DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JORGE AURELIO GARCIA ALVAREZ

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JORGE AURELIO GARCIA ALVAREZ

Diplomado de opción de grado presentado para optar el título 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
UBATE
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

UBATE, 29 de noviembre de 2021

AGRADECIMIENTOS

Agradezco a Dios por la oportunidad que me ha dado de poder estudiar crecer profesionalmente y aprender cada día nuevas cosas, a mis padres Aureliano García y Romelia Álvarez porque siempre me apoyaron ya sea desde un consejo hasta económicamente y nunca dejaron de creer en mí y apoyarme moralmente y a los tutores que a lo largo de mi carrera me han brindado los conocimientos que necesito para lograr ser un ingeniero electrónico.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ENRUTAMIENTO: Es el proceso en el cual se envía información o paquetes a través de redes, en las cuales siempre se buscara el mejor camino para que pase la información.

DIRECCIONAMIENTO: Se entiende como el indicativo de cada equipo o dispositivo el cual es el encargado de direccionar la información a través de un campo para llegar a su destino deseado.

PROGRAMACIÓN: Se entiende como la acción de ejecutar códigos o comandos específicos a un dispositivo para así poder realizar una tarea deseada por el usuario.

REDES: Se comprende a un conjunto de dispositivos que se encuentran conectados mediante algún tipo de conexión y en los cuales siempre se encuentran transportando información o datos.

INALAMBRICO: Es un tipo de conexión que se da por medio de ondas electromagnéticas sin la necesidad de que haya algún tipo de cable por medio de estas ondas puede viajar datos o información.

RESUMEN

El diplomado de profundización CCNP tiene como objetivo el desarrollo de un trabajo enfocado para estudiantes de electrónica y de telecomunicaciones, en él se encuentra un escenario propuesto para el desarrollo y la interacción del usuario para configurarlo y probar su funcionamiento, en el desarrollo de este trabajo iniciamos trabajando en la plataforma CISCO Packet Tracer, el cual es un programa especializado para la solución de esta actividad, este programa nos permite seleccionar los diferentes elementos para llevar a cabo el desarrollo de la actividad, seguido a esto debemos realizar las respetivas configuraciones, enrutamientos, conmutaciones entre otras, para poder establecer una conexión de redes entre cada uno de los elementos.

Finalmente después de desarrollar toda la programación, se deben realizar los respectivos pines para establecer las conexiones y verificar su funcionamiento adecuado, logrando así cumplir con el desarrollo de la actividad.

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

ABSTRACT

The CCNP deepening diploma aims to develop a focused work for students of electronics and telecommunications, in it there is a proposed scenario for the development and interaction of the user to configure it and test its operation, in the development of this work We started working on the CISCO Packet Tracer platform, which is a specialized program for the solution of this activity, this program allows us to select the different elements to carry out the development of the activity, followed by this we must make the respective configurations , routing, switching, among others, in order to establish a network connection between each of the elements.

Finally, after developing all the programming, the selected pins must be made to establish the connections and verify their proper operation, thus achieving compliance with the development of the activity.

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

INTRODUCCIÓN

El desarrollo de este trabajo tiene como objetivo aprender a configurar una red para obtener conexiones de un extremo a otro mediante los comandos correspondientes y la conexión adecuada entre cada uno de los dispositivos con los que cuenta esta topología, la cual fue desarrollada en el programa de Cisco Packet Tracer gracias a la interfaz que se encuentra en este programa se puede ejecutar y desarrollar dicha topología para poner a pruebas nuestros conocimientos adquiridos a lo largo del curso, ya sea realizando conexiones Ethernet, habilitando puestos auxiliares, asignando IP, creando Vlan entre otras, con el fin de poder dar solución a lo requerido en la actividad.

A lo largo del diplomado CCNP se desarrollaron varias actividades colaborativas en las cuales se tenían diferentes tipos de ejercicios y laboratorios los cuales se desarrollaron en los diferentes entonos como de aprendizaje como lo son Cisco Packet Tracer, GNS3 o Smartlab con el fin de aprender y retroalimentar nuestros conocimientos respecto a las redes, simulando las programaciones e incluso programando equipos reales como es en el caso de Smartlab.

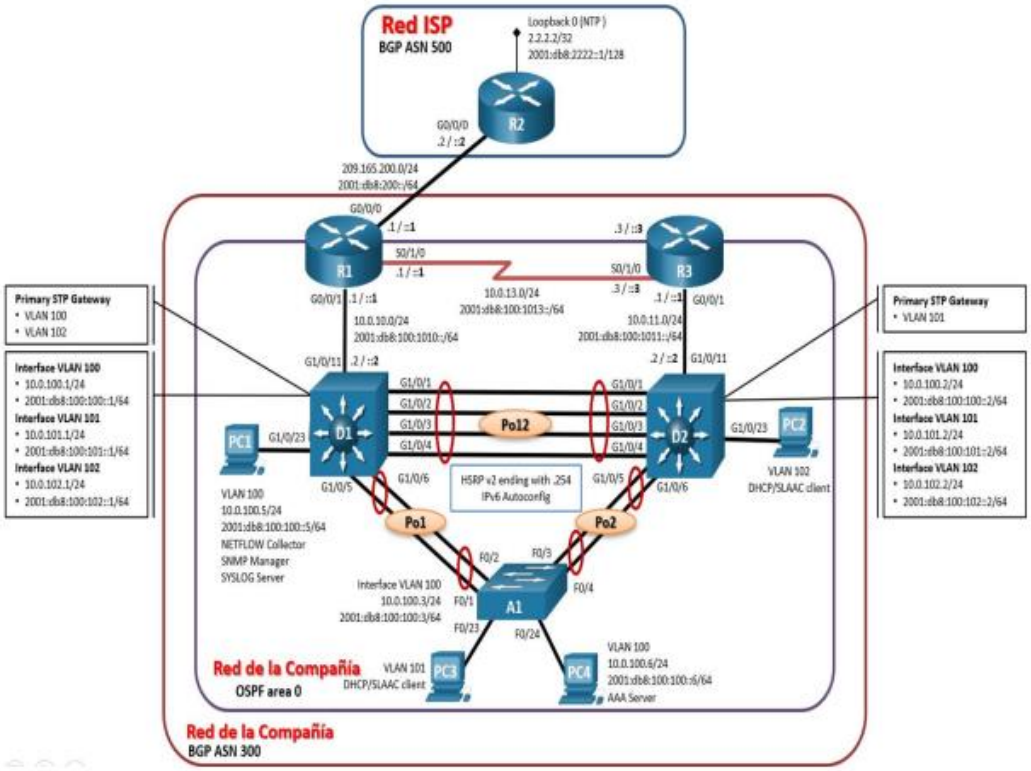
Otro tipo de actividad implementado en el diplomado CCNP es el que se maneja en la plataforma de Cisco Netacad la cual es una plataforma interactiva en la que podemos investigas y retroalimentar nuestros conocimiento así como la presentación de evaluaciones con el fin de evaluar los conocimientos adquiridos a los largo del diplomado.

DESARROLLO

1. ESCENARIO 1

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

Figura 1. Escenario 1



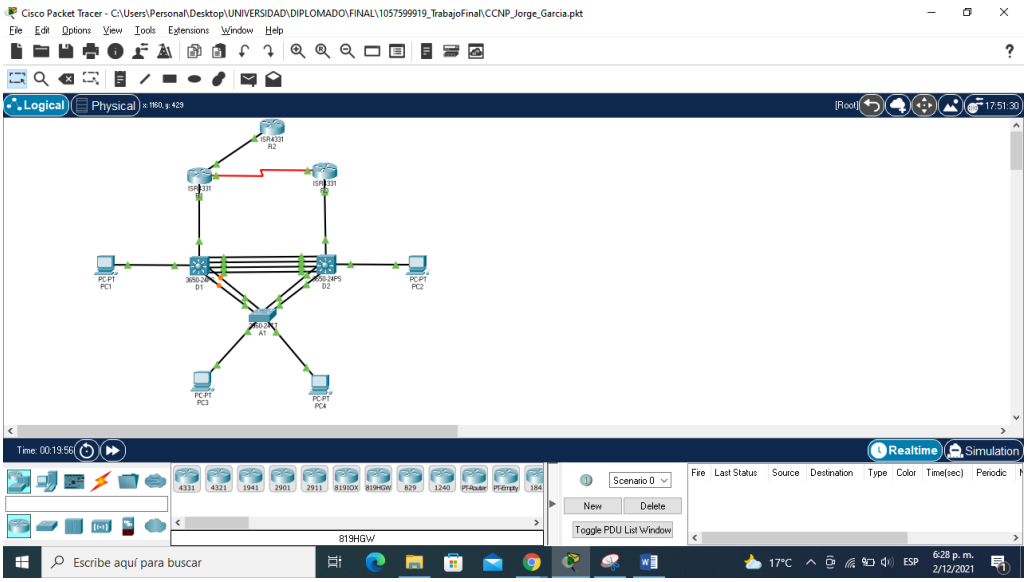
Se puede observar la topología general del ejercicio a desarrollar en el podemos observar (3) routers, (3) Switch y (4) computadores todos con el objetivo de establecer una conexión entre cada uno de los elementos.

