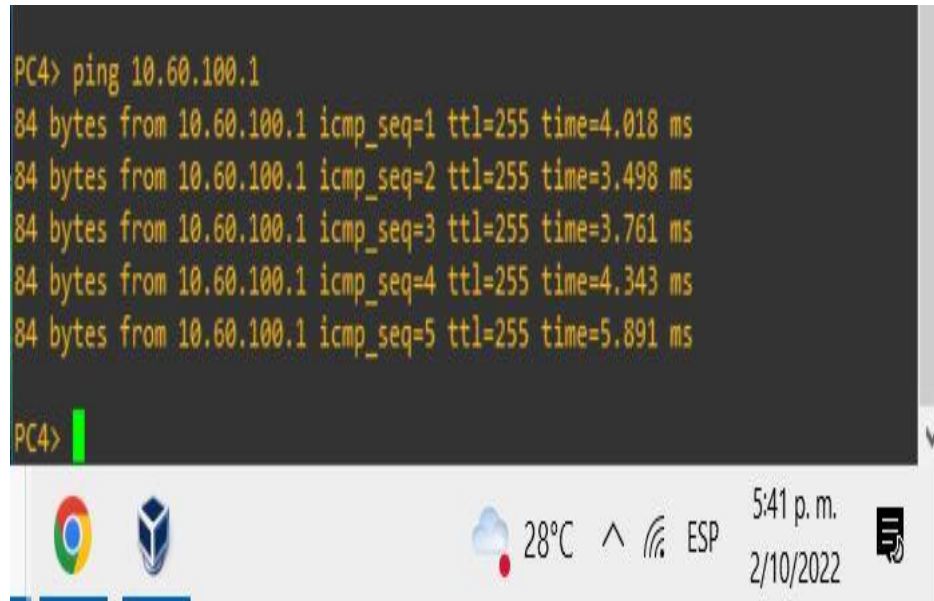
PC3> |
```

The screenshot shows a PuTTY terminal window with a blue title bar and a dark background with yellow text. The window title is '192.168.56.102 - PuTTY'. The terminal shows the results of a previous ping to 10.60.101.1 and a new ping to 10.60.101.2. The new ping command is 'ping 10.60.101.2', and it shows five successful replies with times of 2.704, 3.273, 5.912, 2.102, and 4.954 ms. The prompt 'PC3>' is visible at the top and bottom of the terminal area. The Windows taskbar at the bottom shows the time as 5:50 p.m. on 2/10/2022, along with weather and network icons.

PC4.

- D1: 10.60.100.1

Figura 13. Las figuras 13 y 14 muestran la evidencia de conexión entre PC4 y los dispositivos D1 y PC1 respectivamente.



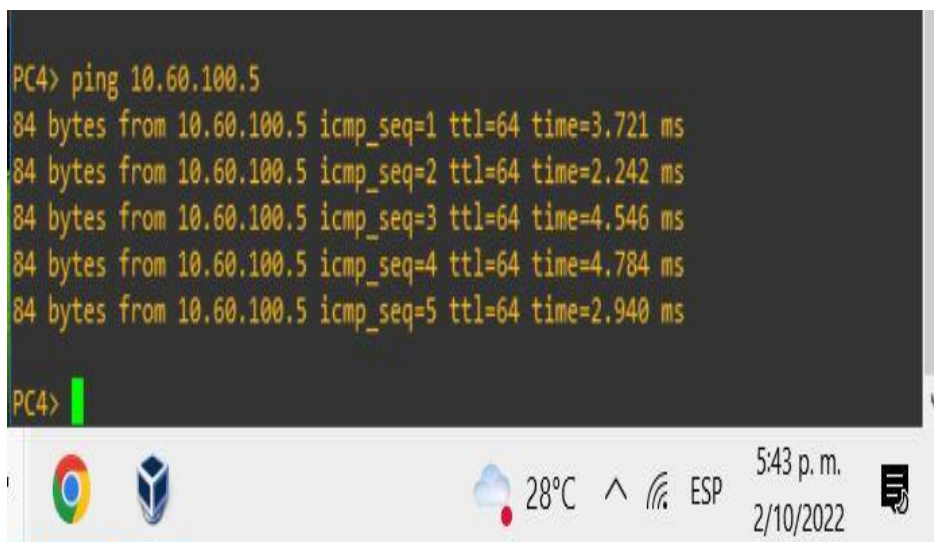
```
PC4> ping 10.60.100.1
84 bytes from 10.60.100.1 icmp_seq=1 ttl=255 time=4.018 ms
84 bytes from 10.60.100.1 icmp_seq=2 ttl=255 time=3.498 ms
84 bytes from 10.60.100.1 icmp_seq=3 ttl=255 time=3.761 ms
84 bytes from 10.60.100.1 icmp_seq=4 ttl=255 time=4.343 ms
84 bytes from 10.60.100.1 icmp_seq=5 ttl=255 time=5.891 ms

