DIPLOMADO DE PROFUNDIZACIÒN CISCO
PRUEBA DE HABILIDADES PRÀCTICAS CCNP

ALBEIRO PEDROZO VILLARRUEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA – UNAD
ESCUELA DE CIENCIAS BÀSICAS, TECNOLOGÌA E INGENIERÌA - ECBTI
INGENIERÌA DE TELECOMUNICACIONES
YOPAL, CASANARE
2021

DIPLOMADO DE PROFUNDIZACIÒN CISCO
PRUEBA DE HABILIDADES PRÀCTICAS CCNP

ALBEIRO PEDROZO VILLARRUEL

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA – UNAD
ESCUELA DE CIENCIAS BÀSICAS, TECNOLOGÌA E INGENIERÌA - ECBTI
INGENIERÌA DE TELECOMUNICACIONES
YOPAL, CASANARE
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Yopal, 28 de noviembre de 2021

AGRADECIMIENTOS

Este trabajo lo dedico a mi señora esposa y a mis hijos; lo dedico a mi esposa porque siempre ha estados en todos los momentos como un gran soporte para alcanzar mis metas y lo dedico a mis hijos porque ha sido mi inspiración para superarme, demostrarle que con constancia y tenacidad se pueden lograr los sueños.

También quiero agradecer a mi hermana que siempre ha estado en los momentos difíciles, los cuales siempre me alentado para continuar cuando sentía que ya no era capaz de continuar.

También agradezco a mis tutores, a todos los que he tenido durante este ciclo de formación; especialmente a aquellos que dedicaron su tiempo, cuando le pedí alguna asesoría, aquellos que lo hicieron de forma positiva y tuvieron paciencia para hacerlo, aquellos que compartieron su tiempo asesorándome cuando podían compartir ese tiempo con su familias.

Finalmente quiero agradecer a mi Dios, ya que me ha dado la fuerza, la tenacidad y constancia, para continuar en el camino de la victoria y así lograr las metas propuesta y mi gran sueño.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

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.

SYSLOG: Se trata de un protocolo estándar utilizado para enviar mensajes de registro o eventos del sistema a un servidor específico, llamado servidor de syslog. El syslog se utiliza principalmente para recopilar varios registros de dispositivos de diversas máquinas diferentes en una ubicación central para la supervisión y su análisis.

SWITCH: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

VLAN: Es una red LAN independiente, Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada.

INTERFACE: Es el medio que permite a una persona comunicarse con una máquina. La interfaz, está compuesta por los puntos de contacto entre un usuario y el ordenador.

SLAAC: es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e información de la dirección de gateway predeterminado de un router IPv6 sin utilizar un servidor de DHCPv6.

RESUMEN

El presente trabajo es de gran importancia, debido a que se desarrolla las habilidades y conocimientos obtenidos durante el desarrollo del curso de diplomado de profundización CCNP de cisco.

Para el desarrollo de este informe se requirió una gran compresión de la topología impuesta y sus protocolos, para darle una solución adecuada a todos sus requerimientos y configuraciones. Se necesitó hacer investigaciones de forma individual, comprender las configuraciones que requería la red; la configuración de esta red es de gran importancia para el futuro ingeniero, debido a que se obtuvo un gran conocimiento para el desarrollo profesional e individual.

En el presente trabajo se realizó el enrutamiento de ipv4 e ipv6 de las redes y subredes, así como la conmutación y protocolos de comunicación, se configuro la capa 2 de la red y el soporte de host, los protocolos de enrutamiento, la redundancia del primer salto , la seguridad y finalmente se configuro las funciones de administración de la red.

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

ABSTRACT

This work is of great importance, because it develops the skills and knowledge obtained during the development of the cisco CCNP in-depth diploma course.

For the development of this report, a great understanding of the imposed topology and its protocols was required, to provide an adequate solution to all its requirements and configurations. It was necessary to do research individually, to understand the configurations that the network required; The configuration of this network is of great importance for the future engineer, because a great deal of knowledge was obtained for professional and individual development.

In the present work, the IPv4 and IPv6 routing of the networks and subnets was carried out, as well as the switching and communication protocols, layer 2 of the network was configured and the host support, the routing protocols, the redundancy of the first jump, security and finally configured the network administration functions.

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

INTRODUCCIÒN

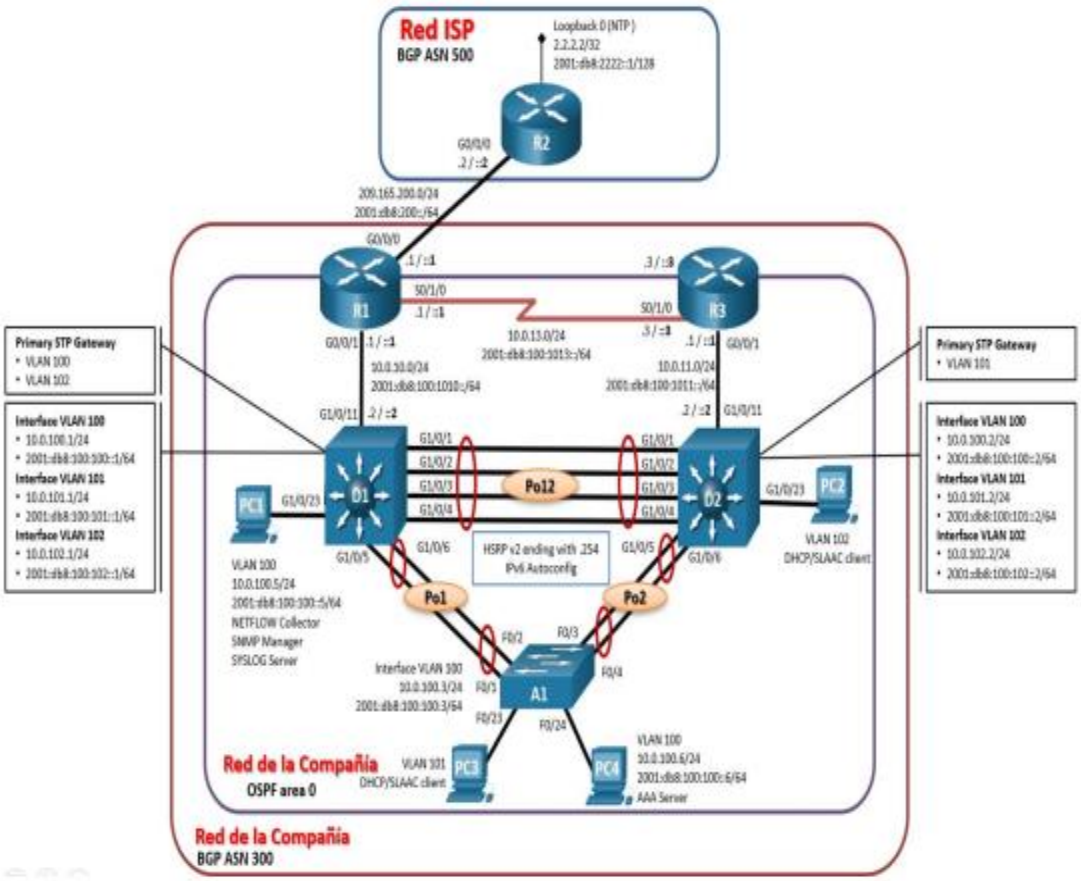
Con la realización del siguiente trabajo nos permite conocer un poco más a fondo sobre las la configuración de redes, sus parámetros básicos de los dispositivos y el direccionamiento de las interfaces, además pudimos averiguar y comprender el funcionamiento y características de los dispositivos que la comprende.

En la primera parte construimos la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces, en la segunda parte se configura la capa 2 de la red y el soporte de host, en la tercera parte se configuran los protocolos de enrutamiento para IPv4 e IPv6 como son OSPFv2 y OSPFv3 y se configura MP – BGP; en la cuarta parte se configura la redundancia del primer salto HSRP versión; en quinta parte consiste en configurar los mecanismos de seguridad en los dispositivos, tales como la protección del EXEC privilegiado usando el algoritmo de encriptación SCRIPT, la habilitación de AAA, la configuración de las especificaciones del servidor RADIUS; finalmente en la sexta parte cofiguramos las funciones de administración de la red.

Además al desarrollar y dar solución a este requerimiento mediante la herramienta de simulación GNS3, se pudo obtener un escenario real y por esta razón es de gran importancia debido a que se adquirió experiencia para configurar un equipo físico y una red real.

