DIPLOMADO DE PRONFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JIMMY FRANCO GARCIA

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

DIPLOMADO DE PRONFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

JIMMY FRANCO GARCIA

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
BOGOTA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 29 de noviembre 2021

AGRADECIMIENTOS

Doy gracias a Dios por guiar mi camino y seguir creciendo profesionalmente a nivel de estudio, a mi familia por su apoyo en esta etapa de mi vida de la cual ya se está cumpliendo una meta más.

La universidad me dio la bienvenida y me brindo la oportunidad de continuar con mis estudios haciendo realidad uno de mis más grandes sueños agradezco inmensamente a los directivos, docentes de esta gran institución y a mis compañeros en general que con su compromiso y ética logramos culminar esta gran carrera.

CONTENIDO

LISTAS DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN: Se le conoce como redes de área local virtuales, es una interfaz que permite crear redes independientes lógicas dentro de una misma red física. El complemento de utilizar VLAN en un entorno, es validar o segmentar debidamente la red usando una subred de forma diferente. Se puede acceder o rechazar el tráfico entre las diferentes VLAN con un dispositivo como un router o switch.

ROUTER: Es un módulo electrónico que recibe y envía datos en redes informáticas, pueden intercalar funciones y conectarse a internet mejorando el acceso y creando redes de alta complejidad como lo son las empresariales o industriales mediante paquetes con diferentes tipos de datos e interacciones con la web.

TOPOLOGIA: Tiene relación de una red física con la diversidad de elementos, componentes, conectores y diferentes representaciones de cables con nodos de interfaz para sus respectivas conexiones, por medio de una topología fluyen los datos de una red, a esto se le puede aplicar diferentes capas y protocolos de comunicación identificando que puestos están conectados y quienes tiene acceso a la red.

PACKET TRACER y GNS3: Son dos softwares de redes con simuladores que se descargan directamente de la red de cisco, en ellos se diseñan topologías de redes para el desarrollo de ejercicios en línea con máquinas virtuales, a su vez se realiza programación con códigos los cuales se utilizan para su respectiva simulación, llegando a ofrecer un muy buen aprendizaje para la vida real.

ETHERNET: Tecnología usada en la conexión de redes cableadas de área local (LAN) permitiendo que dispositivos se comuniquen entre sí por medio de protocolos de comunicación, hay diferentes tipos de redes ethernet entre los más comunes se encuentran, fast ethernet, conmutador ethernet y gigabit ethernet.

RESUMEN

En el desarrollo del ejercicio práctico prueba de habilidades se evidenciará el desarrollo de los escenarios propuestos realizados mediante los softwares de cisco (PACKET TRACER y GNS3), se aplicarán los conocimientos obtenidos a lo largo del diplomado CCNP de una forma concisa implementando una topología con varios elementos para configurar, introduciendo códigos de programación e investigando el uso de cada uno de ellos y su aplicativo en al ejecución de las interfaces, a su vez insertando comandos para verificación del paso a paso de la actividad, para implementar el escenario se utilizara investigación, bibliografías y todo aquello que aporte en conjunto el aprendizaje práctico de la prueba, se plasmara el código editándolo en el documento con su respectiva explicación, las fallas en el momento de realizar la prueba nos enseñaran a solucionar problemas de configuración aplicando métodos comunes como métodos de alta complejidad, la importancia de un buen enrrutamiento desde el principio de la topología hará que sea posible cumplir en la totalidad con la prueba de habilidades.

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

ABSTRACT

In the development of the practical exercise skills test, the development of the proposed scenarios carried out using cisco software (PACKET TRACER and GNS3) will be evidenced, the knowledge obtained throughout the CCNP diploma will be applied in a concise way by implementing a topology with various elements to configure, introducing programming codes and investigating the use of each one of them and their application in the execution of the interfaces, in turn inserting commands to verify the step by step of the activity, to implement the scenario research will be used, bibliographies and everything that jointly contributes to the practical learning of the test, the code will be captured by editing it in the document with its respective explanation, the failures at the time of the test will teach us to solve configuration problems by applying common methods such as test methods. high complexity, the importance of good routing from the beginning ipio of the topology will make it possible to fully comply with the skills test.

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

INTRODUCCION

En la presente actividad a desarrollar se realizará el ejercicio propuesto el cual consta de implementar y diseñar una red con topología CCNP ENCOR v8 habilidades prácticas, con un ejemplo base de la actividad se implementará la programación de elementos de comunicación computacional en estos se incluirán router, switch, computadores y conexiones por medio de cables utilizando puertos de comunicación estándar que se ajusten a la topología requerida con interfaces apropiadas para su enrutamiento entre los diferentes equipos.

Los conocimientos aprendidos durante el desarrollo de este diplomado y de otros cursos de cisco se aplicarán en ejercicio a implementar ya que será de gran importancia para poder programar e intercomunicar los dispositivos de la topología a realizar, se utilizará un software de cisco Packet Tracer o GNS3 para su respectiva programación y ejecución de los escenarios a intervenir.

El curso de este plan de estudio genera al estudiante habilidades necesarias para conformar, actuar y solventar problemas de redes cubriendo una variedad conjunta de aprendizaje con las prácticas y laboratorios realizados durante las diferentes fases implementadas en el cronograma del diplomado, la investigación será pieza clave en la adaptación de la topología ya que requiere de bastantes códigos los cuales el estudiante debe interpretar para incluirlos en la configuración del sistema

