DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GUSTAVO ADOLFO ROMERO CAGUA

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

DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GUSTAVO ADOLFO ROMERO CAGUA

Diplomado de opción de grado presentado para optar eltítulo de
INGENIERO ELECTRONICO.

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTA, 20 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN: es una tecnología de redes, que permite crear redes virtuales lógicas independientes dentro de la misma red física. es una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo.

PROTOCOLO DE ENRUTAMIENTO: son un conjunto de pautas y reglas utilizadas por los router con el fin de permitir y mantener la comunicación de la red.

OSPF: es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta. puede recalcular las rutas en muy poco tiempo cuando cambia la topología de la red.

TOPOLOGIA DE RED: es cómo se organizan los elementos de una red de comunicaciones. La estructura topológica se puede representar física o lógicamente.

IP: es el número que identifica de forma individual la conexión de un equipo o dispositivo a una red interna o externa. Sin una dirección de IP es imposible que ningún dispositivo, sea un ordenador, un smartphone o gadget se conecte a Internet.

ROUTER: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función es la de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

RESUMEN

En el presente informe se desarrolla la prueba de habilidades del curso diplomado de profundización CCNP de cisco, para la carrera ingeniería electrónica. En el cual se realiza la configuración de un escenario propuesto, se establece el enrutamiento de ipv4 e ipv6 de las redes y subredes, así como la conmutación y protocolos de comunicación. Se inicia con la construcción de la topología en el simulador packet tracer. Se configura la capa 2 de la red y su correspondiente soporte host, para el enrutamiento se establece el protocolo ospf versión 2 y 3, y bgp. La redundancia se establece por hsrp para proveer una redundancia de primer salto a la red. En la parte cinco de configuración se asigna usuario y contraseña encriptada para ingresar a los dispositivos de la red de una forma segura. Finalmente se asignan las funciones de administración de la red, y así se da solución al escenario propuesto documentando, explicando cada paso con su respectiva línea de comandos o códigos utilizados para la configuración.

ABSTRACT

This report develops the skills test for the Cisco CCNP in-depth diploma course for the electronic engineering career. In which the configuration of a proposed scenario is carried out, the ipv4 and ipv6 routing of the networks and subnets is established, as well as the switching and communication protocols. It starts with building the topology in the packet tracer simulator. Layer 2 of the network is configured and its corresponding host support, for routing the ospf version 2 and 3 protocol, and bgp are established. Redundancy is established by hsrp to provide first-hop redundancy to the network. In part five of the configuration, an encrypted username and password are assigned to enter the network devices in a secure way. Finally, the network administration functions are assigned, and thus the proposed scenario is solved by documenting and explaining each step and command line or codes used for configuration.

INTRODUCCION

Se presenta el desarrollo de la prueba de habilidades del curso CCNP, en el cual se realiza la configuración de una topología propuesta con el fin de poner en práctica y demostrar los conocimientos adquiridos durante el diplomado de profundización CCNP.

Se caracteriza una red y su configuración desde la capa 2, identificando las necesidades de los dispositivos, sus correspondientes requerimientos técnicos. Se establece una topología de red con una complejidad propia de un escenario real, con la intensión de verificar la configuración de los dispositivos y protocolos de comunicación necesarios. Para crear redes avanzadas con direccionamiento múltiple y segmentación de subredes, para la optimización y buen funcionamiento de la red.

Al enfrentarnos al desarrollo y solución de la simulación de lo que puede ser un escenario real, se adquiere la experiencia para configurar un equipo físico y una red empresarial, puesto que el desarrollo de cada una de las fases nos da la habilidad necesaria para enfrentarnos a la implementación del diseño de redes.

DESARROLLO

Escenario propuesto.

Figura 1. Escenario propuesto

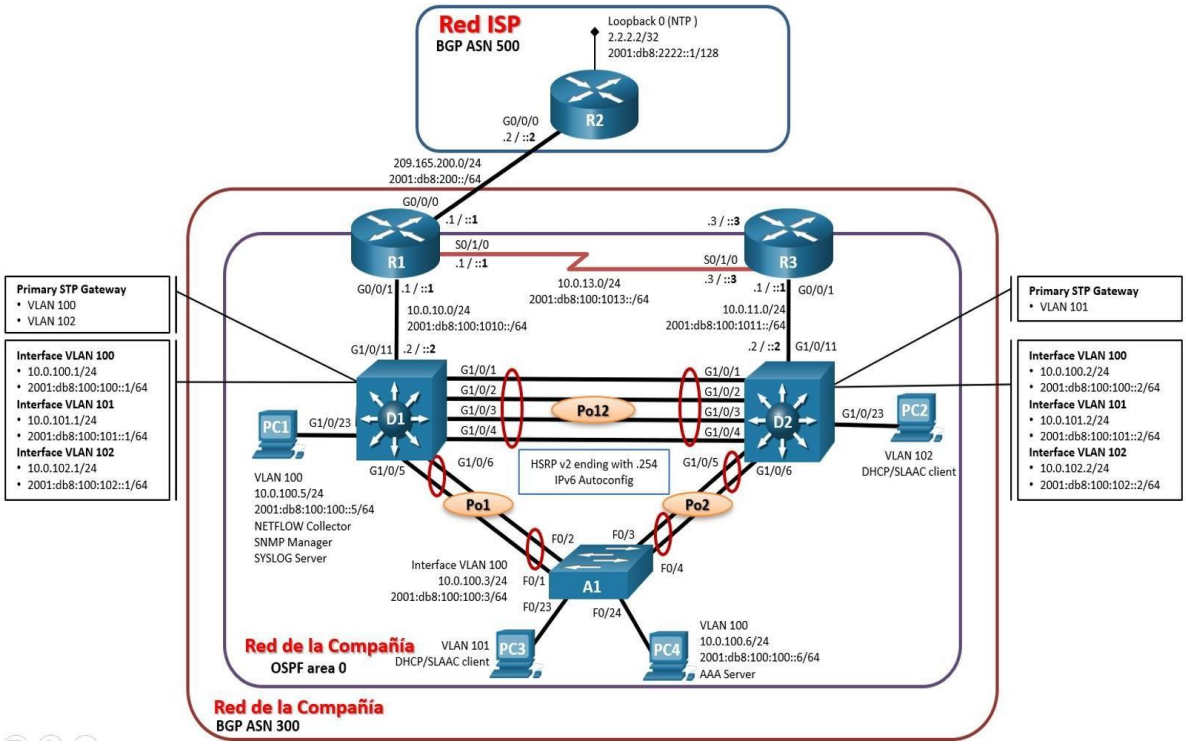


Tabla 1. Enrutamiento escenario propuesto.

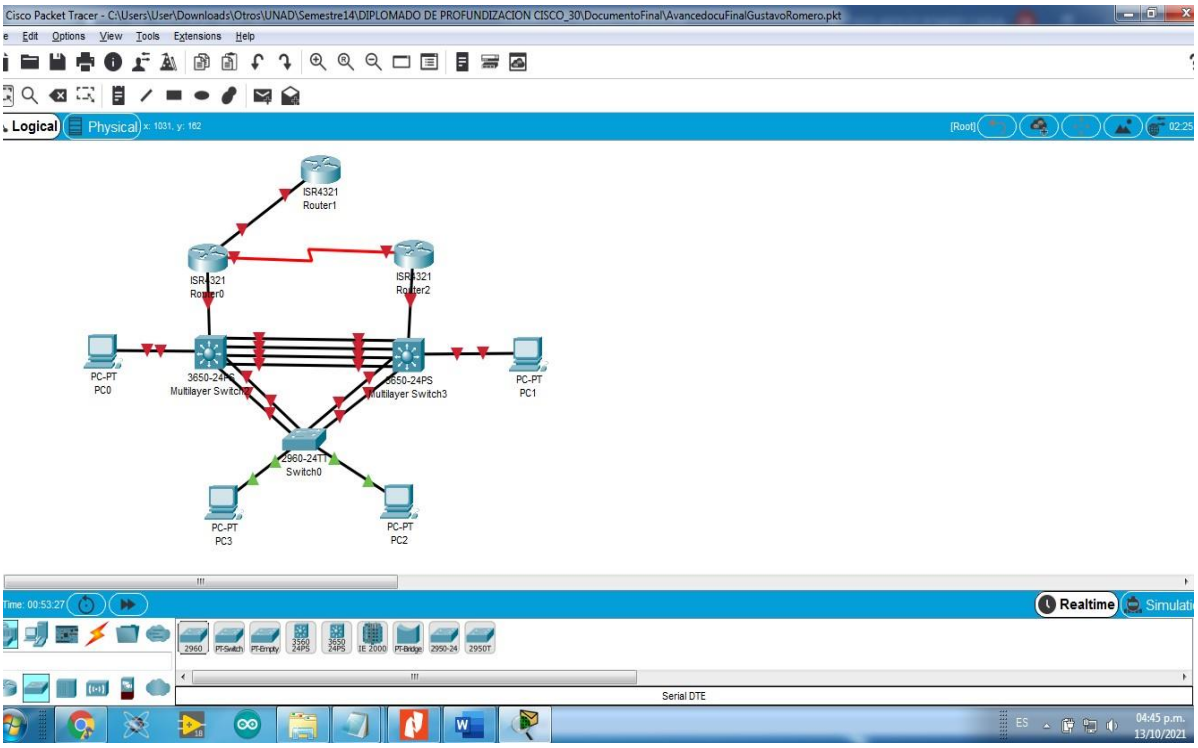
Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	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

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.

Figura 2. Simulación de escenario propuesto.



Paso 2: Configurar los parámetros básicos para cada dispositivo.

