DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CHRISTIAN LEONARDO DÍAZ RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C.
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CHRISTIAN LEONARDO DÍAZ RODRÍGUEZ

Diplomado de opción de grado presentado para optar por el título de INGENIERO ELECTRÓNICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C.
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 29 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

OSPF: Open Shortest Path First es un protocolo que utiliza el costo como métrica con el fin de seleccionar la mejor ruta que puede tomar un paquete al ser enviado a través de la red, mientras es menor el costo, es mayor el ancho de banda, por lo tanto, la ruta es mejor. OSPF utiliza el protocolo IP directamente para su transporte, encapsulando sus paquetes en datagramas, es decir, se agrega un encabezado IP que permite entregar el paquete al host de destino.

RSPT: Rapid Spanning Tree Protocol es un protocolo de enlace de datos correspondiente a la segunda capa del modelo OSI y su principal función dentro de una red es evitar bucles en el transporte de paquetes en conexiones cableadas o inalámbricas con puente.

BGP: Border Gateway Protocol es un protocolo que permite el intercambio de información de enrutamiento entre sistemas autónomos por medio de nodos, proporcionando seguridad y fiabilidad de conexión ya que oculta los detalles de la red por la que opera. El algoritmo que utiliza BGP selecciona la ruta que realiza la menor cantidad de saltos en los sistemas autónomos.

SDM: Security Device Manager es una herramienta utilizada para configurar conexiones de red y seguridad dentro de uno o varios enrutadores de manera sencilla, funciona por medio de una interfaz gráfica de tipo web.

SLAAC: Stateless Address Autoconfiguration es un método que se aplica en un dispositivo con el fin de permitir la obtención de una dirección IPv6 de unidifusión sin contar necesariamente con las funciones de un servidor. Este método permite la configuración automática de nodos dentro de una o varias redes.

RESUMEN

En el presente documento se registra el desarrollo del escenario propuesto por medio de simulación en el software GNS3, iniciando con la generación de la topología sugerida utilizando dispositivos de routing y switching similares a los indicados en la guía para implementar la red solicitada. Luego se realiza la conexión entre los dispositivos de la red, para ello se tuvo en cuenta la tabla de direccionamiento con el fin de conectar las interfaces y puertos adecuados entre ellos. Una vez completada la topología del escenario, se procede con la configuración de la red para generar una accesibilidad completa de un extremo a otro y un soporte confiable entre los hosts y la puerta de enlace predeterminada, para que los protocolos configurados operen correctamente de acuerdo con los lineamientos establecidos dentro de la red de la compañía. En la configuración se aplican y verifican protocolos como STP, RSTP, OSPF, EIGRP y BGP, además de la creación de VLAN, enlaces troncales, LACP, clientes IPv4 e IPv6, DHCP, vecinos, SLA, HSRP, temas de seguridad, administración, entre otros.

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

ABSTRACT

This document records the development of the proposed scenario through simulation in the GNS3 software, starting with the generation of the suggested topology using routing and switching devices like those indicated in the guide to implement the requested network. Then we proceed with the connection between the network devices, for this the addressing table was considered to connect the appropriate interfaces and ports between them. Once the topology of the scenario is completed, the network configuration is carried out to generate complete end-to-end accessibility and reliable support between the hosts and the default gateway, so that the configured protocols operate correctly according to the guidelines established within the company's network. In the configuration, protocols such as STP, RSTP, OSPF, EIGRP and BGP are applied and verified, in addition to the creation of VLANs, trunks, LACP, IPv4 and IPv6 clients, DHCP, neighbors, SLA, HSRP, security issues, administration, among others.

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

INTRODUCCIÓN

En el presente documento se registra el desarrollo y la solución de las actividades correspondientes al escenario propuesto “Diplomado de profundización Cisco Prueba De Habilidades Prácticas CCNP” referente a la entrega final del diplomado de profundización CISCO CCNP y los resultados obtenidos en el software GNS3. Dentro del desarrollo de las actividades se evidencian los comandos utilizados en cada dispositivo para el correcto funcionamiento de la red y sus respectivas notas explicativas.

El escenario se distribuye en seis partes abordando temas de construcción de la red, configuración de los ajustes básicos de cada dispositivo, direccionamiento de las interfaces, configuración de la capa 2 de la red, soporte de host, configuración de los protocolos de enrutamiento, configuración de la redundancia del primer salto, configuración de la seguridad y configuración de las características de administración de red.

En la primera parte se ajustan aspectos básicos de cada dispositivo como asignación de nombre, interfaces, direcciones IP, banner, VLAN, puerta de enlace, entre otros. En la segunda parte se habilitan los enlaces troncales, VLAN Nativas, Protocolo RSTP, Port Channel, puertos de acceso para los PC, clientes DHCP y se verifica la conectividad LAN local. La tercera parte consiste en la configuración de protocolos de enrutamiento como OSPF, OSPFv2, OSPFv3, BGP y MP-BGP. La cuarta parte se utiliza para configurar la redundancia del primer salto por medio de la creación de IP SLA y la implementación de HSRPv2 en los Switches D1 y D2. En la quinta parte se configuran mecanismos de seguridad en los dispositivos por medio de nombres de usuario y contraseña, además de protocolos como AAA y RADIUS. En la sexta y última parte se aplican comandos que permiten configurar las funciones administrativas de la red, hora local UTC, sincronización por medio de NTP, envío de mensajes aplicando Syslog y protocolo SNMP para intercambio de información de administración.

DESARROLLO DEL ESCENARIO PROPUESTO

Topología de la Red

Figura 1. Topología de la red

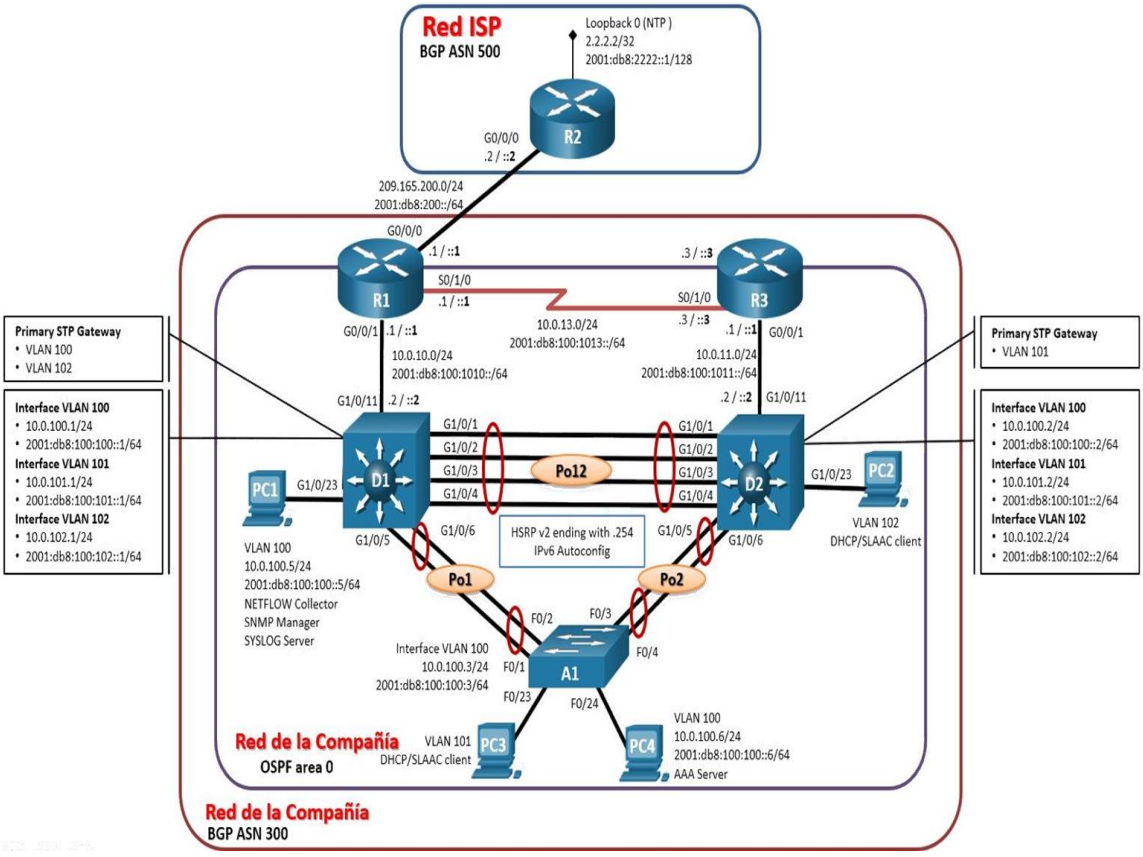


Tabla de Direccionamiento

En la siguiente tabla de direccionamiento ha sido necesario modificar las interfaces para trabajar con el software GNS3.

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.165.200.225 /27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0	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	G1/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E0/0	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	E0/0	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	10.0.100.3/24	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

Objetivos

Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces.

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

Parte 3: Configurar los protocolos de enrutamiento.

Parte 4: Configurar la redundancia del primer salto.

Parte 5: Configurar la seguridad.

Parte 6: Configurar las características de administración de red.

Escenario

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

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

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

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global sdm prefer dual-ipv4-and-ipv6 default. Cambiar la plantilla requerirá el reinicio del switch.

Recursos necesarios

- 3 Router (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable).
- 2 Switch (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable).
- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable).
- 4 PCs (utilice el programa de emulación de terminal).
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola.
- Los cables Ethernet y seriales van como se muestra en la topología.

