DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOHAN ESNEIDER RODRIGUEZ ANGULO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2022

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOHAN ESNEIDER RODRIGUEZ ANGULO

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

DIRECTOR:
Msc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2022

Nota de Aceptación

_____

_____

_____

_____

_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá, 27 de Noviembre de 2022

AGRADECIMIENTOS

Agradezco primordialmente a mi Dios todo poderoso y a mis queridos padres, por todo su sacrificio y esfuerzo apoyándome todos estos años para poder salir adelante con mi carrera y ser un buen profesional.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

BGP: Es un protocolo escalable de dynamic routing usado en la Internet por grupos de enrutadores para compartir información de enrutamiento. BGP usa parámetros de ruta o atributos para definir políticas de enrutamiento y crear un entorno de enrutamiento estable.

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: Es un protocolo para prevenir fallos de red cuando tenemos varios routers instalados. Como ya sabemos, el router es un elemento clave para una red informática compleja, ya que permite la interconexión de diferentes equipos y redes que tienen distintas IP.

IPV4: Protocolo de Internet versión 4 (IPv4) es la forma de direccionamiento IP utilizada habitualmente para identificar hosts en una red y utiliza un formato de 32 bits.

IPV6: Protocolo de Internet versión 6 (IPv6) es el estándar de dirección IP de última generación diseñado para sustituir el formato IPv4. IPv6 resuelve el problema de escasez de direcciones mediante el uso de direcciones de 128 bits en lugar de direcciones de 32 bits que se utilizaban en IPv4.

OSPF: Es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).

SLA: Es una tecnología de Cisco que monitorea activamente el tráfico para medir el desempeño de la red al medir parámetros críticos para el tráfico que pasa a través de los dispositivos con software Cisco IOS y otros servidores de aplicaciones de red.

VLAN: Es una red de área local virtual (Virtual Local Area Network o VLAN), es un segmento lógico más pequeño dentro de una gran red física cableada.

RESUMEN

El desarrollo del presente informe consiste en la configuración de una red para que al final haya accesibilidad de extremo a extremo entre los dispositivos. Inicialmente, se construye la red y se configuran los ajustes básicos de los dispositivos que conforman la misma, se asigna el direccionamiento de cada interfaz; seguidamente se configura la red de capa 2 y la compatibilidad con los host; y se continúa con la configuración de los protocolos de enrutamiento, y así se procederá a seguir con la configuración de la redundancia de primer salto. De esta manera se hace posible por ultimo ejecutar la verificación de accesibilidad de la red por medio de distintos comandos.

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

ABSTRACT

The development of this report consists of configuring a network so that in the end there is end-to-end accessibility between the devices. Initially, the network is built and the basic settings of the devices that make it up are configured, the address of each interface is assigned; then layer 2 network and host compatibility are configured; and continue with the configuration of the routing protocols, and thus proceed with the configuration of the first hop redundancy. In this way it is finally possible to execute the network accessibility check by means of different commands.

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

INTRODUCCIÓN

El presente informe tiene como objetivo configurar una topología de red con el fin de poner en práctica lo aprendido en redes y telecomunicaciones por medio del simulador grafico GNS3; donde este permite realizar tanto el diseño como la configuración de la misma. Por lo que en la red primeramente se realizan las configuraciones básicas de los switches y routers junto con la asignación de direccionamiento IPv4 e IPv6 en cada uno de ellos y en los PCs, se configura la red de capa 2 y la compatibilidad de los host, continuando con la creación de las Vlans y la configuración del protocolo de enrutamiento dhcp, seguidamente se configura el protocolo OSPF y el BGP; por último se realiza la configuración de la tecnología IP SLA junto con la del protocolo HSRP; una vez hechas estas configuración se realizan las verificaciones de conectividad entre los dispositivos por medio principalmente del comando ping.

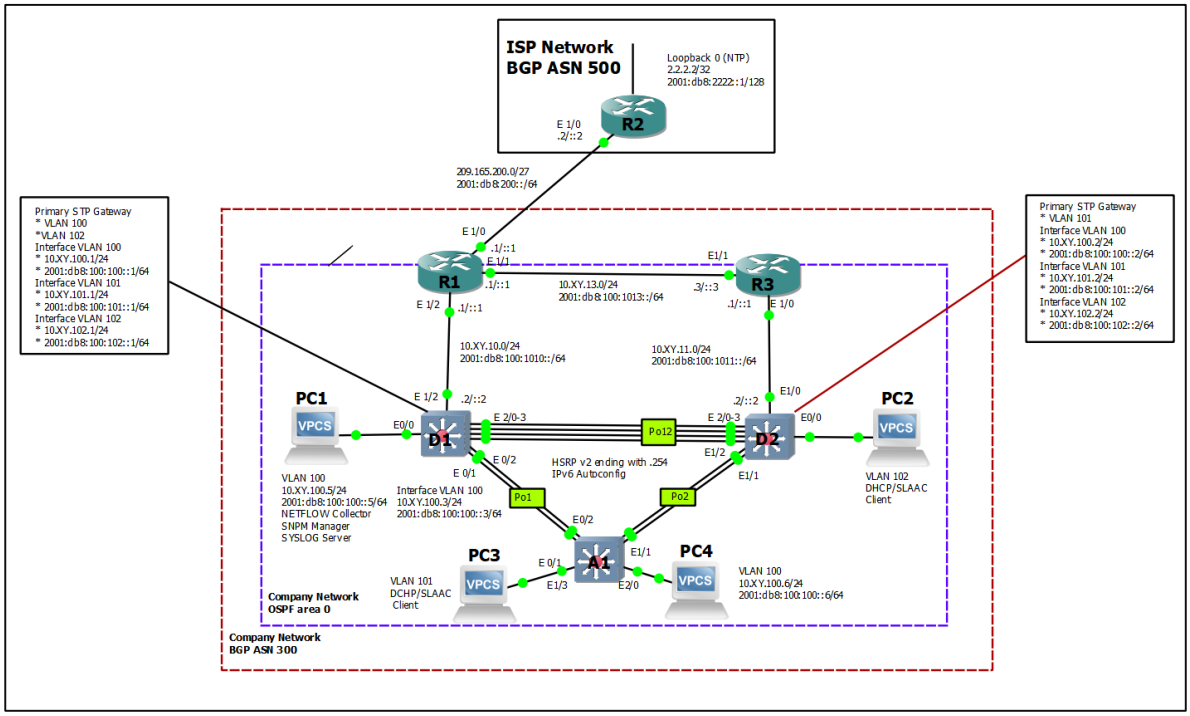
Debido a que la tecnología evoluciona velozmente actualmente es importante mantener los conocimientos actualizados; por lo tanto, el uso del programa GNS3 nos acerca a tener una idea más sencilla y práctica del desarrollo del ámbito laboral como profesional en las telecomunicaciones o profesional en electrónicas.