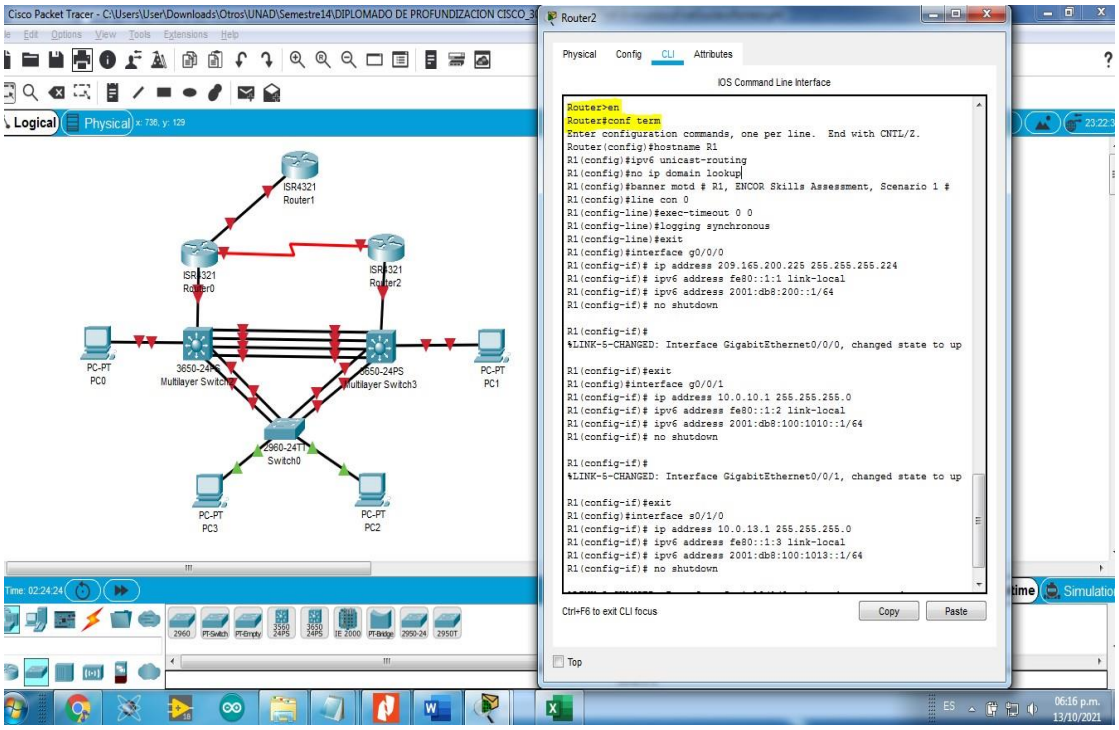
a. Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

Router R1

Router>en /se ingresa a modo privilegiado
Router#conf term /se ingresa a modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostna /se nombra router R1
R1(config)#ipv6 unicast-routing /Tipo de dirección ipv6 unidifusión
R1(config)#no ip domain lookup /evitar retrasos al entrar un comando mal escrito

R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 # /mensaje del día
R1(config)#line con 0 /se ingresa a modo configuración línea
R1(config-line)#exec-timeout 0 0 /se retira el límite de tiempo
R1(config-line)#logging synchronous /depurar mensajes no solicitados consola
R1(config-line)#exit /salir del modo configurar línea
R1(config)#interface g0/0/0 /configurar interfaces
R1(config-if)# ip address 209.165.200.225 255.255.255.224 /asigna ip address
R1(config-if)# ipv6 address fe80::1:1 link-local /asigna ipv6 address
R1(config-if)# ipv6 address 2001:db8:200::1/64
R1(config-if)# no shutdown / Reinicia una interfaz desactivada

Figura 3. configuración básica R1.



De esta forma se replica el código para cada dispositivo según corresponda:

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 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
```

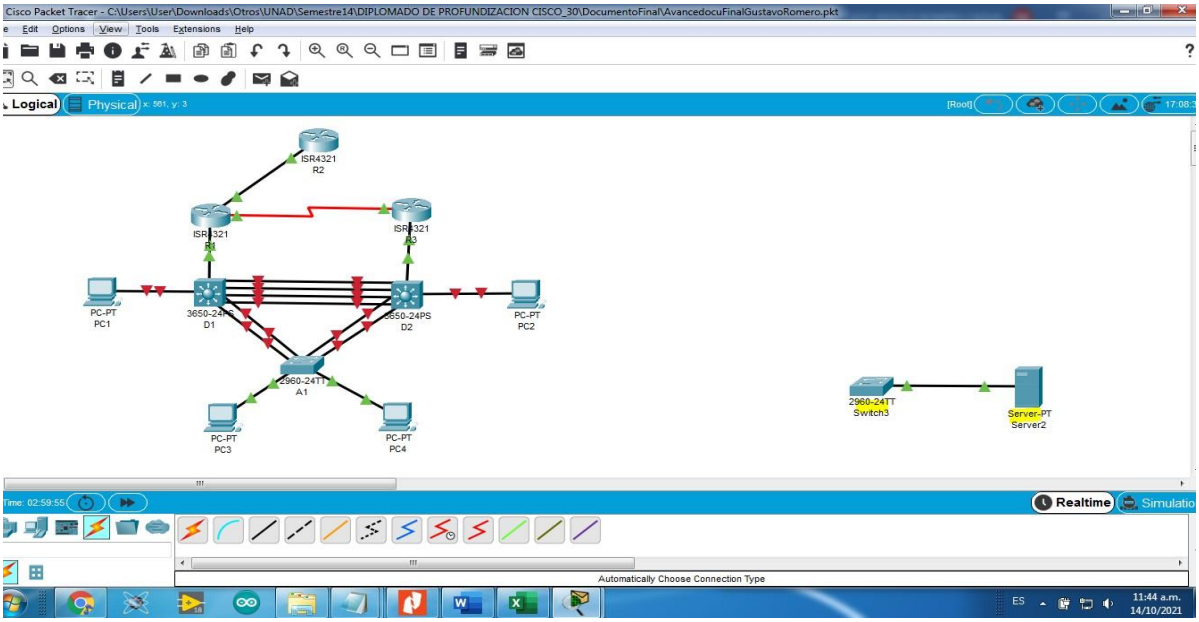
```
vlan 102
 name UserGroupB
 exit
vlan 999
 name NATIVE
 exit
interface g1/0/11
 no switchport
 ip address 10.0.11.2 255.255.255.0
 ipv6 address fe80::d1:1 link-local
 ipv6 address 2001:db8:100:1011::2/64
 no shutdown
 exit
interface vlan 100
 ip address 10.0.100.2 255.255.255.0
 ipv6 address fe80::d2:2 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
```

A1

para configurar el A1 se hizo necesario realizar un procedimiento previo ya que por mi versión el 2960 no reconocía el comando "**sdm prefer dual-ipv4-and-ipv6 default**".

Se conecto con un servidor con el fin de copiar una configuración que aceptara ipv6:

Figura 4. Conexión para configurar A1.



Para realizar este procedimiento se configuro el servidor con una ip 192.168.10.10 Y el switch se asignó vlan e ip con el código:

Switch#en
Switch#conf term
Switch#interface vlan 1
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown

Para verificar la conexión se realizó un ping al servidor:

Switch#ping 192.168.10.10

Como la conexión es correcta se procede con la copia del archivo base del servidor al switch con el código:

Switch#copy tftp: flash

Address or name of remote host []? 192.168.10.10
Source filename []? c2960-lanbasek9-mz.150-2.SE4.bin // este es el archivo que nos permite ipv6

Después de copiado guardamos la configuración con el código y reiniciamos el switch:

Switch(config)#boot system c2960-lanbasek9-mz.150-2.SE4.bin
Switch#reload

Ahora se puede proceder con la configuración de 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
```

b. Copie el archivo running-config al archivo startup-config en todos los dispositivos. Se realiza la copia utilizando el código en cada dispositivo:

R2>en /se ingresa a modo privilegiado
R2#copy running-config startup-config /se realiza la copia de configuración de la ram a Nvram

R1>en
R1#copy running-config startup-config

D1>en
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

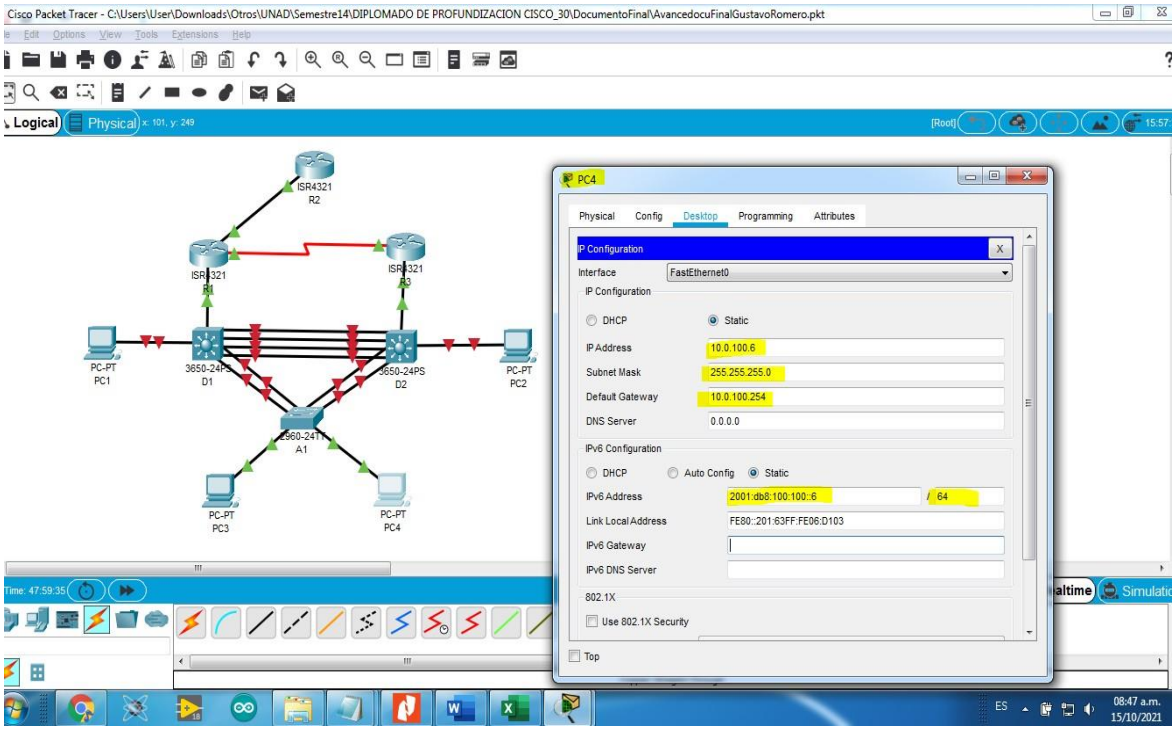
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

R3>en
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

b. 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.

