DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS DIPLOMADO CCNP

ANDRES FELIPE PEÑA NAVARRETE

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS DIPLOMADO CCNP

ANDRES FELIPE PEÑA NAVARRETE

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

DIRECTOR

JUAN ESTEBAN TAPIAS BAENA

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

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

BOGOTA, 18 de noviembre de 2022

AGRADECIMIENTOS

Primeramente, a Dios, A mi familia que me apoyaron en todo para al ser un profesional, a mis tutores, compañeros y amigos que me alentaron a continuar y no desfallecer en el camino.

Contenido

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Cisco: es el modelo de arquitectura de computadores, diseños y pasos a seguir, en la implementación y configuración de dispositivos de enrutamiento como Routers, switch, Hub y otros, en una red ISP.

CCNP: Cisco Certified Networking professional, este certificado de especialización en redes y telecomunicaciones.

ENRUTAMIENTO: es la configuración de la tabla de enrutamiento que permite la comunican en los dispositivos de la red o nodos que están conectados para el acceso de la información en el tráfico de una red convergente.

REDES INFORMATICAS: Es el conjunto de ordenadores, tabletas, smartphone y otros dispositivos conectados en una red LAN, que intercambian datos, voz, video, aplicaciones y servicios.

ELECTRONICA: parte de la física que aprovecha el comportamiento de las cargas eléctricas que están presentes en los circuitos electrónicos de los dispositivos, estos circuitos son semiconductores en los aparatos electrónicos.

LACP: Link Aggregation Control Protocolo grupo de enlace virtual o trunking, que permite agrupar puertos físicos en un único canal lógico con el objetivo de aumentar el rendimiento, el switch interactúa el tráfico de paquetes en un grupo automático .

HSRP: Hot Standby Router protocol, protocolo de Cisco que despliega los enrutadores redundantes. Creando un Clúster maestro, que enruta el tráfico de red y se despliega en el enrutamiento de respaldo.

DHCP: protocolo de configuración dinámica de host (DHCP) cliente/servidor, que le permite proporcionar una dirección de host en forma automática enlazando el dispositivo encontrado a la red

RESUMEN

En el desarrollo de este informe de prueba de habilidades practicas se da solución a una problemática de una red corporativa que está compuesta por dos escenarios, en el primer escenario se realiza una configuración básica de los dispositivos Routers, switch y PCs que son los dispositivos más comunes que integran una red LAN y en el segundo escenario se configura los dispositivos de capa dos, (Switch) donde se crean las vlans, el enrutamiento OSPFv2 y OSPFv3, HSRP y la configuración BGP en los dispositivos que realizan el tráfico de paquetes en el extremo de la red.

Los protocolos OSPF, BGP, HSRP se encargan del tráfico de paquetes y están configurados con un enrutamiento IPv4 e IPv6 para ofrecer una red con alta velocidad, escalable y a prueba de fallos con el protocolo IP SLA que se encarga de evitar o disminuir la redundancia física de la red LAN.

Para realizar la Prueba de Habilidades es necesario el uso de simulador de red GNS3 y la máquina virtual VMGNS3 en Virtual Box, que permite realizar el diseño y la configuración de la red propuesta ENCOR SKILLS ASSESSMENT

En el desarrollo de los dos escenarios, se realiza las respectivas verificaciones del enrutamiento y configuración adecuado siguiendo los protocolos de enrutamiento de la tabla de direcciones y de la configuración básica, además de la implementación de los protocolos propuestos que se visualizan en screenshot simulando una red real demostrando su correcto funcionamiento en la red.

Palabras clave: Cisco, CCNP, enrutamiento Redes, Software, Electrónica, protocolos

ABSTRACT

In the development of this practical skills test report, a solution is given to a problem of a corporate network that is made up of two scenarios, in the first scenario a basic configuration of the router, switch and PC devices is carried out, which are the most important devices. common devices that make up a LAN network and in the second scenario, layer two devices are configured, (Switch) where the vlans, OSPFv2 and OSPFv3 routing, HSRP and BGP configuration are created in the devices that carry out the packet traffic in the end of the network.

The OSPF, BGP, HSRP protocols are in charge of the packet traffic and are configured with IPv4 and IPv6 routing to offer a high-speed, scalable and fail-safe network with the IP SLA protocol that is in charge of avoiding or reducing redundancy. physical LAN.

To carry out the Skills Test, it is necessary to use the GNS3 network simulator and the VMGNS3 virtual machine in Virtual Box, which allows designing and configuring the proposed network ENCOR SKILLS ASSESSMENT

In the development of the two scenarios, the respective verifications of the proper routing and configuration are carried out following the routing protocols of the address table and of the basic configuration, in addition to the implementation of the proposed protocols that are displayed in a screenshot simulating a network. real demonstrating its correct operation in the network.

Keywords: Cisco, CCNP, routing Networks, Software, Electronics, protocols

INTRODUCCIÓN

Este trabajo se desarrolla en el marco de las redes y situaciones que serán recurrentes para el futuro profesional en ingeniería en electrónica; la tecnologíaavanza a grandes pasos y las telecomunicaciones es un campo donde está totalmente inmerso para programación, conectividad y soluciones a diferentes situaciones.

Para la primera etapa se debe programar el direccionamiento IP de todos los dispositivos de la topología la cual comprende 3 Routers, 3 switches y 4 pcs paralo cual se configurará la dirección IPv4 y IPv6; 2 switches multicapa harán la conmutación con una VLAN independiente y sus enlaces redundantes, el otro switch será el punto de acceso trabajando con los enlaces LACP y el RSTP. Se configura para el IPv4 el OSPFv2 y para el IPv6 el OSPF para la red local;

finalmente se configura la conexión para los pcs con servicios ISP y se validara sufuncionamiento con ping entre los mismos para él envió y recepción de información.

En la segunda etapa ya con la base de la anterior se procede a configurar los protocolos de enrutamiento tanto en OSPFv2 como en OSPFv3 además de los parámetros de información para IPv6 para los Routers R1 y R2. Finalmente, se configura la redundancia del primer salto con una IP virtual proporcionada por el HSRPv2.