ESCENARIO PROPUESTO

Figura 1. Escenario propuesto (Topología de red)



DESARROLLO

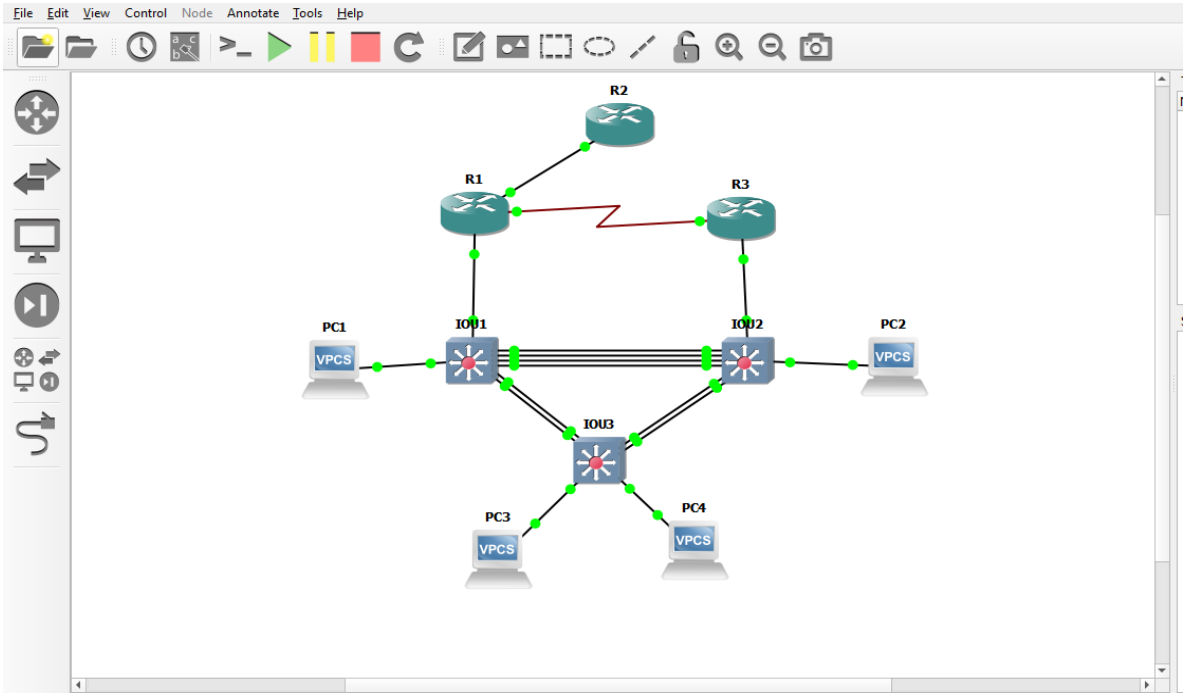
Tabla 1. Tabla de direccionamiento.

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
	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. Topología con las interfaces asignadas.



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Configuración Router 1.

```
R1#en
R1#conf t
R1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface f3/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
```

```
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface ether5/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s1/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

Configuración Router 2

```
R2#en
R2#conf t
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface f0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#do wr
R2(config-if)#exit
R2(config)#do wr
Building configuration...
[OK]
R2(config)#
```

Configuración Router 3

```
R3#en
R3#conf t
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
```

```
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface ether5/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1013::3/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#do wr
Building configuration...
[OK]
```

Configuración D1

```
IOU1#en
IOU1#conf t
IOU1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface ether2/0
D1(config-if)#no switchport
```

```
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range ether 1/2-3
D1(config)#interface range ether 2/1-3
D1(config)#interface range ether 3/0-2
D1(config-if)#shutdown
D1#exit
```

Configuración D2

```
IOU2#en
IOU2#conf t
IOU2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
```

```
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
D2(config)#interface ether2/0
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
```

```
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range ether1/0-1
D2(config-if-range)#interface range ether2/1-3
D2(config-if-range)#interface range ether3/0-2
D2(config-if-range)#shutdown
D2(config-if-range)#exit
```

Configuración A1

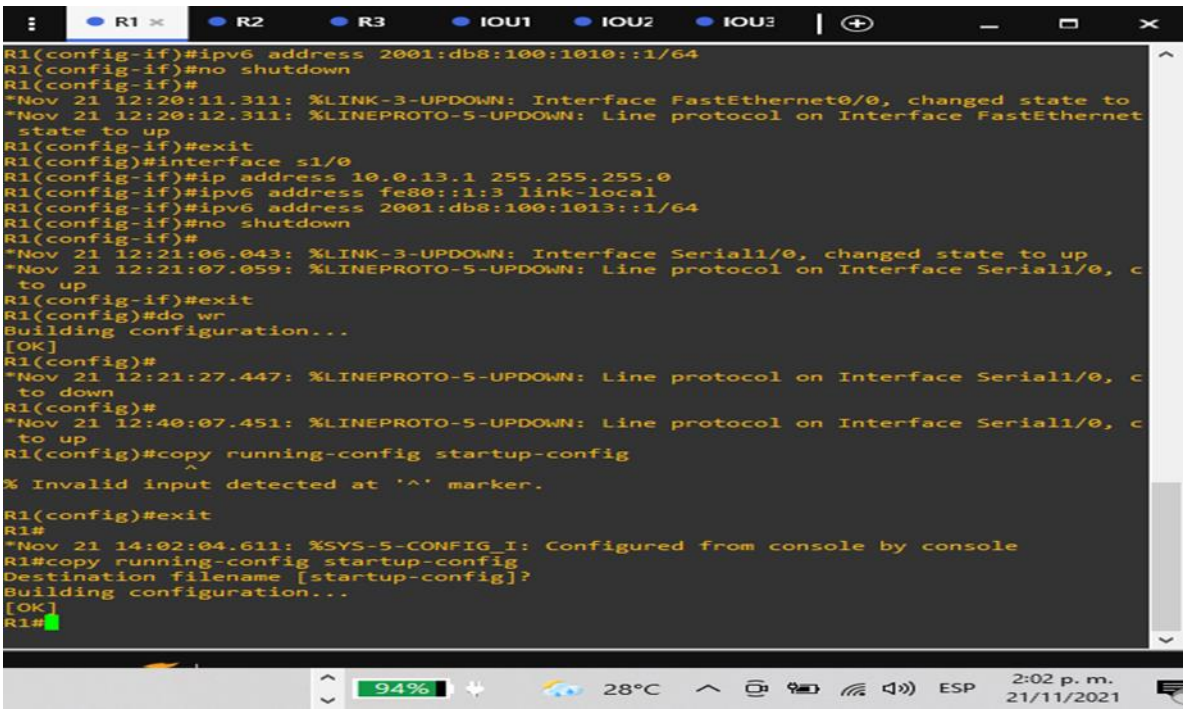
```
IOU3#en
IOU3#conf t
IOU3(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
A1(config)#interface vlan 100
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range ether0/1-3
A1(config-if-range)#interface range ether2/0-3
A1(config-if-range)#interface range ether3/0-1
A1(config-if-range)#shutdown
A1(config-if-range)#exit
```

En este paso se ingresa la configuración básica de los equipos (routers). Se ingresa al modo privilegiado, para poder hacer la configuración básica, donde se configura nombra router, tipo de dirección ipv6, se habilita la traducción de nombre a dirección basado en DNS del host, se crea un mensaje de aviso, se ingresa al modo de configuración de línea de la consola 0, En el puerto de la consola 0 nunca se agotará el tiempo de espera, evita que los mensajes inesperados que aparecen en pantalla, se procede a configurar la interface ether, se asigna la dirección ipv4 y la máscara de subred, se asigna la dirección link local a la interface, se asigna la dirección ipv6, se habilita la interface, se procede a configurar la interface ether, se asigna la dirección ipv4 y la máscara de subred, se asigna la dirección link local, se asigna la dirección ipv6, se habilita la interface ether1/0, se procede a configurar la interface s2/0 de R1, se asigna la dirección ipv4 y la máscara de subred, se asigna la dirección link local, se asigna la dirección ipv6, se habilita la interfaz s2/0.

Se configura los dispositivos de los switches. En el modo de configuración global se asigna el nombre al Switchs, se habilita el routing ipv4, se habilita routing IPv6 Se habilita la traducción de nombre a dirección basado en DNS del host, se crea un mensaje de aviso, se ingresa al modo de configuración de línea de la consola 0, en el puerto de la consola 0 nunca se agotará el tiempo de espera, evita que los mensajes inesperados que aparecen en pantalla desplacen los comandos que estamos escribiendo en el momento, se configura la vlan 100, se le asigna nombre, se configura la vlan 101, se le asigna nombre, se configura la vlan 102, se le asigna nombre, se configura la vlan 999 Se le asigna nombre como la vlan nativa, se procede a configurar la interface ether, se aporta a la interface capacidad de capa3, se asigna la dirección ipv4 y la máscara de subred, se asigna la dirección link local a la interface, se asigna la dirección ipv6.

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

Figura 3. Copia al archivo startup-config en R1



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.

Configuración PC1

PC1> ip 10.0.100.5/24 10.0.100.254
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

Configuración PC4

PC4> ip 10.0.100.6/24 10.0.100.254
PC1 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

En este paso se configura la dirección ipv4 y el Gateway predeterminado.

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.

Tabla 2. Lista de tareas de la parte 2.

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces deinterconexión 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 nativaen los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocoloRapid 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 casode falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades deapoyo 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 seconectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, comose 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 debenrecibir 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

Desarrollo de la tarea 2.1.

D1 and D2

D1#conf t / se ingresa a la configuración del terminal
D1(config)#int range ether0/0-3 / se indica que conexión se va a configurar
D1(config-if-range)#sw trunk encap dot1q / se define la encapsulación protocolo 802.1Q
D1(config-if-range)#sw mode trunk / se define modo trunk (se establece como troncal)
D1(config-if-range)#exit / se sale del modo trunk

D1 and A1

D1#conf t
D1(config)#int range ether1/0-1
D1(config-if-range)#sw trunk encap dot1q
D1(config-if-range)#sw mode trunk
D1(config-if-range)#exit

D2 and A1

D2#en
D2#conf t
D2(config)#int range ether1/2-3
D2(config-if-range)#sw trunk encap dot1q
D2(config-if-range)#sw mode trunk
D2(config-if-range)#exit

En este paso se configura las interfaces de todos los switches en troncales IEEE 802.1Q sobre los enlaces de interconexión en los switches, además se habilita el enlaces trunk 802.1Q.

Desarrollo de la tarea 2.2.

D1:

```
D1#vlan database                          / se utiliza para almacenar datos.
D1(vlan)#vlan 999 name NATIVE             / se la cambia el nombre a la vlan.
VLAN 999 modified:
   Name: NATIVE
```

D2:

```
D2#vlan database
D2(vlan)#vlan 999 name NATIVE
VLAN 999 modified:
   Name: NATIVE
```

A1:

```
A1#vlan database
A1(vlan)#vlan 999 name NATIVE
VLAN 999 modified:
   Name: NATIVE
```

En este paso se cambia el nombre de la vlan 999, como vlan nativa en todos los switches de los enlaces troncales.

Desarrollo de la tarea 2.3 y 2.4.

D1

```
D1#conf t                                        / se ingresa a la configuración del
terminal
D1(config)#spanning-tree vlan 100 root primary   /Se activa el protocolo RSPT y el
                                                   puente RSTP primario.
D1(config)#spanning-tree vlan 101 root secondary  /Se activa el protocolo RSPT y el
                                                   puente RSTP secundario.
D1(config)#spanning-tree vlan 102 root primary
D1(config)#exit
```

D2

```
D2#conf t
D2(config)#spanning-tree vlan 100 root secondary
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 102 root secondary
D2(config)#exit
```

En este paso se está habilitando es protocolo Rapid Spanning-Tree y se configura los puente raíz RSTP.

Desarrollo de la tarea 2.5

D1 a D2 – Port channel 12

D1#conf t / se ingresa a la configuración del terminal

D1(config)#int range ether0/0-3 / Se accede a configurar la interface ether0/0-3
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active / Se activa el protocolo LACP de forma incondicional.
D1(config-if-range)#exit

D2#conf t
D2(config)#int range ether0/0-3
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#exit

D1 a A1 – Port channel 1

D1(config)#int range ether1/0-1
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#exit

A1#conf t
A1(config)#int range ether1/0-1
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 1 mode active
A1(config-if-range)#exit

D2 a A1 – Port channel 2

D2#conf t
D2(config)#int range ether1/2-3
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#exit

A1#conf t
A1(config)#int range ether1/2-3
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#exit

En este paso se crea los canales (12, 1,2), en los dispositivos de los shwitches.

Desarrollo de la tarea 2.6

PC 1

```
D1#conf t
D1(config)#int range ether3/3                    / selección de puerto a configurar.
D1(config-if-range)#switchport mode access     / se coloca en modo de acceso
D1(config-if-range)#switchport 24ccess vlan 100 / se asigna la vlan
D1(config-if-range)#spanning-tree portfast         / se configura protocolo
D1(config-if-range)#no shutdown                    / se sube el servicio en la interface
D1(config-if-range)#exit
```

PC 2

```
D2#conf t
D2(config)#int range ether3/3
D2(config-if-range)#switchport mode 24ccess
D2(config-if-range)#switchport 24ccess vlan 102
D1(config-if-range)#spanning-tree portfast
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
```

PC 3 y PC4

```
A1#conf t
A1(config)#int range ether3/3
A1(config-if-range)#switchport 24ccess vlan 101
A1(config-if-range)#spanning-tree portfast
A1(config-if-range)#no shutdown
A1(config-if-range)#exit

A1#conf t
A1(config)#int range ether0/0
A1(config-if-range)#switchport 24ccess vlan 100
A1(config-if-range)#spanning-tree portfast
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
```

En este paso se configura los puertos de acceso que van conectada hacia los computadores.

Desarrollo de la tarea 2.7

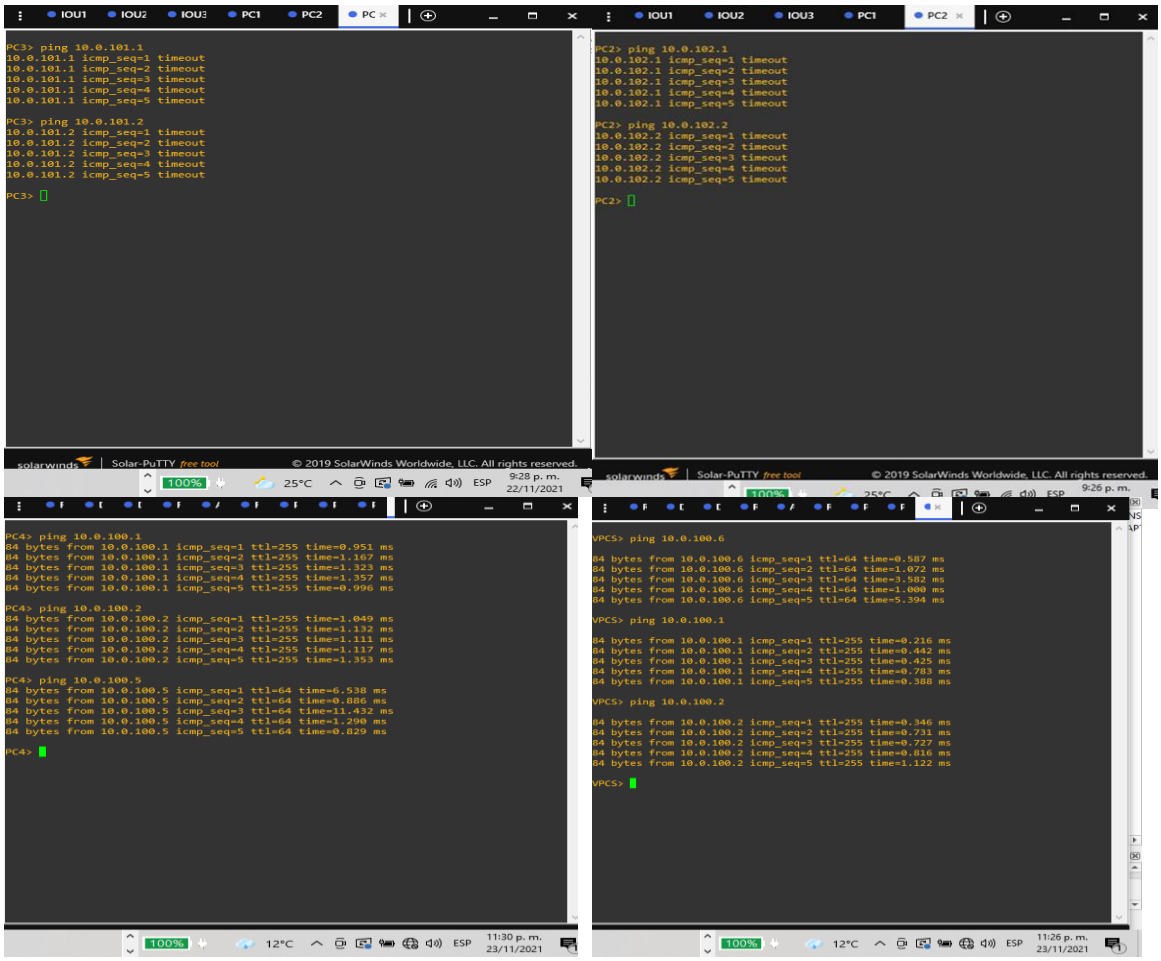
Se emplea el comando “ip dhcp” en PC2 y PC3 para obtener las direcciones ip válidas.

En PC2 se obtuvo:
IP/MASK: 10.0.102.110/24
GATEWAY: 10.0.102.254
DHCP SERVER: 10.0.102.1
LINK-LOCAL SCOPE: fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE: 2001:db8:100:102:2050:79ff:fe66:6801/64

En PC3 se obtuvo:
IP/MASK: 10.0.101.210/24
GATEWAY: 10.0.101.254
DHCP SERVER: 10.0.101.2
LINK-LOCAL SCOPE: fe80::250:79ff:fe66:6802/64
GLOBAL SCOPE: 2001:db8:100:101:2050:79ff:fe66:6802/64

Desarrollo de la tarea 2.8

Figura 4. Pines de los 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.

Tabla 3. Lista de tareas de la parte 3.

Tarea#	Tarea	Especificación
3.1	En la "Red de la Compañía" (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 Compañía" (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 através 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-id2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6con 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 R2en 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.

Desarrollo de la tarea 3.1

R1