Para este paso se debe ingresar a cada PC, en desktop, ip configuración, se asigna los valores de la tabla de enrutamiento como se muestra en la imagen:

Figura 5. Configuración 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:

Tabla 2. Tareas de configuración parte 2.

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).
Tarea#	**Tarea**	**Especificación**
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 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).
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

Solución
Tarea 2.1 y 2.2

para esta solución se debe configurar la encapsulación que hace referencia a 802.1Q la cual es dot1q se utiliza el siguiente código en cada conexión:

Tarea 2.1:
D1>en /se ingresa al modo privilegiado
D1#conf term /se ingresa a la configuración del terminal
D1(config)#int g1/0/1 /se indica que conexión se va a configurar
D1(config-if)#switchport trunk encapsulation dot1q /se define la encapsulación protocolo 802.1Q
D1(config-if)#switchport mode trunk / se define modo trunk (se establece como troncal)

Tarea 2.2:
D1(config-if)#switchport trunk native vlan 999 /se asigna la vlan nativa 999

Se realiza esta configuración con cada conexión entre D1 y D2.

D1(config)#int g1/0/2
D1(config-if)#switchport trunk encapsulation dot1q

```
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
```

Para g1/0/3 y g1/0/4 se usó la configuración de rango con el código:

```
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 and A1

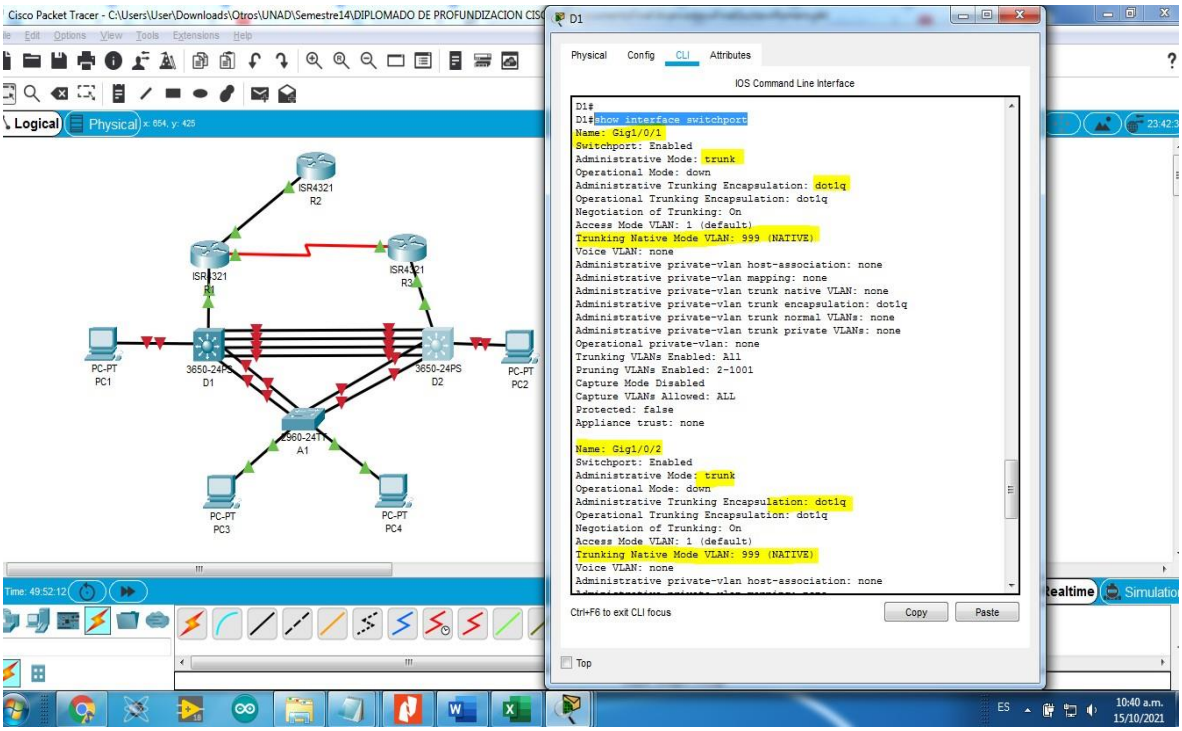
```
D1(config)#int range g1/0/5-6
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
```

D2 and A1