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

Paso 1: Cablear la red como se muestra en la topología. Conecte los dispositivos como se muestra en el diagrama de topologia y conecte los cables según sea necesario.

Figura 2. Simulación de escenario 1



Se realizan las conexiones correspondientes en cada uno de los puertos indicados basandonos en la topologia de la figura 1, y usando los elementos adecuados suministrados por Cisco.

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>enable                                   // Ingreso a modo privilegiado
Router#config terminal                          // Ingreso a modo de configuración
Router(config)#hostname R1                      // Asigno nombre al Router
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                // Asignación de tiempo de espera
R1(config-line)#logging synchronous             // Asignación de registro sincrónico
R1(config-line)#exit                            // Salir
R1(config)#interface g0/0/0                     //  Ingresa a la interfaz para configurar
R1(config-if)#ip address 209.165.200.225 255.255.255.224        //Dirección y mascara
R1(config-if)#ipv6 address fe80::1:1 link-local                 //Asigna el Router
```

```
R1(config-if)#ipv6 address 2001:db8:200::1/64                    //Asigna IPV6 del Router
R1(config-if)#no shutdown                                        //Inicia la interfaz
R1(config-if)#exit                                               //Salir
R1(config-if)#interface g0/0/1                          //Ingresa a la interfaz para configurar
R1(config-if)#ip address 10.0.10.1 255.255.255.0                 //Dirección y  mascara
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64               //Asigna IPV6 del Router
R1(config-if)#no shutdown                                        //Inicia la interfaz
R1(config-if)#exit                                               // Salir
R1(config)#interface s0/1/0
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
```

Figura 3. Implementación del código comandos básicos R1

```
03:05:39: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on Serial0/1/0 from LOADING to FULL,
Loading Done

 R1, ENCOR Skills Assessment, Scenario 1

R1>enable
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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 g0/0/0
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 g0/0/1
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 s0/1/0
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
R1(config)#
```

Se configura el Router 1, con los comandos básicos como nombre, mensaje de alerta, tiempo de espera, direcciones IP con mascara, IPV6 entre otros comandos para iniciar a establecer las comunicaciones entre cada uno de los dispositivos, de igual manera se configura el Router 2.

Router 2

```
Router>enable                          // Ingreso a modo privilegiado
Router#config terminal                 // Ingreso a modo de configuración
Router(config)#hostname R2             // Asigno nombre al Router
```

```
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          // Asignación de tiempo de espera
R2(config-line)#logging synchronous       // Asignación de registro sincrónico
R2(config-line)#exit                      // Salir
R2(config)#interface g0/0/0               //Ingresa a la interfaz para configurarla interfaz
R2(config-if)#ip address 209.165.200.226 255.255.255.224   //Dirección y mascara
R2(config-if)#ipv6 address fe80::2:1 link-local            // Asigna el Router
R2(config-if)#ipv6 address 2001:db8:200::2/64              // Asigna IPV6 del Router
R2(config-if)#no shutdown                                  // Inicia la interfaz
R2(config-if)#exit                                         // Salir
R2(config-if)#interface Loopback 0                         // Ingresa a la interfaz para configurar
R2(config-if)#ip address 2.2.2.2 255.255.255.255           // Dirección y  mascara
R2(config-if)#ipv6 address fe80::2:3 link-local            // Asigna el Router
R2(config-if)#ipv6 address 2001:db8:2222::1/128            // Asigna IPV6 del Router
R2(config-if)#no shutdown                                  // Inicia la interfaz
R2(config-if)#exit                                         // Salir
R2(config)#
```

Router 3

```
Router>enable                                              // Ingreso a modo privilegiado
Router#config terminal                                     // Ingreso a modo de
configuración
Router(config)#hostname R3                                 // Asigno nombre al Router
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                           // Asignación de tiempo de espera
R3(config-line)#logging synchronous                        // Asignación de registro sincrónico
R3(config-line)#exit                                       // Salir
R3(config)#interface g0/0/1                  // Ingresa a la interfaz para configurarla interfaz
R3(config-if)#ip address 10.0.11.1 255.255.255.0           // Dirección y mascara
R3(config-if)#ipv6 address fe80::3:2 link-local            // Asigna el Router
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64         // Asigna IPV6 del Router
R3(config-if)#no shutdown                                  // Inicia la interfaz
R3(config-if)#exit                                         // Salir
R3(config-if)#interface s0/1/0                             // Ingresa a la interfaz para configurar
R3(config-if)#ip address 10.0.13.3 255.255.255.0           // Dirección y  mascara
R3(config-if)#ipv6 address fe80::3:3 link-local            // Asigna el Router
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64         // Asigna IPV6 del Router
R3(config-if)#no shutdown                                  // Inicia la interfaz
R3(config-if)#exit                                         // Salir
R3(config)
```

Switch D1

```
Switch>enabel                                   // Acceder al modo privilegiado
Switch#config terminal                          // Accede a configuraciones
Switch(config)#hostname D1                      // Asigna nombre
D1(config)#ip routing                           // Accede IP
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skill Assessment, scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0                // Asignación de tiempo//
D1(config-line)#logging synchronous             // Asignación de registro sincrónico//
D1(config-line)#exit                            // Salir//
D1(config)#vlan 100                             // Registro de vlan
D1(config-vlan)#name management                 // Nombre de Vlna
D1(config-vlan)#exit                            // Salir
D1(config)#vlan 101                             // Registro de Vlan
D1(config-vlan)#name userGroupA                 // Nombre de Vlan
D1(config-vlan)#exit                            // Salir
D1(config)#vlan 102                             // Registro de Vlan
D1(config-vlan)#name userGroupB                 // Nombre de Vlan
D1(config-vlan)#exit                            // Salir
D1(config)#vlan 999                             // Registro de Vlan
D1(config-vlan)#name NATIVE                     // Nombre de Vlan
D1(config-vlan)#exit                            // Salir
D1(config)#interface g1/0/11                    // Ingreso a la interfaz para configurar
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0        // Asigna dirección y mascara
D1(config-if)#ipv6 address fe80::d1:1 link-local        // Asigna D1
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64      // Asigna IPv6 del switch
D1(config-if)#no shutdown                               // Inicia la interfaz
D1(config-if)#exit                                      // Salir
D1(config)#interface vlan 100                           // Ingresa a la interfaz de la Vlan
D1(config-if)#ip address 10.0.100.1 255.255.255.0       // Agrega dirección IP con mascar
D1(config-if)#ipv6 address fe80::d1:2 link-local        // Asigna D1
D1(config-if)#ipv6 address 2001:db8:100:100::1/64       // Asigna IPv6 del switch
D1(config-if)#no shutdown                               //  Inicia la interfaz
D1(config-if)#exit                                      // Salir
D1(config)#interface vlan 101                           // Ingresa a la interfaz de la Vlan
D1(config-if)#ip address 10.0.101.1 255.255.255.0       // Agrega dirección IP con mascar
D1(config-if)#ipv6 address fe80::d1:3 link-local        // Asigna D1
D1(config-if)#ipv6 address 2001:db8:100:101::1/64       // Asigna IPv6 del switch
D1(config-if)#no shutdown                               // Inicia la interfaz
D1(config-if)#exit                                      // Salir
D1(config)#interface vlan 102                           // Ingresa a la interfaz de la Vlan
D1(config-if)#ip address 10.0.102.1 255.255.255.0       // Agrega dirección IP con mascar
D1(config-if)#ipv6 address fe80::d1:4 link-local        // Asigna D1
D1(config-if)#ipv6 address 2001:db8:100:102::1/64       // Asigna IPv6 del Switch
D1(config-if)#no shutdown                               // Inicia la interfaz
D1(config-if)#exit                                      // Salir
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                                          //Salir
D1(config)#interface range g1/0/1-10, g1/0/12-24, g1/1/1-4    //Rangos de salidas
D1(config)#shutdown                                           // Inicia interfaz
D1(config)#exit                                               // Salir
```

Switch D2