```
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)#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
```

R3

```
R3(config)#router ospf 4
R3(config-router)# router-id 0.0.4.3
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
R3(config-router)#exit
```

D1

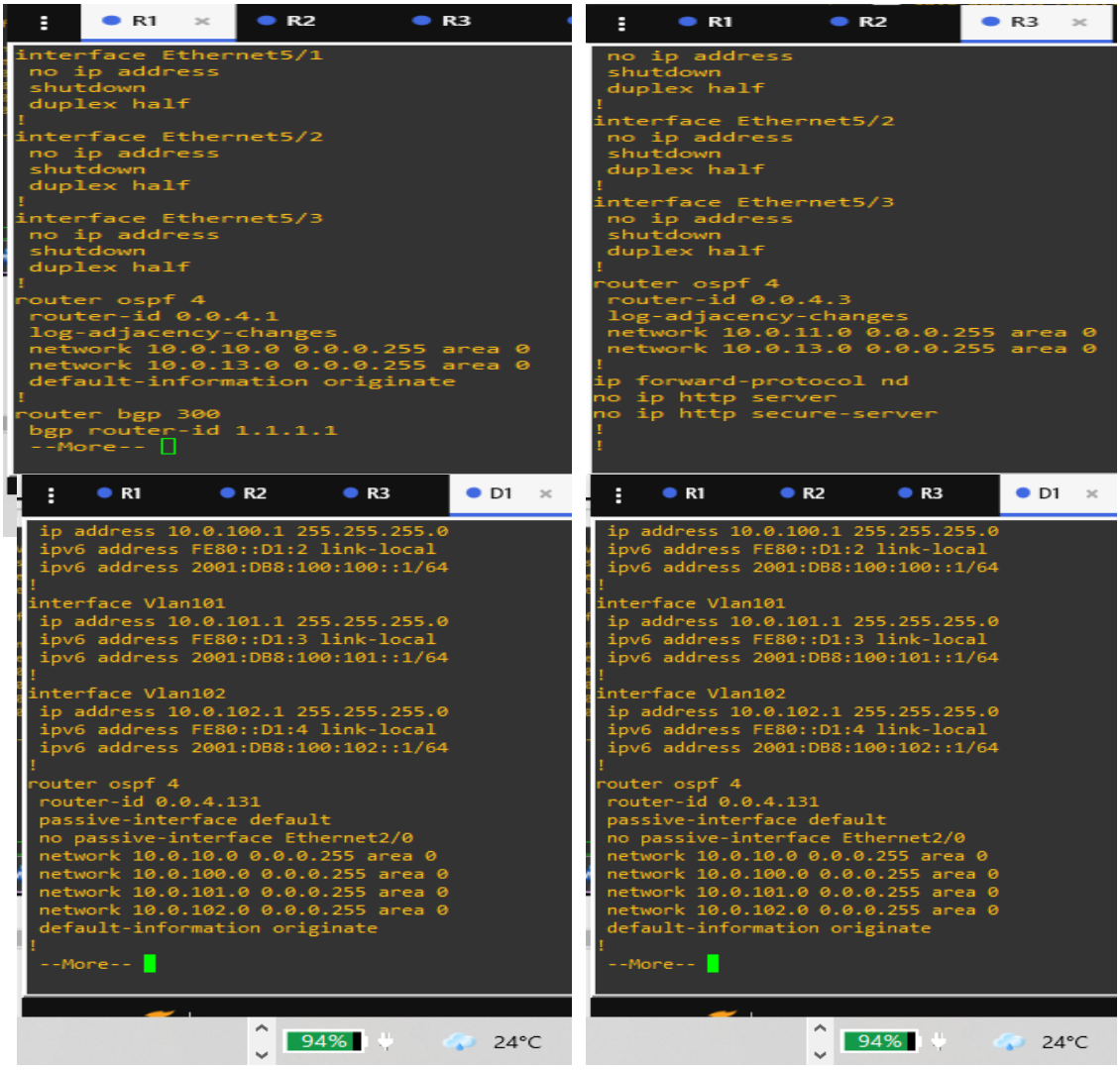
```
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
D1(config-router)# passive-interface default
D1(config-router)# default-information originate
D1(config-router)# no passive-interface ether2/0
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0
D1(config-router)# network 10.0.100.0 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)#exit
```

D2

```
D2#conf t
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)# passive-interface default
D2(config-router)# no passive-interface ether2/0
D2(config-router)# network 10.0.11.0 0.0.0.255 area 0
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)#exit
```

En este paso se configura los protocolos de enrutamiento en IPv4 e IPv6.

Figura 5. Comando show running-conf, verificar la configuración OSPFv2 área 0 en los dispositivos R1, R3, D1 y D2.



Desarrollo de la tarea 3.2.

R1

R1(config-router)#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 configuración
R1(config)#interface ether5/0	/ 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 configuración
R1(config)#interface s1/0	/ 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 configuración

```
R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#exit
```

R3

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface e5/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
```

D1

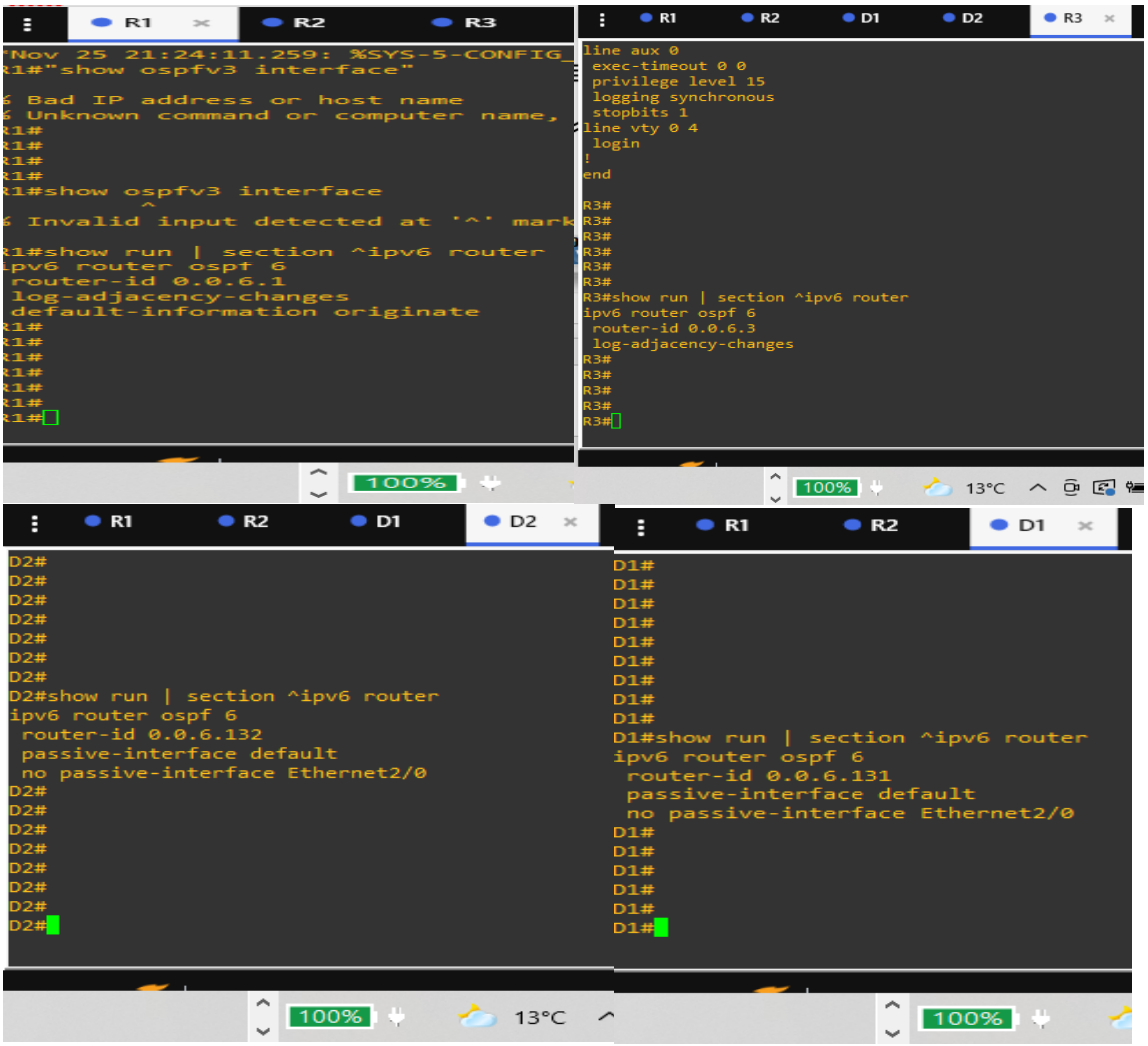
```
D1#conf t
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)# passive-interface default
D1(config)# no passive-interface ether2/0
D1(config)#exit
```

D2

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)# passive-interface default
D2(config)# no passive-interface ether2/0
D2(config-if)#exit
```

En este paso se configura classic single-área OSPFv3 en área 0.

Figura 6. Comando show run | section, verificar la configuración OSPFv3 área 0



Desarrollo de la tarea 3.3

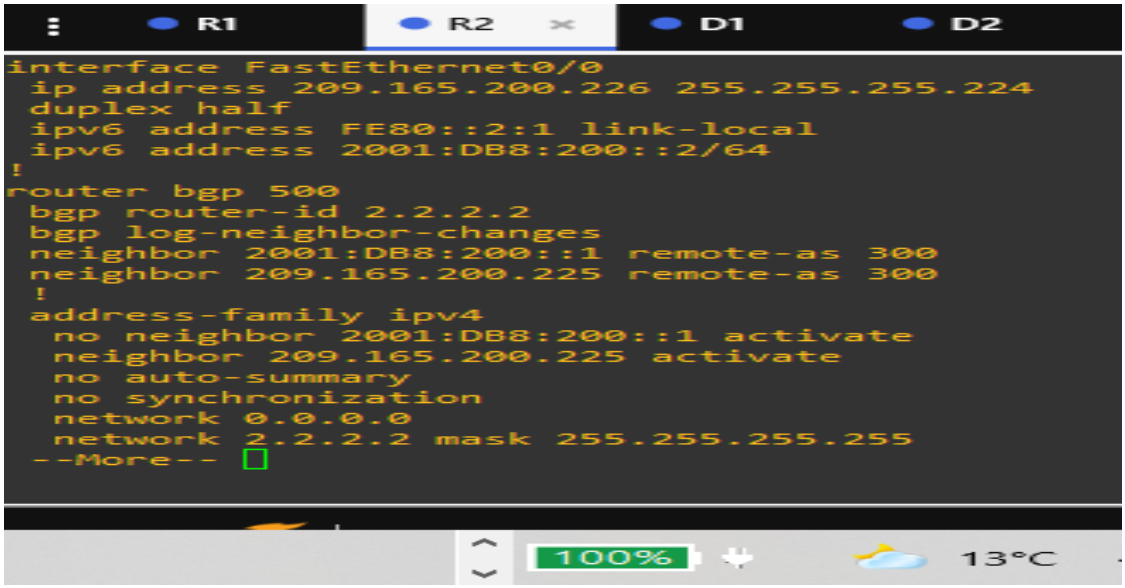
R2

R2(config-if)#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
R2(config-router)# bgp log-neighbor-changes
R2(config-router)#neighbor 2001:DB8:200::1
remote-as 300
R2(config-router)#neighbor 209.165.200.225
remote-as 300
R2(config-router)# address-family ipv4 / Se accede a la familia de direcciones ipv4
R2(config-router-af)#network 0.0.0.0 / Se accede a la familia de direcciones ipv4
R2(config-router-af)#network 2.2.2.2 / Se anuncia la red loopback 0 ipv4 (/32).
mask 255.255.255.255
R2(config-router-af)#no neighbor
2001:DB8:200::1 activate

R2(config-router-af)#neighbor
209.165.200.225 activate
R2(config-router-af)#exit-address-family / Se sale de la configuración de la familia de direcciones ipv4
R2(config-router)#address-family ipv6 / Se accede a la familia de direcciones ipv6
R2(config-router-af)#network ::/0 / En IPv6 address family se anuncia la ruta por defecto (::/0).
R2(config-router-af)#network 2001:DB8:2222::/128 / red Loopback 0 IPv4 (/128)
R2(config-router-af)# neighbor 2001:DB8:200::1
activate
R2(config-router-af)#exit-address-family
R2(config-router)#ip route 0.0.0.0 0.0.0.0
Loopback0
R2(config)#ipv6 route ::/0 Loopback0
R2(config)#exit

En este paso se configura en la Red ISP, la MP-BGP ASN 500, en el router 2.

Figura 7. Verificar la configuración de la bgp 500



Desarrollo de la tarea 3.4

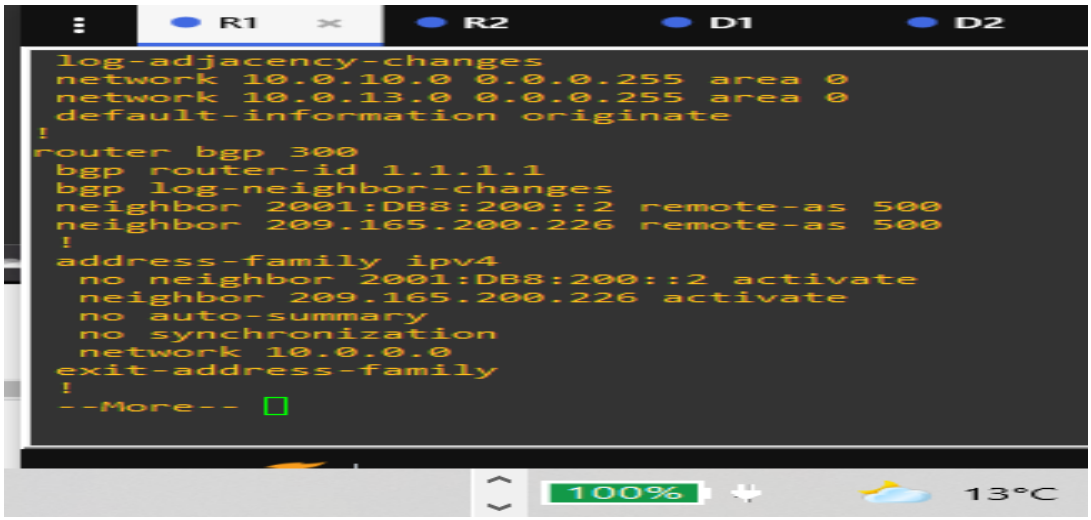
R1

R1#conf t
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
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
R1(config-router)#address-family ipv4 unicast

R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)#no neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226 activate
R1(config-router-af)# neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#exit-address-family

En este paso se configura en la Red ISP, la MP-BGP ASN 300, en el router 1.

Figura 8. Verificar la configuración de la bgp 300



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 Compañia”. Las tareas de configuración son las siguientes:

Tabla 4. Lista de tareas de la 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. • 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 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. 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.

Desarrollo de la tarea 4.1

D1

```
D1#conf t
D1(config)#ip sla 4                          / Se define el número de sesión 4 del SLA
D1(config-ip-sla)#icmp-echo 10.0.10.1        / Se inicia la configuración IP SLA ICMP Echo
                                               con destino a la interfaz ipv4 ether5/0
D1(config-ip-sla-echo)#frequency 5           / Se prueba la disponibilidad de la interfaz
                                               ether3/0 de R1 cada 5 segundos.
D1(config-ip-sla-echo)#exit
D1(config-ip-sla)# ip sla 6                  / Se define el número de sesión 6 del SLA.
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 / Se inicia la configuración IP SLA
                                                   ICMP Echo con destino a la interfaz
                                                   ipv6 ether5/0 de R1
D1(config-ip-sla-echo)#frequency 5           / Se prueba la disponibilidad de la interfaz
                                               ether5/0 de R1 cada 5 segundos
D1(config-ip-sla-echo)#exit
D1(config)##ip sla schedule 4 life forever   / Se programa la SLA 4 para una
start-time now                                 implementación inmediata sin tiempo de
                                               finalización.
D1(config)#ip sla schedule 6 life forever    / Se programa la SLA 6 para una
start-time now                               / implementación inmediata sin tiempo de
                                               finalización

D1(config)#track 4 ip sla 4                  / Se crea el número de rastreo 4 y se asocia
                                               al IP SLA 4.
D1(config-track)#delay down 10 up 15         / Cada 10 segundos se debe notificar el
                                               cambio de estado de la IP SLA cuando
                                               pasa de down a up y cada 15 segundos
                                               cuando para de up a down.

D1(config-track)#exit
D1(config)#track 6 ip sla 6                  / Se crea el número de rastreo 6 y se
                                               asocia al IP SLA 6.
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
```

En este paso se crea la IP SLAs, que prueban la accesibilidad en la interface ether5/0, en el switch 1.

Figura 9. Validaciòn del estado de las IP SLA y los Track en D1.

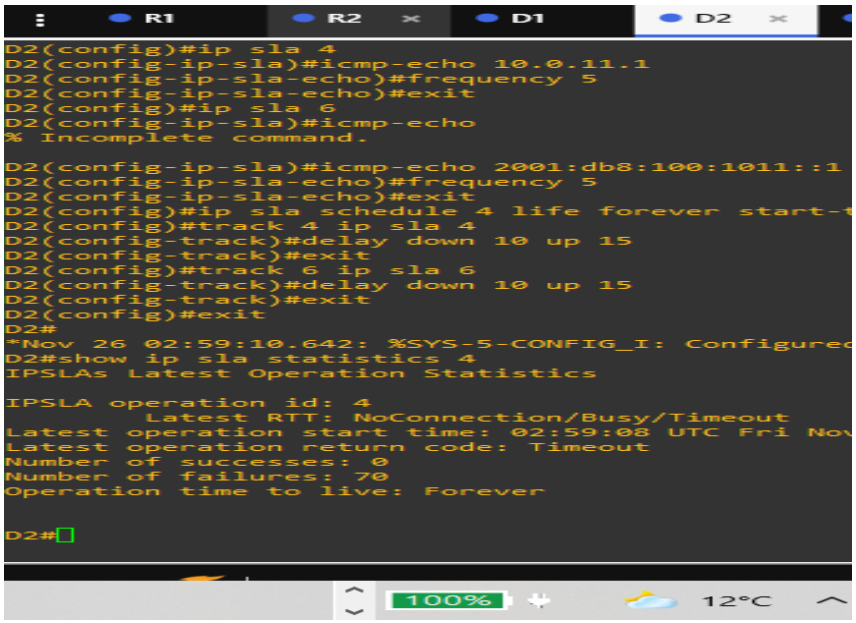
Desarrollo de la tarea 4.2

D2

D2#conf t
D2(config)#ip sla 4 / Se define el número de sesión 4 del SLA.
D2(config-ip-sla)#icmp-echo 10.0.11.1 / Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv4 ether5/0 de R3
D2(config-ip-sla-echo)#frequency 5 / Se prueba la disponibilidad de la interfaz G0/0 de R3 cada 5 segundos.
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6 / Se define el número de sesión 6 del SLA.
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 / Echo con destino a la interfaz ipv6 ether5/0 de R3.
D2(config-ip-sla-echo)#frequency 5 /Se prueba la disponibilidad de la interfaz ether2/0 de R1 cada 5 segundos
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now / Se programa la SLA 4 para una implementación inmediata sin tiempo de finalización.
D2(config)#track 4 ip sla 4 / Se crea el número de rastreo 4 y se asocia al IP SLA 4.
D2(config-track)#delay down 10 up 15 / Cada 10 segundos se debe notificar el cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando pasa de up a down.
D2(config-track)#exit
D2(config)#track 6 ip sla 6 / Se crea el número de rastreo 6 y se asocia al IP SLA 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit

En este paso se crea la IP SLAs, que prueban la accesibilidad en la interface ether5/0, en el switch 2.

Figura 10. Validaciòn del estado de las IP SLA y los Track en D2



Desarrollo de la tarea 4.3

D1

D1#conf t
D1(config)#interface vlan 100 / Se accede a la interfaz VLAN 100.
D1(config-if)#standby version 2 /Se configura el HSRP para usar la versión 2.
D1(config-if)#standby 104 ip 10.0.100.254 / Se inicia la configuración IPv4 HSRP grupo 104 para la VLAN 100.
D1(config-if)#standby 104 priority 150 / Se establece la prioridad del grupo 104 en 150.
D1(config-if)#standby 104 preempt / Se habilita la preferencia al grupo 104
D1(config-if)#standby 104 track 4 decrement 60 / Se rastrea el objeto 4 y se decrementa en 60.
D1(config-if)#standby 106 ipv6 autoconfig / Se inicia la configuración IPv6 HSRP grupo 106.
D1(config-if)#standby 106 priority 150 / Se establece la prioridad del grupo en 150.
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
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

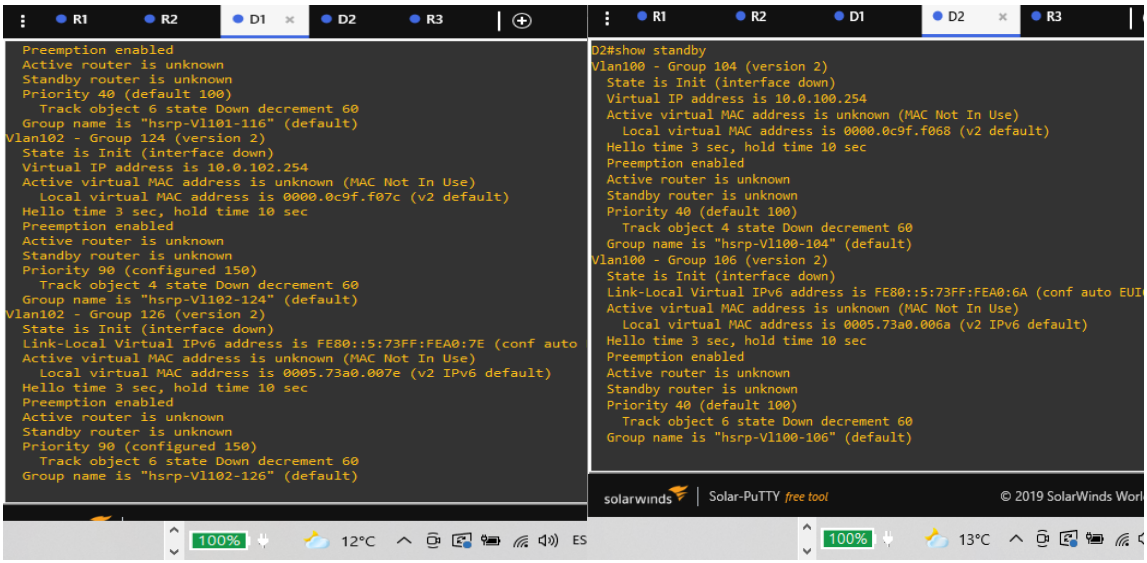
```
D1(config-if)#standby 114 track 4
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 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
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
D1(config-if)#exit
```

D2

```
D2#conf t
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 preempt
D2(config-if)#standby 104 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)#exit
D2(config)#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)#standby 114 track 4 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)#exit
D2(config)#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 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit
```

En este paso se configura la HSRPv2 en el switch 1 y 2.

Figura 11. Verificación implementación de HSRPv2 en D1 y 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. Lista de tareas de la parte 5.

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**.

Desarrollo de la tarea 5.1

R1(config)#enable algorithm-type scrypt secret cisco12345cisco
R2(config)#enable algorithm-type scrypt secret cisco12345cisco
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
A1(config)#enable algorithm-type scrypt secret cisco12345cisco

Desarrollo de la tarea 5.2

R1(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R2(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R3(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D1(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D2(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

A1(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

En este punto se configura la seguridad de los dispositivos de la red y se crea un usuario local; los equipos están usando el algoritmo de encriptación SCRYPT.

Figura 12. Verificaciòn de los 5.1 y 5.2 con el comando show run | include

Desarrollo de la tarea 5.3-5.4-5.5

R1

```
R1#conf t
R1(config)#aaa new-model                    / Se configura la lista de métodos de
                                              autenticación AAA.
R1(config)#radius server RADIUS             / Se inicia la configuración del servidor RADIUS
                                              en R1.
R1(config-radius-server)#$ address ipv4     / Se especifica la dirección IP y los puertos UDP
10.0.100.6 auth-port 1812 acct-port 1813      para R1.
R1(config-radius-server)#key $trongPass     / Se asigna la contraseña al servidor RADIUS
                                              para R1.
R1(config-radius-server)#username sadmin  /Al usuario sadmin se le asigna la contraseña
privilege 15 secret cisco12345cisco
R1(config)#aaa session-id common
R1(config)#aaa authentication login default group radius local
R1(config)#exit
```

R2

```
R2#conf t
R2(config)#aaa new-model
R2(config)#radius server RADIUS
R2(config-radius-server)#$ address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R2(config-radius-server)#key $trongPass
R2(config-radius-server)#username sadmin privilege 15 secret cisco12345cisco
R2(config)#aaa session-id common
R2(config)#aaa authentication login default group radius local
R2(config)#exit
```

D1