```
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
```

Finalmente, con el código “show interface switchport” podemos ver la configuración:

Figura 6. Resultado Configuración 802.1Q y Vlan nativa.



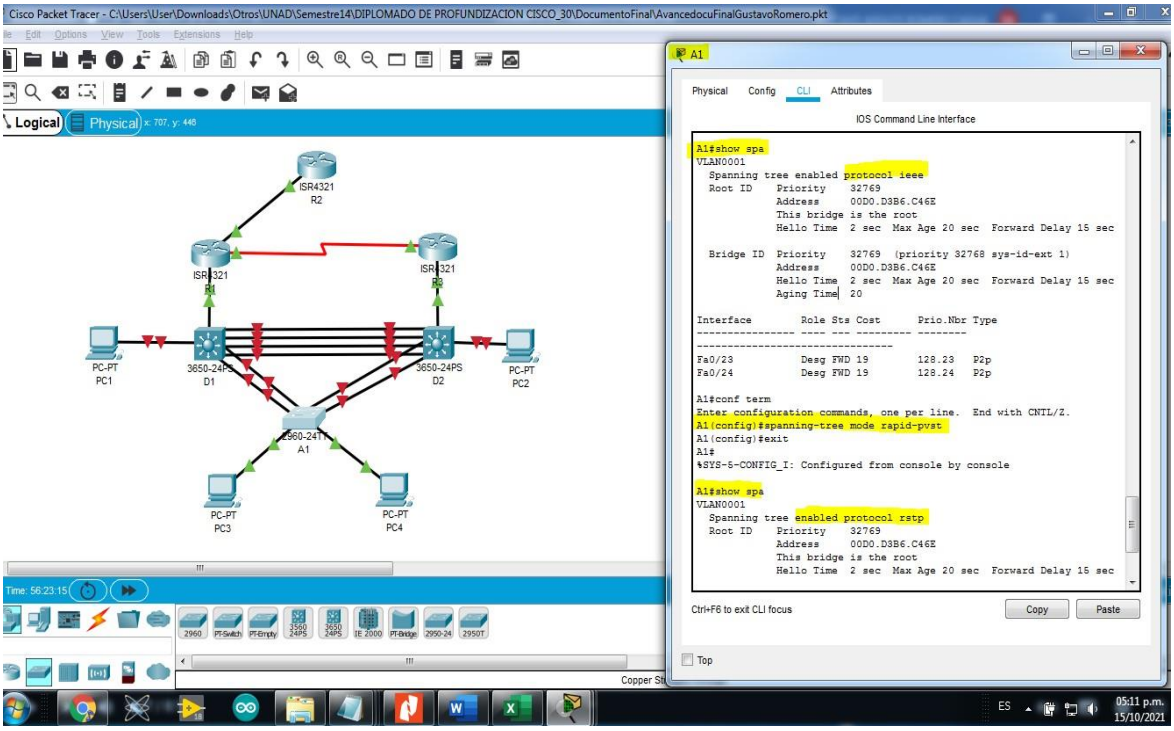
Tarea 2.3

Validar el protocolo actual se realiza con el código: “A1#show spa”

se configura el protocolo Rapid Spanning Tree (RSPT).

A1#conf term /ingreso a modo configuracion
A1(config)#spanning-tree mode rapid-pvst / cambio de protocolo al RSPT
Se realiza lo mismo en todos los dispositivos.

Figura 7. Configuración protocolo RSPT.



Tarea 2.4
Se crea los puentes con propiedades correspondientes con el código:

D1#conf term /se ingresa modo configuración
D1(config)#spanning-tree vlan 100,102 root primary /se coloca prioridad 1 Vlan 100-2
D1(config)#spanning-tree vlan 101 root secondary /se coloca prioridad 2 Vlan 101

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

Tarea 2.5
Se configura los canales según diagrama con el código:

D1 a D2 – Port channel 12

D1#conf term /se ingresa modo configuración

D1(config)#interface range g1/0/1-4 /se ingresa a la configuración de rango
D1(config-if-range)#channel-protocol lacp /se selecciona protocolo lacp
D1(config-if-range)#channel-group 12 mode active / se nombra grupo
D1#(config-if-range)#no shutdown / se cambia de estado el rango de interfaz

Se realiza lo mismo en cada dispositivo según diagrama:

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)#Creating a port-channel interface Port-channel 12
D2(config-if-range)#no shutdown

D1 a A1 – Port channel 1

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

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

D2 a A1 – Port channel 2

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

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

Tarea 2.6

Se configura los puertos según vlan con el código:

D1(config)#int g1/0/23 /selección de puerto a configurar

D1(config-if)#switchport mode Access /se coloca en modo de acceso
D1(config-if)#switchport access vlan 100 /se adigna la vlan 10
D1(config-if)# spanning-tree portfast / se configura protocolo

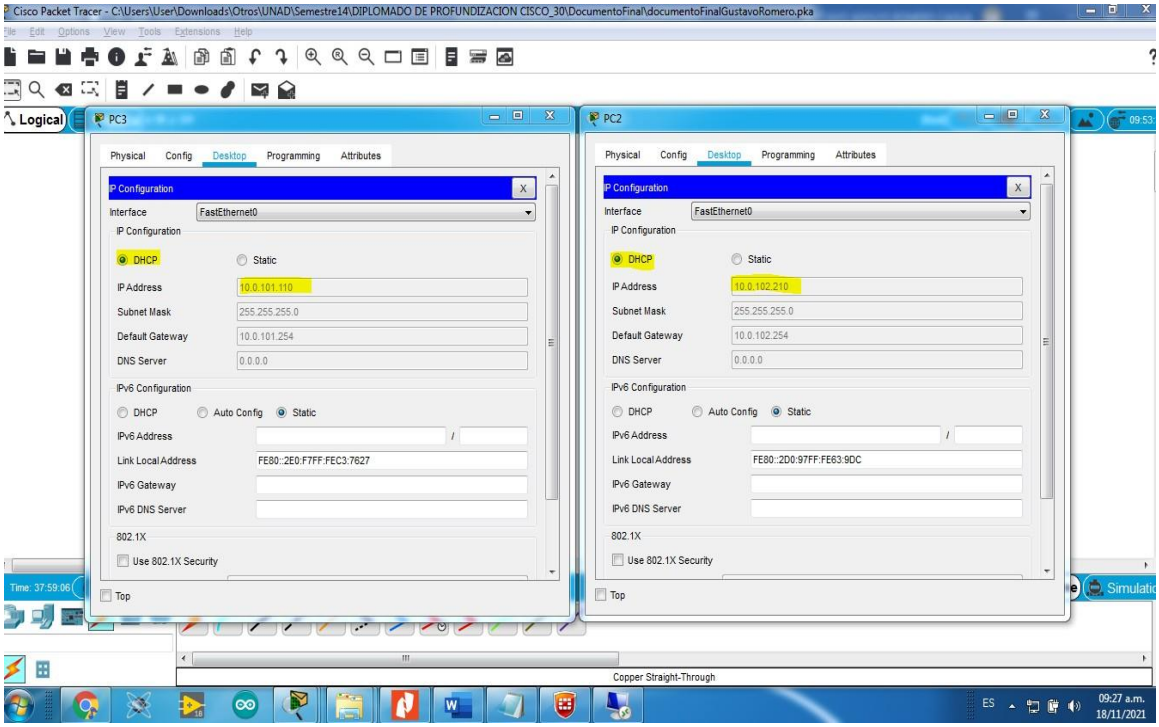
Se configura los demás dispositivos

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

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

Tarea 2.7 Se verifica DHCP

Figura 8. Configuración DHCP PC2 y PC3.



Tarea 2.7

Verifique la conectividad de la LAN local

Nota: La simulación me generaba error y no tomaba unos comandos, así que, para obtener la simulación, tuve que montarla de nuevo y esta vez la hice sobre una actividad ya realizada borre la actividad y la monte sobre ese archivo por este motivo al abrir la simulación se genera la ventana emergente, que corresponde a otra actividad.

Figura 9. Conectividad PC1.

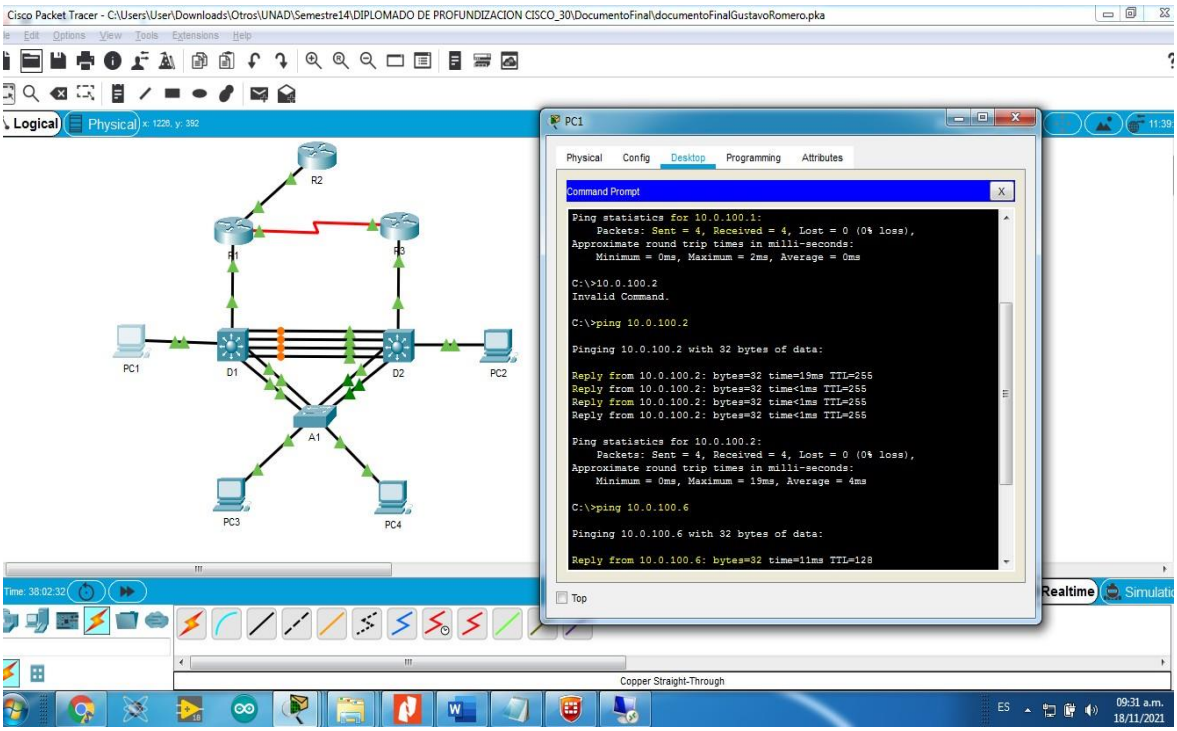


Figura 10. Conectividad PC2.

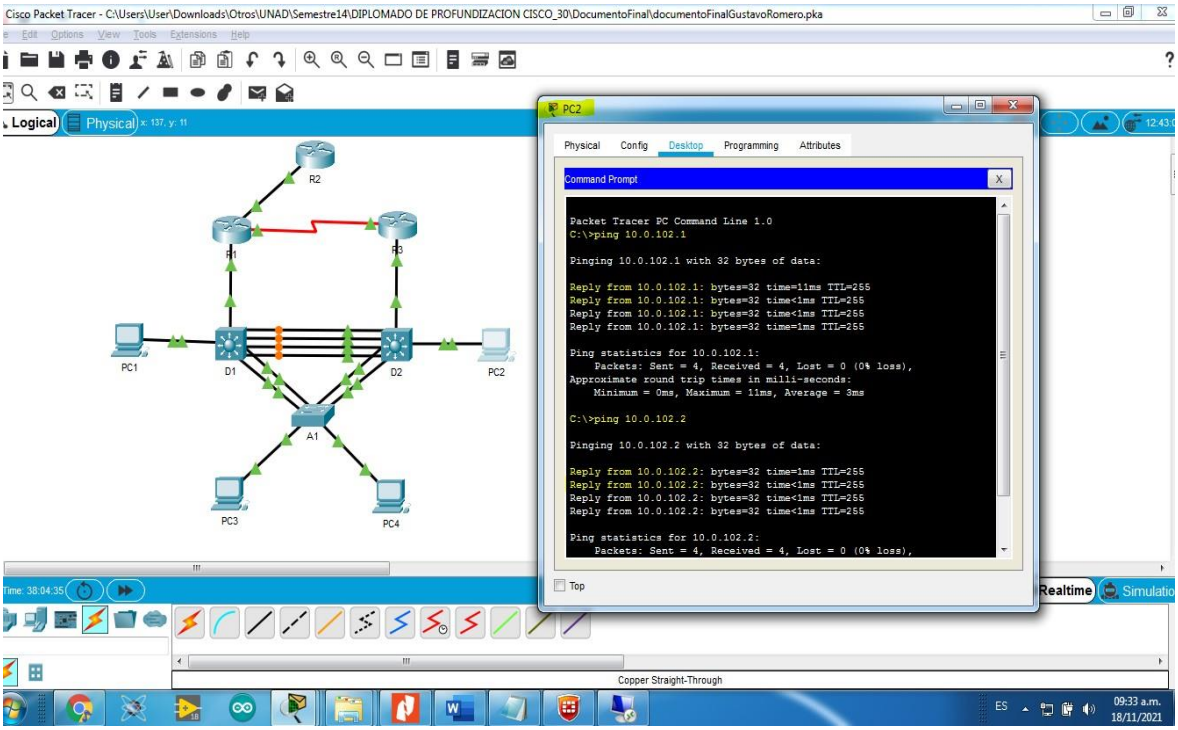


Figura 11. Conectividad PC3.

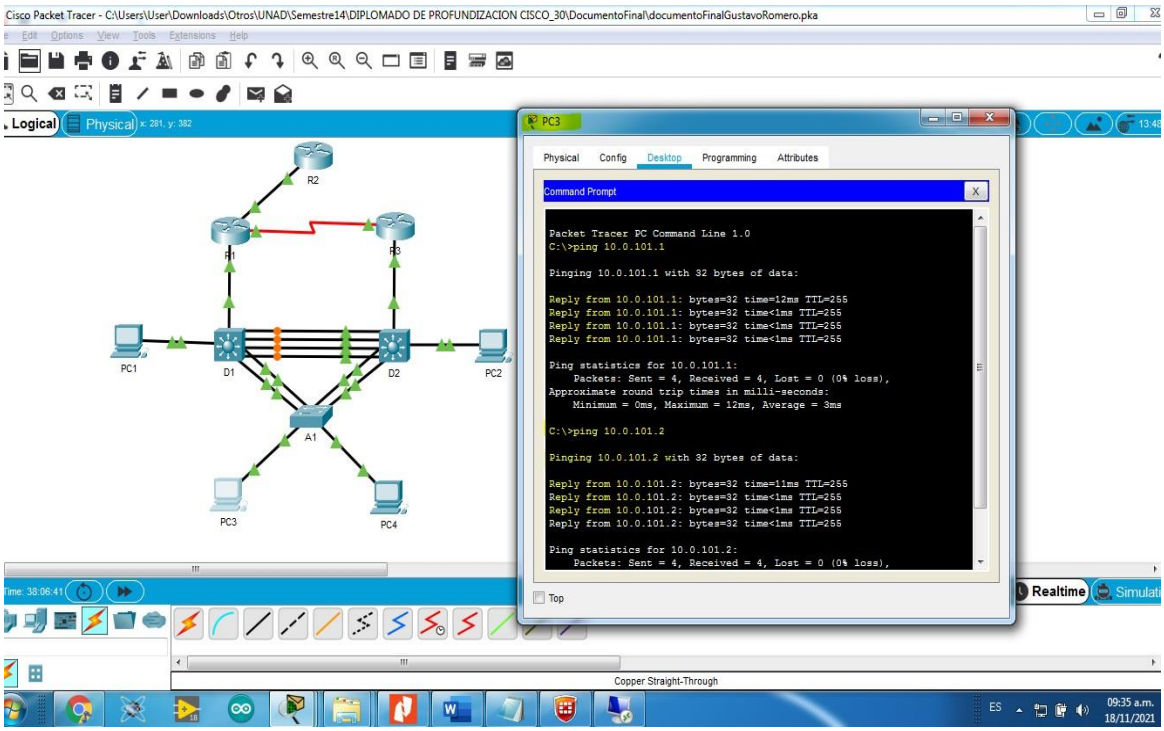
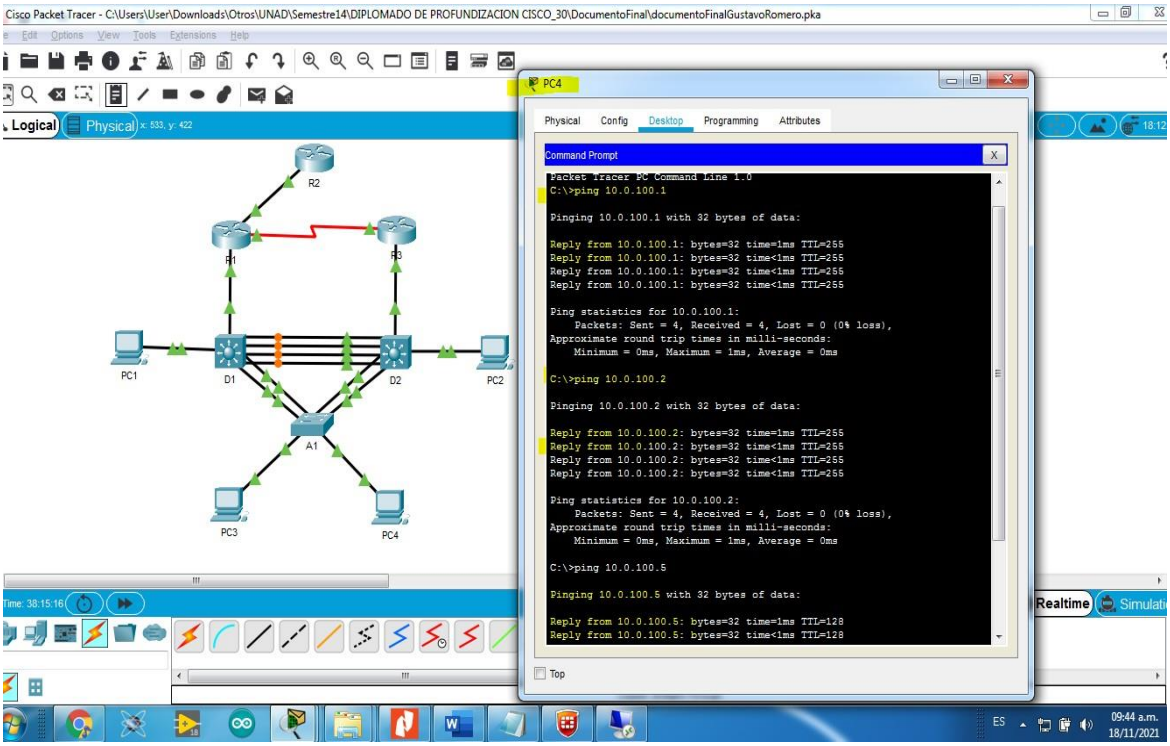


Figura 12. Conectividad PC4.



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:

Tabla 3. Tareas de configuración parte 3.

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 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 Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 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.

Tarea 3.1

R1>en / se ingresa a global
R1#conf term / se ingresa a configuración global
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 4 / se asigna ospf y id 4
R1(config-router)#router-id 0.0.4.1 / se le asigna al router ID
R1(config-router)#do show ip route connected / se listan las interfaces conectadas
C 10.0.10.0/24 is directly connected, GigabitEthernet0/0/1
C 10.0.13.0/24 is directly connected, Serial0/1/0
C 209.165.200.224/27 is directly connected, GigabitEthernet0/0/0

R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 /se asigna área 0 a la interfaz
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0 /se asigna área 0 a la interfaz
R1(config-router)# default-information originate /se declara información predeterminada
R1(config-router)#exit

Se realiza el mismo código en R3, D1, D2:

R3>en
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#do show ip route connected
C 10.0.11.0/24 is directly connected, GigabitEthernet0/0/1
C 10.0.13.0/24 is directly connected, Serial0/1/0
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

D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#do show ip route connected
C 10.0.10.0/24 is directly connected, GigabitEthernet1/0/11
C 10.0.100.0/24 is directly connected, Vlan100

C 10.0.102.0/24 is directly connected, Vlan102
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 / se deshabilita las publicaciones OSPFv2
D1(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
C 10.0.102.0/24 is directly connected, Vlan102
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 / se deshabilita las publicaciones OSPFv2
D2(config-router)#no passive-interface g1/0/11

Tarea 3.2

Se utiliza ahora la configuración para Ipv6:

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 / se declara información predeterminada
R1(config-rtr)#exit / se sale del modo configuracion
R1(config)#int g0/0/1 / se declara la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0 / se asigna área 0 en ipv6
R1(config-if)#exit / se sale del modo configuracion
R1(config)#int s0/1/0 / se declara la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0 / se asigna área 0 en ipv6

Se realiza la configuración para R3, D1 y D2 replicando el código anterior en cada dispositivo.

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


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
D1(config-if)#exit
D1(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 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

Tarea 3.3

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:
• Una ruta estática predeterminada IPv4.
• Una ruta estática predeterminada IPv6.

Para esto utilizamos el siguiente código

R2>en /Se ingresa al modo privilegiado
R2#conf term /Se ingresa a configurar el terminal
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 0 /Se llama la interfaz a conf. Loopback 0
R2(config-if)# ipv6 route ::/0 loopback 0/ se establece los parámetros a configurar con ip y mascara de red, como indica el diagrama del escenario.

Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.

Para esto se configura las redes directamente conectadas en el R2 usando el siguiente código:

R2#en / Se ingresa al modo privilegiado
R2#conf term / Se ingresa a configurar el terminal
R2(config-router)#router bgp 500 / se establece el router con bgp 500
R2(config-router)#bgp router-id 2.2.2.2 /se asigna el id 2.2.2.2

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

R2(config-router)#neighbor 209.165.200.225 remote-as 300 /se define la relación vecino ipv4
R2(config-router)#neighbor 2001:db8:200::1/64 remote-as 300/se define la relación vecino ipv6

En IPv4 address family, anuncie:
• La red Loopback 0 IPv4 (/32).
• La ruta por defecto (0.0.0.0/0).

R2(config-router)#address-family ipv4 / se llama a configurar la familia ipv4
R2(config-router)# neighbor 209.165.200.225 activate /red loopback
R2(config-router)# no neighbor 2001:db8:200::1 activate /red loopback
R2(config-router)# network 2.2.2.2 mask 255.255.255.255 /red y mascara
R2(config-router)#neighbor 0.0.0.0/0 / ruta por defecto
R2(config-router)# exit-address-family / salir de la configuración de familia

En IPv6 address family, anuncie:
• La red Loopback 0 IPv4 (/128).
• La ruta por defecto (::/0).

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

Tarea 3.4

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.
R1#conf term / se ingresa a configuración de terminal
R1(config)#ip route 10.0.0.0 255.255.255.255 null0 / se configura interfaz null ipv4
R1(config)#ip route 2001:db8:100::/48 null0 / interfaz null opv6

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

R1#conf term / se ingresa a la configuración de terminal
R1(config)#router bgp 300 / se asigna bgp y ns 300
R1(config-router)#bgp router-id 1.1.1.1 / se asigan id del router

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

R1(config-router)#neighbor 209.165.200.226 remote-as 500 /se define la relación vecino ipv4

R1(config-router)#neighbor 2001:db8:200::2 remote-as 500 /se define la relación vecino ipv6

En IPv4 address family:
• Deshabilite la relación de vecino IPv6.
• Habilite la relación de vecino IPv4.
• Anuncie la red 10.0.0.0/8.

```
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
```

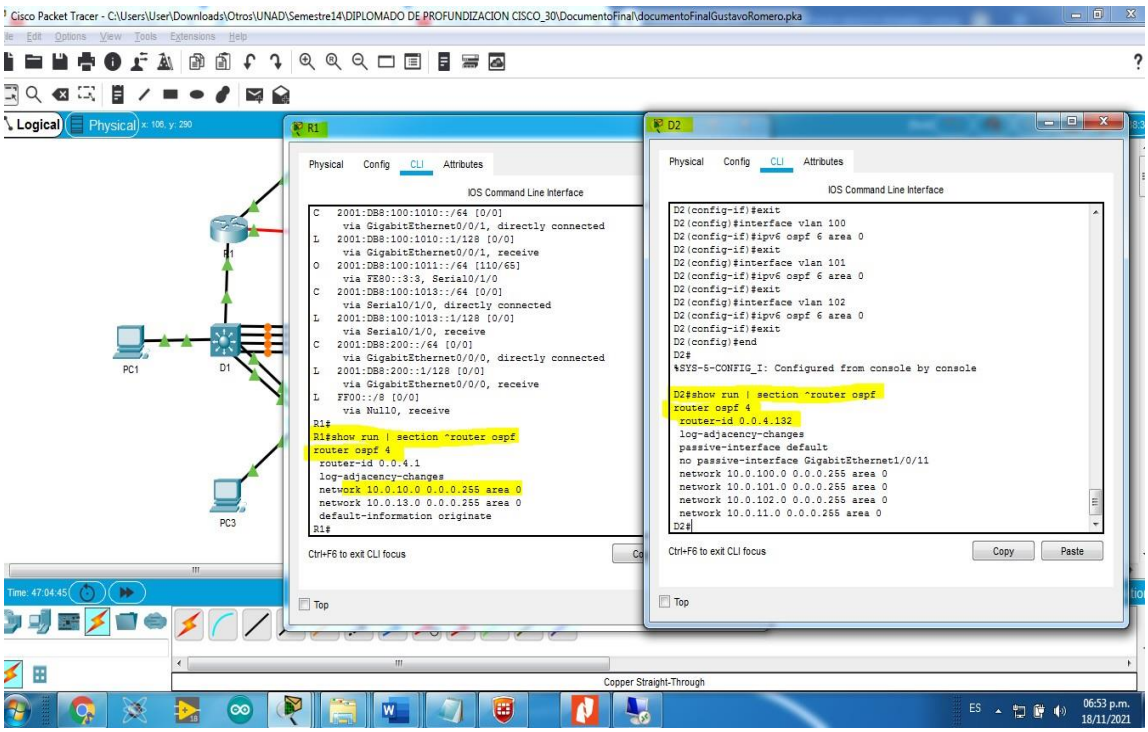
En IPv6 address family:
• Deshabilite la relación de vecino IPv4.
• Habilite la relación de vecino IPv6.
• Anuncie la red 2001:db8:100::/48.

```
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
```

Validación tarea 3

Se valida con el comando “Show run”

Figura 13. configuración parte 3.



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 hosts en la “Red de la Compañia”. Las tareas de configuración son las siguientes:

Tabla 4. Tareas de configuración parte 4.

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.
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.

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 version 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.

4.4	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 version 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.

Tarea 4.1:

Para la solución de esta se implementa el código:

Cree dos IP SLAs.
• Use la SLA número 4 para IPv4.
• Use la SLA número 6 para IPv6.

```
D1>en                    /se ingresa al modo global
D1#conf term             /se ingresa a la configuración del dispositivo
D1(config)# ip sla 4     / se nombra el seguidor del servidor a configurar
D1(config-ip-sla)# icmp-echo 10.0.10.1 / se indica la ip a configurar
```

Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

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

Se realiza el mismo código 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
```

Programe la SLA para una implementación inmediata sin tiempo de finalización.

D1(config-ip-sla)# ip sla schedule 4 life forever start-time now /se define el inicio y que se mantenga implementada.
D1(config-ip-sla)# 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.

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.

D1(config-ip-sla)# track 4 ip sla 4 / es el que permite actualizar el estatus de los cambios en la conexión o configuracion.
D1(config-ip-sla-track)# delay down 10 up 15 / se declara el tiempo en el que actualiza los cambios o notifica.

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

Tarea 4.2

Para la solución de esta se implementa el código de 4.1 pero en el terminal D2:

Cree dos IP SLAs.
• Use la SLA número 4 para IPv4.
• Use la SLA número 6 para IPv6.

D2>en /se ingresa al modo global
D2#conf term /se ingresa a la configuración del dispositivo
D2(config)# ip sla 4 / se nombra el seguidor del servidor a configurar
D2(config-ip-sla)# icmp-echo 10.0.11.1 / se indica la ip a configurar

Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

D2(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit

Se realiza el mismo código 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

Programe la SLA para una implementación inmediata sin tiempo de finalización.

D2(config-ip-sla)# ip sla schedule 4 life forever start-time now /se define el inicio y que se mantenga implementada.
D2(config-ip-sla)# 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.

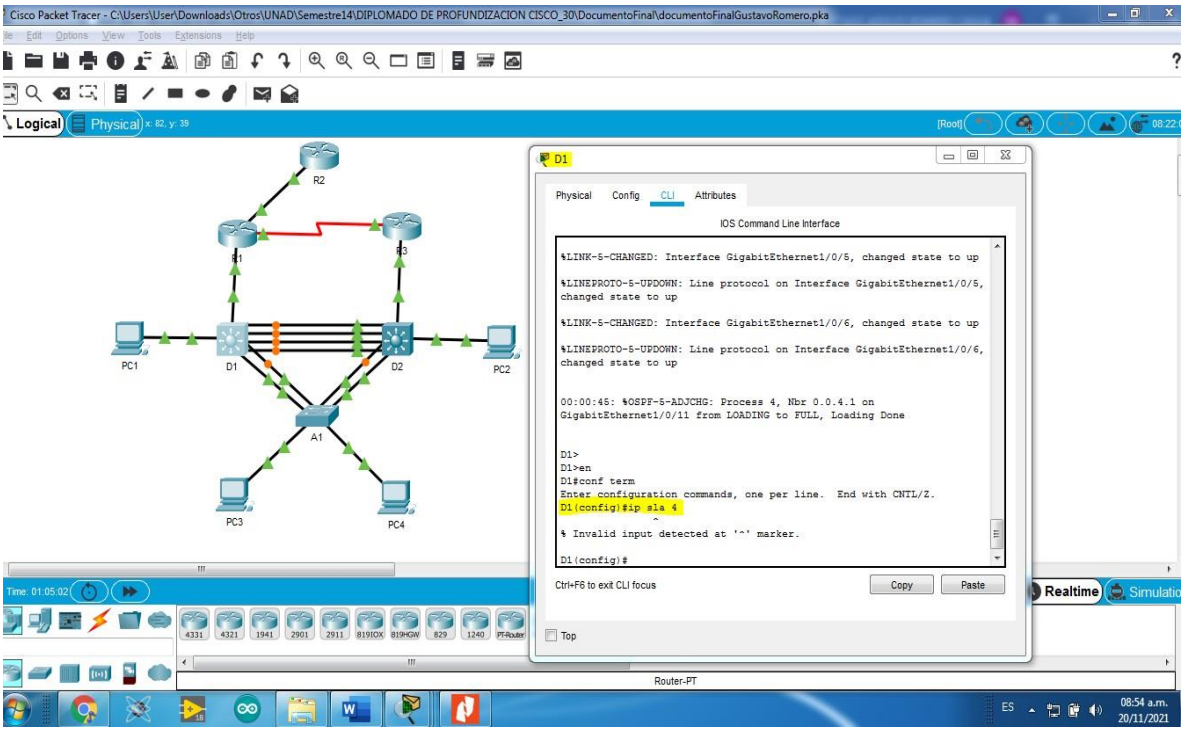
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

D2(config-ip-sla)# track 4 ip sla 4 / es el que permite actualizar el estatus de los cambios en la conexión o configuracion.
D2(config-ip-sla-track)# delay down 10 up 15 / se declara el tiempo en el que actualiza los cambios o notifica.
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

Nota: para la tarea 4.1 y 4.2 a pesar de haber cambiado la simulación y migrarla a una actividad previa, el packet tracer no reconoce los comandos para realizar esta configuración debería implementarse en un ambiente real con los servidores físicos.

Figura 14. Configuración IP SLAS.



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

Para esto se utiliza el código:

D1(config)#interface vlan 100 / se ingresa a la vlan a configurar
D1(config-if)#standby version 2 /se configura HSRP en la vlan
D1(config-if)#standby 104 ip 10.0.100.254 /se asigna la ip virtual
D1(config-if)#standby 104 priority 150 /se establece prioridad en 150
D1(config-if)#standby 104 preempt /se configura como preferencia
D1(config-if)#standby 104 track 4 decrement 60 /se configura el rastreo del objeto y decremento 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.

Se utiliza el código del paso anterior, y se configura la vlan 101, se cambia la ip virtual:

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

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.

Se utiliza el código del paso 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
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.

Para este paso continuamos utilizando el código de configuración anterior y se cambia a ipv6, se cambia la vlan y la ip virtual:

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

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.

Continuamos con los mismos pasos de configuración cambiando el grupo y la vlan y no se establece prioridad:

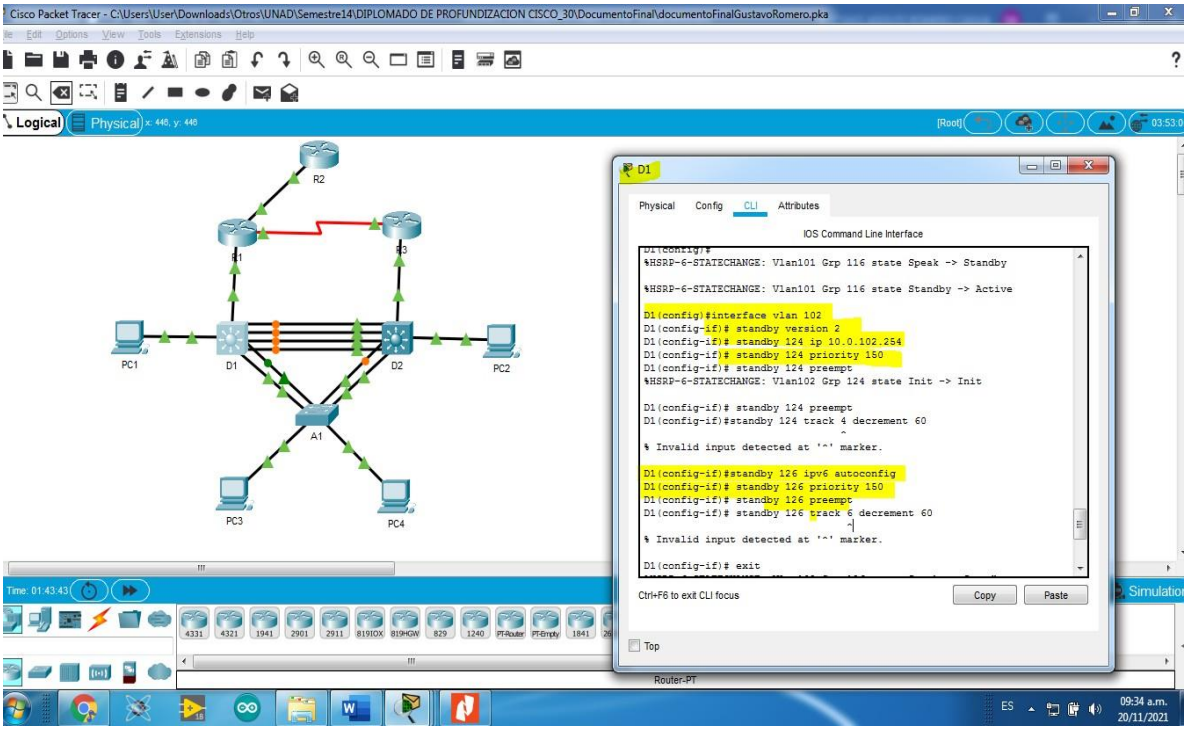
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track 6 decrement 60

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.

Continuamos con los mismos pasos de configuración cambiando el grupo y la vlan y se establece prioridad:

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

Figura 15. Configuración HSRPv2 en D1.



Tarea 4.4
En D2, configure HSRPv2.

Para esta tarea utilizamos el mismo código de configuración de la tarea 4.3 y cambiamos las vlan e ip según corresponda:

D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP versión 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.

D2(config)#interface vlan 100 / se ingresa a la vlan a configurar
D2(config-if)# standby version 2 /se configura HSRP en la vlan
D2(config-if)# standby 104 ip 10.0.100.254 /se asigna la ip virtual
D2(config-if)# standby 104 track 4 decrement 60 /se configura el rastreo del objeto y decremento 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.

Utilizamos los códigos del paso inmediatamente anterior cambiando la vlan, la ip virtual y el grupo. Se establece la prioridad 150:

```
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
```

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.

Continuamos con la serie de codigos utilizados en el paso anterior cambiando la vlan y la ip virtual en este paso no se establece prioridad:

```
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
```

De acá en adelante se replica el código, pero ahora se configura la ipv6:

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.

```
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# 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.

Utilizamos los comandos anteriores se cambia a ipv6 se determina prioridad a la vlan correspondiente:

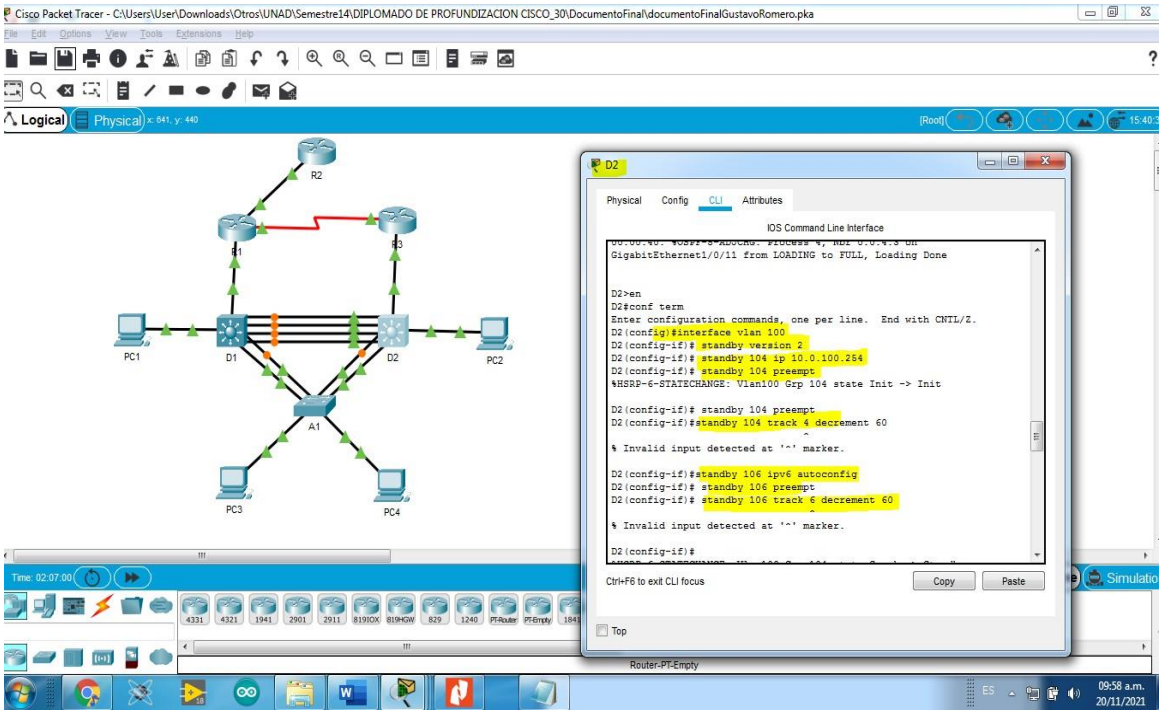
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)# standby 116 priority 150
D2(config-if)# standby 116 preempt
D2(config-if)# standby 116 track 6 decrement 60

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.

Continuamos con la serie de códigos de configuración cambiando la vlan y grupo:

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

Figura 16. Configuración HSRPv2 en D2.



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:

Tabla 5. Tareas de configuración parte 5.

Tarea	Tare	Es
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**
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
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
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**.

Tarea 5.1, 5.2 y 5.3

En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT. Contraseña: cisco12345cisco

Detalles de la cuenta encriptada SCRYPT:
• Nombre de usuario Local: sadmin
• Nivel de privilegio 15
• Contraseña: cisco12345cisco
-Habilite AAA (no en R2).

Para esta configuración de seguridad se debe ingresar a cada dispositivo y utilizar el siguiente código:

R2>en / se ingresa a modo privilegiado
R2#conf term / se ingresa a configurar terminal
R2(config)#enable password cisco12345cisco /se asigna contraseña a modo privilegiado
R2(config)#service password-encryption / se encripta la contraseña
R2(config)#exit / se sale del modo configuracion
R2(config)#enable secret level 15 cisco12345cisco / se crea sesión privilegio 15
R2(config)#username sadmin privilege 15 secret cisco12345cisco / se crea usuario y contraseña encriptada para el usuario.

R1>en
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
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

Tarea 5.4, 5.5 y 5.6

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

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.

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

Para estos pasos utilizamos los códigos:

R1(config)#aaa new-model / llamamos el modelo a configurar
R1(config)#radius server RADIUS /se indica el servidor a configurar Radius
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813 /se asigna la dirección ip y puertos del servidor Radius
R1(config-radius-server)#key $trongPass / se asigna la contraseña $trongPass

Se replica los códigos de configuración para los demás dispositivos exepto R2:

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

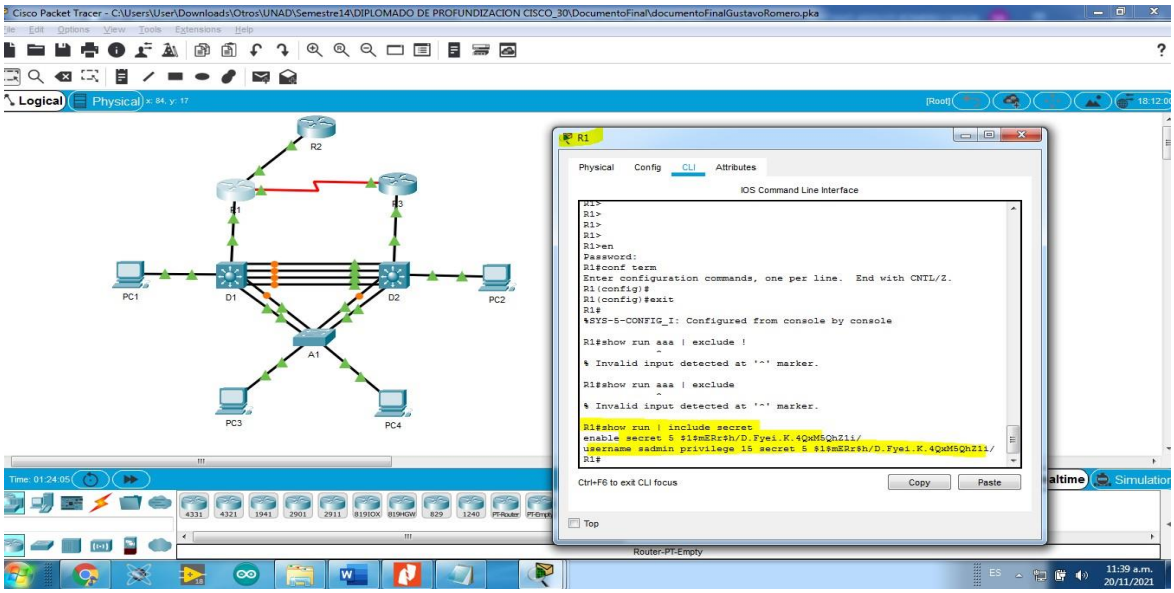
```
D2(config-radius-server)#exit
D2(config)#aaa authentication login default group radius local
D2(config)#end

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
```

En algunos dispositivos A1 y D1 no fue posible realizar la configuración ya que arroja error la configuración de packet tracer, pero son los códigos para utilizar en un escenario real no simulado.

Figura 17. Configuración seguridad.



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:

Tabla 6. Tareas de configuración parte 6.

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*.

Tarea 6.1

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

Para esto validamos en los dispositivos la hora configurada con el código:

R1#show clock / verificar la hora configurada
*2:9:46.478 UTC Mon Mar 1 1993

Como se evidencia que la hora no corresponde a la actual se configura con el código:

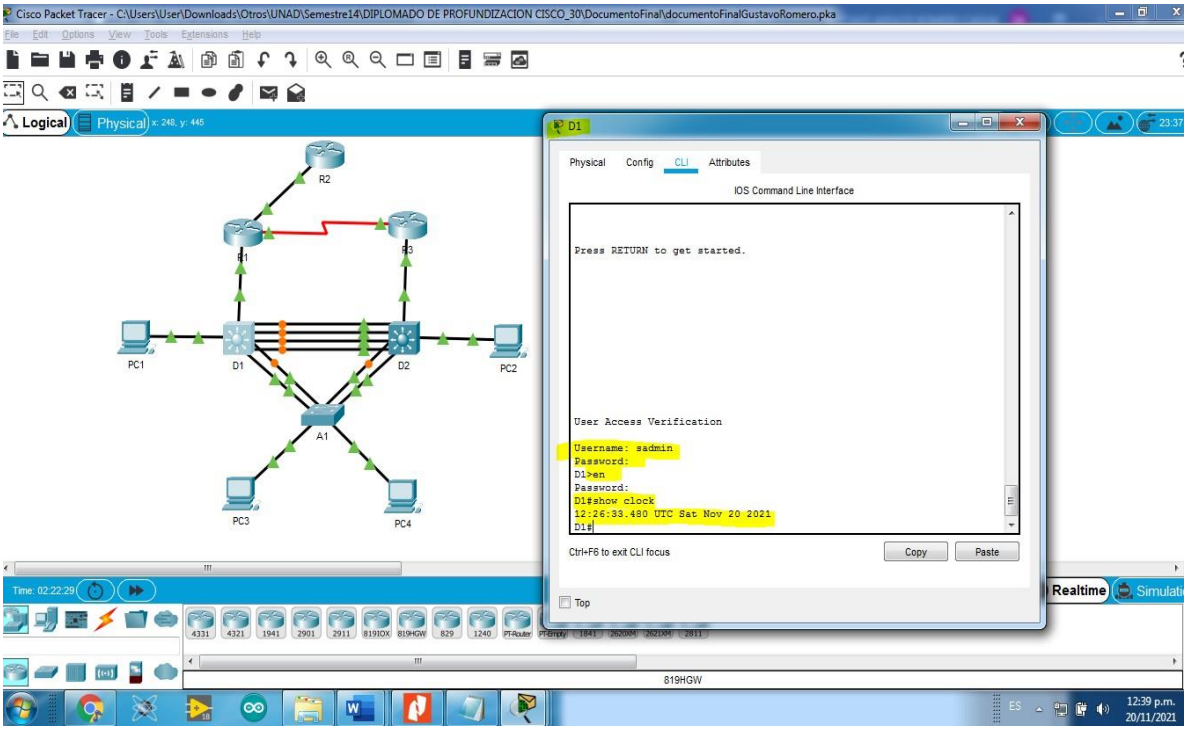
R1# clock set 12:24:00 20 Nov 2021/ se configura fecha y hora actual

Se repite el proceso en todos los dispositivos:

R2#clock set 12:24:00 20 Nov 2021

R3#clock set 12:24:00 20 Nov 2021
D2#clock set 12:24:00 20 Nov 2021
D1#clock set 12:24:00 20 Nov 2021
A1#clock set 12:24:00 20 Nov 2021

Figura 18. Verificación configuración hora UTC actual.



Tarea 6.2

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

Para esto utilizamos el código:
R2(config)#ntp master 3 / se configura NTP maestro en el nivel de estrato 3

Tarea 6.3, 6.4 y 6.5

Para esta parte utilizamos el código:

R1(config)#ntp server 2.2.2.2 / se configura NTP
R1(config)#logging trap warning / Syslogs en nivel warning
R1(config)#logging host 10.0.100.5 / enviarse a la PC1 en 10.0.100.5
R1(config)#logging on / se cambia a estado encendido

R1(config)#ip access-list standard SNMP-NMS / se cinfigura SNMP lectura
R1(config-std-nacl)#permit host 10.0.100.5 / se declara límite de acceso
R1(config-std-nacl)#exit

R1(config- snmp)#snmp-server contact Cisco gustavoR / valor de contacto SNP
R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS /se establece
R1(config- snmp)#snmp-server host 10.0.100.5 versión 2c ENCORSA /se declara el host
R1(config- snmp)#snmp-server ifindex persist /se habilita el envío de traps
R1(config- snmp)#snmp-server enable traps bgp /se habilita el envío de traps bgp
R1(config- snmp)#snmp-server enable traps config /se habilita traps
R1(config- snmp)# snmp-server enable traps ospf /se habilita el envió de traps osfp
R1(config- snmp)#end /se finaliza la configuración

Se replica en los demás dispositivos:

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

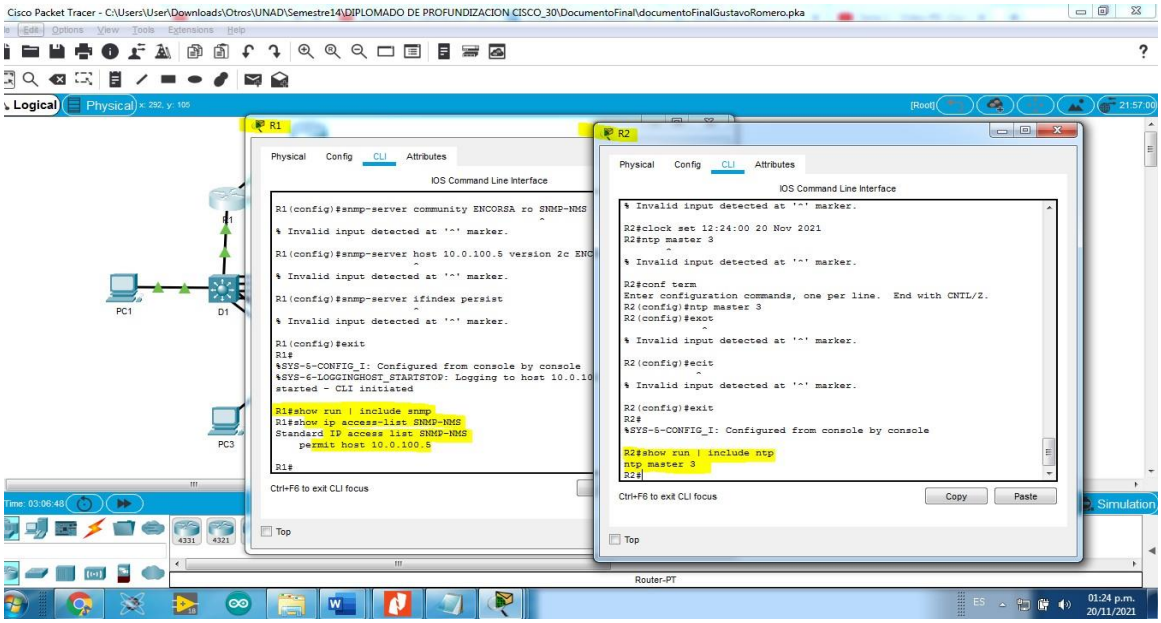
D2(config)#ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS

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

Nota: en los dispositivos configurados se relaciona la configuracion pero packet tracer no funciona la simulación de snmp-server.

Figura 19. Verificación configuración 6.3 a 6.5.



CONCLUSIONES

Se construye la topología y se configura los dispositivos necesarios, para el desarrollo de la actividad en el simulador packet tracer.

Se realiza la configuración de capa de 2 de red, con la implementación de enlaces troncales, se habilita el protocolo RSTP y se configura puentes raíz. Lo cual permite el direccionamiento DHCP y SLAAC en la red, dando conexión a todos los switches.

Se implementa los protocolos de enrutamiento de la red, configurando OSPF tanto para ipv4 como ipv6, enrutando por familias y áreas de red.

Se establece la comunicación de la red y subredes del escenario planteado, en una simulación de packet tracer dando solución a una situación de diseño e implementación de redes actual y real en la industria.

BIBLIOGRÁFIA

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

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

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei- NT1IlnMfy2rhPZHwEoWx