```
Switch>enabel                                  // Acceder al modo privilegiado
Switch#config terminal                         // Accede a configuraciones
Switch(config)#hostname D2                     // Asigna nombre
D2(config)#ip routing                          // Accede IP
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skill Assessment, scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0               // Asignación de tiempo
D2(config-line)#logging synchronous            //Asignación de registro sincrónico
D2(config-line)#exit                           // Salir
D2(config)#vlan 100                            // Registro de vlan
D2(config-vlan)#name management                // Nombre de Vlna
D2(config-vlan)#exit                           // Salir
D2(config)#vlan 101                            // Registro de Vlan
D2(config-vlan)#name userGroupA                // Nombre de Vlan
D2(config-vlan)#exit                           // Salir
D2(config)#vlan 102                            // Registro de Vlan
D2(config-vlan)#name userGroupB                // Nombre de Vlan
D2(config-vlan)#exit                           // Salir
D2(config)#vlan 999                            // Registro de Vlan
D2(config-vlan)#name NATIVE                    // Nombre de Vlan
D2(config-vlan)#exit                           // Salir
D2(config)#interface g1/0/11                   // Ingreso a la interfaz para configurar
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0          // Asigna dirección y mascara
D2(config-if)#ipv6 address fe80::d1:1 link-loca            // Asigna D2
D2(config-if)#ipv6 address 2001:db8:100:1011::2/6         // Asigna IPv6 del Switch
D2(config-if)#no shutdown                                  // Inicia la interfaz
D2(config-if)#exit                                         // Salir
D2(config)#interface vlan 100                              // Ingresa a la interfaz de la Vlan
D2(config-if)#ip address 10.0.100.2 255.255.255.0          // Agrega dirección IP con mascar
D2(config-if)#ipv6 address fe80::d2:2 link-local           // Asigna D2
D2(config-if)#ipv6 address 2001:db8:100:100::2/64          // Asigna IPv6 del Switch
D2(config-if)#no shutdown                                  // Inicia la interfaz
D2(config-if)#exit                                         // Salir
D2(config)#interface vlan 101                              // Ingresa a la interfaz de la Vlan
D2(config-if)#ip address 10.0.101.2 255.255.255.           // Agrega dirección IP con mascar
D2(config-if)#ipv6 address fe80::d2:3 link-local           // Asigna D2
D2(config-if)#ipv6 address 2001:db8:100:101::2/64          // Asigna IPv6 del Switch
```

```
D2(config-if)#no shutdown                                   // Inicia la interfaz
D2(config-if)#exit                                          // Salir
D2(config)#interface vlan 102                               // Ingresa a la interfaz de la Vlan
D2(config-if)#ip address 10.0.102.2 255.255.255.0           // Agrega dirección IP con mascar
D2(config-if)#ipv6 address fe80::d2:4 link-local            // Asigna D2
D2(config-if)#ipv6 address 2001:db8:100:102::2/64           // Asigna IPv6 del Switch
D2(config-if)#no shutdown                                   // Inicia la interfaz
D2(config-if)#exit                                          // Salir
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            // Agrega dirección y mascara
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit                                        // Salir
D2(config)#ip dhcp pool VLAN-102                            // Agrega DHCP de Vlan
D2(dhcp-config)#network 10.0.102.0 255.255.255.0            // Agrega dirección y mascara
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit                                        // Salir
D2(config)#interface range g1/0/1-10, g1/0/12-24, g1/1/1-4  // Rangos de salidas
D2(config)#shutdown                                         // Inicia interfaz
D2(config)#exit                                             // Salir
```

Figura 4. Implementación código básico Switch

```
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skill 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
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/5 (1),
with Al FastEthernet0/3 (999).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/6 (1),
with Al FastEthernet0/3 (999).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/5 (1),
with Al FastEthernet0/4 (999).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/6 (1),
with Al FastEthernet0/4 (999).

D2(config-vlan)#
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 g1/0/11
D2(config-if)#
```

Se configura los Switch D1 y D2 con las configuraciones básicas como nombre, mensaje de alerta, IP, mascara entre otros, aunque en ellos también se implementa la creación de Vlan para establecer una conexión y una asignación de las mismas.

Switch A1

```
Switch>enabel                                    // Acceder al modo privilegiado
Switch#config terminal                           // Accede a configuraciones
Switch(config)#hostname A1                       // Asigna nombre
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skill Assessment, scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0                 // Asignación de tiempo
A1(config-line)#logging synchronous              // Asignación de registro sincrónico
A1(config-line)#exit                             // Salir
A1(config)#vlan 100                              // Registro de vlan
A1(config-vlan)#name management                  // Nombre de Vlna
A1(config-vlan)#exit                             // Salir
A1(config)#vlan 101                              // Registro de Vlan
A1(config-vlan)#name userGroupA                  // Nombre de Vlan
A1(config-vlan)#exit                             // Salir
A1(config)#vlan 102                              // Registro de Vlan
A1(config-vlan)#name userGroupB                  // Nombre de Vlan
A1(config-vlan)#exit                             // Salir
A1(config)#vlan 999                              // Registro de Vlan
A1(config-vlan)#name NATIVE                      // Nombre de Vlan
A1(config-if)#exit                               // Salir
A1(config)#interface vlan 100                    // Ingresa a la interfaz de la Vlan
A1(config-if)#ip address 10.0.100.3 255.255.255.0    // Agrega dirección IP con mascar
A1(config-if)#ipv6 address fe80::a1:1 link-local     // Asigna A1
A1(config-if)#ipv6 address 2001:db8:100:100::3/64    // Asigna IPv6 del Switch
A1(config-if)#no shutdown                        // Inicia la interfaz
A1(config-if)#exit                               // Salir
A1(config)#interface range  f0/5-22              // Rangos de salidas
A1(config)#shutdown                              // Inicia interfaz
A1(config)#exit                                  // Salir
```

Figura 5. Implementación código básico A1

```
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
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3 (999),
with D2 GigabitEthernet1/0/5 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (999),
with D2 GigabitEthernet1/0/6 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/4 (999),
with D2 Port-channel2 (1).

A1(config-vlan)#
A1(config-vlan)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (999),
with D1 GigabitEthernet1/0/6 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (999),
with D1 GigabitEthernet1/0/5 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (999),
with D1 Port-channel1 (1).

A1(config-vlan)#name NATIVE
A1(config-vlan)#
```

Al igual que cada uno de los elementos ya configurados en la topología, se realiza la configuración del Switch A1 el cual al igual se le implementa comandos básicos de configuración y se registra en el la Vlan para establecer las conexiones.

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

R1#copy running-config startup-config

R2#copy running-config startup-config

R3#copy running-config startup-config

D1#copy running-config startup-config

D2#copy running-config startup-config

A1#copy running-config startup-config

Este comando se ejecuta en todos los dispositivos con el propósito que la configuración en ejecución es la configuración actual en el funcionamiento que se está ejecutando en la memoria RAM.

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.

Figura 6. Configuración de direccionamiento PC1

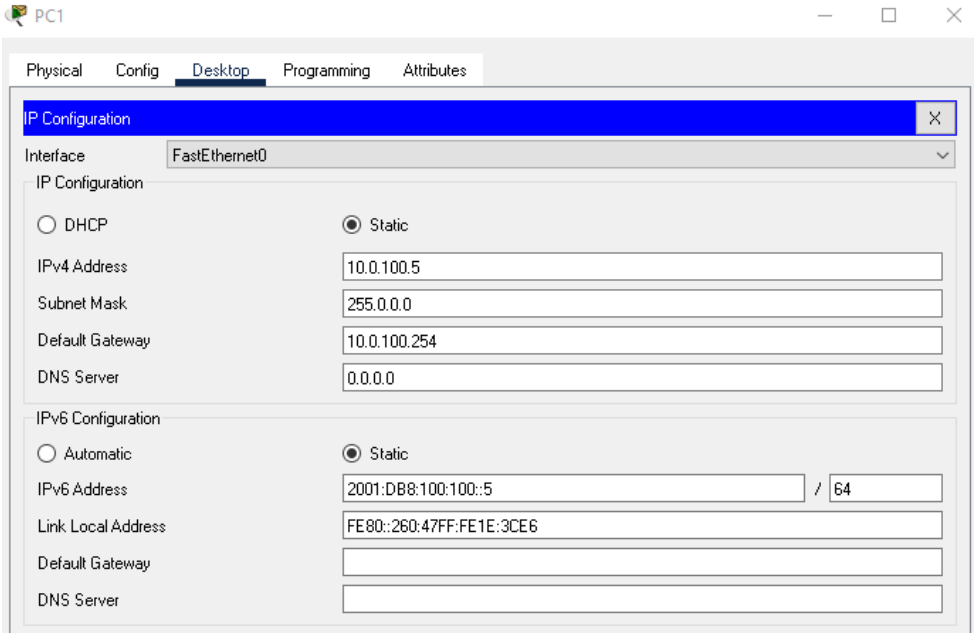
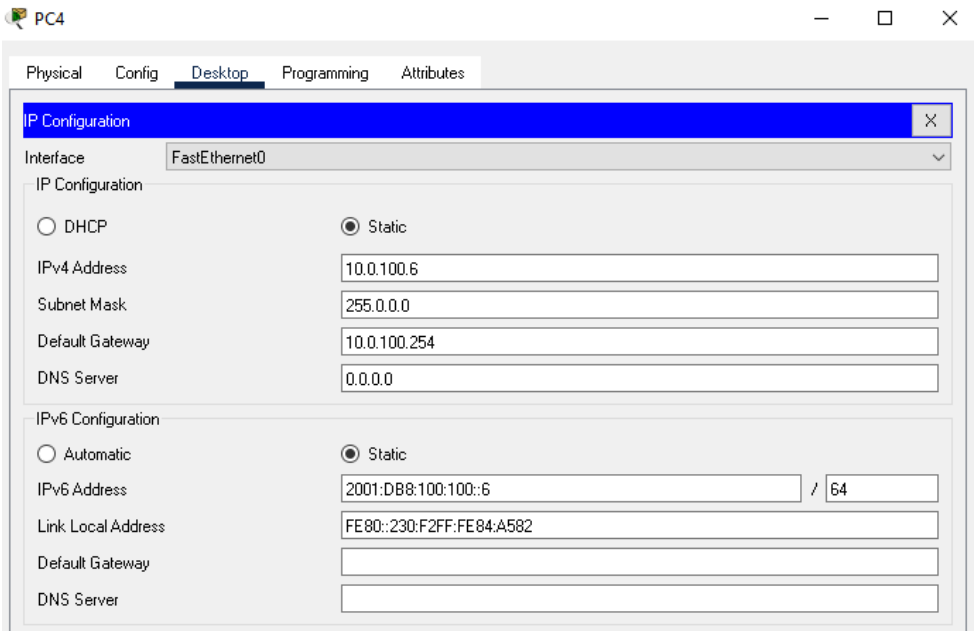


Figura 7. Configuración de direccionamiento PC4



Se configura la PC1 y PC4 ingresando en cada una de ellas a la IP Configuration para asignar la dirección de la puerta del enlace predeterminada.

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 deben poder comunicarse. PC2 y PC3 deben recibirdireccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tabla 2. Paso 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 nativaen los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en casode 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 seconectan 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

Los siguientes comandos utilizados en cada uno de los elementos implementados para el desarrollo del paso 2 son.

Switch D1

```
interface range g1/0/1-4                    // Establece un rango en la interfaz
switchport mode trunk                       // Activa el modo trunk
switchport trunk native vlan 999            // Activa la Vlan native
channel-group 12 mode active                // Implementa el Ethernet y el channel
no shutdown                                 // Inicia la interfaz
exit                                        // salir
interface range g1/0/5-6                    // Establece un rango en la interfaz
switchport mode trunk                       // Activa el modo trunk
switchport trunk native vlan 999            // Activa la Vlan native
channel-group 1 mode active                 // Implementa el Ethernet y el channel
no shutdown                                 // Inicia la interfaz
exit                                        // Salir
spanning-tree mode rapid-pvst               // Habilita el protocolo spanning-tree
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
interface g1/0/23                           // Establece la conexión de la interfaz
switchport mode Access                      //Habilita el protocolo de acceso
switchport access vlan 100                  // Accede a la vlan
spanning-tree portfast
no shutdown                                 // Inicia la interfaz
exit                                        // Salir
end                                         // Finalizar
```

Switch D2

```
interface range g1/0/1-4                    // Establece un rango en la interfaz
switchport mode trunk                       // Activa el modo trunk
switchport trunk native vlan 999            // Activa la Vlan native
channel-group 12 mode active                // Implementa el Ethernet y el channel
no shutdown                                 // Inicia la interfaz
exit                                        // salir
interface range g1/0/5-6                    // Establece un rango en la interfaz
switchport mode trunk                       // Activa el modo trunk
switchport trunk native vlan 999            // Activa la Vlan native
channel-group 2 mode active                 // Implementa el Ethernet y el channel
no shutdown                                 // Inicia la interfaz
exit                                        // Salir
spanning-tree mode rapid-pvst               // Habilita el protocolo spanning-tree
spanning-tree vlan 101 root primary
spanning-tree vlan 100, 102 root secondary
interface g1/0/23                           // Establece la conexión de la interfaz
switchport mode Access                      //Habilita el protocolo de acceso
switchport access vlan 102                  // Accede a la vlan
spanning-tree portfast
no shutdown                                 // Inicia la interfaz
exit                                        // Salir
end                                         // Finalizar
```

Switch A1

```
Spanning-tree mode rapid-rapid-pvst
interface range f0/1-2                      // Establece un rango en la interfaz
switchport mode trunk                       // Activa el modo trunk
switchport trunk native vlan 999            // Activa la Vlan native
channel-group 1 mode active                 // Implementa el Ethernet y el channel
no shutdown                                 // Inicia la interfaz
exit                                        // salir
interface range f0/3-4                      // Establece un rango en la interfaz
switchport mode trunk                       // Activa el modo trunk
switchport trunk native vlan 999            // Activa la Vlan native
channel-group 2 mode active                 // Implementa el Ethernet y el channel
no shutdown                                 // Inicia la interfaz
exit                                        // Salir
Interfce f0/23
Switchport mode Access                      // Habilita el protocolo spanning-tree
Switchport access vlan 101
spanning-tree portfast
no shutdown
exit
Interface f0/24
Switchport mode Access                      // Habilita el protocolo spanning-tree
Switchport access vlan 100
spanning-tree portfast
No shutdown                                 // Inicia la interfaz
Exit                                        // Salir
End                                         // Finalizar
```

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 y D2, D1 y A1 y D2 y A1.

Verificamos los comando ingresados anteriormente Emitiendo el comando **show interfaces trunk** en D1 y la salida debe aparecer como se muestra a continuación. Con ello se verifique las tareas 2.1, 2.2 y 2.5 en el Switch D1.

```
D1# show interface trunk

Port      Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      999
Po12        on           802.1q         trunking      999

Port      Vlans allowed on trunk
Po1         1-4094
Po12        1-4094
```

2.2 En todos los switches cambie la VLAN nativaen los enlaces troncales.

```
Port      Vlans allowed and active in management domain
Po1         1,100-102,999
Po12        1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po1         1,100-102,999
Po12        1,100-102,999
```

Se puede apreciar que con la implementación del código expuesto en el inicio podemos usar la VLAN 999 como la VLAN nativa.

2.3 En todos los switches habilite el protocoloRapid Spanning-Tree (RSTP)

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).

Para comprobar el desarrollo ejecutamos en D1 y D2 el comando **show run | include spanning-tree**, con ello Verificamos las tareas 2.3 y 2.4 en el Switch D1.