1. ESCENARIO 1

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

Figura 1. Escenario en gns3

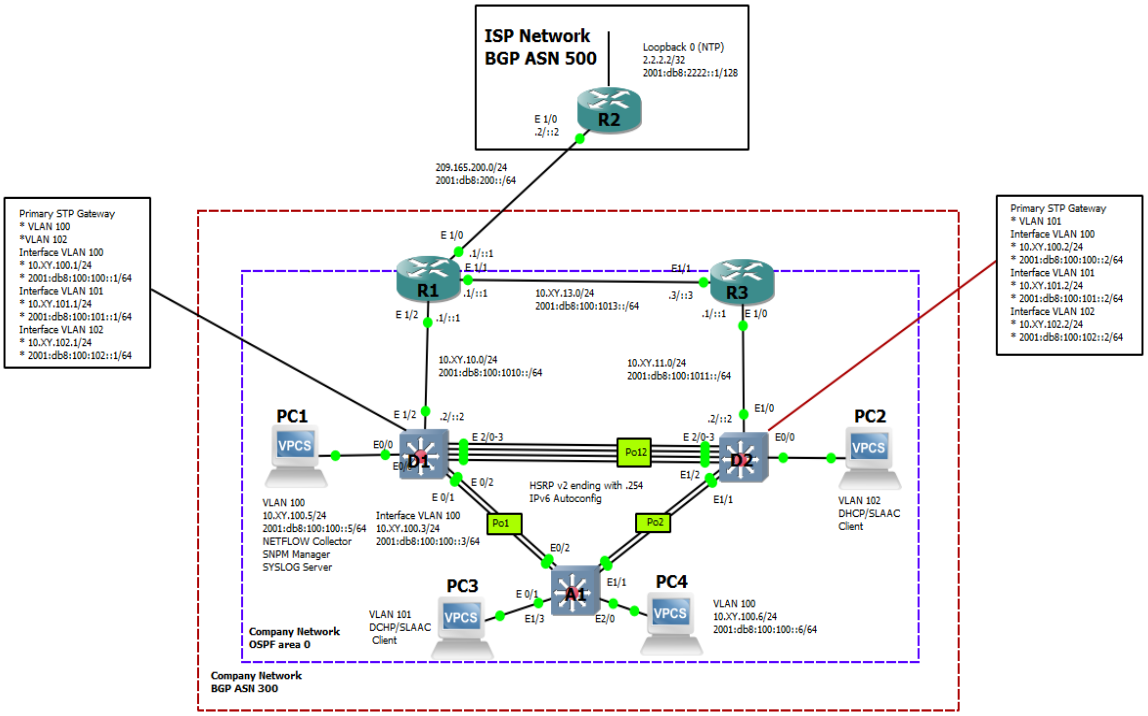


Tabla 1. Direccionamiento IP				
Device	**Interface**	**IPv4 address**	**Ipv6 Address**	**Ipv6 Link-local**
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10. 37.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10. 37.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	209.165.200.226/27	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. 37.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10. 37.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10. 37.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.37.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10. 37.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10. 37.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10. 37.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10. 37.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10. 37.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10. 37.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10. 37.100.3/23	2001:db8:100:100::3/64	fe80::a1:1

PC1	NIC	10. 37.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10. 37.100.6/24	2001:db8:100:100::6/64	EUI-64

Objetivos

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

Parte 2: Configurar la red de capa 2 y la compatibilidad con el host

Parte 3: Configurar protocolos de enrutamiento

Parte 4: Configurar la redundancia de primer salto

Antecedentes / Escenario

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

Los Routers utilizados con los laboratorios prácticos CCNP son Routers Cisco 7200. Los switches utilizados en los laboratorios son switches Cisco Catalyst L2 s Se pueden utilizar otros Routers, switches y versiones de Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y la salida producida pueden variar de lo que se muestra en los laboratorios.

Recursos requeridos

- 3 Routers (Cisco 7200).

- 3 switches (Cisco IOU L2).
- 4 PC (Utilice la VPCS de GNS3)

Paso 1. Cablee la red como se muestra en la topología.

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

Se realiza la configuración en el simulador GNS3 con las imágenes de Reuters 7200, los switches IOSvL2 y los respectivos PC

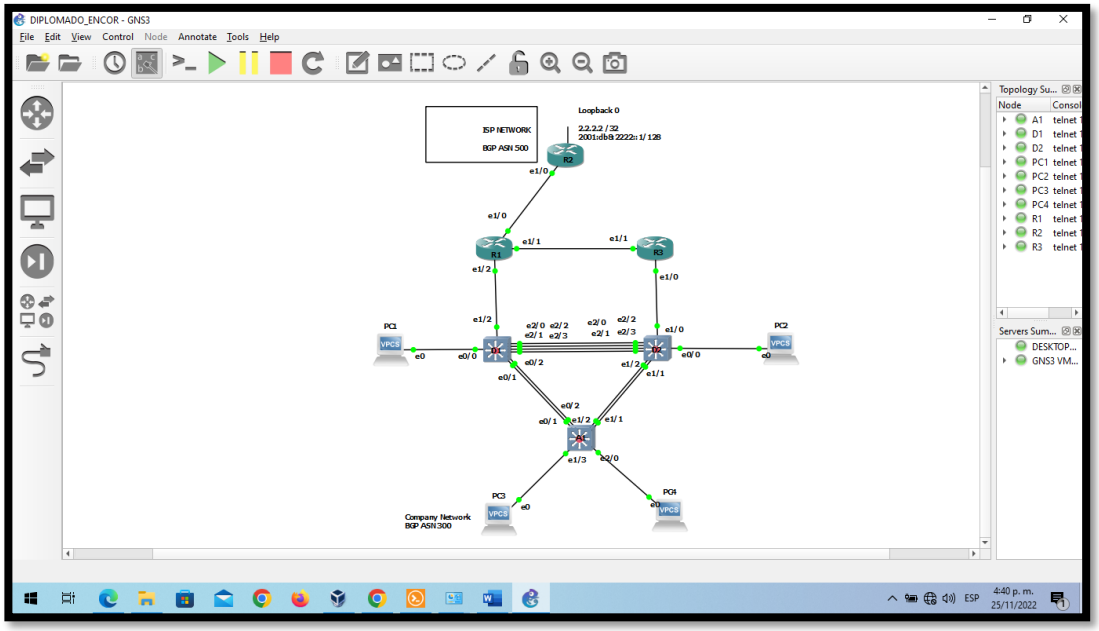
Los requisitos de hardware son:

Routers c7200-advipservicesk9-mz.152-4.S5

Switch CISCO IOSvL2

Diseño de la red

Figura 2 construcción del escenario en gns3



Paso 2: Configurar los parámetros básicos para cada dispositivo

Se configura los parámetros básicos de los dispositivos que forman la red comoson los nombres, las ip para las interfaces tanto IPv4 como IPv6, se crean las VLAN, un pool DHCP y sus exclusiones.

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 10.37.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface e1/1
ip address 10.37.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
copy run star
```

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
copy run star
```

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 10.37.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface e1/1
ip address 10.37.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
copy run star
```

Switch

```
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 10.37.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.37.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.37.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.37.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.37.101.1 10.37.101.109
ip dhcp excluded-address 10.37.101.141 10.37.101.254
ip dhcp excluded-address 10.37.102.1 10.37.102.109
ip dhcp excluded-address 10.37.102.141 10.37.102.254
ip dhcp pool VLAN-101
network 10.37.101.0 255.255.255.0
default-router 10.37.101.254
```

```
exit
ip dhcp pool VLAN-102
network 10.37.102.0 255.255.255.0
default-router 10.37.102.254
exit
interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
shutdown
exit
copy run starSwitch D2
```

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 10.37.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit

interface vlan 100
ip address 10.37.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.37.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.37.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.37.101.1 10.37.101.209
ip dhcp excluded-address 10.37.101.241 10.37.101.254
ip dhcp excluded-address 10.37.102.1 10.37.102.209
ip dhcp excluded-address 10.37.102.241 10.37.102.254
ip dhcp pool VLAN-101
network 10.37.101.0 255.255.255.0
default-router 10.37.101.254
exit
ip dhcp pool VLAN-102
```

```
network 10.37.102.0 255.255.255.0
default-router 10.37.102.254
exit
interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
shutdown
exit
copy run star
```

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 10.37.100.3 255.255.255.0
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
copy run star
```

Guarde la configuración en ejecución en startup-config en todos los dispositivos. R1, R2, R3, D1, D2,

Comandos en:

R1

```
R1#copy running-config startup-config
```

R2

```
R2#copy running-config startup-config
```

R3

```
R3#copy running-config startup-config
```

D1

```
D1#copy running-config startup-config
```

A1

```
A1#copy running-config startup-config
```

D2

```
D2#copy running-config startup-config
```

Paso 3: Configuración del direccionamiento de los PC1 y PC4

la tabla de direccionamiento asigna una dirección de puerta de enlace predeterminada de 10.37.100.254, que será la dirección IP virtual HSRP utilizada en la Parte 4.

Pc1: ip 10.37.100.5/24 10.37.100.254
save

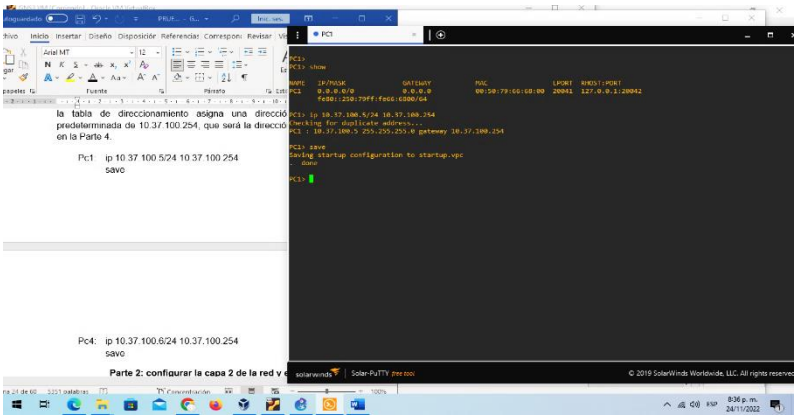


Figura 3. Configuración en PC1

Pc4: ip 10.37.100.6/24 10.37.100.254
save

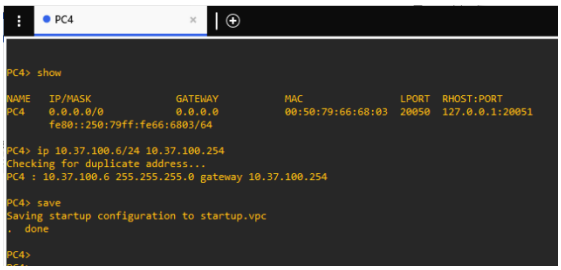


Figura 4. Configuración en PC4

Parte 2: configurar la capa 2 de la red y el soporte del host

Paso 1: En todos los switches configurar las interfaces troncales IEEE 802.1Q

Habilitar los vínculos troncales 802.1Q

Switch D1

```
conf term
interface range e2/0-3, e0/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

Switch D2

```
conf term
interface range e2/0-3, e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

Switch A1

```
conf term
interface range e0/1-2, e1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
exit
```

Paso 2: En todos los switches cambiar la VLAN nativa en los enlaces troncales por la VLAN 999 como VLAN native

Switch D1

```
interface range e2/0-3, e0/1-2
switchport trunk native vlan 999
exit
```

Switch D2

```
interface range e2/0-3, e1/1-2
switchport trunk native vlan 999
exit
```

Switch A1

```
interface range e0/1-2, e1/1-2
switchport trunk native vlan 999
exit
```

Paso 3: En todos los switches habilitar el protocolo spanning-Tree protocol

Switch D1

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

Switch D2

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

Switch A1

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

Paso 4: En D1 y D2 configurar apropiadamente el RSTP basado en el diagramade topología

En D1 y D2 se proporciona copia de seguridad en caso de latencia en puente raíz.

Switch D1

```
spanning-tree vlan 100 root primary
spanning-tree vlan 102 root primary
spanning-tree vlan 101 root secondary
```

Switch D2

```
spanning-tree vlan 101 root primary
spanning-tree vlan 100 root primary
spanning-tree vlan 102 root secondary
```

Paso 5: En todos los switches crear LACP Etherchannels como se muestra en eldiagrama de topología.

Se utiliza los números de canal para:
D1 a D2 – Canal del puerto 12
D1 a A1 – Canal de puerto 1
D2 a A1 – Canal de puerto 2

Switch D1

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

Switch D2

```
interface range e2/0-3
channel-protocol lacp
channel-group 12 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
exit
interface range e1/1-2
channel-protocol lacp
channel-group 2 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
```

Switch A1

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

channel-protocol lacp
channel-group 2 mode passive
exit
interface port-channel 2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 100-102
switchport mode trunk
exit

Paso 6: En todos los switches configurar los puertos de acceso del host que se conectan al PC1, PC2, PC3 y PC4

Se sigue el enrutamiento como se muestra en el diagrama de la topología, los puertos de host pasan al estado de reenvío

Switch D1

interface e0/0
switchport mode access
switchport access vlan 100

Switch D2

interface e0/0
switchport mode access
switchport access vlan 102

Switch A1

interface e1/3
switchport mode access
switchport access vlan 101
exit
interface e2/0
switchport mode access
switchport access vlan 100
exit

Paso 7: Verificar los servicios DHCP IPv4

PC2 y PC3 son clientes DHCP y reciben direcciones dentro de la red.

Pc2

Pc2>ip dhcp

IP: 10.37.102.110/24
GW: 10.37.101.254

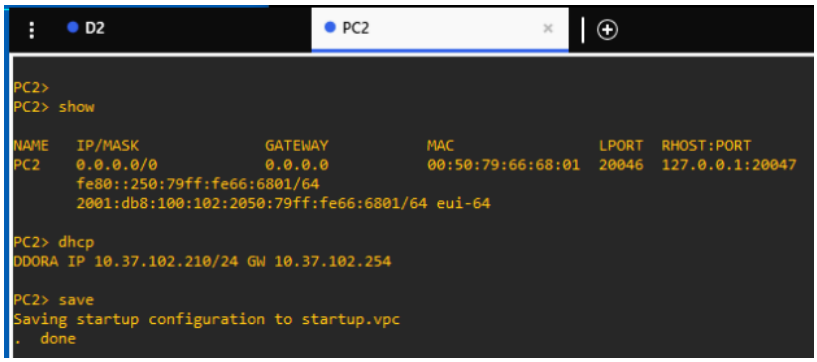


Figura 5. Configuración dhcp en Pc2

Pc3

Pc3>ip dhcp

IP: 10.37.101.110/24
GW: 10.37.101.254

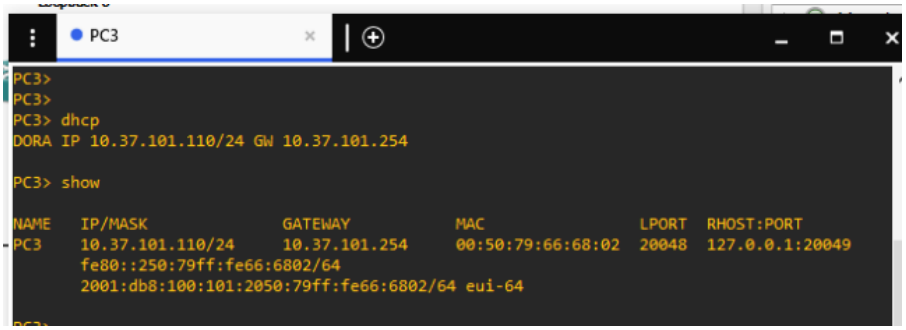


Figura 6. Configuración dhcp en Pc3

Paso 8: Verificar la conectividad LAN Local

PC1 hace ping correctamente:

- D1: 10.37.100.1
- D2: 10.37.100.2
- PC4: 10.37.100.6

PC1> ping 10.37.100.1
84bytes from 10.37.100.1 icmp_seq=1 ttl=255 time=751.055 ms
84bytes from 10.37.100.1 icmp_seq=2 ttl=255 time=329.231 ms
84bytes from 10.37.100.1 icmp_seq=3 ttl=255 time=135.005 ms
84bytes from 10.37.100.1 icmp_seq=4 ttl=255 time=181.045 ms
84bytes from 10.37.100.1 icmp_seq=5 ttl=255 time=321.755 ms

PC1> ping 10.37.100.2
84 bytes from 10.37.100.2 icmp_seq=1 ttl=255 time=245.187 ms
84 bytes from 10.37.100.2 icmp_seq=2 ttl=255 time=201.524 ms
84 bytes from 10.37.100.2 icmp_seq=3 ttl=255 time=127.233ms
84 bytes from 10.37.100.2 icmp_seq=4 ttl=255 time=139.244 ms
84 bytes from 10.37.100.2 icmp_seq=5 ttl=255 time=222.412 ms

PC1> ping 10.37.100.6
84 bytes from 10.37.100.6 icmp_seq=1 ttl=64 time=59.326 ms
84 bytes from 10.37.100.6 icmp_seq=2 ttl=64 time=59.254 ms
84 bytes from 10.37.100.6 icmp_seq=3 ttl=64 time=62.015 ms
84 bytes from 10.37.100.6 icmp_seq=4 ttl=64 time=77.895 ms
84 bytes from 10.37.100.6 icmp_seq=5 ttl=64 time=81.278 ms

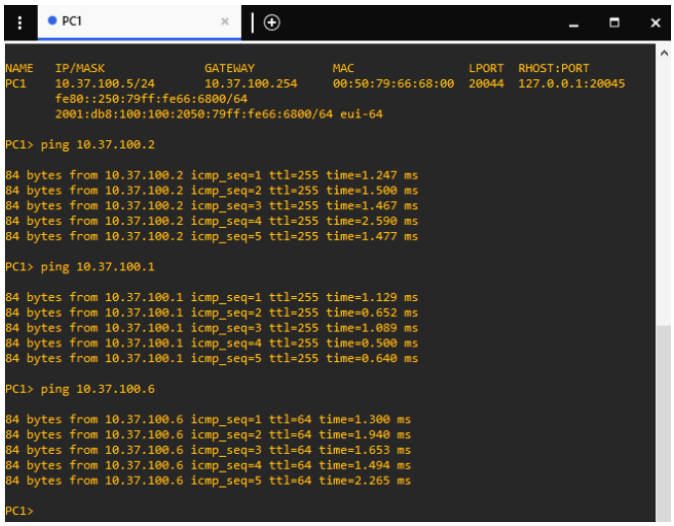


Figura 7. Ping de Pc1 a D1, D2 , Pc4

PC2 hace ping correctamente:

- D1: 10.37.102.1
- D2: 10.37.102.2

PC2> ping 10.37.102.1
84 bytes from 10.37.102.1 icmp_seq=1 ttl=255 time=211.233 ms
84 bytes from 10.37.102.1 icmp_seq=2 ttl=255 time=453.257 ms
84 bytes from 10.37.102.1 icmp_seq=3 ttl=255 time=352.107 ms
84 bytes from 10.37.102.1 icmp_seq=4 ttl=255 time=483.110 ms
84 bytes from 10.37.102.1 icmp_seq=5 ttl=255 time=287.014 ms

PC2> ping 10.37.102.2

84 bytes from 10.37.102.2 icmp_seq=1 ttl=255 time=305.647 ms
84 bytes from 10.37.102.2 icmp_seq=2 ttl=255 time=407.245 ms
84 bytes from 10.37.102.2 icmp_seq=3 ttl=255 time=411.652 ms
84 bytes from 10.37.102.2 icmp_seq=4 ttl=255 time=223.166 ms
84 bytes from 10.37.102.2 icmp_seq=5 ttl=255 time=184.104 ms

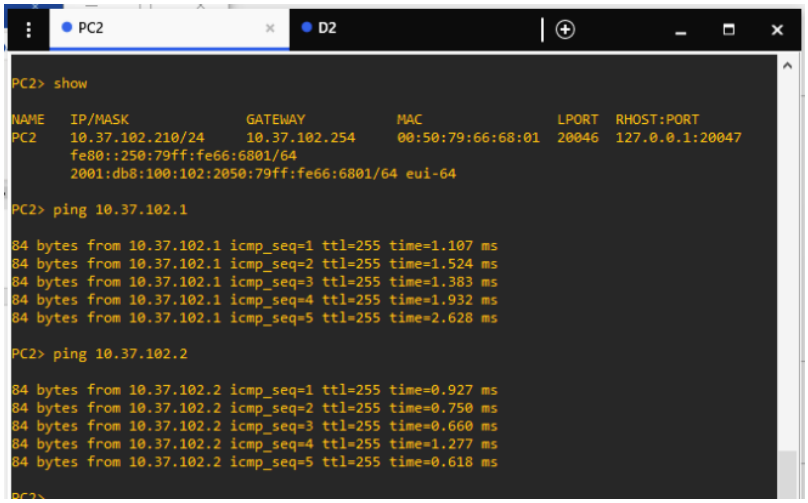


Figura 8. Ping de Pc2 a D1 y D2

PC3 hace ping correctamente:

- D1: 10.37.101.1
- D2: 10.37.101.2

PC3> ping 10.37.101.1
84 bytes from 10.37.101.1 icmp_seq=1 ttl=255 time=197.241 ms
84 bytes from 10.37.101.1 icmp_seq=2 ttl=255 time=252.122 ms
84 bytes from 10.37.101.1 icmp_seq=3 ttl=255 time=263.879 ms
84 bytes from 10.37.101.1 icmp_seq=4 ttl=255 time=211.874 ms
84 bytes from 10.37.101.1 icmp_seq=5 ttl=255 time=187.014 ms