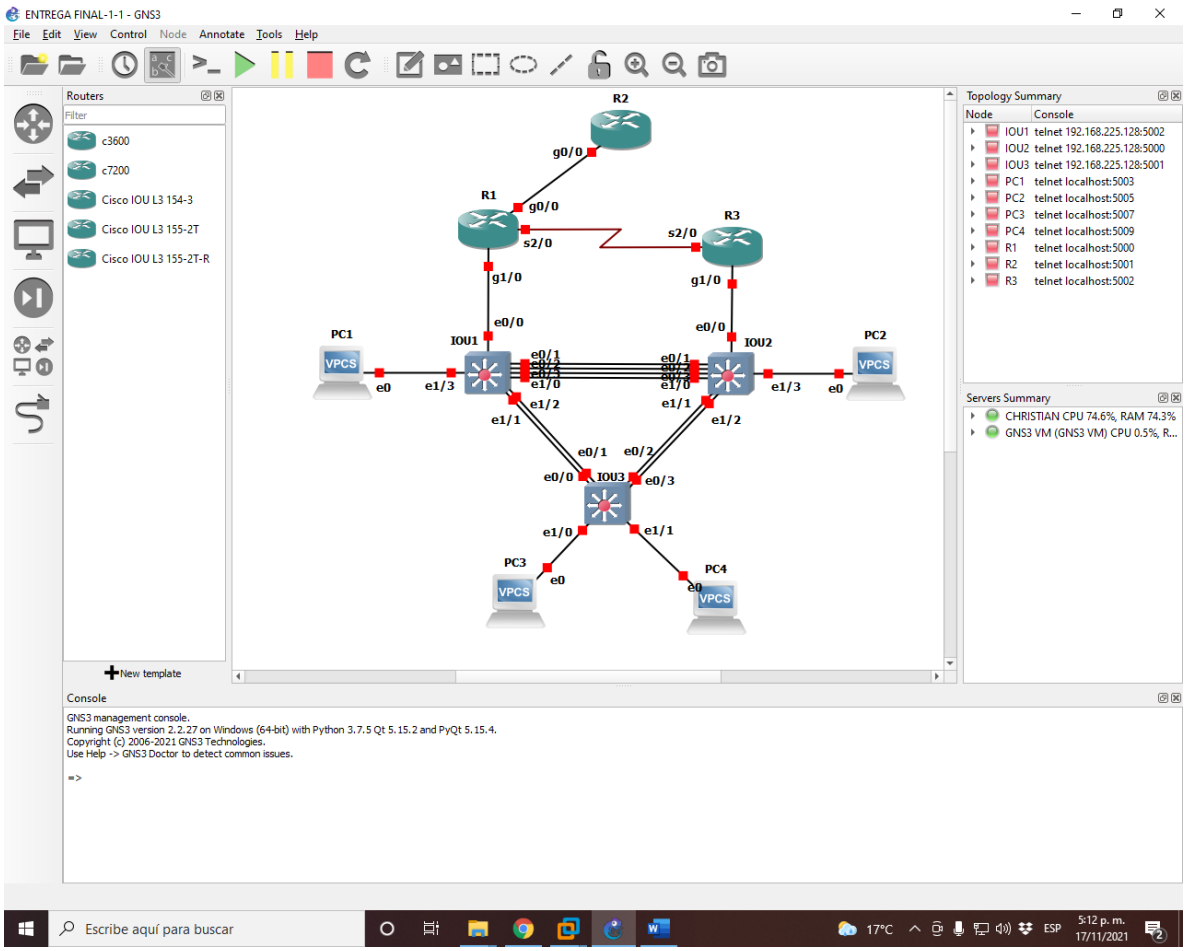
Nota: Durante el desarrollo del diplomado se ha determinado que la solución se debe desarrollar en el software GNS3 con el fin de que todos los comandos funcionen. Las versiones de imagen sugeridas se encuentran en la página de CISCO con opción de pago, por lo que se han utilizado versiones similares gratuitas sugeridas por el tutor.

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES

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

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

Figura 2. Conexión de los Dispositivos según Diagrama de Topología



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:

- Ingreso al modo EXEC Privilegiado.

```
Router>enable
```

- Configuro manualmente desde la terminal de consola.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- Asigno el nombre al dispositivo.

```
Router(config)#hostname R1
```

- Habilito el dispositivo para reenviar paquetes IPv6.

```
R1(config)#ipv6 unicast-routing
```

- Desactivo la traducción de nombres a dirección del dispositivo.

```
R1(config)#no ip domain lookup
```

- Configuro el mensaje del día, el cual mostrará el dispositivo.

```
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
```

- Ingreso al modo de configuración de línea de la consola.

```
R1(config)#line con 0
```

- Configuro un tiempo de espera ilimitado para la sesión.

```
R1(config-line)#exec-timeout 0 0
```

- Bloqueo interrupción de mensajes inesperados.

```
R1(config-line)#logging synchronous
```

- Regreso al modo de configuración de consola.

R1(config-line)#exit

- Selecciono la interfaz que voy a configurar.

R1(config)#interface g0/0

- Asigno la dirección IPv4 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

R1(config-if)#ip address 209.165.200.225 255.255.255.224

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

R1(config-if)#ipv6 address fe80::1:1 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

R1(config-if)#ipv6 address 2001:db8:200::1/64

- Habilito la interfaz que se ha configurado.

R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

- Regreso al modo de configuración de consola.

R1(config-if)#exit

- Siguiendo el procedimiento anterior, configuro las demás interfaces y las direcciones IP del dispositivo de acuerdo con la tabla de direccionamiento suministrada.

R1(config)#interface g1/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up

```
R1(config-if)#exit
R1(config)#interface s2/0
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

%LINK-5-CHANGED: Interface Serial2/0, changed state to down
R1(config-if)#exit
R1(config)#exit
R1#
```

Router R2:

- Ingreso al modo EXEC Privilegiado.

```
Router>enable
```

- Configuro manualmente desde la terminal de consola.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- Asigno el nombre al dispositivo.

```
Router(config)#hostname R2
```

- Habilito el dispositivo para reenviar paquetes IPv6.

```
R2(config)#ipv6 unicast-routing
```

- Desactivo la traducción de nombres a dirección del dispositivo.

```
R2(config)#no ip domain lookup
```

- Configuro el mensaje del día, el cual mostrará el dispositivo.

```
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
```

- Ingreso al modo de configuración de línea de la consola.

```
R2(config)#line con 0
```

- Configuro un tiempo de espera ilimitado para la sesión.

R2(config-line)#exec-timeout 0 0

- Bloqueo interrupción de mensajes inesperados.

R2(config-line)#logging synchronous

- Regreso al modo de configuración de consola.

R2(config-line)#exit

- Selecciono la interfaz que voy a configurar.

R2(config)#interface g0/0

- Asigno la dirección IPv4 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

R2(config-if)#ip address 209.165.200.226 255.255.255.224

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

R2(config-if)#ipv6 address fe80::2:1 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

R2(config-if)#ipv6 address 2001:db8:200::2/64

- Habilito la interfaz que se ha configurado.

R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

- Regreso al modo de configuración de consola.

R2(config-if)#exit

- Habilito una interfaz virtual.

R2(config)#interface Loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

- Asigno a la interfaz virtual los parámetros indicados en la tabla de direccionamiento.

R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
R2#

Router R3:

- Ingreso al modo EXEC Privilegiado.

Router>enable

- Configuro manualmente desde la terminal de consola.

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

- Asigno el nombre al dispositivo.

Router(config)#hostname R3

- Habilito el dispositivo para reenviar paquetes IPv6.

R3(config)#ipv6 unicast-routing

- Desactivo la traducción de nombres a dirección del dispositivo.

R3(config)#no ip domain lookup

- Configuro el mensaje del día, el cual mostrará el dispositivo.

R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #

- Ingreso al modo de configuración de línea de la consola.

R3(config)#line con 0

- Configuro un tiempo de espera ilimitado para la sesión.

R3(config-line)#exec-timeout 0 0

- Bloqueo interrupción de mensajes inesperados.

R3(config-line)#logging synchronous

- Regreso al modo de configuración de consola.

R3(config-line)#exit

- Selecciono la interfaz que voy a configurar.

R3(config)#interface g1/0

- Asigno la dirección IPv4 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

R3(config-if)#ip address 10.0.11.1 255.255.255.0

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

R3(config-if)#ipv6 address fe80::3:2 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

R3(config-if)#ipv6 address 2001:db8:100:1011::1/64

- Habilito la interfaz que se ha configurado.

R3(config-if)#no shutdown
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to up

- Regreso al modo de configuración de consola.

R3(config-if)#exit

- Siguiendo el procedimiento anterior, configuro las demás interfaces y las direcciones IP del dispositivo de acuerdo con la tabla de direccionamiento suministrada.

R3(config)#interface s2/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1013::3/64
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

R3(config-if)#exit
R3(config)#exit
R3#

Switch D1:

- Ingreso al modo EXEC Privilegiado.

Switch>enable

- Configuro manualmente desde la terminal de consola.

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

- Asigno el nombre al dispositivo.

Switch(config)#hostname D1

- Habilito el enrutamiento en el dispositivo.

D1(config)#ip routing

- Habilito el dispositivo para reenviar paquetes IPv6.

D1(config)#ipv6 unicast-routing

- Desactivo la traducción de nombres a dirección del dispositivo.

D1(config)#no ip domain lookup

- Configuro el mensaje del día, el cual mostrará el dispositivo.

D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #

- Ingreso al modo de configuración de línea de la consola.

D1(config)#line con 0

- Configuro un tiempo de espera ilimitado para la sesión.

D1(config-line)#exec-timeout 0 0

- Bloqueo interrupción de mensajes inesperados.

D1(config-line)#logging synchronous

- Regreso al modo de configuración de consola.

D1(config-line)#exit

- Genero una VLAN de acuerdo con la tabla de direccionamiento suministrada.

D1(config)#vlan 100

- Asigno un nombre VLAN creada.

D1(config-vlan)#name Management

- Regreso al modo de configuración de consola.

D1(config-vlan)#exit

- Utilizo el procedimiento anterior para generar las demás VLAN de acuerdo con la tabla de direccionamiento suministrada.

D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit

- De igual manera genero la VLAN nativa teniendo en cuenta que más adelante se debe configurar como enlace troncal.

D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit

- Selecciono la interfaz que voy a configurar.

D1(config)#interface e0/0

- Establezco el puerto de la interfaz como enrutador.

D1(config-if)#no switchport
D1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up

- Asigno la dirección IPv4 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

D1(config-if)#ip address 10.0.10.2 255.255.255.0

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

D1(config-if)#ipv6 address fe80::d1:1 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

D1(config-if)#ipv6 address 2001:db8:100:1010::2/64

- Habilito la interfaz que se ha configurado.

D1(config-if)#no shutdown

- Regreso al modo de configuración de consola.

D1(config-if)#exit

- Selecciono la interfaz VLAN que voy a configurar.

```
D1(config)#interface vlan 100
D1(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up
```

- Asigno la dirección IPv4 y la máscara de subred correspondiente a la VLAN como se indica en la tabla de direccionamiento.

```
D1(config-if)#ip address 10.0.100.1 255.255.255.0
```

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

```
D1(config-if)#ipv6 address fe80::d1:2 link-local
```

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

```
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
```

- Habilito la interfaz que se ha configurado.

```
D1(config-if)#no shutdown
```

- Regreso al modo de configuración de consola.

```
D1(config-if)#exit
```

- Sigo el procedimiento anterior para configurar las demás VLAN.

```
D1(config)#interface vlan 101
D1(config-if)#
%LINK-5-CHANGED: Interface Vlan101, changed state to up

D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit

D1(config)#interface vlan 102
D1(config-if)#
%LINK-5-CHANGED: Interface Vlan102, changed state to up
```

```
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
```

- Defino el rango de direcciones IP reservadas para excluirlas del direccionamiento DHCP.

```
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
```

- Accedo al grupo de direcciones de la VLAN que voy a configurar.

```
D1(config)#ip dhcp pool VLAN-101
```

- Asigno la dirección IPv4 y la máscara de subred correspondiente para la VLAN como se indica en la tabla de direccionamiento.

```
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
```

- Asigno una Puerta de enlace predeterminada al dispositivo.

```
D1(dhcp-config)#default-router 10.0.101.254
```

- Regreso al modo de configuración de consola.

```
D1(dhcp-config)#exit
```

- Sigo el procedimiento anterior para configurar grupos de direcciones en otras VLAN.

```
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
```

- Dejo encendida la interfaz que se conecta con R1 y deshabilito las restantes.

```
D1(config)#interface e0/0
D1(config-if)#no shutdown
D1(config-if)#interface e0/1
```

```
D1(config-if)#shutdown
D1(config-if)#interface e0/2
D1(config-if)#shutdown
D1(config-if)#interface e0/3
D1(config-if)#shutdown
D1(config-if)#interface e1/0
D1(config-if)#shutdown
D1(config-if)#interface e1/1
D1(config-if)#shutdown
D1(config-if)#interface e1/2
D1(config-if)#shutdown
D1(config-if)#interface e1/3
D1(config-if)#shutdown
D1(config-if)#exit
```

Switch D2:

- Ingreso al modo EXEC Privilegiado.

```
Switch>enable
```

- Configuro manualmente desde la terminal de consola.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- Asigno el nombre al dispositivo.

```
Switch(config)#hostname D2
```

- Habilito el enrutamiento en el dispositivo.

```
D2(config)#ip routing
```

- Habilito el dispositivo para reenviar paquetes IPv6.

```
D2(config)#ipv6 unicast-routing
```

- Desactivo la traducción de nombres a dirección del dispositivo.

```
D2(config)#no ip domain lookup
```

- Configuro el mensaje del día, el cual mostrará el dispositivo.

D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #

- Ingreso al modo de configuración de línea de la consola.

D2(config)#line con 0

- Configuro un tiempo de espera ilimitado para la sesión.

D2(config-line)#exec-timeout 0 0

- Bloqueo interrupción de mensajes inesperados.

D2(config-line)#logging synchronous

- Regreso al modo de configuración de consola.

D2(config-line)#exit

- Genero una VLAN de acuerdo con la tabla de direccionamiento suministrada.

D2(config)#vlan 100

- Asigno un nombre VLAN creada.

D2(config-vlan)#name Management

- Regreso al modo de configuración de consola.

D2(config-vlan)#exit

- Utilizo el procedimiento anterior para generar las demás VLAN de acuerdo con la tabla de direccionamiento suministrada.

D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit

- De igual manera genero la VLAN nativa teniendo en cuenta que más adelante se debe configurar como enlace troncal.

D2(config)#vlan 999

D2(config-vlan)#name NATIVE
D2(config-vlan)#exit

- Selecciono la interfaz que voy a configurar.

D2(config)#interface e0/0

- Establezco el puerto de la interfaz como enrutador.

D2(config-if)#no switchport
D2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet 0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet 0/0, changed state to up

- Asigno la dirección IPv4 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

D2(config-if)#ip address 10.0.11.2 255.255.255.0

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

D2(config-if)#ipv6 address fe80::d2:1 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

D2(config-if)#ipv6 address 2001:db8:100:1011::2/64

- Habilito la interfaz que se ha configurado.

D2(config-if)#no shutdown

- Regreso al modo de configuración de consola.

D2(config-if)#exit

- Selecciono la interfaz VLAN que voy a configurar.

D2(config)#interface vlan 100
D2(config-if)#

%LINK-5-CHANGED: Interface Vlan100, changed state to up

- Asigno la dirección IPv4 y la máscara de subred correspondiente a la VLAN como se indica en la tabla de direccionamiento.

D2(config-if)#ip address 10.0.100.2 255.255.255.0

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

D2(config-if)#ipv6 address fe80::d2:2 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

D2(config-if)#ipv6 address 2001:db8:100:100::2/64

- Habilito la interfaz que se ha configurado.

D2(config-if)#no shutdown

- Regreso al modo de configuración de consola.

D2(config-if)#exit

- Sigo el procedimiento anterior para configurar las demás VLAN.

D2(config)#interface vlan 101
D2(config-if)#
%LINK-5-CHANGED: Interface Vlan101, changed state to up

D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#
%LINK-5-CHANGED: Interface Vlan102, changed state to up

D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit

- Defino el rango de direcciones IP reservadas para excluirlas del direccionamiento DHCP.

```
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
```

- Accedo al grupo de direcciones de la VLAN que voy a configurar.

```
D2(config)#ip dhcp pool VLAN-101
```

- Asigno la dirección IPv4 y la máscara de subred correspondiente para la VLAN como se indica en la tabla de direccionamiento.

```
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
```

- Asigno una Puerta de enlace predeterminada al dispositivo.

```
D2(dhcp-config)#default-router 10.0.101.254
```

- Regreso al modo de configuración de consola.

```
D2(dhcp-config)#exit
```

- Sigo el procedimiento anterior para configurar grupos de direcciones en otras VLAN.

```
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
```

- Dejo encendida la interfaz que se conecta con R3 y deshabilito las restantes.

```
D2(config)#interface e0/0
D2(config-if)#no shutdown
D2(config-if)#interface e0/1
D2(config-if)#shutdown
D2(config-if)#interface e0/2
D2(config-if)#shutdown
D2(config-if)#interface e0/3
D2(config-if)#shutdown
```

```
D2(config-if)#interface e1/0
D2(config-if)#shutdown
D2(config-if)#interface e1/1
D2(config-if)#shutdown
D2(config-if)#interface e1/2
D2(config-if)#shutdown
D2(config-if)#interface e1/3
D2(config-if)#shutdown
D2(config-if)#exit
```

Switch A1:

- Ingreso al modo EXEC Privilegiado.

```
Switch>enable
```

- Configuro manualmente desde la terminal de consola.

```
Switch#configure terminal
```

- Cambio la plantilla del Switch, con el fin de habilitar el soporte de IPv6 en el dispositivo.

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
```

- Regreso al modo de configuración de consola.

```
Switch(config)#exit
```

- Verifico en la configuración que el Router tiene ahora funcionalidades de IPv6.

```
Switch#show sdm prefer

 number of unicast mac addresses: 8K
 number of IPv4 IGMP groups + multicast routes: 0.25K
 number of IPv4 unicast routes: 0
 number of IPv6 multicast groups: 0
 number of directly-connected IPv6 addresses: 0
 number of indirect IPv6 unicast routes: 0
 number of IPv4 policy based routing aces: 0
 number of IPv4/MAC qos aces: 0.125k
 number of IPv4/MAC security aces: 0.375k
```

number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 20
number of IPv6 security aces: 25

On next reload, template will be "dual-ipv4-and-ipv6 default" template.

- Reinicio el dispositivo para que tome la nueva configuración.

Switch#reload

System configuration has been modified. Save? [yes/no]:y
Building configuration...
[OK]
Proceed with reload? [confirm]

- Configuro manualmente desde la terminal de consola.

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

- Asigno el nombre al dispositivo.

Switch(config)#hostname A1

- Desactivo la traducción de nombres a dirección del dispositivo.

A1(config)#no ip domain lookup

- Configuro el mensaje del día, el cual mostrará el dispositivo.

A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #

- Ingreso al modo de configuración de línea de la consola.

A1(config)#line con 0

- Configuro un tiempo de espera ilimitado para la sesión.

A1(config-line)#exec-timeout 0 0

- Bloqueo interrupción de mensajes inesperados.

A1(config-line)#logging synchronous

- Regreso al modo de configuración de consola.

A1(config-line)#exit

- Genero una VLAN de acuerdo con la tabla de direccionamiento suministrada.

A1(config)#vlan 100

- Asigno un nombre VLAN creada.

A1(config-vlan)#name Management

- Regreso al modo de configuración de consola.

A1(config-vlan)#exit

- Utilizo el procedimiento anterior para generar las demás VLAN de acuerdo con la tabla de direccionamiento suministrada.

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

- De igual manera genero la VLAN nativa teniendo en cuenta que más adelante se debe configurar como enlace troncal.

A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit

- Selecciono la interfaz VLAN que voy a configurar.

A1(config)#interface vlan 100

- Asigno la dirección IPv4 y la máscara de subred correspondiente a la VLAN como se indica en la tabla de direccionamiento.

A1(config-if)#ip address 10.0.100.3 255.255.255.0

- Asigno un parámetro de link local que permite a los dispositivos de la red reconocer fácilmente el dispositivo al que pertenece una dirección IPv6.

A1(config-if)#ipv6 address fe80::a1:1 link-local

- Asigno la dirección IPv6 y la máscara de subred correspondiente para el dispositivo como se indica en la tabla de direccionamiento.

A1(config-if)#ipv6 address 2001:db8:100:100::3/64

- Habilito la interfaz que se ha configurado.

A1(config-if)#no shutdown

- Regreso al modo de configuración de consola.

A1(config-if)#exit

- Deshabilito las interfaces de A1 temporalmente, estás se habilitarán más adelante.

```
A1(config)#interface e0/0
A1(config-if)#shutdown
A1(config-if)#interface e0/1
A1(config-if)#shutdown
A1(config-if)#interface e0/2
A1(config-if)#shutdown
A1(config-if)#interface e0/3
A1(config-if)#shutdown
A1(config-if)#interface e1/0
A1(config-if)#shutdown
A1(config-if)#interface e1/1
A1(config-if)#shutdown
A1(config-if)#interface e1/2
A1(config-if)#shutdown
A1(config-if)#interface e1/3
A1(config-if)#shutdown
A1(config-if)#exit
```

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

- Guardo la configuración en todos los dispositivos.

Router R1:

R1>enable

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Router R2:

R2>enable
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#

Router R3:

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

Switch D1:

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

Switch D2:

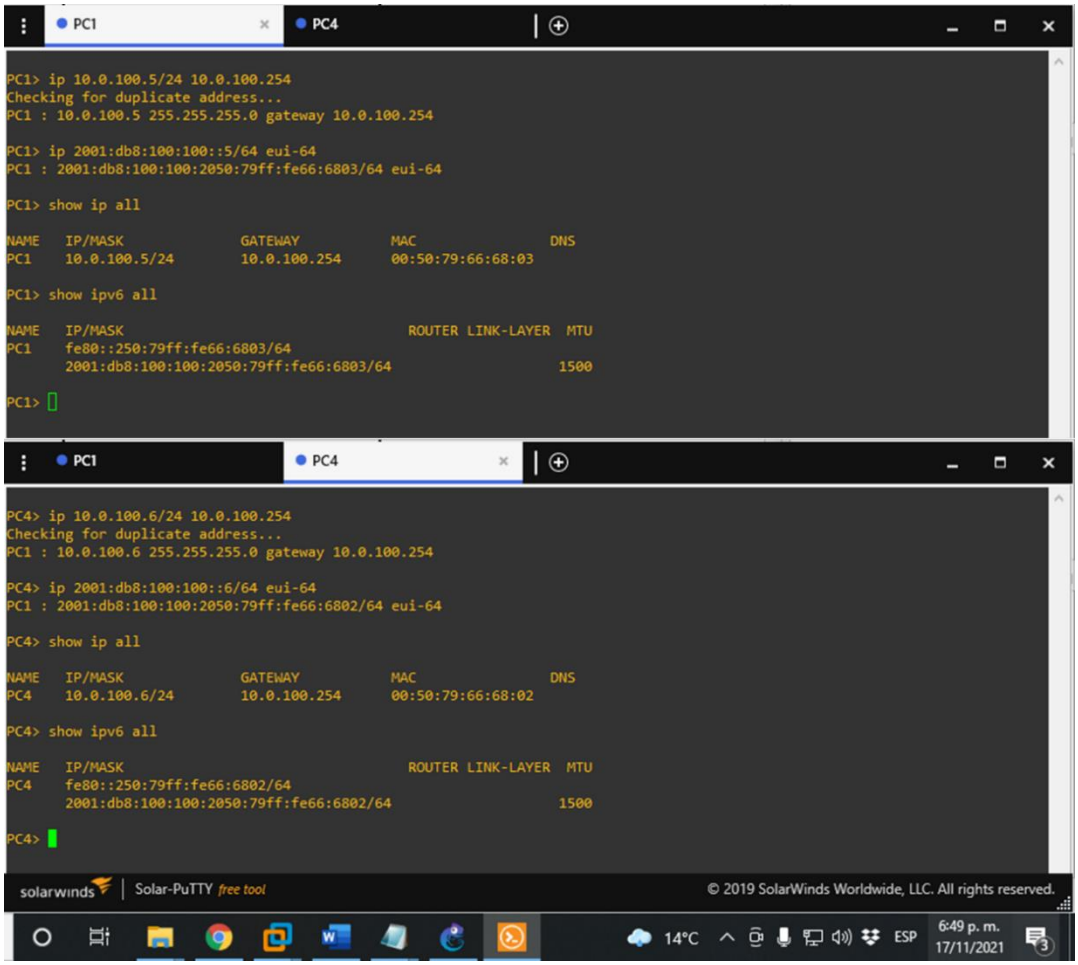
D2>enable
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Switch A1:

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

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 3. Configuración de los Host PC1 Y PC4



PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST

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

Las tareas de configuración son las siguientes:

Tabla 2. Actividades por desarrollar en la Parte 2

Tarea #	**Tarea**	**Especificación**
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
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 2 D2 a A1 – Port channel 1
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: D1: 10.0.100.1 D2: 10.0.100.2 PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: D1: 10.0.102.1 D2: 10.0.102.2 PC3 debería hacer ping con éxito a: D1: 10.0.101.1 D2: 10.0.101.2 PC4 debería hacer ping con éxito a: D1: 10.0.100.1 D2: 10.0.100.2 PC1: 10.0.100.5

Solución 2.1

En todos los switches configuro 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

```
D1>en
D1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#interface range Ethernet 0/1 - 3
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config)#interface Ethernet 1/0
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config)#interface range Ethernet 1/1 – 2
```

```
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk

D2>en
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#interface range Ethernet 0/1 - 3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config)#interface Ethernet 1/0
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config)#interface range Ethernet 1/1 – 2
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk

A1>en
A1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
A1(config)#interface range Ethernet 0/0 - 1
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config)#interface range Ethernet 0/2 - 3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
```

Solución 2.2

En todos los switches asigno la VLAN nativa en los enlaces troncales. Uso VLAN 999 como la VLAN nativa.

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

D2(config-if-range)#switchport trunk native vlan 999

A1(config-if-range)#switchport trunk native vlan 999
```

Para habilitar los rangos de enlaces troncales en cada interfaz aplico el comando “no shutdown” en cada switch.

Solución 2.3

En todos los switches habilito el protocolo Rapid Spanning-Tree (RSTP)

D1(config)#spanning-tree mode rapid-pvst

D2(config)#spanning-tree mode rapid-pvst

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

Solución 2.4

En D1 y D2, configuro 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).

Configuro D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

D1(config)#spanning-tree vlan 100,102 priority 24576
D1(config)#spanning-tree vlan 101 priority 28672

D2(config)#spanning-tree vlan 101 priority 24576
D2(config)#spanning-tree vlan 100,102 priority 28672

Solución 2.5

En todos los switches, creo EtherChannels LACP como se muestra en el diagrama de topología. Usando los siguientes números de canales:

D1 a D2 – Port channel 12
D1 a A1 – Port channel 1
D2 a A1 – Port channel 2

En cada Switch selecciono el rango de interfaces y asigno el Port-channel al cual va a pertenecer.

- Switch D1 a Switch D2

D1(config)#interface range Ethernet 0/1 - 3
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)# switchport mode trunk

D1(config-if-range)#channel-group 12 mode active

D1(config)#interface Ethernet 1/0
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#channel-group 12 mode active

D2(config)#interface range Ethernet 0/1 - 3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)# switchport mode trunk
D2(config-if-range)#channel-group 12 mode active

D2(config)#interface Ethernet 1/0
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#channel-group 12 mode active

- Switch D1 a Switch A1

D1(config)#interface range Ethernet 1/1 - 2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#channel-group 1 mode active

A1(config)#interface range Ethernet 0/0 - 1
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#channel-group 1 mode active

- Switch D2 a Switch A1

D2(config)#interface range Ethernet 1/1 - 2
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#channel-group 2 mode active

A1(config)#interface range Ethernet 0/2 - 3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#channel-group 2 mode active

- A cada Port-channel creado le asigno la VLAN Nativa.

A1(config)#int port-channel 1

```
A1(config-if)#switchport trunk native vlan 999
A1(config)#int port-channel 2
A1(config-if)#switchport trunk native vlan 999

D1(config)#int port-channel 1
D1(config-if)#switchport trunk native vlan 999
D1(config)#int port-channel 12
D1(config-if)#switchport trunk native vlan 999

D2(config)#int port-channel 2
D2(config-if)#switchport trunk native vlan 999
D2(config)#int port-channel 12
D2(config-if)#switchport trunk native vlan 999
```

Solución 2.6

En todos los switches, configuro los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4. Configuro los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host pasaron inmediatamente al estado de reenvío (forwarding).

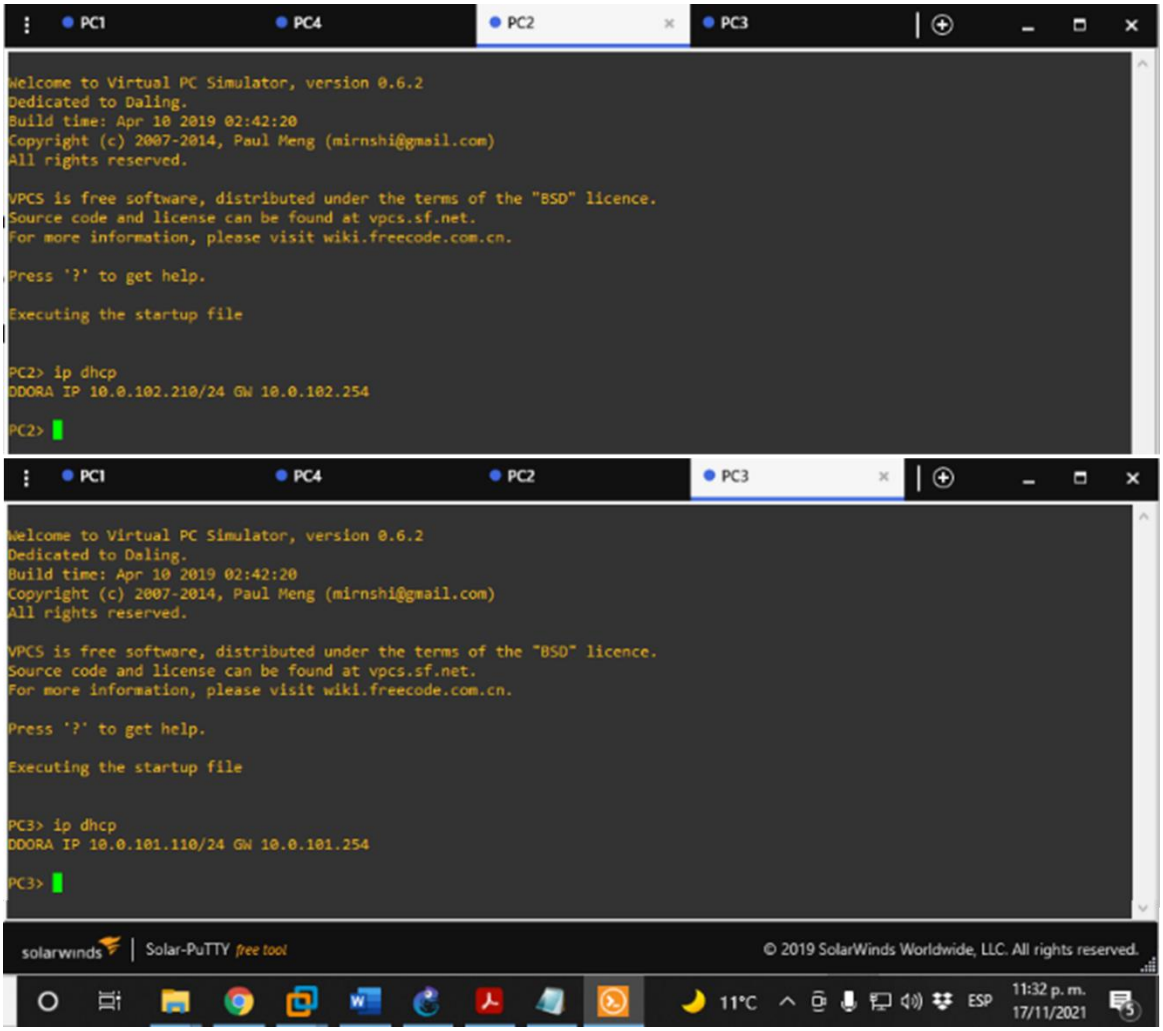
```
D1(config)#int e1/3
D1(config-if)#switchport mode access
D1(config-if)# switchport access vlan 100
D1(config-if)#spanning-tree portfast
D1(config)#no shutdown
D1(config)#exit

D2(config)#int e1/3
D2(config-if)#switchport mode access
D2(config-if)# switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config)#no shutdown
D2(config)#exit

A1(config)#int e1/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config)#no shutdown
A1(config)#exit
A1(config)#int e1/1
A1(config-if)#switchport mode access
```

A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config)#no shutdown
A1(config)#exit

Solución 2.7

Verifico los servicios DHCP IPv4. PC2 y PC3 son clientes DHCP y recibieron direcciones IPv4 válidas.

Figura 4. Configuración DHCP de los Host PC2 Y PC3



Solución 2.8

Verifico la conectividad de la LAN local

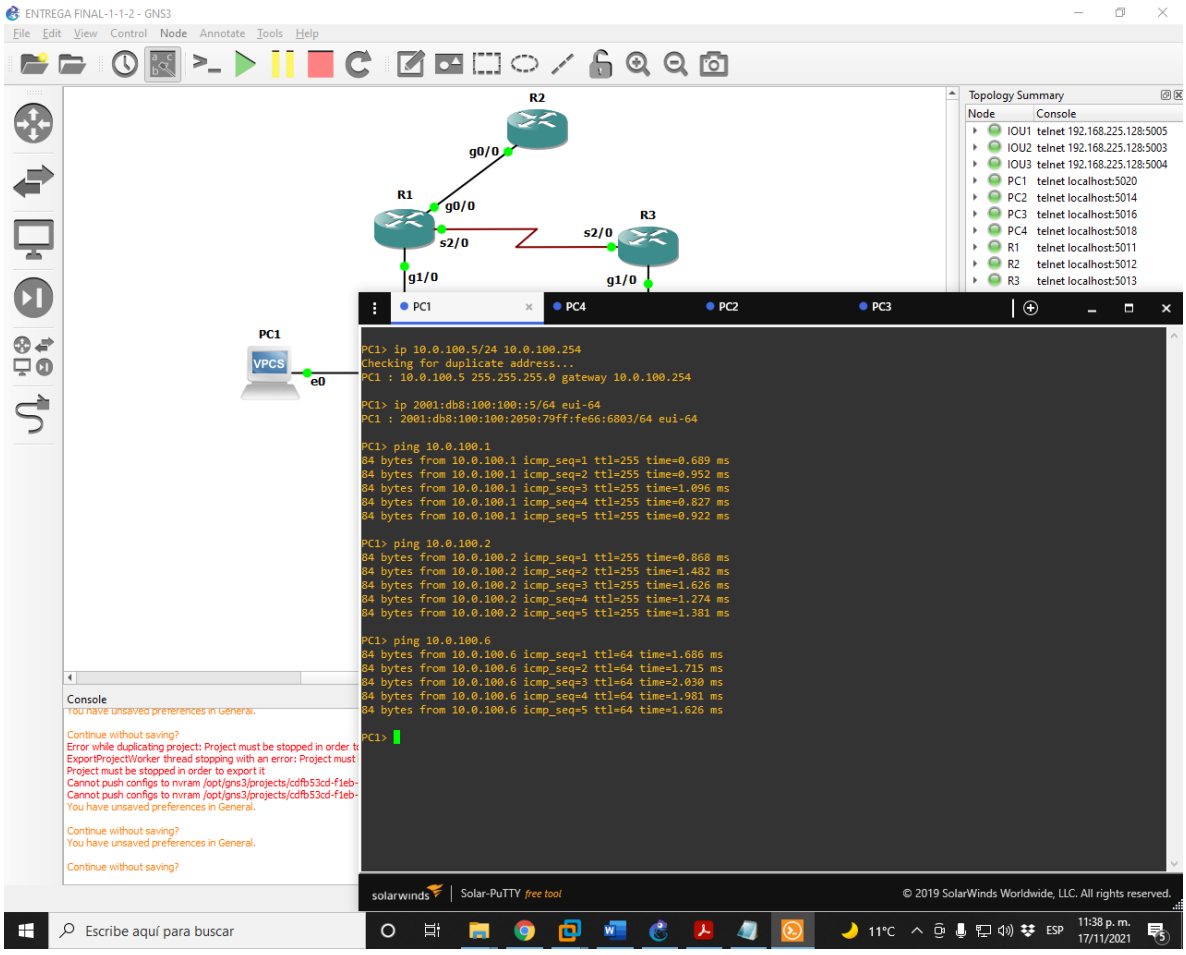
PC1 hace ping con éxito a:

D1: 10.0.100.1

D2: 10.0.100.2

PC4: 10.0.100.6

Figura 5. Verificación de conectividad desde PC1

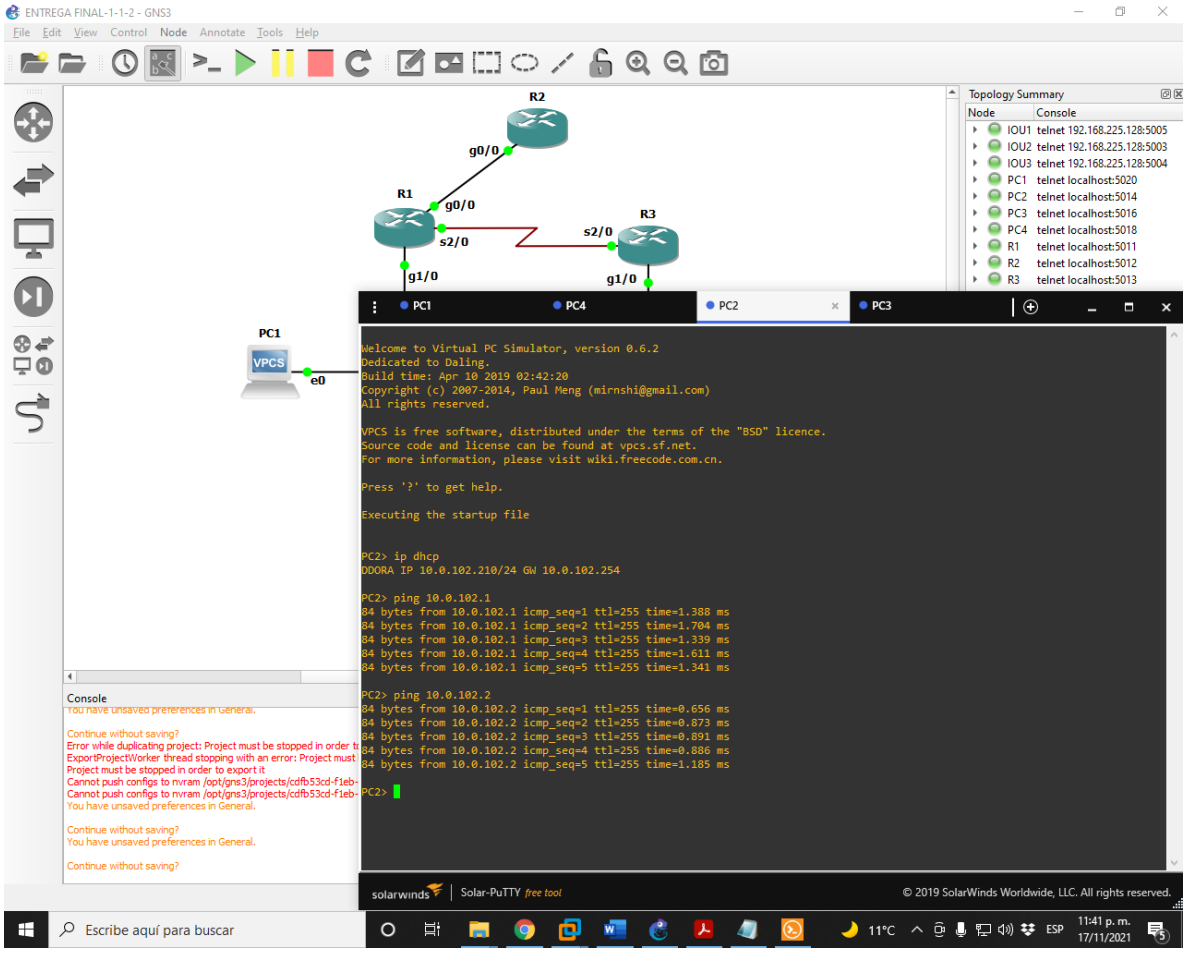


PC2 hace ping con éxito a:

D1: 10.0.102.1

D2: 10.0.102.2

Figura 6. Verificación de conectividad desde PC2

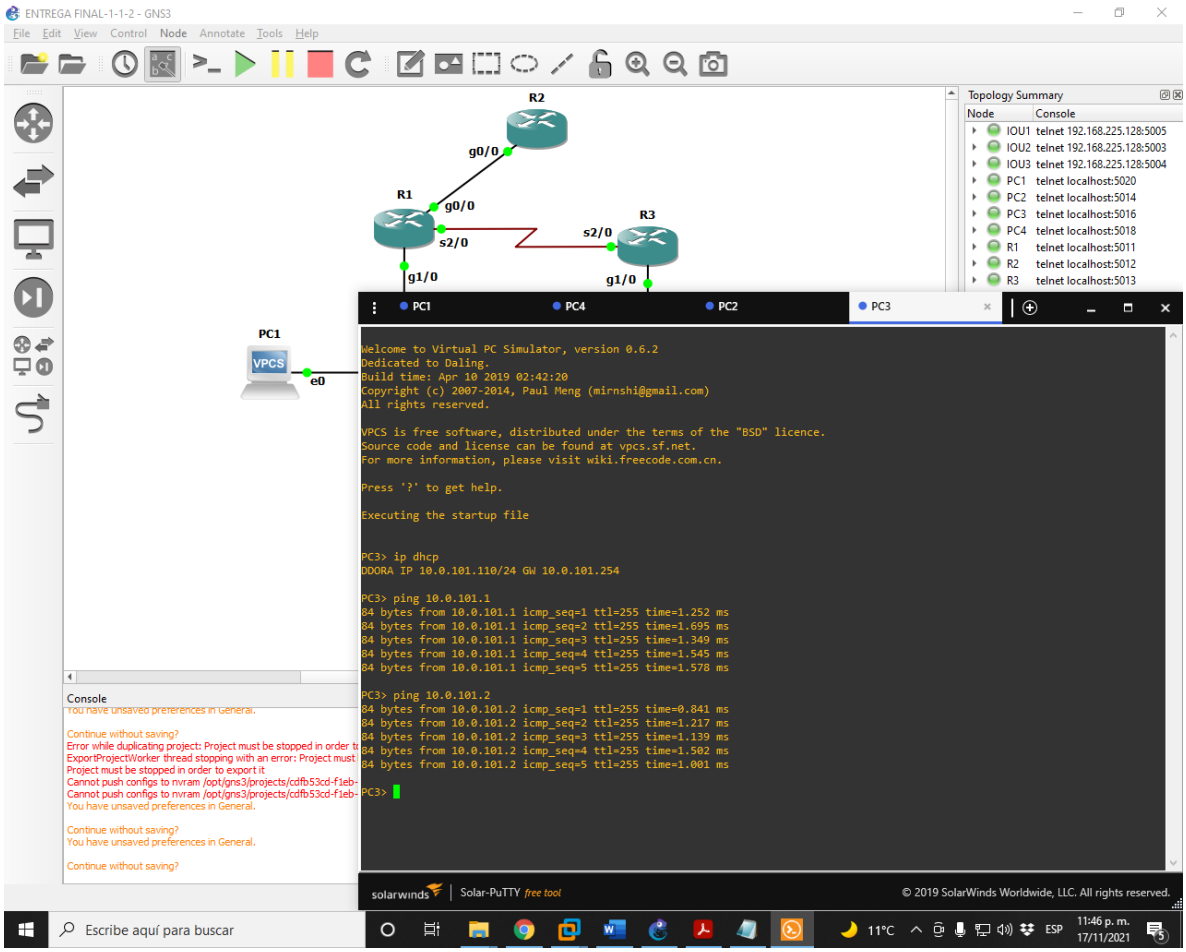


PC3 hace ping con éxito a:

D1: 10.0.101.1

D2: 10.0.101.2

Figura 7. Verificación de conectividad desde PC3



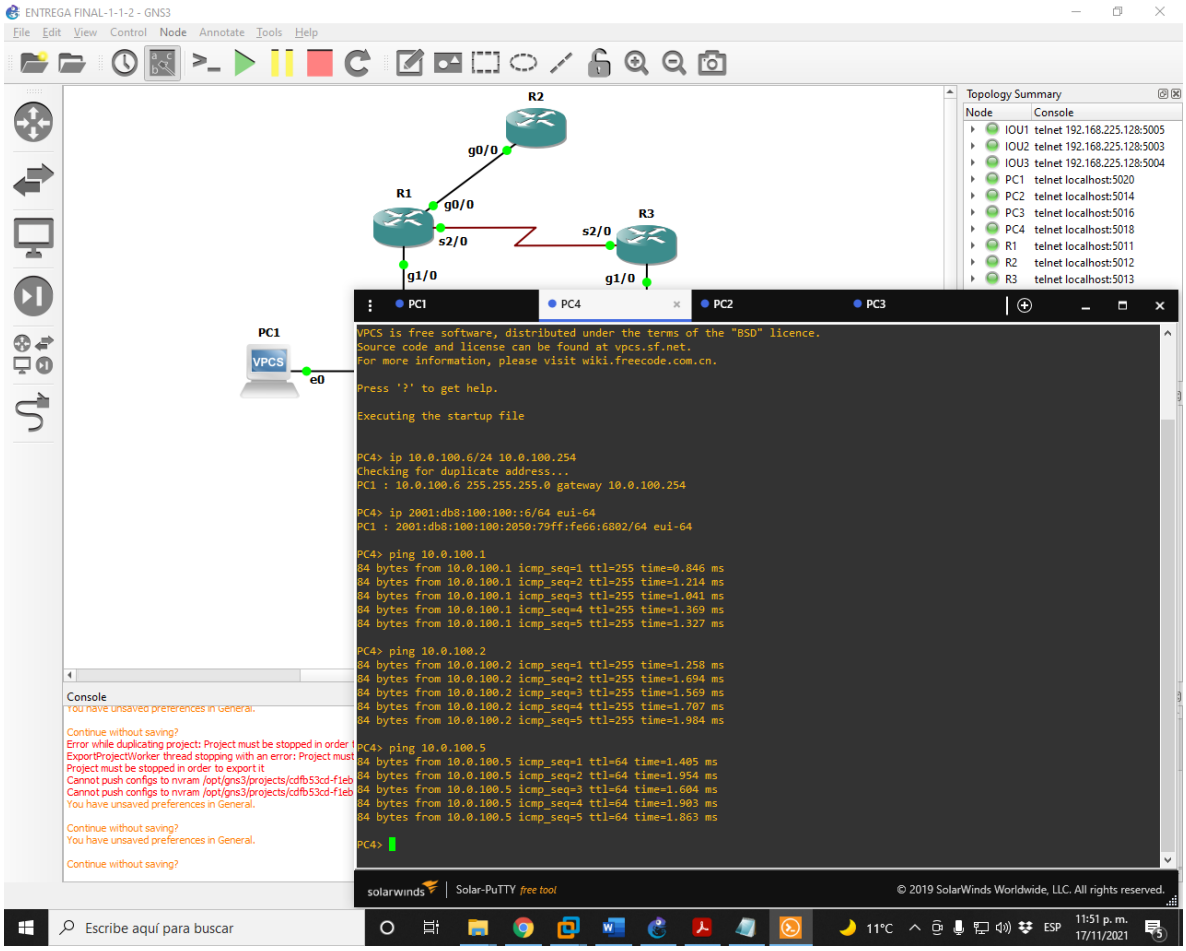
PC4 hace ping con éxito a:

D1: 10.0.100.1

D2: 10.0.100.2

PC1: 10.0.100.5

Figura 8. Verificación de conectividad desde PC4



PARTE 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

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

Las tareas de configuración son las siguientes:

Tabla 3. Actividades por desarrollar en la Parte 3

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

Solución 3.1

En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configuro single-area OSPFv2 en área 0. Uso OSPF Process ID 4 y asigno los siguientes router- IDs:

- R1: 0.0.4.1

```
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
```

- R3: 0.0.4.3

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

- D1: 0.0.4.131

```
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
```

- D2: 0.0.4.132

```
D2(config)#router ospf 4
D2(config-router)# router-id 0.0.4.132
```

En R1, R3, D1, y D2, verifico y anuncio todas las redes directamente conectadas / VLANs en Área 0 aplicando el comando #do show ip route connected

```
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0

R3(config-router)# network 10.0.11.0 0.0.0.255 area 0
R3(config-router)# network 10.0.13.0 0.0.0.255 area 0

D1(config-router)# network 10.0.100.0 0.0.0.255 area 0
```

```
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0
D1(config-router)# network 10.0.102.0 0.0.0.255 area 0
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0

D2(config-router)# network 10.0.100.0 0.0.0.255 area 0
D2(config-router)# network 10.0.101.0 0.0.0.255 area 0
D2(config-router)# network 10.0.102.0 0.0.0.255 area 0
D2(config-router)# network 10.0.11.0 0.0.0.255 area 0
```

- En R1, no publico la red R1 – R2.

La red R1-R2 corresponde a la dirección ip 209.165.200.224/27 y no la publico.

- En R1, propago una ruta por defecto. La ruta por defecto será provista por BGP.

```
R1(config-router)#default-information originate
```

Deshabilito las publicaciones OSPFv2 en:

- D1: todas las interfaces excepto e0/0

```
D1(config-router)# passive-interface default
D1(config-router)# no passive-interface e0/0
```

- D2: todas las interfaces excepto e0/0

```
D2(config-router)# passive-interface default
D2(config-router)# no passive-interface e0/0
```

Solución 3.2

En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configuro classic single-area OSPFv3 en área 0. Uso OSPF Process ID 6 y asigno los siguientes router-IDs:

- R1: 0.0.6.1

```
R1(config)#ipv6 router ospf 6
R1(config-rtr)# router-id 0.0.6.1
```

- R3: 0.0.6.3

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)# router-id 0.0.6.3
```

- D1: 0.0.6.131

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)# router-id 0.0.6.131
```

- D2: 0.0.6.132

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)# router-id 0.0.6.132
```

En R1, R3, D1, y D2, verifico y anuncio todas las redes directamente conectadas / VLANs en Área 0 utilizando el comando #show ipv6 route

```
R1(config)#interface g1/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit
R1(config)#interface s2/0
R1(config-if)# ipv6 ospf 6 area 0
R1(config-if)# exit

R3(config)#interface g1/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
R3(config)#interface s0/1/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit

D1(config-rtr)#interface e0/0
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#end
D1#
```

Anuncio redes en D2

```
D2(config-rtr)#interface e0/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#end
D2#
```

- En R1, no publico la red R1 – R2.

La red R1-R2 corresponde a la interfaz g0/0 y no la publico.

- En R1, propago una ruta por defecto. La ruta por defecto será provista por BGP.

```
R1(config-router)#default-information originate
```

Deshabilito las publicaciones OSPFv3 en:

- D1: todas las interfaces excepto e0/0

```
D1(config-router)# passive-interface default
D1(config-router)# no passive-interface e0/0
```

- D2: todas las interfaces excepto e0/0

```
D2(config-router)# passive-interface default
D2(config-router)# no passive-interface e0/0
```

Solución 3.3

En R2 en la “Red ISP”, configuro MP-BGP. Configuro dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada IPv4.

```
R2(config)#int loopback0
R2(config-if)#ip route 0.0.0.0 0.0.0.0 loopback 0
```

- Una ruta estática predeterminada IPv6.

```
R2(config-if)#ipv6 route ::/0 loopback 0
R2(config-if)#exit
```

Configuro R2 en BGP ASN 500 y uso el router-id 2.2.2.2.

```
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
```

Configuro y habilito una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

```
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
```

En IPv4 address family anuncio:

- La red Loopback 0 IPv4 (/32)

```
R2(config-router)#address-family ipv4
R2(config-router)#neighbor 209.165.200.225 activate
```

- La ruta por defecto (0.0.0.0/0)

```
R2(config-router)#no neighbor 2001:db8:200::1 activate network 2.2.2.2 mask 255.255.255.255 network 0.0.0.0
R2(config-router)#exit-address-family
```

En IPv6 address family, anuncio:

- La red Loopback 0 IPv4 (/128)

```
R2(config-router)#address-family ipv6
R2(config-router)#no neighbor 209.165.200.225 activate neighbor 2001:db8:200::1 activate
```

- La ruta por defecto (::/0)

```
R2(config-router)#network 2001:db8:2222::/128
```

R2(config-router)#network ::/0
R2(config-router)#exit-address-family

Solución 3.4

En R1 en la “Red ISP”, configuro MP-BGP. Configuro dos rutas resumen estáticas a la interfaz Null 0:

- Una ruta resumen IPv4 para 10.0.0.0/8.

R1(config)#ip route 10.0.0.0 255.0.0.0 null0

- Una ruta resumen IPv6 para 2001:db8:100::/48.

R1(config)#ipv6 route 2001:db8:100::/48 null0

Configuro R1 en BGP ASN 300 y uso el router-id 1.1.1.1
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1

Configuro una relación de vecino IPv4 e IPv6 con R2 en ASN 500.
En IPv4 address family:

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

- Habilito la relación de vecino IPv4.

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

- Deshabilito la relación de vecino IPv6.

R1(config-router)#no neighbor 2001:db8:200::2 activate network 10.0.0.0 mask 255.0.0.0

- Anuncio la red 10.0.0.0/8.

R1(config-router)#neighbor 209.165.200.226 activate

En IPv6 address family:

- Deshabilito la relación de vecino IPv4.

R1(config-router)#no neighbor 209.165.200.226 activate neighbor 2001:db8:200::2 activate

- Habilito la relación de vecino IPv6.

R1(config-router)#address-family ipv6 unicast

- Anuncio la red 2001:db8:100::/48.

R1(config-router)#network 2001:db8:100::/48

R1(config-router)#exit-address-family

R1(config-router)#exit-address-family%BGP-5-ADJCHANGE:neighbor 209.165.200.226 Up

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 de la Compañía”.

Las tareas de configuración son las siguientes:

Tabla 4. Actividades por desarrollar en la Parte 4

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. • Use la SLA número **4** para IPv4. • Use la SLA número **6** para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1G0/0/1 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 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 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 R3G0/0/1 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 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 estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
	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**.

4.3		• 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.

	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP versión 2. Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. 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.

Solución 4.1

En D1, implemento IP SLAs que prueben la accesibilidad de la interfaz R1 G1/0.

Creo dos IP SLAs

- Configuro la SLA número 4 para IPv4.
- Configuro la SLA número 6 para IPv6.

```
D1#en
D1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D1(config)#ip sla 4
D1(config)#ip sla 6
```

Las IP SLAs probarán la disponibilidad de la interfaz R1 G1/0 cada 5 segundos. Programo la SLA para una implementación inmediata sin tiempo de finalización. Creo una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

```
D1(config)#ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
D1(config)#ip sla 6
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
```

- Configuro el número de rastreo 4 para la IP SLA 4.
- Configuro el número de rastreo 6 para la IP SLA 6.

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

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

```
D1(config)#track 4 ip sla 4
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
```

Solución 4.2

En D2, implemento IP SLAs que prueben la accesibilidad de la interfaz R3 G1/0.

Creo IP SLAs.

- Configuro la SLA número 4 para IPv4.
- Configuro la SLA número 6 para IPv6.

```
D2#
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D2(config)#ip sla 4
D2(config)#ip sla 6
```

Las IP SLAs probarán la disponibilidad de la interfaz R3 G1/0 cada 5 segundos. Programo la SLA para una implementación inmediata sin tiempo de finalización. Creo una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.

```
D2(config)#ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)#exit
```

- Configuro el número de rastreo 4 para la IP SLA 4.
- Configuro el número de rastreo 6 para la IP SLA 6.

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

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

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

Solución 4.3

En D1 configuro HSRPv2.

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

Configuro HSRP versión 2.

```
D1(config)#interface vlan 100
D1(config-if)# standby version 2
D1(config)#interface vlan 102
D1(config-if)# standby version 2
```

Configuro IPv4 HSRP grupo 104 para la VLAN 100:

- Asigno la dirección IP virtual 10.0.100.254.
- Establezco la prioridad del grupo en 150.
- Habilito la preferencia (preemption).
- Rastreo el objeto 4 y decremento en 60.

```
D1(config-if)# standby 104 ip 10.0.100.254
D1(config-if)# standby 104 priority 150
D1(config-if)# standby 104 preempt
D1(config-if)# standby 104 track 4 decrement 60
```

Configuro IPv4 HSRP grupo 114 para la VLAN 101:

- Asigno la dirección IP virtual 10.0.101.254.
- Habilito la preferencia (preemption).
- Rastreo el objeto 4 para disminuir en 60.

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

Configuro IPv4 HSRP grupo 124 para la VLAN 102:

- Asigno la dirección IP virtual 10.0.102.254.
- Establezco la prioridad del grupo en 150.
- Habilito la preferencia (preemption).

- Rastreo el objeto 4 para disminuir en 60.

```
D1(config-if)# standby 124 ip 10.0.102.254
D1(config-if)# standby 124 priority 150
D1(config-if)# standby 124 preempt
D1(config-if)# standby 124 track 4 decrement 60
```

Configuro IPv6 HSRP grupo 106 para la VLAN 100:

- Asigno la dirección IP virtual usando ipv6 autoconfig.
- Establezco la prioridad del grupo en 150.
- Habilito la preferencia (preemption).
- Rastreo el objeto 6 y decremento en 60.

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

Configuro IPv6 HSRP grupo 116 para la VLAN 101:

- Asigno la dirección IP virtual usando ipv6 autoconfig.
- Habilito la preferencia (preemption).
- Registro el objeto 6 y decremento en 60.

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

Configuro IPv6 HSRP grupo 126 para la VLAN 102:

- Asigno la dirección IP virtual usando ipv6 autoconfig.
- Establezco la prioridad del grupo en 150.
- Habilito la preferencia (preemption).
- Rastreo el objeto 6 y decremento en 60.

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

En D2, configuro HSRPv2.

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

Configuro HSRP version 2.

```
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config)#interface vlan 101
D2(config-if)# standby version 2
D2(config)#interface vlan 102
D2(config-if)# standby version 2
```

Configuro IPv4 HSRP grupo 104 para la VLAN 100:

- Asigno la dirección IP virtual 10.0.100.254.
- Habilito la preferencia (preemption).
- Rastreo el objeto 4 y decremento en 60.

```
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60
```

Configuro IPv4 HSRP grupo 114 para la VLAN 101:

- Asigno la dirección IP virtual 10.0.101.254.
- Establezco la prioridad del grupo en 150.
- Habilito la preferencia (preemption).
- Rastreo el objeto 4 para disminuir en 60.

```
D2(config-if)# standby 114 ip 10.0.101.254
D2(config-if)# standby 114 priority 150
D2(config-if)# standby 114 preempt
D2(config-if)# standby 114 track 4 decrement 60
```

Configuro IPv4 HSRP grupo 124 para la VLAN 102:

- Asigno la dirección IP virtual 10.0.102.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

```
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
```

D2(config-if)# standby 124 track 4 decrement 60

Configuro IPv6 HSRP grupo 106 para la VLAN 100:

- Asigno la dirección IP virtual usando ipv6 autoconfig.
- Habilito la preferencia (preemption).
- Rastreo el objeto 6 para disminuir en 60.

D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 106 track 6 decrement 60
D2(config-if)# exit

Configuro IPv6 HSRP grupo 116 para la VLAN 101:

- Asigno la dirección IP virtual usando ipv6 autoconfig.
- Establezco la prioridad del grupo en 150.
- Habilito la preferencia (preemption).
- Rastreo el objeto 6 para disminuir en 60.

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

Configuro IPv6 HSRP grupo 126 para la VLAN 102:

- Asigno la dirección IP virtual usando ipv6 autoconfig.
- Habilito la preferencia (preemption).
- Rastreo el objeto 6 para disminuir en 60.

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

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. Actividades por desarrollar en la Parte 5

Tarea #	**Tarea**	**Especificación**
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.

5.6	Verifique el servicio AAA en todos losdispositivos (excepto R2).	Cierre e inicie sesión en todos los dispositivos (excepto R2) con el usuario: **raduser** y lacontraseña: **upass123**.

Solución 5.1

En todos los dispositivos, protejo el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

Contraseña: cisco12345cisco

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

Solución 5.2

En todos los dispositivos, creo un usuario local y lo protejo usando el algoritmo de encripción SCRYPT.

Detalles de la cuenta encriptada SCRYPT:

Nombre de usuario Local: sadmin
Nivel de privilegio 15
Contraseña: cisco12345cisco

R1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

A1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

Solución 5.3

En todos los dispositivos (excepto R2),habilito AAA.

R1(config)#aaa new-model

R3(config)#aaa new-model

D1(config)#aaa new-model

D2(config)#aaa new-model

A1(config)#aaa new-model

Solución 5.4

En todos los dispositivos (excepto R2), configuro 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

R1(config)#radius server RADIUS
R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $trongPass
R1(config-radius-server)# exit

R3(config)#radius server RADIUS
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass

```
R3(config-radius-server)# exit

D1(config)#radius server RADIUS
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $trongPass
D1(config-radius-server)# exit

D2(config)#radius server RADIUS
D2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)# key $trongPass
D2(config-radius-server)# exit

A1(config)#radius server RADIUS
A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $trongPass
A1(config-radius-server)# exit
```

Solución 5.5

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

Especificaciones de autenticación AAA:

- Rastreo el objeto 6 para disminuir en 60.
- Uso la lista de métodos por defecto.
- Valido contra el grupo de servidores RADIUS.
- De lo contrario, utilizo la base de datos local.

```
R1(config)#aaa authentication login default group radius local
R1(config)#username raduser password upass123
R1(config)#end

R3(config)#aaa authentication login default group radius local
R3(config)#username raduser password upass123
R3(config)#end

D1(config)#aaa authentication login default group radius local
D1(config)#username raduser password upass123
D1(config)#end

D2(config)#aaa authentication login default group radius local
D2(config)#username raduser password upass123
```

D2(config)#end

A1(config)#aaa authentication login default group radius local
A1(config)#username raduser password upass123
A1(config)#end

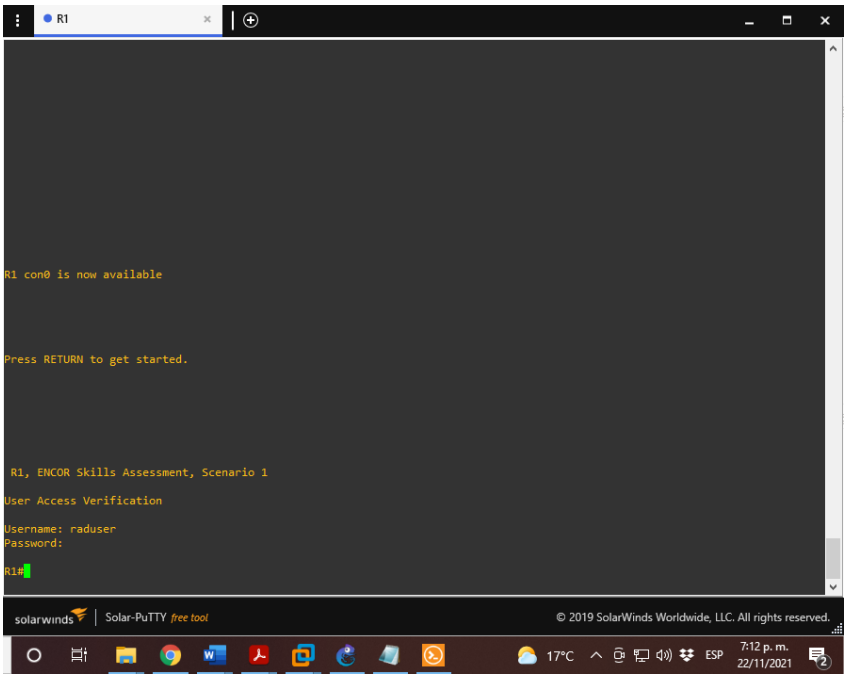
Solución 5.6

Verifico el servicio AAA en todos los dispositivos (excepto R2).

Cierro e inicio sesión en todos los dispositivos (excepto R2) con el usuario: raduser y la contraseña: upass123.

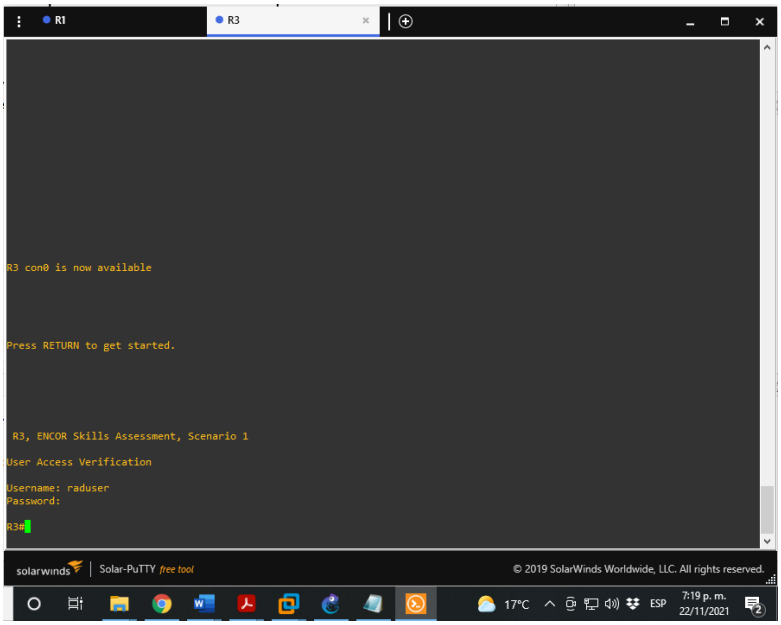
Para R1

Figura 9. Verificación del servicio AAA en R1



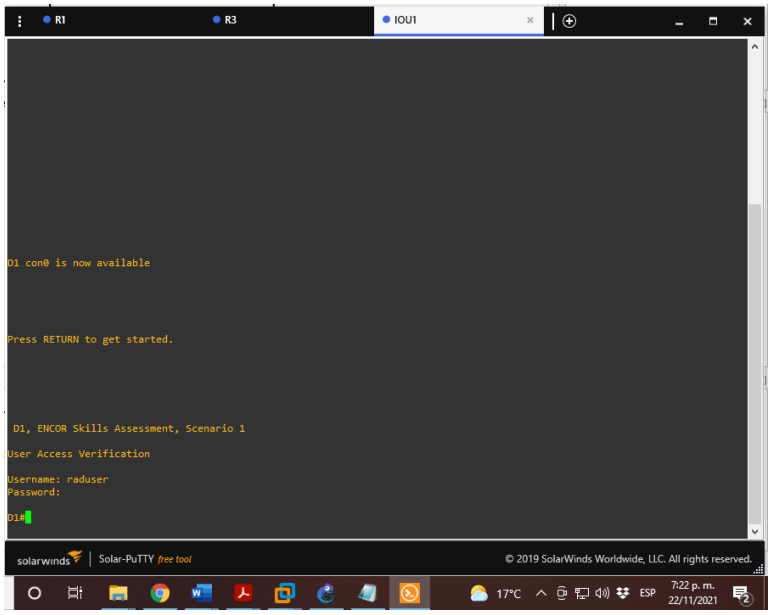
Para R3

Figura 10. Verificación del servicio AAA en R3



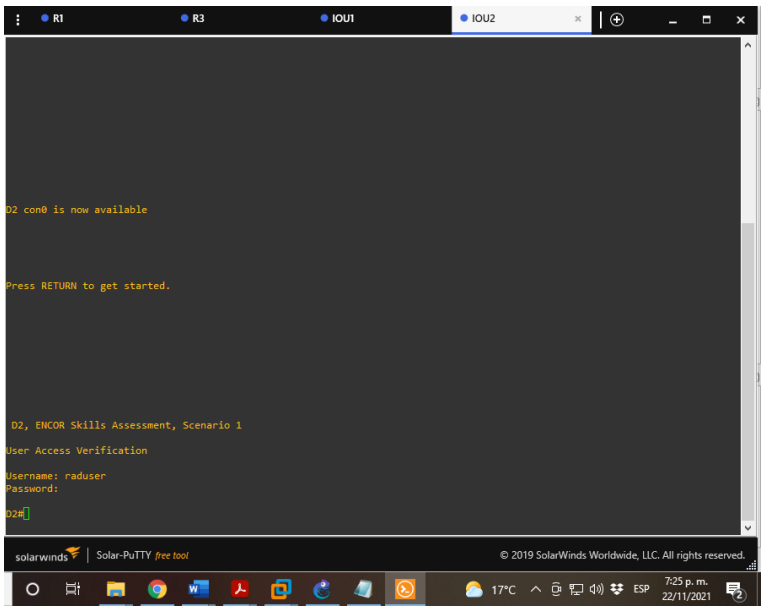
Para D1

Figura 11. Verificación del servicio AAA en D1



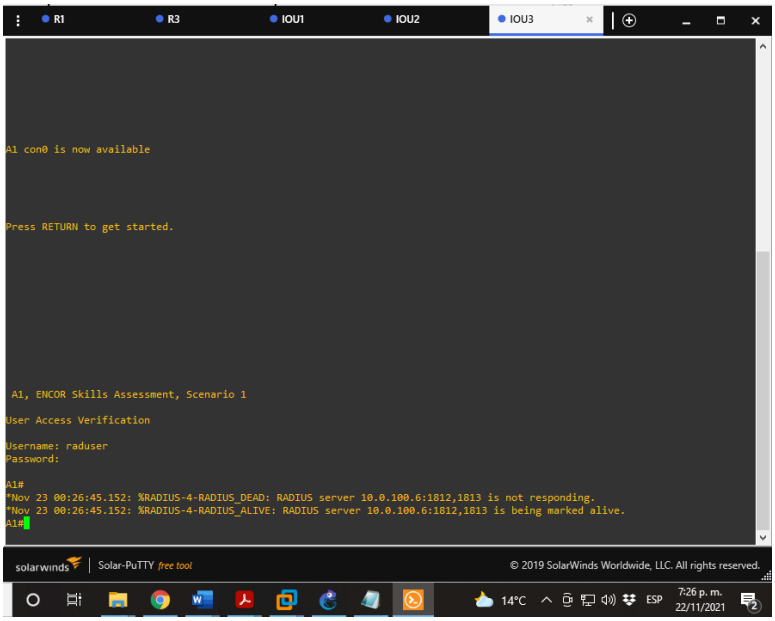
Para D2

Figura 12. Verificación del servicio AAA en D2



Para A1

Figura 13. Verificación del servicio AAA en A1



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. Actividades por desarrollar en la Parte 6

Tarea #	**Tarea**	**Especificación**
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTPmaestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2,y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos losdispositivos 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 laPC1. • Configure el valor de contacto SNMP con su nombre. • 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.

Solución 6.1

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

R1#clock set 20:56:00 November 11 2021

R2#clock set 20:56:00 November 11 2021

R3#clock set 20:56:00 November 11 2021

D1#clock set 20:56:00 November 11 2021

D2#clock set 20:56:00 November 11 2021

D3#clock set 20:56:00 November 11 2021

A1#clock set 20:56:00 November 11 2021

Solución 6.2

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

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

Solución 6.3

Configuro NTP en R1, R3, D1, D2 y A1.

Configuro 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.

R1(config)#ntp server 2.2.2.2

R3(config)#ntp server 10.0.10.1

D1(config)#ntp server 10.0.10.1

D2(config)#ntp server 10.0.10.1

A1(config)#ntp server 10.0.10.1

Solución 6.4

Configuro Syslog en todos los dispositivos excepto R2

Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

```
R1(config)# logging trap warning
R1(config)# logging host 10.0.100.5
R1(config)# logging on
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)#  permit host 10.0.100.5
R1(config-std-nacl)#  exit

R3(config)# logging trap warning
R3(config)# logging host 10.0.100.5
R3(config)# logging on
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#  permit host 10.0.100.5
R3(config-std-nacl)#  exit

D1(config)# logging trap warning
D1(config)# logging host 10.0.100.5
D1(config)# logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#  permit host 10.0.100.5
D1(config-std-nacl)#  exit

D2(config)# logging trap warning
D2(config)# logging host 10.0.100.5
D2(config)# logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#  permit host 10.0.100.5
D2(config-std-nacl)#  exit

A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5
A1(config)# logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#  permit host 10.0.100.5
A1(config-std-nacl)#  exit
```

Solución 6.5

Configuro 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 PC 1.
- Configuro el valor de contacto SNMP con su nombre.
- Establezco el community string en **ENCORSA**.
- En R3, D1, y D2, habilito el envío de traps config y ospf.
- En R1, habilito el envío de traps bgp, config, y ospf.
- En A1, habilito el envío de traps config.

```
R1(config)# snmp-server contact Cisco Student
R1(config)# snmp-server community ENCORSA ro SNMP-NMS
R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)# snmp-server ifindex persist
R1(config)# snmp-server enable traps bgp
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps ospf
R1(config)#end

R3(config)# snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#end

D1(config)# snmp-server contact Cisco Student
D1(config)# snmp-server community ENCORSA ro SNMP-NMS
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps config
D1(config)# snmp-server enable traps ospf
D1(config)#end

D2(config)# snmp-server contact Cisco Student
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)# snmp-server enable traps config
```

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

A1(config)# snmp-server contact Cisco Student
A1(config)# snmp-server community ENCORSA ro SNMP-NMS
A1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)# snmp-server ifindex persist
A1(config)# snmp-server enable traps config
A1(config)# snmp-server enable traps ospf
A1(config)#end
```

CONCLUSIONES

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

Se evidencia la importancia del diseño y la implementación de una red escalable, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN; los comandos IOS de configuración avanzada en routers no solo se aplican en la solución del escenario actual, sino que funcionan en diferentes tipos de red con características similares.

La implementación del enrutamiento entre VLAN, junto con la configuración de las direcciones IP, enlaces troncales, subinterfaces, y la puerta de enlace, permiten comprobar que la conectividad es correcta en R1, R3, D1, D2, pues el envío y recepción de paquetes entre ellos fue exitoso, los dispositivos PC2 y PC3 son clientes DHCP y recibieron direcciones IPv4 válidas.

El presente escenario se trabajó inicialmente con el software Packet Tracer, logrando parcialmente la configuración solicitada, por lo tanto, se desarrolló nuevamente el escenario en el software GNS3, notando que este último cuenta con un nivel de simulación más privilegiado que procesa correctamente todos los comandos utilizados. Debido a este cambio, fue necesario utilizar versiones diferentes de equipos a las sugeridas, pero con la misma funcionalidad dentro de la red, los cambios principales se realizaron sobre las interfaces de cada dispositivo y el desarrollo del escenario completo en GNS3 fue exitoso.

BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Services. 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). Multicast. 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). QoS. 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

ICONTEC NORMA TECNICA COLOMBIANA – NTC 1486 (En línea), consultado octubre 2021)

http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf