

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

CARLOS ANDRES GONZALEZ RAMIREZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
IBAGUÉ
2022**

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

CARLOS ANDRES GONZALEZ RAMIREZ

**Diplomado de opción de grado presentado para optar el título de INGENIERO
EN ELECTRÓNICA**

**DIRECTOR:
Msc. HÉCTOR JULIÁN PARRA MOGOLLÓN**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA ELECTRÓNICA
IBAGUÉ
2022**

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Ibagué, 27 de Noviembre de 2022

AGRADECIMIENTOS

Quiero expresar mi gratitud primeramente a Dios por ser mi guía, apoyo, fortaleza y sustento en este proceso de formación académica, pero sobre todo en cada paso de mi vida.

A mi madre y a mi padre que con su esfuerzo, amor, dedicación, consejos y confianza me han dado fuerza para alcanzar tan anhelada meta.

A mi director de trabajo de grado Juan Esteban Tapias Baena por su paciencia y dedicación.

A los docentes de la Universidad Nacional Abierta y a Distancia UNAD, por haberme formado a lo largo de mi carrera profesional.

Y por último a todas y cada una de las personas que de una u otra manera aportaron su granito de arena para que pudiera culminar esta meta.

CONTENIDO

	Pág.
RESUMEN.....	9
ABSTRACT	9
INTRODUCCIÓN	10
DESARROLLO.....	11
ESCENARIO.....	11
PARTE 1: CONSTRUCCIÓN Y CONFIGURACION BASICA DE LA RED	12
PARTE 3: CONFIGURACION DE LA RED DE CAPA 2 Y LA COMPATIBILIDAD CON LOS HOSTS	21
PARTE 3: CONFIGURACION DE LOS PROTOCOLOS DE ENRUTAMIENTO...30	
PARTE 4: CONFIGURACION DE LA REDUNDANCIA DEL PRIMER SALTO....37	
CONCLUSIONES	45
REFERENCIAS	46

LISTA DE FIGURAS

	Pág.
Figura 1. Escenario.....	11
Figura 2 Configuración física de los Routers	12
Figura 3. Configuración física de los Switches.....	13
Figura 4. Simulación del escenario	13
Figura 5. Guardando las configuraciones en R1	19
Figura 6. Guardando las configuraciones en R2.....	19
Figura 7. Guardando las configuraciones en R3.....	20
Figura 8. Guardando las configuraciones en D1	20
Figura 9. Guardando las configuraciones en D2.....	20
Figura 10. Guardando las configuraciones en A1	20
Figura 11. Asignación de direccionamiento IPv4 e IPv6 a PC1.	21
Figura 12. Asignación de direccionamiento IPv4 e IPv6 a PC4.	21
Figura 13. Verificación de RSTP en D1	23
Figura 14. Verificación de RSTP en D2	24
Figura 15. Verificación de los puertos Etherchannel en D1	26
Figura 16. Verificación de los puertos Etherchannel en D2	26
Figura 17. Verificación de los puertos Etherchannel en A1	27
Figura 18. Verificación del protocolo DHCP en PC2.....	28
Figura 19. Verificación del protocolo DHCP en PC3.....	28
Figura 20. Verificación de conexión desde PC1	29
Figura 21. Verificación de conexión desde PC2	29
Figura 22. Verificación de conexión desde PC3	30
Figura 23. Verificación de conexión desde PC4	30
Figura 24. Verificación de la configuración OSPF en R1	34
Figura 25. Verificación de la configuración OSPF en R3	34
Figura 26. Verificación de la configuración OSPF en D1	34
Figura 27. Verificación de la configuración OSPF en D2	35
Figura 28. Verificación de la configuración BGP en R1	37
Figura 29. Verificación de la configuración BGP en R2	37
Figura 30. Verificación de la configuración IP SLA en D1	39
Figura 31. Verificación de la configuración IP SLA en D2.....	40
Figura 32. Verificación de HSRP en D1	43
Figura 33. Verificación de HSRP en D2.....	44

LISTA DE TABLAS

	Pág.
Tabla 1. Tabla de direccionamiento.....	11

GLOSARIO

BGP: Es el protocolo que hace que Internet funcione permitiendo el enrutamiento de datos.

DHCP: Es un protocolo de red que utiliza una arquitectura cliente-servidor. Por tanto, tendremos uno o varios servidores DHCP y también uno o varios clientes, que se deberán comunicar entre ellos correctamente para que el servidor DHCP brinde información a los diferentes clientes conectados.

GNS3: Es un simulador gráfico de red, que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

HSRP: (Hot Stand-by Redundancy Protocol) es un protocolo de capa 3, propietario de Cisco, que proporciona redundancia a nivel de gateway.

IPV4: Utiliza direcciones de 32 bits con hasta 12 caracteres en cuatro bloques de tres caracteres cada uno, como 212.227.142.131.

IPV6: Tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPV4.

OSPF: Protocolo de routing de estado de enlace que se implementa con frecuencia y se desarrolló como un reemplazo para el protocolo de routing vector distancia RIP.

PROTOSCOLOS DE ENRUTAMIENTO: Los protocolos administran la actividad de enrutamiento en un sistema. Los enrutadores intercambiar información de enrutamiento con otros hosts para mantener las rutas conocidas a las redes remotas.

SLA: Permite a los enrutadores y conmutadores de Cisco realizar diversas pruebas de red mediante el intercambio de datos simulados con otros dispositivos de Cisco ("respondedores") o servidores de red comunes.

VLAN: (redes de área local virtuales) pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas.

RESUMEN

El presente escenario tuvo como finalidad la realización de la construcción y configuración de una red, teniendo en cuenta que la red al final tiene accesibilidad completa de extremo a extremo.

Para llevar a cabo dicha configuración se basó en cuatro partes, como primera instancia la construcción y configuración de los ajustes básicos de cada uno de los dispositivos que conforman la red junto con la asignación del direccionamiento de cada interfaz; en segunda medida se configura la capa 2 de la red y la compatibilidad con el host; en la tercera parte se configuran los protocolos de enrutamiento y por último en la fase cuatro se configura el protocolo de redundancia de primer salto, garantizando la integridad y seguridad de la red.

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

ABSTRACT

The purpose of this scenario was to carry out the construction and configuration of a network, taking into account that the network ultimately has complete end-to-end accessibility.

To carry out this configuration, it was based on four parts, as a first instance the construction and configuration of the basic settings of each of the devices that make up the network together with the address assignment of each interface; secondly, layer 2 of the network and compatibility with the host are configured; in the third part the routing protocols are configured and finally in phase four the first hop redundancy protocol is configured, guaranteeing the integrity and security of the network.

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

INTRODUCCIÓN

El presente trabajo está basado en la construcción y configuración de una red para que haya accesibilidad completa de extremo a extremo, para que los hosts tengan soporte confiable y para que los protocolos de administración sean operativos dentro de la red de la empresa.

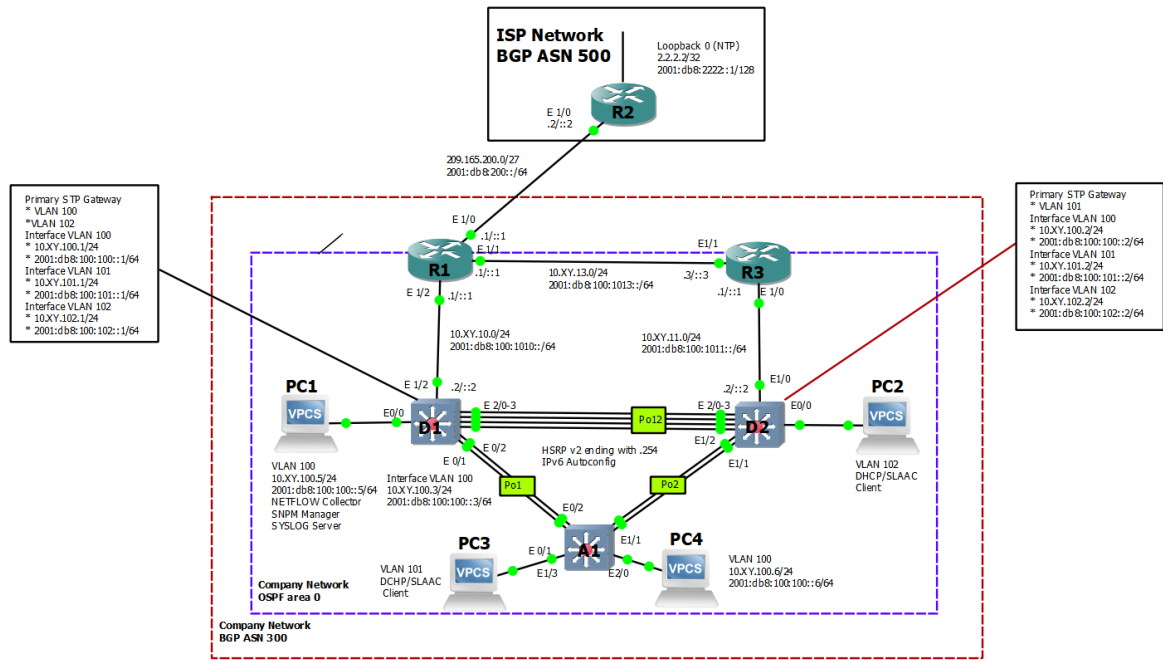
La característica principal de esta red es que a diferencia de la mayoría de redes, su diseño es completo al incluir configuraciones detalladas de los protocolos OSPF y BGP entre otros; además se fortalecen los conocimientos adquiridos utilizando el software GNS3 para la respectiva simulación.

A causa de que en esta época las redes de comunicaciones deben estar en la capacidad de responder a todas las constantes necesidades de sus clientes, se ve en esto una oportunidad para construir y configurar una red empresarial LAN y WAN, cumpliendo con el objetivo de asegurar la conexión, calidad y la seguridad de la misma.

DESARROLLO

ESCENARIO

Figura 1. Escenario.



Fuente: Guía Prueba de habilidades prácticas CCNP

Tabla 1. Tabla de direccionamiento.

Dispositivo	Interfaz	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	10.62.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10.62.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10.62.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.62.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10.62.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN100	10.62.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN101	10.62.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN102	10.62.102.1/24	2001:db8:100:102::1/64	fe80::d1:4

D2	E1/0	10.62.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN100	10.62.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN101	10.62.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN102	10.62.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.62.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.62.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.62.100.6/24	2001:db8:100:100::6/64	EUI-64

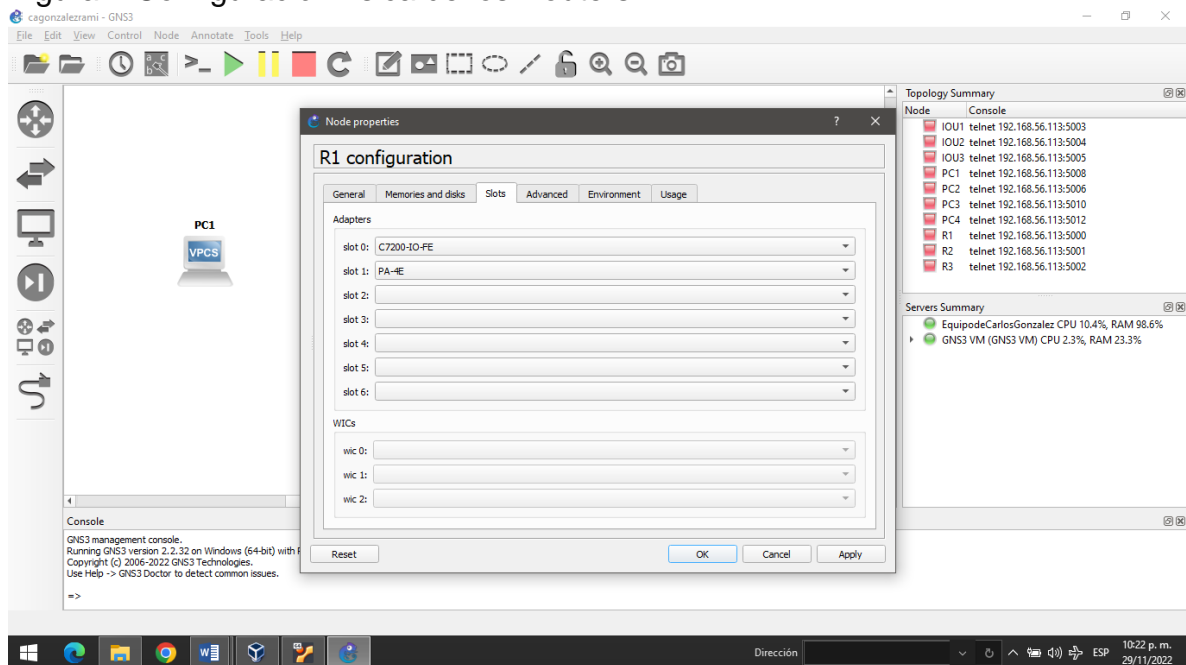
Fuente: Guía Prueba de habilidades prácticas CCNP

La configuración de la red empresarial, se lleva a cabo por medio de las cuatro partes con su respectiva verificación de configuración y de conexión que se detallan a continuación:

PARTE 1: CONSTRUCCIÓN Y CONFIGURACION BASICA DE LA RED

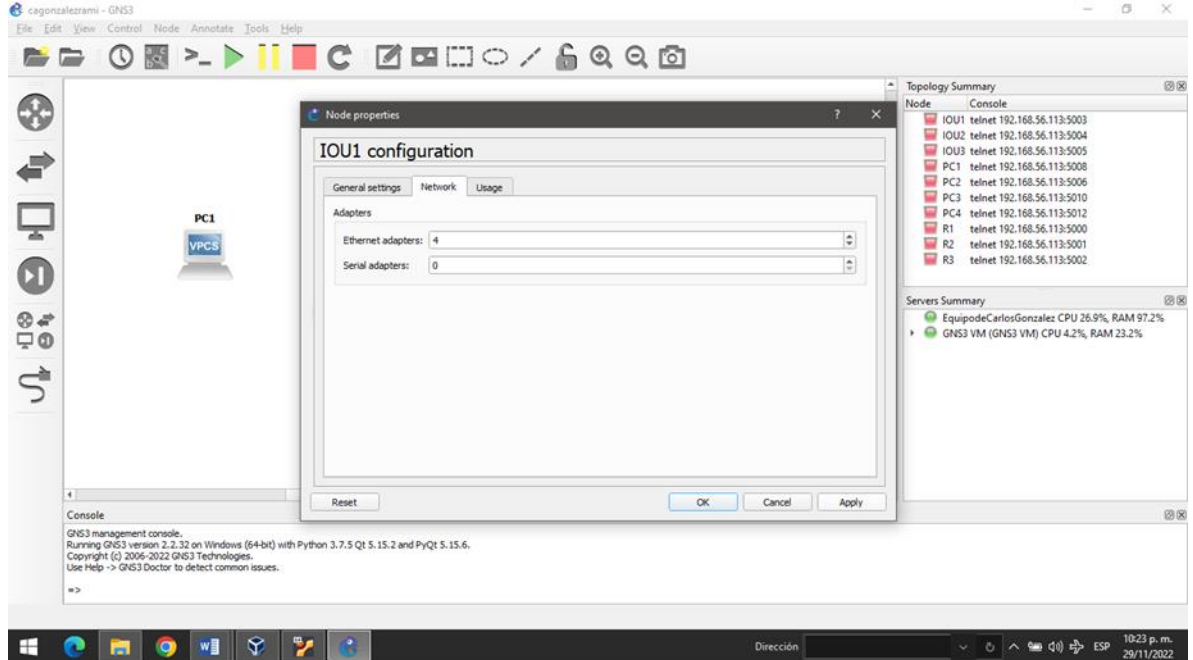
Este escenario se elabora en el simulador grafico GNS3, se crea la topología de red agregando a la pantalla principal tres routers (Cisco 7200), tres switches (Cisco IOU L2) y cuatro PC (VPCS), todos los dispositivos se conectan a través de cables Ethernet y se continúa con la configuración de los Slots de los adaptadores de red del SW.

Figura 2 Configuración física de los Routers



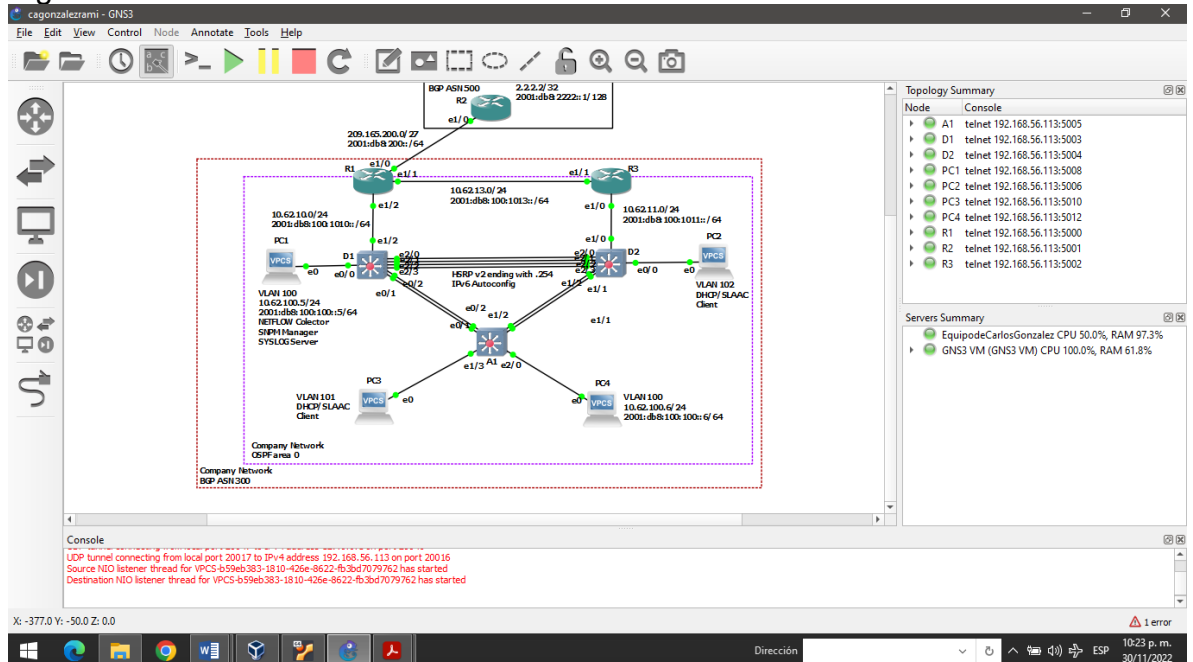
Fuente: Propia

Figura 3. Configuración física de los Switches



Fuente: Propia

Figura 4. Simulación del escenario



Fuente: Autoría propia

Se realizan las configuraciones de los Routers, Switches y PCs atendiendo las tareas establecidas del escenario. Los ajustes se realizan en modo de configuración global por medio del comando configure terminal. A partir de lo anterior se inicia aplicando los siguientes comandos que permiten realizar las configuraciones básicas y a la asignación de la dirección de cada interfaz que compone a los dispositivos:

Router R1

```
#hostname R1
#ipv6 unicast-routing
#no ip domain lookup
#banner motd # R1, ENCOR Skills Assessment#
#line con 0
#exec-timeout 0 0
#logging synchronous
#exit
#interface e1/0
#ip address 209.165.200.225 255.255.255.224
#ipv6 address fe80::1:1 link-local
#ipv6 address 2001:db8:200::1/64
#no shutdown
#exit
#interface e1/2
#ip address 10.62.10.1 255.255.255.0
#ipv6 address fe80::1:2 link-local
#ipv6 address 2001:db8:100:1010::1/64
#no shutdown
#exit
#interface e1/1
#ip address 10.62.13.1 255.255.255.0
#ipv6 address fe80::1:3 link-local
#ipv6 address 2001:db8:100:1013::1/64
#no shutdown
#exit
```

Router R2

```
#hostname R2
#ipv6 unicast-routing
#no ip domain lookup
#banner motd # R2, ENCOR Skills Assessment#
#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

```
#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 10.62.11.1 255.255.255.0
#ipv6 address fe80::3:2 link-local
#ipv6 address 2001:db8:100:1011::1/64
#no shutdown
#exit
#interface e1/1
#ip address 10.62.13.3 255.255.255.0
#ipv6 address fe80::3:3 link-local
#ipv6 address 2001:db8:100:1010::2/64
#no shutdown
#exit
```

Switch D1

```
#hostname D1
#ip routing
#ipv6 unicast-routing
#no ip domain lookup
#banner motd # D1, ENCOR Skills Assessment#
#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 10.62.10.2 255.255.255.0
#ipv6 address fe80::d1:1 link-local
#ipv6 address 2001:db8:100:1010::2/64
#no shutdown
#exit
#interface vlan 100
#ip address 10.62.100.1 255.255.255.0
#ipv6 address fe80::d1:2 link-local
#ipv6 address 2001:db8:100:100::1/64
#no shutdown
#exit
#interface vlan 101
#ip address 10.62.101.1 255.255.255.0
#ipv6 address fe80::d1:3 link-local
#ipv6 address 2001:db8:100:101::1/64
#no shutdown
#exit
#interface vlan 102
#ip address 10.62.102.1 255.255.255.0
#ipv6 address fe80::d1:4 link-local
#ipv6 address 2001:db8:100:102::1/64
#no shutdown
#exit
#ip dhcp excluded-address 10.62.101.1 10.62.101.109
#ip dhcp excluded-address 10.62.101.141 10.62.101.254
#ip dhcp excluded-address 10.62.102.1 10.62.102.109
#ip dhcp excluded-address 10.62.102.141 10.62.102.254
#ip dhcp pool VLAN-101
#network 10.62.101.0 255.255.255.0
#default-router 10.62.101.254
```



```
#exit
#ip dhcp pool VLAN-102
#network 10.62.102.0 255.255.255.0
#default-router 10.62.102.254
#exit
#interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
#shutdown
#exit
```

Switch D2

```
#hostname D2
#ip routing
#ipv6 unicast-routing
#no ip domain lookup
#banner motd # D2, ENCOR Skills Assessment#
#line con 0
#exec-timeout 0 0
#logging synchronous
#exit
#vlan 100
#name Management
#exit
#vlan 101
#name UserGroupA
#exit
#vlan 102
#name UserGroupB
#exit
#vlan 999
#name NATIVE
#exit
#interface e1/0
#no switchport
#ip address 10.62.11.2 255.255.255.0
#ipv6 address fe80::d1:1 link-local
#ipv6 address 2001:db8:100:1011::2/64
#no shutdown
#exit
#interface vlan 100
#ip address 10.62.100.2 255.255.255.0
#ipv6 address fe80::d2:2 link-local
#ipv6 address 2001:db8:100:100::2/64
#no shutdown
#exit
#interface vlan 101
```

```
#ip address 10.62.101.2 255.255.255.0
#ipv6 address fe80::d2:3 link-local
#ipv6 address 2001:db8:100:101::2/64
#no shutdown
#exit
#interface vlan 102
#ip address 10.62.102.2 255.255.255.0
#ipv6 address fe80::d2:4 link-local
#ipv6 address 2001:db8:100:102::2/64
#no shutdown
#exit
#ip dhcp excluded-address 10.62.101.1 10.62.101.209
#ip dhcp excluded-address 10.62.101.241 10.62.101.254
#ip dhcp excluded-address 10.62.102.1 10.62.102.209
#ip dhcp excluded-address 10.62.102.241 10.62.102.254
#ip dhcp pool VLAN-101
#network 10.62.101.0 255.255.255.0
#default-router 10.62.101.254
#exit
#ip dhcp pool VLAN-102
#network 10.62.102.0 255.255.255.0
#default-router 10.62.102.254
#exit
#interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
#shutdown
#exit
```

Switch A1

```
#hostname A1
#no ip domain lookup
#banner motd # A1, ENCOR Skills Assessment#
#line con 0
#exec-timeout 0 0
#logging synchronous
#exit
#vlan 100
#name Management
#exit
#vlan 101
#name UserGroupA
#exit
#vlan 102
#name UserGroupB
#exit
#vlan 999
```

```

#name NATIVE
#exit
#interface vlan 100
#ip address 10.62.100.3 255.255.255.0
#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

```

En esta instancia, para guardar la configuración de todos los dispositivos de la topología de red que hayamos creado con GNS3, se coloca en cada uno de ellos el comando running-config al archivo startup-config, debido a que el archivo running-config permite obtener una copia del archivo mediante el archivo startup-config al iniciar ya sea un Router o un Switch. De esta forma cuando el administrador requiera modificar la configuración de un dispositivo o desee añadir y/o eliminar líneas de comando, el archivo de configuración actual sea el que se modifique.

```
#copy running-config startup-config
```

Si hay PCs en la topología y hemos hecho algún cambio en ellos, se coloca el comando

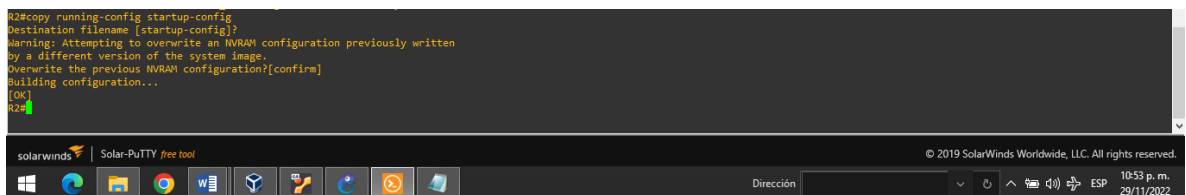
```
#save
```

Figura 5. Guardando las configuraciones en R1



Fuente: Autoría propia

Figura 6. Guardando las configuraciones en R2



Fuente: Autoría propia

Figura 7. Guardando las configuraciones en R3

```
R3#copy running-config startup-config
*Nov 29 22:56:59.115: %SYS-5-COMFIG I: Configured from console by console
R3#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...
[OK]
R3#
```

Fuente: Autoría propia

Figura 8. Guardando las configuraciones en D1

```
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 2490 bytes to 1392 bytes[OK]
D1#
```

Fuente: Autoría propia

Figura 9. Guardando las configuraciones 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 2490 bytes to 1392 bytes[OK]
D2#
*Nov 29 23:16:39.200: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/0 (not f
ull duplex), with R3 Ethernet1/0 (full duplex).
D2#
```

Fuente: Autoría propia

Figura 10. Guardando las configuraciones 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 988 bytes[OK]
A1#
```

Fuente: Autoría propia

Seguidamente, se asignan las direcciones IPv4 e IPv6 en PC1 y PC4 con la respectiva puerta de enlace 10.55.100.254; Por consiguiente a través de las siguientes figuras al emitir el comando sh se observa la dirección IP previamente configurada y asimismo se emite el comando save.

> ip 10.62.100.5/24 10.62.100.254

Figura 11. Asignación de direccionamiento IPv4 e IPv6 a PC1.

```
PC1> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC1 10.62.100.5/24 10.62.100.254 08:50:79:66:68:01 20046 127.0.0.1:20047
fe80::250:79ff:fe66:6801/64
2001:db8:100::5/64
PC1>
```

Fuente: Autoría propia

> ip 10.62.100.6/24 10.62.100.254

Figura 12. Asignación de direccionamiento IPv4 e IPv6 a PC4.

```
PC4> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC4 10.62.100.6/24 10.62.100.254 08:50:79:66:68:03 20050 127.0.0.1:20051
fe80::250:79ff:fe66:6803/64
2001:db8:100::6/64
PC4>
```

Fuente: Autoría propia

PARTE 3: CONFIGURACION DE LA RED DE CAPA 2 Y LA COMPATIBILIDAD CON LOS HOSTS

En esta parte se completa 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, por ello se seguirá el siguiente procedimiento. Para lo cual, primero en todos los Switches se establecen las interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre Switches de la consiguiente forma:

- D1 y D2
- D1 y A1
- D2 y A1

Se configura la VLAN 999 como la VLAN nativa, para esta parte se utilizan los siguientes comandos:

D1 hacia D2

```
#interface range e2/0-3
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#no shutdown
```

D1 hacia A1

```
#interface range e0/1-2
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#no shutdown
```

D2 hacia D1

```
#interface range e2/0-3
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#no shutdown
#exit
```

D2 hacia A1

```
#interface range e1/1-2
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#no shutdown
```

A1 hacia D1

```
#interface range e0/1-2
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#no shutdown
```

A1 hacia D2

```
#interface range e1/1-2
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#no shutdown
```

Inmediatamente se colocan los comandos anteriores, en todos los switches se habilita el protocolo Rapid Spanning-Tree (RSTP) también llamado protocolo de

árbol de expansión; un protocolo de red de la segunda capa OSI (nivel de enlace de datos), que gestiona enlaces redundantes.

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

En los Switches D1 y D2, se configuran los puentes raíz RSTP (root bridges). Teniendo en cuenta que D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge). De este modo se configura D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

Switch D1

```
#spanning-tree vlan 100,102 root primary  
#spanning-tree vlan 101 root secondary  
#exit
```

Switch D2

```
#spanning-tree vlan 101 root primary  
#exit
```

Por medio del siguiente comando se puede verificar y monitorear la configuración RSTP que determina el puente raíz.

```
#show spanning-tree
```

Figura 13. Verificación de RSTP en D1



```
D1#show spanning-tree  
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  
-----  
Et0/0 Desg FWD 100 128.1 Shr Edge  
Po1 Desg FWD 56 128.65 Shr  
Po12 Desg FWD 41 128.66 Shr  
  
VLAN0101  
Spanning tree enabled protocol rstp  
Root ID Priority 24677  
Address aabb.cc00.0200  
Cost 41  
Port 66 (Port-channel12)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
  
Bridge ID Priority 28773 (priority 28672 sys-id-ext 101)  
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  
-----  
Po1 Desg FWD 56 128.65 Shr  
Po12 Root FWD 41 128.66 Shr  
  
--More--
```

Fuente: Autoría propia

Figura 14. Verificación de RSTP en D2

```

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 28772 (priority 28672 sys-id-ext 100)
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
-----
Po2 Desg FWD 56 128.65 Shr
Po12 Root FWD 41 128.66 Shr

VLAN0101
Spanning tree enabled protocol rstp
Root ID Priority 24677
Address aabb.cc00.0200
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 24677 (priority 24576 sys-id-ext 101)
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
-----
Po2 Desg FWD 56 128.65 Shr
Po12 Desg FWD 41 128.66 Shr

VLAN0102
Spanning tree enabled protocol rstp
Root ID Priority 24676
Address aabb.cc00.0100
Cost 41
Port 66 (Port-channel12)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
--More--

```

Fuente: Autoría propia

La configuración de un EtherChannel se puede hacer de dos formas diferentes: negociación o manual, LACP es un protocolo abierto definido por el estándar 802.3ad para intercambiar mensajes. Para esta red en todos los Switches, se crean EtherChannels LACP de la consiguiente forma:

- D1 hacia D2 – Port channel 12
- D1 hacia A1 – Port channel 1
- D2 hacia A1 – Port channel 2

Switch D1

```

#interface range e2/0-3
#channel-protocol lacp
#channel-group 12 mode active
#exit
#interface range e0/1-2
#channel-protocol lacp
#channel-group 1 mode active
#exit
#interface port-channel 12
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#switchport trunk allowed vlan 100-102

```



```
#interface port-channel 1
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#switchport trunk allowed vlan 100-102
```

Switch D2

```
#interface range e1/1-2
#channel-protocol lacp
#channel-group 2 mode active
#exit
#interface range e2/0-3
#channel-protocol lacp
#channel-group 12 mode active
#exit
#interface port-channel 2
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#switchport trunk allowed vlan 100-102
#exit
#interface port-channel 12
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk native vlan 999
#switchport trunk allowed vlan 100-102
#exit
```

Switch A1

```
#interface range e0/1-2
#channel-protocol lacp
#channel-group 1 mode active
#exit
#interface range e1/1-2
#channel-group 2 mode active
#exit
#interface port-channel 1
#switchport trunk encapsulation dot1q
#switchport trunk native vlan 999
#switchport mode trunk
#switchport trunk allowed vlan 100-102
#exit
#interface port-channel 2
#switchport trunk encapsulation dot1q
#switchport trunk native vlan 999
```

```
#switchport mode trunk
#switchport trunk allowed vlan 100-102
#exit
```

La importancia de la configuración anterior radica en que mientras el Portchannel no se establezca Spanning-tree toma un puerto del grupo como Root (FWD) y los demás los bloquea. Cuando se establece el Portchannel las interfaces individuales ya no se muestran en STP y sólo aparece la interfaz lógica del portchannel.

El siguiente comando permite realizar la verificación de la configuración de los puertos Etherchannel

```
#show etherchannel summary
```

Figura 15. Verificación de los puertos Etherchannel en D1

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

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

       A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
-----
1      Po1(SU)          LACP        Et0/1(P)  Et0/2(P)
12     Po12(SU)         LACP        Et2/0(P)  Et2/1(P)  Et2/2(P)
                          Et2/3(P)

D1#
```

Fuente: Autoría propia

Figura 16. Verificación de los puertos Etherchannel en D2

```
D2#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

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

       A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
-----
2      Po2(SU)          LACP        Et1/1(P)  Et1/2(P)
12     Po12(SU)         LACP        Et2/0(P)  Et2/1(P)  Et2/2(P)
                          Et2/3(P)

D2#
```

Fuente: Autoría propia

Figura 17. Verificación de los puertos Etherchannel en A1

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

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

       A - formed by Auto LAG

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

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

A1#
```



Fuente: Autoría propia

Consecutivamente en todos los Switches, se configura los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

Switch D1

```
#interface e0/0
#switch mode access
#switch access vlan 100
#spanning-tree portfast
#no shutdown
#exit
```

Switch D2

```
#interface e0/0
#switch mode access
#switch access vlan 102
#spanning-tree portfast
#no shutdown
#exit
```

Switch A1

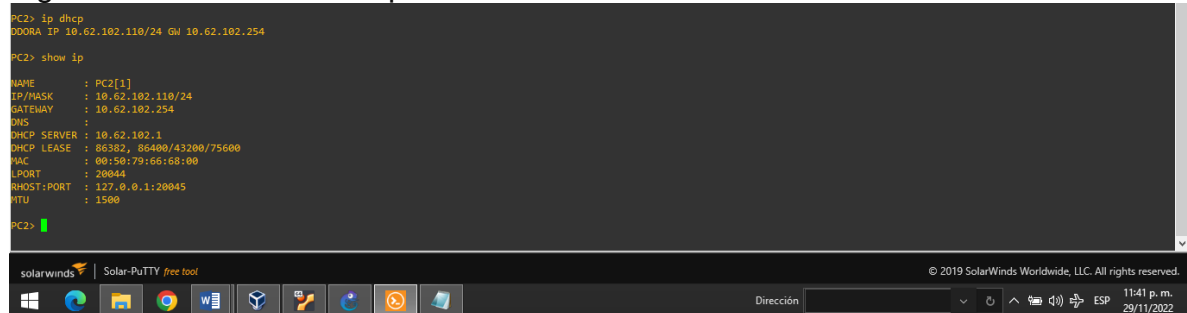
```
#interface e1/3
#switch mode access
#switch access vlan 101
#spanning-tree portfast
#no shutdown
#interface e2/0
#switch mode access
#switch access vlan 100
#spanning-tree portfast
#no shutdown
```

#exit

Se utiliza el comando ip dhcp para que se asignen estáticamente las direcciones ipv4 e ipv6 en los PC2 y PC3.

```
PC2> ip dhcp
IP 10.62.102.110/24 GW 10.62.102.254
```

Figura 18. Verificación del protocolo DHCP en PC2



```
PC2> ip dhcp
DHCPA IP 10.62.102.110/24 GW 10.62.102.254

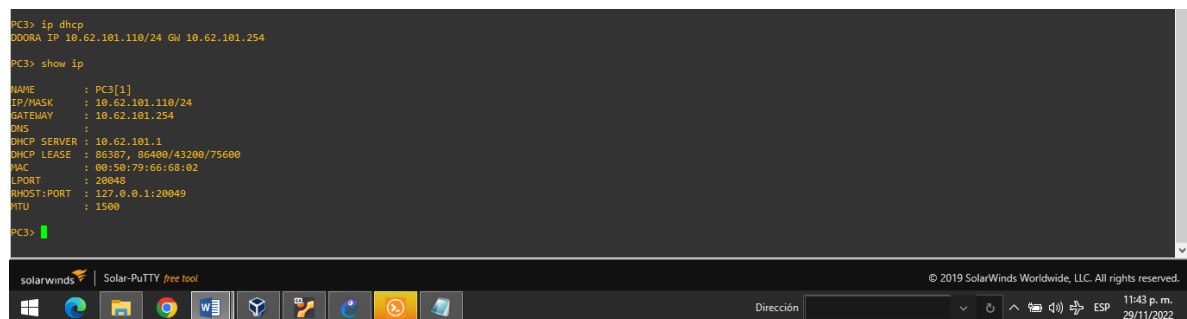
PC2> show ip
NAME       : PC2[1]
IP/MASK    : 10.62.102.110/24
GATEWAY    : 10.62.102.254
DNS        :
DHCP SERVER : 10.62.102.1
DHCP LEASE : 86382, 86400/43200/75600
MAC        : 00:50:79:66:68:00
LPORT     : 20044
RHOST:PORT : 127.0.0.1:20045
MTU        : 1500

PC2> |
```

Fuente: Autoría propia

```
PC3> ip dhcp
IP 10.62.101.110/24 GW 10.62.101.254
```

Figura 19. Verificación del protocolo DHCP en PC3



```
PC3> ip dhcp
DHCPA IP 10.62.101.110/24 GW 10.62.101.254

PC3> show ip
NAME       : PC3[1]
IP/MASK    : 10.62.101.110/24
GATEWAY    : 10.62.101.254
DNS        :
DHCP SERVER : 10.62.101.1
DHCP LEASE : 86387, 86400/43200/75600
MAC        : 00:50:79:66:68:02
LPORT     : 20048
RHOST:PORT : 127.0.0.1:20049
MTU        : 1500

PC3> |
```

Fuente: Autoría propia

Para probar y verificar la conectividad de extremo a extremo, se usa el comando ping para probar la conectividad ipv4 entre todos los dispositivos de la red.

Verificación de conexión desde PC1

- D1: 10.62.100.1
- D2: 10.62.100.2
- PC4: 10.62.100.6

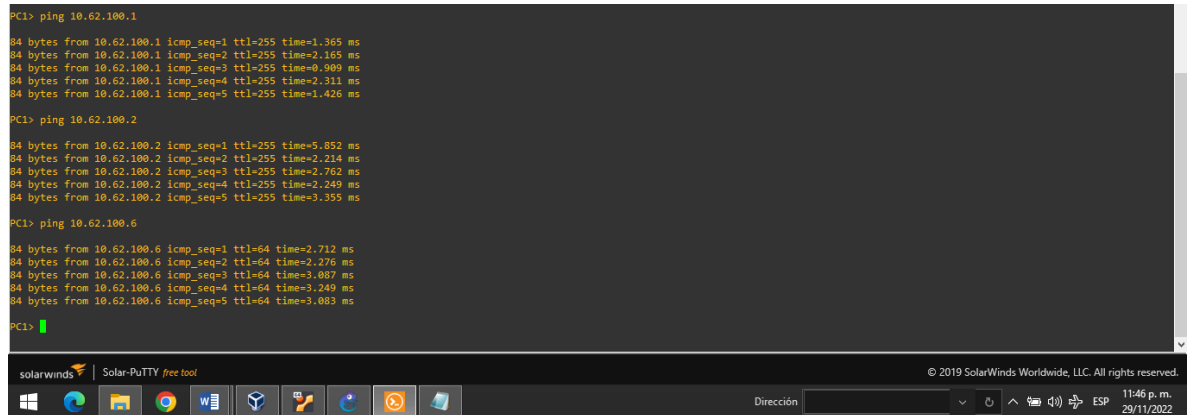
Figura 20. Verificación de conexión desde PC1

```
PC1> ping 10.62.100.1
84 bytes from 10.62.100.1 icmp_seq=1 ttl=255 time=1.365 ms
84 bytes from 10.62.100.1 icmp_seq=2 ttl=255 time=2.165 ms
84 bytes from 10.62.100.1 icmp_seq=3 ttl=255 time=0.909 ms
84 bytes from 10.62.100.1 icmp_seq=4 ttl=255 time=0.311 ms
84 bytes from 10.62.100.1 icmp_seq=5 ttl=255 time=1.426 ms

PC1> ping 10.62.100.2
84 bytes from 10.62.100.2 icmp_seq=1 ttl=255 time=5.852 ms
84 bytes from 10.62.100.2 icmp_seq=2 ttl=255 time=2.214 ms
84 bytes from 10.62.100.2 icmp_seq=3 ttl=255 time=2.762 ms
84 bytes from 10.62.100.2 icmp_seq=4 ttl=255 time=2.249 ms
84 bytes from 10.62.100.2 icmp_seq=5 ttl=255 time=3.355 ms

PC1> ping 10.62.100.6
84 bytes from 10.62.100.6 icmp_seq=1 ttl=64 time=2.712 ms
84 bytes from 10.62.100.6 icmp_seq=2 ttl=64 time=2.276 ms
84 bytes from 10.62.100.6 icmp_seq=3 ttl=64 time=3.007 ms
84 bytes from 10.62.100.6 icmp_seq=4 ttl=64 time=3.249 ms
84 bytes from 10.62.100.6 icmp_seq=5 ttl=64 time=3.083 ms

PC1> █
```



Fuente: Autoría propia

Verificación de conexión desde PC2

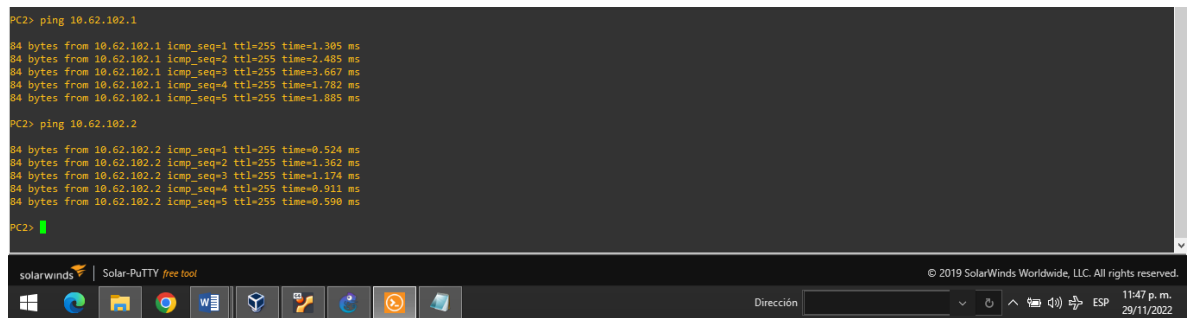
- D1: 10.62.102.1
- D2: 10.62.102.2

Figura 21. Verificación de conexión desde PC2

```
PC2> ping 10.62.102.1
84 bytes from 10.62.102.1 icmp_seq=1 ttl=255 time=1.305 ms
84 bytes from 10.62.102.1 icmp_seq=2 ttl=255 time=2.485 ms
84 bytes from 10.62.102.1 icmp_seq=3 ttl=255 time=3.667 ms
84 bytes from 10.62.102.1 icmp_seq=4 ttl=255 time=1.702 ms
84 bytes from 10.62.102.1 icmp_seq=5 ttl=255 time=1.885 ms

PC2> ping 10.62.102.2
84 bytes from 10.62.102.2 icmp_seq=1 ttl=255 time=0.524 ms
84 bytes from 10.62.102.2 icmp_seq=2 ttl=255 time=1.362 ms
84 bytes from 10.62.102.2 icmp_seq=3 ttl=255 time=1.174 ms
84 bytes from 10.62.102.2 icmp_seq=4 ttl=255 time=0.911 ms
84 bytes from 10.62.102.2 icmp_seq=5 ttl=255 time=0.590 ms

PC2> █
```



Fuente: Autoría propia

Verificación de conexión desde PC3

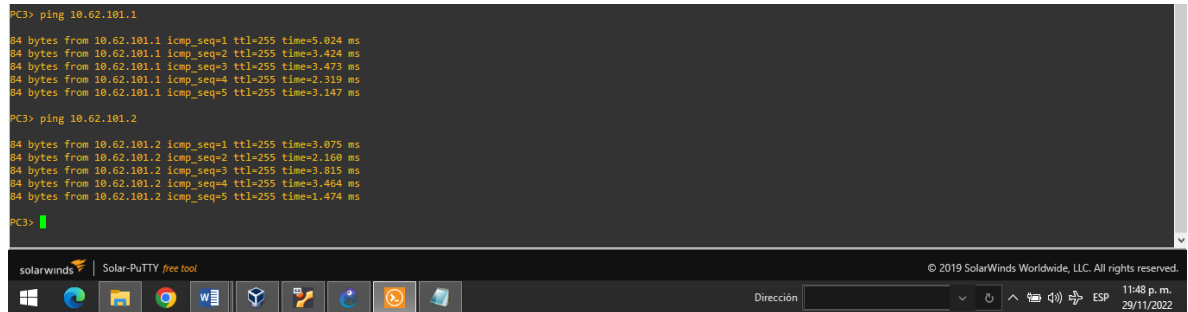
- D1: 10.62.101.1
- D2: 10.62.101.2

Figura 22. Verificación de conexión desde PC3

```
PC3> ping 10.62.101.1
84 bytes from 10.62.101.1 icmp_seq=1 ttl=255 time=5.024 ms
84 bytes from 10.62.101.1 icmp_seq=2 ttl=255 time=3.424 ms
84 bytes from 10.62.101.1 icmp_seq=3 ttl=255 time=3.473 ms
84 bytes from 10.62.101.1 icmp_seq=4 ttl=255 time=2.319 ms
84 bytes from 10.62.101.1 icmp_seq=5 ttl=255 time=3.147 ms

PC3> ping 10.62.101.2
84 bytes from 10.62.101.2 icmp_seq=1 ttl=255 time=3.075 ms
84 bytes from 10.62.101.2 icmp_seq=2 ttl=255 time=2.160 ms
84 bytes from 10.62.101.2 icmp_seq=3 ttl=255 time=3.815 ms
84 bytes from 10.62.101.2 icmp_seq=4 ttl=255 time=3.464 ms
84 bytes from 10.62.101.2 icmp_seq=5 ttl=255 time=1.474 ms

PC3> |
```



Fuente: Autoría propia

Verificación de conexión desde PC4

- D1: 10.62.100.1
- D2: 10.62.100.2
- PC1: 10.62.100.5

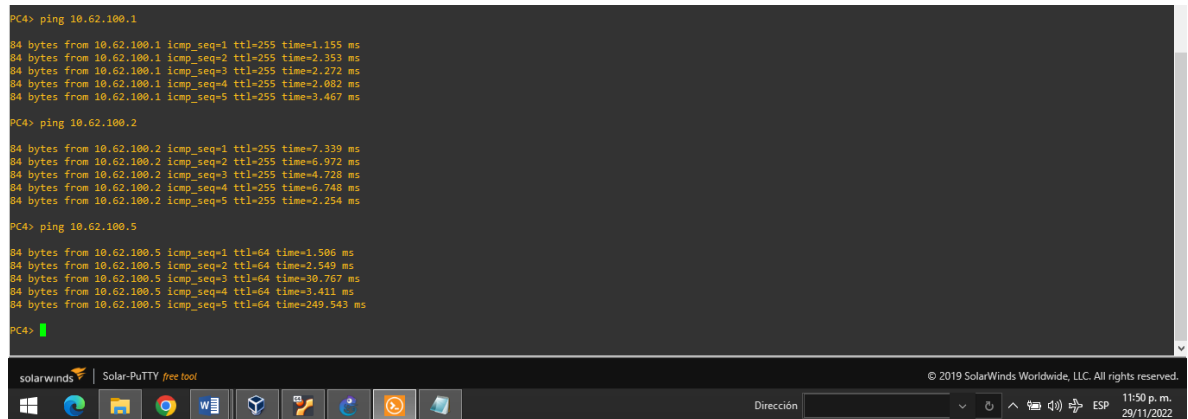
Figura 23. Verificación de conexión desde PC4

```
PC4> ping 10.62.100.1
84 bytes from 10.62.100.1 icmp_seq=1 ttl=255 time=1.155 ms
84 bytes from 10.62.100.1 icmp_seq=2 ttl=255 time=2.353 ms
84 bytes from 10.62.100.1 icmp_seq=3 ttl=255 time=2.272 ms
84 bytes from 10.62.100.1 icmp_seq=4 ttl=255 time=2.082 ms
84 bytes from 10.62.100.1 icmp_seq=5 ttl=255 time=3.467 ms

PC4> ping 10.62.100.2
84 bytes from 10.62.100.2 icmp_seq=1 ttl=255 time=7.339 ms
84 bytes from 10.62.100.2 icmp_seq=2 ttl=255 time=6.972 ms
84 bytes from 10.62.100.2 icmp_seq=3 ttl=255 time=4.728 ms
84 bytes from 10.62.100.2 icmp_seq=4 ttl=255 time=5.748 ms
84 bytes from 10.62.100.2 icmp_seq=5 ttl=255 time=2.254 ms

PC4> ping 10.62.100.5
84 bytes from 10.62.100.5 icmp_seq=1 ttl=64 time=1.586 ms
84 bytes from 10.62.100.5 icmp_seq=2 ttl=64 time=2.549 ms
84 bytes from 10.62.100.5 icmp_seq=3 ttl=64 time=30.767 ms
84 bytes from 10.62.100.5 icmp_seq=4 ttl=64 time=3.411 ms
84 bytes from 10.62.100.5 icmp_seq=5 ttl=64 time=249.543 ms

PC4> |
```



Fuente: Autoría propia

PARTE 3: CONFIGURACION DE LOS PROTOCOS DE ENRUTAMIENTO

En esta parte se configuran los protocolos de enrutamiento Ipv4 e Ipv6. Para lo cual, primero se configura OSPFv2 en área 0 en la red de la empresa esto incluye a los dispositivos R1, R3, D1 y D2, para lo cual se utiliza el ID de proceso OSPF 4 y se asigna 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 los dispositivos R1, R3, D1 y D2, se anuncian todas las redes/VLAN conectadas directamente en el Área 0. Teniendo en cuenta principalmente las siguientes condiciones:

- En el router R1, no se anuncia la red R1 – R2.
- En el router R1, se propaga una ruta predeterminada. Teniendo en cuenta que BGP proporcionará la ruta predeterminada para realizar el proceso.

Asimismo se deshabilitan los anuncios OSPFv2 en:

- D1: Todas las interfaces excepto e1/2
- D2: Todas las interfaces excepto e1/0

Router R1

```
#router ospf 4
#router-id 0.0.4.1
#network 10.62.10.0 0.0.0.255 area 0
#network 10.62.13.0 0.0.0.255 area 0
#network 209.165.200.0 0.0.0.31 area 0
#default-information originate
#exit
```

Router R3

```
#router ospf 4
#router-id 0.0.4.3
#network 10.62.11.0 0.0.0.255 area 0
#network 10.62.13.0 0.0.0.255 area 0
#exit
```

Switch D1

```
#router ospf 4
#router-id 0.0.4.131
#passive-interface default
#no passive-interface e1/2
#network 10.62.10.0 0.0.0.255 area 0
#network 10.62.100.0 0.0.0.255 area 0
#network 10.62.101.0 0.0.0.255 area 0
#network 10.62.102.0 0.0.0.255 area 0
#exit
```

Switch D2

```
#router ospf 4
#router-id 0.0.4.132
#passive-interface default
#no passive-interface e1/0
#network 10.62.11.0 0.0.0.255 area 0
#network 10.62.100.0 0.0.0.255 area 0
#network 10.62.101.0 0.0.0.255 area 0
#network 10.62.102.0 0.0.0.255 area 0
#exit
```

Seguidamente se configura el protocolo OSPFv3 en área 0, para lo cual se utiliza el ID de proceso OSPF 6 y se asigna los siguientes ID de enrutador:

- R1: 0.0.6.1
- R3: 0.0.6.3
- D1: 0.0.6.131
- D2: 0.0.6.132

En los dispositivos R1, R3, D1 y D2, se anuncian todas las redes/VLAN conectadas directamente en el Área 0. Teniendo en cuenta principalmente las siguientes condiciones:

- En el router R1, no se anuncia la red R1 – R2.
- En el router R1, se propaga una ruta predeterminada. Teniendo en cuenta que BGP proporcionará la ruta predeterminada para realizar el proceso.

Asimismo se deshabilitan los anuncios OSPFv3 en:

- D1: Todas las interfaces excepto e1/2
- D2: Todas las interfaces excepto e1/0

Router R1

```
#ipv6 router ospf 6
#router-id 0.0.6.1
#default-information originate
#exit
#interface e1/1
#ipv6 ospf 6 area 0
#exit
#interface e1/2
#ipv6 ospf 6 area 0
#exit
#ipv6 route ::/0 e1/0
```



```
#ipv6 router ospf 6
#default-information originate
#exit
```

Router R3

```
#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
```

Switch D1

```
#ipv6 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
```

Switch D2

```
#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
```

Para realizar la respectiva verificación de la configuración OSPF Ipv4 e Ipv6, en cada uno de los dispositivos que conforman la red (R1, R3, D1, D2); emitiendo el siguiente comando

```
#show run | section router ospf
```

Figura 24. Verificación de la configuración OSPF en R1

```
R1#show run | section router ospf
*Dec 1 00:44:24.243: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/2 (not half duplex), with D1 Ethernet1/2 (half duplex).
router ospf 4
router-id 0.0.4.1
network 10.62.10.0 0.0.0.255 area 0
network 10.62.13.0 0.0.0.255 area 0
network 200.165.200.0 0.0.0.31 area 0
default-information originate
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
R1#
```

Fuente: propia

Figura 25. Verificación de la configuración OSPF en R3

```
R3#show run | section router ospf
router ospf 4
router-id 0.0.4.3
network 10.62.11.0 0.0.0.255 area 0
network 10.62.13.0 0.0.0.255 area 0
ipv6 router ospf 6
router-id 0.0.6.3
R3#
```

Fuente: propia

Figura 26. Verificación de la configuración OSPF en D1

```
D1#show run | section router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface Ethernet1/2
network 10.62.10.0 0.0.0.255 area 0
network 10.62.100.0 0.0.0.255 area 0
network 10.62.101.0 0.0.0.255 area 0
network 10.62.102.0 0.0.0.255 area 0
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet1/2
D1#
```

Fuente: propia

Figura 27. Verificación de la configuración OSPF en D2

```
D2#show run | section router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface Ethernet1/0
network 10.62.11.0 0.0.0.255 area 0
network 10.62.100.0 0.0.0.255 area 0
network 10.62.101.0 0.0.0.255 area 0
!
router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface Ethernet1/0
D2#
```

Fuente: pro pia

En el dispositivo R2 que incluye la red ISP, se configura MP-BGP que es una extensión al BGP que permite al BGP transportar información de enrutamiento para varias capas de red y familias de direcciones. Para lo cual, se configuran dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada de IPv4.
- Una ruta estática predeterminada de IPv6.

Se configura el dispositivo R2 en BGP ASN 500 y se usa la identificación del enrutador 2.2.2.2. Seguidamente se configura y habilita una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

Por lo que en la familia de direcciones IPv4, se anuncia:

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0).

Por lo que en la familia de direcciones IPv6, se anuncia:

- La red Loopback 0 IPv4 (/128).
- La ruta por defecto (::/0).

Router R2

```
#ip route 0.0.0.0 0.0.0.0 Loopback0
#ipv6 route ::/0 Loopback0
#router bgp 500
#bgp router-id 2.2.2.2
#no bgp default ipv4-unicast
#neighbor 209.165.200.225 remote-as 300
#neighbor 2001:db8:200::1 remote-as 300
#address-family ipv4 unicast
#neighbor 209.165.200.225 activate
```

```
#network 2.2.2.2 mask 255.255.255.255
#network 0.0.0.0 mask 0.0.0.0
#exit-address-family
#address-family ipv6 unicast
#no neighbor 2001:db8:200::1 activate
#network 2001:db8:2222::1/128
#network ::/0
#exit-address-family
```

En el dispositivo R1 que incluye la red ISP, se configura también la extensión MP-BGP. Se configuran dos rutas resumidas estáticas a la interfaz Null 0:

- Una ruta IPv4 resumida para 10.62.0.0/8.
- Una ruta IPv6 resumida para 2001:db8:100::/48.

En este mismo dispositivo se configura R1 en BGP ASN 300 y use la identificación del enrutador 1.1.1.1. Consecutivamente se configura una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

Por lo que en la familia de direcciones IPv4:

- Deshabilitar la relación de vecino IPv6.
- Habilite la relación de vecino IPv4.
- Anuncie la red 10.62.0.0/8.

Por lo que en la familia de direcciones IPv6:

- Deshabilitar la relación de vecino IPv4.
- Habilite la relación de vecino IPv6.
- Anuncie la red 2001:db8:100::/48.

Router R1

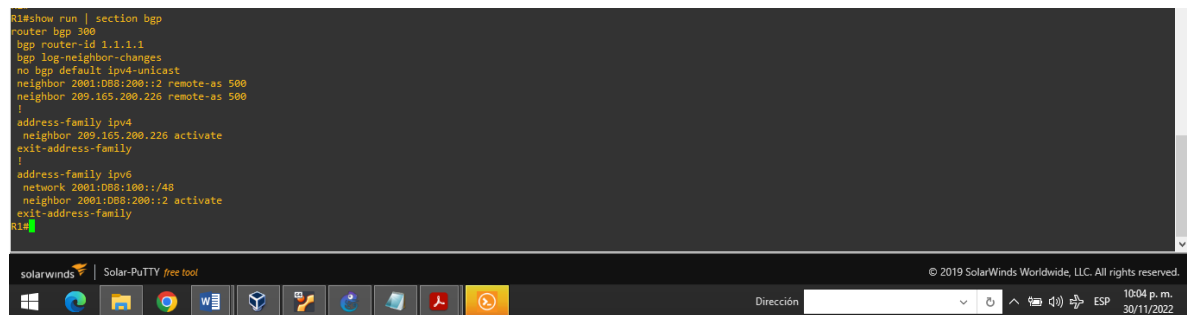
```
#ip route 10.62.0.0 255.255.255.0 null0
#ipv6 route 2001:db8:100::/48 null0
#router bgp 300
#bgp router-id 1.1.1.1
#no bgp default ipv4-unicast
#neighbor 209.165.200.226 remote-as 500
#neighbor 2001:db8:200::2 remote-as 500
#address-family ipv4 unicast
#neighbor 209.165.200.226 activate
#no neighbor 2001:db8:200::2 activate
```

```
#network 10.62.0.0 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
```

Para verificar la configuración BGP en el Router R1 y R2, se emite el siguiente comando

```
#show run | section bgp
```

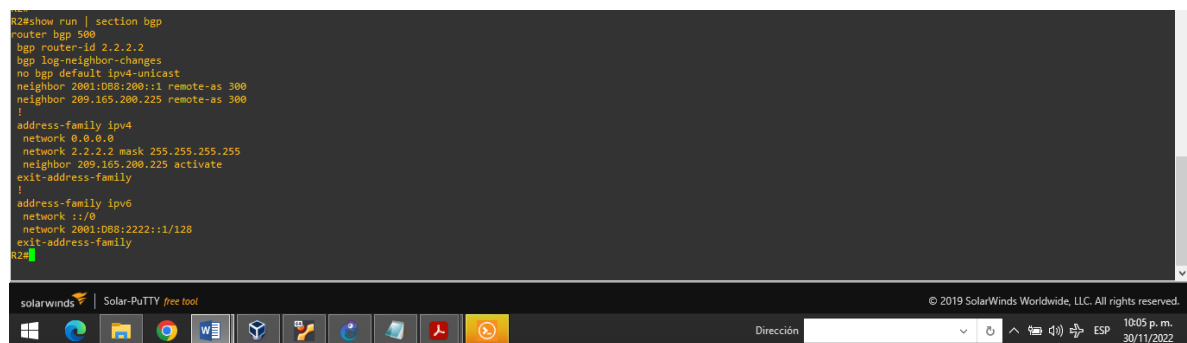
Figura 28. Verificación de la configuración BGP en R1



```
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    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#
```

Fuente: propia

Figura 29. Verificación de la configuración BGP en R2



```
R2#show run | section bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  no bgp default ipv4-unicast
  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
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network 2::/3
    network 2001:DB8:2222::1/128
  exit-address-family
R2#
```

Fuente: propia

PARTE 4: CONFIGURACION DE LA REDUNDANCIA DEL PRIMER SALTO

En esta parte, se configurará la versión 2 de HSRP (Hot Standby Router Protocol) que es un protocolo que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red, por lo que en la presente configuración proporciona

redundancia de primer salto para hosts en la "Red de la empresa". En esta configuración primero tenemos el dispositivo D1, en cual se crea la IP SLA y de esta forma probar la accesibilidad de la interfaz e1/2 del router R1. Principalmente se crean dos IP SLA:

- Utilice el SLA número 4 para IPv4.
- Utilice el SLA número 6 para IPv6.

Hay que tener en cuenta que los IP SLA probarán la disponibilidad de la interfaz R1 E1/2 cada 5 segundos. Entonces se programa el SLA para implementación inmediata sin tiempo de finalización y se crea 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 D1

```
#ip sla 4
#icmp-echo 10.62.10.1
#source-ip 10.62.10.2
#frequency 5
#exit
#ip sla 6
#icmp-echo 2001:db8:100:1010::1 source-interface e1/2
#frequency 5
#exit
#ip sla schedule 4 start-time now life forever
#ip sla schedule 6 start-time now life forever
#track 4 ip sla 4 reachability
#delay down 10 up 15
#exit
#track 6 ip sla 6 reachability
#delay down 10 up 15
#exit
```

Seguidamente en D2, se crea la IP SLA que prueba la accesibilidad de la interfaz E1/0 de R3. Por lo tanto se crean dos IP SLA:

- Utilice el SLA número 4 para IPv4.
- Utilice el SLA número 6 para IPv6.

En este punto hay que tener en cuenta que los IP SLA también probarán la disponibilidad de la interfaz R3 E1/0 cada 5 segundos. Entonces se programa el SLA para implementación inmediata sin tiempo de finalización y se crea 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.

Es importante que 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.

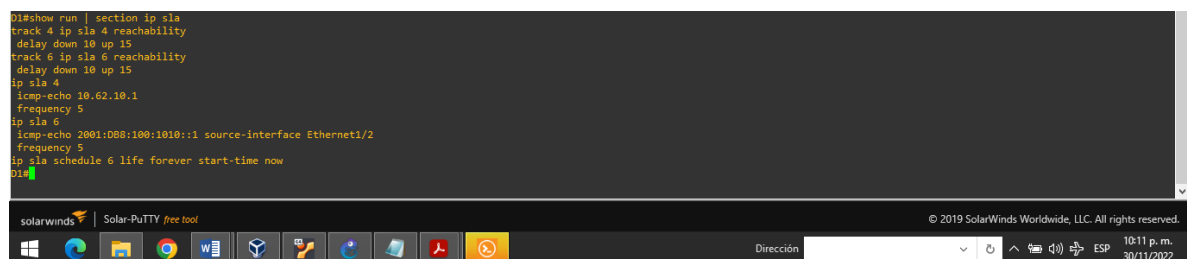
Switch D2

```
#ip sla 4
#icmp-echo 10.62.11.1 source-interface e1/0
#frequency 5
#exit
#ip sla 6
#icmp-echo 2001:DB8:100:1011::1
#source-interface e1/0
#frequency 5
#ip sla schedule 4 start-time now life forever
#ip sla schedule 6 start-time now life forever
#track 4 ip sla 4 reachability
#delay down 10 up 15
#track 6 ip sla 6 reachability
#delay down 10 up 15
#exit
```

Para realizar la respectiva verificación de la configuración IP SLA en D1, se emite el siguiente comando tanto en D1 como en D2

```
#show run | section ip sla
```

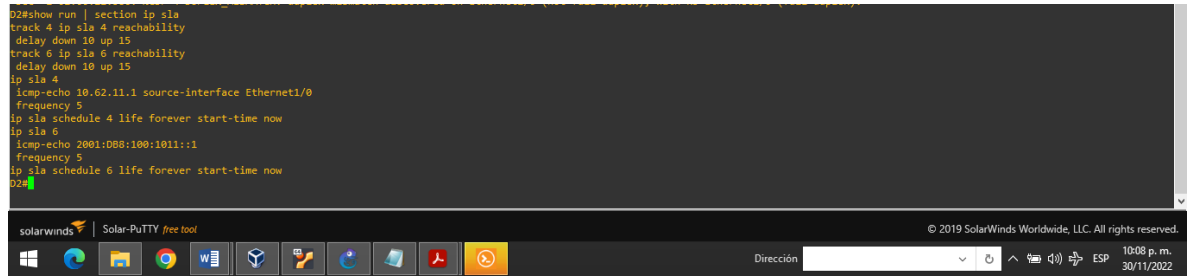
Figura 30. Verificación de la configuración IP SLA en D1



```
D1#show run | section ip sla
track 4 ip sla 4 reachability
delay down 10 up 15
track 6 ip sla 6 reachability
delay down 10 up 15
ip sla 4
icmp-echo 10.62.10.1
frequency 5
ip sla 6
icmp-echo 2001:DB8:100:1010::1 source-interface Ethernet1/2
frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

Fuente: propia

Figura 31. Verificación de la configuración IP SLA en D2



```
D2#show run | section ip sla
track 4 ip sla 4 reachability
delay down 10 up 15
track 6 ip sla 6 reachability
delay down 10 up 15
ip sla 4
icmp-echo 10.62.11.1 source-interface Ethernet1/0
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#
```

Fuente: propia

Seguidamente en esta parte en D1, se configura HSRPv2 para establecer una puerta de enlace predeterminada tolerante a fallas. Ya que el dispositivo D1 es el enrutador principal para las VLAN 100 y 102; por lo tanto, su prioridad también se cambiará a 150. Entonces primero se configura la versión 2 de HSRP y seguidamente se configura el grupo 104 de HSRP de IPv4 para la VLAN 100:

- Asigne la dirección IP virtual 10.62.100.254.
- Establezca la prioridad del grupo en 150.
- Habilitar preferencia.
- Siga el objeto 4 y disminuya en 60.

Se configura el grupo 114 de HSRP de IPv4 para la VLAN 101:

- Asigne la dirección IP virtual 10.62.101.254.
- Habilitar preferencia.
- Seguimiento del objeto 4 para disminuir en 60.

Se configura el grupo 124 de HSRP de IPv4 para la VLAN 102:

- Asigne la dirección IP virtual 10.62.102.254.
- Establezca la prioridad del grupo en 150.
- Habilitar preferencia.
- Seguimiento del objeto 4 para disminuir en 60.

Se configura el grupo 106 de HSRP de IPv6 para la VLAN 100:

- 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.

Se configura el grupo 116 de HSRP de IPv6 para la VLAN 101:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Habilitar preferencia.
- Siga el objeto 6 y disminuya en 60.

Se configura el grupo 126 de HSRP de IPv6 para la VLAN 102:

- 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.

Switch D1

```
#interface vlan 100
#standby version 2
#standby 104 ip 10.62.100.254
#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 10.62.101.254
#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 10.62.102.254
#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
```

Continuamos configurando HSRPv2 en D2, para lo cual D2 es el enrutador principal para la VLAN 101; por lo tanto, la prioridad también se cambiará a 150. Primero se configura la versión 2 de HSRP, seguidamente se configura el grupo 104 de HSRP de IPv4 para la VLAN 100:

- Asigne la dirección IP virtual 10.62.100.254.
- Habilitar preferencia.
- Siga el objeto 4 y disminuya en 60.

Se configura el grupo 114 de HSRP de IPv4 para la VLAN 101:

- Asigne la dirección IP virtual 10.62.101.254.
- Establezca la prioridad del grupo en 150.
- Habilitar preferencia.
- Seguimiento del objeto 4 para disminuir en 60.

Se configura el grupo 124 de HSRP de IPv4 para la VLAN 102:

- Asigne la dirección IP virtual 10.62.102.254.
- Habilitar preferencia.
- Seguimiento del objeto 4 para disminuir en 60.

Se configura el grupo 106 de HSRP de IPv6 para la VLAN 100:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Habilitar preferencia.
- Siga el objeto 6 y disminuya en 60.

Se configura el grupo 116 de HSRP de IPv6 para la VLAN 101:

- 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.

Se configura el grupo 126 de HSRP de IPv6 para la VLAN 102:

- Asigne la dirección IP virtual mediante la configuración automática de ipv6.
- Habilitar preferencia.
- Siga el objeto 6 y disminuya en 60.

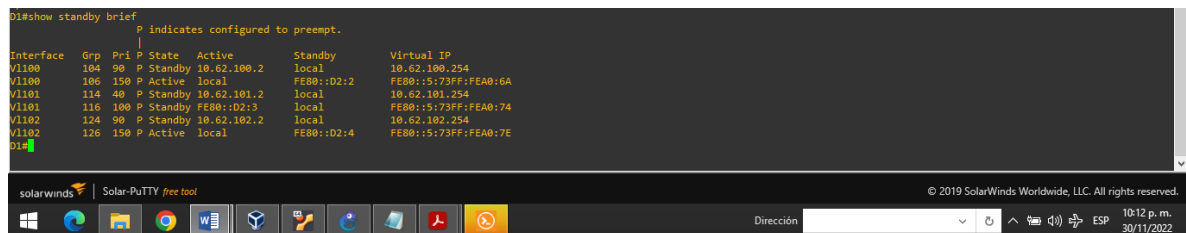
Switch D2

```
#interface vlan 100
#standby version 2
#standby 104 ip 10.62.100.254
#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 10.62.101.254
#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 10.62.102.254
#standby 124 preempt
#standby 124 track 4 decrement 60
#standby 126 ipv6 autoconfig
#standby 126 preempt
#standby 126 track 6 decrement 60
#exit
```

Seguidamente se verifica la configuración HSRP en D1 y D2

```
#show standby brief
```

Figura 32. Verificación de HSRP en D1

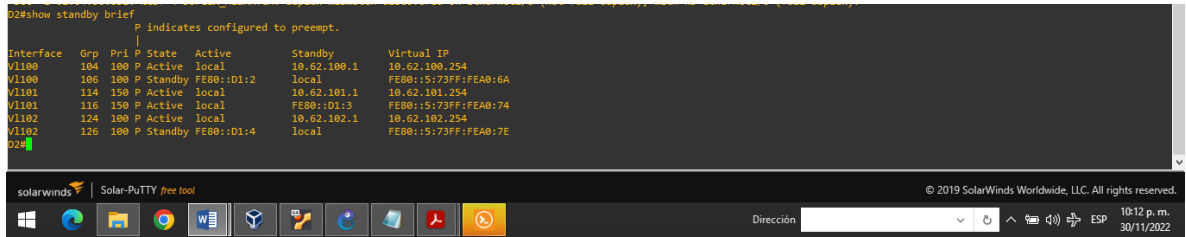


```
D1#show standby brief
P indicates configured to preempt.
|
Interface  Grp  Pri  P State Active Standby Virtual IP
V1100     104  90  P Standby 10.62.100.2 local 10.62.100.254
V1100     106  150 P Active local FE80::D2:2 FE80::5:73FF:FEA0:6A
V1101     114  40  P Standby 10.62.101.2 local 10.62.101.254
V1101     116  100 P Standby FE80::D2:3 local FE80::5:73FF:FEA0:74
V1102     124  90  P Standby 10.62.102.2 local 10.62.102.254
V1102     126  150 P Active local FE80::D2:4 FE80::5:73FF:FEA0:7E
D1#
```

Fuente: propia

Figura 33. Verificación de HSRP en D2

```
D2#show standby brief
P indicates configured to preempt.
|
Interface  Grp  Pri  P State Active Standby Virtual IP
V1100     104  100  P Active local 10.62.100.1 10.62.100.254
V1100     106  100  P Standby FE80::D1:2 local FE80::5:73FF:FEA0:6A
V1101     114  150  P Active local 10.62.101.1 10.62.101.254
V1101     116  150  P Active local FE80::D1:3 FE80::5:73FF:FEA0:74
V1102     124  100  P Active local 10.62.102.1 10.62.102.254
V1102     126  100  P Standby FE80::D1:4 local FE80::5:73FF:FEA0:7E
D2#
```



Fuente: propia

CONCLUSIONES

A lo largo de este trabajo se han ido observando las ventajas que ofrece realizar este tipo de simulaciones; la cual es una herramienta que nos facilita y mejora el análisis de cualquier tipo de topología de red y esto se ve facilitándonos entender el funcionamiento desde una red pequeña hasta una gran red y también facilita nuestro desempeño en el tema de redes al manejar distintos tipos de protocolos.

Así que sabiendo los comandos que maneja cada protocolo podemos esperar que la administración de redes de aquí en adelante sea mucho más efectiva, ya que se hizo necesario profundizar acerca de los protocolos de enrutamiento OSPF y BGP y del protocolo que proporciona redundancia en una red HSRP; un protocolo clave para la seguridad de cualquier tipo de red, ya que como se observó su función principal es prevenir fallos en una red cuando tenemos varios Routers instalados como es el caso.

Por otro lado, tras configurar el protocolo DHCP y evidenciar su funcionamiento; se sugiere que relevante la incorporación de este, ya que garantiza que los dispositivos puedan conectarse a la red sin ningún problema al facilitar la administración de las dirección IP.

Después de realizar las configuraciones correspondientes y utilizar los comandos adecuados para verificar el éxito de las mismas; se concluye que el uso del programa GNS3, nos acerca a tener una idea más sencilla y práctica del desarrollo del ámbito laboral como profesional en las telecomunicaciones o profesional en electrónica. Donde tenemos una gran herramienta para desarrollar simulaciones de todo tipo de sistemas de redes, logrando entender y comprender a mejor las temáticas principales de las comunicaciones entre los dispositivos que las constituyen.

REFERENCIAS

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). 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). Advanced Spanning Tree. 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). VLAN Trunks and EtherChannel Bundles. 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). IP Routing Essentials. 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). Advanced 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>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced BGP. 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). IP Services. 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). Enterprise Network Architecture. 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). Fabric Technologies. 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). Network Assurance. 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). Secure Access Control. 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). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCORA 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Flor, P. (2022). Introducción al protocolo BGP [OVI]. <https://repository.unad.edu.co/handle/10596/49573>