```
D1#conf t
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)#username sadmin privilege 15 secret cisco12345cisco
D1(config)#aaa session-id common
D1(config)#aaa authentication login default group radius local
D1(config)#exit
```

D2

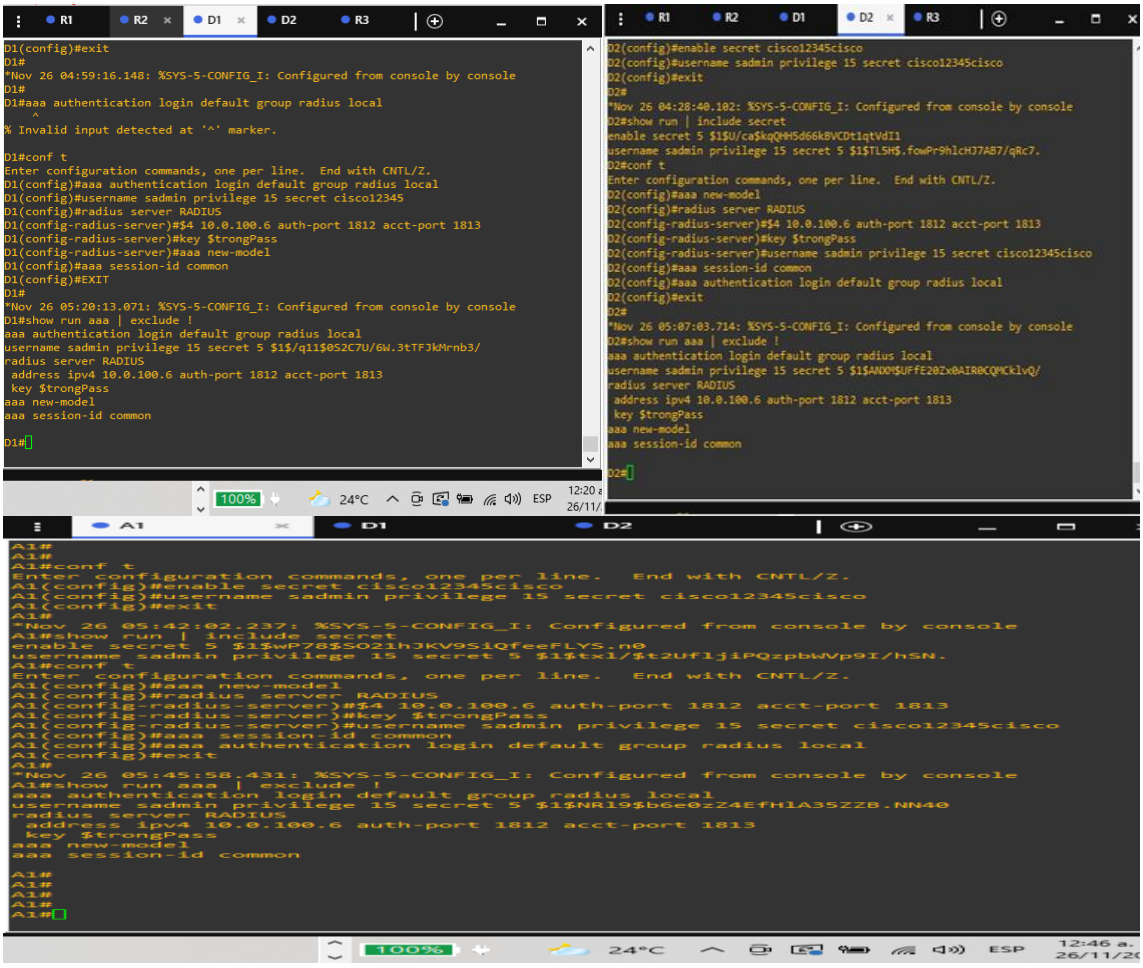
```
D2#conf t
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#$ address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $trongPass
D2(config-radius-server)#username sadmin privilege 15 secret cisco12345cisco
```

D2(config)#aaa session-id common
D2(config)#aaa authentication login default group radius local
D2(config)#exit

A1

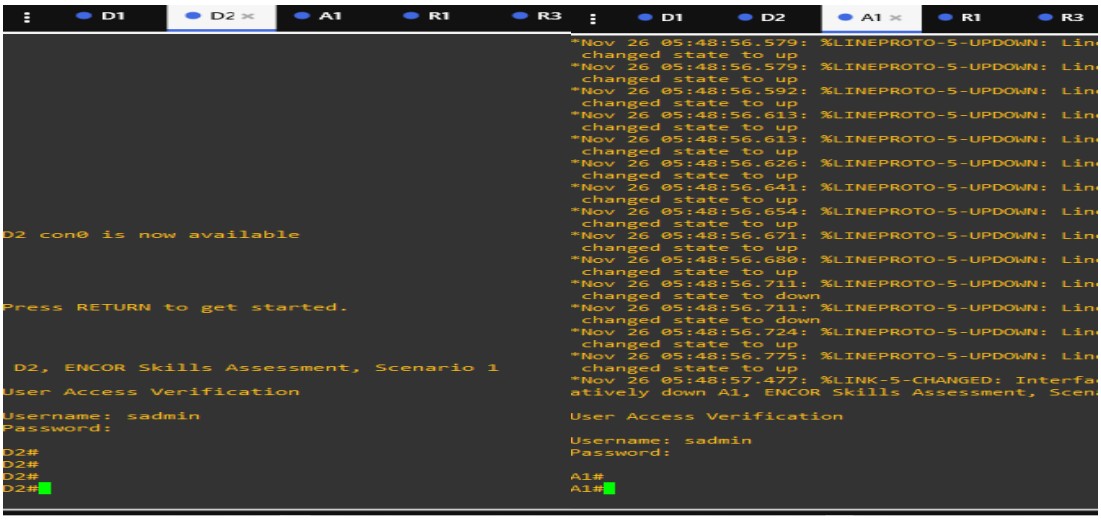
A1#conf t
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#$ address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)#key $trongPass
A1(config-radius-server)#username sadmin privilege 15 secret cisco12345cisco
A1(config)#aaa session-id common
A1(config)#aaa authentication login default group radius local
A1(config)#exit

Figura 13. Verificaciòn de los 5.3, 5.4 y 5.5 con el comando show run | exclude



Desarrollo de la tarea 5.6

Figura 14. Verificación del servicio AAA en los dispositivos (excepto R2).



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. Lista de tareas de la 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*.

Desarrollo de la tarea 6.1, 6.2 y 6.3

En todos los dispositivos

R1(config)#ntp server 2.2.2.2 / Se configura el reloj local de R1 a la hora UTC actual, Para ello se configura NTP para que R1 se sincronice por medio de la interfaz loopback 0 de R2.

R3(config)#ntp server 10.0.10.1 / Se configura el reloj local de R3 a la hora UTC actual. Para ello se configura NTP para que R3 se sincronice por medio de la interfaz ether5/0 de R1

D1(config)#ntp server 10.0.10.1 / Se configura el reloj local de D3 a la hora UTC actual, para ello se configura NTP para que R3 se sincronice por medio de la interfaz ether2/0 de R1

D2(config)#ntp server 10.0.10.1 / Se configura el reloj local de D2 a la hora UTC actual, para ello se configura NTP para que D2 se sincronice por medio de la interfaz ether5/0 de R3.

A1(config)#ntp server 10.0.10.1 / Se configura el reloj local de A1 a la hora UTC actual. Para ello se configura NTP para que R3 se sincronice por medio de la interfaz ether2/0 de R1.

R2(config)#ntp master 3 / Se configura R2 como NTP maestro en el nivel de estrato 3.

Figura 15. Verificación de la configuración de NTP en los equipos.

Desarrollo de la tarea 6.4

R1

R1(config)#logging host 10.0.100.5 / Se configura el host PC1 para que sea el host de registro de destino para R1.
R1(config)#logging trap warning / Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.
R1(config)#logging on / Se habilita el registro para que los mensajes puedan ser enviados.

R3

```
R3#conf t
R3(config)#logging host 10.0.100.5
R3(config)#logging trap warning
R3(config)#logging on
R3(config)#exit
```

D1