```
D1 # show run | incluir árbol de expansión
modo de árbol de expansión rapid-pvst
extensión del árbol de expansión id del sistema
spanning-tree vlan 100,102 prioridad 24576
árbol de expansión vlan 101 prioridad 28672
Portfast árbol de expansión


D2# show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 28672
```

spanning-tree vlan 101 priority 24576
spanning-tree portfast

Figura 8. Comprobación de Spanning-tree

```
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
 spanning-tree portfast
```

Se utiliza el comando Rapid Spanning Tree (RSPT) y se Configura 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 EtherChannelsLACP como se muestra en el diagrama de topología.

Se ingresa el comando **show interfaces trunk** en D2, para verificar la tarea 2.5 en el Switch D2.

D2# show interfaces trunk

Port	Mode	Encapsulation	Status	Native vlan
Po2	on	802.1q	trunking	999
Po12	on	802.1q	trunking	999

Port	Vlans allowed on trunk
Po2	1-4094
Po12	1-4094

Port	Vlans allowed and active in management domain
Po2	1,100-102,999
Po12	1,100-102,999

Port	Vlans in spanning tree forwarding state and not pruned
Po2	1,100-102,999
Po12	1,100-102,999

Utilizamos los diferentes números de canales

2.6 En todos los conmutadores, configure los puertos de acceso del host que se conecten a PC1, PC2, PC3 y PC4.

Ingresando el comando **show run interface f0 / 23** y show run interface f0 / 24 en A1 y D2, podemos visualizar la configuración realizada y Verificar la tarea 2.6 en el Switch A1 y en D2.

A1# show run interface f0/23
Building configuration...

Current configuration : 115 bytes

```
interface FastEthernet0/23
switchport access vlan 101
switchport mode Access
spanning-tree portfast edge
end

A1# show run interface f0/24
Building configuration...

Current configuration : 115 bytes
interface FastEthernet0/24
switchport access vlan 100
switchport mode Access
spanning-tree portfast edge
end


D2# show run interface g1/0/23
Building configuration...

Current configuration : 115 bytes

interface GigabitEthernet1/0/23
switchport access vlan 102
switchport mode Access
spanning-tree portfast
```

Se configura 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, para ellos se habilita DHCP en cada uno de los PC ingresando a configuraciones de IP.

2.8 Se realizan ping con los elementos PC1, PC2, PC3, PC4.

Figura 9. Ping PC1 a D1, D2, PC4

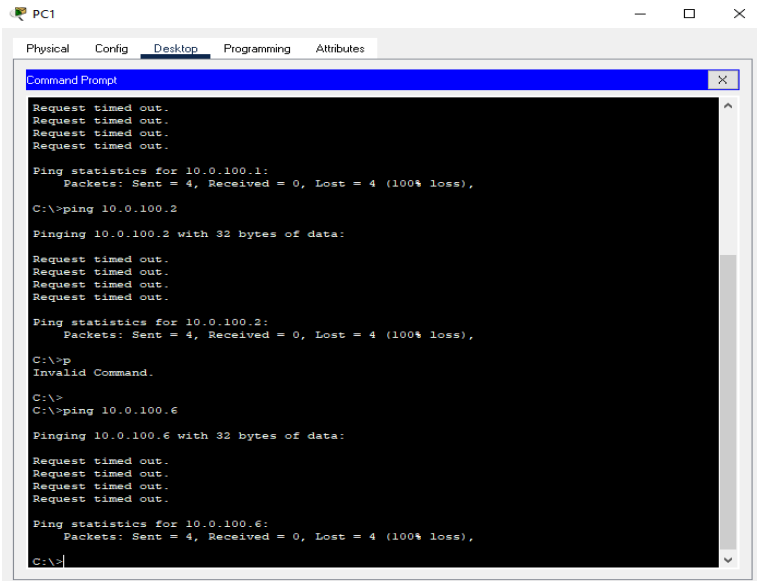


Figura 10. Ping PC2 a D1, D2

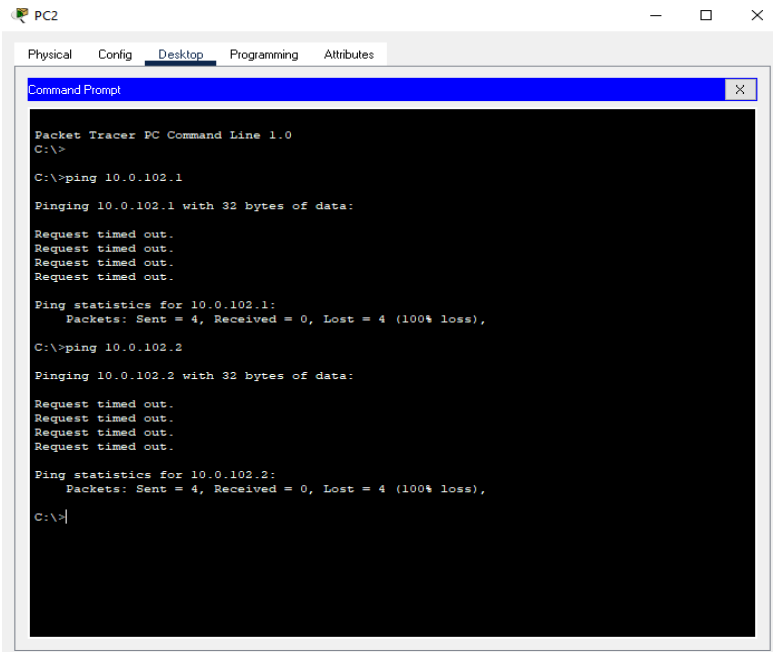


Figura 11. Ping PC3 a D1, D2

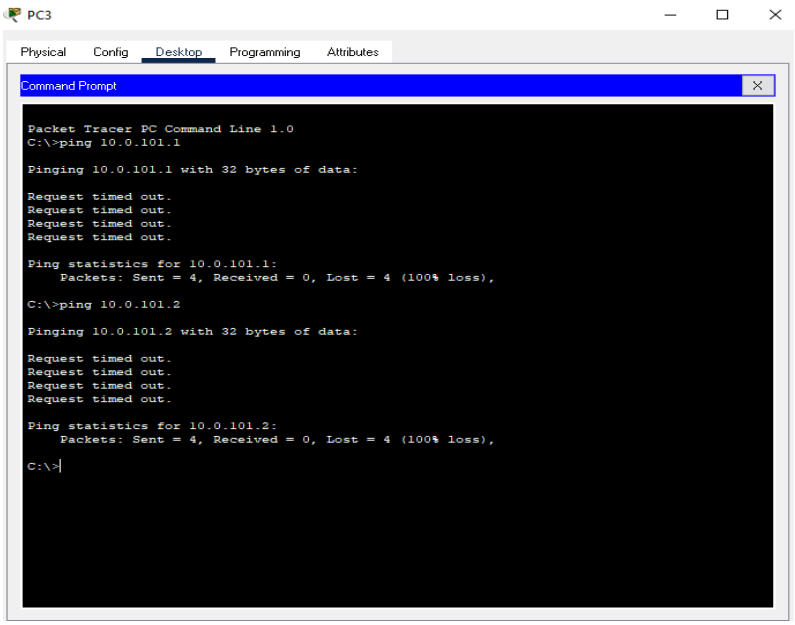
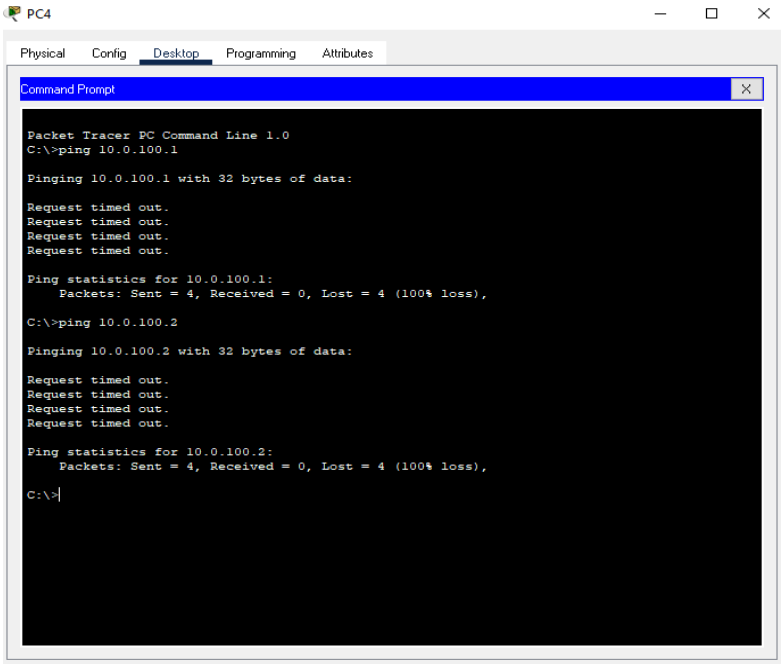


Figura 12. Ping PC4 a D1, D2, PC4



Los ping se ejecutan con el fin de comprobar la conexión que existe entre los dispositivos de la topología y por verificar el funcionamiento mediante el código digitado cada uno de ellos.

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 ladirección HSRP que se habilitará en la Parte 4.
Las tareas de configuración son las siguientes:

Tabla 3. Paso 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 redesdirectamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que laruta 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 redesdirectamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que laruta 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

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-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 interfazNull 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.

Para el desarrollo del paso 3 se implementa los siguientes comandos en cada uno de los dispositivos como los son los Router y los Switch.

Router R1

```
router ospf 4                                   // Habilita el proceso ospf
router-id 0.0.4.1
Network 10.0.10.0 0.0.0.255 area 0              // Se configura el área ospf en área 0
Network 10.0.13.0 0.0.0.255 area 0              // Se configura el área ospf en área 0
Default-information originate
exit                                            // Salir
ipv6 router ospf 6
```

```
router-id 0.0.6.1
Default-information originate                    // Origina la información predeterminada
exit                                             // Salir
Interface g0/0/1                                 // Ingresa a la interfaz
ipv6 ospf 6 area 0
exit                                             // Salir
Interface s0/1/0                                 // Ingresa a la interfaz
ipv6 ospf 6 area 0                               // Se configura el área
exit                                             // Salir
ip route 10.0.0.0 255.0.0.0 null0                // Configura las rutas estáticas a la interfaz
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
No neighbor 2001:db8:200::2 activate
Network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
No neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
Network 2001:db8:100::/48
exit-address-family
```

Router R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0              // Configura la ruta estática
ipv6 route ::/0 loopback 0
router bgp 500                                   // Habilita el proceso BGP
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4                              // Habilita la acción del vecino
neighbor 209.165.200.225 activate                // Activa las interfaces
No neighbor 2001:db8:200::1 activate
Network 2.2.2.2 mask 255.255.255.255
Network 0.0.0.0
exit-address-family                              // Salir
address-family ipv6                              // Habilita la acción del vecino
No neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
Network 2001:db8:2222::/128
Network ::/0
exit-address-family
```

Router R3

```
router ospf 4                                    // Ingresa al modo ospf
router-id 0.0.4.3
```

```
Network 10.0.11.0 0.0.0.255 area 0          // Se configura el área ospf en área 0
Network 10.0.13.0 0.0.0.255 area 0          // Se configura el área ospf en área 0
exit                                        // Salir
ipv6 router ospf 6                          // ingresa a la configuración ospf
router-id 0.0.6.3
exit                                        // Salir
Interface g0/0/1                            // Ingresa a la interfaz
ipv6 ospf 6 area 0                          //configura ospf
exit                                        // Salir
Interface s0/1/0                            // Ingresa a la interfaz
ipv6 ospf 6 ar                              // Configura ospf
exit                                        // Salir
end                                         // Finalizar
```

Switch D1

```
Router ospf 4                               // Ingresa al modo ospf
Router-id 0.0.4.131                         // Se configura el área ospf en área 0
Network 10.0.100.0 0.0.0.255 area 0
Network 10.0.101.0 0.0.0.255 area 0
Network 10.0.102.0 0.0.0.255 area 0
Network 10.0.10.0 0.0.0.255 area 0
Passive-interface default                   // Asigna la interfaz predeterminada
No passive-interface g1/0/11                // Deshabilita la interfaz
exit                                        // Salir
ipv6 router ospf 6
router-id 0.0.6.131
Passive-interface default
No passive-interface g1/0/11
Exit
Interface g1/0/11                           // ingresa a la interfaz
ipv6 ospf 6 area 0                          // Accedemos al área
exit                                        // Salir
Interface vlan 100
ipv6 ospf 6 area 0
exit
Interface vlan 101                          // Ingresa a las vlan 101
ipv6 ospf 6 area 0                          // Accedemos al área
exit                                        // Salir
Interface vlan 102                          // Ingresa a las vlan 102
ipv6 ospf 6 area 0                          // Accedemos al área
exit                                        // Salir
end                                         // Finalizar
```

Switch D2

```
router ospf 4                               // Ingresa al modo ospf
router-id 0.0.4.132                         // Se configura el área ospf en área 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
```

```
network 10.0.11.0 0.0.0.255 area 0
Passive-interface default                    // Asigna la interfaz predeterminada
No passive-interface g1/0/11                 // Deshabilita la interfaz
exit                                         // Salir
ipv6 router ospf 6
router-id 0.0.6.132
Passive-interface default
No passive-interface g1/0/11
Exit
Interface g1/0/11                            // ingresa a la interfaz
ipv6 ospf 6 area 0                           // Accedemos al área
exit                                         // Salir
Interface vlan 100                           // Ingresa a las vlan 100
ipv6 ospf 6 area 0                           // Accedemos al área
exit                                         // Salir
Interface vlan 101                           // Ingresa a las vlan 101
ipv6 ospf 6 area 0                           // Accedemos al área
exit                                         // Salir
Interface vlan 102                           // Ingresa a las vlan 102
ipv6 ospf 6 area 0                           // Accedemos al área
exit                                         // Salir
end                                          // Finalizares
```

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

Para verificar que los comandos ingresados son los correctos en el 3.1, se debe digitar el siguiente comando **show run | section ^ router ospf** en cada uno de los dispositivos.

```
R1 # show run | section ^ router ospf
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
```

Figura 13. Código de verificación punto 3.1

```
R1#show run | section ^router ospf
router ospf 4
 router-id 0.0.4.1
 log-adjacency-changes
 network 10.0.10.0 0.0.0.255 area 0
 network 10.0.13.0 0.0.0.255 area 0
 default-information originate
R1#
```

```
R3 # show run | section ^ router ospf
router ospf 4
router-id 0.0.4.3
```

```
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
```

```
D1 # show run | section ^ router ospf
router ospf 4
router-id 0.0.4.131
passive-interface default
no passive-interface GigabitEthernet1/0/11
network 10.0.10.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
```

```
D2 # show run | section ^ router ospf
router ospf 4
router-id 0.0.4.132
passive-interface default
no passive-interface GigabitEthernet1/0/11
network 10.0.11.0 0.0.0.255 area 0
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
```

Utilizamos OSPF Process ID 4 y asigne los siguientes routers R1, R3, D1 y D2. Donde anuncie todas las redes directamente conectadas / VLANs en Area 0.

Se deshabilito las publicaciones OSPFv2 y todas las interfaces excepto G1/0/11 de D1 y en todas las interfaces excepto G1/0/11 de D2

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

El desarrollo del paso 3.2 lo podemos verificar mediante la aplicación del siguiente código **show run | section ^ router ipv6** y **show ipv6 ospf interface** brief al igual que el anterior ejercicio se debe realizar en cada uno de los dispositivos.

R1

```
R1# show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
R1# show ipv6 ospf interface brief
```

Interface	PID	Area	Intf ID	Cost	State	Nbrs F/C
Se0/1/0	6	0	7	49	P2P	1/1
Gi0/0/1	6	0	6	1	DR	1/1

R3

```
R3# show run | section ^ipv6 router
ipv6 router ospf 6
```

```
router-id 0.0.6.3
R3# show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/1/0      6     0               7          50    P2P   1/1
Gi0/0/1      6     0               6          1     DR    1/1
```

D1

```
D1# show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface GigabitEthernet1/0/11
D1# show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Vl102        6     0               41         1     DR    0/0
Vl101        6     0               40         1     DR    0/0
Vl100        6     0               39         1     DR    0/0
Gi1/0/11     6     0               38         1     BDR   1/1
```

D2

```
D2# show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface GigabitEthernet1/0/11
D2# show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Vl102        6     0               41         1     DR    0/0
Vl101        6     0               40         1     DR    0/0
Vl100        6     0               39         1     DR    0/0
Gi1/0/11     6     0               38         1     BDR   1/1
```

Figura 14. Código de verificación punto 3.2

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.132
 log-adjacency-changes
 passive-interface default
D2#show ipv6 ospf interface brief
```

Configure dos rutas estáticas predeterminadas através de la interfaz Loopback 0, una ruta estática predeterminada IPv4 y una ruta estática predeterminada IPv6.

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

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

3.3 En R2 en la “Red ISP”, configure MP- BGP, al configurar dos rutas estáticas predeterminadas a través de la interfaz Loopback 0, cada una predeterminada IPV4 y IPV6, Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

R2 # show run | sección enrutador bgp
R2 # show run | incluir ruta

R2# show run | section router bgp
router bgp 500
bgp router-id 2.2.2.2
bgp log-neighbor-changes
neighbor 2001:DB8:200::1 remote-as 300
neighbor 209.165.200.225 remote-as 300

address-family ipv4
network 0.0.0.0
network 2.2.2.2 mask 255.255.255.255
no neighbor 2001:DB8:200::1 activate
neighbor 209.165.200.225 activate
exit-address-family

address-family ipv6
network ::/0
network 2001:DB8:2222::/128
neighbor 2001:DB8:200::1 activate
exit-address-family

R2# show run | include route
router bgp 500
bgp route-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0

3.4 En este paso únicamente se revisa el Router 1 para verificar que se haya realizado bien la configuración se digita el código **show run | sección bgp** utilizado en el paso 3.1.

R1 # show run | section bgp
router bgp 300
bgp router-id 1.1.1.1
bgp log-neighbor-changes
neighbor 2001:DB8:200::2 remote-as 500
neighbor 209.165.200.226 remote-as 500

address-family ipv4
network 10.0.0.0
no neighbor 2001:DB8:200::2 activate
neighbor 209.165.200.226 activate
exit-address-family

address-family ipv6
network 2001:DB8:100::/48

neighbor 2001:DB8:200::2 activate
exit-address-family

Y con el comando **show ipv6 Route** Revisamos toda la configuración realizada que se encuentre correcta.

Figura 15. Código de verificación punto 3.4

```
R1#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:DB8:100:1010::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:100:1010::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
O   2001:DB8:100:1011::/64 [110/65]
     via FE80::3:3, Serial0/1/0
C   2001:DB8:100:1013::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:100:1013::1/128 [0/0]
     via Serial0/1/0, receive
C   2001:DB8:200::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:200::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Se debe realizar el mismo paso con el comando anterior en cada uno de los dispositivos Routers para revisar y verificar que todo este correcto.

R3# show ip route ospf | begin Gateway
Gateway of last resort is 10.0.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 01:56:36, Serial0/1/0
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O   10.0.10.0/24 [110/51] via 10.0.13.1, 01:56:47, Serial0/1/0
O   10.0.100.0/24 [110/2] via 10.0.11.2, 01:30:02, GigabitEthernet0/0/1
O   10.0.101.0/24 [110/2] via 10.0.11.2, 01:30:02, GigabitEthernet0/0/1
O   10.0.102.0/24 [110/2] via 10.0.11.2, 01:30:02, GigabitEthernet0/0/1

Figura 16. Código de verificación R3

```
R3#show ipv6 route ospf
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2001:DB8:100:1013::/64 [110/128]
     via FE80::1:3, Serial0/1/0
```

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

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

Las tareas de configuración son las siguientes:

Tabla 4. Paso 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 R1G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sintiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
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 R3G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sintiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 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 estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

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

4.4	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, suprioridad 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. 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.

La configuración implementada en cada uno de los elementos de la actividad para el desarrollo del paso 4 se encuentra a continuación.

Switch D1

```
ip sla 4
icmp-echo 10.0.10.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
ip sla 41chedule 4 life forever start-time now
ip sla 41chedule 6 life-forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
end
```

Switch D2

```
ip sla 4
icmp-echo 10.0.11.1
frequency
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency
exit
ip sla 42chedule 4 life forever start-time now
ip sla 42chedule 6 life forever start-time now
track 4 ip sla 4
Delay down 10 up 15
exit
track 6 ip sla 6
Delay down 10 up 15
exit
Interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
Interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
Interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
end
```

En el desarrollo de paso 4 se configuro específicamente los switches D1 y D2 en los cuales se crean dos IP SLAs las cuales son necesarias para probar la accesibilidad de la interfaz R1 en D1 y R3 en D2, usando la SLA número 4 para la IPV4 y la numero 6 para la IPV6, por último los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

4.1 Verificamos que la programación haya sido correcto mediante el siguiente código **show run | section ip sla** en el Switch D1.

```
D1# show run | section ip sla
track 4 ip sla 4
delay down 10 up 15
track 6 ip sla 6
delay down 10 up 15
ip sla 4
icmp-echo 10.0.10.1
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:1010::1
frequency 5
ip sla schedule 6 life forever start-time now
```

4.2 En el podemos revisar que la parte 4.1 hasta la parte 4.3 quedo realizada y verificamos que las configuraciones de las IP a los grupos haya sido correcta, se visualiza este proceso para el Switch 2.

```
D2# show run | section ip sla
track 4 ip sla 4
delay down 10 up 15
track 6 ip sla 6
delay down 10 up 15
ip sla 4
icmp-echo 10.0.11.1
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:1011::1
frequency 5
ip sla schedule 6 life forever start-time now
```

4.3 y 4.4 En D1 y D2 se configura HSRPv2, D1 es el router primario para las VLANs 100 y 102; por lotanto, su prioridad también se cambiará a 150, Configuramos HSRP versión 2 asignando una configuración Ipv4 HSRP grupo **104** para la VLAN 100 y con esto:

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 decremento en 60.

Después configure Ipv4 HSRP grupo **114** para la VLAN 101, Asignando la dirección IP virtual **10.0.101.254**, Habilitando la preferencia (preemption), rastree el objeto 4 para disminuir en 60.

Configure Ipv4 HSRP grupo **124** para la VLAN 102:
Asignando 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.

Figura 17. Revisión parte 4.1, 4.2, 4.3 y 4.4

```
D1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl100       104  150 P Active   local           unknown         10.0.100.254
Vl1         106  150 P Active   local           unknown         FE80::5:73FF:FEA0:106
Vl101       114  100 P Active   local           unknown         10.0.101.254
Vl1         116  100 P Active   local           unknown         FE80::5:73FF:FEA0:116
Vl102       124  150 P Active   local           unknown         10.0.102.254
Vl1         126  150 P Active   local           unknown         FE80::5:73FF:FEA0:126
D1#
```

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. Paso 5

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmode encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando elalgoritmo 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 es10.0.100.6. • Puertos UDP del servidor RADIUS son1812 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 servidoresRADIUS • De lo contrario, utilice la base de datoslocal.
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**.

Desarrollamos el paso 5 mediante la aplicación del siguiente código:

```
Enable algorithm-type SCRYPT secret cisco12345cisco
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

All devices except R2:
aaa new-model
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
exit
aaa authentication login default group radius local
end
```

Con esto se planea crear una contraseña y lograr encriptar para proteger el equipo y que nadie lo configure teniendo acceso a él y poniendo en riesgo el equipo y el trabajo desarrollado por cada uno de nosotros, a continuación podemos observar la aplicación del código a uno de los Switch de la topología.

Figura 18. Aplicación de comando de seguridad

```
D1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)#
```

5.1 y 5.2 En todos los dispositivos debemos proteger el EXEC privilegiado usando el algoritmode encripción SCRYPT. Creando de igual forma un usuario en todos los dispositivos, revisamos que la configuración haya sido la adecuada mediante el siguiente código.

```
R1# show run | include secret
enable secret 9 $9$0C3pnVdgrnhnY9$uzGA.WZfcLg5IhuyJu22mIf.YyZ/83VgqbO3rXBDuwo
username sadmin privilege 15 secret 9 $9$XCO4pzqbRT.3EP$ymouLOQI5/o0FO kY DtA1z
tejFra67MnkJJ5Y3bhyQe6
```

Con este comando pudimos verificar que efectivamente la contraseña aparece encriptado.

5.3 En todos los dispositivos (excepto R2),habilite AAA.
5.4 En todos los dispositivos (excepto R2),configure las especificaciones del servidor RADIUS.
5.5 En todos los dispositivos (excepto R2),configure la lista de métodos de autenticación AAA.

Se desarrolla los puntos 5.3, 5.4, 5.5 mediante la habilitación de AAA según las especificaciones del servidor RADIUS en el cual debemos asignar una dirección IP del servidor RADIUS10.0.100.6 y los puertos UDP del servidor RADIUS son1812 y 1813, a la cual se le asigna la contraseña: **$trongPass**, los pasos realizados anteriormente se comprueban mediante el siguiente código, estos comandos se realizan en todos los dispositivos menos en el Router R2.

```
R1# show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$XCO4pzqbRT.3EP$ymouLOQI5/o0FOkYDtA1zt
ejFra67MnkJJ5Y3bhyQe6
```

radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
aaa new-model
aaa session-id common

5.6 Verifique el servicio AAA en todos losdispositivos (Excepto R2).

Cierre e inicie sesión en todos los dispositivos

(Excepto R2) con el usuario: **raduser** y lacontraseña: **upass123**.

Figura 19. Verificación de la contraseña

```
D1>ENABLE
Password:
Password:
D1#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/5 (1),
with A1 FastEthernet0/1 (999).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/6 (1),
with A1 FastEthernet0/1 (999).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/5 (1),
with A1 FastEthernet0/2 (999).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/6 (1),
with A1 FastEthernet0/2 (999).
config
D1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#
```

Al cerrar la sesión se ingresa nuevamente a uno de los dispositivos configurados y se verifica el funcionamiento de la clave.

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. Paso 6

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configureel reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTPmaestro.	Configurar R2 como NTP maestro en el nivel deestrato 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 losdispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 enel nivel WARNING.
6.5	Configure SNMPv2c en todos losdispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura(Read-Only). • Limite el acceso SNMP a la dirección IP de laPC1. • Configure el valor de contacto SNMP con sunombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *trapsconfig* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

En el desarrollo de este punto se debe implementar el siguiente código en cada uno de los dispositivos.

Router R2

```
ntp master 3
end
```

Router R1

```
ntp server 2.2.2.2
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server enable traps ospf
end
```

Router R3

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end
```

Switch D1

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
```

```
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end
```

Switch D2

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf
end
```

Switch A1

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end
```

6.1 y 6.2 En todos los dispositivos, configure el reloj local a la hora UTC actual y Configure R2 como maestro NTP.

Configuramos el reloj local a la hora UTC actual y R2 como maestro NTP en el nivel de estrato 3, Verificando la hora UTC actual y publicando el comando show clock en R2; la salida debe indicar la hora UTC actual correcta. Esto verifica la tarea 6.1 en R2.

Emitir la ejecución del espectáculo | incluir el comando ntp en R2; la salida debe aparecer como se muestra a continuación. Esto verifica la tarea 6.2.

R2# show run | include ntp

Figura 20. Código de verificación punto 6.1 y 6.2

```
R2#show run | include ntp
ntp master 3
```

6.3 Configure NTP en R1, R3, D1, D2 y A1.

Implementando el comando **show ntp status | include stratum** en R1; la salida debe aparecer como se muestra a continuación. Esto verifica la tarea 6.3 en el enrutador R1 y **show ntp status | include stratum** en R3, D1, D2, y A1 para verificar la tarea 6.3 en estos dispositivos.

R1# show ntp status | include stratum
Clock is synchronized, stratum 4, reference is 2.2.2.2

A1# show ntp status | include stratum
Clock is synchronized, stratum 5, reference is 10.0.10.1

6.4 Configure Syslog en todos losdispositivos excepto R2

Al configurar Syslogs deben enviarse a la PC1 en 10.0.100.5 enel nivel WARNING. El desarrollo de eta tarea lo obtenemos con el código **show run | include logging** y nos debe imprimir el siguiente mesaje.

R1# show run | include logging
logging trap warnings
logging host 10.0.100.5
 logging synchronous

6.5 Configure SNMPv2c en todos losdispositivos excepto R2

Emitiendo el comando **show ip access-list SNMP-NMS** a cualquier dispositivo excepto R2 obtenemos la siguiente salida.

D1# show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
  10 permit 10.0.100.5

Figura 21. Código de Verificación punto 6.4

```
R1#show run | include logging
logging 10.0.100.5
 logging synchronous
R1#
```

Para verificar el último paso utilizamos los siguientes comando en cada uno de los dispositivos excepto en el Router 2, se ejecuta solo en el Switch D1 para probar la implementación del código.

D1# show ip access-list SNMP-NMS
D1# show run | include snmp

Figura 22. Código de Verificación punto 6.5

```
D1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
    permit host 10.0.100.5

D1#show run | include snmp
```

Con la implementación de estos códigos a cada uno de los dispositivos que componen la actividad se pretende configurar un reloj local a la hora UTC actual, seguido a esto se pretende configurar un NPT en todos los dispositivos menos en R2, ya que se generó otro NPT, de igual forma se configura Syslog y SNMPv2c en todos los dispositivos menos en R2.

Por ultimo revisamos todos los dispositivos mediante el siguiente código.

R1# show run

R2# show run

R3# show run

D1# show run

D2# show run

A1# show run

R1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server enable traps bgp
snmp-server host 10.0.100.5 version 2c ENCORSA

R3# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit

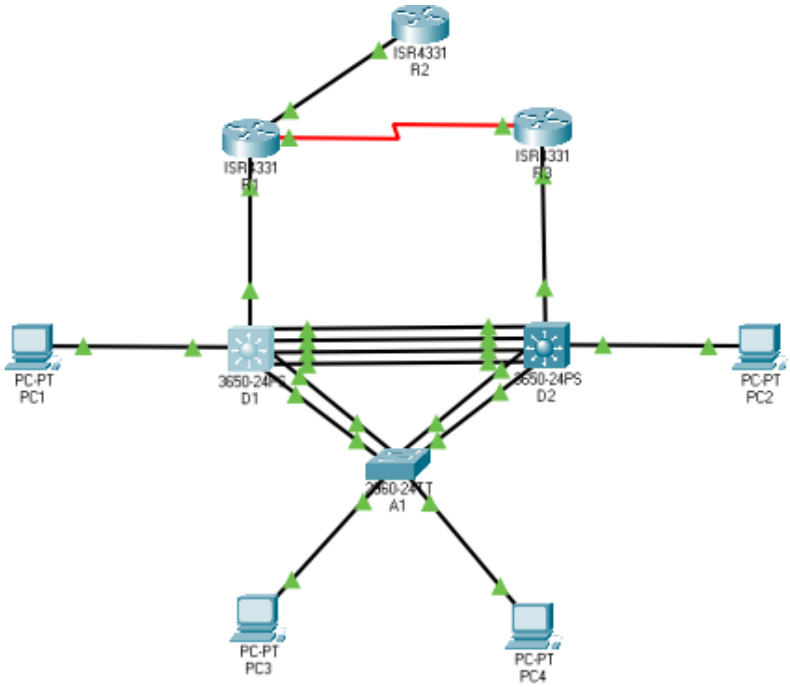
```
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA

D1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA

D2# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA

A1# show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
```

Figura 23. Topologia final programada



CONCLUSIONES

Al trabajar con el programa GNS3 es muy complejo debido a que se debe instalar una máquina virtual para poder simular los dispositivos con los que se va a trabajar, sin este tipo de máquina virtual no se puede desarrollar ningún proceso en el programa, para ellos se debe contar con espacio suficiente de RAM en nuestras computadores para que el programa cargue adecuadamente y poder trabajar con él ya que nos permite correr comandos que en otro tipo de programas no se podrían usar.

Cuando desarrollamos la topología de la actividad en el programa de Packet Tracer y extraemos los routers se debe tener en cuanta habilitar los puestos auxiliares con el fin de establecer todas las conexiones pertinentes, siempre que se vaya a conectar unos de estos módulos se debe apagar el equipo, conectarlo y volverlo a encender para que así no les arroje un error al momento de implementar esos puertos.

Al programar los diferentes Switch que cuenta la topología cada uno de ellos tenía sus respectivas Vlan, si queremos transportar datos a través de ellos se implementa una Vlan native la cual se encarga de transportar dichos datos a través del rango de puertos que se habilite y se verifica la conexión mediante los ping que realicemos entre las computadoras a las Switch.

Siempre que iniciemos una topología y debamos conectar algún tipo de puerto auxiliar o conector, se debe tener presente apagar el Router o el Switch ya que al no realizar este paso no arrojara un error siempre el programa y si queremos conectarlo con otro dispositivo seguirá presentando ese tipo de falla.

BIBLIOGRÁFIA

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