1 DESARROLLO

1.1 ESCENARIO

En este escenario se configurara para que haya accesibilidad completa de extremo a extremo y para que los hosts tengan soporte de puerta de enlace predeterminada confiable; a fin de que los protocolos de administración estén operativos dentro de la parte de "Red de la empresa" de la topología. Asimismo se verificara que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen.

Figura 1. Topología del 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	10.55.10.1/24	2001:db8:100:1010::1/64	fe80::1:2

	E1/1	10.55.13.1/24	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. 55.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10. 55.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10. 55.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN100	10. 55.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN101	10.55.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN102	10.55.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.55.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN100	10.55.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN101	10.55.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN102	10.55.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.55.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.55.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.55.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente: Guía Prueba de habilidades prácticas CCNP

La configuración de la red se elabora por medio del procedimiento que se explica a continuación:

1.1.1 PARTE 1: CONSTRUCCIÓN DE LA RED

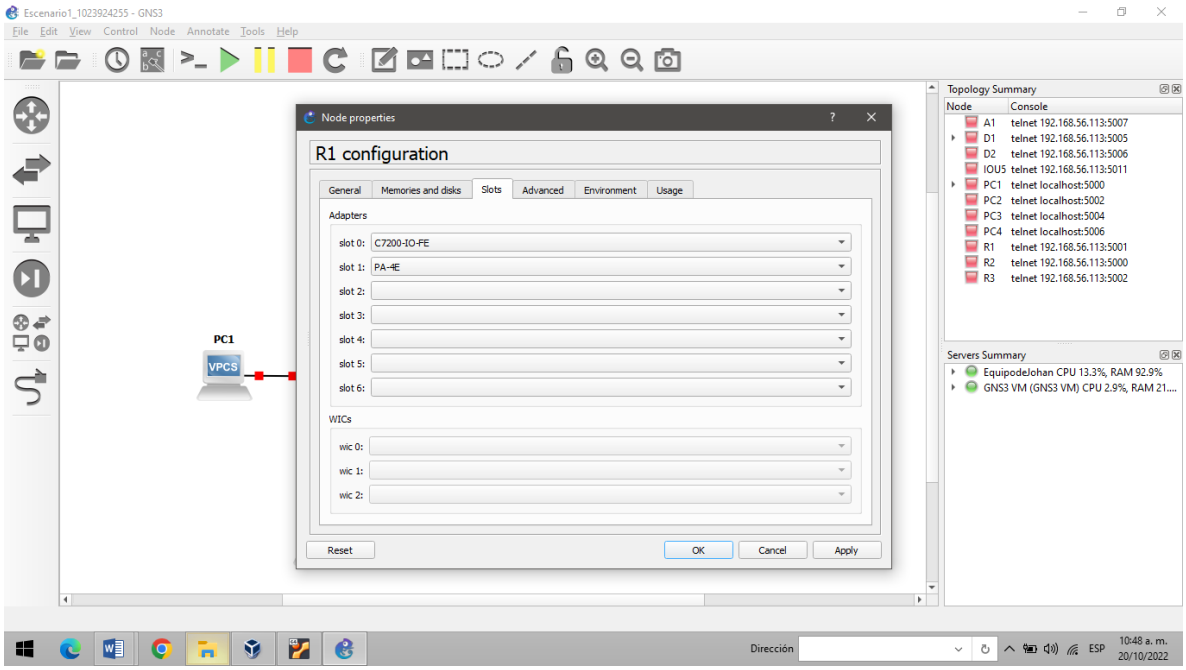
Para el desarrollo de este escenario se instala el entorno de simulación de GNS3, una vez instalado se crea la topología de red con los siguientes dispositivos:

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

Los enrutadores utilizados con los laboratorios prácticos de CCNP son enrutadores Cisco 7200. Los conmutadores utilizados en las prácticas de laboratorio son conmutadores Cisco Catalyst L2. Se pueden utilizar otros enrutadores, conmutadores y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