ESCENARIO 1

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

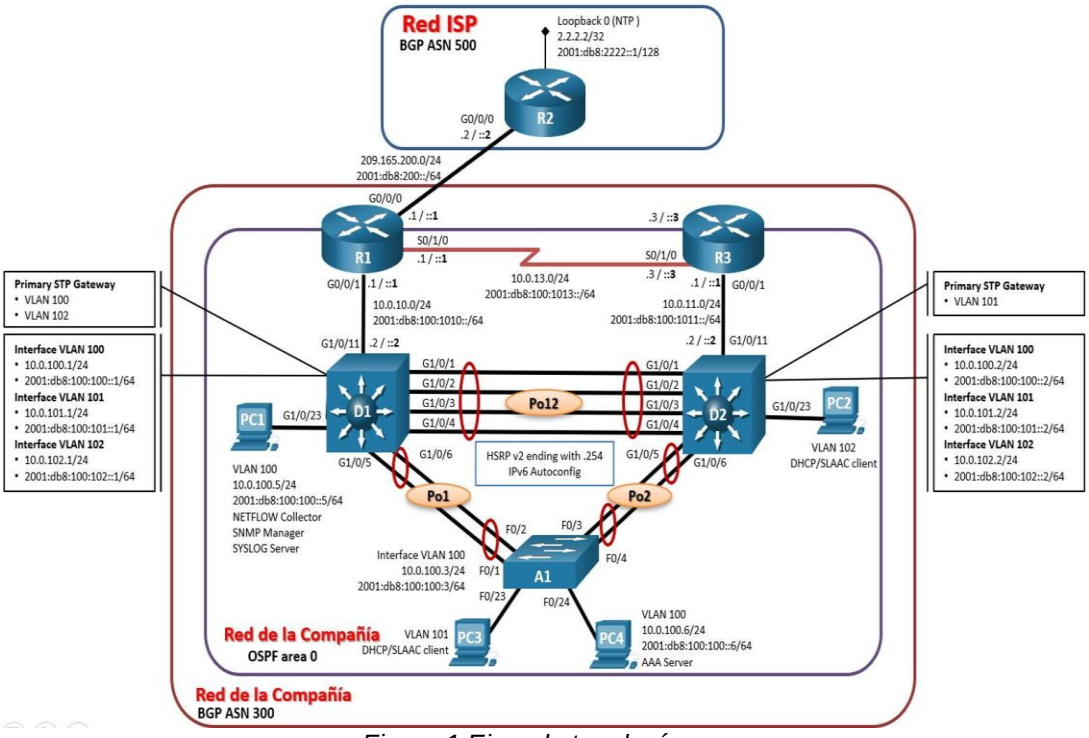

Figura 1 Ejemplo topología

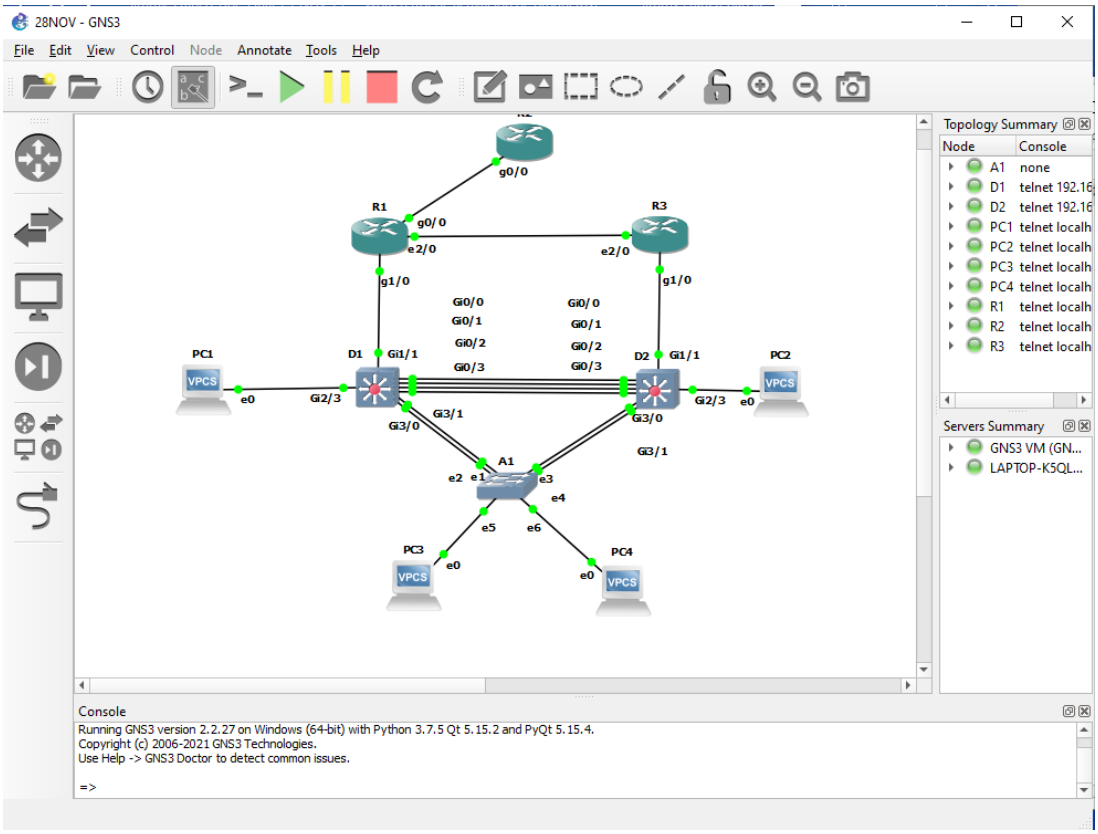

Figura 2 Diseño topología GNS3

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.

Tabla 1. 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 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:

Se adjunta código y pantallazos con veracidad del código.

Router R1

hostname R1
// Asignación nombre router
ipv6 unicast-routing
// Habilita ipv6 en el router
no ip domain lookup
// Desactiva la traducción del nombre
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
//Mensaje de aviso
line con 0
exec-timeout 0 0
// Tiempo de espera inactivo
logging synchronous
// Evita que mensajes desplacen comandos
Verificación código ingresado para R1-R2-R3
R1# Show ip interface brief

exit
// Salida configuración
interface g0/0/0
// Interfaz del gigabit
ip address 209.165.200.225 255.255.255.224
// Asignación dirección y mascara sub red
ipv6 address fe80::1:1 link-local
// Reconoce el router
ipv6 address 2001:db8:200::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz

EL comando visualiza interfaces del router.

```
R1(config)#exit
R1#show
*Oct 11 19:38:44.816: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip interf
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Prot
ocol
Ethernet0/0            10.0.10.1       YES manual up                    up

Ethernet0/1            209.165.200.225 YES manual up                    up

Ethernet0/2            unassigned      YES NVRAM  administratively down down

Ethernet0/3            unassigned      YES NVRAM  administratively down down

Ethernet1/0            unassigned      YES NVRAM  administratively down down

Ethernet1/1            unassigned      YES NVRAM  administratively down down

Ethernet1/2            unassigned      YES NVRAM  administratively down down

Ethernet1/3            unassigned      YES NVRAM  administratively down down

Serial2/0              10.0.13.1       YES manual up                    up
```

Figura 3 verificación R1

exit
// Salida configuración
interface g0/0/1
// Interfaz del gigabit
ip address 10.0.10.1 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::1:2 link-local
// Reconoce el router
ipv6 address 2001:db8:100:1010::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz

exit
// Salida configuración
interface s0/1/0 // Interfaz
ip address 10.0.13.1 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::1:3 link-local // Reconoce el router
ipv6 address 2001:db8:100:1013::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit// Salida configuración

Router R2

hostname R2
// *Asignación nombre*
ipv6 unicast-routing
// *Habilita ipv6 en el router*
no ip domain lookup
// *Desactiva la traducción del nombre a dirección*
banner motd # R2, ENCOR Skills Assessm
// *Mensaje de aviso*
line con 0
// Ingreso al modo de configuración
exec-timeout 0 0
// Tiempo de espera inactivo
logging synchronous
// Evita que mensajes desplacen comandos
exit
// Salida configuración
interface g0/0/0
// Interfaz
ip address 209.165.200.226 255.255.255.224
// Asignación dirección y mascara sub red
ipv6 address fe80::2:1 link-local
// Reconoce el router
ipv6 address 2001:db8:200::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface Loopback 0
// Prueba y administra el dispositivo
ip address 2.2.2.2 255.255.255.255
// Asignación dirección y mascara sub red
ipv6 address fe80::2:3 link-local
// Reconoce el router
ipv6 address 2001:db8:2222::1/128
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración

Router R3

hostname R3
// Asignación nombre
ipv6 unicast-routing
// Habilita ipv6 en el router
no ip domain lookup
// Desactiva la traducción del nombre
banner motd # R3, ENCOR Skills Assessment // Mensaje de aviso
line con 0
// Ingreso al modo de configuración
exec-timeout 0 0
// Tiempo de espera inactivo
logging synchronous
// Evita que mensajes desplacen comandos
exit
// Salida configuración
interface g0/0/1
// Interfaz

```
ip address 10.0.11.1 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::3:2 link-local
// Reconoce el router
ipv6 address 2001:db8:100:1011::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface s0/1/0
// Interfaz
ip address 10.0.13.3 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::3:3 link-local
// Reconoce el router
ipv6 address 2001:db8:100:1010::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
```

Switch D1

```
hostname D1
// Asignación nombre
ip routing
// Redes conectadas
ipv6 unicast-routing
// Habilita ipv6 en el router
no ip domain lookup
// Desactiva la traducción del nombre a
dirección
banner motd # D1, ENCOR Skills
Assessment, Scenario 1 #
// Mensaje de aviso
line con 0
// Ingreso al modo de configuración
exec-timeout 0 0
// Tiempo de espera inactivo
logging synchronous
// Evita que mensajes desplacen comandos
exit
// Salida configuración
vlan 100
// Crea una red lógica
name Management
// Gestiona nombres
exit
// Salida configuración
vlan 101
// Crea una red lógica
name UserGroupA
// Nombre de usuario predeterminado
exit
// Salida configuración
vlan 102
// Crea una red lógica
name UserGroupB
// Nombre de usuario predeterminado
exit
// Salida configuración
vlan 999
// Crea una red lógica
name NATIVE
// Nombre vlan NATIVA
exit
// Salida configuración
interface g1/0/11
// Interfaz
no switchport
// Configuración de puerto
ip address 10.0.10.2 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::d1:1 link-local
// Reconoce el router
ipv6 address 2001:db8:100:1010::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface vlan 100
// Crea una red lógica
ip address 10.0.100.1 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::d1:2 link-local
// Reconoce el router
ipv6 address 2001:db8:100:100::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface vlan 101
// Crea una red lógica
```

```
ip address 10.0.101.1 255.255.255.0
// Asignación dirección
ipv6 address fe80::d1:3 link-local
// Reconoce el router
ipv6 address 2001:db8:100:101::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface vlan 102
// Crea una red lógica
ip address 10.0.102.1 255.255.255.0
// Asignación dirección
ipv6 address fe80::d1:4 link-local
// Reconoce el router
ipv6 address 2001:db8:100:102::1/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
ip dhcp excluded-address
10.0.101.1 10.0.101.109
// excluir direcciones especificas
ip dhcp excluded-address
10.0.101.141 10.0.101.254
// excluir direcciones especificas
ip dhcp excluded-address
10.0.102.1 10.0.102.109
// excluir direcciones especificas
ip dhcp excluded-address
10.0.102.141 10.0.102.254
// excluir direcciones especificas
ip dhcp pool VLAN-101
// Router en modo configuración
network 10.0.101.0 255.255.255.0
// Define interfaces del dispositivo
default-router 10.0.101.254
// Router predeterminado
exit
// Salida configuración
ip dhcp pool VLAN-102
// Router en modo configuración
network 10.0.102.0 255.255.255.0
// Define interfaces del dispositivo
default-router 10.0.102.254
// Router predeterminado
exit
// Salida configuración
interface range
g1/0/1-10, g1/0/12-24, g1/1/1-4
// Rango de interfaz
shutdown
// El ordenador se apaga directamente
exit
// Salida configuración
```

Switch D2

```
hostname D2
// Asignación nombre
ip routing
// Redes conectadas
ipv6 unicast-routing
// Habilita ipv6 en el router
no ip domain lookup
// No ip domain lookup
banner motd # D2, ENCOR
Skills Assessment, Scenario 1 #
// Mensaje de aviso
line con 0
// Ingreso al modo de configuración
exec-timeout 0 0
// Tiempo de espera inactivo
logging synchronous
exit
// Evita que mensajes desplacen comandos
exit
// Salida configuración
vlan 100
// Crea una red lógica dentro de una misma
red
name Management
// Gestiona nombres
exit
// Salida configuración
vlan 101
// Crea una red lógica dentro de una misma
red
name UserGroupA
// Nombre de usuario predeterminado

// Salida configuración
```

vlan 102
// Crea una red lógica
name UserGroupB
// Usuario predeterminado
exit

// Salida configuración
vlan 999
// Crea una red lógica
name NATIVE
// Nombre vlan NATIVA

```
!
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
!
ip dhcp pool VLAN-101
 network 10.0.101.0 255.255.255.0
 default-router 10.0.101.254
!
ip dhcp pool VLAN-102
 network 10.0.102.0 255.255.255.0
 default-router 10.0.102.254
!
!
```

Figura 4 Código funcionamiento para D1 yD2

Visualización en D1 y D2

#Show running-config

Observamos informacion direcciones e interfaz

#show vlan brief

Observamos puertos asignados con las VLAN

```
D1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
                                                Et3/1, Et3/2, Et3/3
100  Management                       active
101  UserGroupA                       active
102  UserGroupB                       active
999  NATIVE                           active
```

Figura 5 Puertos asignados D1

```
exit
// Salida configuración
interface g1/0/11
// Interfaz
no switchport
// Configuración de puerto
ip address 10.0.11.2 255.255.255.0
// Asignación dirección
ipv6 address fe80::d1:1 link-local
// Reconoce el router
ipv6 address 2001:db8:100:1011::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface vlan 100
// Crea una red lógica
ip address 10.0.100.2 255.255.255.0
// Asignación dirección
ipv6 address fe80::d2:2 link-local
// Reconoce el router
ipv6 address 2001:db8:100:100::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface vlan 101
// Crea una red lógica
ip address 10.0.101.2 255.255.255.0
// Asignación dirección
ipv6 address fe80::d2:3 link-local
// Reconoce el router
ipv6 address 2001:db8:100:101::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface vlan 102
// Crea una red lógica
ip address 10.0.102.2 255.255.255.0
// Asignación dirección
ipv6 address fe80::d2:4 link-local
// Reconoce el router
ipv6 address 2001:db8:100:102::2/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
ip dhcp excluded-address
10.0.101.1 10.0.101.209
// excluir direcciones especificas
ip dhcp excluded-address
10.0.101.241 10.0.101.254
// excluir direcciones especificas
ip dhcp excluded-address 1
0.0.102.1 10.0.102.209
// excluir direcciones especificas
ip dhcp excluded-address
10.0.102.241 10.0.102.254
// excluir direcciones especificas
ip dhcp pool VLAN-101
// Ingresa el router en modo configuración
network 10.0.101.0 255.255.255.0
// Define interfaces del dispositivo
default-router 10.0.101.254
// Router predeterminado
exit
// Salida configuración
ip dhcp pool VLAN-102
// Ingresa el router en modo configuración
network 10.0.102.0 255.255.255.0
// Define interfaces del dispositivo
default-router 10.0.102.254
// Router predeterminado
exit
// Salida configuración
interface range
g1/0/1-10, g1/0/12-24, g1/1/1-4
// Rango de interfaz
shutdown
// El ordenador se apaga directamente
exit
// Salida configuración
```

A1

hostname A1
// Asignación nombre
no ip domain lookup
// Desactiva la traducción del nombre a dirección
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
// Mensaje de aviso
line con 0
// Ingreso al modo de configuración
exec-timeout 0 0
// Tiempo de espera inactivo

```
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 ip address 10.0.100.3 255.255.255.0
 ipv6 address FE80::A1:1 link-local
 ipv6 address 2001:DB8:100:100::3/64
```

Figura 6 Configuración direccionamiento A1

Código insertado

#show running-config

```
logging synchronous
// Evita que mensajes desplacen comandos
exit
// Salida configuración
vlan 100
// Crea una red lógica dentro de una misma
red
name Management
// Gestiona nombres
exit
// Salida configuración
vlan 101
// Crea una red lógica dentro de una misma
red
name UserGroupA
// Nombre de usuario predeterminado
exit
// Salida configuración
vlan 102
// Crea una red lógica dentro de una misma
red
name UserGroupB
// Nombre de usuario predeterminado
exit
// Salida configuración
vlan 999
// Crea una red lógica dentro de una misma
red
name NATIVE
// Nombre vlan NATIVA
exit
// Salida configuración
interface vlan 100
// Crea una red lógica dentro de una misma
red
ip address 10.0.100.3 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::a1:1 link-local
// Reconoce el router
ipv6 address 2001:db8:100:100::3/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface range f0/5-22
// Rango de interfaz
shutdown
// El ordenador se apaga rápida y
directamente
exit
// Salida configuración
```

```
logging synchronous
//Evita que mensajes desplacen comandos
exit
// Salida configuración
vlan 100
// Crea una red lógica dentro de una misma
red
name Management
// Gestiona nombres
exit
// Salida configuración
vlan 101
// Crea una red lógica dentro de una misma
red
name UserGroupA
// Nombre de usuario predeterminado
exit
// Salida configuración
vlan 102
// Crea una red lógica dentro de una misma
red
name UserGroupB
// Nombre de usuario predeterminado
exit
// Salida configuración
vlan 999
// Crea una red lógica dentro de una misma
red
name NATIVE
// Nombre vlan NATIVA
exit
// Salida configuración
interface vlan 100
// Crea una red lógica dentro de una misma
red
ip address 10.0.100.3 255.255.255.0
// Asignación dirección y mascara sub red
ipv6 address fe80::a1:1 link-local
// Reconoce el router
ipv6 address 2001:db8:100:100::3/64
// Dirección unicast global de interfaz
no shutdown
// Habilita interfaz
exit
// Salida configuración
interface range f0/5-22
// Rango de interfaz
shutdown
// El ordenador se apaga rápida y
directamente
exit
// Salida configuración
```

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

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

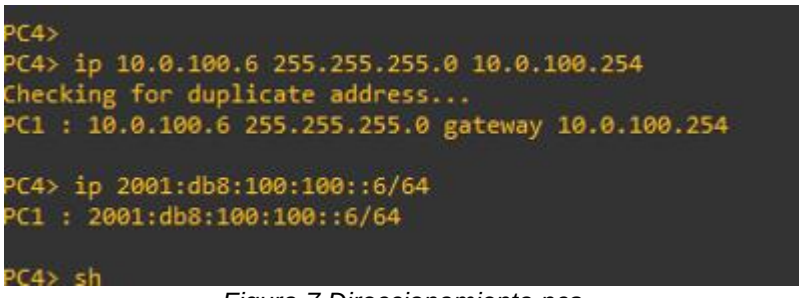

Figura 7 Direccionamiento pcs

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

Tabla 2. Soporte de host

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
Tarea#	**Tarea**	**Especificación**
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Verificación de la instrucción:

Insertamos el comando show interfaces trunk en D1; en la salida se obtiene como se muestra a continuación. Verificamos las tareas 2.1, 2.2 y 2.5 en el Switch D1.

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

protocolo IEEE 802.1q, nos permite la interfaz con el protocolo RSTP mejorando tiempo de enlace.

```
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
```

```
D1#
*Oct 11 22:35:39.753: %SYS-5-CONFIG_I: Configured from console by console
D1#show inter
D1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et1/1       on               802.1q         trunking      999
Et1/2       on               802.1q         trunking      999

Port        Vlans allowed on trunk
Et1/1       1-4094
Et1/2       1-4094

Port        Vlans allowed and active in management domain
Et1/1       1,100-102,999
Et1/2       1,100-102,999

Port        Vlans in spanning tree forwarding state and not pruned
Et1/1       1,100-102,999
Et1/2       1,100-102,999
```

Figura 8 Troncales D1

2.2 En todos los switches cambie la VLAN nativa en 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

Ejecutamos la prueba del problema incluimos el comando de árbol de expansión en D1; El desarrollo de salida aparece como se muestra a continuación. Verificamos las tareas 2.3 y 2.4 en el Switch D1.

2.3 y 2.4 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

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

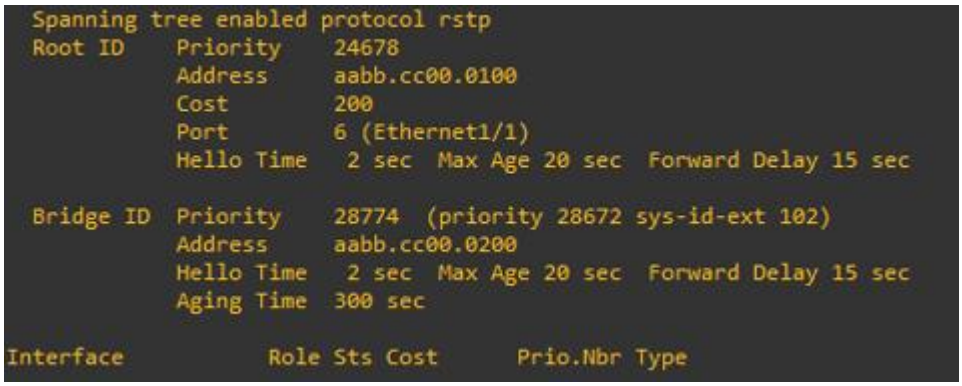

Figura 9 Ejecución de código spanning tree

Ejecutamos el desarrollo del problema incluimos el comando de árbol de expansión en D2; la salida aparece como se muestra a continuación. Verificamos las tareas 2.3 y 2.4 en el Switch D2.

```
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 portfas
```

Ejecutamos el comando show interfaces trunk en D2; el desarrollo de la salida aparece como se muestra a continuación. Verificamos la tarea 2.5 en el Switch D2.

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

```
D2# show interfaces trunk
Port        Mode Encapsulación 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
```

2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

Ejecutamos el comando show run interface g1 / 0/23 en D1; el desarrollo de la salida aparece como se muestra a continuación. Verificamos la tarea 2.6 en el Switch D1.

```
D1# show run interface g1/0/23
Building configuration...
Current configuration: 115 bytes
interface GigabitEthernet1/0/23

switchport access vlan 100
switchport mode access
spanning-tree portfast
end
```

Ejecutamos el comando show run interface g1 / 0/23 en D2; en la salida aparece como se muestra a continuación. Verificamos la tarea 2.6 en el Switch D2.

```
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
```

Ejecutamos los comandos show run interface f0 / 23 y show run interface f0 / 24 en A1; la salida aparece como se muestra a continuación. Verifique la tarea 2.6 en el Switch A1.

```
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

2.7 Verifique los servicios DHCP IPv4.

General
interface Ethernet (enp0s3)
Hardware Address 08:00:27:A6:1A:14
Driver e1000
Speed 1000 Mb/s
Security None

IPv4
IP Address 10.0.102.110
Broadcast Address 10.0.102.255
Subnet Mask 255.255.255.0
Default Route 10.0.102.254

General
interface Ethernet (enp0s3)
Hardware Address 08:00:27:AD:B6:ED
Driver e1000
Speed 1000 Mb/s
Security None

IPv4
IP Adress 10.0.102.110
Broadcast Address 10.0.102.255
Subnet Mask 255.255.255.0
Default Route 10.0.101.254

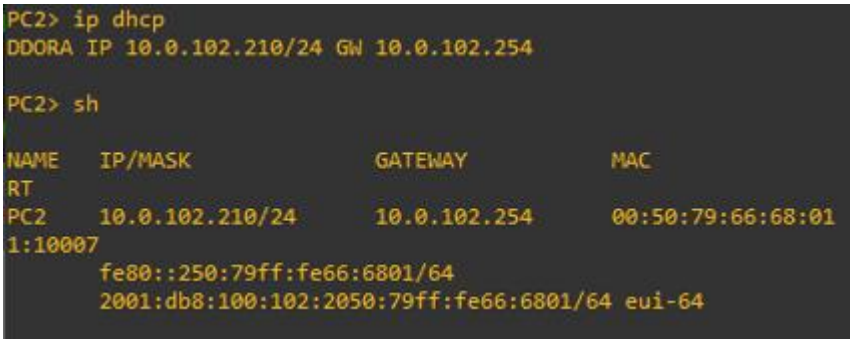

Figura 10 Servicios DHCP

2.8 Verifique la conectividad de la LAN local

```
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=2.177 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=2.508 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=2.773 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=2.557 ms
```

Figura 11 Ping IP 10.0.100.1

Parte 3: Configurar los protocolos de enrrutamiento

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.

Tabla 3. Protocolos de enrrutamiento

Tarea #	**Tarea**	**Especificación**
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-arena OSPFv2 en arena 0.	Use OSPF Process ID **4** y asigne los siguientes router- IDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2

		en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID **6** y asigne los siguientes router- IDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

Tarea#	Tarea	Especificación
3.3	En R2 en la “Red ISP”, configure MP-BGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MP-BGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

Verificación de la instrucción.

Ejecutamos el desarrollo del escenario sección ^ router ospf en R1, R3, D1 y D2; la salida aparece como se edita a continuación. Verificamos la actividad 3.1 en cada dispositivo.

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

```
R1# show run | section ^router ospf          // Ejecutamos el comando
router ospf 4                                 show run | section ^router ospf
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

R3# show run | section ^router ospf          // Configuramos OSPF v3 asignando 0.0.4.3
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          // Asignacion Ospf process ID, router ID
router ospf 4                                 0.0.4.131
router-id 0.0.4.131
passive-inte
rface 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          // Asignacion Ospf process ID, router ID
router ospf 4                                 0.0.4.132
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
```

Ejecutamos el desarrollo del escenario sección ^ enrutador ipv6 y observamos el resumen de la interfaz ipv6 ospf en R1, R3, D1 y D2; en salida aparece como se edita a continuación. Verificamos la actividad 3.2 en cada dispositivo.

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

```
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# 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# 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# 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
```

Ejecutamos el desarrollo del escenario sección bgp y show run incluimos la ruta en R2; la salida aparece como se edita a continuación. Verificamos la actividad 3.3.

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

```
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
```

Ejecutamos el desarrollo del escenario sección bgp en R1; la salida aparece como se edita a continuación. Verificamos la actividad 3.4.

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

```
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
```

Verificamos las tablas:

Escenario show ip route | incluir O | B en R1; la salida aparece como se edita a continuación. Verificamos que OSPF y BGP para IPv4 funcionen.

```
R1# show ip route | include O|B
Codes:L-local, C-connected, S-static, R-RIP, M-mobile, B- BGP
      D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF inter area
      N1-OSPF NSSA external type 1, N2-OSPF NSSA external    type 2
      E1-OSPF external type 1, E2-OSPF external type 2
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
B*    0.0.0.0/0 [20/0] via 209.165.200.2, 01:51:16
B     2.2.2.2 [20/0] via 209.165.200.2, 01:51:16
O     10.0.11.0/24 [110/50] via 10.0.13.3, 01:24:41, Serial0/1/0
O     10.0.100.0/24 [110/2] via 10.0.10.2, 01:49:44, GigabitEthernet0/0/1
O     10.0.101.0/24 [110/2] via 10.0.10.2, 01:49:44, GigabitEthernet0/0/1
O     10.0.102.0/24 [110/2] via 10.0.10.2, 01:49:44, GigabitEthernet0/0/1
```

Ejecutamos el comando show ipv6 route en el R1; aparece como se edita a continuación.

Verificamos que OSPFv3 para IPv6 funcione.

```
R1# show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes:C-Connected, L-Local, S-Static, U- er-user Static route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2-SIS L2, IA-ISIS interarea, IS-ISIS summary, D- EIGRP
      EX-EIGRP external, ND-ND Default, NDp-ND Prefix, DCE- Destination
      NDr-Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
      OE1-OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
      ON2 - OSPF NSSA ext 2, a - Application
B   ::/0 [20/0]
    via FE80::2:1, GigabitEthernet0/0/0
S   2001:DB8:100::/48 [1/0]
    via Null0, directly connected
O   2001:DB8:100:100::/64 [110/2]
    via FE80::D1:1, GigabitEthernet0/0/1
O   2001:DB8:100:101::/64 [110/2]
    via FE80::D1:1, GigabitEthernet0/0/1
O   2001:DB8:100:102::/64 [110/2]
    via FE80::D1:1, GigabitEthernet0/0/1
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 [110/50]
```

```
    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
```

Escenario show ip route ospf empieza el comando Gateway en R3; la salida, aparece.como se edita a continuación. Verificamos que OSPF para IPv4 funcione.

```
R3# show ip route ospf | begin Gateway
Gateway of last resort is 10.0.13.1 to network 0.0.0.0
0*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
0        10.0.10.0/24 [110/51] via 10.0.13.1, 01:56:47, Serial0/1/0
0        10.0.100.0/24 [110/2] via 10.0.11.2, 01:30:02, GigabitEthernet0/0/1
0        10.0.101.0/24 [110/2] via 10.0.11.2, 01:30:02, GigabitEthernet0/0/1
0        10.0.102.0/24 [110/2] via 10.0.11.2, 01:30:02, GigabitEthernet0/0/1
```

Ejecutamos el comando show ipv6 route ospf en R3; la salida aparece como se edita a continuación. Verificamos que OSPFv3 para IPv6 funcione.

```
R3# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, a - Application
OE2 ::/0 [110/1], tag 6
    via FE80::1:3, Serial0/1/0
0   2001:DB8:100:100::/64 [110/2]
    via FE80::D1:1, GigabitEthernet0/0/1
0   2001:DB8:100:101::/64 [110/2]
    via FE80::D1:1, GigabitEthernet0/0/1
0   2001:DB8:100:102::/64 [110/2]
    via FE80::D1:1, GigabitEthernet0/0/1
0   2001:DB8:100:1013::/64 [110/99]
    via FE80::1:3, Serial0/1/0
```

ESCENARIO 2

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

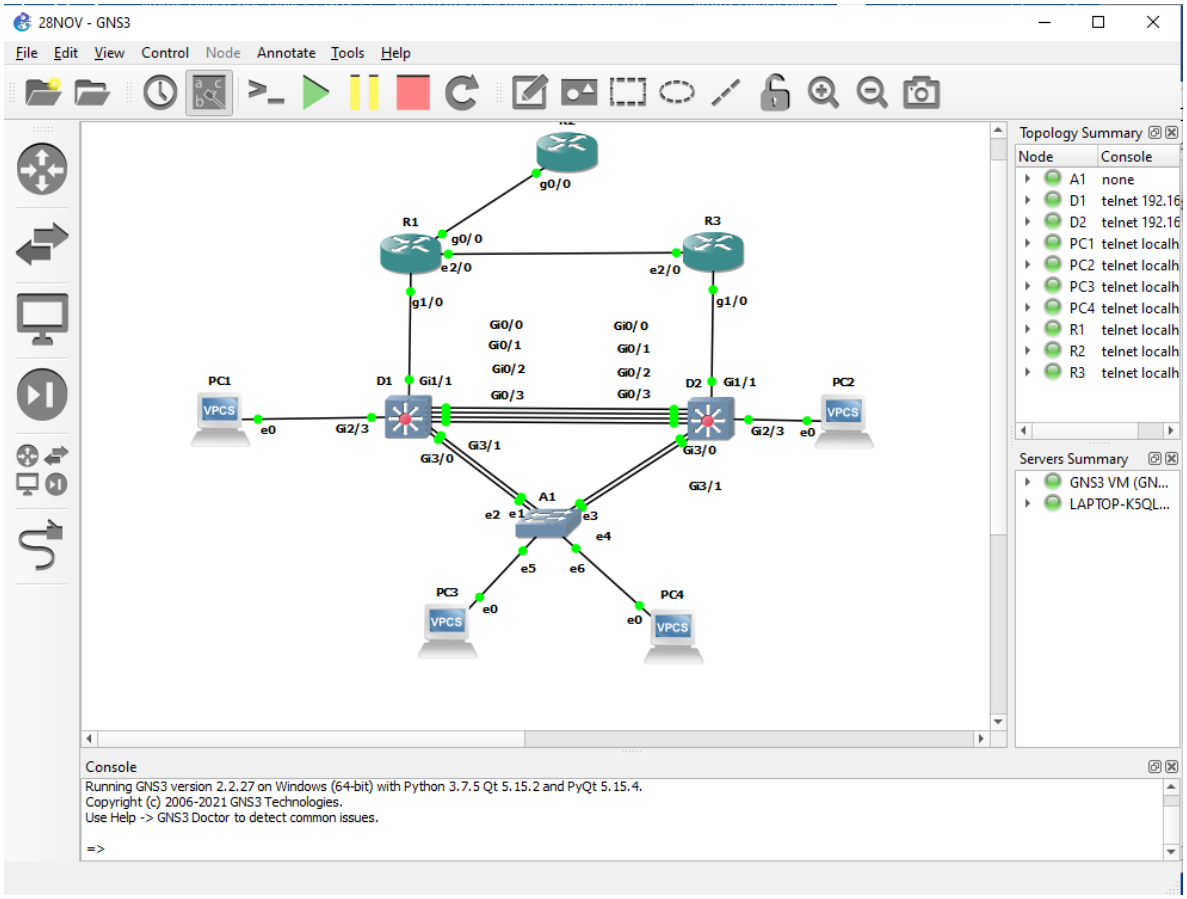

Figura 12 Topología escenario 2

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

Las tareas de configuración son las siguientes:

Tabla 4. Tareas de configuración

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 versión 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption).

		• Rastree el objeto 6 y decremente en 60.
Tarea #	**Tarea**	**Especificación**
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 versión 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. 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.

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

Se ejecuta el | comando sección ip sla en D1; aparece como se edita a continuación.

Verificamos la tarea 4.1 y el punto 3 de la tarea 4.3 para el conmutador D1

```
D1 # show run | sección ip sla
pista 4 ip sla 4
 retrasar 10 hasta 15
pista 6 ip sla 6
 retrasar 10 hasta 15
ip sla 4
 icmp-echo 10.0.10.1
 frecuencia 5
ip sla horario 4 hora de inicio ahora
ip sla 6
 icmp-echo 2001: DB8: 100: 1010 :: 1
 frecuencia 5
ip sla horario 6 hora de inicio ahora
```

```
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#
D1(config)#exit
D1#
*Nov 17 18:19:16.814: %SYS-5-CONFIG_I: Configured from console by console
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
```

Figura 13 Visualización SLA

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

Se ejecuta el | comando sección ip sla en D2; aparece como se edita a continuación. Verificamos la tarea 4.2 y el punto 3 de la tarea 4.3 para el

conmutador D2.

```
D2 # show run | sección ip sla
pista 4 ip sla 4
 retrasar 10 hasta 15
pista 6 ip sla 6
 retrasar 10 hasta 15
ip sla 4
 icmp-echo 10.0.11.1
 frecuencia 5
ip sla horario 4 hora de inicio ahora
ip sla 6
 icmp-echo 2001: DB8: 100: 1011 :: 1
 frecuencia 5
ip sla horario 6 hora de inicio ahora
```

4.3 En D1 configure HSRPv2.

Se inserta el comando show standby brief en D1; aparece como se edita a continuación. Verificamos la tarea 4.3.

```
D1 # muestra el resumen de espera
P indica configurado para apropiarse.
                |
Interfaz Grp Pri P Estado Activo Standby Virtual IP
Vl100 104   150 P Activo local 10.0.100.2 10.0.100.254
Vl100 106   150 P Local activo FE80 :: D2: 2 FE80 :: 5: 73FF: FEA0: 6A
Vl101 114   100 P En espera 10.0.101.2 local 10.0.101.254
Vl101 116   100 P En espera FE80 :: D2: 3 local FE80 :: 5: 73FF: FEA0: 74
Vl102 124   150 P Activo local 10.0.102.2 10.0.102.254
Vl102 126   150 P Local activo FE80 :: D2: 4 FE80 :: 5: 73FF: FEA0: 7E
```

```
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
D1#show stand
D1#show standby brie
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
Vl100       106  150 P Active  local           unknown         FE80::5:73FF:FEA0
:6A
Vl101       114  100 P Active  local           unknown         10.0.101.254
Vl101       116  100 P Active  local           unknown         FE80::5:73FF:FEA0
:74
```

Figura 14 Visualización VLAN

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. Mecanismos de seguridad

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**.

5.1 y 5.2 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

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

Se ejecuta la evidencia de la cuestión | incluir secreto en cada dispositivo; aparece como se edita a continuación. Verificamos la tarea 5.1 y 5.2.

R1 # show run | incluir secreto
habilitar secreto 9 $ 9 $ 0C3pnVdgrnhnY9 $ uzGA.WZfcLg5IhuyJu22mIf.YyZ / 83VgqbO3rXBDuwo
nombre de usuario sadmin privilegio 15 secreto 9 $ 9 $ XCO4pzqbRT.3EP $ ymouLOQI5 / o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6

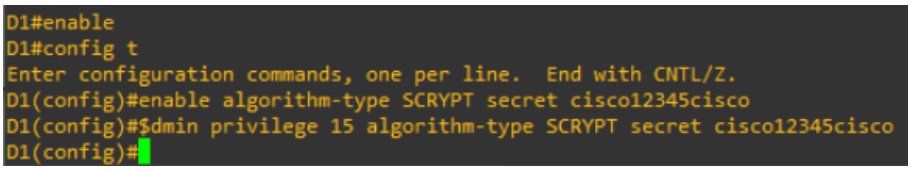

Figura 15 Scrypt

5.3, 5.4 y 5.5 En todos los dispositivos (excepto R2), habilite AAA.

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

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

¡Se ejecuta la evidencia de la cuestión aaa | excluir! en todos los dispositivos excepto R2; aparece como se edita a continuación. Verificamos la tarea 5.3, 5.4 y 5.5.

R1 # show run aaa | excluir!
aaa autenticación inicio de sesión grupo predeterminado radio local
nombre de usuario sadmin privilegio 15 secreto 9 $ 9 $ XCO4pzqbRT.3EP $ ymouLOQI5 / o0FOkYDtA1ztejFra67MnkJJ5Y3bhyQe6
servidor de radio RADIUS
dirección ipv4 10.0.100.6 auth-port 1812 acct-port 1813
clave $ trongPass
aaa nuevo modelo
aaa id de sesión común

```
R1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$Sg3OrQU06bC/4X$VgwDV6AnpJUXJjQ8ogQpBYJg
5G807bb9LxGFtuz0urY
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
aaa new-model
aaa session-id common
```

Figura 16 Configuración AAA

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. Administración de red

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.

Tarea#	Tarea	Especificación
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: • Únicamente 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*.

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

Verifique la hora UTC actual.

Publique el comando show clock en R2; la salida debe indicar la hora UTC actual correcta. Esto verifica la tarea 6.1 en R2.

Validación de parámetros de reloj en los dispositivos

Codigo ejecutado: show clock detail

```
D1#show clock de
D1#show clock detail
*01:28:44.979 UTC Thu Nov 18 2021
Time source is hardware calendar
D1#
```

Figura 17 Reloj

6.2 Configure R2 como un NTP maestro.

Ejecutamos elcomando | incluir el comando ntp en R2; aparece como se muestra a continuación. se verifica la tarea 6.2.

```
R2 #  show run | incluir ntp
enable
config term
ntp master 3
exit
```

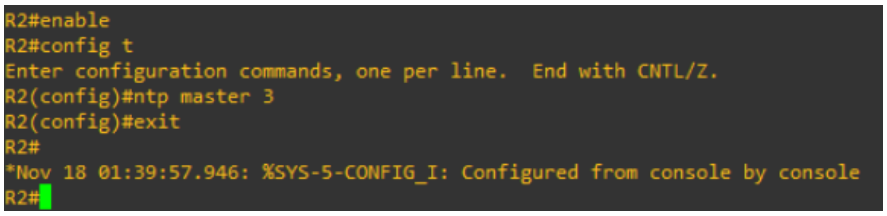

Figura 18 NTP maestro

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

Publique el estado del ntp de la demostración | incluir comando de estrato en R1; la salida debe aparecer como se muestra a continuación. Esto verifica la tarea 6.3 en el enrutador R1.

Sincroniza R1 con R2, A1 y D1 sincroniza la hora con R1, R3 sincroniza la hora con R3.

R2 # show run | incluir ntp
ntp master 3
R1 # muestra el estado de ntp | incluir estrato
reloj está sincronizado, estrato 4, la referencia es 2.2.2.2

Publicamos el estado del ntp de la demostración | Incluya el comando de estrato en R3, D1, D2 y A1. La salida debería aparecer como se muestra a continuación. Esto verifica la tarea 6.3 en estos dispositivos.

A1 # muestra el estado de ntp | incluir estrato
reloj está sincronizado, estrato 5, la referencia es 10.0.10.1

6.4 Configure Syslog en todos los dispositivos excepto R2.

Codigo ejecutado:
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 persistsnmp-server enable traps bgp

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

```
end
```

Insertamos | incluir comando de registro en todos los dispositivos excepto R2; la salida debe aparecer como se muestra a continuación. Esto verifica la tarea 6.4 en estos dispositivos

```
R1 #  show run | incluir registro
advertencias de trampa de registro
host de registro 10.0.100.5
registro sincrónico
```

6.5 Configure SNMPv2c en todos los dispositivos excepto R2.

Emitimos el comando show ip access-list SNMP-NMS en todos los dispositivos excepto R2; aparecer como se edita a continuación. Esto confirma la tarea 6.5.

```
D1 # muestre la lista de acceso IP SNMP-NMS
Lista de acceso IP estándar SNMP-NMS
 10 permiso 10.0.100.5
```

Ejecutamos el código | incluir el comando snmp en todos los dispositivos excepto R2; la salida debe aparecer como se muestra a continuación. Esto verifica el punto 2 de la tarea 6.5.

```
R1 # show run | incluir snmp
comunidad SNMP-servidor ENCORSA RO SNMP-NMS
snmp-server contacto con el estudiante de Cisco
snmp-server habilitar trampas ospf state-change
snmp-server enable traps errores de ospf
snmp-server habilitar trampas ospf retransmitir
snmp-server habilitar trampas ospf lsa
snmp-server enable traps ospf cambio de estado específico de Cisco nssa-trans-change
snmp-server enable traps ospf interfaz shamlink de cambio de estado específico de Cisco
snmp-server enable traps ospf vecino shamlink de cambio de estado específico de Cisco
snmp-server enable traps errores específicos de Cisco OSPF
snmp-server enable traps ospf retransmisión específica de Cisco
snmp-server enable traps ospf lsa específico de Cisco
configuración de trampas de habilitación del servidor snmp
snmp-server habilitar trampas bgp
host del servidor snmp 10.0.100.5 versión 2c ENCORSA
```

```
R3 # show run | incluir snmp
comunidad SNMP-servidor ENCORSA RO SNMP-NMS
```

snmp-server contacto con el estudiante de Cisco
snmp-server habilitar trampas ospf state-change
snmp-server enable traps errores de ospf
snmp-server habilitar trampas ospf retransmitir
snmp-server habilitar trampas ospf lsa
snmp-server enable traps ospf cambio de estado específico de Cisco nssa-trans-change
snmp-server enable traps ospf interfaz shamlink de cambio de estado específico de Cisco
snmp-server enable traps ospf vecino shamlink de cambio de estado específico de Cisco
snmp-server enable traps errores específicos de Cisco OSPF
snmp-server enable traps ospf retransmisión específica de Cisco
snmp-server enable traps ospf lsa específico de Cisco
configuración de trampas de habilitación del servidor snmp
host del servidor snmp 10.0.100.5 versión 2c ENCORSA

D1 # show run | incluir snmp
comunidad SNMP-servidor ENCORSA RO SNMP-NMS
snmp-server contacto con el estudiante de Cisco
snmp-server habilitar trampas ospf state-change
snmp-server enable traps errores de ospf
snmp-server habilitar trampas ospf retransmitir
snmp-server habilitar trampas ospf lsa
snmp-server enable traps ospf cambio de estado específico de Cisco nssa-trans-change
snmp-server enable traps ospf interfaz shamlink de cambio de estado específico de Cisco
snmp-server enable traps ospf vecino shamlink de cambio de estado específico de Cisco
snmp-server enable traps errores específicos de Cisco OSPF
snmp-server enable traps ospf retransmisión específica de Cisco
snmp-server enable traps ospf lsa específico de Cisco
configuración de trampas de habilitación del servidor snmp
host del servidor snmp 10.0.100.5 versión 2c ENCORSA

D2 # show run | incluir snmp
comunidad SNMP-servidor ENCORSA RO SNMP-NMS
snmp-server contacto con el estudiante de Cisco
snmp-server habilitar trampas ospf state-change
snmp-server enable traps errores de ospf
snmp-server habilitar trampas ospf retransmitir
snmp-server habilitar trampas ospf lsa
snmp-server enable traps ospf cambio de estado específico de Cisco nssa-trans-change
snmp-server enable traps ospf interfaz shamlink de cambio de estado específico de Cisco
snmp-server enable traps ospf vecino shamlink de cambio de estado específico de Cisco
snmp-server enable traps errores específicos de Cisco OSPF
snmp-server enable traps ospf retransmisión específica de Cisco
snmp-server enable traps ospf lsa específico de Cisco
configuración de trampas de habilitación del servidor snmp
host del servidor snmp 10.0.100.5 versión 2c ENCORSA

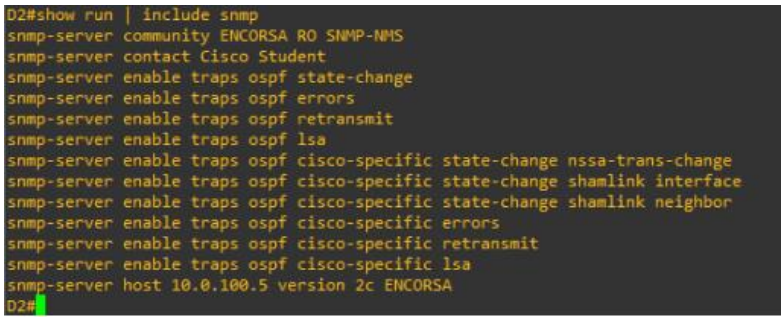

Figura 19 SNMP

A1 # show run | incluir snmp
comunidad SNMP-servidor ENCORSA RO SNMP-NMS
snmp-server contacto con el estudiante de Cisco
configuración de trampas de habilitación del servidor snmp
host del servidor snmp 10.0.100.5 versión 2c ENCORSA

A continuación se relaciona el código base utilizado en la programación de los equipos de la topología escenario 1 y 2 prueba de habilidades.

D1
interface range g1/0/1-4
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g1/0/5-6
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
interface g1/0/23
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end

D2

```
interface range g1/0/1-4
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g1/0/5-6
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
!
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
!
interface g1/0/23
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
end
```

A1

```
spanning-tree mode rapid-pvst
interface range f0/1-2
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
interface range f0/3-4
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
interface f0/23
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface f0/24
switchport mode access
switchport access vlan 100
```

```
spanning-tree portfast
no shutdown
exit
end
```

R1

```
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
exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface g0/0/1
ipv6 ospf 6 area 0
exit
interface s0/1/0
ipv6 ospf 6 area 0
exit
!
ip route 10.0.0.0 255.0.0.0 null0
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
```

R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
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
neighbor 209.165.200.225 activate
```

no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family

R3
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
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface g0/0/1
ipv6 ospf 6 area 0
exit
interface s0/1/0
ipv6 ospf 6 area 0
exit

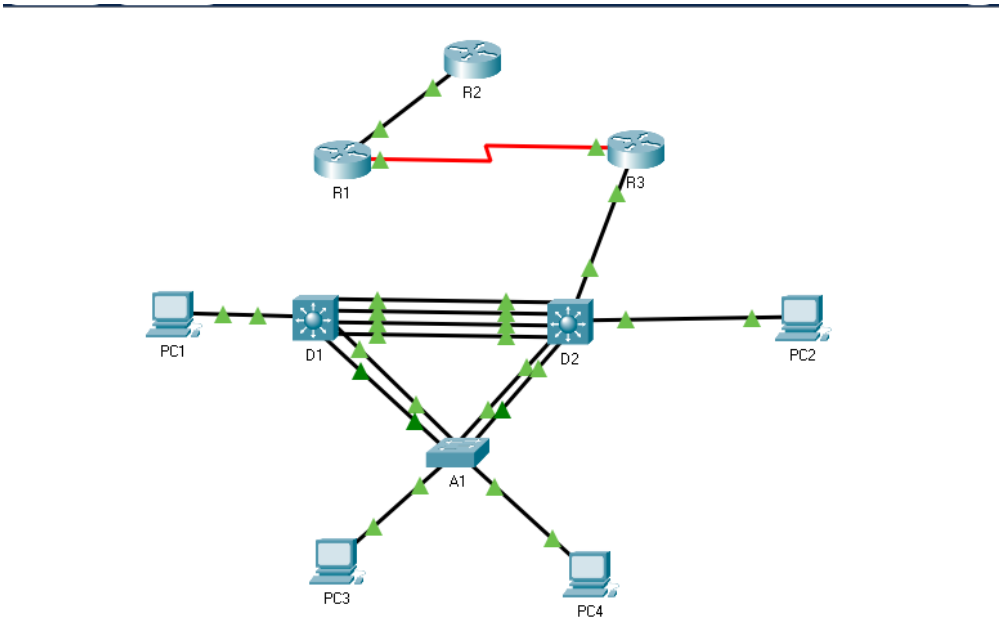

Figura 20 Topología ejercicio finalizado

CONCLUSIONES

En la actividad desarrollada se configura la topología requerida en el escenario, el ejercicio nos indica la conexión y enrrutamiento de varios equipos los cuales se crearon de acuerdo a las bases obtenidas durante el diplomado y cursos anteriores.

Los códigos de programación asignados en la primera parte con su respectiva explicación de cada uno enriquecen el conocimiento ya que el paso a paso que se realiza nos ayuda a descifrar y entender lo que se está implementando en una red, así mismo notamos errores de los cuales aprendemos a solucionar.

El método de configuración de la topología fue de gran utilidad ya que por medio de este escenario comprendemos y aprendemos en cierta parte a realizar una red con distintos equipos y con base a esto observamos en la parte de hardware virtual que hay conexiones como tarjetas que se implementan para enrutar los router, esto es de gran importancia ya que en la realidad todo esto existe y es el día a día de nuestra ingeniería.

EL software utilizado para el desarrollo de la prueba de habilidades fue de gran importancia ya que se asimila a la realidad en campos de programación, los comandos utilizados requieren de ser bien estructurados a la hora de ejecutarlos, cualquier letra mal escrita no deja avanzar la actividad, se cumple con un buen nivel a aprendizaje en cuanto a los conocimiento obtenidos durante el diplomado.

BIBLIOGRAFIA

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

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

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

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

The bryantadvantage.com. (2017). CCNP SWITCH Tutorial: EtherChannel Fundamentals. Recuperado de: https://www.thebryantadvantage.com/videos-and- tutorials/ccnp-switch-tshoot-tutorials/etherchannel-fundamentals/