PC4>
```

The screenshot shows a Windows taskbar at the bottom with icons for Google Chrome and a university logo. The system tray displays a temperature of 28°C, network status, and the time 5:41 p.m. on 2/10/2022.

- PC1: 10.60.100.5

Figura 14.



```
PC4> ping 10.60.100.5
84 bytes from 10.60.100.5 icmp_seq=1 ttl=64 time=3.721 ms
84 bytes from 10.60.100.5 icmp_seq=2 ttl=64 time=2.242 ms
84 bytes from 10.60.100.5 icmp_seq=3 ttl=64 time=4.546 ms
84 bytes from 10.60.100.5 icmp_seq=4 ttl=64 time=4.784 ms
84 bytes from 10.60.100.5 icmp_seq=5 ttl=64 time=2.940 ms

PC4>
```

The screenshot shows a Windows taskbar at the bottom with icons for Google Chrome and a university logo. The system tray displays a temperature of 28°C, network status, and the time 5:43 p.m. on 2/10/2022.

6. Configurar protocolos de enrutamiento.

En esta parte, configurará los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debe estar completamente convergente. Los pings IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings de los hosts no tendrán éxito porque sus puertos de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Sus tareas de configuración se presentan en la tabla 12:

Tabla 12. Tareas de configuración.

Tarea #	Tarea	Especificaciones	Puntos
3.1	En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv2 de área única en el área 0.	<p>Utilice el ID de proceso OSPF 4 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 <p>En R1, R3, D1 y D2, anuncie todas las redes/VLAN conectadas directamente en el Área 0.</p> <ul style="list-style-type: none"> • En R1, no anuncie la red R1 – R2. • En el R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada. <p>Deshabilite los anuncios OSPFv2 en:</p> <ul style="list-style-type: none"> • D1: Todas las interfaces excepto E1/2 D2: Todas las interfaces excepto E1/0 	8
3.2	En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv3	<p>Utilice el ID de proceso OSPF 6 y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> • R1: 0.0.6.1 	8

	clásico de área única en el área 0.	<ul style="list-style-type: none"> • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 <p>En R1, R3, D1 y D2, anuncie todas las redes/VLAN conectadas directamente en el Área 0.</p> <ul style="list-style-type: none"> • En R1, no anuncie la red R1 – R2. • En el R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada. <p>Deshabilite los anuncios OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: Todas las interfaces excepto E1/2 D2: Todas las interfaces excepto E1/0 	
3.3	En R2 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use la identificación del enrutador 2.2.2.2.</p> <p>Configure y habilite una relación de vecino ipv4 e ipv6 con R1 en ASN 300.</p> <p>En la familia de direcciones IPv4, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). 	4

		<p>En la familia de direcciones IPv6, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0). 	
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas resumidas estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • Una ruta IPv4 resumida para 10.60.0.0/8. • Un resumen de la ruta IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y use la identificación del enrutador 1.1.1.1.</p> <p>Configure una relación de vecino Ipv4 e Ipv6 con R2 en ASN 500.</p> <p>En la familia de direcciones IPv4:</p> <ul style="list-style-type: none"> • Deshabilitar la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.60.0.0/8. <p>En la familia de direcciones IPv6:</p> <ul style="list-style-type: none"> • Deshabilitar la relación de vecino IPv4. • Habilite la relación de vecino IPv6. <p>Anuncie la red 2001:db8:100::/48.</p>	4

6.1 Código en los diferentes dispositivos con base en las especificaciones dadas en la tabla 12.

Router R1

En la tabla 13 se presenta la secuencia de configuración de OSPF para ipv6 en el router R1.

Tabla 13. Código configuración para el router R1.

```
router ospf 4
router-id 0.0.4.1
network 10.60.10.0 0.0.0.255 area 0
network 10.60.13.0 0.0.0.255 area 0
default-information originate
exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface e1/2
ipv6 ospf 6 area 0
exit
interface e1/1
ipv6 ospf 6 area 0
exit
!ip route 10.60.0.0 255.0.0.0 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 10.60.0.0 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
```

Router R2.

En la tabla 14 se presenta la secuencia de configuración del protocolo BGP e ipv6 para el sistema autónomo 500 para el router R2.

Tabla 14. Código de configuración para el sistema autónomo 500 en el 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
```

Router R3.

En la tabla 15 se presenta la secuencia de configuración de OSPF para el router R3.

Tabla 15. Configuración OSPF para el router R3.

```
router ospf 4
router-id 0.0.4.3
network 10.60.11.0 0.0.0.255 area 0
network 10.60.13.0 0.0.0.255 area 0
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface e1/1
ipv6 ospf 6 area 0
exit
end
```

En la tabla 16 se presenta la secuencia de configuración de OSPF para el switch D1.

Tabla 16. Configuración de OSPF para el switch D1.

```
router ospf 4
router-id 0.0.4.131
network 10.60.100.0 0.0.0.255 area 0
network 10.60.101.0 0.0.0.255 area 0
network 10.60.102.0 0.0.0.255 area 0
network 10.60.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/2
exit
router ospf 6
router-id 0.0.6.131
```

```
passive-interface default
no passive-interface e1/2
exit
interface e1/2
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

En la tabla 17 se presenta la secuencia de configuración de OSPF para el switch D2.

Tabla 17. Configuración de OSPF para el switch D2.

```
router ospf 4
router-id 0.0.4.132
network 10.60.100.0 0.0.0.255 area 0
network 10.60.101.0 0.0.0.255 area 0
network 10.60.102.0 0.0.0.255 area 0
network 10.60.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/0
exit
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
```

6.2 Verificación de configuración en los dispositivos R1, R3, D1 y D2 de acuerdo con las especificaciones de la tabla 12.

Router R1.

En la figura 15 se observa que el protocolo OSPF está correctamente configurado en el router R1.

Figura 15.



```
R1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.1
  network 10.60.10.0 0.0.0.255 area 0
  network 10.60.13.0 0.0.0.255 area 0
  default-information originate
R1#
```

Router R3.

En la figura 16 se observa que el protocolo OSPF está correctamente configurado en el router R3.

Figura 16.

```
R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  network 10.60.11.0 0.0.0.255 area 0
  network 10.60.13.0 0.0.0.255 area 0
R3#
```



Switch D1.

En la figura 17 se observa que el protocolo OSPF está correctamente configurado en el switch D1.

Figura 17.

```
D1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.131
  passive-interface default
  no passive-interface Ethernet1/2
  network 10.60.10.0 0.0.0.255 area 0
  network 10.60.100.0 0.0.0.255 area 0
  network 10.60.101.0 0.0.0.255 area 0
  network 10.60.102.0 0.0.0.255 area 0
router ospf 6
  router-id 0.0.6.131
  passive-interface default
  no passive-interface Ethernet1/2
D1#
```



Switch D2.

En la figura 18 se observa que el protocolo OSPF está correctamente configurado en el switch D2.

Figura 18

```
D2#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.132
  passive-interface default
  no passive-interface Ethernet1/0
  network 10.60.11.0 0.0.0.255 area 0
  network 10.60.100.0 0.0.0.255 area 0
  network 10.60.101.0 0.0.0.255 area 0
  network 10.60.102.0 0.0.0.255 area 0
router ospf 6
  router-id 0.0.6.132
  passive-interface default
  no passive-interface Ethernet1/0
D2#
```



6.3 Verificación de configuración de la interfaz ipv6 OSPF en R1, R3, D1 y D2 de acuerdo con las especificaciones dadas en la tabla 12.

Router R1.

En la figura 19 se observa la interfaz ipv6 OSPF configurada en el router R1.

Figura 19.

```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  default-information originate
R1#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID  Cost  State Nbrs F/C
Et1/1     6   0             5        10   DR    1/1
Et1/2     6   0             6        10   DR    1/1
R1#
```

Router R3.

En la figura 20 se observa la interfaz ipv6 OSPF configurada en el router R3.

Figura 20.

```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
R3#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID  Cost  State Nbrs F/C
Et1/1     6   0             5        10   BDR   1/1
Et1/0     6   0             4        10   DR    0/0
R3#
```

Switch D1.

En la figura 21 se observa la interfaz ipv6 OSPF configurada en el switch D1.

Figura 21.

```
D1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.131
  passive-interface default
  no passive-interface Ethernet1/2
D1#show ipv6 ospf interface brief
Interface  PID  Area          Intf ID  Cost  State Nbrs F/C
Vl102     6   0             29         1   DR    0/0
Vl101     6   0             28         1   DR    0/0
Vl100     6   0             27         1   DR    0/0
Et1/2     6   0             25        10   BDR   1/1
D1#
```

Switch D2.

En la figura 22 se observa la interfaz ipv6 OSPF configurada en el switch D2.

Figura 22.

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.132
  passive-interface Ethernet1/0
D2#show ipv6 ospf interface brief
Interface      PID  Area      Intf ID   Cost  State  Nbrs F/C
Vl102          6    0         48        1    DR    0/0
Vl101          6    0         47        1    DR    0/0
Vl100          6    0         46        1    DR    0/0
Et1/0          6    0         44        10   DR    0/0
D2#
```



6.4 Verificación de configuración del protocolo BGP en el sistema autónomo 500 con base en las especificaciones dadas en la tabla 12.

Router R2.

En las figuras 23 y 24 se observa la correcta configuración del protocolo BGP en el router R2.

Figura 23.

```
R2#show run | section router bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.225 remote-as 300
  !
  address-family ipv4
    network 0.0.0.0
    network 2.2.2.2 mask 255.255.255.255
    no neighbor 2001:DB8:200::1 activate
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network ::/0
    network 2001:DB8:2222::/128
    neighbor 2001:DB8:200::1 activate
  exit-address-family
R2#
```

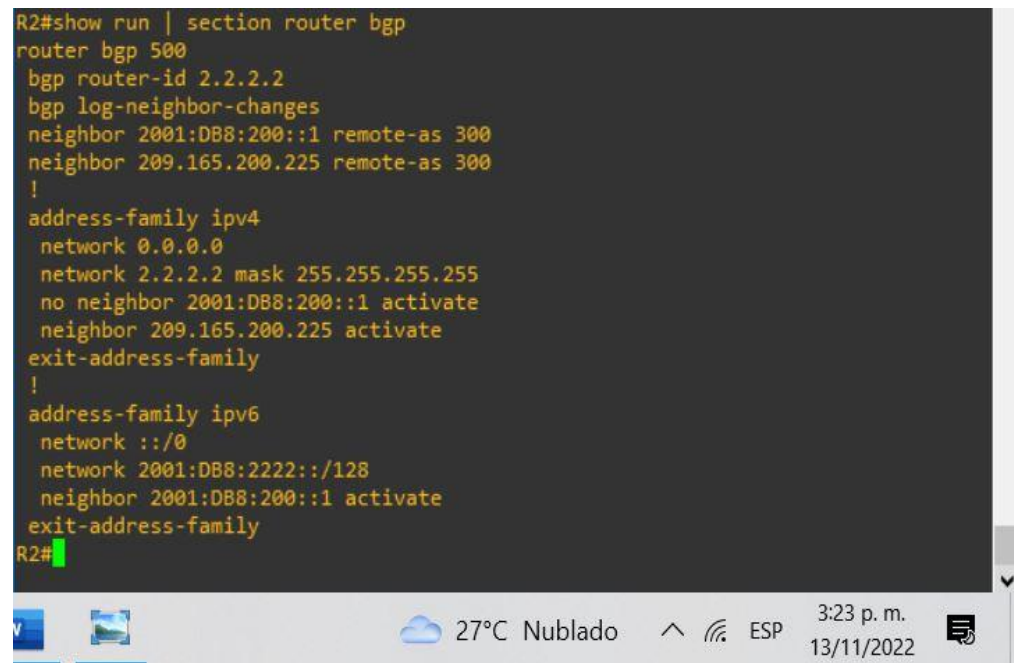
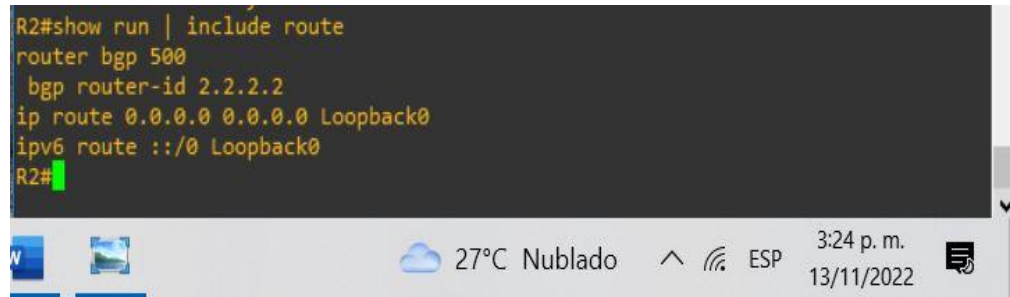


Figura 24.

```
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
R2#
```



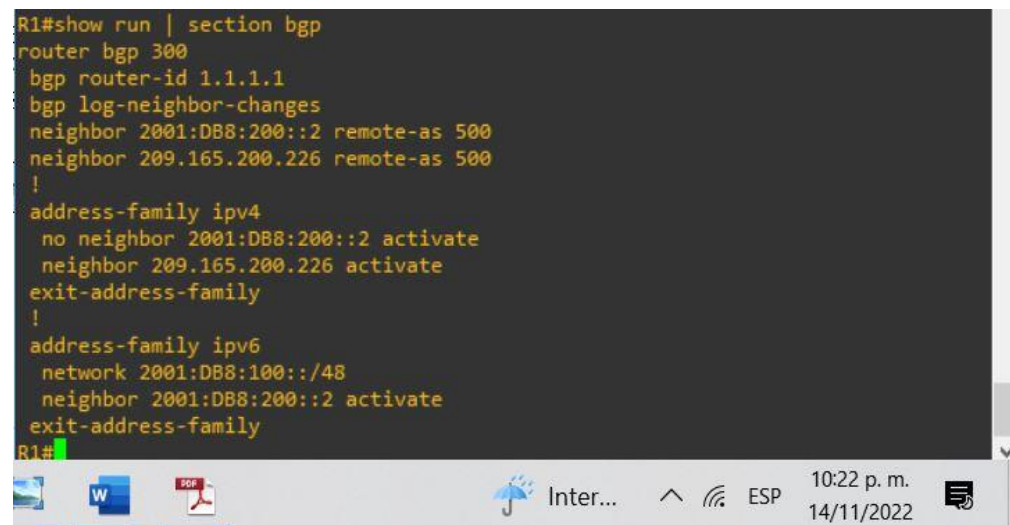
6.5 Verificación de configuración del protocolo BGP en el sistema autónomo 300 con base en las especificaciones dadas en la tabla 12.

Router R1.

En la figura 25 se observa la correcta configuración en el router R1 del protocolo BGP

Figura 25.

```
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
    neighbor 2001:DB8:200::2 activate
  exit-address-family
R1#
```



6.6 Verificación de las tablas de enrutamiento en el router R1 con base en las especificaciones dadas en la tabla 12.

Router R1.

En la figura 26 se observa que OSPF y BGP trabajan correctamente para ipv4.

Figura 26.

```
R1#show ip route | include O|B
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
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
B*    0.0.0.0/0 [20/0] via 209.165.200.226, 06:40:54
B     2.2.2.2 [20/0] via 209.165.200.226, 07:36:16
O     10.60.11.0/24 [110/20] via 10.60.13.3, 07:49:01, Ethernet1/1
O     10.60.100.0/24 [110/11] via 10.60.10.2, 05:42:11, Ethernet1/2
O     10.60.101.0/24 [110/11] via 10.60.10.2, 05:42:11, Ethernet1/2
O     10.60.102.0/24 [110/11] via 10.60.10.2, 05:42:11, Ethernet1/2
R1#
```

6.7 Verificación de configuración del protocolo OSPF funcione apropiadamente en ipv6 en el router R1.

Router R1.

En la figura 27 se observa la forma como está configurada la tabla de enrutamiento para ipv6 en el router R1.

Figura 27.

```
R1#show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       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, I - LISP
B    ::0 [20/0]
S    2001:DB8:100::/48 [1/0]
O    2001:DB8:100:100::/64 [110/11]
O    2001:DB8:100:101::/64 [110/11]
O    2001:DB8:100:102::/64 [110/11]
C    2001:DB8:100:1010::/64 [0/0]
L    2001:DB8:100:1010::1/128 [0/0]
O    2001:DB8:100:1011::/64 [110/20]
C    2001:DB8:100:1013::/64 [0/0]
L    2001:DB8:100:1013::1/128 [0/0]
C    2001:DB8:200::/64 [0/0]
L    2001:DB8:200::1/128 [0/0]
L    FF00::/8 [0/0]
```

6.8 Verificación de configuración del protocolo OSPF funcione apropiadamente en ipv6 en el router R3.

Router R3.

En la figura 28 se observa la forma como está configurada la tabla de enrutamiento para ipv6 en el router R3.

Figura 28.

```

R3#show ipv6 route ospf
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
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, I - LISP
OE2 ::0 [110/1], tag 6
    via FE80::1:3, Ethernet1/1
O  2001:DB8:100:100::/64 [110/21]
    via FE80::1:3, Ethernet1/1
O  2001:DB8:100:101::/64 [110/21]
    via FE80::1:3, Ethernet1/1
O  2001:DB8:100:102::/64 [110/21]
    via FE80::1:3, Ethernet1/1
O  2001:DB8:100:1013::/64 [110/10]
    via Ethernet1/1, directly connected
R3#
  
```

7. Configurar la redundancia del primer salto.

En esta parte, configurará la versión 2 de HSRP para proporcionar redundancia de primer salto para los hosts en la "Red de la empresa".

Sus tareas de configuración se presentan en la tabla 18:

Tabla 18. Tareas de configuración HSRP.

Tarea#	Tarea	Especificaciones	Puntos
4.1	En D1, cree IP SLA que prueben la accesibilidad de la interfaz E1/2 de R1.	<p>Cree dos IP SLA.</p> <ul style="list-style-type: none"> • Utilice el SLA número 4 para Ipv4. • Utilice el SLA número 6 para IPv6. <p>Los IP SLA probarán la disponibilidad de la interfaz R1 E1/2 cada 5 segundos.</p> <p>Programa el SLA para implementación inmediata sin tiempo de finalización.</p> <p>Cree un objeto IP SLA para IP SLA 4 y otro para IP SLA 6.</p> <ul style="list-style-type: none"> • Use la pista número 4 para IP SLA 4. • Use la pista número 6 para IP SLA 6. 	2

		Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de abajo a arriba después de 10 segundos, o de arriba a abajo después de 15 segundos.	
4.2	En D2, cree IP SLA que prueben la accesibilidad de la interfaz E1/0 de R3.	<p>Cree dos IP SLA.</p> <ul style="list-style-type: none"> • Utilice el SLA número 4 para Ipv4. • Utilice el SLA número 6 para IPv6. <p>Los IP SLA probarán la disponibilidad de la interfaz R3 E1/0 cada 5 segundos.</p> <p>Programa el SLA para implementación inmediata sin tiempo de finalización.</p> <p>Cree un objeto IP SLA para IP SLA 4 y otro para IP SLA 6.</p> <ul style="list-style-type: none"> • Use la pista número 4 para IP SLA 4. • Use la pista número 6 para IP SLA 6. <p>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.</p>	2
4.3	En D1, configure HSRPv2.	<p>D1 es el enrutador principal para las VLAN 100 y 102; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure la versión 2 de HSRP.</p> <p>Configure el grupo Ipv4 HSRP 104 para VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.60.100.254. • Establezca la prioridad del grupo en 150. • Habilitar preferencia. • Siga el objeto 4 y disminuya en 60. <p>Configure el grupo 114 de IPv4 HSRP para la VLAN 101:</p>	8

		<ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.60.101.254. • Habilitar preferencia. • Seguimiento del objeto 4 para disminuir en 60. <p>Configure el grupo 124 de IPv4 HSRP para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.60.102.254. • Establezca la prioridad del grupo en 150. • Habilitar preferencia. • Seguimiento del objeto 4 para disminuir en 60. <p>Configure el grupo 106 de IPv6 HSRP para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne 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. <p>Configure el grupo 116 de IPv6 HSRP para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual mediante la configuración automática de ipv6. • Habilitar preferencia. • Siga el objeto 6 y disminuya en 60. <p>Configure el grupo 126 de IPv6 HSRP para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne 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.	
--	--	-------------------------------------	--

7.1 Configuración de dispositivos con base en especificaciones dadas en la tabla 18.

Switch D1.

En la tabla 19 se presenta el código de configuración en donde se crean las IP SLA para ipv4 e ipv6 y haciendo el switch D1 como el enrutador principal.

Tabla 19. Configuración del ICMP en el switch D1.

```

ip sla 4
icmp-echo 10.60.10.1
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
interface vlan 100
standby version 2
standby 104 ip 10.60.100.254
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 10.60.101.254
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 10.60.102.254
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
```

Switch D2.

En la tabla 20 se presenta el código de configuración en donde se crean las IP SLA para ipv4 e ipv6 en el switch D2.

Tabla 20. Configuración del ICMP en el switch D2.

```
ip sla 4
icmp-echo 10.60.11.1
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
interface vlan 100
standby version 2
standby 104 ip 10.60.100.254
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 10.60.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
```

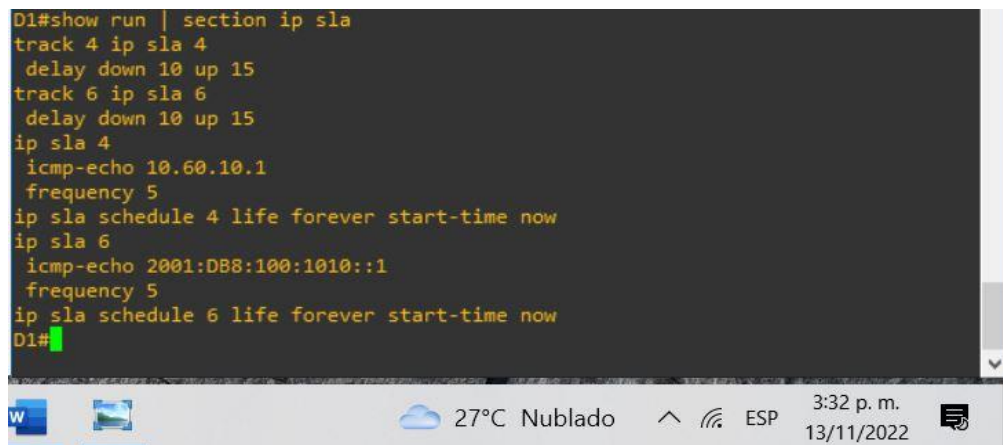
```
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.60.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

7.2 Verificación de la configuración de los dispositivos D1 y D2 con base en las especificaciones dadas en la tabla 18.

Switch D1.

En la figura 29 se observa la ejecución del comando *show run | section ip sla* en el switch D1, el cual nos muestra el estado de configuración.

Figura 29.

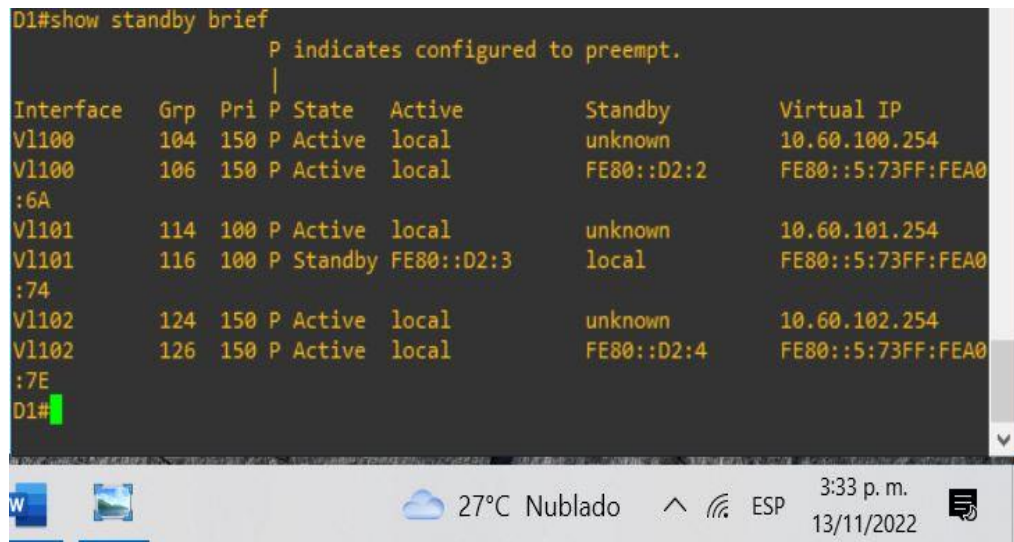


```
D1#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.60.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

En la figura 30 se observa la ejecución del comando *show standby brief* en el switch D1, el cual nos presenta la configuración de prioridades respecto al switch D1.

Figura 30.

```
D1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri  P State  Active          Standby          Virtual IP
Vl100     104  150  P Active local          unknown         10.60.100.254
Vl100     106  150  P Active local          FE80::D2:2      FE80::5:73FF:FEA0
:6A
Vl101     114  100  P Active local          unknown         10.60.101.254
Vl101     116  100  P Standby FE80::D2:3      local           FE80::5:73FF:FEA0
:74
Vl102     124  150  P Active local          unknown         10.60.102.254
Vl102     126  150  P Active local          FE80::D2:4      FE80::5:73FF:FEA0
:7E
D1#
```

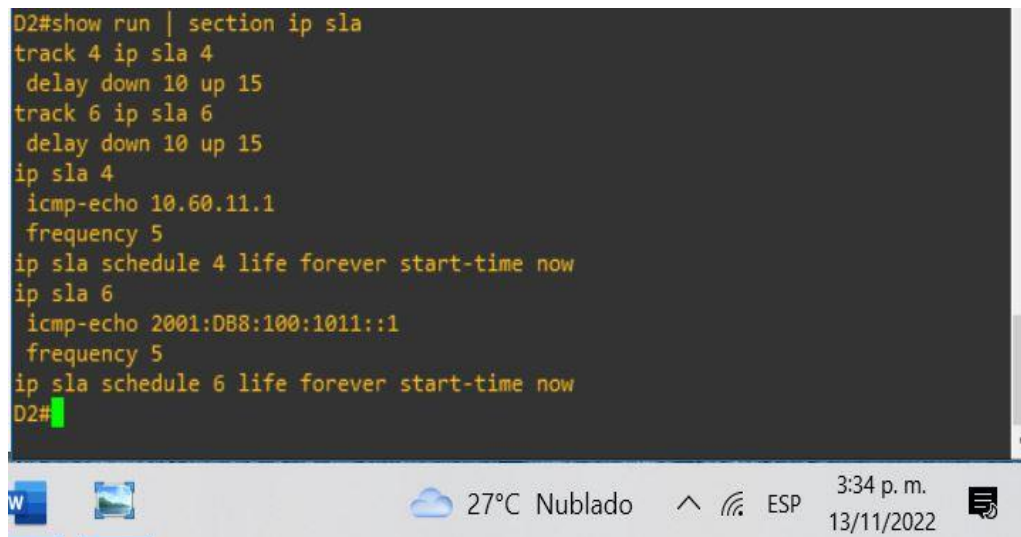


Switch D2.

En la figura 31 se observa la ejecución del comando show standby brief en el switch D1, el cual nos presenta la configuración de prioridades respecto al switch D2.

Figura 31.

```
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.60.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
D2#
```



CONCLUSIONES

La utilización del programa GNS3 requiere de experiencia ya que se presentó mucha dificultad en lo que se refiere a las imágenes de cada dispositivo de modo que si no se utiliza la imagen correcta tendrá serias dificultades para su configuración, también otro punto que hace dificultoso la utilización de GNS3 es que requiere la utilización de una máquina virtual para que funcione de modo que si la PC no posee buenas características de hardware tendrá más dificultad en la ejecución de otros programas necesarios y al mismo tiempo el programa GNS3 se bloqueará de modo que la única solución será cerrarlo y reiniciarlo nuevamente lo cual quita tiempo y concentración en la realización del trabajo.

Respecto a la instalación al principio de cada imagen presentaba error al instalar, también se presentó dificultad en probar la comunicación realizando un ping desde la PC1 a D2 en el punto 4 ya que no lograba comunicación de modo que reinició el equipo y al parecer funcionó, otro problema que se presentó fue durante la configuración de la dirección *!ip route 10.60.0.0 255.0.0.0 null0* del protocolo OSPF en ipv6 en el router R1 en el punto 6.1, en donde el dispositivo no recibía el comando ni la dirección ingresada de modo que investigando le adicioné el carácter "!" y funcionó, debido a estos problemas presentados se requirió de consultar ejemplos con topologías y conexiones similares para resolver estos problemas.

En general durante la realización de este diplomado se profundizaron en los conceptos de protocolos como OSPF, EIGRP, BGP, direccionamiento ipv4 e ipv6, VLAN's, enlaces troncales, Spanning tree, configuración de cuentas de usuario entre otros conceptos y también se afianzaron los conocimientos en cuanto a la configuración de dispositivos de redes con topologías complejas y de solución problemas en una infraestructura tecnológica dada.

Se adquirieron habilidades específicas como son planear, implementar, mantener, asegurar y solucionar problemas relacionados con redes orientadas a un entorno profesional y corporativo.

BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCORA 350-401.

<https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCORA 350-401.

<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 ENCORA 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 ENCORA 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 ENCORA 350-401.

<https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). BGP. CCNP and CCIE Enterprise Core ENCORA 350-401.

<https://1drv.ms/b/s!AAIGg5JUgUBthk8>