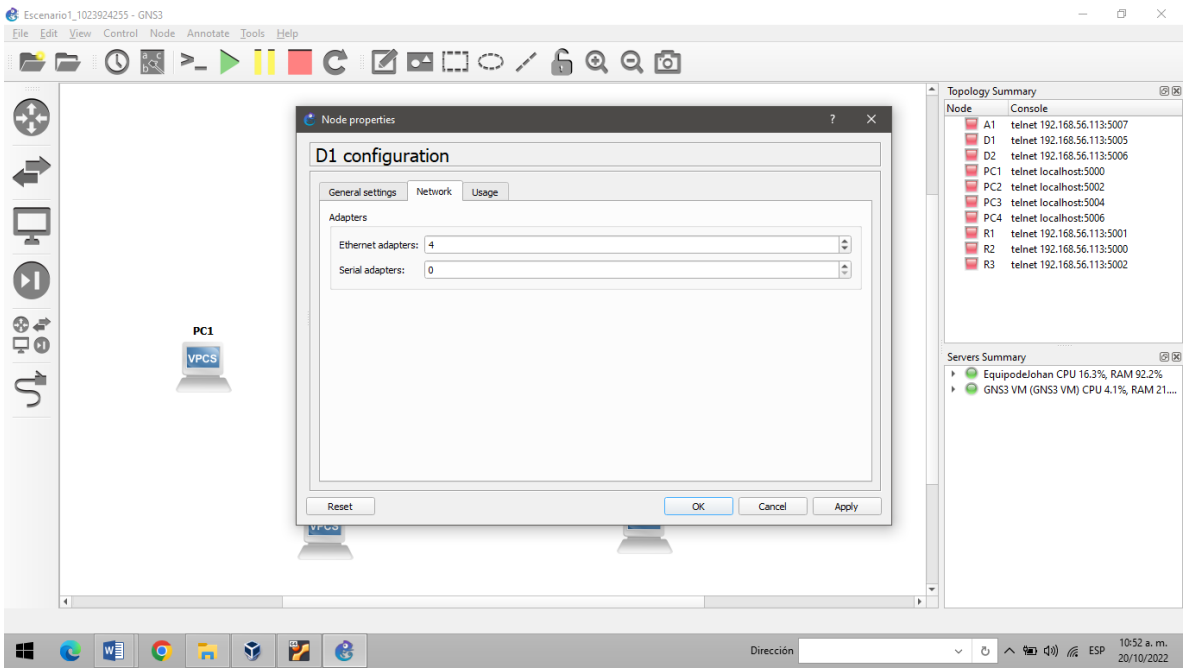
Inmediatamente al agregar los requeridos dispositivos a la pantalla principal de GNS3, se continúa con la configuración de los Slots de los adaptadores de red del SW según corresponde en los Routers y en los Switches, para así cablear la red y conectar los dispositivos como se muestra en la topología.

Figura 2 Configuración de los Slot en los Routers



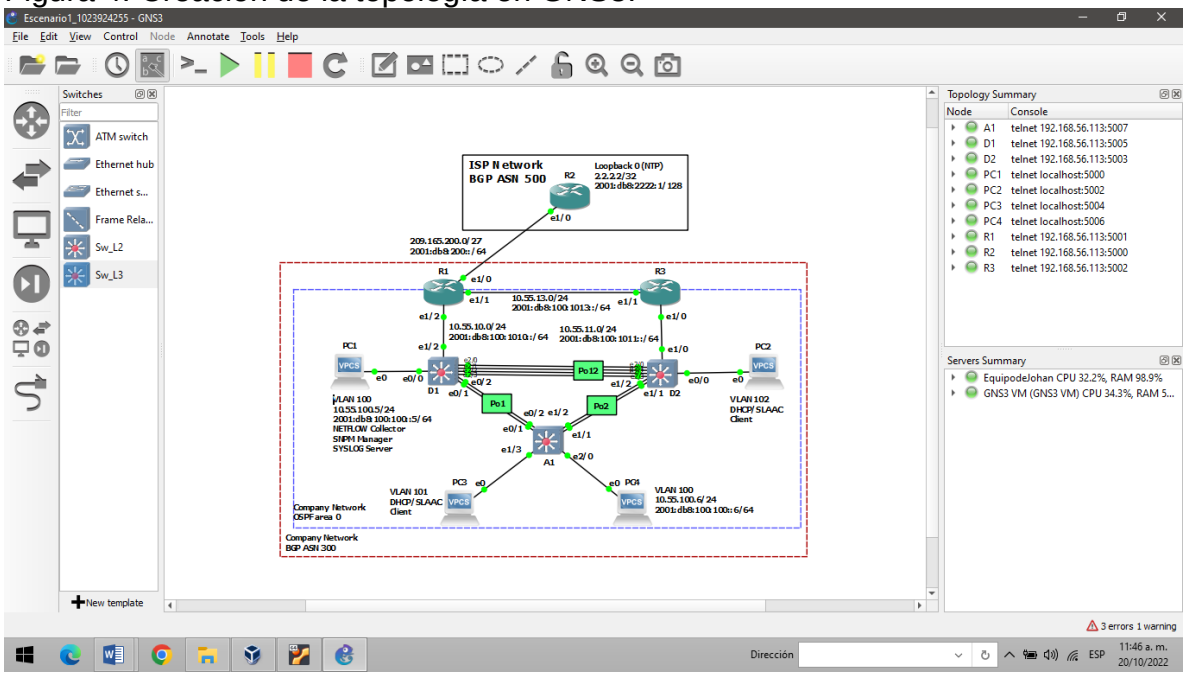
Fuente: Propia

Figura 3. Configuración de los Slot en los Switches



Fuente: Propia

Figura 4. Creación de la topología en GNS3.



Fuente: Autoría propia

1.1.2 PARTE 2: CONFIGURACION DE LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DE SUS INTERFACES

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 aplicando los siguientes comandos:

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 10.55.10.1 255.255.255.0
#ipv6 address fe80::1:2 link-local
#ipv6 address 2001:db8:100:1010::1/64
#no shutdown
#exit
#interface e1/1
#ip address 10.55.13.1 255.255.255.0
#ipv6 address fe80::1:3 link-local
#ipv6 address 2001:db8:100:1013::1/64
#no shutdown
#exit

Después de escribir en el Router R1 los comandos anteriores, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas por medio del comando

#copy running-config startup-config

Figura 5. Guardando las configuraciones en el Router R1

Fuente: Autoría propia

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

Después de escribir en el Router R2 los comandos anteriores, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas por medio del comando

#copy running-config startup-config

Figura 6. Guardando las configuraciones en el Router R2

Fuente: Autoría propia

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 10.55.11.1 255.255.255.0
#ipv6 address fe80::3:2 link-local
#ipv6 address 2001:db8:100:1011::1/64
#no shutdown
#exit
#interface e1/1
#ip address 10.55.13.3 255.255.255.0
#ipv6 address fe80::3:3 link-local
#ipv6 address 2001:db8:100:1010::2/64
#no shutdown
#exit

Después de escribir en el Router R3 los comandos anteriores, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas por medio del comando

#copy running-config startup-config

Figura 7. Guardando las configuraciones en el Router R3

Fuente: Autoría propia

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 10.55.10.2 255.255.255.0
#ipv6 address fe80::d1:1 link-local
#ipv6 address 2001:db8:100:1010::2/64
#no shutdown

```
#exit
#interface vlan 100
#ip address 10.55.100.1 255.255.255.0
#ipv6 address fe80::d1:2 link-local
#ipv6 address 2001:db8:100:100::1/64
#no shutdown
#exit
#interface vlan 101
#ip address 10.55.101.1 255.255.255.0
#ipv6 address fe80::d1:3 link-local
#ipv6 address 2001:db8:100:101::1/64
#no shutdown
#exit
#interface vlan 102
#ip address 10.55.102.1 255.255.255.0
#ipv6 address fe80::d1:4 link-local
#ipv6 address 2001:db8:100:102::1/64
#no shutdown
#exit
#ip dhcp excluded-address 10.55.101.1 10.55.101.109
#ip dhcp excluded-address 10.55.101.141 10.55.101.254
#ip dhcp excluded-address 10.55.102.1 10.55.102.109
#ip dhcp excluded-address 10.55.102.141 10.55.102.254
#ip dhcp pool VLAN-101
#network 10.55.101.0 255.255.255.0
#default-router 10.55.101.254
#exit
#ip dhcp pool VLAN-102
#network 10.55.102.0 255.255.255.0
#default-router 10.55.102.254
#exit
#interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
#shutdown
#exit
```

Después de escribir en el Switch D1 los comandos anteriores, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas por medio del comando

#copy running-config startup-config

Figura 8. Guardando las configuraciones en el Switch D1

Fuente: Autoría propia

Switch D2

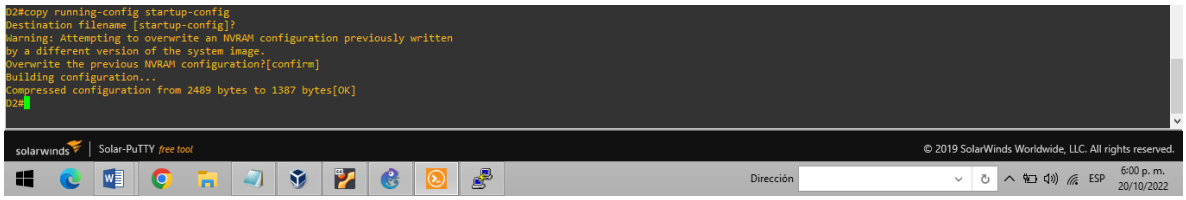
#hostname D2
#ip routing
#ipv6 unicast-routing
#no ip domain lookup
#banner motd # D2, ENCOR Skills Assessment#
#line con 0
#exec-timeout 0 0
#logging synchronous
#exit
#vlan 100
#name Management
#exit
#vlan 101
#name UserGroupA
#exit
#vlan 102
#name UserGroupB
#exit
#vlan 999
#name NATIVE
#exit
#interface e1/0
#no switchport
#ip address 10.55.11.2 255.255.255.0
#ipv6 address fe80::d1:1 link-local
#ipv6 address 2001:db8:100:1011::2/64
#no shutdown
#exit
#interface vlan 100
#ip address 10.55.100.2 255.255.255.0
#ipv6 address fe80::d2:2 link-local
#ipv6 address 2001:db8:100:100::2/64
#no shutdown
#exit
#interface vlan 101

#ip address 10.55.101.2 255.255.255.0
#ipv6 address fe80::d2:3 link-local
#ipv6 address 2001:db8:100:101::2/64
#no shutdown
#exit
#interface vlan 102
#ip address 10.55.102.2 255.255.255.0
#ipv6 address fe80::d2:4 link-local
#ipv6 address 2001:db8:100:102::2/64
#no shutdown
#exit
#ip dhcp excluded-address 10.55.101.1 10.55.101.209
#ip dhcp excluded-address 10.55.101.241 10.55.101.254
#ip dhcp excluded-address 10.55.102.1 10.55.102.209
#ip dhcp excluded-address 10.55.102.241 10.55.102.254
#ip dhcp pool VLAN-101
#network 10.55.101.0 255.255.255.0
#default-router 10.55.101.254
#exit
#ip dhcp pool VLAN-102
#network 10.55.102.0 255.255.255.0
#default-router 10.55.102.254
#exit
#interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
#shutdown
#exit

Después de escribir en el Switch D2 los comandos anteriores, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas por medio del comando

#copy running-config startup-config

Figura 9. Guardando las configuraciones en el Switch D2



Fuente: Autoría propia

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 10.55.100.3 255.255.255.0
#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

Después de escribir en el Switch A1 los comandos anteriores, se pasa las líneas de configuración de la RAM a la NVRAM para ser almacenadas por medio del comando

#copy running-config startup-config

Figura 10. Guardando las configuraciones en el Switch A1

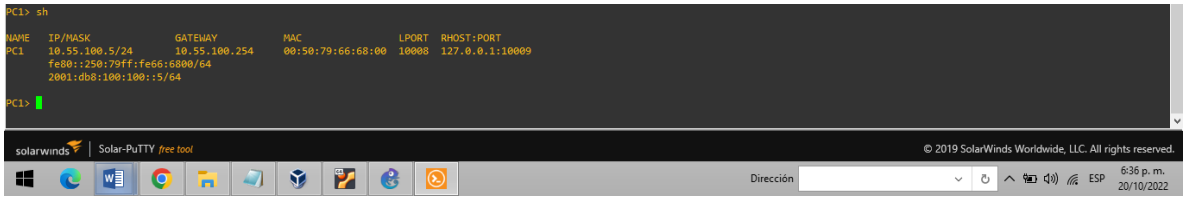
Fuente: Autoría propia

Se asignan las direcciones IPv4 e IPv6 en PC1 y PC4, que se encuentran en la tabla 1, con la respectiva puerta de enlace 10.55.100.254; esta puerta de enlace será la

dirección IP virtual HSRP. Por consiguiente a través de las siguientes figuras al emitir el comando sh se observa la dirección IP previamente configurada.

> ip 10.55.100.5/24 10.55.100.254

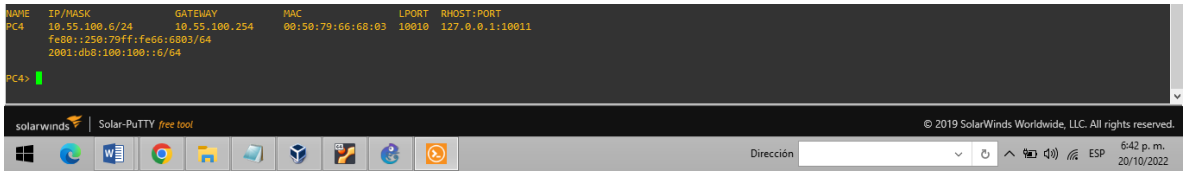
Figura 11. Asignación de direccionamiento IPv4 e IPv6 a PC1.



Fuente: Autoría propia

> ip 10.55.100.6/24 10.55.100.254

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



Fuente: Autoría propia

1.1.3 PARTE 3: CONFIGURACION DE LA RED DE CAPA 2 Y LA COMPATIBILIDAD CON EL HOST

En esta parte se 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, por ello se seguirá el siguiente procedimiento

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

Asimismo en todos los switches, se configura la VLAN 999 como la VLAN nativa, para ello se usan 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

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

Seguidamente en todos los switches se habilita el protocolo Rapid Spanning-Tree (RSTP) Use Rapid Spanning Tree (RSPT)

#spanning-tree mode rapid-pvst

En D1 y D2, se configuran los puentes raíz RSTP (root bridges) según la información del diagrama de topología de la figura 1. 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

Switch D2
#spanning-tree vlan 101 root primary
#spanning-tree vlan 100,102 root secondary

En todos los switches, se crean EtherChannels LACP como se muestra en el diagrama de topología de la figura 1. 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

Posteriormente en todos los switches, se configura los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4. Se configura los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología de la figura 1. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

Switch D1
#interface e0/0
#switch mode access
#switch access vlan 100
#spanning-tree portfast
#no shutdown
#exit

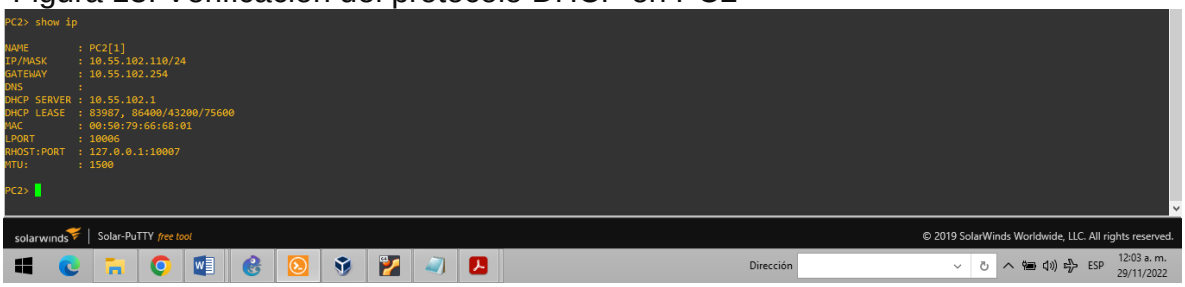
Switch D2
#interface e0/0
#switch mode access
#switch access vlan 102
#spanning-tree portfast
#no shutdown
#exit

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

En esta parte por último se realizan las verificaciones correspondientes, se verifican los servicios DHCP IPv4 PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

PC2> ip dhcp
IP 10.55.102.110/24 GW 10.55.102.254

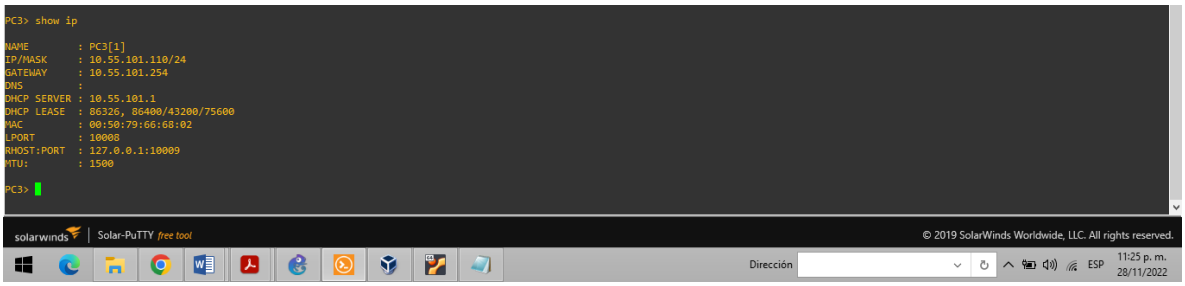
Figura 13. Verificación del protocolo DHCP en PC2



Fuente: Autoría propia

PC3> ip dhcp
IP 10.55.101.110/24 GW 10.55.101.254

Figura 14. Verificación del protocolo DHCP en PC3



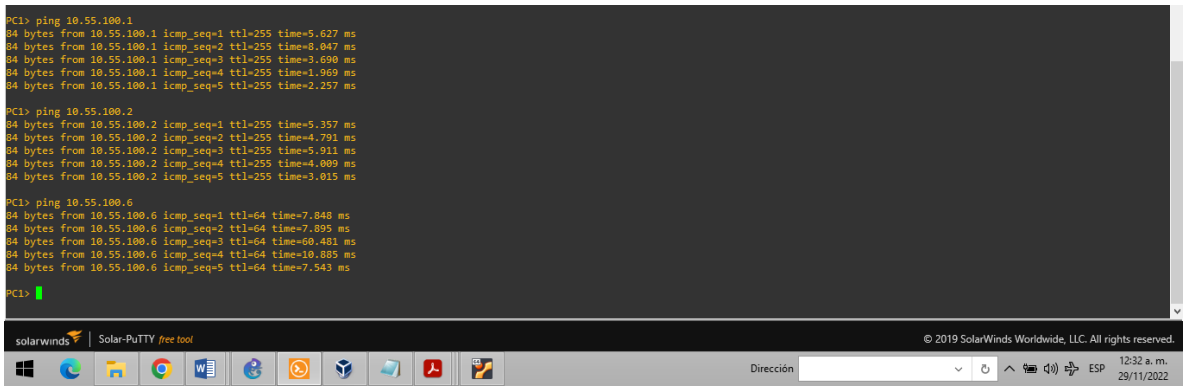
Fuente: Autoría propia

Por medio del comando ping podemos probar la conectividad para verificar la conectividad de la LAN local de cada PC

Verificación de conexión desde PC1

- D1: 10.55.100.1
- D2: 10.55.100.2
- PC4: 10.55.100.6

Figura 15. Verificación de conexión desde PC1



Fuente: Autoría propia

Verificación de conexión desde PC2

- D1: 10.55.102.1
- D2: 10.55.102.2

Figura 16. Verificación de conexión desde PC2

Fuente: Autoría propia

Verificación de conexión desde PC3

- D1: 10.55.101.1
- D2: 10.55.101.2

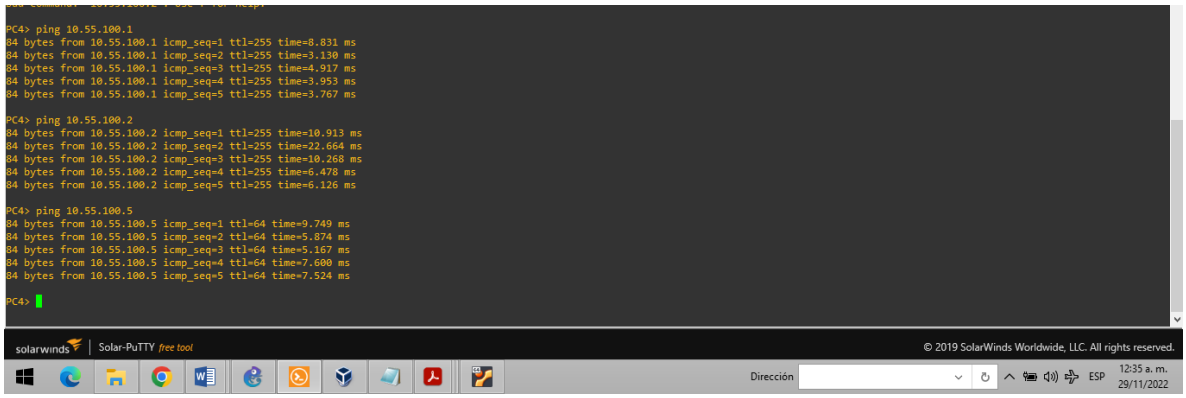
Figura 17. Verificación de conexión desde PC3

Fuente: Autoría propia

Verificación de conexión desde PC4

- D1: 10.55.100.1
- D2: 10.55.100.2
- PC1: 10.55.100.5

Figura 18. Verificación de conexión desde PC4



Fuente: Autoría propia

1.1.4 PARTE 4: CONFIGURACION DE LOS PROTOCOLOS DE ENRUTAMIENTO

En esta parte se configuran los protocolos de enrutamiento Ipv4 e Ipv6. Teniendo presente que al final la red será convergente completamente; es decir tendrá todos sus servicios activos, ya que los pings de la interfaz loopback 0 desde D1 y D2 serán exitosos. Por ello se seguirá el siguiente procedimiento:

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 10.55.10.0 0.0.0.255 area 0
#network 10.55.13.0 0.0.0.255 area 0
#network 209.165.200.0 0.0.0.31 area 0
#default-information originate

Router R3
#router ospf 4
#router-id 0.0.4.3
#network 10.55.11.0 0.0.0.255 area 0
#network 10.55.13.0 0.0.0.255 area 0

Switch D1
#router ospf 4
#router-id 0.0.4.131
#passive-interface default
#no passive-interface e1/2
#network 10.55.10.0 0.0.0.255 area 0
#network 10.55.100.0 0.0.0.255 area 0
#network 10.55.101.0 0.0.0.255 area 0
#network 10.55.102.0 0.0.0.255 area 0

Switch D2
#router ospf 4
#router-id 0.0.4.132
#passive-interface default
#no passive-interface e1/0
#network 10.55.11.0 0.0.0.255 area 0
#network 10.55.100.0 0.0.0.255 area 0
#network 10.55.101.0 0.0.0.255 area 0
#network 10.55.102.0 0.0.0.255 area 0

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

Posteriormente 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 en la 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 10.55.0.0/8.
- 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 10.55.0.0/8.

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 10.55.0.0 255.0.0.0 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 10.55.0.0 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
```

1.1.5 PARTE 5: 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.

Switch D1
#ip sla 4
#icmp-echo 10.55.10.1
source-ip 10.55.10.2
#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

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
#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.

Switch D2
#ip sla 4
#icmp-echo 10.55.11.1 source-interface e1/0
#frequency 5
#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

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
#track 4 ip sla 4 reachability
#delay down 10 up 15
#track 6 ip sla 6 reachability
#delay down 10 up 15

Seguidamente en esta parte en D1, se configura HSRPv2 para 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 10.30.100.254.
- 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 10.55.101.254.
- 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 10.55.102.254.
- 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 10.55.100.254

```
#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 10.55.101.254
#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 10.55.102.254
#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 10.55.100.254.
- 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 10.55.101.254.
- 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 10.55.102.254.
- 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 10.55.100.254
#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 10.55.101.254
#standby 114 priority 150
#standby 114 preempt
```

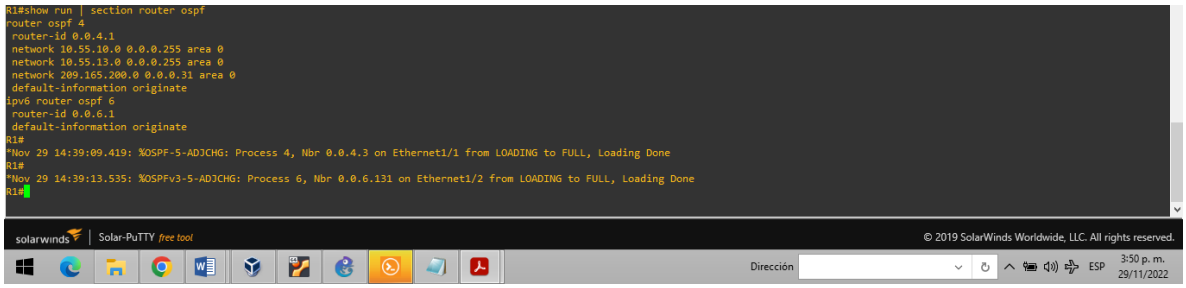
#standby 114 track 4 decrement 60
#standby 116 ipv6 autoconfig
#standby 116 priority 150
#standby 116 preempt
#standby 116 track 6 decrement 60
#exit
#interface vlan 102
#standby version 2
#standby 124 ip 10.55.102.254
#standby 124 preempt
#standby 124 track 4 decrement 60
#standby 126 ipv6 autoconfig
#standby 126 preempt
#standby 126 track 6 decrement 60
#exit

1.1.6 PARTE 6: VERIFICACIÓN DE LA CONFIGURACIÓN OSPF

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); se emiten los siguientes comandos de verificación:

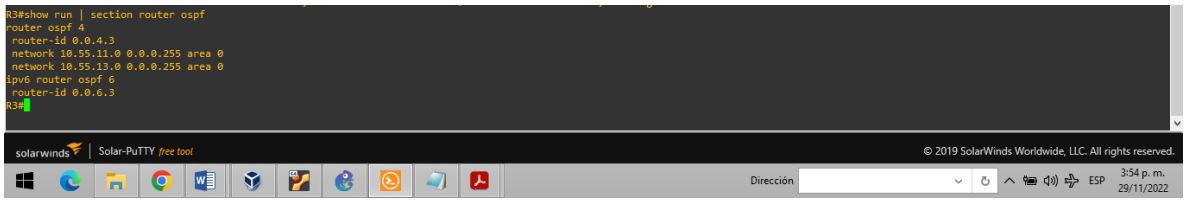
#show run | section router ospf

Figura 19. Verificación de la configuración OSPF en R1



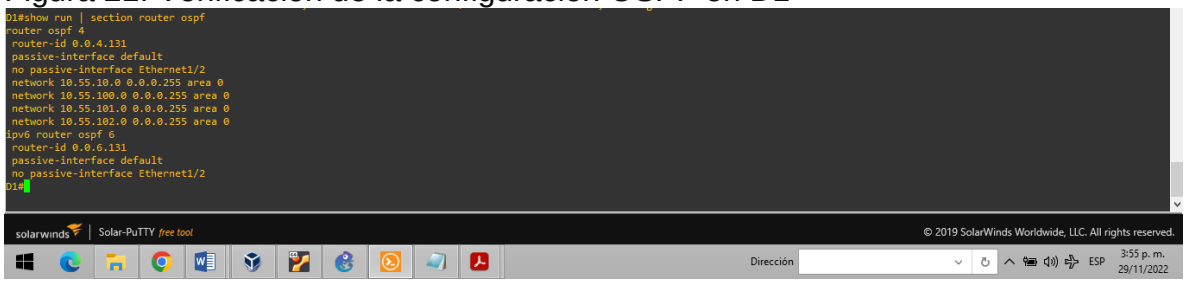
Fuente: propia

Figura 20. Verificación de la configuración OSPF en R3



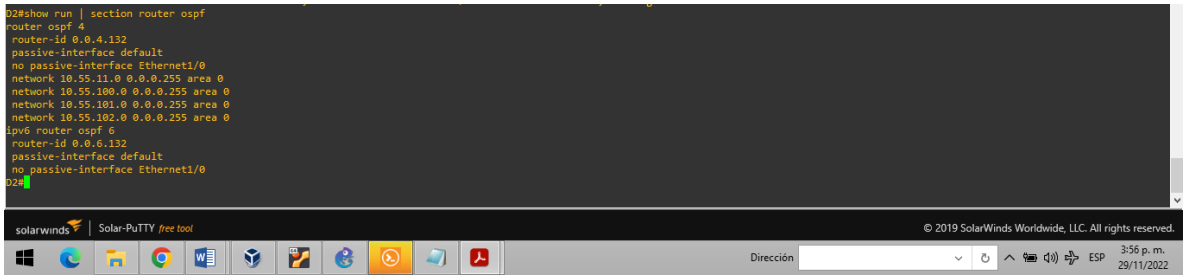
Fuente: propia

Figura 21. Verificación de la configuración OSPF en D1



Fuente: propia

Figura 22. Verificación de la configuración OSPF en D2



Fuente: propia

1.1.7 PARTE 7: VERIFICACIÓN DE LA CONFIGURACIÓN BGP

Para realizar la respectiva verificación de la configuración en el router R1 y R2, se emite el siguiente comando

#show run | section bgp

Figura 23. Verificación de la configuración BGP en R1

Fuente: propia

Figura 24. Verificación de la configuración BGP en R2

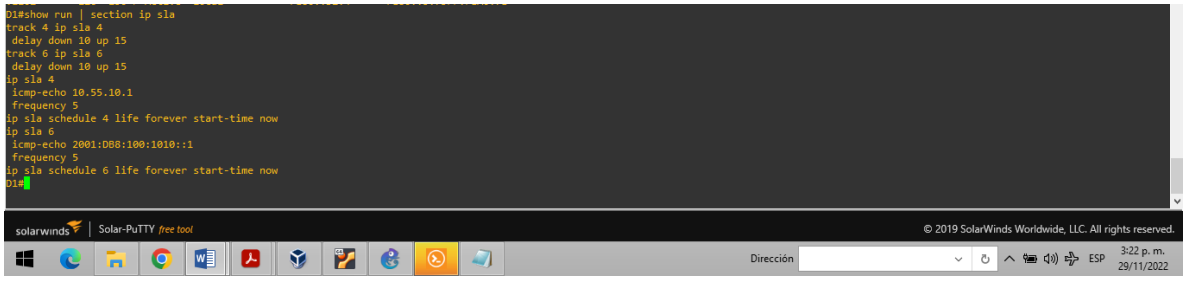
Fuente: propia

1.1.8 PARTE 8: VERIFICACIÓN DE LA CONFIGURACIÓN IP SLA

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

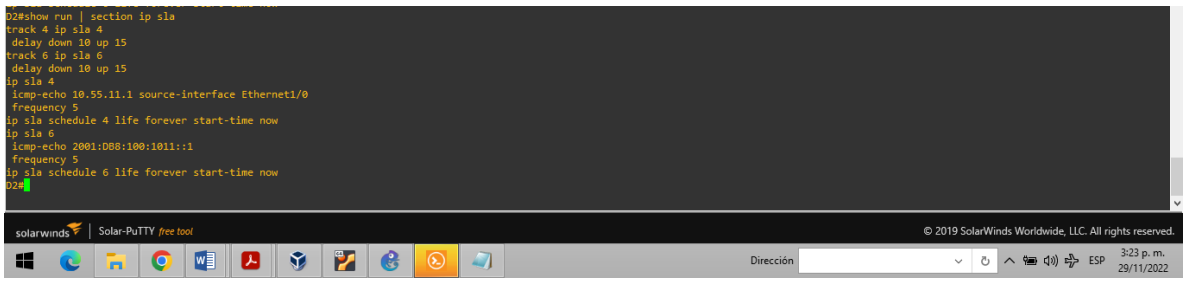
#show run | section ip sla

Figura 25. Verificación de la configuración IP SLA en D1



Fuente: propia

Figura 26. Verificación de la configuración IP SLA en D2

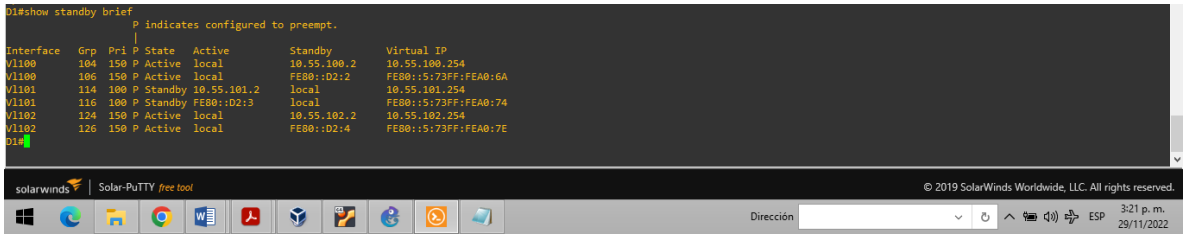


Fuente: propia

Seguidamente se verifica la configuración HSRP en D1 y D2

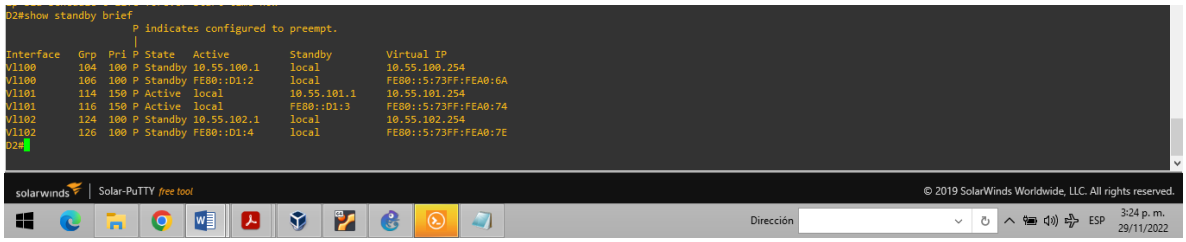
#show standby brief

Figura 27. Verificación de HSRP en D1



Fuente: propia

Figura 28. Verificación de HSRP en D2



Fuente: propia

CONCLUSIONES

Con el desarrollo del actual trabajo, se logró fortalecer los conocimientos necesarios y básicos para el correcto funcionamiento del simulador GNS3 y de la configuración de redes; de esta manera se adquirieron las bases y habilidades para configurar, analizar, diagnosticar y corregir problemas a nivel de red y a nivel de configuración de los dispositivos que la conforman.

Luego de realizar las configuraciones correspondientes a la red, se concluye la importancia de los protocolos de enrutamiento para poder enviar y recibir paquetes IP desde un dispositivo de origen hacia un dispositivo de destino que no necesariamente está cerca.

De igual manera, en el desarrollo del trabajo se pudo concluir la importancia que tiene la creación de Vlans en una red para no solamente crear y administrar estaciones de trabajo, sino también para cambiar de forma más fácil las configuraciones a las LAN y controlar el tráfico de red mejorando la seguridad de la red que es lo primordial.

Por otra parte se presentó un buen desenvolvimiento en la configuración de la red al utilizar el comando ping; una herramienta muy simple pero útil. Ya que este comando envía un paquete de solicitud del protocolo de mensajes de control de Internet al dispositivo de destino, que devuelve un paquete de respuesta y de esta forma aseguramos la comunicación efectiva entre los mismos. Asimismo el manejo de otros comandos como show ip route, show standby brief, show run entre otros permitieron realizar verificaciones específicas de las configuraciones y realizar de forma más fácil correcciones.

Por último se llega a la conclusión de que la configuración de red realizada nos acerca a tener una idea más sencilla y practica del desarrollo del ámbito laboral como profesional en las telecomunicaciones o profesional en electrónicas.

REFERENCIAS

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

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

UNAD (2020). Configuración de Switches y Routers [OVA]. https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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

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

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

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