DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANYI PAOLA SIMIJACA GUZMÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA COLOMBIA
2021

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANYI PAOLA SIMIJACA GUZMÁN

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

DIRECTOR
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA COLOMBIA
2021

NOTA ACEPTACION

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

BOGOTA COLOMBIA, 29 de noviembre de 2021

AGRADECIMIENTOS

Al finalizar este trabajo quiero utilizar este espacio para agradecer a Dios por todas sus bendiciones, a mis Padres que han sabido darme su ejemplo de trabajo y honradez, por su apoyo y paciencia en este proyecto de estudio.

También quiero agradecer a la Universidad y docentes, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

REDES: Una red de telecomunicación es un conjunto de medios, tecnologías, protocolos y facilidades en general, necesarios para el intercambio de información y archivos entre los usuarios de una red. La red es una estructura, que, para su estudio suele dividirse en dos componentes: Red de acceso, Red de tránsito o núcleo de red, Servidor, Estaciones de trabajo, Recursos Periféricos y Compartidos

SPANNING TREE: es un protocolo de red de capa 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario.

CONMUTACION: La Conmutación se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor y un receptor a través de nodos o equipos de transmisión. La conmutación permite la entrega de la señal desde el origen hasta el destino requerido

ENRUTAMIENTO: o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

TELECOMUNICACIONES: es toda transmisión y recepción de señales de cualquier naturaleza, típicamente electromagnéticas, que contengan signos, sonidos, imágenes o, en definitiva, cualquier tipo de información que se desee comunicar a cierta distancia

RESUMEN

Nuestro entorno tal como lo conocemos, se mantiene en un intercambio constante de información en medios digitales, las redes de cómputo hacen posible esta tarea, cada día aumenta de forma exponencial, ya que se agregan nuevos dispositivos, tales como celulares, televisores, lavadoras y todo lo que comprende el IoT o internet de las cosas, entre otros.
Es por ello que surge una necesidad en el ámbito de las tecnologías de la información y es el de ingenieros que puedan realizar las implementaciones que contribuyan a la integración del mundo Electrónico y tecnológico.

En el siguiente trabajo escrito, se desarrollan las habilidades prácticas del diplomado CCNP, plasma el conocimiento adquirido, se puede apreciar, como todas y cada una de las actividades están enfocadas a la solución de problemas de la vida cotidiana de las empresas, las cuales dependen en gran medida de las tecnologías de la información.

Se realiza configuración de plataformas de conmutación y enrutamiento mediante el uso de herramientas de simulación como lo es cisco packet tracer entre otros.

ABSTRACT

Our environment as we know it is kept in constant ódigo of information in digital media, computer networks make this ódigo task, each day increases exponentially, as new devices, such as cell ódig, televisions, washing machines and everything that comprises the IoT or internet of things, among others.
That is why a need arises in the field of information technologies and is that of engineers who can perform the implementations that contribute to the integration of the Electronic and technological world.

In the following work, you write develop the practical skills of the CCNP diploma, reflects the knowledge acquired, it can be appreciated, as each and every one of the activities is focused on solving problems of the daily life of companies, which depend to a large extent on the information technology.

The configuration of switching and routing platforms is carried out through the use of simulation ódig such as cisco packet tracer among others.

INTRODUCCION

Mediante el presenta trabajo se configurarán plataformas de conmutación basadas en switches, mediante el uso de protocolos como STP y la configuración de VLANs en escenarios de red corporativos, para comprender el modo de operación de las subredes y los beneficios de administrar dominios de broadcast independientes, en múltiples escenarios al interior de una red jerárquica convergente.

También se usarán comandos IOS de configuración avanzada en routers (con direccionamiento Ipv4 e Ipv6) para protocolos de enrutamiento como: OSPF, EIGRP y BGP, en entornos de direccionamiento sin clase, con el fin diseñar e implementar soluciones de red escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.

Por medio de packet tracer se realizarán simulaciones y montajes basados en la vida real se abarca conceptos relacionados con el día a día de un ingeniero. Se logra establecer a topología de red, se verifica su correcto funcionamiento con el fin de resolver conflictos de configuración y conectividad.

ESCENARIO PROPUESTO

Topología de la Red:

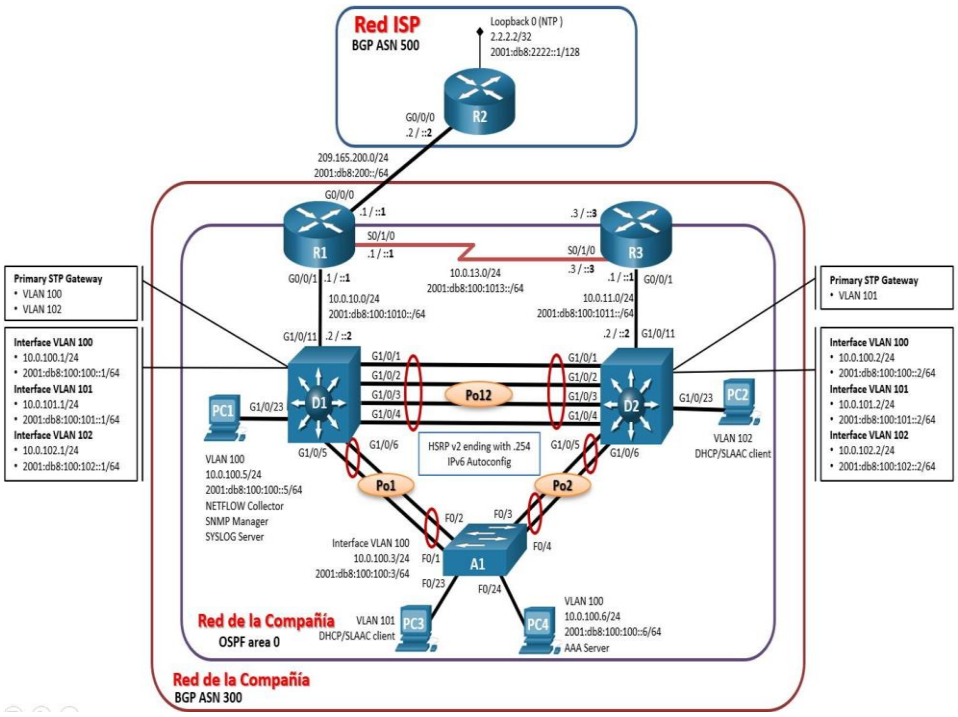

Ilustración 1. Topología Escenario propuesto

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección Ipv4	Dirección Ipv6	Ipv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	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	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

Tabla 1. Direccionamiento

Objetivos

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
Part 2: Configurar la capa 2 de la ed y el soporte de Host
Part 3: Configurar los protocolos de enrutamiento
Part 4: Configurar la redundancia del primer salto
Part 5: Configurar la seguridad
Part 6: Configurar las características de administración de red

Escenario

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default ódigo) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "**Red de la Compañía**" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere

Nota: Los routers usados son Cisco 4221 con CISCO IOS XE ódigo 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE ódigo 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tengan configuraciones de inicio.

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta Ipv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global **sdm prefer dual-ipv4-and-ipv6 default**. Cambiar la plantilla requerirá el reinicio del switch.

Recursos necesarios

- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

- 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
- 4 PCs (utilice el programa de emulación de terminal)
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
- Los cables Ethernet y seriales van como se muestra en la topología

.

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

Paso 1: Cablear la red como se muestra en la topología.

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

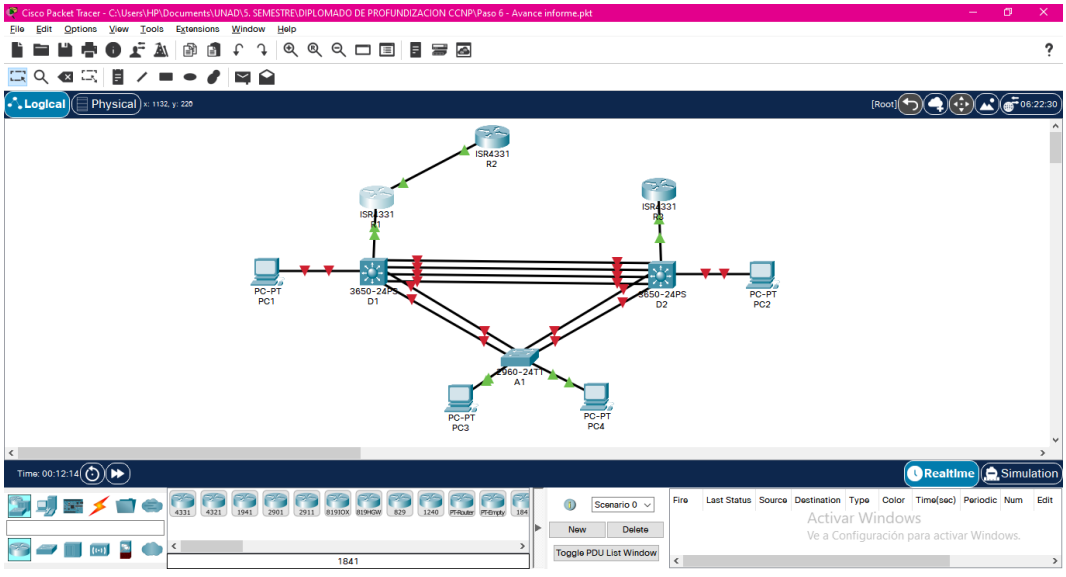

Ilustración 2. Diagrama diseñado

Paso 2: Configurar los parámetros básicos para cada dispositivo.

a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a

continuación:

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
```

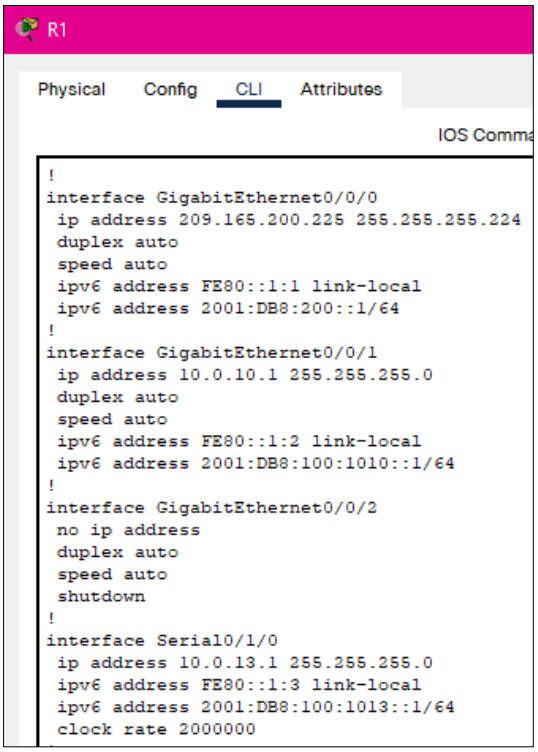

Ilustración 3. Configuración aplicada a R1

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

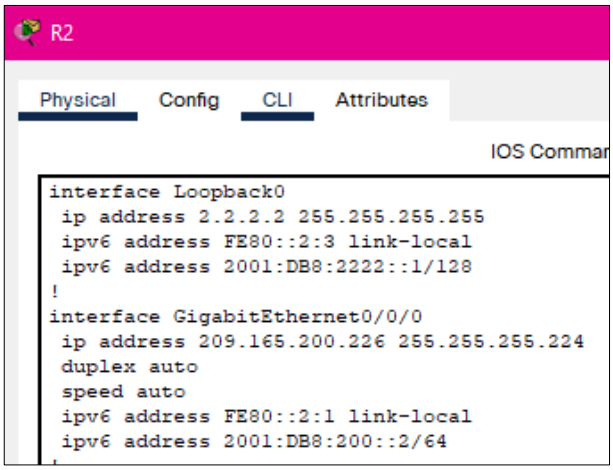

Ilustración 4. Configuración aplicada a R2

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

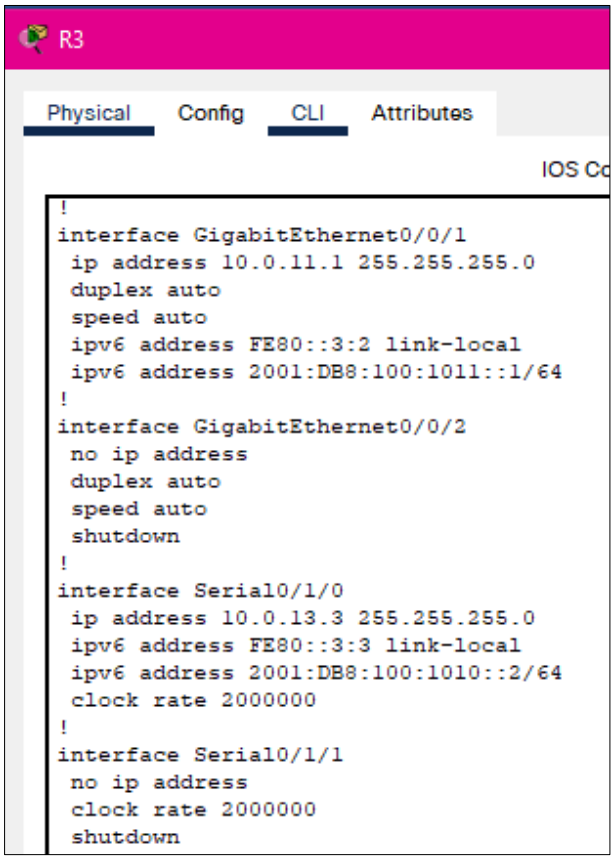

Ilustración 5. Configuración aplicada a R3

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

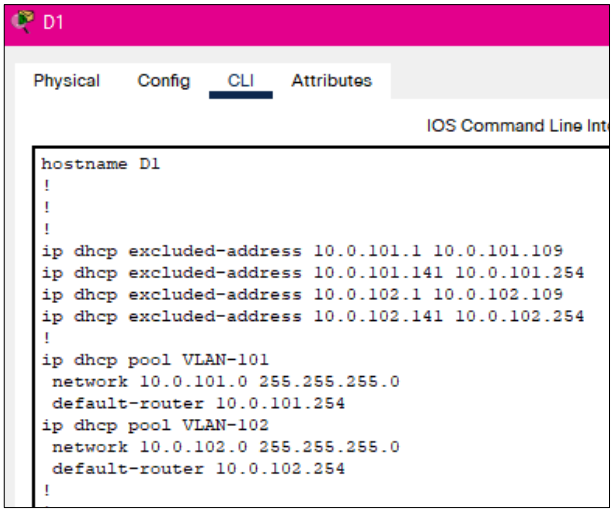

Ilustración 6. Configuración aplicada a D1

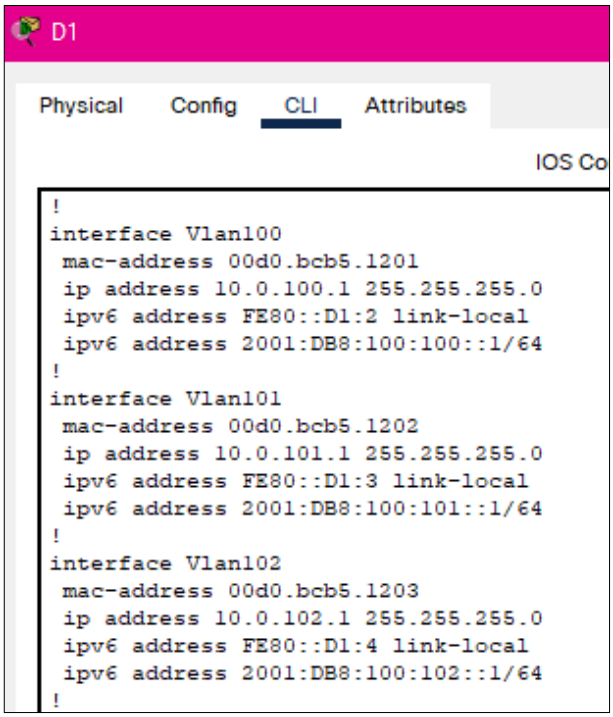

Ilustración 7. Configuración aplicada a D1

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

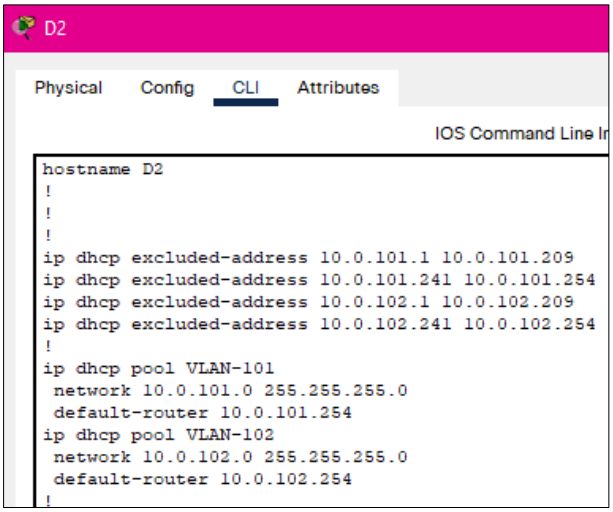

Ilustración 8. Configuración aplicada a D2

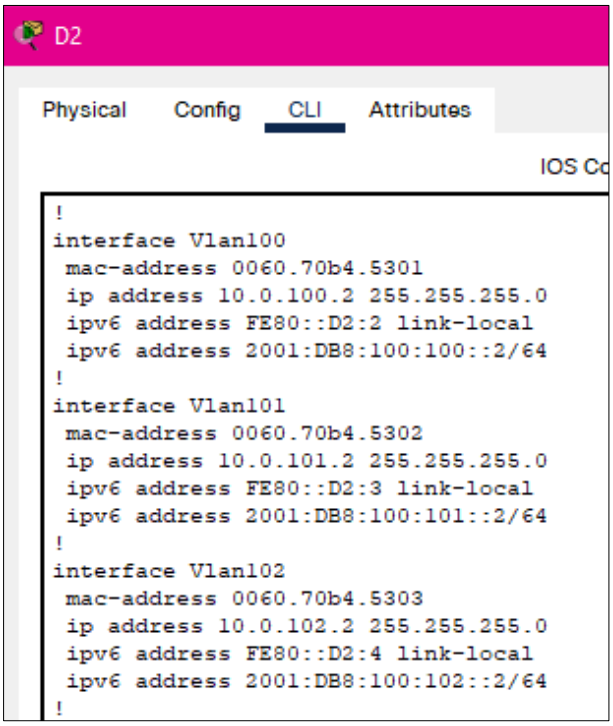

Ilustración 9. Configuración aplicada a D2

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

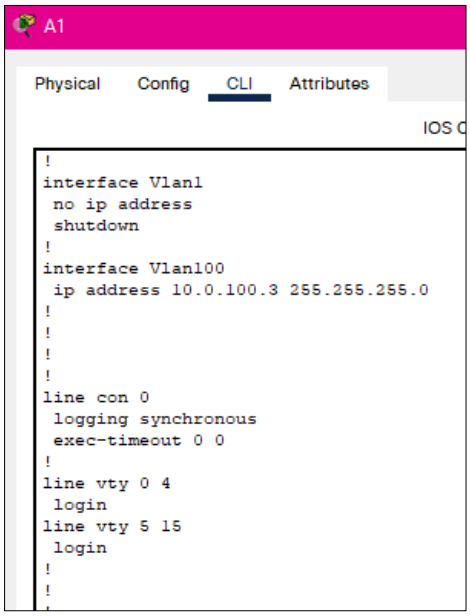

Ilustración 10. Configuración aplicada a A1

b. Copie el archivo **running-config** al archivo **startup-config** en todos los dispositivos.

c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

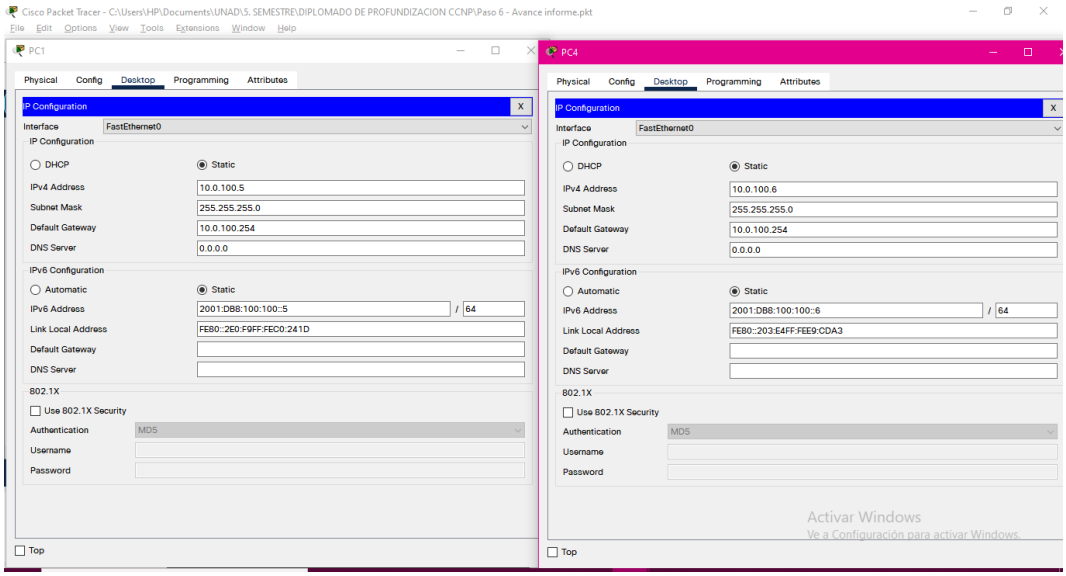

Ilustración 11. Direccionamiento PC1 Y PC4

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

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).

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.
2.5	En todos los switches, cree EtherChannels 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
2.6	En todos los switches, configure los puertos de acceso del host (host ódigo 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).
2.7	Verifique los servicios DHCP Ipv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones Ipv4 válidas.
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 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 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2

		• PC1: 10.0.100.5

Tabla 2. Configuración parte 2

Solución 2.1 y 2.2

Aquí se configurar la encapsulación que hace referencia a 802.1Q la cual es dot1q y se asigna la vlan nativa 999

CODIGO

```
D1>en
D1#conf term
D1(config)#int g1/0/1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#exit
```

```
Dl>en
Dl#config ter
Enter configuration commands, one per line.  End with CNTL/Z.
Dl(config)#int gl/0/l
Dl(config-if)#switchport trunk encapsulation dotlq
Dl(config-if)#switchport mode trunk
Dl(config-if)#
Dl(config-if)#
Dl(config-if)#switchport trunk native vlan 999
Dl(config-if)#exit
```

Ilustración 12. Configuración 802.1Q y vlan nativa

configuración conexión entre D1 y D2.

CODIGO

```
D1(config)#int g1/0/2
D1(config-if)#
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config)#int range g1/0/3-4
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if)#exit
D1(config)#int range g1/0/5-6
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
```

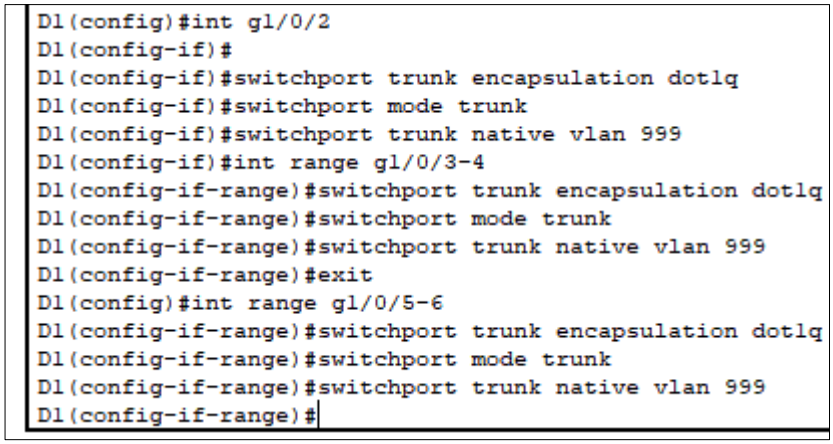

Ilustración 13.Configuración 802.1Q y vlan nativa

CODIGO

```
D2(config)#int range g1/0/5-6
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
```

```
D2(config)#int range gl/0/5-6
D2(config-if-range)#switchport trunk encapsulation dotlq
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#
```

Ilustración 14.Configuración 802.1Q y vlan nativa

Ilustración 12 – 13 y 14. Se ingresa al modo privilegiado, luego se ingresa a la configuración del terminal y se indica que conexión o interfaz se va a configurar, se define la encapsulación protocolo 802.1Q y se establece como troncal, por ultimo se configura la vlan nativa también

Se rectifica la configuración

CODIGO

D1# show interface switchport

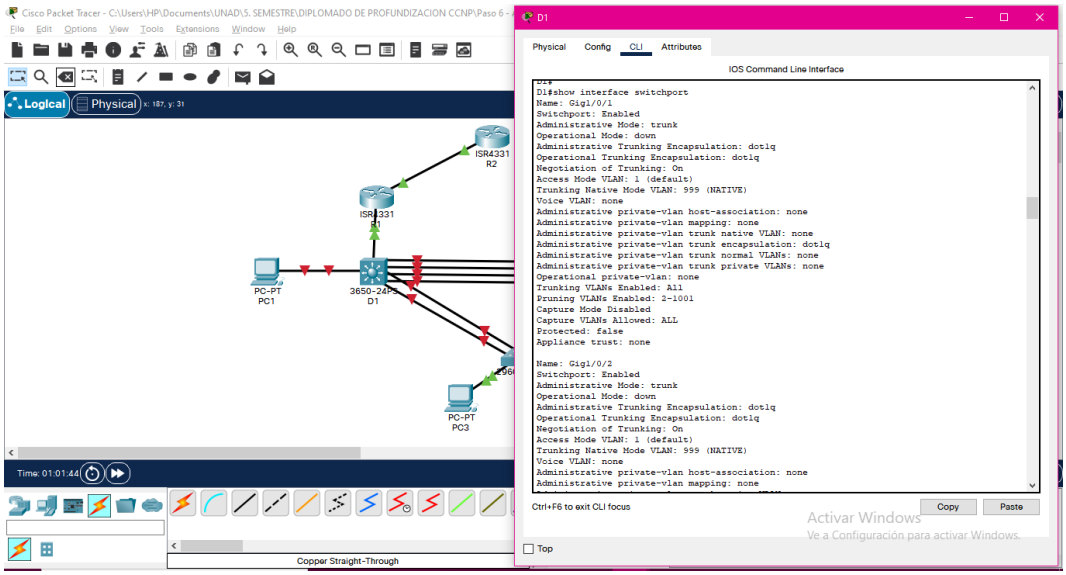

Ilustración 15. Show int swithport en D1

Ilustración 15. Aquí Vemos la configuración aplicada mediante los códigos anterior

Solución 2.3

Se realiza configuración protocolo RSPT

CODIGO

A1#conf term

A1(config)#spanning-tree mode rapid-pvst

A1#show spa

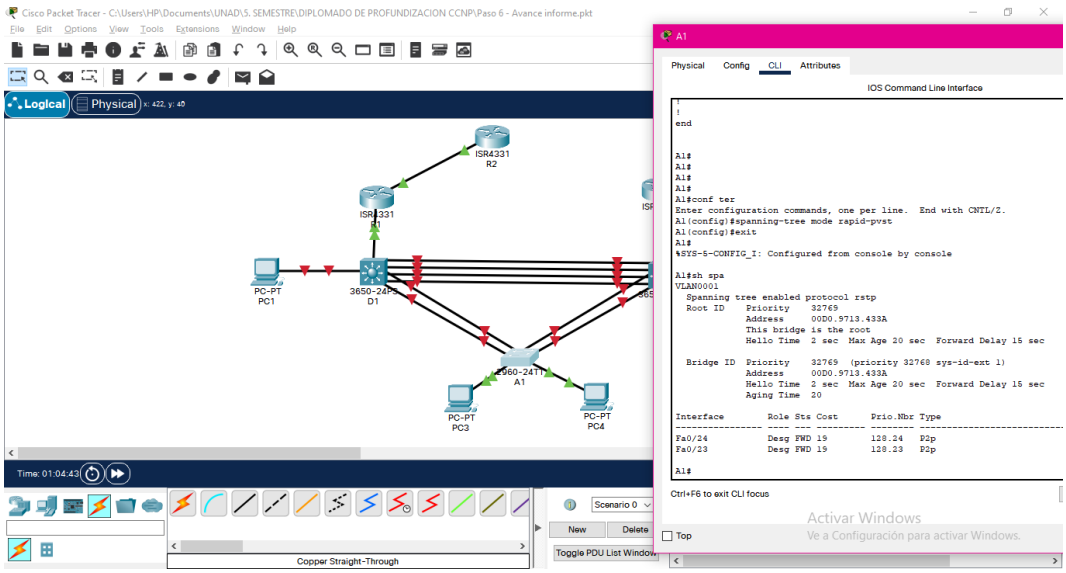

Ilustración 16. Configuración RSPT

Ilustración 16. Se realiza configuración del protocolo Rapid Spanning Tree (RSPT) y posteriormente de confirma su aplicación por medio del comando ***sh spa***

Solución 2.4

CODIGO

D1#conf term

D1(config)#spanning-tree vlan 100,102 root primary

D1(config)#spanning-tree vlan 101 root secondary

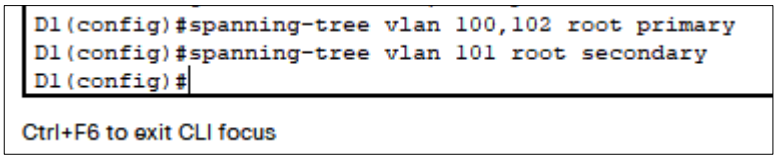

Ilustración 17. Configuración root D1

Ilustración 17. Se crean los puentes con propiedades “root”

CODIGO

D2#conf term
D2#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary

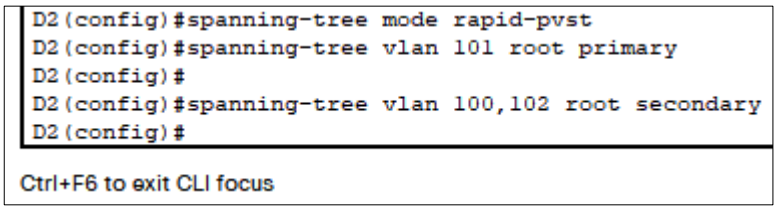

Ilustración 18. Configuración root D2

Solución 2.5

CODIGO

D1#conf term
D1(config)#interface range g1/0/1-4
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active
D1#(config-if-range)#no shutdown

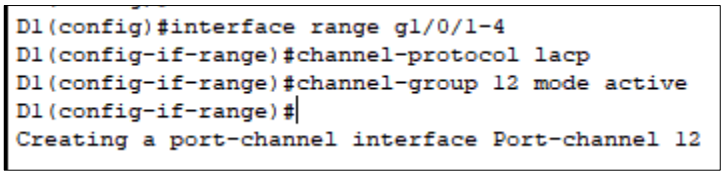

Ilustración 19. Configuración EtherChannels LACP en D1

CODIGO

D2#conf term
D2(config)#spanning-tree vlan 101 root primary
D2(config)#interface range g1/0/1-4
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active

D2(config-if-range)#no shutdown

```
D2(config)#spanning-tree vlan 101 root primary
D2(config)#interface range g1/0/1-4
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 12
```

Ilustración 20.Configuración EtherChannels LACP en D2

Ilustración 19 y 20 Se configura los canales en D1 a D2 – Port channel 12, se selecciona el protocolo lacp y se nombre el grupo por ultimo se cambia estado de la interfaz

CODIGO

D1(config)#interface range g1/0/5-6

D1(config-if-range)#channel-protocol lacp

D1(config-if-range)#channel-group 1 mode active

```
D1(config)#interface range g1/0/5-6
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 1
```

Ilustración 21.Configuración EtherChannels LACP D1

CODIGO

A1#conf term

A1(config)#interface range f0/1-2

A1(config-if-range)#channel-protocol lacp

A1(config-if-range)#channel-group 1 mode active

A1(config-if-range)#no shutdown

```
A1(config)#interface range f0/1-2
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#
Creating a port-channel interface Port-channel 1
```

Ilustración 22.Configuración EtherChannels LACP A1

Ilustración 21 y 22 Se configura los canales en D1 a A1 – Port channel 1, se selecciona el protocolo lacp y se nombre el grupo.

CODIGO

D2(config)#interface range g1/0/1-6
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active

```
D2(config)#interface range g1/0/1-6
D2(config-if-range)#
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
```

Ilustración 23.Configuración EtherChannels LACP D2

CODIGO

A1(config)#interface range f0/3-4
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode active

```
A1(config)#interface range f0/3-4
A1(config-if-range)#
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode active
```

Ilustración 24.Configuración EtherChannels LACP A1

Ilustración 23 y 24 Se configura los canales en D2 a A1 – Port channel 2, se selecciona el protocolo lacp y se nombre el grupo.

Solución 2.6

CODIGO

D1(config)#int g1/0/23
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)# spanning-tree portfast

```
D1(config)#int g1/0/23
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
```

Ilustración 25. Configuración host ódigo port D1

CODIGO

```
A1(config)#interface f0/23
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#exit
A1(config)#interface f0/24
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
```

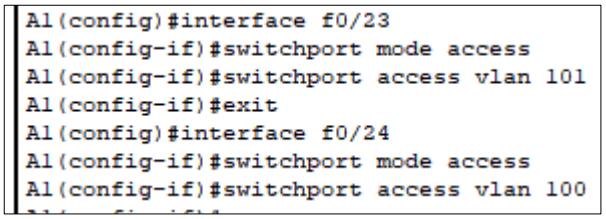

Ilustración 26.Configuración host ódigo port A1

CODIGO

```
D2(config)#int g1/0/23
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
```

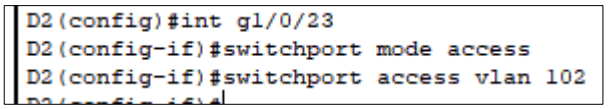

Ilustración 27.Configuración host ódigo port D2

Ilustración 25, 26 y 27 se selección los puertos a configurar, se pone en modo acceso, luego se asigna la vlan

Solución 2.7

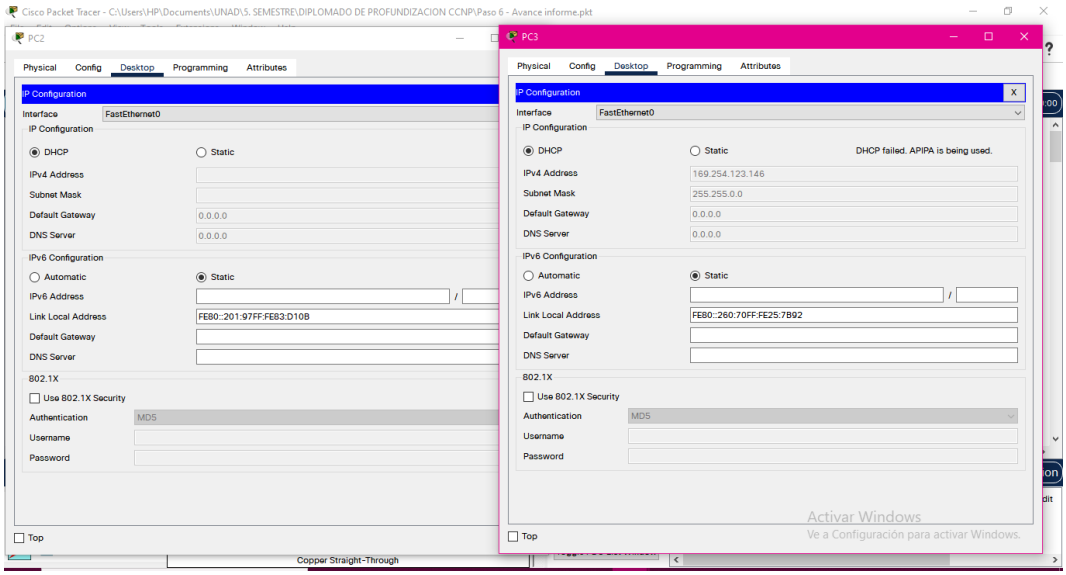

Ilustración 28. Configuración DHCP en PC2 Y PC3

Ilustración 28. Revisamos que los equipos PC2 y PC3 estén configurados con DHCP

Solución 2.8

```
C:\>ping 10.0.100.2

Pinging 10.0.100.2 with 32 bytes of data:

Reply from 10.0.100.2: bytes=32 time=19ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms
```

Ilustración 29.Conectividad PC1

```
Pinging 10.0.102.1 with 32 bytes of data:

Reply from 10.0.102.1: bytes=32 time=11ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.0.102.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Ilustración 30.Conectividad PC2

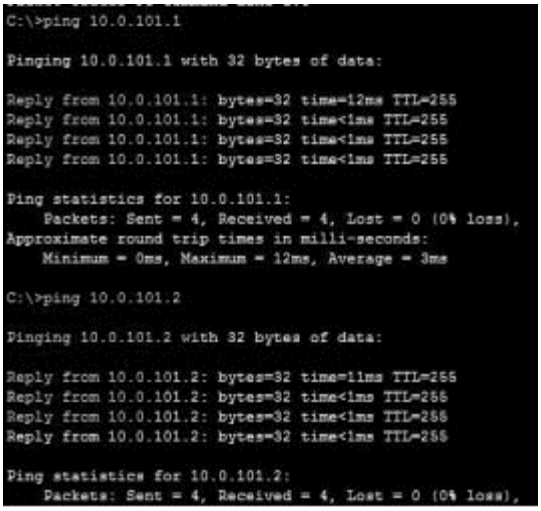

Ilustración 31.Conectividad PC3

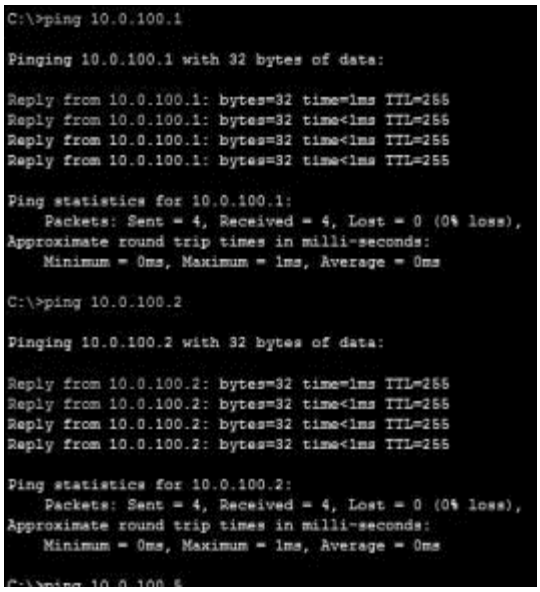

Ilustración 32.Conectividad PC4

Ilustración 29, 30, 31 y 32 se realizan pruebas de conectivas sobre los 4 PC

Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento Ipv4 e Ipv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de Ipv4 e Ipv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- ódi OSPFv2 en ódi 0.	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 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en ódi 0.	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 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

Tarea #	Tarea	Especificación
3.3	En R2 en la “Red ISP”, configure MP- BGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada Ipv4. • Una ruta estática predeterminada Ipv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino Ipv4 e Ipv6 con R1 en ASN 300. En Ipv4 address family, anuncie: • La red Loopback 0 Ipv4 (/32). • La ruta por defecto (0.0.0.0/0). En Ipv6 address family, anuncie: • La red Loopback 0 Ipv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MP- BGP.	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. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino Ipv4 e Ipv6 con R2 en ASN 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. En Ipv6 address

		family: • Deshabilite la relación de vecino Ipv4. • Habilite la relación de vecino Ipv6. • Anuncie la red 2001:db8:100::/48.

Tabla 3. Configuración parte 3

Solución 3.1

CODIGO

```
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#do show ip route connected
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)# default-information originate
R1(config-router)#exit
```

```
R1(config-router)#router-id 0.0.4.1
R1(config-router)#do show ip route connected
 C   10.0.10.0/24  is directly connected, GigabitEthernet0/0/1
 C   209.165.200.224/27  is directly connected, GigabitEthernet0/0/0

R1(config-router)#network 10.0.10.0 0.0.0.255
% Incomplete command.
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
```

Ilustración 33. Configuración OSPF en R1

CODIGO

```
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#do show ip route connected
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
```

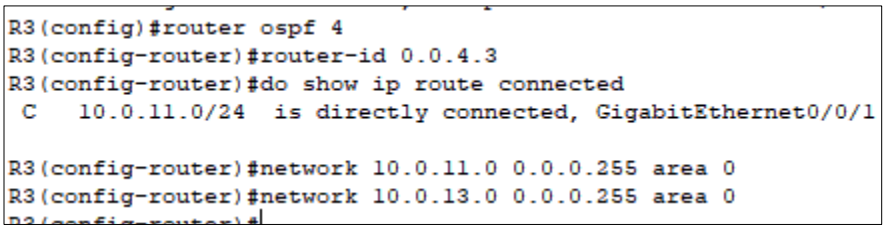

Ilustración 34. Configuración OSPF en R3

CODIGO

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#do show ip route connected
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface g1/0/11
```

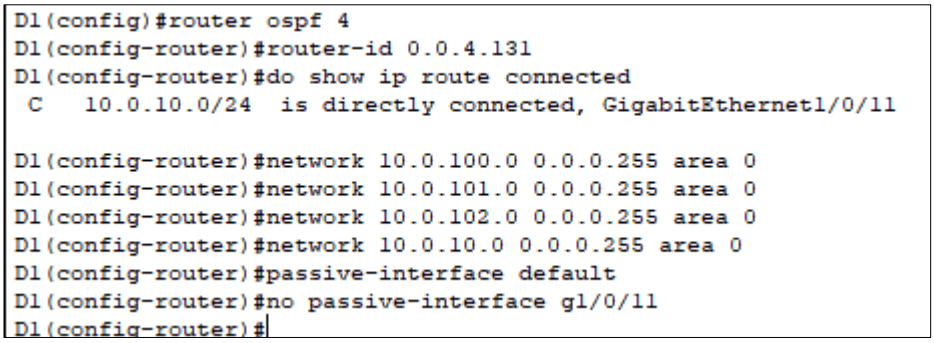

Ilustración 35. Configuración OSPF en D1

CODIGO

```
D2(config)#router ospf 4
```

D2(config-router)#router-id 0.0.4.132
D2(config-router)#do show ip route connected
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface g1/0/11

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#do show ip route connected
 C    10.0.11.0/24  is directly connected, GigabitEthernet1/0/11

D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#
01:43:35: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on GigabitEthernet1/0/11 from EXSTART to
DOWN, Neighbor Down: Interface down or detached

D2(config-router)#no passive-interface g1/0/11
D2(config-router)#
D2(config-router)#
01:43:43: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on GigabitEthernet1/0/11 from LOADING to
FULL, Loading Done
```

Ilustración 36.Configuración OSPF en D2

Ilustracion 33, 34, 35 y 36 – Compañía se asigna ospf y id 4, se le asigna al router ID de acuerdo a su respectiva ódigo ón se listan las interfaces conectadas, Se realiza el mismo código en R1,R3,D1 y D2

Solución 3.2

CODIGO

R1(config)#ipv6 router ospf 6 / se configura ospf en ipv6
R1(config-rtr)#router-id 0.0.6.1 /se asigna id
R1(config-rtr)# default-information originate
R1(config-rtr)#exit
R1(config)#int g0/0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ipv6 ospf 6 area 0

```
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#int g0/0/1
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#
```

Ilustración 37. Configuración Ipv6 en R1

CODIGO

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)# interface g0/0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#int s0/1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
```

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface g0/0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#int s0/1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#
```

Ilustración 38.. Configuración Ipv6 en R3

CODIGO

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)# passive-interface default
D1(config-rtr)# no passive-interface g1/0/11
D1(config-rtr)#exit
D1(config)# interface g1/0/11
D1(config-if-range)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int interface vlan 100
```

D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int interface vlan 101
D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int interface vlan 102
D1(config)#ipv6 ospf 6 area 0

```
Dl(config)#ipv6 router ospf 6
Dl(config-rtr)#router-id 0.0.6.131
Dl(config-rtr)#passive-interface default
Dl(config-rtr)#no passive-interface gl/0/ll
```

Ilustración 39.. Configuración Ipv6 en D1

```
Dl(config-rtr)#exit
Dl(config)#interface gl/0/ll
Dl(config-if)#ipv6 ospf 6 area 0
Dl(config-if)#exit
Dl(config)#int vlan l00
Dl(config-if)#ipv6 ospf 6 area 0
Dl(config-if)#exit
Dl(config)#int vlan l01
Dl(config-if)#ipv6 ospf 6 area 0
Dl(config-if)#exit
Dl(config)#int vlan l02
Dl(config-if)#ipv6 ospf 6 area 0
```

Ilustración 40.. Configuración Ipv6 en D1

CODIGO

D2(config)#ipv6 router ospf 6
D2(config-rtr) #router-id 0.0.6.132
D2(config-rtr)# passive-interface default
D2(config-rtr)# no passive-interface g1/0/11
D2(config-rtr)#exit
D2(config)#int range g1/0/11
D2(config-if-range)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#int g1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0

D2(config-if)#exit
D2(config-if)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#end

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface gl/0/11
```

Ilustración 41.. Configuración Ipv6 en D2

```
D2(config-rtr)#exit
D2(config)#int range gl/0/11
D2(config-if-range)#ipv6 ospf 6 area 0
D2(config-if-range)#exit
D2(config)#int gl/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
```

Ilustración 42.. Configuración Ipv6 en D2

Ilustración 37, 38, 39, 40, 41 y 42 Compañía por medio de los ódigo se configura ospf en ipv6, se asigna id, se declara información predeterminada, se asigna área 0 en ipv6 en las interfaces requerida, se aplica el mismo ódigo para R1, R3, D1 y D2

Solución 3.3

CODIGO

```
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 0
R2(config-if)# ipv6 route ::/0 loopback 0
R2(config-router)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1/64 remote-as 300
```

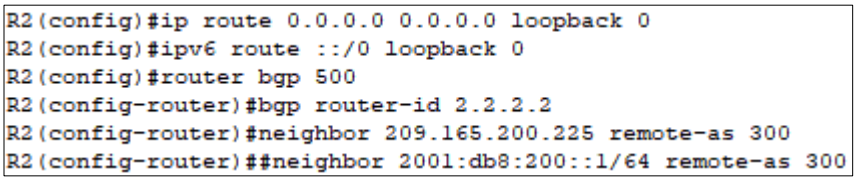

Ilustración 43.Configuración ruta estática en R2

Ilustracion 43. Por medio de esta ódig de comandos Se nombra la interfaz a configurar y se establece los parámetros a configurar con ip y mascara de red, luego se establece el router con bgp 500, se asigna el id y se define la relación vecino ipv4 e ipv6

CODIGO

```
R2(config-router)#address-family ipv4
R2(config-router)# neighbor 209.165.200.225 activate
R2(config-router)# no neighbor 2001:db8:200::1 activate
R2(config-router)# network 2.2.2.2 mask 255.255.255.255
R2(config-router)#neighbor 0.0.0.0/0
R2(config-router)# exit-address-family
R2(config-router)#address-family ipv6
R2(config-router)# no neighbor 209.165.200.225 activate
R2(config-router)# neighbor 2001:db8:200::1 activate
R2(config-router)# network 2001:db8:2222::/128
R2(config-router)# network ::/0
R2(config-router)# exit-address-family
```

En el ódigo anterior se anuncia La red Loopback 0 Ipv4 y La ruta por defecto,

Solución 3.4

CODIGO

R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500

```
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 209.165.200.226 Up

R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
```

Ilustración 44.Configuración BGP ASN

Ilustración 44. Se asigna bgp y ns 300, se asigan id del route y r se define la relación vecino ipv4 e ipv6

En este momento En Ipv4 address family: se deshabilita la relación de vecino Ipv6.se habilita la relación de vecino Ipv4. Y se Anuncie la red 10.0.0.0/8.

CODIGO

R1(config-router)# address-family ipv4 unicast
R1(config-router)# neighbor 209.165.200.226 activate
R1(config-router)# no neighbor 2001:db8:200::2 activate
R1(config-router)# network 10.0.0.0 mask 255.0.0.0
R1(config-router)# exit-address-family

Ahora En Ipv6 address family se deshabilita la relación de vecino Ipv4, se habilita la relación de vecino Ipv6.y se anuncia la red 2001:db8:100::/48

CODIGO

R1(config-router)# address-family ipv6 unicast
R1(config-router)# no neighbor 209.165.200.226 activate
R1(config-router)# neighbor 2001:db8:200::2 activate
R1(config-router)# network 2001:db8:100::/48
R1(config-router)# exit-address-family

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

En esta parte, debe configurar HSRP version 2 para proveer redundancia de primer salto para los host en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. • Use la SLA número **4** para Ipv4. • Use la SLA número **6** para Ipv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. 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. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. • Use la SLA número **4** para Ipv4. • Use la SLA número **6** para Ipv6. Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Tarea #	Tarea	Especificación
4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP ódigo 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. 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. 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. 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. 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. 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.

Tarea #	Tarea	Especificación
	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP ódigo 2. 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. 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. 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. 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. 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. 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.

Tabla 4.Configuración parte 4

Solución 4.1

En D1 – Se crean dos IP SLAs: SLA número 4 para Ipv4 y SLA número 6 para Ipv6, se prueba disponibilidad de la interfaz cada 5 segundos

```
D1(config)# ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
```

El código anterior lo usamos también para Ipv6

```
D1(config)# ip sla 6
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
```

Se programa SLA para una implementación inmediata, sin tiempo de finalización.

```
D1(config-ip-sla)# ip sla schedule 4 life forever start-time
D1(config-ip-sla)# ip sla schedule 6 life-forever start-time now
```

Se crea una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. Se usa el número de rastreo 4 para la IP SLA 4. Y el número de rastreo 6 para la IP SLA 6

```
D1(config-ip-sla)# track 4 ip sla 4
D1(config-ip-sla-track)# delay down 10 up 15
D1(config-ip-sla-track)#exit
D1(config-ip-sla)# track 6 ip sla 6
D1(config-ip-sla-track)# delay down 10 up 15
D1(config-ip-sla-track)#exit
```

Solución 4.2

En D2 – Se crean dos IP SLAs: SLA número 4 para Ipv4 y SLA número 6 para Ipv6, se prueba disponibilidad de la interfaz cada 5 segundos

```
D2(config)# ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.
D2(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
```

El ódigo anterior lo usamos también para Ipv6

```
D2(config)# ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)# exit
```

Se programa SLA para una implementación inmediata, sin tiempo de finalización.

```
D2(config-ip-sla)# ip sla schedule 4 life forever start-time now
D2(config-ip-sla)# ip sla schedule 6 life-forever start-time now
```

Se crea una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. Se usa el número de rastreo 4 para la IP SLA 4. Y el número de rastreo 6 para la IP SLA 6

```
D2(config-ip-sla)# track 4 ip sla 4
D2(config-ip-sla-track)# delay down 10 up 15
D2(config-ip-sla-track)#exit
D2(config-ip-sla)# track 6 ip sla 6
D2(config-ip-sla-track)# delay down 10 up 15
D2(config-ip-sla-track)#exit
```

Solucion 4.3

Ahora para D1 – se configura Ipv4 HSRP grupo 104 para la VLAN 100, se asigna la dirección IP virtual 10.0.100.254, se habilita la prioridad del grupo en 150 y la preferencia (preemption) Por ultimo se rastrea el objeto 4 y decremente en 60

```
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
```

Se configura Ipv4 HSRP grupo 114 para la VLAN 101, se asigna la dirección IP virtual 10.0.101.254. se habilita la preferencia (preemption) y se rastree el objeto 4 para disminuir en 60.

```
D1(config)#interface vlan 101
D1(config-if)# standby version 2
D1(config-if)# standby 114 ip 10.0.101.254
D1(config-if)# standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
```

Ahora se utiliza el ódigo anterior, y se configura la vlan 102, se cambia la ip virtual.

```
D1(config)#interface vlan 102
D1(config-if)# standby version 2
D1(config-if)# standby 124 ip 10.0.102.254
D1(config-if)# standby 124 priority 150
D1(config-if)# standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
```

Utilizando el ódigo anterior se cambia a ipv6, se cambia la vlan y la ip virtua

```
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
```

Usando de nuevo el codigo anterior, cambiamos el grupo y la vlan y no se establece prioridad

```
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track 6 decrement 60
```

Con los mismos codigos anteriores se configura Ipv6 HSRP grupo 126 para la VLAN 102: se asigna la dirección IP virtual , se establece la prioridad del grupo en 150. Y se habilita la preferencia (preemption). Por ultimo se rastrea el objeto 6 y decremente en 60.

```
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)# standby 126 priority 150
D1(config-if)# standby 126 preempt
D1(config-if)# standby 126 track 6 decrement 60
```

Solucion 4.4

En D2, configure HSRPv2, se utiliza el código del punto anterior solo que se realiza cambio de ip y vlan

```
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 track 4 decrement 60
D2(config-if)#interface vlan 101
D2(config-if)# standby version 2
D2(config-if)# standby 114 ip 10.0.101.254
D2(config-if)# standby 114 priority 150
D2(config-if)# standby 114 preempt
D2(config-if)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)#standby 124 track 4 decrement 60.
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 106 track 6 decrement 60
```

```
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)# standby 116 priority 150
D2(config-if)# standby 116 preempt
D2(config-if)# standby 116 track 6 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60
```

Parte 5: Seguridad

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

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **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**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**

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.
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**.

Tabla 5. Configuración parte 5

Solución 5.1, 5.2 y 5.3

En cada dispositivo se protege el EXEC privilegiado usando el algoritmo de encripción SCRYPT. Contraseña: cisco12345cisc.
Primero se asigna contraseña a modo privilegiado, luego se encripta la contraseña, se crea sesión privilegio 15 y por ultimo se crea usuario y contraseña encriptada para el usuario.

```
R2(config)#enable password cisco12345cisco
R2(config)#service password-encryption
R2(config)#exit
R2(config)#enable secret level 15 cisco12345cisco
R2(config)#username sadmin privilege 15 secret

R1(config)#enable password cisco12345cisco
R1(config)#service password-encryption
R1(config)#enable secret level 15 cisco12345cisco
R1(config)#username sadmin privilege 15 secret cisco12345cisco
R1(config)#aaa new-model / se declara el modelo AAA

R3(config)#enable password cisco12345cisco
```

```
R3(config)#service password-encryption
R3(config)#enable secret level 15 cisco12345cisco
R3(config)#username sadmin privilege 15 secret cisco12345cisco
R3(config)#aaa new-model

D1(config)#enable password cisco12345cisco
D1(config)#service password-encryption
D1(config)#enable secret level 15 cisco12345cisco
D1(config)#username sadmin privilege 15 secret cisco12345cisco
D1(config)#aaa new-model

D2(config)#enable password cisco12345cisco
D2(config)#service password-encryption
D2(config)#enable secret level 15 cisco12345cisco
D2(config)#username sadmin privilege 15 secret cisco12345cisco
D2(config)#aaa new-model
```

Solución 5.4, 5.5 y 5.6

Ahora en cada uno de los dispositivos, se procede a configurar RADIUS, primero llamamos el modelo a configurar, luego se indica el servidor a configurar, se asigna los puertos y la dirección del servidor

```
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)#key $trongPass

R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)#key $trongPass
R3(config-radius-server)#exit
R3(config)#aaa authentication login default group radius local
R3(config)#end
```

```
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port
1813
D2(config-radius-server)#key $trongPass
D2(config-radius-server)#exit
D2(config)#aaa authentication login default group radius local
D2(config)#end

D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port
1813
D1(config-radius-server)#key $trongPass
D1(config-radius-server)#exit
D1(config)#aaa authentication login default group radius local
D1(config)#end

A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port
1813
A1(config-radius-server)#key $trongPass
A1(config-radius-server)#exit
A1(config)#aaa authentication login default group radius local
A1(config)#end
```

Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

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

6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
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.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *traps config* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

Tabla 6. Configuración parte 6

Solución 6.1

En todos los dispositivos, se configura el reloj local a la hora UTC actual

```
R1#show clock
*2:9:46.478 UTC Mon Mar 1 1993
```

```
R1# clock set 12:34:00 27 Nov 2021
R2# clock set 12:34:00 27 Nov 2021
R3# clock set 12:34:00 27 Nov 2021
D2# clock set 12:34:00 27 Nov 2021
D1# clock set 12:34:00 27 Nov 2021
A1# clock set 12:34:00 27 Nov 2021
```

Solución 6.2

Se configura NTP maestro en el nivel de estrato 3

```
R2(config)#ntp master 3
```

Solución 6.3, 6.4 y 6.5

En los siguientes puntos vamos a configurar: NTP, Syslogs en nivel warning, se envían a la PC1 en 10.0.100.5 tambien se cambia a encendido, se configura SNMP lectura, se declara límite de acceso se asigna el valor de contacto SNP, se establece y se declara el host, se habilita el envío de traps

```
R1(config)#ntp server 2.2.2.2
R1(config)#logging trap warning
R1(config)#logging host 10.0.100.5
R1(config)#logging on
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)#permit host 10.0.100.5
R1(config-std-nacl)#exit
R1(config- snmp)#snmp-server contact Cisco gustavoR
R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
R1(config- snmp)#snmp-server host 10.0.100.5 versión 2c ENCORSA
R1(config- snmp)#snmp-server ifindex persist
R1(config- snmp)#snmp-server enable traps bgp
R1(config- snmp)#snmp-server enable traps config
R1(config- snmp)# snmp-server enable traps ospf
R1(config- snmp)#end
```

```
R3(config)#logging host 10.0.100.5
R3(config)#logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#permit host 10.0.100.5
R3(config-std-nacl)#exit
R3(config- snmp)#snmp-server contact Cisco gustavoR
R3(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
R3(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config- snmp)#snmp-server ifindex persist
R3(config- snmp)#snmp-server enable traps config
R3(config- snmp)#snmp-server enable traps ospf
```

```
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Cisco gustavoR
D1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config- snmp)#snmp-server ifindex persist
D1(config- snmp)#snmp-server enable traps config
D1(config- snmp)#snmp-server enable traps ospf
```

```
D2(config)#ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config)#snmp-server contact Cisco GustavoR
D2(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
D2(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config- snmp)# snmp-server enable traps config
```

```
D2(config- snmp)#snmp-server enable traps ospf

A1(config)#ntp server 10.0.10.1
A1(config)#logging trap warning
A1(config)#logging host 10.0.100.5
A1(config)#logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#exit
A1(config)#snmp-server contact Cisco gustavoR
A1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
A1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config- snmp)#snmp-server ifindex persist
A1(config- snmp)#snmp-server enable traps config
A1(config- snmp)#snmp-server enable traps ospf
```

CONCLUSIONES

Esta práctica sirve para poder afianzar los conocimientos adquiridos a lo largo del curso, temas como enrutamiento, configuración de vlan, son temas que se usan en el día a día del ingeniero de telecomunicaciones sistemas o electrónico.

La mínima configuración básica del switch debe incluir desde el nombre del dispositivo, es decir el nombre con el cuál se va a referir en la configuración, la forma detallada de la estructura de interfaces que lo componen, la asignación de contraseñas, el mensaje de alerta (MOTD), la tabla de direccionamiento en donde se señala la asignación de las IP, las direcciones MAC, dinámicas o estática y administración remota del switch

Spanning Tree es un protocolo utilizado para enfrentar los inconvenientes de bucles y tramas duplicadas al asegurar que exista sólo una ruta lógica entre todos los destinos de la red, al bloquear de forma intencional aquellas rutas redundantes.

Por medio del simulador cisco packet tracer, se logra realizar un análisis de los múltiples protocolos, se logra definir su comportamiento, así como el de los equipos y routers usados.

BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **OSPF v3**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Cómo Utilizar HSRP para Proporcionar Redundancia en una Roja de BGP con Varias Conexiones. (2021, 7 julio). Cisco. Recuperado 12 de noviembre de 2021, de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocolbgp/13768-hsrp-bgp.html