```
D1(config)# logging host 10.0.100.5
D1(config)#logging trap warning
D1(config)# logging on
D1(config)#exit
```

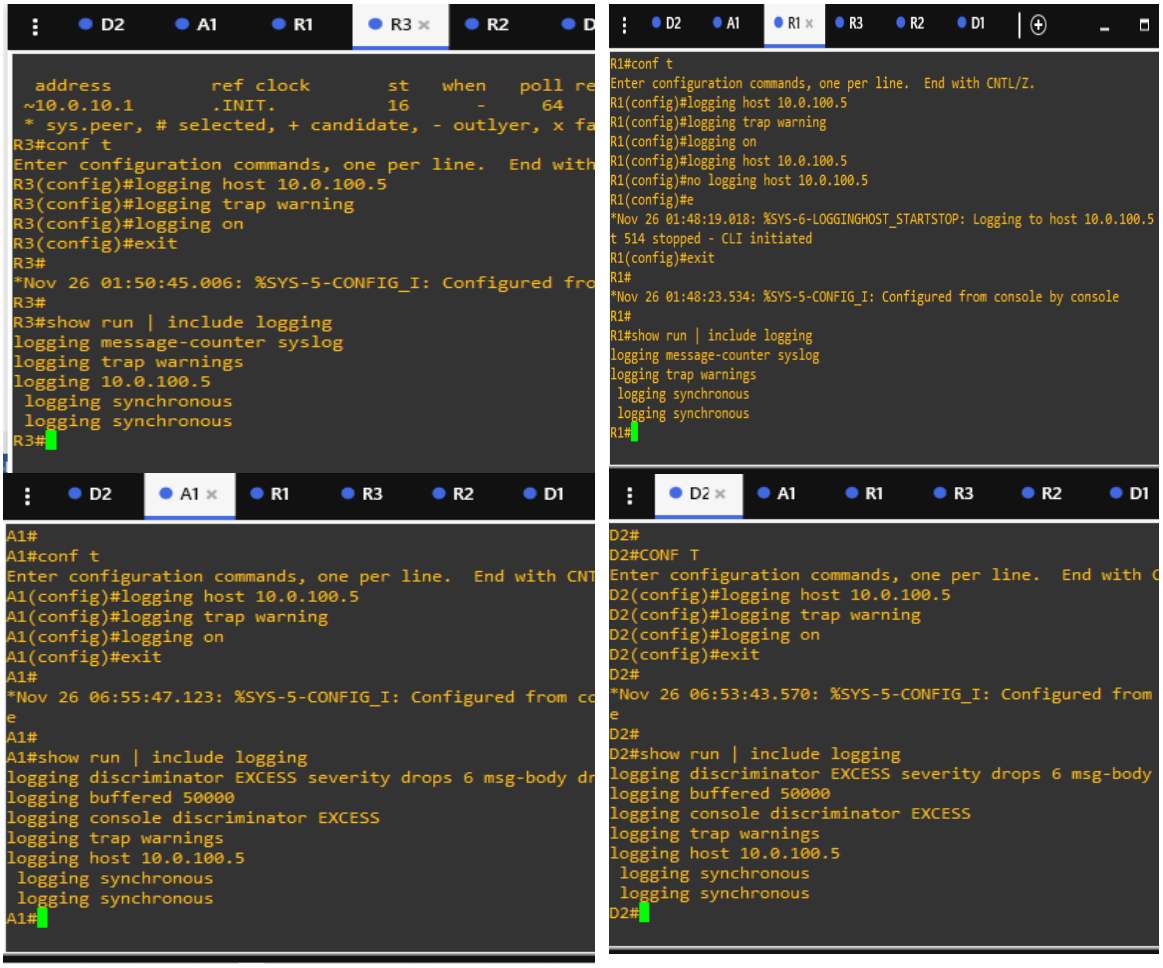
D2

```
D2#conf t
D2(config)#logging host 10.0.100.5
D2(config)#logging trap warning
D2(config)#logging on
D2(config)#exit
```

A1

```
A1#conf t
A1(config)#logging host 10.0.100.5
A1(config)#logging trap warning
A1(config)#logging on
A1(config)#exit
```

Figura 16. Verificaciòn de la syslog en los equipos.



Desarrollo de la tarea 6.5

R1

R1#conf t

R1(config)#snmp-server community ENCORSA ro SNMP-NMS / Se establece el “community string” en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.

R1(config)#ip access-list standard SNMP-NMS / Se limita el acceso SNMP a la dirección IP de PC1.

R1(config-std-nacl)#permit host 10.0.100.5

R1(config-std-nacl)#exit

R1(config)#snmp-server contact Albeiro Pedrozo / Se configura el valor de contacto SNMP con mi nombre.

R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA / Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.

R1(config)#snmp-server enable traps bgp / En R1, se habilita el envío de traps: bgp, config, y ospf.

```
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
R1(config)#end                                  / Se sale del modo configuración.
```

R3

```
R3#conf t
R3(config)#snmp-server community ENCORSA ro SNMP-NMS
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-server contact Albeiro Pedrozo
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#end
```

D1

```
D1#conf t
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
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 Albeiro Pedrozo
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
D1(config)#end
```

A1

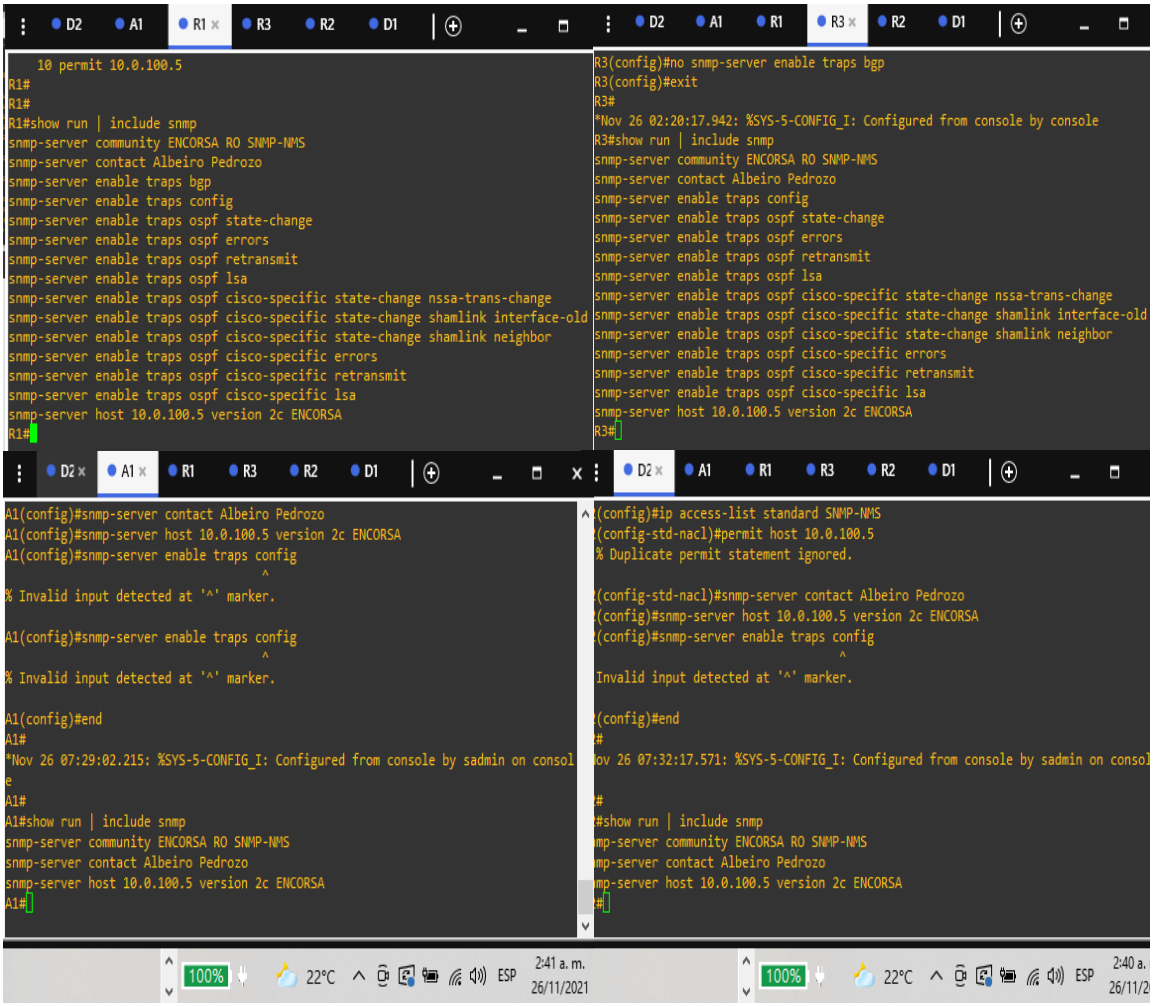
```
A1#conf t
A1(config)#snmp-server community ENCORSA ro SNMP-NMS
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)#exit
A1(config)#snmp-server contact Albeiro Pedrozo
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server enable traps config
A1(config)#end
```

D2

```
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#snmp-server contact Albeiro Pedrozo
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
```

D2(config)#snmp-server enable traps config
D2(config)#end

Figura 17. Se limita el acceso SNMP a la dirección IP de la PC1.



CONCLUSIONES

Con el desarrollo de la presente actividad brinda que el estudiante de ingenierìa en telecomunicaciones adquiera conocimientos, sobre la configuraciòn de una red de una compañía, con base a los conceptos, definiciones y características principales de los dispositivos para configurar la red ante mencionada.

Se construye una topologia con la herramienta GNS3, donde se configura los dispositivos de acuerdo a los requerimientos exigidos.

Se configura cada dispositivos con ajustes bàsicos y el direccionamiento basico, se configura la capa 2 de la red y el soporte de Host, los protocolos de enrutamiento, la redundancia del primer salto, la seguridad y las características de administración de red,

Con el aprendizaje y la información sobre los códigos que utilizamos para configurar los dispositivos, pudimos comprender y aprender un mejor conocimiento para colocarlo en práctica en nuestras vidas laboral y profesional sobre mencionado tema.

Con el aprendizaje de mencionados temas adquirí un mayor conocimiento sobre los conceptos básicos, que se utilizan en la configuraciòn de una red de una empresa.

En general, logre comprender y adquirir nuevos conocimientos sobre las configuraciones que utiliza una empresa; al igual logre comprender el funcionamiento de los códigos que se utilizaron en GNS3; esta información que adquirir nos serán útil para el desarrollo personal del futuro ingeniero, al igual que nuestra vida personal y laboral.

REFERENCIAS BIBLIOGRÁFICAS

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

UNAD (2017). **Configuración de Switches y Routers [OVA]**. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC