DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YENISON LUBIN MORA CAMPO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA **ELECTRÓNICA**
MEDELLÍN
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YENISON LUBIN MORA CAMPO

Diplomado de opción de grado presentado para optar el
título de INGENIERO **ELECTRÓNICO.**

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA **ELECTRÓNICA**
MEDELLÍN
2021

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

MEDELLÍN, 29 de noviembre del 2021

AGRADECIMIENTOS

Al ingeniero Héctor Julián Parra y demás profesionales que, con el objetivo de entregar este documento bajo los parámetros requeridos, hicieron revisión de los segmentos aportados y entregaron claras y oportunas recomendaciones que ayudaron a realizar las actividades propuestas y la redacción adecuada de este documento.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Red: Una red es la interconexión física o inalámbrica que vincula varios dispositivos informáticos (servidores, computadoras, dispositivos móviles, periféricos, entre otros) para que se comuniquen entre sí, con la finalidad de compartir información y ofrecer diferentes servicios.

VLAN: También conocidas como “virtual LAN” son redes lógicamente independientes dentro de una misma red física, las cuales pueden ser generadas haciendo uso de equipos compatibles que permitan segmentar adecuadamente la red, ofreciendo ventajas en la infraestructura de las topologías, seguridad, segmentación, flexibilidad y optimización de la red.

Direccionamiento: El concepto se refiere a dotar de una identificación o también llamado esquema de dirección, a una red especifica o a un dispositivo de red con el cual se pueda establecer comunicación.

HSRP: Hot Standby Router Protocol es un protocolo que permite lograr que el tiempo de actividad de la red esté cerca del 100%, ofreciendo redundancia a través de enrutadores tolerantes a fallos de red, asegurando que el tráfico de usuarios se recupere de forma inmediata y transparente de errores de primer salto y fallos en la red.

MP-BGP: Border Gateway Protocol, es un protocolo que permite tener control de las rutas entre diferentes empresas u organizaciones a lo largo del tránsito de la información por internet, es considerado como un medio de transporte establecido para llevar cualquier paquete IP a cualquier rincón del planeta a través de ISP y grandes organizaciones.

Servidor RADIUS: Es un servidor que proporciona conectividad a internet con autentificación donde se solicita un usuario y contraseña para poder acceder a la red inalámbrica. También RADIUS (Remote Access Dial In User Service) es un protocolo que se destaca por ofrecer un mecanismo de seguridad y una administración de las credenciales de acceso a un recurso de red.

RESUMEN

Este documento es un informe el cual recoge el desarrollo de las actividades propuestas en el diplomado CCNP de Cisco, en el cual paso a paso se desarrolla una red de comunicación compuesta por diferentes dispositivos de red que normalmente están presente en cualquier topología cotidiana.

En etapa, se parte de la configuración básica de una red y poco a poco se van configurando los equipos de conmutación y enrutamiento para ir formando distintos enlaces con diferentes características de funcionamiento y seguridad y finalmente, estas configuraciones y dispositivos nos van a permitir obtener comunicaciones completas y funcionales a través de las redes y usando diferentes dispositivos electrónicos.

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

ABSTRACT

This document is a report that collect the develop of all activities proposed within the CCNP course, step by step a network is configured through different network devices that normally they are in any current topology.

Therefore, the process of basic configuration begins with a basic network, then the switching and routing devices are going to be configured in order to build differents links with several charateristics of running, security and protocols. Finally all these configurations and devices are going to allow us to get functional and complete communications through networking using different electronic devices.

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

INTRODUCCIÓN

El presente documento es el informe final del diplomado CCNP en el cual se logra dar desarrollo y explicación a las actividades propuestas para un escenario especifico. Mediante la implementación del networking se logra dar solución y aplicación a diferentes parámetros y requisitos solicitados para que, en el escenario propuesto, se logre la implementación de procesos de identificación, enrutamiento, conexión, seguridad y demás elementos característicos que componen una red.

Es importante el desarrollo de este trabajo como evidencia clara de los aspectos cognitivos que se han desarrollado en networking a través de los cursos anteriormente realizados y del escenario propuesto para este trabajo. En este caso en búsqueda de crear una red con todos sus elementos característicos, se abordan diferentes partes o etapas en las cuales partiendo de lo más básico a lo más complejo y paso a paso, se arma una topología con sus dispositivos electrónicos, conectándolos y ajustándolos con sus configuraciones básicas.

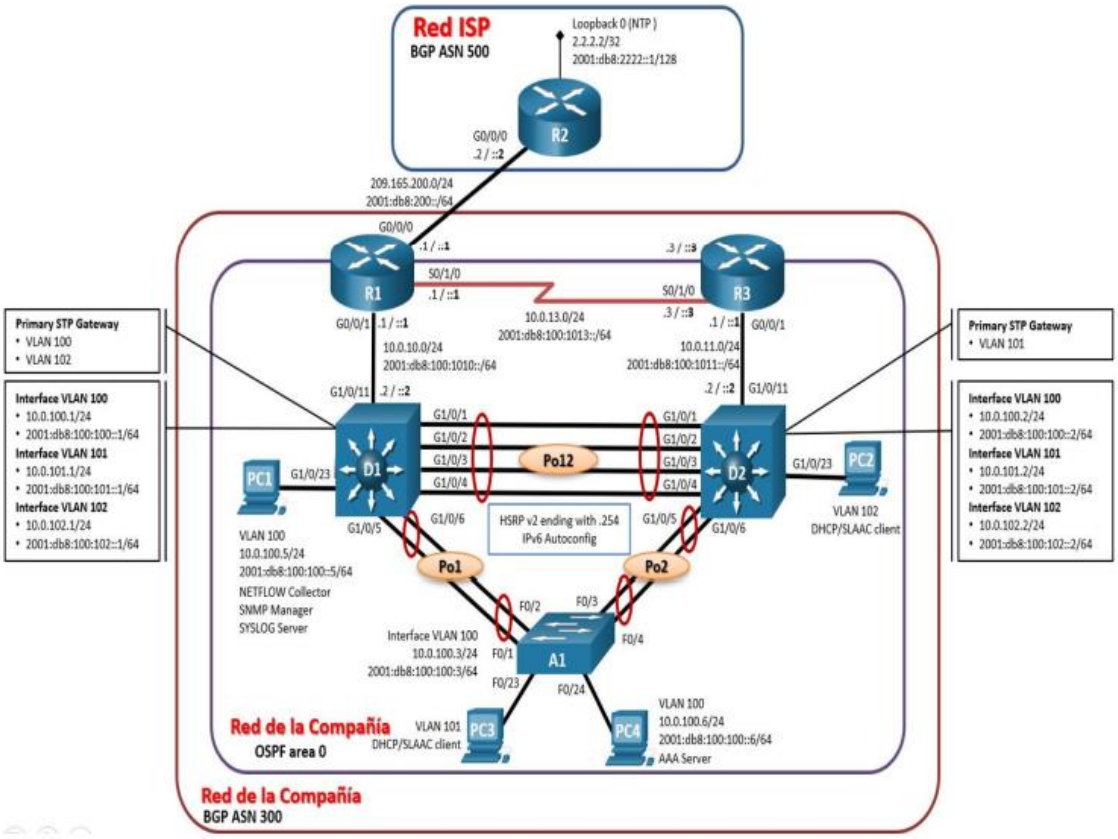
Al ir abordando las diferentes etapas del escenario, se dan direcciones a las interfaces de los equipos, se aplican las configuraciones básicas de red y se implementan los protocolos de enrutamiento en los equipos, para finalmente, ajustar la red y dotarla de elementos característicos que permitan el correcto funcionamiento en caso de fallos, una seguridad adecuada y un funcionamiento con una administración de red bien definida.

Para ello, mediante el uso de los conocimientos ya obtenidos, las múltiples asesorías, la autonomía, creatividad, las herramientas teleinformáticas adecuadas y demás aspectos se logra dar desarrollo a este último trabajo, a este último esfuerzo que no solo representa la materialización del conocimiento en un escenario realista, sino la culminación del proceso de aprendizaje en redes emprendido en periodos anteriores.

DESARROLLO

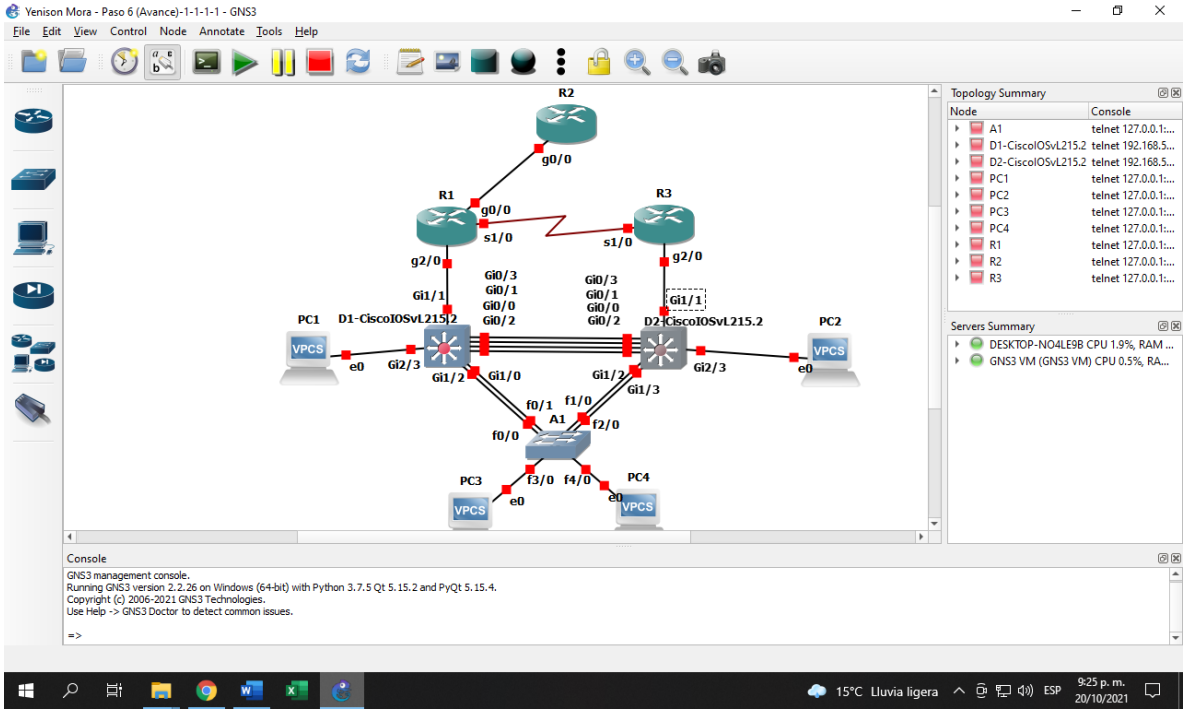
Escenario Propuesto:

Figura 1.Topología de red del escenario propuesto.



Objetivo del escenario: En esta prueba de habilidades, se completó la configuración de la red para que fuera posible una accesibilidad completa de un extremo a otro, para que los hosts tuvieran un soporte confiable de la puerta de enlace predeterminada y para que los protocolos configurados estuvieran operativos dentro de la parte correspondiente a la "Red de la compañía" en la topología.

Figura 2. Simulación del escenario en GNS3



Tablas 1. Direccionamiento del escenario propuesto.

Dispositivo	Interfaz	Reemplazo Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	G2/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	S1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	G0/0	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	G0/0/1	G2/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	S1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	e1/1	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100		10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101		10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102		10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	e1/1	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100		10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101		10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102		10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100		10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC		10.0.100.5/24	2001:db8:100:100::5/64	EUI-64

PC2	NIC		DHCP	SLAAC	EUI-64
PC3	NIC		DHCP	SLAAC	EUI-64
PC4	NIC		10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

1. **Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces.**

Configuración de los parámetros básicos para cada dispositivo, tal como especifica la guía de actividades.

En esta parte, se configuran los equipos con los comandos más usuales, que permiten llevar los equipos a condiciones iniciales para trabajarlos. Aspectos como el nombre, las contraseñas, la nula búsqueda de direcciones, las direcciones IP, entre otros son configurados aquí.

Router R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
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 g0/0/1
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
```

```
interface s0/1/0
ip address 10.0.13.1 255.255.255.0
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, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
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, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
interface g0/0/1
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s0/1/0
ip address 10.0.13.3 255.255.255.0
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, Scenario 1 #
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 g1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
```

```
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface
vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain
lookup banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
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 g1/0/11
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
```

```
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
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 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown
exit
```

2. Parte 2: Configurar la capa 2 de la red y el soporte de Host.

2.1. En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches. Se Habilita enlaces trunk 802.1Q entre:

D1 and D2
D1 and A1
D2 and A1

Descripción de los comandos: En el 2.1 se activan las interfaces para realizar enlaces trunk mediante el comando "*Switchport mode trunk* " en cada una de las interfaces que se usara para dichos enlaces. El comando "*Switchport trunk encapsulation dot1q*" se usa para habilitar 802.1Q de forma manual, ya que este por defecto se encuentra en modo automático y no permite habilitar el modo trunk.

Switch D1

Interface range e0/0-3	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport mode trunk	Se activa enlace trunk para la interfaz.

Interface range g1/2, g1/0	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport mode trunk	Se activa enlace trunk para la interfaz.

Switch D2

Interface range e0/0-3	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport mode trunk	Se activa enlace trunk para la interfaz.
Interface range g1/2, g1/3	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport mode trunk	Se activa enlace trunk para la interfaz.

Switch A1

Interface range f0/0-1	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport mode trunk	Se activa enlace trunk para la interfaz.
Interface range f1/0, f2/0	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport mode trunk	

2.2. En todos los switches cambie la VLAN nativa en los enlaces troncales. Use VLAN 999 como la VLAN nativa.

Descripción de los comandos: Nuevamente se usa el comando "*Switchport trunk encapsulation dot1q*" para habilitar 802.1Q en las interfaces donde debe especificarse la VLAN nativa como VLAN 99, esto se realiza mediante el comando *"Switchport trunk native VLAN 999"* en cada una de las interfaces predeterminadas.

Switch D1

Interface range e0/0-3	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport trunk native vlan 999	Se especifica la VLAN nativa
exit	
Interface range g1/2, g1/0	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport trunk native vlan 999	Se especifica la VLAN nativa
exit	

Switch D2

Interface range e0/0-3	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport trunk native vlan 999	Se especifica la VLAN nativa
exit	
Interface range g1/2, g1/3	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport trunk native vlan 999	Se especifica la VLAN nativa
exit	

Switch A1

Interface range f0/0-1	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport trunk native vlan 999	Se especifica la VLAN nativa
exit	
Interface range f1/0, f2/0	
Switchport trunk encapsulation dot1q	Para habilitar 802.1Q de forma manual.
Switchport trunk native vlan 999	Se especifica la VLAN nativa
Exit	

2.3. En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP). Use Rapid Spanning Tree (RSPT).

Descripción de los comandos: En cada uno de los dispositivos sugeridos, se activa RSTP mediante el comando *“Spanning-tree mode rapid-pvst”.*

Switch D1

Spanning-tree mode rapid-pvst

Switch D2

Spanning-tree mode rapid-pvst

Switch A1

Spanning-tree mode rapid-pvst

2.4. En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge). Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

Descripción de los comandos: Se configura el puente principal de comunicación entre los puertos y un puerto secundario en caso de fallas, mediante *"Spanning-tree vlan".*

Switch D1

Spanning-tree vlan 100, 102 root primary	Puentes principales en D1.
Spanning-tree vlan 101 root secondary	Puente secundario en D1.

Switch D2

Spanning-tree vlan 101 root primary	Puente principal en D2.
Spanning-tree vlan 100,102 root secondary	Puentes secundarios en D1.

2.5. En todos los switches, cree EtherChannel LACP como se muestra en el diagrama de topología. Use los siguientes números de canales:

D1 a D2 – Port channel 12
D1 a A1 – Port channel 1
D2 a A1 – Port channel 2

Descripción de los comandos: Se realiza configuración de los canales en cada interfaz de los dispositivos, para así generar los canales ether con los números designados, es decir especificando el número de los canales mediante el comando *"channel-group"* en cada una de las interfaces.

Switch D1

Interface range e0/0-3

Channel-group 12 mode active
No shutdown

Interface range g1/2, g1/0
Channel-group 1 mode active
No shutdown

Switch D2

Interface range e0/0-3
Channel-group 12 mode active
No shutdown

Interface range g1/2, g1/3
Channel-group 2 mode active
No shutdown

Switch A1

Interface range f0/0-1
Channel-group 1 mode active
No shutdown

Interface range f1/0, f2/0
Channel-group 2 mode active

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

Descripción de los comandos: En las interfaces conectadas a cada pc, se configura la VLAN adecuada y designada a cada equipo mediante el comando *"Switchport access vlan #".* También para que las interfaces entren en modo de actualizaciones o forwarding, se aplica el comando *"Spanning-tree portfast".*

Switch D1

Interface g2/3	
Switchport mode access	Configuración de puerto para host
Switchport access vlan 100	El puerto se asocia a la VLAN
Spanning-tree portfast	Puerto en estado de reenvío

Switch D2

Interface g2/3	
Switchport mode Access	Configuración de puerto para host
Switchport access vlan 102	El puerto se asocia a la VLAN
Spanning-tree portfast	Puerto en estado de reenvío

Switch A1

Interface f3/0	
Switchport mode Access	Configuración de puerto para host
Switchport access vlan 101	El puerto se asocia a la VLAN
Spanning-tree portfast	Puerto en estado de reenvío
Interface f4/0	
Switchport mode Access	Configuración de puerto para host
Switchport access vlan 100	El puerto se asocia a la VLAN
Spanning-tree portfast	Puerto en estado de reenvío

2.7. Verifique los servicios DHCP IPv4. PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

Descripción de los comandos: A pesar de que PC2 y PC3 son clientes DHCP, esta opción debe ser habilitada, por ello se usa el comando *"IP DHCP"* y se guarda, para que el equipo mantenga esa dirección DHCP.

PC2

Ip dhcp	Se genera la dirección DHCP
Save	Se guarda dirección.
Ping…	Se generan ping

PC3

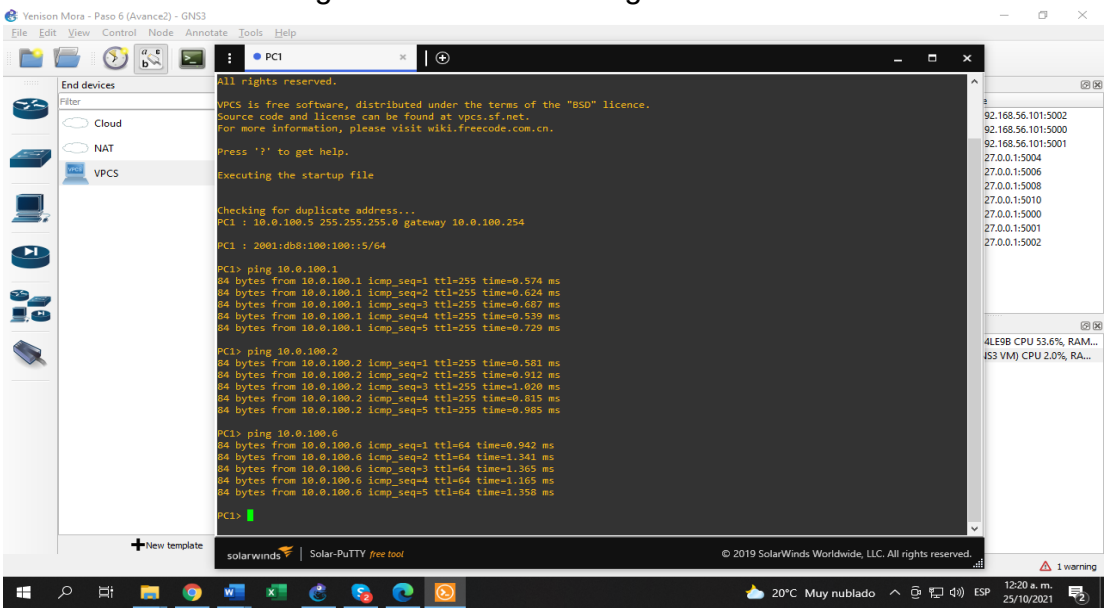
Ip dhcp	Se genera la dirección DHCP
Save	Se guarda dirección.
Ping…	Se generan ping

2.8. Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1
D2: 10.0.100.2
PC4: 10.0.100.6

Figura 3. Diferentes Ping desde PC1.



PC2 debería hacer ping con éxito a:

D1: 10.0.102.1
D2: 10.0.102.2

PC3 debería hacer ping con éxito a:

D1: 10.0.101.1
D2: 10.0.101.2

Figura 4. Diferentes Ping desde PC2

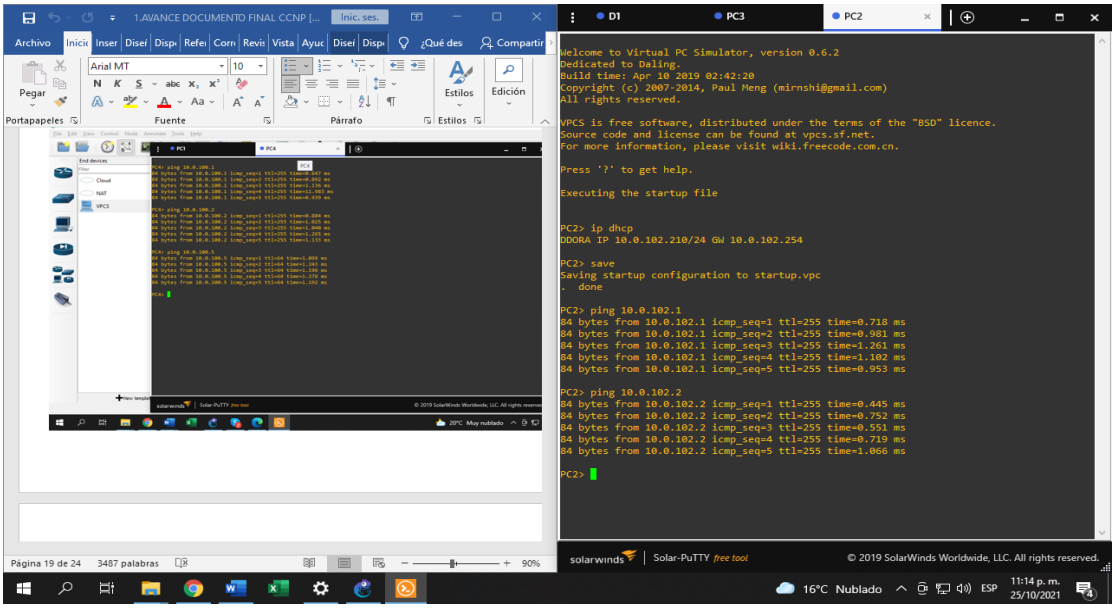
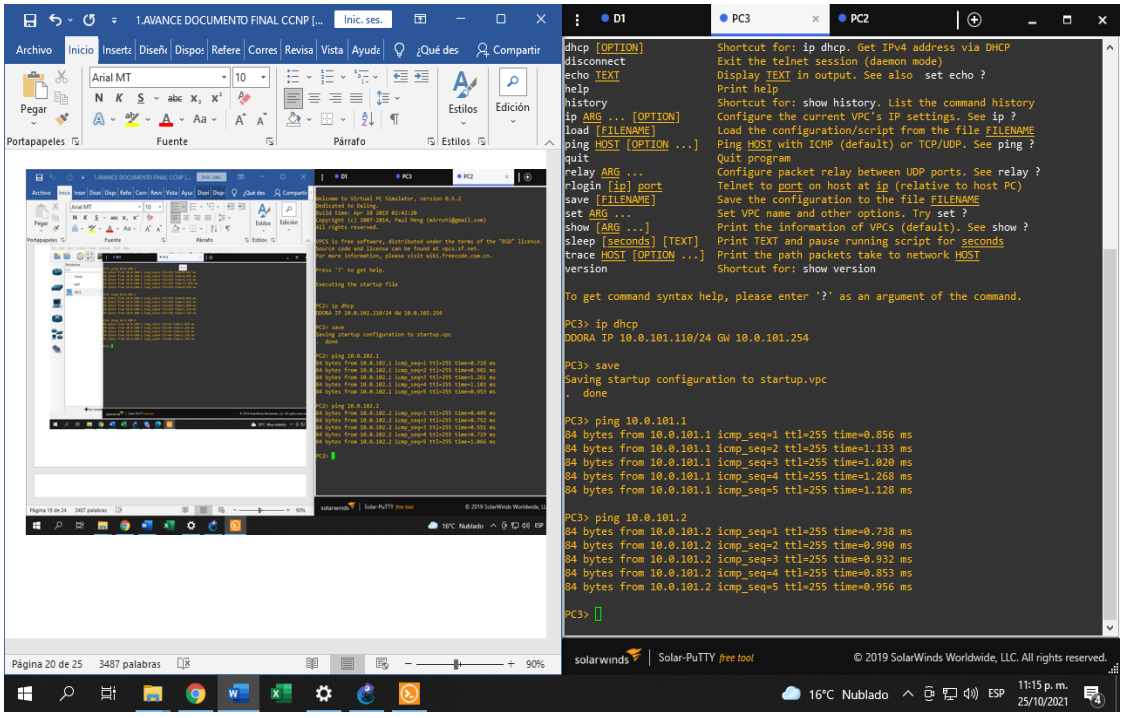


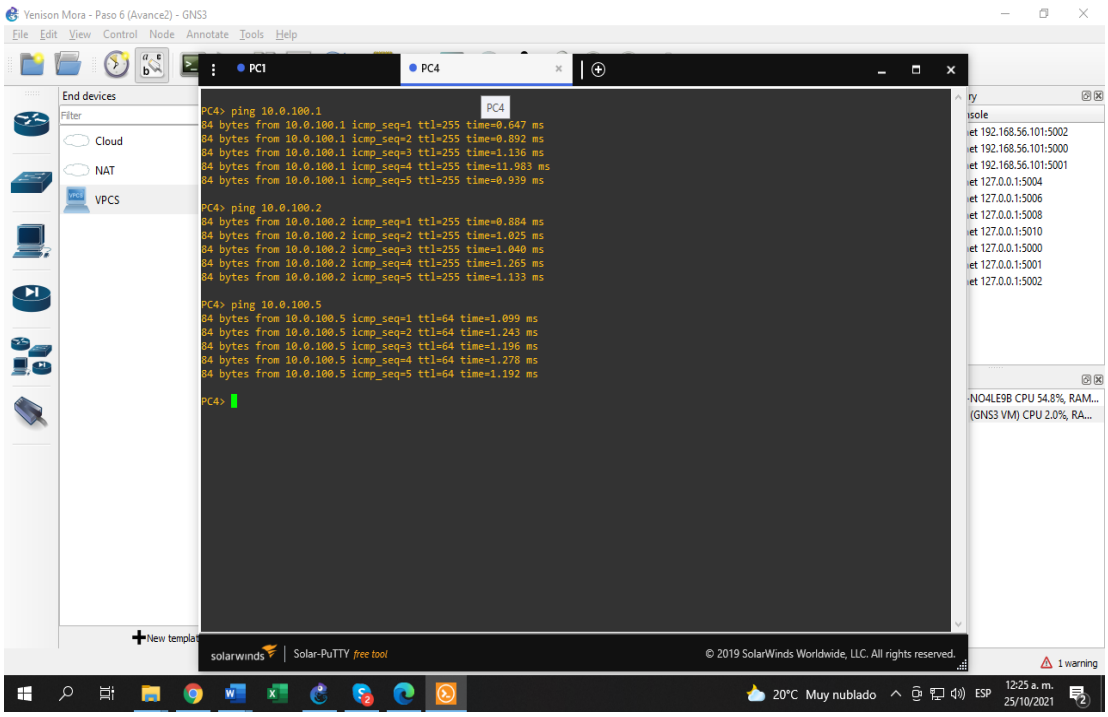
Figura 5. Diferentes Ping desde PC3.



PC4 debería hacer ping con éxito a:

D1: 10.0.100.1
D2: 10.0.100.2
PC1: 10.0.100.5

Figura 6. Diferentes Ping desde PC4.



3. Parte 3: Configurar los protocolos de enrutamiento.

3.1. En la “Red de la Compañía” (es decir,R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.

Descripción de los comandos: En esta caso se inicializa el proceso OSPF con un ID determinado para ipv4 y se le da un id propio a cada router mediante el comando *“Router-id #.#.#.#”.* Además, se anuncian las redes directamente conectadas a las interfaces, teniendo en cuenta el área, la dirección y la subnet, la cual en este caso se especifica de una forma inversa.

También se deshabilitan las actualizaciones de las interfaces, a excepción de algunas en específico, esto se realiza mediante los comandos “passive-interface

default” y “no passive-interface default”.

Use OSPF Process ID 4 y asigne los siguientes router-IDs:

R1: 0.0.4.1
R3: 0.0.4.3
D1: 0.0.4.131
D2: 0.0.4.132

Router R1

Router ospf 4	Habilitación de OSPF con proceso ID4
Router-id 0.0.4.1	ID para el router

Router R3

Router ospf 4	Habilitación de OSPF con proceso ID4
Router-id 0.0.4.3	ID para el router

Switch D1

Router ospf 4	Habilitación de OSPF con proceso ID4
Router-id 0.0.4.131	ID para el router

Switch D2

Router ospf 4	Habilitación de OSPF con proceso ID4
Router-id 0.0.4.132	ID para el router

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

Router R1

Router ospf 4	
Network 10.0.10.0 0.0.0.255 area 0	Red directa con D1
Network 10.0.13.0 0.0.0.255 area 0	Red directa con R3

Router R3

Router ospf 4

Network 10.0.11.0 0.0.0.255 area 0	Red directa con D2
Network 10.0.13.0 0.0.0.255 area 0	Red directa con R1

Switch D1

Router ospf 4	
Network 10.0.10.0 0.0.0.255 area 0	Red directa con R1
Network 10.0.100.0 0.0.0.255 area 0	Red asociada a VLAN 100
Network 10.0.101.0 0.0.0.255 area 0	Red asociada a VLAN 101
Network 10.0.102.0 0.0.0.255 area 0	Red asociada a VLAN 102

Switch D2

Router ospf 4	
Network 10.0.11.0 0.0.0.255 area 0	Red directa con R3
Network 10.0.100.0 0.0.0.255 area 0	Red asociada a VLAN 100
Network 10.0.101.0 0.0.0.255 area 0	Red asociada a VLAN 101
Network 10.0.102.0 0.0.0.255 area 0	Red asociada a VLAN 102

Deshabilite las publicaciones OSPFv2 en:

D1: todas las interfaces excepto G1/0/11

Switch D1

Router ospf 4	
Passive-interface default	Se desactivan las actualizaciones de routing
No passive-interface g2/0	Esta interfase si enviara actualizaciones.
Exit	

D2: todas las interfaces excepto G1/0/11

Switch D2

Passive-interface default	Se desactivan las actualizaciones de routing
No passive-interface g2/0	Esta interfase si enviara actualizaciones.
Exit	

3.2. En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.

Descripción de los comandos: En esta caso se inicializa el routing ipv6 mediante el comando "*Ipv6-unicast-routing* " y el proceso OSPF con un ID determinado para ipv6 y se le da un id propio a cada router mediante el comando *"Router-id #.#.#.#".* Además, se anuncian las redes directamente conectadas a las interfaces.

También se deshabilitan las actualizaciones de las interfaces, a excepción de algunas en específico, esto se realiza mediante los comandos "passive-interface default" y "no passive-interface default".

Use OSPF Process ID 6 y asigne los siguientes router-IDs:

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

Router R1

Ipv6-unicast-routing	Habilitación de routing ipv6
Ipv6 router ospf 6	Configuración OSPF con ID 6
Router-id 0.0.6.1	ID del router
exit	

Router R3

Ipv6-unicast-routing	Habilitación de routing ipv6
Ipv6 router ospf 6	Configuración OSPF con ID 6
Router-id 0.0.6.3	ID del router
exit	

Switch D1

Ipv6-unicast-routing	Habilitación de routing ipv6
Ipv6 router ospf 6	Configuración OSPF con ID 6
Router-id 0.0.6.131	ID del router
exit	

Switch D2

Ipv6-unicast-routing	Habilitación de routing ipv6
Ipv6 router ospf 6	Configuración OSPF con ID 6
Router-id 0.0.6.132	ID del router
Exit	

En R1, R3, D1, y D2, anuncie todas las redesdirectamente conectadas / VLANs en Area 0.

Router R1

```
Interface g2/0
Ipv6 ospf 6 area 0
Exit
Interface s1/0
Ipv6 ospf 6 area 0
Exit
```

Router R3

```
Interface g2/0
Ipv6 ospf 6 area 0
Exit
Interface s1/0
Ipv6 ospf 6 area 0
Exit
```

Switch D1

```
Interface g1/1
Ipv6 ospf 6 area 0
Exit
Interface vlan 100
Ipv6 ospf 6 area 0
Exit
Interface vlan 101
Ipv6 ospf 6 area 0
Exit
Interface vlan 102
Ipv6 ospf 6 area 0
Exit
```

Switch D2

```
Interface g1/1
Ipv6 ospf 6 area 0
Exit
Interface vlan 100
```

Ipv6 ospf 6 area 0
Exit
Interface vlan 101
Ipv6 ospf 6 area 0
Exit
Interface vlan 102
Ipv6 ospf 6 area 0
Exit

- Deshabilite las publicaciones OSPFv3 en:

D1: todas las interfaces excepto G1/0/11

Switch D1

Ipv6 router ospf 6
Passive-interface default Se desactivan las actualizaciones de routing
No passive-interface g1/1 Esta interfase si enviara actualizaciones.
exit

D2: todas las interfaces excepto G1/0/11

Switch D2

Ipv6 router ospf 6
Passive-interface default Se desactivan las actualizaciones de routing
No passive-interface g1/1 Esta interfase si enviara actualizaciones.
exit

3.3. En R2 en la “Red ISP”, configure MP-BGP.

Descripción de los comandos: Se habilita una ruta estática para ipv4 y ipv6, mediante el comando “ip route” y “ipv6 route”. Se habilita BGP en R2 y se especifica un ID BGP para el router mediante el comando “bgp router-id”. Después a manera de generar un enlace vecino en ipv4 y ipv6 con R1, se especifican las redes a relacionar, teniendo en cuenta que R1 será BGP 300 y R2 es BGP 500, mediante el comando “neighbor”.
También mediante el comando “ip address-family” se realiza una especificación mucho más clara, ya que se asocian directamente las direcciones ipv4 y ipv6 en cada uno de los dispositivos, que serán vecinas.

Configure dos rutas estáticas predeterminadas através de la interfaz Loopback 0:

Una ruta estática predeterminada IPv4.

Router R2

Ip route 0.0.0.0 0.0.0.0 loopback 0

Una ruta estática predeterminada IPv6.

Router R2

Ipv6 route ::/0 loopback 0

Configure R2 en BGP ASN 500 y use el router-id2.2.2.2.

Router R2

Router bgp 500
Bgp router-id 2.2.2.2
exit

Configure y habilite una relación de vecino IPv4 e IPv6con R1 en ASN 300.

Router R2

Router bgp 500
Neighbor 209.165.200.225 remote-as 300
Neighbor 2001:db8:200::1 remote-as 300

En IPv4 address family, anuncie:

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

Router R2

Router bgp 500
Address-family ipv4
Neighbor 209.165.200.225 activate
No neighbor 2001:db8:200::1 activate
Network 2.2.2.2 mask 255.255.255.255
Network 0.0.0.0
Exit-address-family

En IPv6 address family, anuncie:

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

Router R2

Router bgp 500
Address-family ipv6
Neighbor 2001:db8:200::1 activate
No neighbor 209.165.200.225 activate
Network 2001:db8:2222::/128
Network ::/0
Exit-address-family

3.4. En R1 en la “Red ISP”, configure MP-BGP.

Descripción de los comandos: Se habilita una ruta estática para ipv4 y ipv6, mediante el comando “ip route” y “ipv6 route”. Se habilita BGP en R1 y se especifica un ID BGP para el router mediante el comando “bgp router-id”. Después a manera de generar un enlace vecino en ipv4 y ipv6 con R2, se especifican las redes a relacionar, teniendo en cuenta que R1 será BGP 300 y R2 es BGP 500, mediante el comando “neighbor”.
También mediante el comando “ip address-family” se realiza una especificación mucho más clara, ya que se asocian directamente las direcciones ipv4 y ipv6 en cada uno de los dispositivos, que serán vecinas.

Configure dos rutas resumen estáticas a la interfaz Null 0:
Una ruta resumen IPv4 para 10.0.0.0/8.
Una ruta resumen IPv6 para 2001:db8:100::/48.

Router R1

Ip route 10.0.0.0 255.0.0.0 null0
Ipv6 route 2001:db8:100::/48 null0

Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.

Router R1

Router bgp 300
Bgp router-id 1.1.1.1

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

Router R1

Router bgp 300
Neighbor 209.165.200.226 remote-as 500
Neighbor 2001:db8:200::2 remote-as 500

En IPv4 address family:

Deshabilite la relación de vecino IPv6.
Habilite la relación de vecino IPv4.
Anuncie la red 10.0.0.0/8.

Router R1

Router bgp 300
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

En IPv6 address family:

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

Router R1

Router bgp 300
Address-family ipv6 unicast
Neighbor 2001:db8:200::2 activate
No neighbor 209.165.200.226 activate
Network 2001:db8:100::/48
Exit-address-family

4. Parte 4. Configurar la Redundancia del Primer Salto (First Hop Redundancy).

En esta parte, se configura HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

4.1. En D1, cree IP SLAs que prueben la accesibilidad dela interfaz R1 G0/0/1.

Cree dos IP SLAs.

Use la SLA número 4 para IPv4.

Use la SLA número 6 para IPv6.

Se crea la SLA 4 y SLA 6 en D1 para monitorear la accesibilidad, en este caso de la interfaz g2/0.

Switch D1

Ip sla 4
exit
Ip sla 6
Exit

Las IP SLAs probarán la disponibilidad de la interfaz R1, g2/0 cada 5 segundos. Para ello consideramos las direcciones IP asociadas a dicha interfaz en ipv4 y ipv6 y a estas se envía un ICMP-echo, luego se define el intervalo de tiempo entre ping generados a la interfaz mediante el

comando “*frecuency”,* entonces:

Switch D1

Ip sla 4
Icmp-echo 10.0.10.1
Frecuency 5
exit
Ip sla 6
Icmp-echo 2001:db8:100:1010::1
Frecuency 5
Exit

Programe la SLA para una implementación inmediata sin tiempo de finalización, para lo cual se implementan los siguientes comandos en la configuración global:

Switch D1

Ip sla Schedule 4 life forever start-time now
Ip sla Schedule 6 life forever start-time now

Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6.
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la IP SLA 6.

Usando el comando track y el número de la IP SLA, se comienza preparar HSRP para que use IP SLA, de la siguiente manera:

Switch D1

Track 4 ip sla 4

Exit

Track 6 ip sla 6

Exit

Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos, para ello consideramos el comando "*delay down # up #* ", de la siguiente manera:

Switch D1

Track 4 ip sla 4

Delay down 10 up 15

Exit

Track 6 ip sla 6

Delay down 10 up 15

Exit

4.2. En D2, cree IP SLAs que prueben la accesibilidad dela interfaz R3 G0/0/1.

Cree IP SLAs.

Use la SLA número 4 para IPv4.

Use la SLA número 6 para IPv6.

Se crea la SLA 4 y SLA 6 en D2 para monitorear la accesibilidad, en este caso de la interfaz g2/0.

Switch D2

Ip sla 4

exit

Ip sla 6

Exit

Las IP SLAs probarán la disponibilidad de la interfaz R3, g2/0 cada 5 segundos. Para ello consideramos las direcciones IP asociadas a dicha interfaz en ipv4 y ipv6 y a estas se envía un ICMP-echo, luego se define el intervalo de tiempo entre ping generados a la interfaz mediante el comando frecuency, entonces:

Switch D2

Ip sla 4
Icmp-echo 10.0.11.1
Frecuency 5
exit
Ip sla 6
Icmp-echo 2001:db8:100:1011::1
Frecuency 5
Exit

Programe la SLA para una implementación inmediata sin tiempo de finalización, para lo cual se implementan los siguientes comandos en la configuración global:

Switch D2

Ip sla Schedule 4 life forever start-time now
Ip sla Schedule 6 life forever start-time now

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.
Use el número de rastreo 4 para la IP SLA 4.
Use el número de rastreo 6 para la IP SLA 6.

Usando el comando track y el número de la IP SLA, se comienza preparar HSRP para que use IP SLA, de la siguiente manera:

Switch D2

Track 4 ip sla 4

Exit

Track 6 ip sla 6

Exit

Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos, para ello consideramos el comando "*delay down # up #* ", de la siguiente manera:

Switch D2

Track 4 ip sla 4

Delay down 10 up 15

Exit

Track 6 ip sla 6

Delay down 10 up 15

Exit

4.3. En D1 configure HSRPv2.

D1 es el router primario para las VLANs 100 y 102; por lotanto, su prioridad también se cambiará a 150.

Configure HSRP versión 2. Para ello usamos el comando "standby versión 2" en cada una de las VLAN implicadas.

Switch D1

Interface vlan #

Standby versión 2

Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 y decremente en 60.

Descripción de los comandos: Se comienza por configurar el grupo 104 en la VLAN 100, se procede a asignar la IP virtual mediante el comando "*standby 104 ip #"* , luego se establece la prioridad mediante el comando "*priority"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D1

Interface vlan 100

Standby 104 ip 10.0.100.254

Standby 104 priority 150

Standby 104 preempt

Standby 104 track 4 decrement 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 114 en la VLAN 101, se procede a asignar la IP virtual mediante el comando "*standby 104 ip #"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D1

Interface vlan 101

Standby 114 ip 10.0.101.254

Standby 114 preempt

Standby 114 track 4 decrement 60

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 124 en la VLAN 102, se procede a asignar la IP virtual mediante el comando "*standby 104 ip #"* , luego se establece la prioridad mediante el comando "*priority"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D1

Interface vlan 102

Standby 124 ip 10.0.102.254

Standby 124 priority 150

Standby 124 preempt

Standby 124 track 4 decrement 60

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 6 y decremente en 60.

Descripción de los comandos: Se comienza por configurar el grupo 106 en la VLAN 100, se procede a asignar la IP virtual mediante el comando "*standby 106 ipv6 autoconfig",* luego se establece la prioridad mediante el comando "*priority"* y se

habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D1

Interface vlan 100
Standby 106 ipv6 autoconfig
Standby 106 priority 150
Standby 106 preempt
Standby 106 track 6 decrement 60

Configure IPv6 HSRP grupo 116 para la VLAN 101:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Habilite la preferencia (preemption).
Registre el objeto 6 y decremente en 60.

Descripción de los comandos: Se comienza por configurar el grupo 116 en la VLAN 101, se procede a asignar la IP virtual mediante el comando "*standby 106 ipv6 autoconfig",* se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D1

Interface vlan 101
Standby 116 ipv6 autoconfig
Standby 116 preempt
Standby 116 track 6 decrement 60

Configure IPv6 HSRP grupo 126 para la VLAN 102:
Asigne la dirección IP virtual usando ipv6 autoconfig.
Establezca la prioridad del grupo en 150.
Habilite la preferencia (preemption).

Rastree el objeto 6 y decremente en 60.

Descripción de los comandos: Se comienza por configurar el grupo 126 en la VLAN 102, se procede a asignar la IP virtual mediante el comando "*standby 106 ipv6 autoconfig",* luego se establece la prioridad mediante el comando "*priority"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D1

Interface vlan 102

Standby 126 ipv6 autoconfig

Standby 126 priority 150

Standby 126 preempt

Standby 126 track 6 decrement 60

4.4. En D2, configure HSRPv2.

D2 es el router primario para la VLAN 101; por lo tanto, superioridad también se cambiará a 150.

Configure HSRP versión 2. Para ello usamos el comando "standby versión 2" en cada una de las vlan implicadas.

Switch D2

Interface vlan #

Standby versión 2

D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 y decremente en 60.

Descripción de los comandos: Se comienza por configurar el grupo 104 en la VLAN 100, se procede a asignar la IP virtual mediante el comando "*standby 104 ip #"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D2

Interface vlan 100

Standby 104 ip 10.0.100.254

Standby 104 preempt

Standby 104 track 4 decrement 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 114 en la VLAN 101, se procede a asignar la IP virtual mediante el comando "*standby 104 ip #"* luego se establece la prioridad mediante el comando "*priority"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D2

Interface vlan 101

Standby 114 ip 10.0.101.254

Standby 114 priority 150

Standby 114 preempt

Standby 114 track 4 decrement 60

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

Habilite la preferencia (preemption).

Rastree el objeto 4 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 124 en la VLAN 102, se procede a asignar la IP virtual mediante el comando "*standby 104 ip #"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D2

Interface vlan 102

Standby 124 ip 10.0.102.254

Standby 124 preempt

Standby 124 track 4 decrement 60

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 106 en la VLAN 100, se procede a asignar la IP virtual mediante el comando "*standby 106 ipv6 autoconfig" y* se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D2

Interface vlan 100

Standby 106 ipv6 autoconfig

Standby 106 preempt

Standby 106 track 6 decrement 60

Configure IPv6 HSRP grupo 116 para la VLAN 101:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Establezca la prioridad del grupo en 150.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 116 en la VLAN 101, se procede a asignar la IP virtual mediante el comando "*standby 106 ipv6 autoconfig"* luego se establece la prioridad mediante el comando "*priority"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D2

Interface vlan 101

Standby 116 ipv6 autoconfig

Standby 116 priority 150

Standby 116 preempt

Standby 116 track 6 decrement 60

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6 autoconfig.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

Descripción de los comandos: Se comienza por configurar el grupo 126 en la VLAN 102, se procede a asignar la IP virtual mediante el comando "*standby 106 ipv6 autoconfig"* y se habilita la preferencia mediante "*preempt".* Por último, mediante el comando *"track*" se realizará el rastreo y se decrementará usando "*decrement*".

Switch D2

Interface vlan 102

Standby 126 ipv6 autoconfig

Standby 126 preempt

Standby 126 track 6 decrement 60

5. Parte 5. Seguridad

En esta parte se debían configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración fueron las siguientes:

5.1. En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

Contraseña: cisco12345cisco

En todos los dispositivos de la topología, se habilita la contraseña sugerida, pero teniendo en cuenta un método de encriptación mucho más seguro a través del comando “algorithm-type scrypt secret”.

All Devices

Enable algorithm-type scrypt secret cisco12345cisco

5.2. En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.

Detalles de la cuenta encriptada SCRYPT:

Nombre de usuario Local: sadmin

Nivel de privilegio 15

Contraseña: cisco12345cisco

Descripción de los comandos: En este caso se habilita en todos los dispositivos la epecificacion del usuario y la contraseña de este, implementando “algorithm-type scrypt secret”.

All Devices

Enable algorithm-type scrypt secret cisco12345cisco
Username sadmin privilege 15 algorithm-type scrypt secret cisco12345cisco

5.3. En todos los dispositivos (excepto R2), habilite AAA.

Habilite AAA.

Descripción de los comandos: En este caso se habilita AAA Authentication for Console Access, a excepción del Router R2.

All Devices, except R2.

Aaa new-model

5.4. En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

Especificaciones del servidor RADIUS.:

Dirección IP del servidor RADIUS es10.0.100.6.
Puertos UDP del servidor RADIUS son1812 y 1813.
Contraseña: $trongPass

Descripción de los comandos: Se procede a habilitar la relación entre los dispositivos y el RADIUS, para ello, se especifica la dirección IP del servidor en los dispositivos y los puertos UDP de esté mediante los comandos “auth-port” y “acct-port”, por último, se designa mediante el comando “key” la contraseña para el acceso.

All Devices, except R2.

En
Configure terminal
Radius server RADIUS
Address ipv4 10.0.100.6
Auth-port 1812 acct-port 1813
Key $trongPass

exit

5.5. En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA

Especificaciones de autenticación AAA:

Use la lista de métodos por defecto

Valide contra el grupo de servidores RADIUS

De lo contrario, utilice la base de datos local.

Descripción de los comandos: En este caso, se habilitarán los accesos a través del servidor RADIUS y se utilizará la base de datos local.

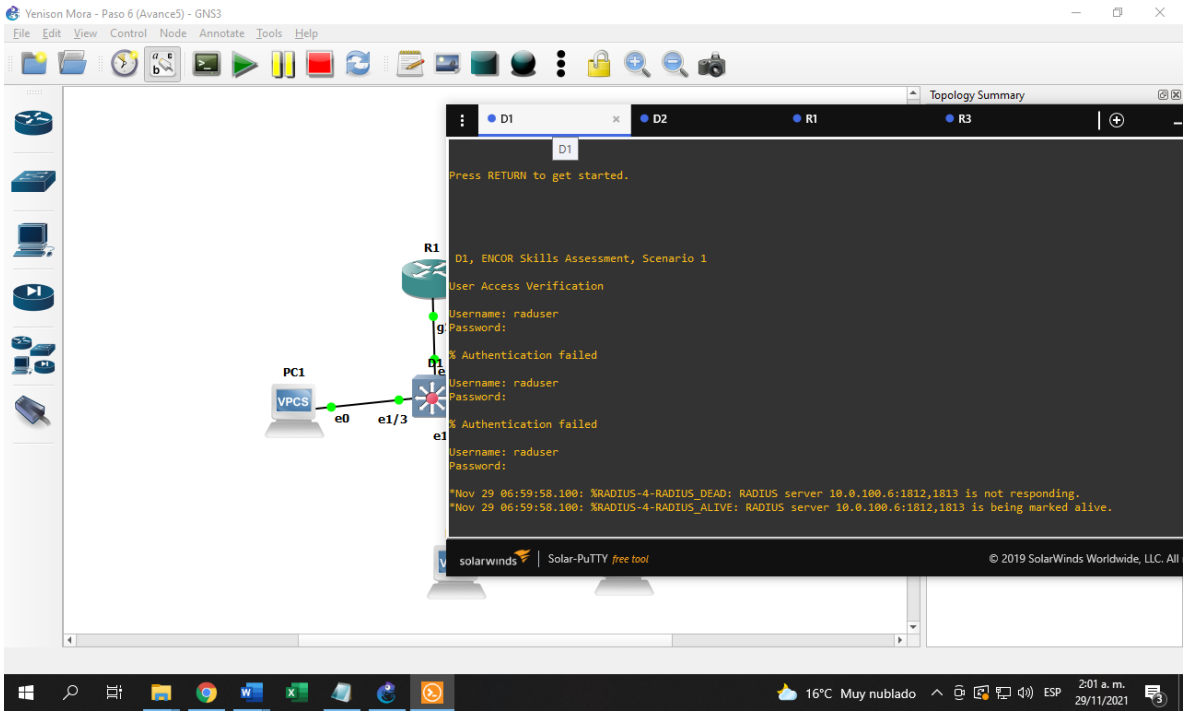
All Devices, except R2.

Aaa authentication login default group radius local

5.6. Verifique el servicio AAA en todos los dispositivos (except R2).

Cierre e inicie sesión en todos los dispositivos
(except R2) con el usuario: raduser y la contraseña: upass123.

Figura 7. Servicio y logging AAA.



6. Parte 6. Configure las funciones de administración de red.

En esta parte, se debían configurar varias funciones de administración de red. Las tareas de configuración fueron las siguientes:

6.1. En todos los dispositivos, configure el reloj local a la hora UTC actual. Configure el reloj local a la hora UTC actual.

All Devices

Clock set…

6.2. Configure R2 como un NTP maestro. Configurar R2 como NTP maestro en el nivel de estrato 3.

Descripción de los comandos: Se usa el comando NTP master 3, indicando que el dispositivo será master y que su estrato será el tercero.

Router R2

Enable
Configure terminal
Ntp master 3
end

6.3. Configure NTP en R1, R3, D1, D2,y A1. Configure NTP de la siguiente manera:

R1 debe sincronizar con R2, para ello se tiene en cuenta la dirección IP de loopback 0, la cual sería NTP.

R3, D1 y A1 para sincronizar la hora con R1. Para ellos se tiene en cuenta tomar como server la dirección IP que relación a R1, en este caso 10.0.10.1.
D2 para sincronizar la hora con R3.

Router R1

NTP server 2.2.2.2

Router R3, Switch D1, Switch D2. Switch A1.

NTP 10.0.10.1

6.4. Configure Syslog en todos los dispositivos excepto R2. Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

Descripción de los comandos: Se configura Syslog, para ello se usa el comando “logging trap warning” para seleccionar el nivel warning en el cual se enviará la información, luego mediante “logging host” seleccionamos la IP destino, la cual en este caso será PC1.

All Devices, except R2

Enable
Configure terminal
Logging trap warning
Logging host 10.0.100.5
Logging on
end

6.5. Configure SNMPv2c en todos losdispositivos excepto R2:

Especificaciones de SNMPv2:

Únicamente se usará SNMP en modo lectura (Read-Only).

Descripción de los comandos: En ese caso, se debe usar el comando “snmp-server community public ro”. Para habilitar el modo Read-only, donde “public” es el community string designado por defecto.

All Devices, except R2.

```
enable
configure terminal
snmp-server community public ro
end
```

Limite el acceso SNMP a la dirección IP de laPC1.

Descripción de los comandos: Mediante el comando “IP access-list standard SNMP-NMS” se logra establecer una sola ruta de acceso, la cual será a través de PC1.

All Devices, except R2.

```
Ip Access-list standard snmp-nms
Permit host 10.0.100.5
```

Configure el valor de contacto SNMP con su nombre.

Descripción de los comandos: En este caso, hacemos uso del comando “snmp-server contact” el cual permite añadir el nombre que se desee como valor de contacto SNMP.

All Devices, except R2

```
Snmp-server contact Yenison_Mora
```

Establezca el *community string* en ENCORSA.

Descripción de los comandos: En este caso, se especifica el community string asociado a SNMP.

All Devices, except R2.

```
enable
configure terminal
snmp-server community ENCORSA ro snmp-nms
end
```

En R3, D1, y D2, habilite el envío de *trapsconfig* y *ospf*.

Descripción de los comandos: Se realiza uso de los comandos “snmp-server enable traps config” y “snmp-server enable traps ospf”.

Router R3

```
snmp-server enable traps config
snmp-server enable traps ospf
```

Switch D1

```
snmp-server enable traps config
snmp-server enable traps ospf
```

Switch D2

```
snmp-server enable traps config
snmp-server enable traps ospf
```

En R1, habilite el envío de *traps bgp, config*, y *ospf*.

Descripción de los comandos: Se realiza uso de los comandos “snmp-server enable traps config”, “snmp-server enable traps ospf” y”, “snmp-server enable

traps bgp” para habilitar el envio traps bgp, config y ospf.

Router R1

snmp-server enable traps config
snmp-server enable traps ospf
snmp-server enable traps bgp

En A1, habilite el envío de *traps config*.

Switch A1

snmp-server enable traps config

CONCLUSIONES

A través de la implementación de los comandos usados para dar forma a la red del escenario, se pudo observar cómo se compone una verdadera red en nuestro entorno, que tipo de elementos deben tenerse en cuenta, pormenores que en ocasiones pueden presentarse en los equipos y demás características que en ocasiones pueden presentarse cuando se toma un escenario tan amplio y se combina con las temáticas vistas durante el estudio de CISCO.

A medida que se fue abordando cada parte del escenario y se fue desarrollando, se pudo evidenciar como se iban implementando temáticas que, en conjunto con muchas otras vistas en los laboratorios, todas estas integras hicieron de la red propuesta una excelente herramienta metodológica que no solo ayudo a repasar temáticas, sino que sintetizó en buena medida los elementos cognitivos adquiridos a lo largo de los cursos de CISCO y de los laboratorios del diplomado.

Son muchas las herramientas existentes para conformar una topología funcional, desde múltiples comandos, equipos o dispositivos de red electrónicos, protocolos de comunicación, modos de operación, entre otros, sin embargo mediante el paso a paso del escenario pudo verse como se constituye una red y que etapas y procesos son importantes y necesarios para dotar a todo nuestro sistema de una coherencia operativa y segura.

Se pudo observar como dependiendo de los softwares manejados y de la información base para trabajar el escenario, aún se presentaron dudas en la implementación de algunas características de los equipos, que en ocasiones varían dependiendo de los equipos, softwares manejados o interacción con otros comandos de otras configuraciones, lo que sin duda permite apreciar que el networking es un mundo amplio y que requiere un constante estudio que permita a través del tiempo, ir conociendo todas las características de una red e ir actualizando y mejorando estas con los múltiples avances, que muy seguramente vendrán a futuro.

BIBLIOGRAFÍA

CISCO. (2021, March 31). Funciones Y Funcionalidad de hot standby router protocol. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

CISCO. (2005, October 26). How to configure SNMP community strings. Recuperado de https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html

CISCO. (2019). Redes empresariales. Recuperado de https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdfs/smb-redes-mx.pdf

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

IBM. (2020). Direccionamiento TCP/IP. Recuperado de https://www.ibm.com/docs/es/aix/7.1?topic=protocol-tcpip-addressing

Luz, S. D. (2021, August 12). Que son las VLAN, para Que sirven Y Como funcionan con ejemplos de USO. Recuperado de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Luz, S. D. (2021, September 20). Que es un servidor RADIUS Y Como funciona para autenticar clientes. Recuperado de https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/

Sánchez, A. F. (2021, August 1). Routing dinámico con el protocolo BGP (teoría). Recuperado de https://network-tic.com/protocolo-bgp-teoria-routing-dinamico/