PC3> ping 10.37.101.2
84 bytes from 10.37.101.2 icmp_seq=1 ttl=255 time=128.004 ms
84 bytes from 10.37.101.2 icmp_seq=2 ttl=255 time=140.586 ms
84 bytes from 10.37.101.2 icmp_seq=3 ttl=255 time=243.751 ms
84 bytes from 10.37.101.2 icmp_seq=4 ttl=255 time=117.587 ms
84 bytes from 10.37.101.2 icmp_seq=5 ttl=255 time=78.254 ms

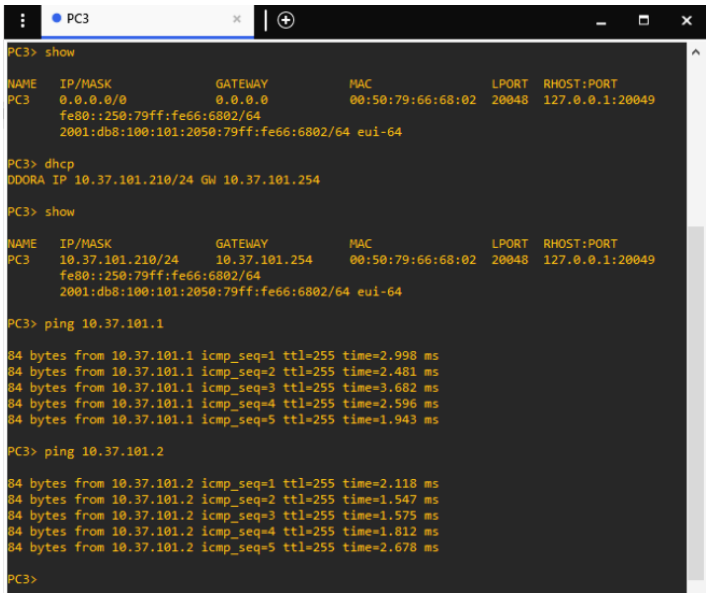


Figura 9. Ping de Pc3 a D1 y D2

PC4 debería hacer ping correctamente:

- D1: 10.37.100.1
- D2: 10.37.100.2
- PC1: 10.37.100.5

PC4> ping 10.37.100.1
84 bytes from 10.37.100.1 icmp_seq=1 ttl=255 time=261.1541ms
84 bytes from 10.37.100.1 icmp_seq=2 ttl=255 time=256.520 ms
84 bytes from 10.37.100.1 icmp_seq=3 ttl=255 time=308.512 ms
84 bytes from 10.37.100.1 icmp_seq=4 ttl=255 time=341.510 ms
84 bytes from 10.37.100.1 icmp_seq=5 ttl=255 time=305.482 ms

PC4> ping 10.37.100.2
84 bytes from 10.37.100.2 icmp_seq=1 ttl=255 time=302.379 ms
84 bytes from 10.37.100.2 icmp_seq=2 ttl=255 time=298.774 ms
84 bytes from 10.37.100.2 icmp_seq=3 ttl=255 time=126.132 ms
84 bytes from 10.37.100.2 icmp_seq=4 ttl=255 time=365.701 ms
84 bytes from 10.37.100.2 icmp_seq=5 ttl=255 time=227.042 ms

PC4> ping 10.37.100.5
84 bytes from 10.37.100.5 icmp_seq=1 ttl=64 time=37.578 ms
84 bytes from 10.37.100.5 icmp_seq=2 ttl=64 time=82.945 ms
84 bytes from 10.37.100.5 icmp_seq=3 ttl=64 time=82.581 ms
84 bytes from 10.37.100.5 icmp_seq=4 ttl=64 time=91.221 ms
84 bytes from 10.37.100.5 icmp_seq=5 ttl=64 time=87.658 ms

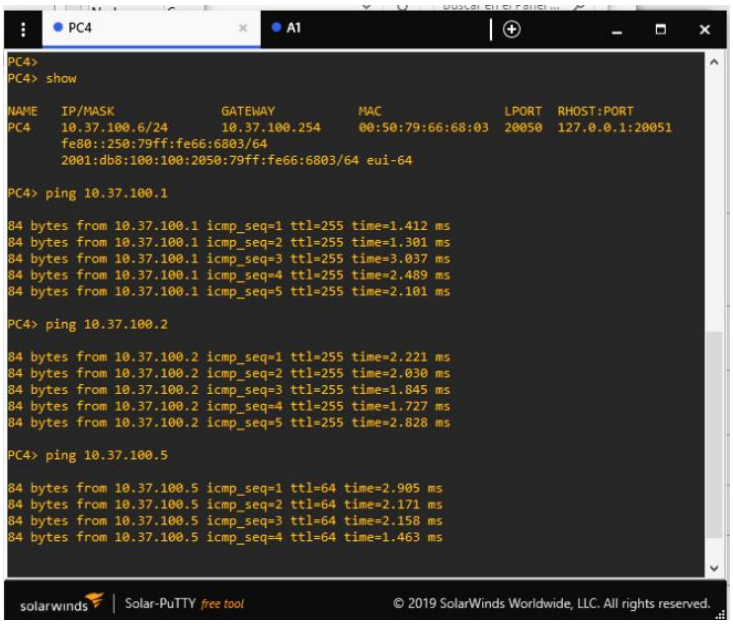


Figura 10. Ping de Pc3 a D1, D2 y Pc1

2. ESCENARIO 2

Parte 3: Configurar protocolos de enrutamiento

Se configura los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debe ser completamente convergente.
Los pings IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 se realiza correctamente al final de la configuración.
Los pings de los hosts no se realizarán correctamente porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Paso 1: En la “Company Network” configurar OSPFv2 en el área 0

Asigne lo ID 4

En R1: 0.0.4.1

Router R1

Show ip route connected

conf term

router ospf 4

router-id 0.0.4.1

network 10.37.10.0 0.0.0.255 area 0

network 10.37.13.0 0.0.0.255 area 0

network 209.165.200.0 0.0.0.31 area 0

default-information originate
exit

En R3: 0.0.4.3

Router R3

Show ip route connected

conf term

router ospf 4

router-id 0.0.4.3

network 10.37.11.0 0.0.0.255 area 0

network 10.37.13.0 0.0.0.255 area 0

exit

copy run star

En D1: 0.0.4.131

Switch D1

Show ip route connected

conf term

router ospf 4

router-id 0.0.4.131

network 10.37.10.0 0.0.0.255 area 0

network 10.37.100.0 0.0.0.255 area 0

network 10.37.101.0 0.0.0.255 area 0

network 10.37.102.0 0.0.0.255 area 0

passive-interface default

no passive-interface e1/2

exit

copy run star

En D2: 0.0.4.132

Switch D2

Show ip route connected

conf term

router ospf 4

router-id 0.0.4.132

network 10.37.11.0 0.0.0.255 area 0

network 10.37.100.0 0.0.0.255 area 0

network 10.37.101.0 0.0.0.255 area 0

network 10.37.102.0 0.0.0.255 area 0

passive-interface default

no passive-interface e1/0

exit

copy run star

Paso 2: Configurar OSPFv3 de área única en el área 0

Utilice OSPF Process ID **6** y asigne los siguientes ID de router:

R1: 0.0.6.1

Router R1

conf term
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

copy run star

R3: 0.0.6.3

Router R3

conf term
ipv6 router ospf 6

router-id 0.0.6.3

exit

interface e1/1

ipv6 ospf 6 area 0

interface e1/0

ipv6 ospf 6 area 0

exit

copy run star

D1: 0.0.6.131

Switch D1

conf term
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

copy run star

D2: 0.0.6.132

Switch D2

conf term
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

copy run star
```

Paso 3: Configurar MP-BGP para R2 en la red ISP

Se Configura dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

Una ruta estática predeterminada IPv4 y Una ruta estática predeterminada IPv6.

Se configura R2 en BGP ASN **500** y utilice el router-id 2.2.2.2.

Se configura y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

Router R2

```
conf term
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
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
ipv6 unicast
no neighbor 2001:db8:200::1 activate
network 2001:db8:2222::1/128
network ::/0
exit address-family
```

Paso 4: Configurar MP-BGP en R1 en la red ISP

Se Configuran dos rutas de resumen estáticas para la interfaz Null 0, Un resumen de la ruta IPv4 para 10.37.0.0/8, Un resumen de la ruta IPv6 para 2001:db8:100::/48.

En R1 se configura en BGP ASN **300** y se utiliza el router-id 1.1.1.1.

Se Configura una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

Router R1

```
ip route 10.37.0.0 255.255.255.0 null 0
ipv6 route 2001:db8:100::/48 null 0
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 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family
```

verificación OSF en los dispositivos

comando show run | section router ospf en R1, R3, D1 Y D2

En R1

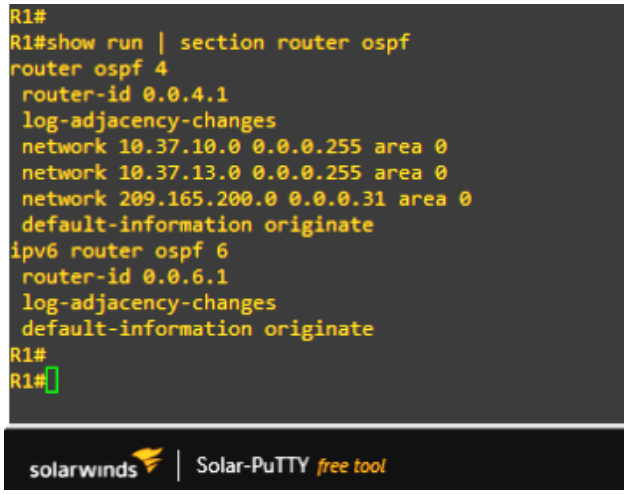


Figura 11. OSPF en R1

En R3

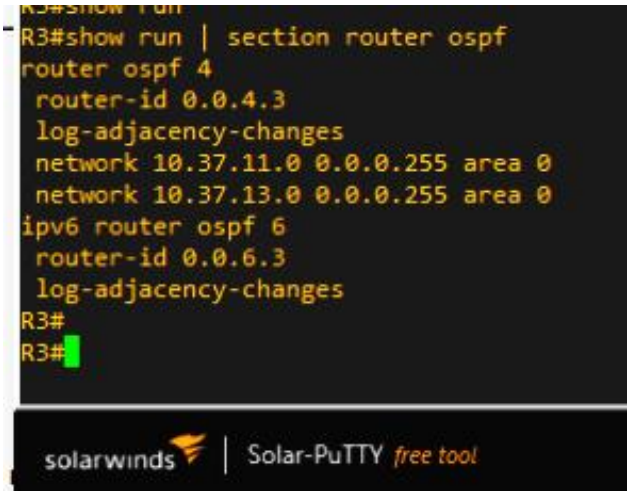


Figura 12. OSPF en R3

En D1

```
D1#
D1#show run | section router ospf
router ospf 4
 router-id 0.0.4.3
 passive-interface default
 no passive-interface Ethernet1/2
 network 10.37.11.0 0.0.0.255 area 0
 network 10.37.13.0 0.0.0.255 area 0
ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
D1#
D1#
```

solarwinds | Solar-PuTTY *free tool*

Figura 13. OSPF en D1

En D2

```
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 10.37.11.0 0.0.0.255 area 0
 network 10.37.100.0 0.0.0.255 area 0
 network 10.37.101.0 0.0.0.255 area 0
 network 10.37.102.0 0.0.0.255 area 0
ipv6 router ospf 6
 router-id 0.0.6.132
 passive-interface default
 no passive-interface Ethernet1/0
D2#
D2#
```

solarwinds | Solar-PuTTY *free tool*

Figura 14. OSPF en D2

Verificación de OSPF en Ipv6

comando show run | section ipv6 router en R1,R3, D1 Y D2

en R1

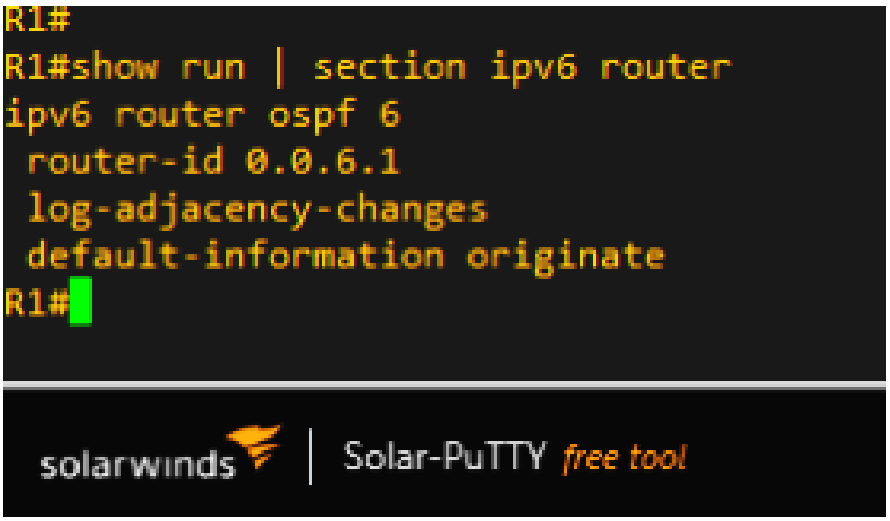


Figura 15. OSPF Ipv6 en R1

En R3

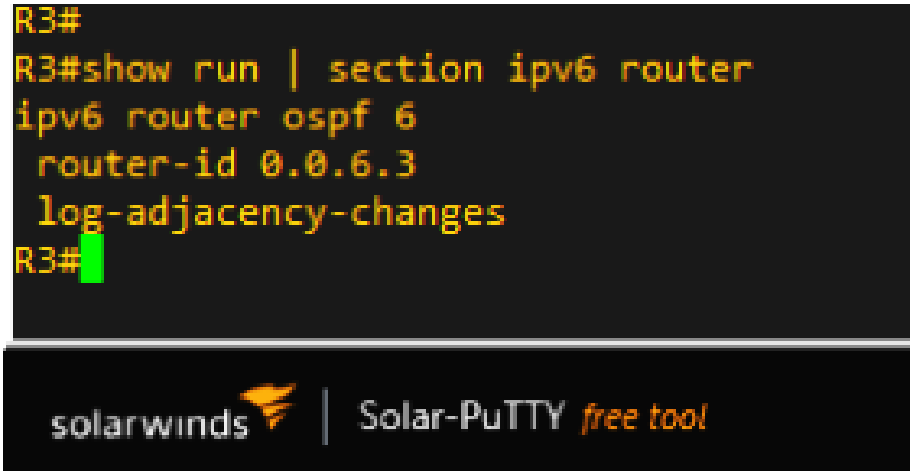


Figura 16. OSPF Ipv6 en R3

En D1

Figura 17. OSPF Ipv6 en D1

En D2

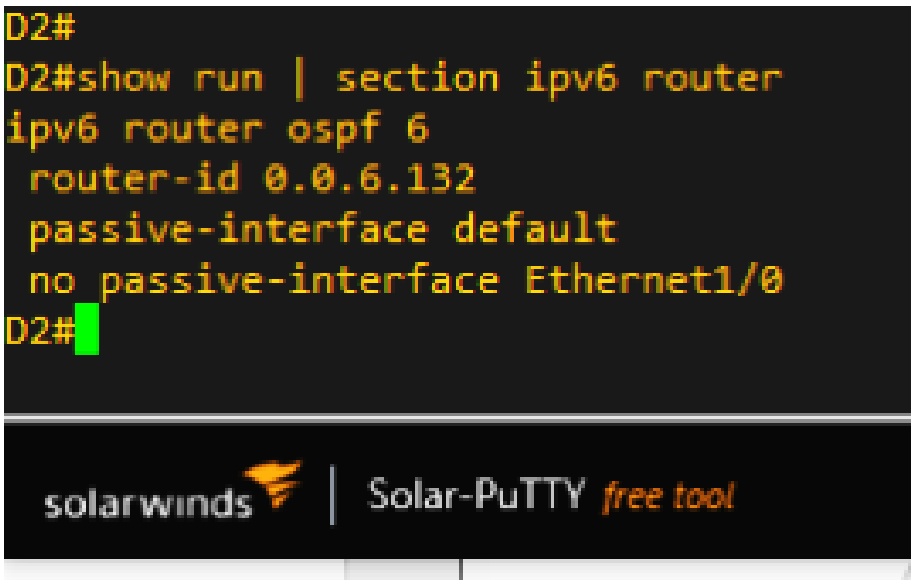


Figura 18. OSPF Ipv6 en D2

Verificación de BGP en R2,

comando show run | section bgp en R2

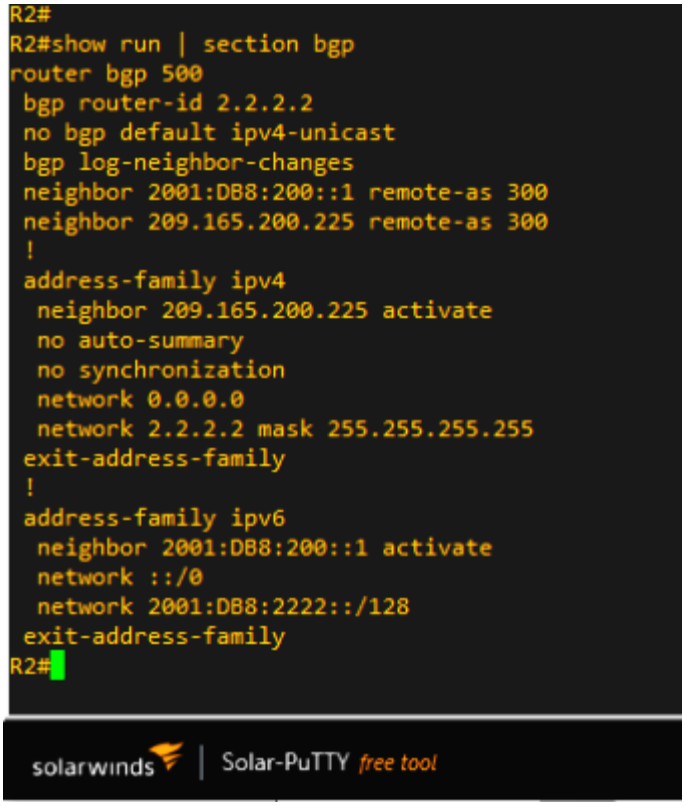


Figura 19. Configuración BGP en R2

comando show run | include route en R2

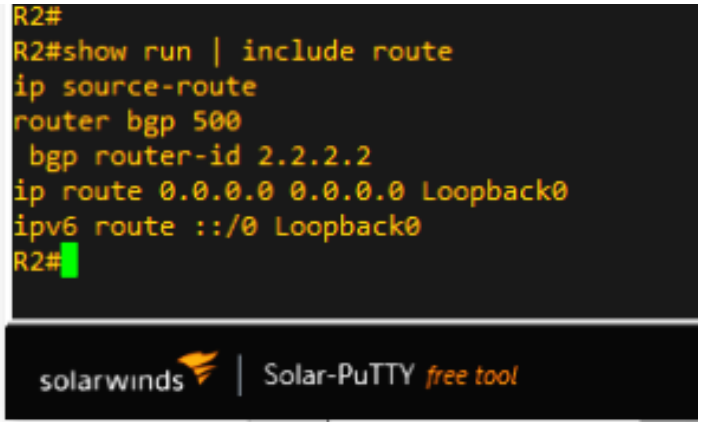


Figura 20. Configuración include route en R2

Verificación BGP en R1

comando show run | section bgp en R1

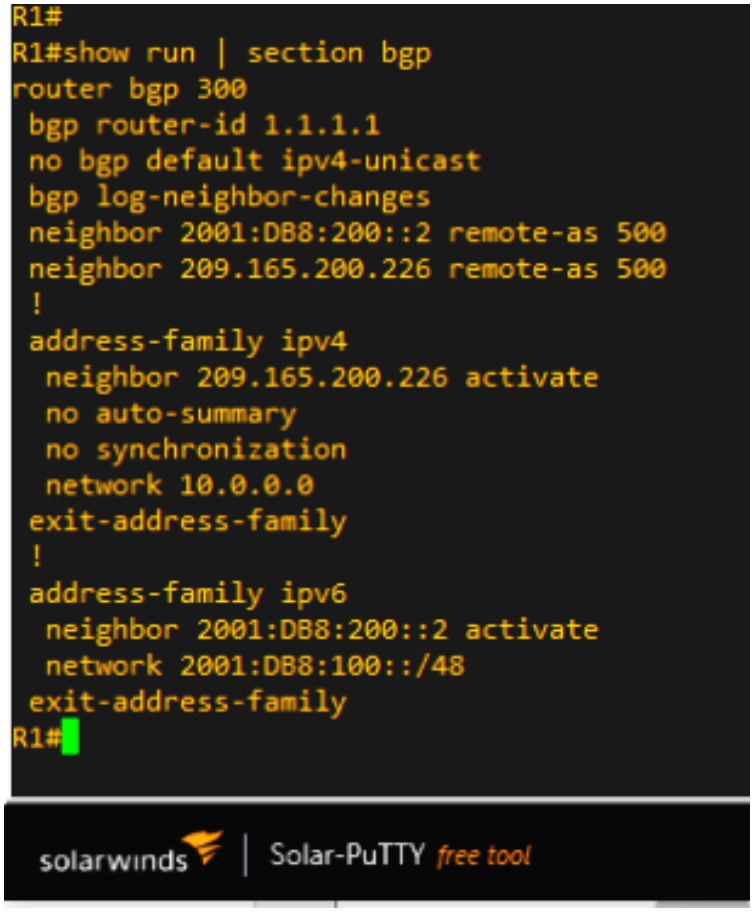


Figura 21. Configuración section BGP en R1

Verificación conectividad Ipv6 en R1

Comando show ipv6 route en R1

Figura 22. Conectividad Ipv6 en R1

Verificación de OSPF Ipv6 en R3

Comando Show ipv6 route ospf

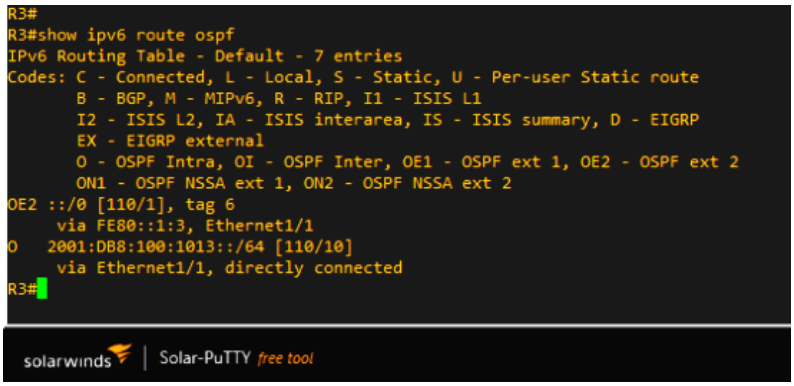


Figura 23. Ipv6 route OSPF en R3

Parte 4: configurar la redundancia del primer salto

Paso 1. En D1 se crea SLA IP que prueben la accesibilidad de la interfaz R1 E1/2.

Paso 1: En D1, crear IP SLAs que prueben la accesibilidad de la interfaz R1, E1/2

Se Crean dos SLA IP.

el SLA número **4** para IPv4 y el SLA número **6** para IPv6.

Los SLA IP probarán la disponibilidad de la interfaz R1 E1/2 cada 5 segundos.

Programe el SLA para su implementación inmediata sin hora de finalización.

Se Crea un objeto de SLA de IP para:

Switch D1

```
conf t
ip sla 4
icmp-echo 10.37.10.1
source-ip 10.37.10.2
frequency 5
exit
ip sla schedule 4 start-time now life forever
track 4 ip sla 4 reachability
delay up 10 down 15
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1 source-interface e1/2
frequency 5
exit
ip sla schedule 6 start-time now life forever
track 6 ip sla 6 reachability
delay up 10 down 15
exit
```

Paso 2: En D2, crear IP SLAs que prueben la accesibilidad de la interfaz R3 E1/0

Se Crean dos SLA IP.

Se utiliza el SLA número **4** para IPv4.
Se uutiliza el SLA número **6** para IPv6.

Los SLA IP probarán la disponibilidad de la interfaz R3 E1/0 cada 5 segundos.

Programe el SLA para su implementación inmediata sin hora de finalización. Y un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.

Switch D2

```
conf terminal

ip sla 4

icmp-echo 10.37.11.1 source-interface e1/0

frequency 5

exit
ip sla schedule 4 start-time now life forever

track 4 ip sla 4 reachability

delay up 10 down 15

exit

ip sla 6
icmp-echo 2001:db8:100:1011::1

source-interface e1/0

frequency 5

exit
ip sla schedule 6 start-time now life forever

track 6 ip sla 6 reachability

delay up 10 down 15

exit
```

Paso 3: En D1 se configura HSRPv2

En el switch D1 como el router principal para VLAN 100 y 102; y su prioridad se cambia a 150, en el switch D2 es el router principal para VLAN 101 y la prioridad se cambia a 150.

Se Configura HSRP versión 2.

El grupo 104 de HSRP IPv4 para VLAN 100 se configura de acuerdo a:
Asignar la dirección IP virtual 10.37.100.254**.** Se Establece la prioridad del grupo en **150** Habilitando la preferencia.
Y se Realiza un seguimiento del objeto 4 y disminuya en 60.

Switch D1

```
conf t
interface vlan 100
standby version 2
standby 104 ip 10.37.100.254
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 10.37.101.254
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 10.37.102.254
standby 124 priority 150
standby 124 preempt
```

```
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

En switch D2, configurar HSRPv2

Se Configura el grupo 104 de HSRP IPv4 para VLAN 100:

Se asigne la dirección IP virtual 10.37.100.254**.**
Se Habilita la preferencia y se realice un seguimiento del objeto 4 y se disminuye en 60.

Al Configurar el grupo **114** de HSRP IPv4 para VLAN 101 se adjuntan as siguientes configuraciones:

- Asignar la dirección IP virtual 10. 37.10 1,254.
- Establecer la prioridad del grupo en 150.
- Habilitar la preferencia.
- Realizar un seguimiento del objeto 4 hasta disminuir en 60.

Configurar el grupo HSRP IPv4 124 para VLAN 102:

- Asignar la dirección IP virtual 10. 37.10 2.254.
- Habilitar la preferencia.
- Realizar un seguimiento del objeto 4 hasta disminuir en 60.

Configure IPv6 HSRP grupo 10 6 para VLAN 100:

- Asignar la dirección IP virtual mediante la configuración automática de ipv6.
- Habilitar la preferencia.

Switch D2

```
conf term
interface vlan 100
standby version 2
standby 104 ip 10.37.100.254
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 10.37.101.254
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 10.37.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

verificación de la configuración Ip SLA en D1

commando show run | section ip sla

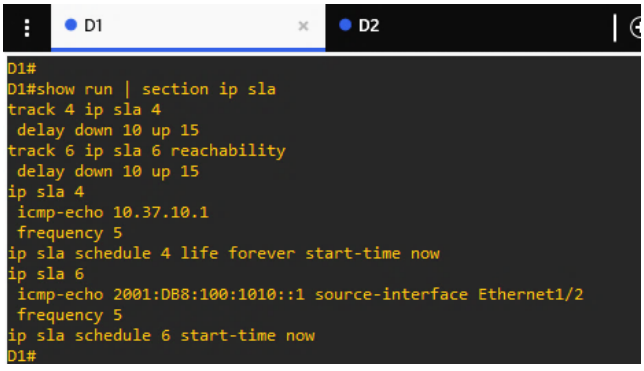


Figura 24. Ip SLA en D1

Verificación de standby en D1 y D2

Comando Show standby brief en D1

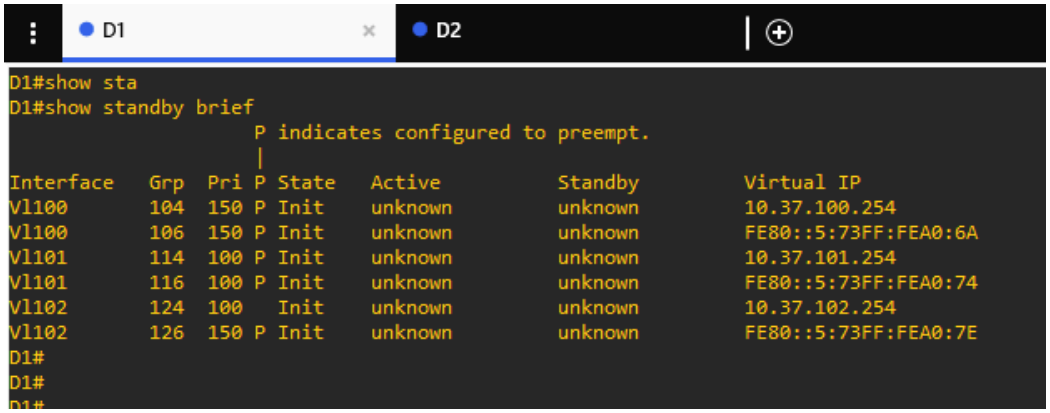


Figura 25. Standby brief en D1

Verificación IP SLA y Standby en D2

Comando Show run | section ip sla en D2

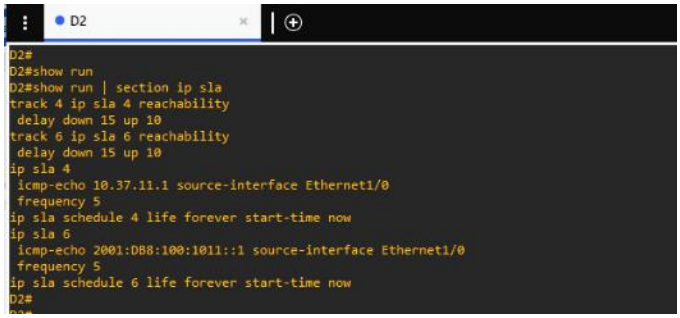


Figura 26. Section Ip SLA en D2

Comando Show standby brief

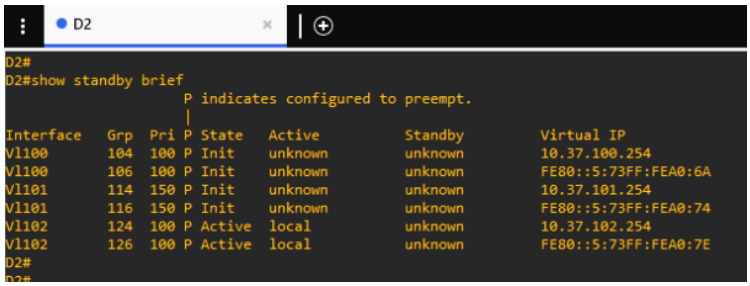


Figura 27. Standby brief en D2

CONCLUSIONES

Durante el Diplomado de profundización CCNP se adquirieron destrezas y habilidades que permiten la preparación profesional asertiva para el diseño, configuración e implementación de una red LAN o WAN.

Se desarrolla una práctica simulada de un entorno real donde se refuerzan los conocimientos adquiridos en el curso de Cisco Netacad, las herramientas informáticas como los simuladores de red permiten realizar un diseño de red y hacer todos los pasos necesarios para el adecuado comportamiento de la red antes de implementar en un dispositivo real.

Los planteamientos en los dos escenarios se aplican la configuración básica de los dispositivos que conforman la red, según la tabla de enrutamiento asignada para la red, durante la configuración del escenario 2, se implementan protocolos de enrutamiento como es OSPFv2, OSPFv3, DHCP, HSRP y el protocolo BGP relación con el vecino, y IP SLA que componen un grupo de puertos físicos enrutados en un solo canal de enrutamiento lógico

El enrutamiento configurado corresponde a protocolo IPv4 e IPv6 que hacen una red robusta, escalable y con una alta velocidad en la red, el protocolo de encapsulamiento de los enlaces troncales 802.1q ofrecen seguridad y conexión más estable en el tráfico de paquetes en los dispositivos de capa 2

BIBLIOGRAFÍA

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). *EIGRP*. CCNP and CCIE Enterprise Core ENCOR 350-401. https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

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

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

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

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