# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NELSON RICARDO TORRES DE LEON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
SANTA MARTA
2021

# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NELSON RICARDO TORRES DE LEON

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
SANTA MARTA
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

SANTA MARTA, 29 de Noviembre de 2021

## AGRADECIMIENTOS

Primeramente, quiero agradecer a Dios por permitirme aprovechar la oportunidad de superarme académicamente, darme la fuerza y la voluntad para llevar acabo todo este proceso, a mi familia y amigos que me apoyaron a lo largo de mi proceso académico, que en muchas ocasiones comprendieron mi esfuerzo y me dieron ánimos para seguir adelante, a cada uno de los tutores que me brindaron su ayuda en mi formación profesional, a mis compañeros de trabajo que me brindaron acompañamiento en momentos complejos y todos aquellos que me impulsaron en algún momento determinado.

**CONTENIDO**

## LISTA DE TABLAS

## LISTA DE FIGURAS

## GLOSARIO

Red: Es un conjunto de equipos conectados mediante de cables, señales, ondas o cualquier otro medio de transporte de información, que comparten información, recursos y servicios, etc.

Enrutamiento: Hace referencia al procedimiento de reenviar paquetes a través de las redes, siempre buscando la mejor ruta.

DHCP: Hace referencia a la extensión del protocolo Bootstrap, que se utiliza para conectar dispositivos como terminales y workstation sin disco duro con un Bootserver, del cual adquieren su OS.

Protocolo: Son sintaxis o lenguajes de comunicación entre sistemas de información, que permiten a los diferentes sistemas tecnológicos, comunicarse entre sí.

Port-Security: Es cualidad o característica de los switches Cisco que les permite retener las direcciones MAC conectadas a cada puerto del dispositivo y permitir solamente a esas direcciones MAC comunicarse mediante de esa puerta del switch.

VLAN: Hace referencia a una Red LAN Virtual.

EtherChannel: Hace referencia a una tecnología desarrollada por Cisco constituida con los estándares 802.3 Full-Duplex y Fast Ethernet; permite la agrupación lógica de varios enlaces físicos Ethernet.

## RESUMEN

Por medio del desarrollo del siguiente trabajo se demostraran todos los conocimientos adquiridos a lo largo del diplomado de profundización donde a través del desarrollo del escenario propuesto y elaborado por CISCO en su programa de CCNP, se evidenciaran las configuraciones que se requieren para poder conectar las redes preestablecidas, implementando métodos de seguridad electrónica y protocolos de conexión que actualmente se implementan en el mercado a nivel global.

Todo el proceso de implementación y configuración se realizara mediante el software GNS3, ya que permite realizar una simulación idónea de una red con todas sus funciones y características, haciendo posible configurar plataformas de conmutación basadas en switches, mediante el uso de protocolos como STP y la configuración de VLANs en escenarios de red corporativos, para comprender el modo de operación de las subredes y los beneficios de administrar dominios de transmisión independientes, en múltiples escenarios al interior de una red jerárquica convergente. También permite usar comandos IOS de configuración avanzada en routers (con direccionamiento IPv4 e IPv6) para protocolos de enrutamiento como: OSPF, EIGRP y BGP, en entornos de direccionamiento sin clase, con el fin diseñar e implementar soluciones de red escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes LAN y WAN.



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

## ABSTRACT

Through the development of the following work, the knowledge acquired throughout the in-depth diploma will be demonstrated where, through the development of the scenario proposed and elaborated by CISCO in its CCNP program, the configurations that are required to connect the pre-established networking will be evidenced. , implementing electronic security methods and connection protocols that are currently implemented in the global market.
The entire implementation and configuration process is carried out using the GNS3 software, since it allows an ideal simulation of a network with all its functions and characteristics, making it possible to configure switching platforms based on switches, through the use of protocols such as STP and the VLAN configuration in corporate network scenarios, to understand the operation mode of the subnets and the benefits of managing independent transmission domains, in multiple scenarios within a hierarchical converged network. It also allows the use of advanced configuration IOS commands in routers (with IPv4 and IPv6 addressing) for routing protocols such as: OSPF, EIGRP and BGP, in classless addressing environments, in order to design and implement scalable network solutions, by using of the principles of routing and packet switching in LAN and WAN environments.



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

# INTRODUCCIÓN

Hoy en día, debido a la gran cantidad de información que manejan las diferentes organizaciones, se ha hecho necesario crear sistemas que puedan gestionar y procesar toda estos datos, es por ello que se implementan redes de todas las clases, dependiendo de las necesidades particulares de cada una de las organizaciones. Por tal motivo, se hace necesario que las personas estén capacitadas para desarrollar, diseñar, implementar, configurar y gestionar estos sistemas de información, la Universidad Nacional Abierta y a Distancia, permite la realización de diferentes cursos académicos que hacen posible el desarrollo de estas habilidades y competencias. Este es el caso del Diplomado de Profundización CISCO CCNP, el cual nos permite desarrollar muchas de las cualidades anteriormente mencionadas y llevar acabo todo lo necesario.

Mediante el uso de herramientas de simulación en los escenarios propuestos, protocolos de administración de redes para la solución de problemas, evaluación de desempeños de routers y switches, además, de enseñarnos el diseño de políticas de enrutamiento estático y/o dinámico bajo un esquema de direccionamiento IP, entre otras cosas.

Por ende, se desarrolló un Proyecto aplicado que consiste en un escenario propuesto por el tutor, mostrando el paso a paso con su respectiva evidencia, además, de la simulación en el software Packet Tracer. Las evidencias se basan en describir cada fase, configurar de manera correcta cada uno de los dispositivos de la red, en el simulador y evidenciarlo en el trabajo final. Se detallan las respectivas configuraciones que se hacen en cada dispositivo, los comandos que se utilizan para evidenciar el correcto desarrollo de los diferentes puntos requeridos por la guía, dejando claridad adicional con imágenes del uso del software GNS3.

## DESARROLLO

### ESCENARIO 1

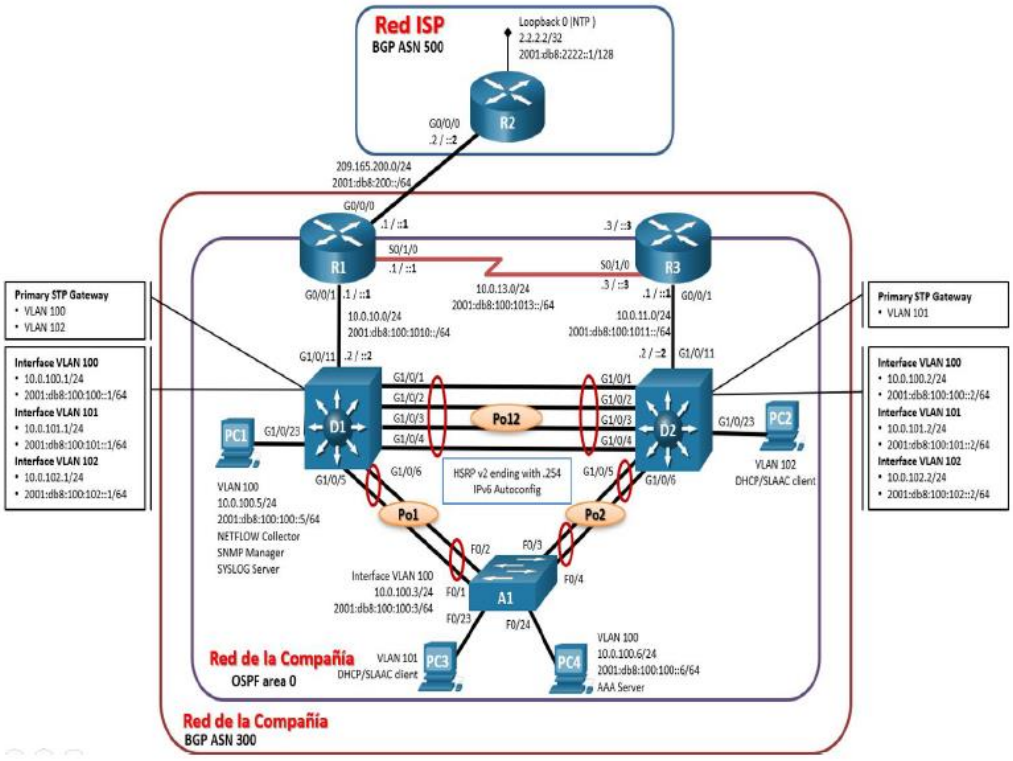


*Figura 1 - Escenario 1 – Topología de la Red*

## 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 | 10.0.100.3/23 | 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 |

*Tabla 1 - Tabla de direccionamiento*

## Objetivos

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
Part 2: Configurar la capa 2 de la red y el soporte de Host
Part 3: Configurar los protocolos de enrutamiento
Part 4: Configurar la redundancia del primer salto (**no se entrega aún)
Part 5: Configurar la seguridad (**no se entrega aún)
Part 6: Configurar las características de administración de red (** no se entrega aún)

## 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 Compañia" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

**Nota:** Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers 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 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
• 2 Switches (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.

**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.
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**

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0
ip address 209.165.200.225 255.255.255.224
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown
exit
interface g1/0
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s2/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
```

```
no shutdown
exit
```

**Router R2**

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

**Router R3**

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g1/0
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s2/0
ip address 10.0.13.3 255.255.255.0
```

```
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

**Switch D1**

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface e0/0
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
```

```
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
```

**Switch D2**

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
```

```
exit
interface e0/0
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
```

**Switch A1**

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
```

```
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
```

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.

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

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

Las tareas de configuración son las siguientes:

| 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:<br>• D1 and D2<br>• D1 and A1<br>• 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.<br>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 deapoyo mutuo en caso de falla del switch. |
| **Tarea#** | **Tarea** | **Especificación** |
| 2.5 | En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología. | Use los siguientes números de canales:<br>• D1 a D2 – Port channel 12<br>• D1 a A1 – Port channel 1<br>• 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, comose muestra en el diagrama de topología.<br>Los puertos de host deben pasar inmediatamente al estado de reenvío(forwarding). |
| 2.7 | Verifique los servicios DHCP IPv4. | PC2 y PC3 son clientes DHCP y debenrecibir direcciones IPv4 válidas. |

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

*Tabla 2 - Tarea Parte 2*

Los comandos para las configuraciones de cada dispositivo son los siguientes:

D1

```
interface range e1/0-3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
 channel-group 12 mode active
 no shutdown
 exit
interface range e2/0-1
 switchport trunk encapsulation dot1q
 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 e3/3
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
 no shutdown
 exit
end
```

D2

```
interface range e1/0-3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
 channel-group 12 mode active
 no shutdown
 exit
interface range e2/0-1
 switchport trunk encapsulation dot1q
 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 e3/3
 switchport mode access
 switchport access vlan 102
 spanning-tree portfast
 no shutdown
 exit
end
```

A1

```
spanning-tree mode rapid-pvst
interface range e0/0-1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
 channel-group 1 mode active
 no shutdown
 exit
interface range e0/2-3
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
 channel-group 2 mode active
 no shutdown
 exit
interface e1/0
 switchport mode access
 switchport access vlan 101
 spanning-tree portfast
 no shutdown
 exit
interface e1/1
 switchport mode access
 switchport access vlan 100
 spanning-tree portfast
 no shutdown
 exit
end
```

Podemos verificar la configuración de interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches, el cambio de la VLAN nativa en los enlaces troncales, la implementación del protocolo Rapid Spanning-Tree, la implementación de los puentes raíces para las VLANs apropiadas y la existencia de los EtherChannels LACP mediante el comando “show interfaces trunk” y el comando “show run | include spanning-tree” en D1, dando solución a los puntos 2.1, 2.2, 2.3, 2.4 y 2.5:

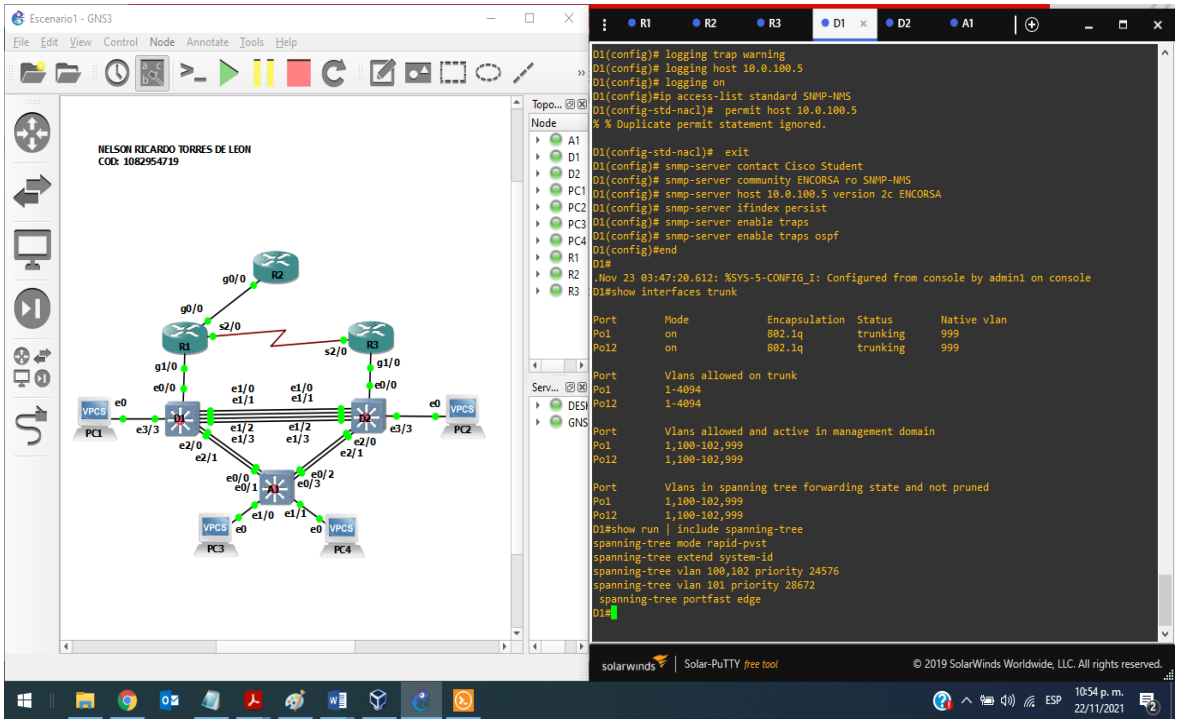


*Figura 2 - Evidencia 2a*

También mediante el comando “show run interface e3/3” en D1 se pueden verificar los puertos de acceso del host que se conectan a PC1, PC2, PC3 y PC4, dando solución al punto 2.6:

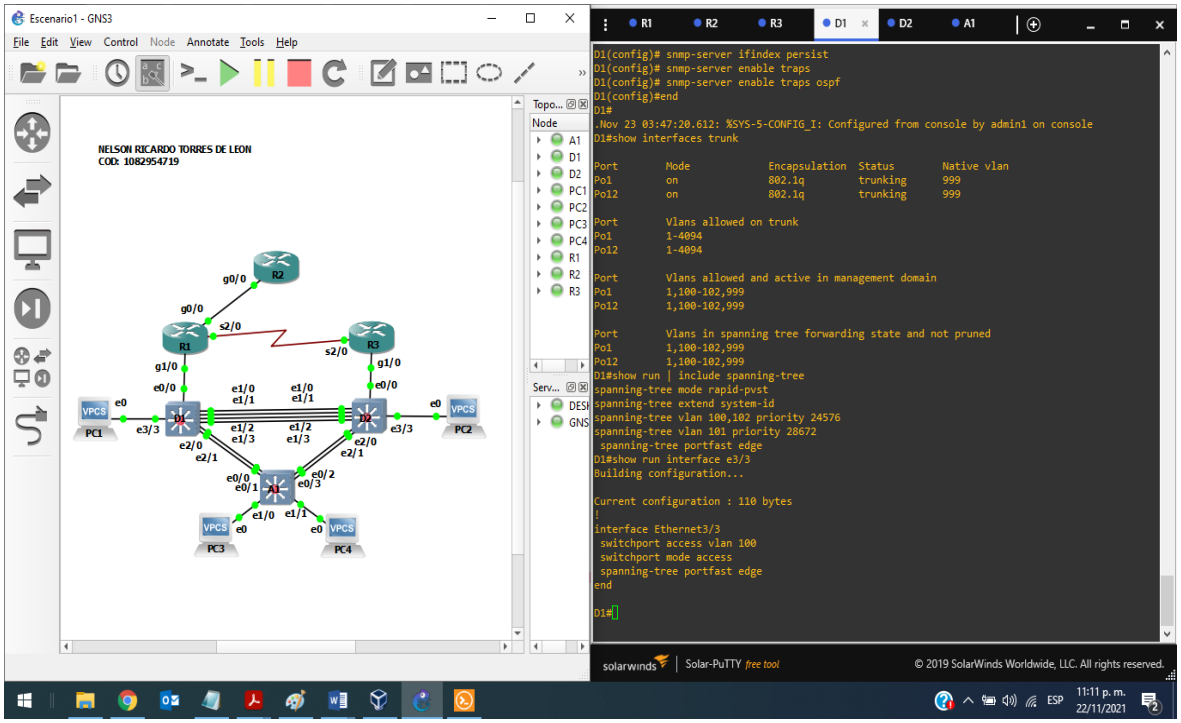


*Figura 3 - Evidencia 2b*

En D2 podemos verificar la misma configuración respectiva que en D1, mediante los comando “show interfaces trunk**”** y el comando “show run | include spanning-tree”, dando solución a los puntos 2.3, 2.4 y 2.5:

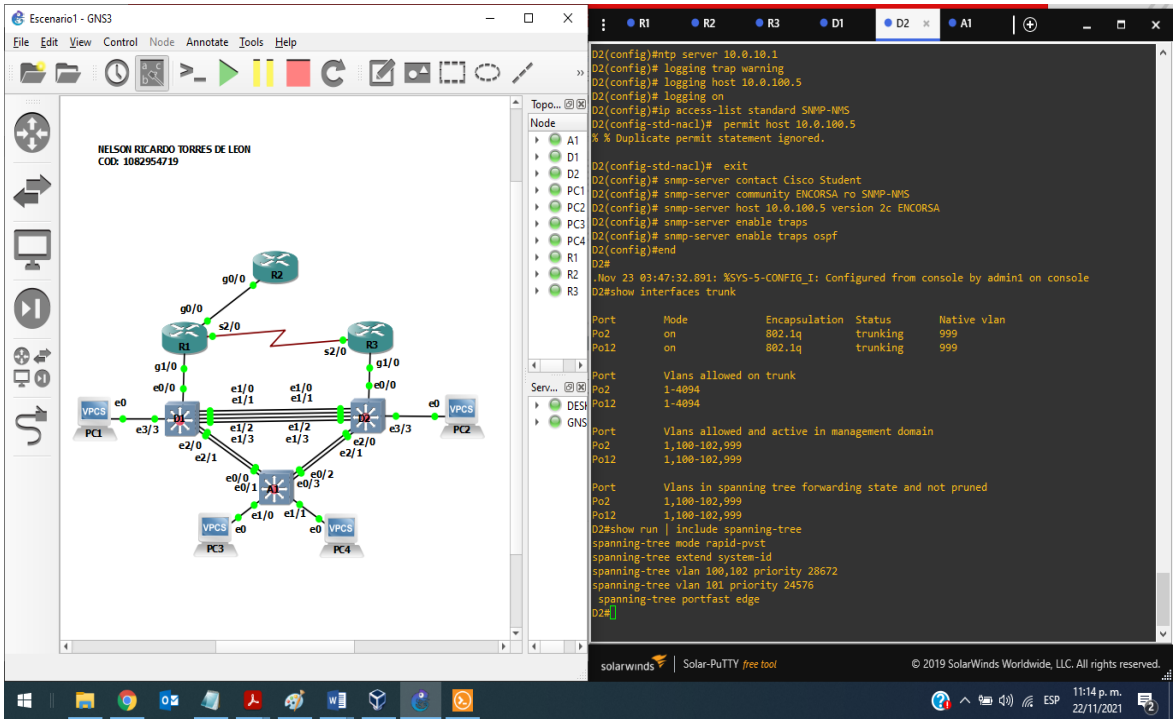


*Figura 4 - Evidencia 2c*

También mediante el comando “show run interface e3/3” en D2 se puede verificar la configuración de los puertos de acceso conectados a la VLAN, dando solución al punto 2.6:

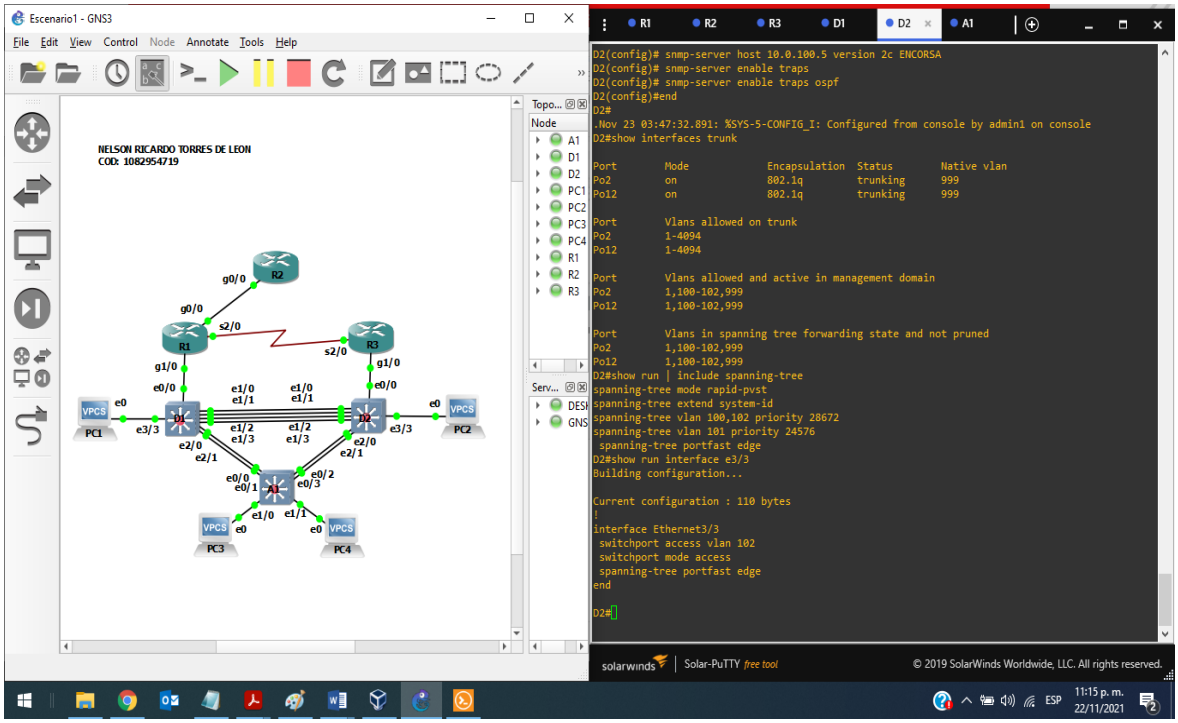


*Figura 5 - Evidencia 2d*

En A1 podemos verificar la configuración correcta mediante el comando “show run interface” para las interfaces e1/0 y e1/1 respectivamente:

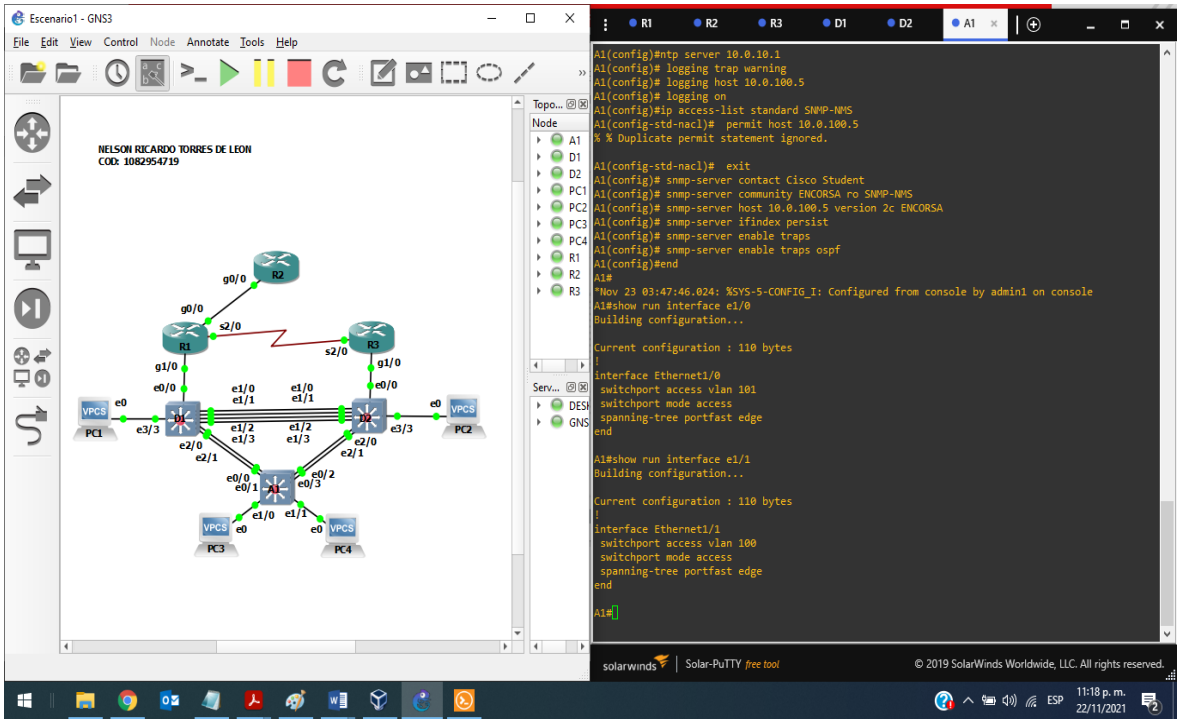


*Figura 6 - Evidencia 2e*

Las IPv4 DHCP en los PC2 y PC3 se verifican mediante el comando “show”, dando cumplimento al punto 2.7:

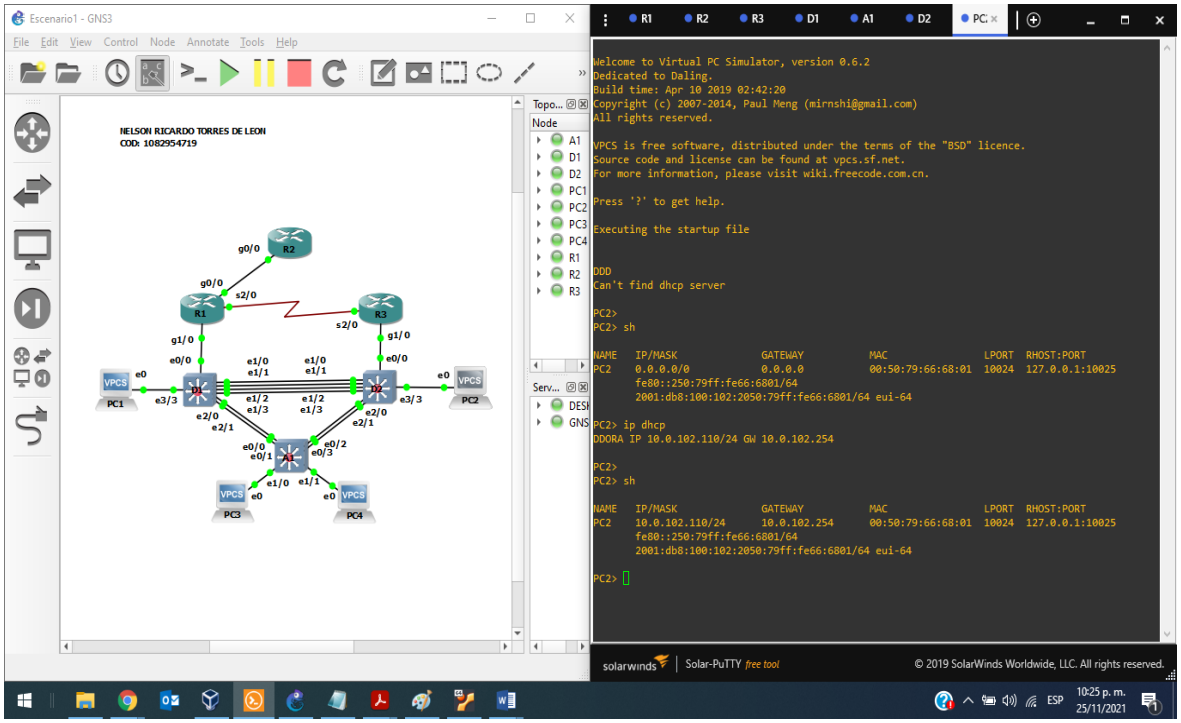


*Figura 7 - Evidencia 2f*

Haciendo ping desde PC1 a D1, D2 y PC4, podemos verificar que se cumple con las configuraciones y por ende con el punto 2.8:

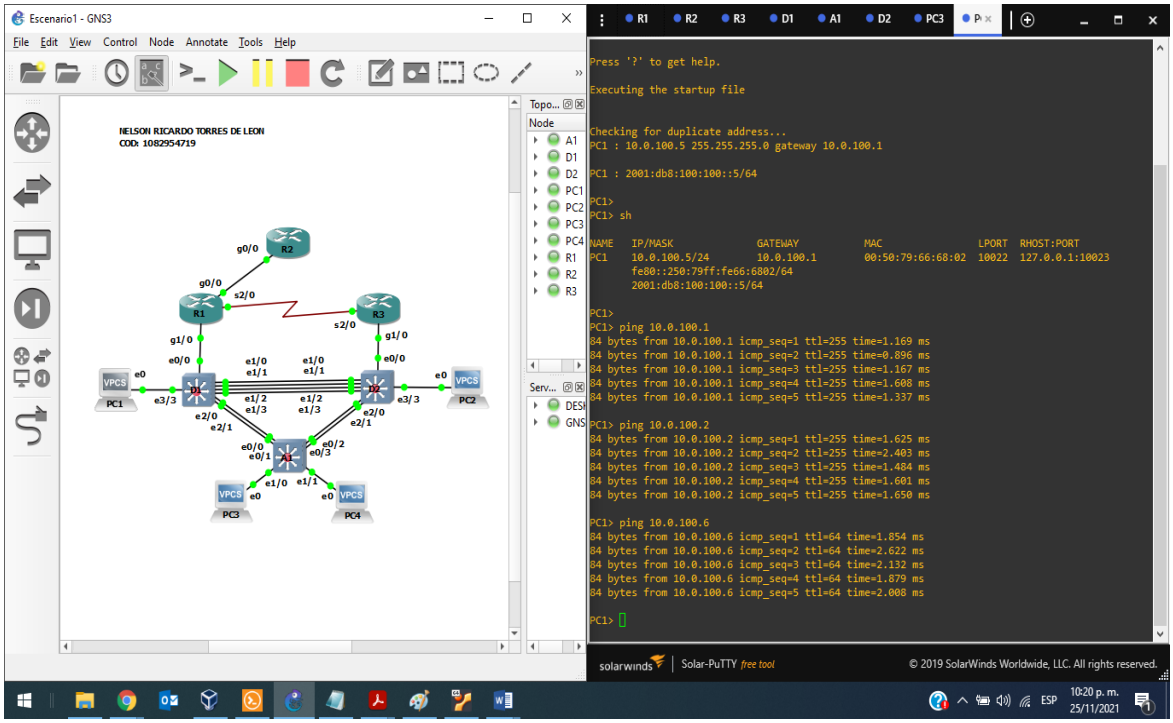


*Figura 8 - Evidencia 2g*

## Parte 3: Configurar los protocolos de enrutamiento

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

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

Las tareas de configuración son las siguientes:

| Tarea# | Tarea | Especificación |
|---|---|---|
| 3.1 | En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0. | Use OSPF Process ID **4** y asigne los siguientes router-IDs:<br>• R1: 0.0.4.1<br>• R3: 0.0.4.3<br>• D1: 0.0.4.131<br>• D2: 0.0.4.132<br>En R1, R3, D1, y D2, anuncie todas las redesdirectamente conectadas / VLANs en Area 0.<br>• En R1, no publique la red R1 – R2.<br>• En R1, propague una ruta por defecto. Note que laruta por defecto deberá ser provista por BGP.<br>Deshabilite las publicaciones OSPFv2 en:<br>• D1: todas las interfaces excepto G1/0/11<br>• 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:<br>• R1: 0.0.6.1<br>• R3: 0.0.6.3<br>• D1: 0.0.6.131<br>• D2: 0.0.6.132<br>En R1, R3, D1, y D2, anuncie todas las redesdirectamente conectadas / VLANs en Area 0.<br>• En R1, no publique la red R1 – R2.<br>• On R1, propague una ruta por defecto. Note que laruta por defecto deberá ser provista por BGP.<br>Deshabilite las publicaciones OSPFv3 en:<br>• D1: todas las interfaces excepto G1/0/11<br>• D2: todas las interfaces excepto G1/0/11 |
| **Tarea#** | **Tarea** | **Especificación** |

| | | |
|---|---|---|
| 3.3 | En R2 en la “Red ISP”, configure MP-BGP. | Configure dos rutas estáticas predeterminadas através de la interfaz Loopback 0:<br>• Una ruta estática predeterminada IPv4.<br>• Una ruta estática predeterminada IPv6.<br><br>Configure R2 en BGP ASN **500** y use el router-id2.2.2.2.<br><br>Configure y habilite una relación de vecino IPv4 e IPv6con R1 en ASN 300.<br><br>En IPv4 address family, anuncie:<br>• La red Loopback 0 IPv4 (/32).<br>• La ruta por defecto (0.0.0.0/0).<br><br>En IPv6 address family, anuncie:<br>• La red Loopback 0 IPv4 (/128).<br>• La ruta por defecto (::/0). |
| 3.4 | En R1 en la “Red ISP”, configure MP-BGP. | Configure dos rutas resumen estáticas a la interfazNull 0:<br>• Una ruta resumen IPv4 para 10.0.0.0/8.<br>• Una ruta resumen IPv6 para 2001:db8:100::/48.Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1.<br>Configure una relación de vecino IPv4 e IPv6 con R2en ASN 500.<br>En IPv4 address family:<br>• Deshabilite la relación de vecino IPv6.<br>• Habilite la relación de vecino IPv4.<br>• Anuncie la red 10.0.0.0/8.En IPv6 address family:<br>• Deshabilite la relación de vecino IPv4.<br>• Habilite la relación de vecino IPv6.<br>• Anuncie la red 2001:db8:100::/48. |

*Tabla 3 - Tarea Parte 3*

Para dar solución a estos requerimientos implementamos los siguientes comandos

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 g1/0
 ipv6 ospf 6 area 0
 exit
interface s2/0
 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 g1/0
 ipv6 ospf 6 area 0
 exit
interface s2/0
 ipv6 ospf 6 area 0
 exit
end
```

D1

```
router ospf 4
 router-id 0.0.4.131
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.101.0 0.0.0.255 area 0
 network 10.0.102.0 0.0.0.255 area 0
 network 10.0.10.0 0.0.0.255 area 0
 passive-interface default
 no passive-interface e0/0
 exit
ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
```

```
 no passive-interface e0/0
 exit
interface e0/0
 ipv6 ospf 6 area 0
 exit
interface vlan 100
 ipv6 ospf 6 area 0
 exit
interface vlan 101
 ipv6 ospf 6 area 0
 exit
interface vlan 102
 ipv6 ospf 6 area 0
 exit
end
```

D2

```
router ospf 4
 router-id 0.0.4.132
 network 10.0.100.0 0.0.0.255 area 0
 network 10.0.101.0 0.0.0.255 area 0
 network 10.0.102.0 0.0.0.255 area 0
 network 10.0.11.0 0.0.0.255 area 0
 passive-interface default
 no passive-interface e0/0
 exit
ipv6 router ospf 6
 router-id 0.0.6.132
 passive-interface default
 no passive-interface e0/0
 exit
interface e0/0
 ipv6 ospf 6 area 0
 exit
interface vlan 100
 ipv6 ospf 6 area 0
 exit
interface vlan 101
 ipv6 ospf 6 area 0
 exit
interface vlan 102
 ipv6 ospf 6 area 0
```

exit
end

Las configuraciones single-area OSPFv2 en area 0 y classic single-area OSPFv3 en area 0, realizadas en R1 se pueden corroborar con los comandos "show run | section ^router ospf", "show run | section ^ipv6 router" y "show ipv6 ospf interface brief", dando cumplimiento a los puntos 3.1 y 3.2:

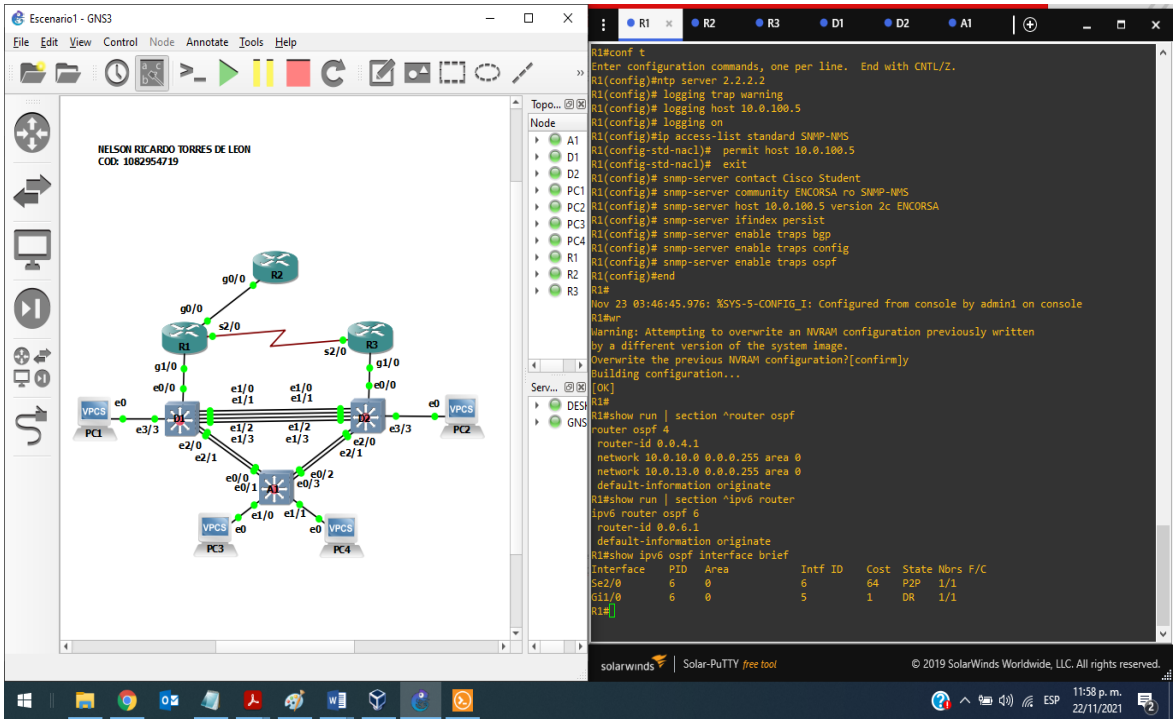


*Figura 9 - Evidencia 3a*

Las configuraciones single-area OSPFv2 en area 0 y classic single-area OSPFv3 en area 0, realizadas en R3 se pueden corroborar con los comandos "show run | section ^router ospf", "show run | section ^ipv6 router" y "show ipv6 ospf interface brief", dando cumplimiento a los puntos 3.1 y 3.2:

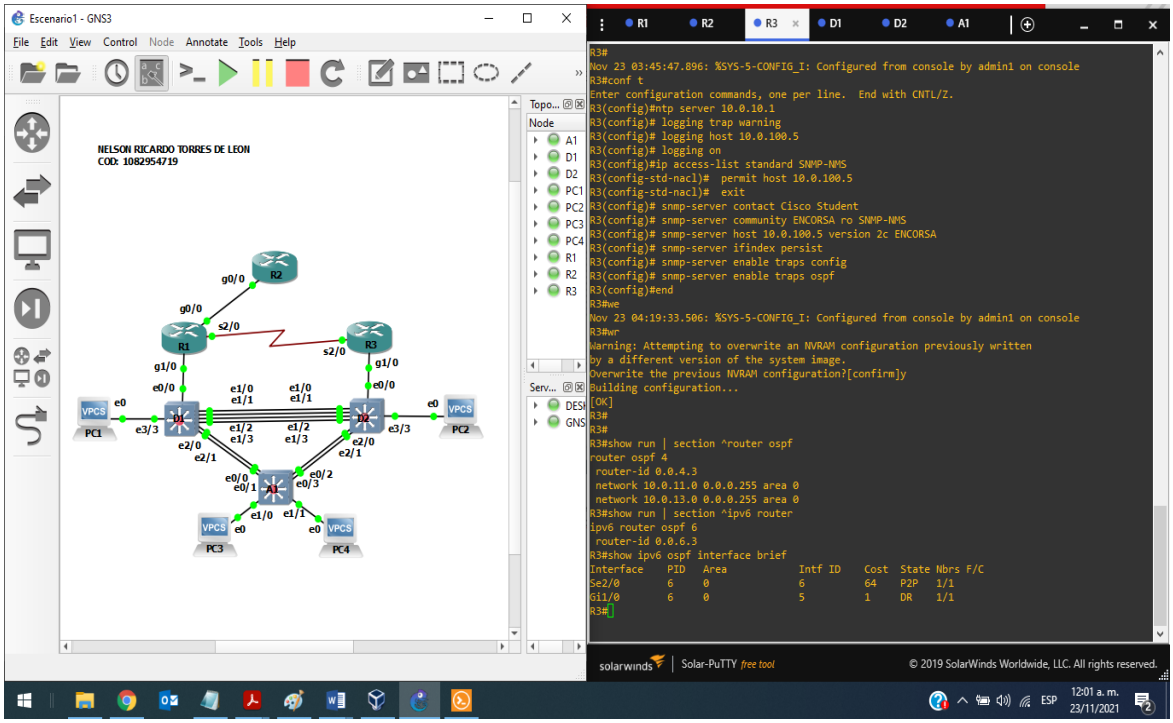


*Figura 10 - Evidencia 3b*

Las configuraciones single-area OSPFv2 en area 0 y classic single-area OSPFv3 en area 0, realizadas en D1 se pueden corroborar con los comandos “show run | section ^router ospf”, “show run | section ^ipv6 router” y “show ipv6 ospf interface brief”, dando cumplimiento a los puntos 3.1 y 3.2:

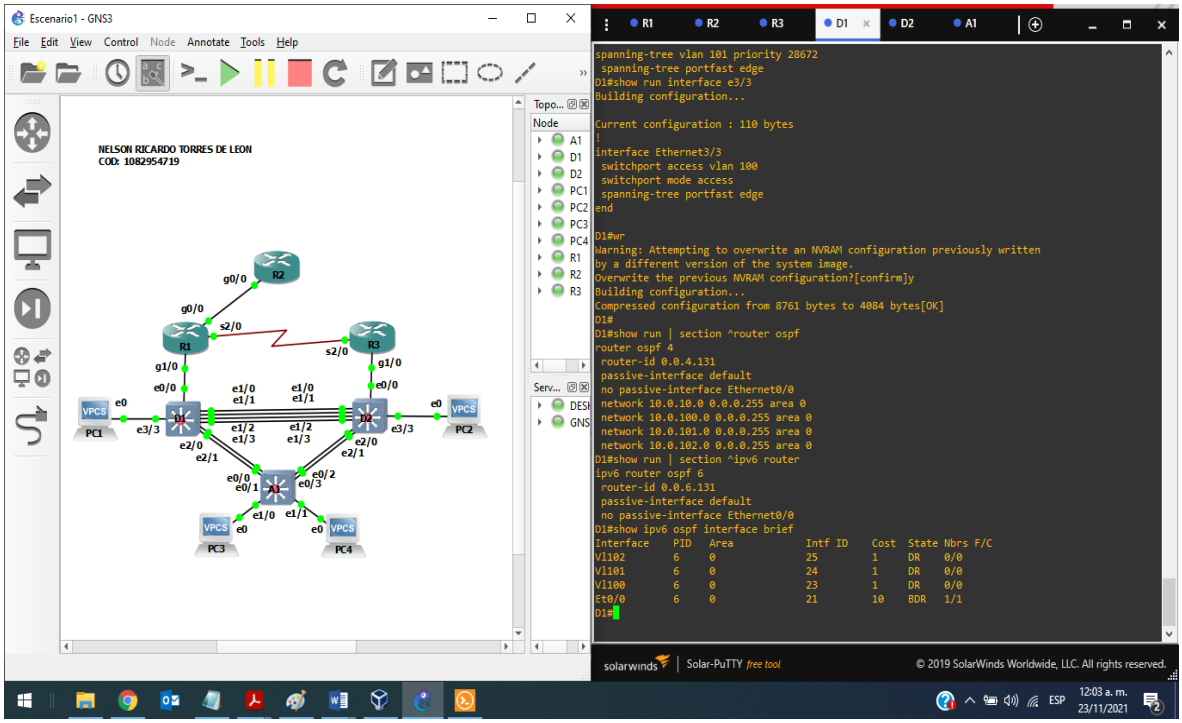


*Figura 11 - Evidencia 3c*

Las configuraciones classic single-area OSPFv3 en área 0, realizadas en D2 se pueden verificar con los comandos "show run | section ^router ospf", "show run | section ^ipv6 router" y "show ipv6 ospf interface brief", esto permite dar cumplimiento al punto 3.2:

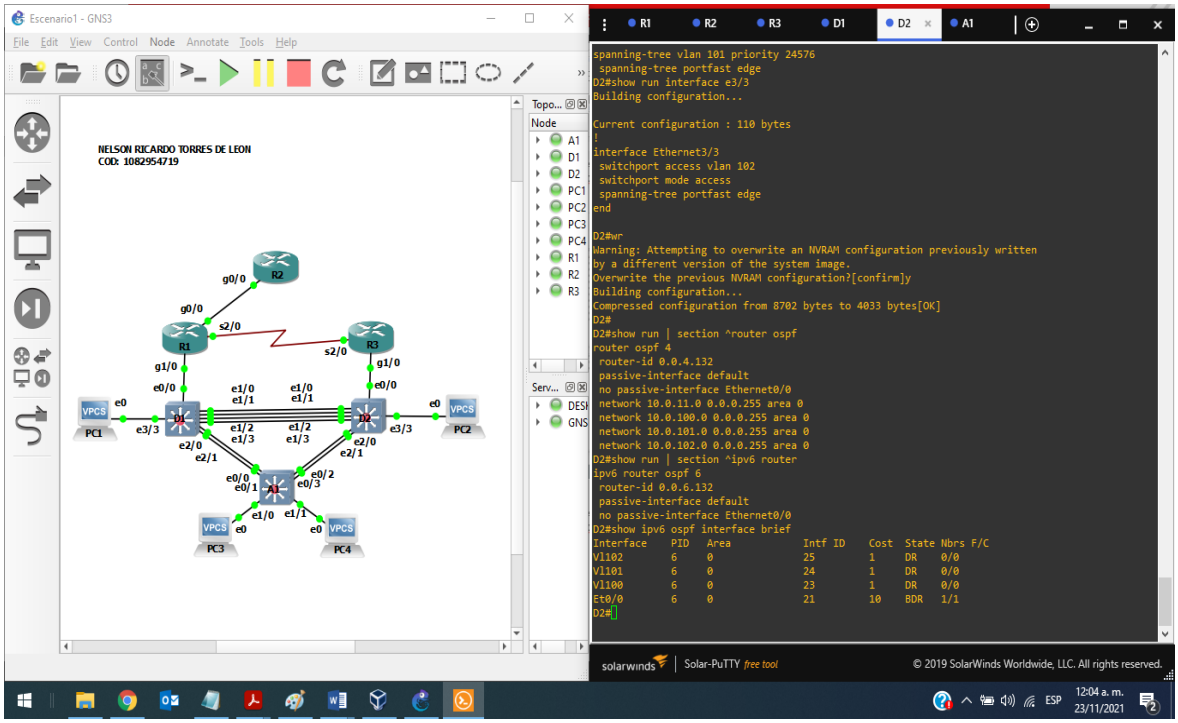


*Figura 12 - Evidencia 3d*

En cuanto a R2, podemos utilizar los comandos “show run | section bgp” y “show run | include route” respectivamente para verificar la configuración de MP-BGP, dando solución al punto 3.3:

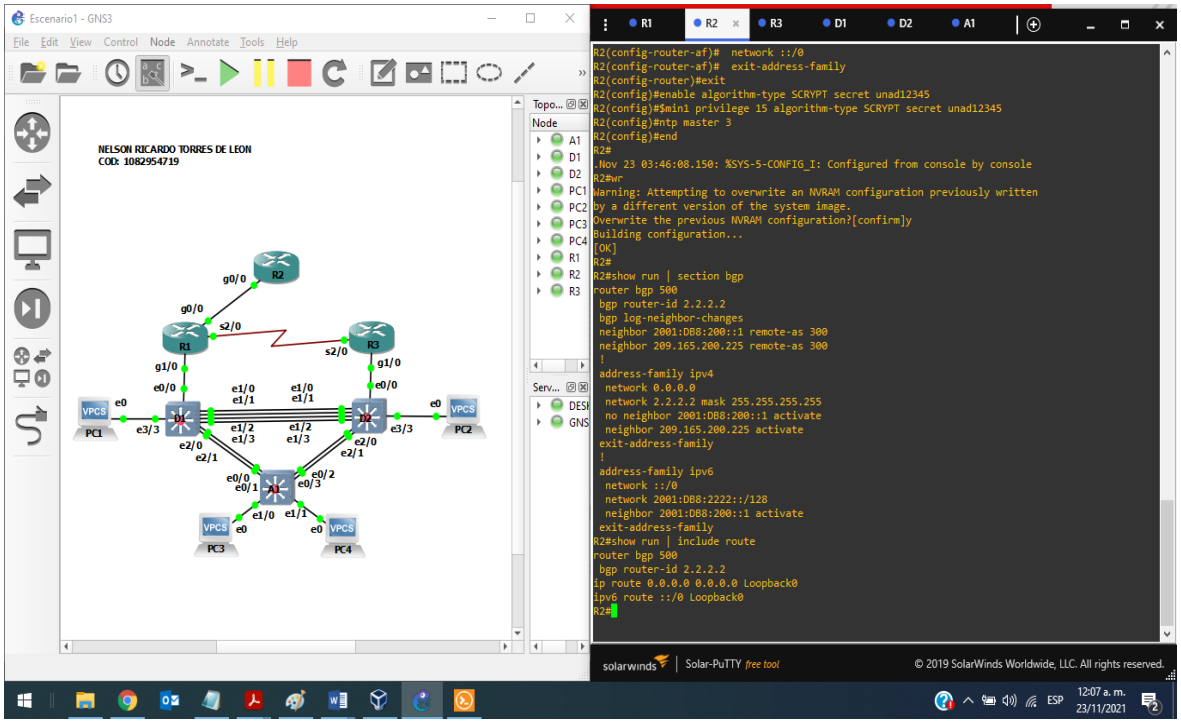


*Figura 13 - Evidencia 3e*

En R1 también podemos verificar la configuración MP-BGP establecida mediante el comando “show run | section bgp”, dando solución al punto 3.4:

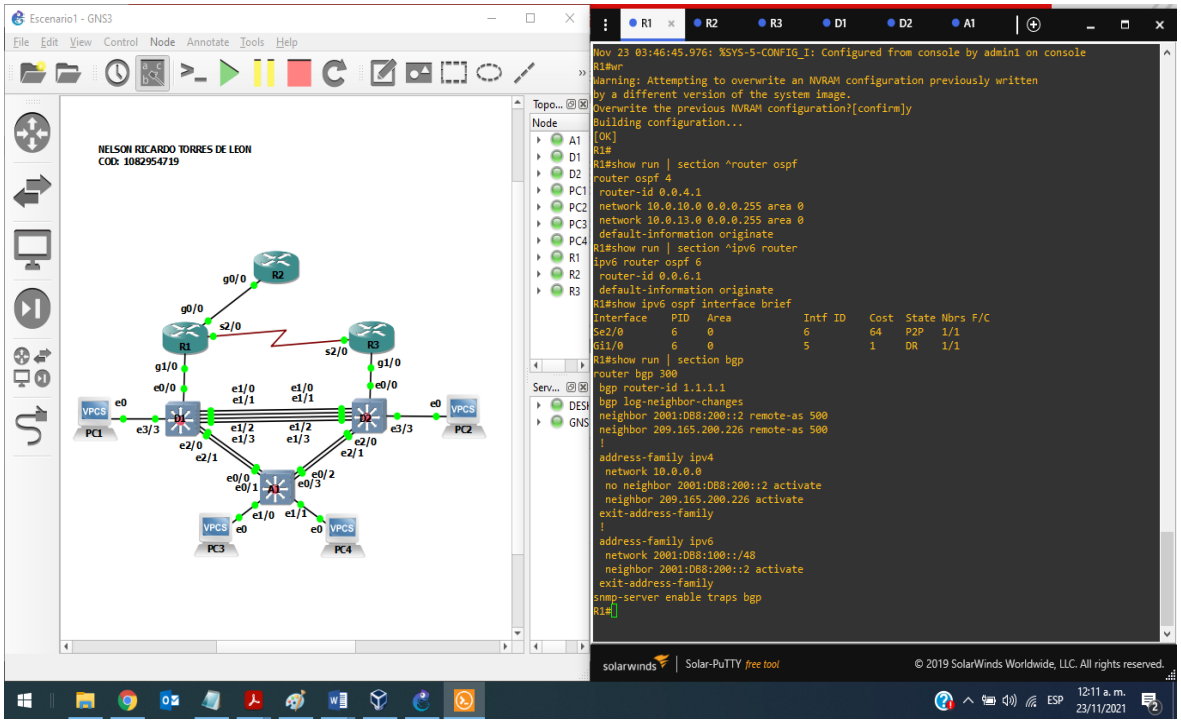


*Figura 14 - Evidencia 3f*

Verificamos la tabla de enrutamiento en R1 mediante el comando “show ip route | include O|B”, en donde se evidencia que OSPF y BGP para IPv4 funcionan correctamente, dando solución al punto 3.4:

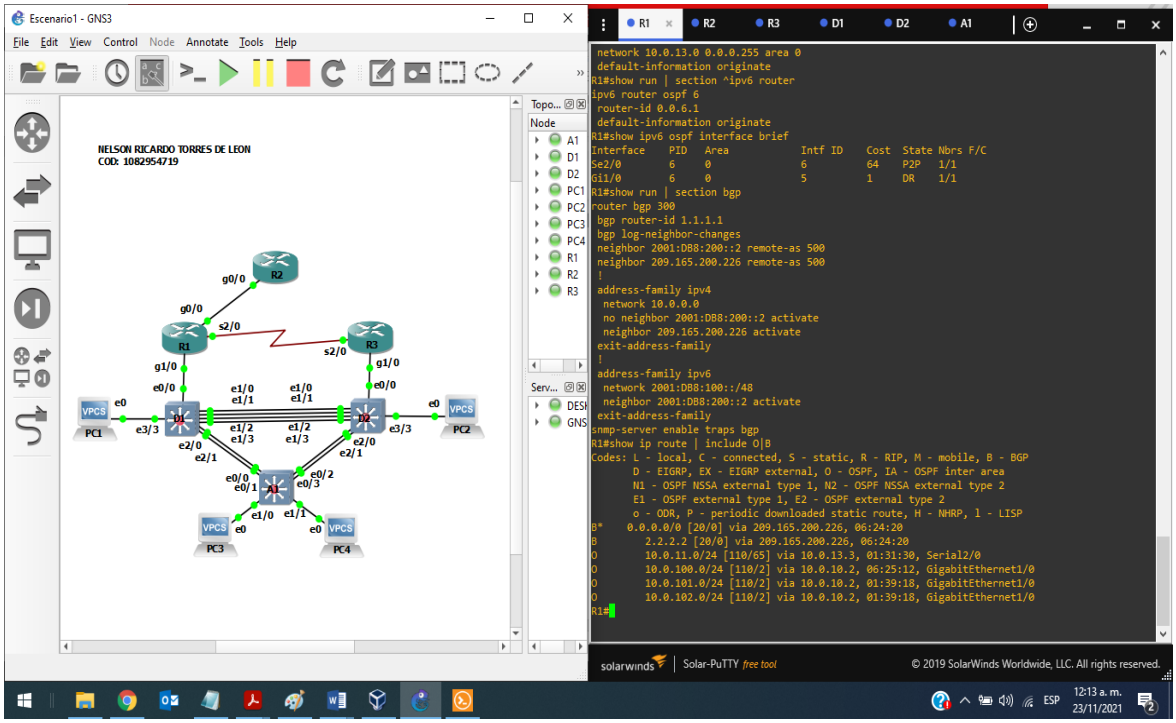


*Figura 15 - Evidencia 3g*

Utilizando el comando “show ipv6 route” podemos corroborar la configuración de enrutamiento de ipv6 en R1, verificando que OSPFv3 para IPv6 funciona correctamente, dando solución al punto 3.4

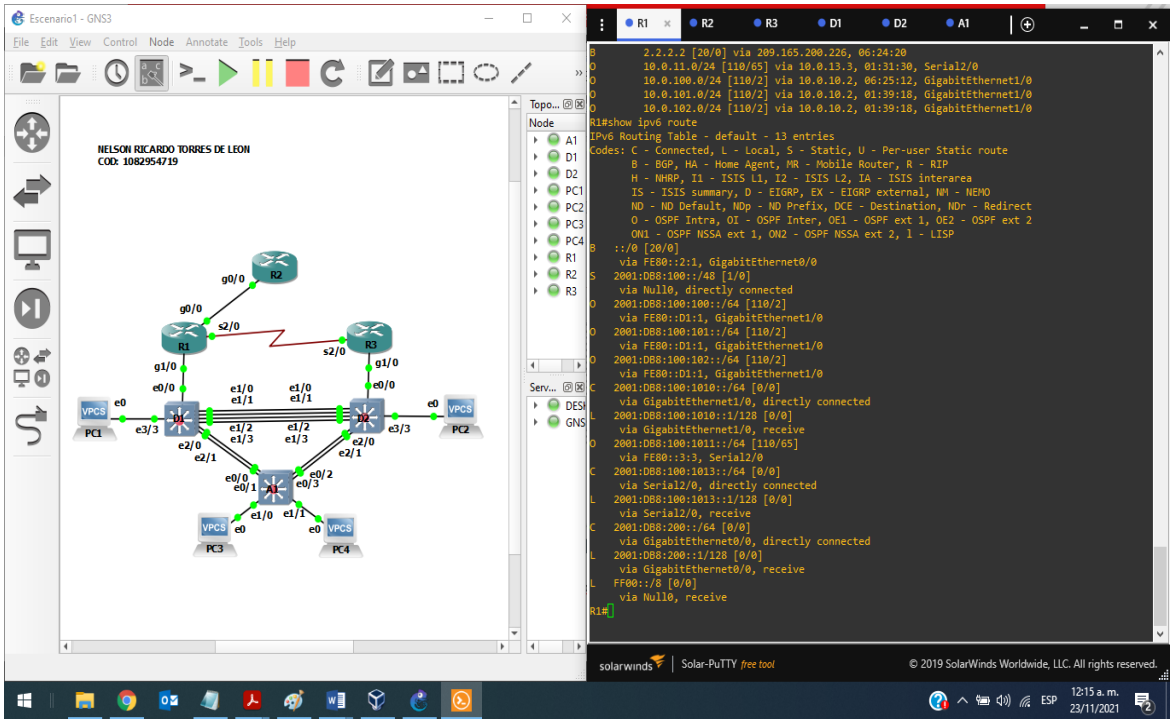


*Figura 16 - Evidencia 3h*

En R3 utilizando los comandos “show ip route ospf | begin Gateway” y “show ipv6 route ospf” podemos verificar que OSPF para ipv4 y OSPFv3 están trabajando adecuadamente, dando solución al punto 3.4:

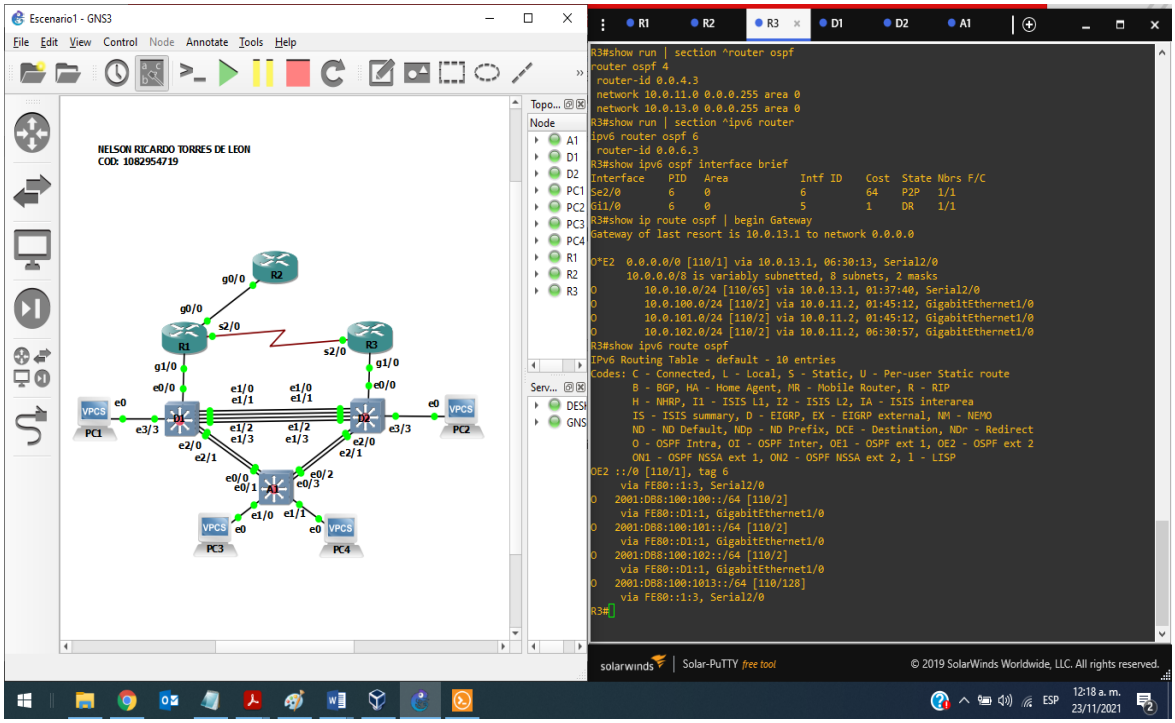


*Figura 17 - Evidencia 3i*

## 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:

| 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.<br>• Use la SLA número **4** para IPv4.<br>• Use la SLA número **6** para IPv6.<br>Las IP SLAs probarán la disponibilidad de la interfaz R1G0/0/1 cada 5 segundos.<br>Programe la SLA para una implementación inmediata sintiempo de finalización.<br>Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 6.<br>• Use el número de rastreo **4** para la IP SLA 4.<br>• Use el número de rastreo **6** para la IP SLA 6.<br>Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos. |
| 4.2 | En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1. | Cree IP SLAs.<br>• Use la SLA número **4** para IPv4.<br>• Use la SLA número **6** para IPv6.<br>Las IP SLAs probarán la disponibilidad de la interfaz R3G0/0/1 cada 5 segundos.<br>Programe la SLA para una implementación inmediata sintiempo de finalización.<br>Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 6.<br>• Use el número de rastreo **4** para la IP SLA 4.<br>• Use el número de rastreo **6** para la SLA 6.<br>Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos. |

| Tarea# | Tarea | Especificación |
|---|---|---|
| 4.3 | En D1 configure HSRPv2. | D1 es el router primario para las VLANs 100 y 102; por lotanto, su prioridad también se cambiará a 150..<br><br>Configure HSRP version 2.<br><br>Configure IPv4 HSRP grupo **104** para la VLAN 100:<br>• Asigne la dirección IP virtual **10.0.100.254**.<br>• Establezca la prioridad del grupo en **150**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 4 y decremente en 60.<br><br>Configure IPv4 HSRP grupo **114** para la VLAN 101:<br>• Asigne la dirección IP virtual **10.0.101.254**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 4 para disminuir en 60.<br><br>Configure IPv4 HSRP grupo **124** para la VLAN 102:<br>• Asigne la dirección IP virtual **10.0.102.254**.<br>• Establezca la prioridad del grupo en **150**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 4 para disminuir en 60.<br><br>Configure IPv6 HSRP grupo **106** para la VLAN 100:<br>• Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>• Establezca la prioridad del grupo en **150**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 6 y decremente en 60.<br><br>Configure IPv6 HSRP grupo **116** para la VLAN 101:<br>• Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>• Habilite la preferencia (preemption).<br>• Registre el objeto 6 y decremente en 60.<br><br>Configure IPv6 HSRP grupo **126** para la VLAN 102:<br>• Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>• Establezca la prioridad del grupo en **150**.<br>• Habilite la preferencia (preemption). |

| | | |
|---|---|---|
| | | • Rastree el objeto 6 y decremente en 60. |
| **Tarea#** | **Tarea** | **Especificación** |

| | | |
|---|---|---|
| | En D2, configure HSRPv2. | D2 es el router primario para la VLAN 101; por lo tanto, suprioridad también se cambiará a 150.<br><br>Configure HSRP version 2.<br><br>Configure IPv4 HSRP grupo **104** para la VLAN 100:<br>• Asigne la dirección IP virtual **10.0.100.254**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 4 y decremente en 60.<br><br>Configure IPv4 HSRP grupo **114** para la VLAN 101:<br>• Asigne la dirección IP virtual **10.0.101.254**.<br>• Establezca la prioridad del grupo en **150**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 4 para disminuir en 60.<br><br>Configure IPv4 HSRP grupo **124** para la VLAN 102:<br>• Asigne la dirección IP virtual **10.0.102.254**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 4 para disminuir en 60.<br><br>Configure IPv6 HSRP grupo **106** para la VLAN 100:<br>• Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 6 para disminuir en 60.<br><br>Configure IPv6 HSRP grupo **116** para la VLAN 101:<br>• Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>• Establezca la prioridad del grupo en **150**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 6 para disminuir en 60.<br><br>Configure IPv6 HSRP grupo **126** para la VLAN 102:<br>• Asigne la dirección IP virtual usando **ipv6 autoconfig**.<br>• Habilite la preferencia (preemption).<br>• Rastree el objeto 6 para disminuir en 60. |

*Tabla 4 - Tarea Parte 4*

Para estas configuraciones se utilizaron los siguientes comandos:

D1

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

```
 standby 124 track 4 decrement 60
 standby 126 ipv6 autoconfig
 standby 126 priority 150
 standby 126 preempt
 standby 126 track 6 decrement 60
 exit
end
```

D2

```
ip sla 4
 icmp-echo 10.0.11.1
 frequency
exit
ip sla 6
 icmp-echo 2001:db8:100:1011::1
 frequency
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
 delay down 10 up 15
 exit
track 6 ip sla 6
 delay down 10 up 15
 exit
interface vlan 100
 standby version 2
 standby 104 ip 10.0.100.254
 standby 104 preempt
 standby 104 track 4 decrement 60
 standby 106 ipv6 autoconfig
 standby 106 preempt
 standby 106 track 6 decrement 60
 exit
interface vlan 101
 standby version 2
 standby 114 ip 10.0.101.254
 standby 114 priority 150
 standby 114 preempt
 standby 114 track 4 decrement 60
 standby 116 ipv6 autoconfig
 standby 116 priority 150
```

```
 standby 116 preempt
 standby 116 track 6 decrement 60
 exit
interface vlan 102
 standby version 2
 standby 124 ip 10.0.102.254
 standby 124 preempt
 standby 124 track 4 decrement 60
 standby 126 ipv6 autoconfig
 standby 126 preempt
 standby 126 track 6 decrement 60
 exit
end
```

Mediante los comandos “show run | section ip sla” y “show standby brief “podemos corroborar la configuración de la IP SLAs en D1 y HSRPv2 para D1, dando solución a los puntos 4.1 y 4.3:

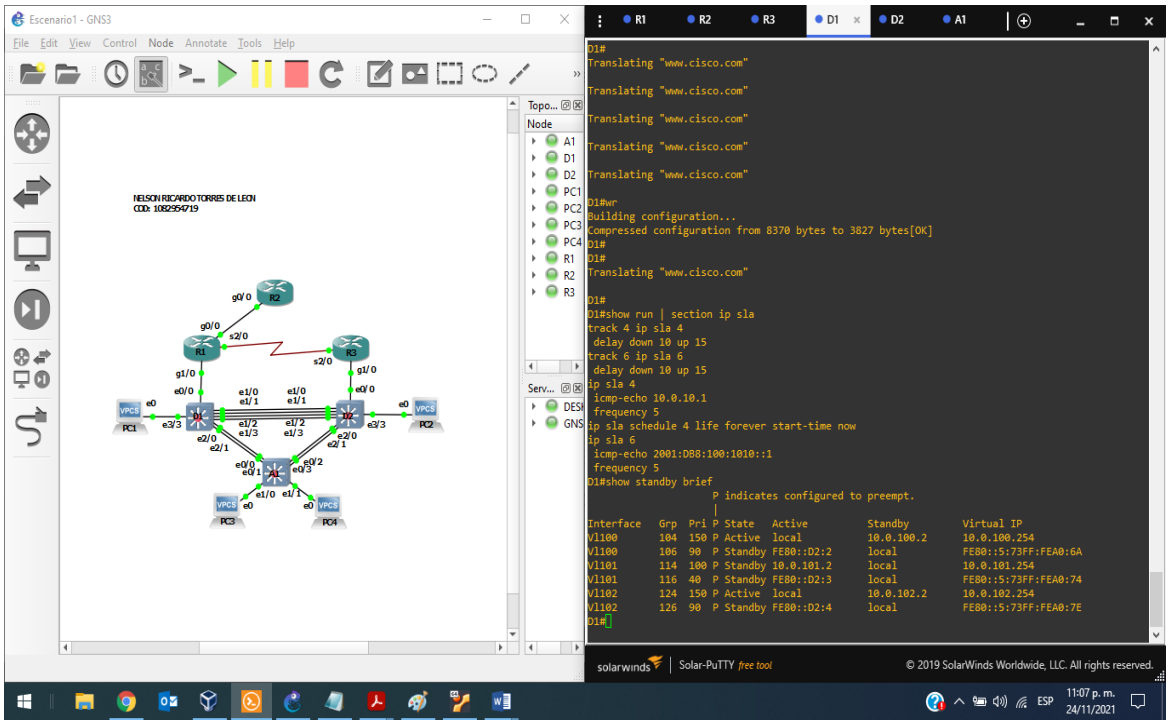


*Figura 18 - Evidencia 4a*

En D2 utilizamos el comando “show run | section ip sla” y verificamos la configuración de la IP SLAs y HSRPv2 para D1, dando solución a los puntos 4.2 y

4.3:

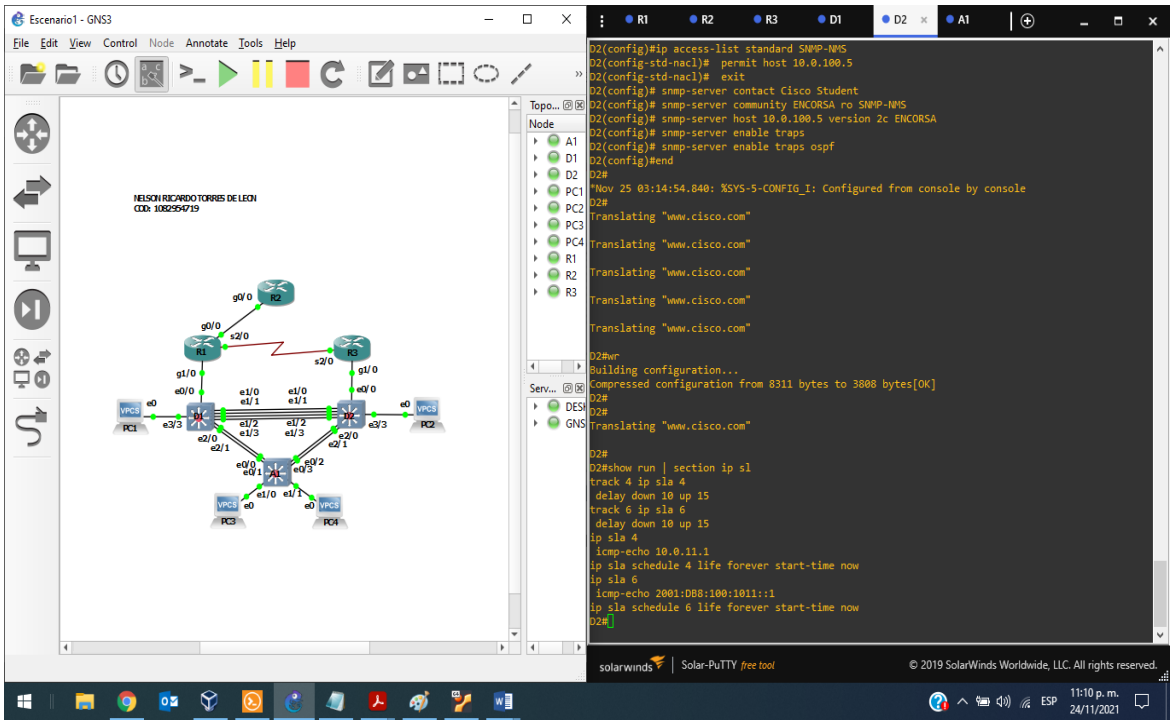


*Figura 19 - Evidencia 4b*

## 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:

| 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:<br>• Nombre de usuario Local: **sadmin**<br>• Nivel de privilegio **15**<br>• 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.:<br>• Dirección IP del servidor RADIUS es10.0.100.6.<br>• Puertos UDP del servidor RADIUS son1812 y 1813.<br>• Contraseña: **$trongPass** |
| 5.5 | En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA | Especificaciones de autenticación AAA:<br>• Use la lista de métodos por defecto<br>• Valide contra el grupo de servidoresRADIUS<br>• De lo contrario, utilice la base de datoslocal. |
| 5.6 | Verifique el servicio AAA en todos los dispositivos (except R2). | Cierre e inicie sesión en todos los dispositivos<br>(except R2) con el usuario: **raduser** y lacontraseña: **upass123**. |

*Tabla 5 - Tarea Parte 5*

Para estas configuraciones se utilizaron los siguientes comandos en todos los dispositivos:

enable algorithm-type SCRYPT secret cisco12345cisco

username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

También se utilizó la siguiente línea de comandos en todos los dispositivos a excepción de R2:

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

Esto lo podemos corroborar mediante el comando “show run | include secret” en cualquier dispositivo, en donde se verifica la protección EXEC privilegiado al usar el algoritmo de encriptación SCRYPT, creando una cuenta encriptada con las credenciales “Nombre de usuario Local: sadmin - Contraseña: cisco12345cisco”, dando solución a los puntos 5.1 y 5.2:

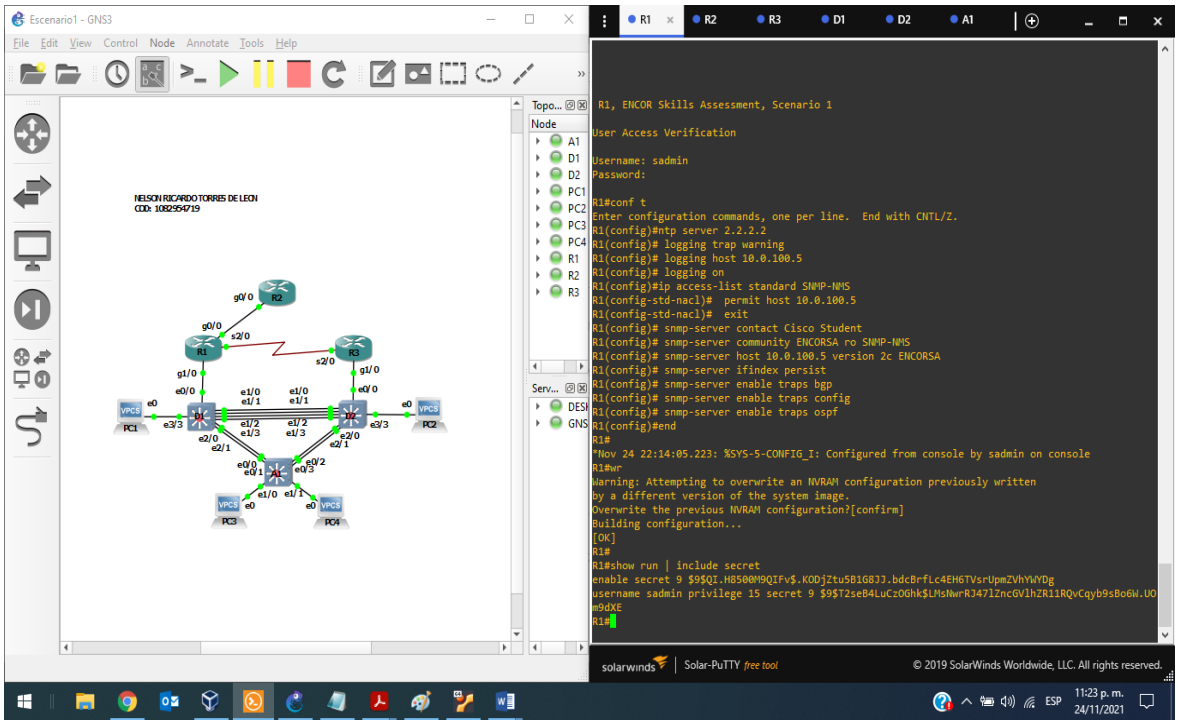

*Figura 20 - Evidencia 5ª*

Y también en todos los dispositivos, excepto en R2, mediante le comando “show run aaa | exclude !”, verificando la correcta configuración de AAA, los métodos de

autenticación y las especificaciones del servidor RADIUS, dando solución a los puntos 5.3, 5.4 y 5.5:

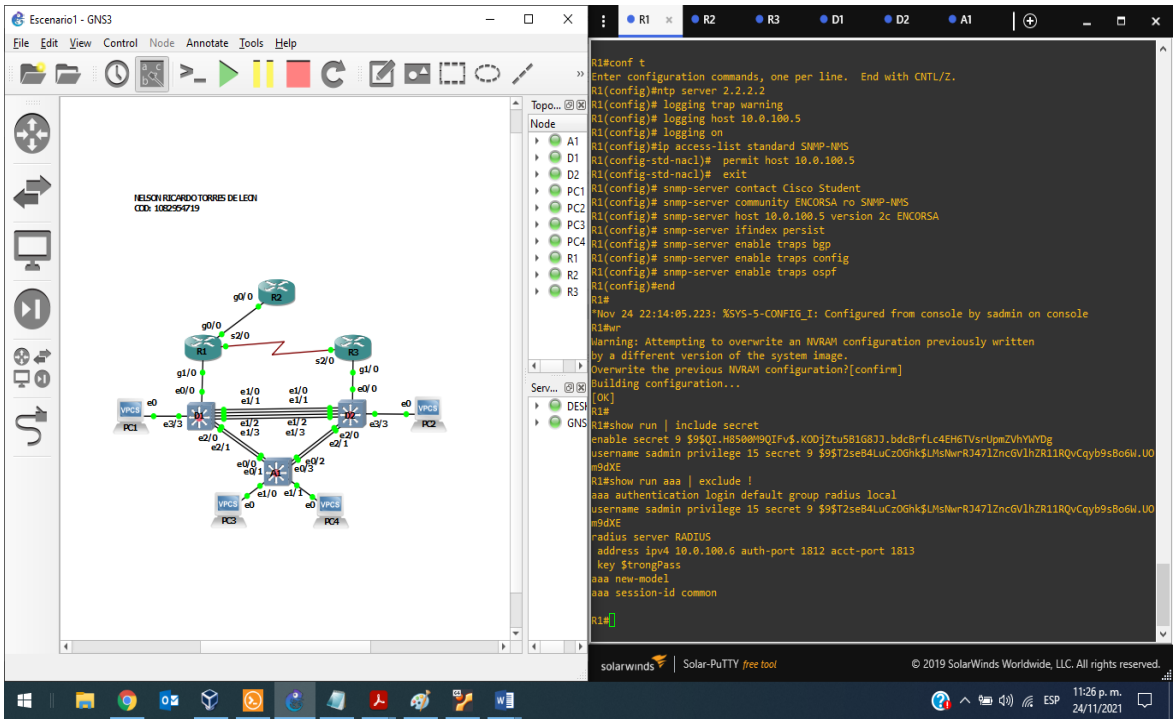


*Figura 21 - Evidencia 5b*

Mediante el comando telnet y la ip de cualquier dispositivo en red podemos corroborar, la autenticación AAA y su correcto funcionamiento al acceder mediante las credenciales desde otro dispositivo diferente, dando solución al punto 5.6:

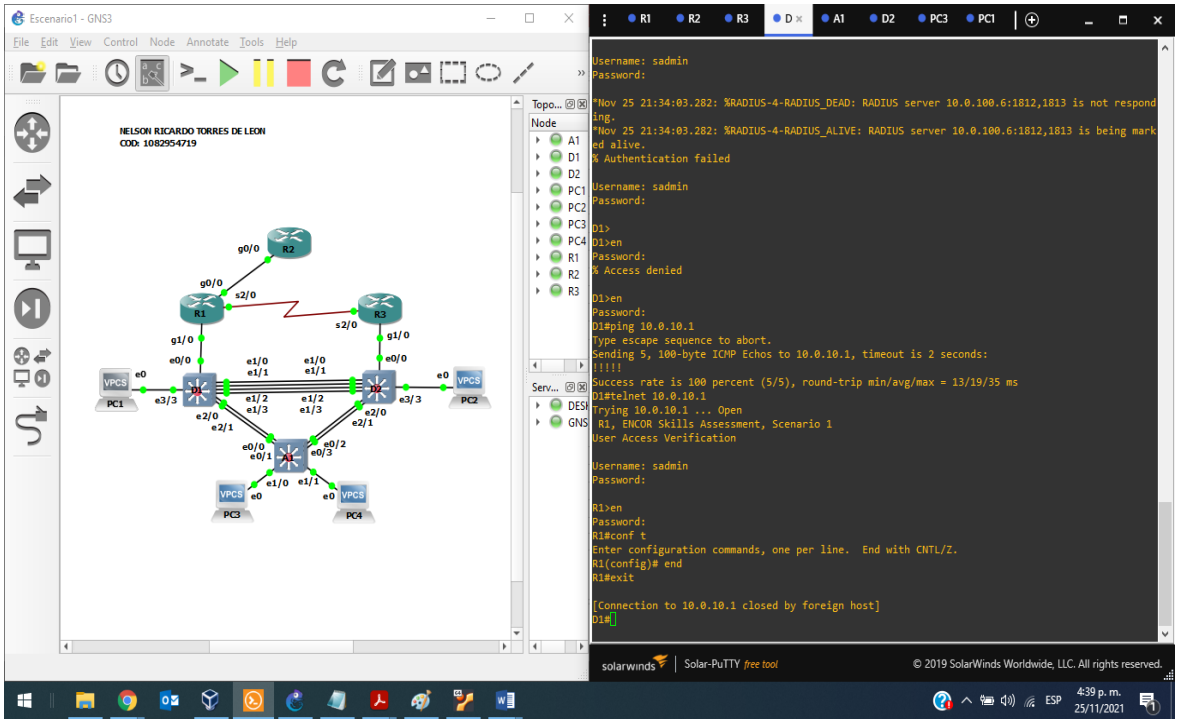


*Figura 22 - Evidencia 5c*

### 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:

| 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 deestrato 3. |
| **Tarea#** | **Tarea** | **Especificación** |
| 6.3 | Configure NTP en R1, R3, D1, D2, y A1. | Configure NTP de la siguiente manera:<br>• R1 debe sincronizar con R2.<br>• R3, D1 y A1 para sincronizar la hora con R1.<br>• 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 enel nivel WARNING. |
| 6.5 | Configure SNMPv2c en todos los dispositivos excepto R2 | Especificaciones de SNMPv2:<br>• Unicamente se usará SNMP en modo lectura(Read-Only).<br>• Limite el acceso SNMP a la dirección IP de laPC1.<br>• Configure el valor de contacto SNMP con sunombre.<br>• Establezca el *community string* en **ENCORSA**.<br>• En R3, D1, y D2, habilite el envío de *trapsconfig* y *ospf*.<br>• En R1, habilite el envío de *traps bgp, config*, y *ospf*.<br>• En A1, habilite el envío de *traps config*. |

*Tabla 6 - Tarea Parte 6*

Mediante el comando “show clock” podemos verificar la hora UTC en R2 y con el

comando “show run | include ntp” la configuración NTP maestro en el nivel estrato 3 correspondiente, dando solución a los puntos 6.1 y 6.2:

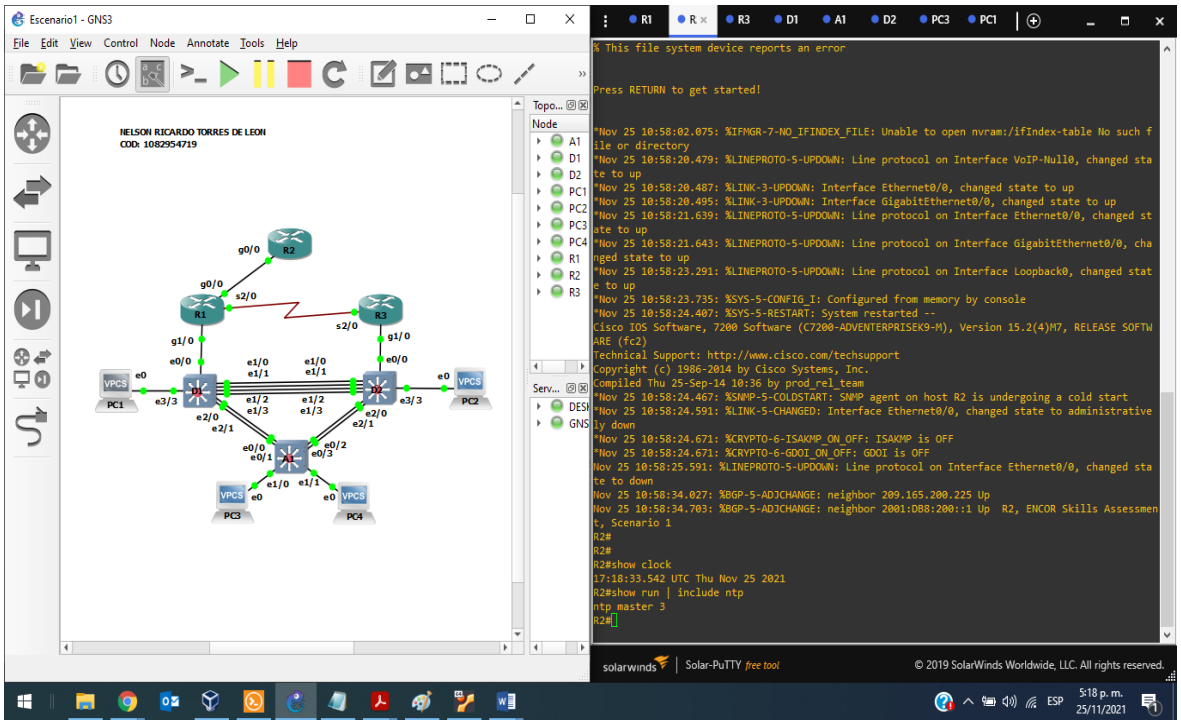


*Figura 23 - Evidencia 6a*

Mediante los comandos “show ntp status | include stratum” y “show run | include logging” podemos corroborar la configuración NTP y Syslog correspondiente en R1, dando solución a los puntos 6.3 y 6.4:

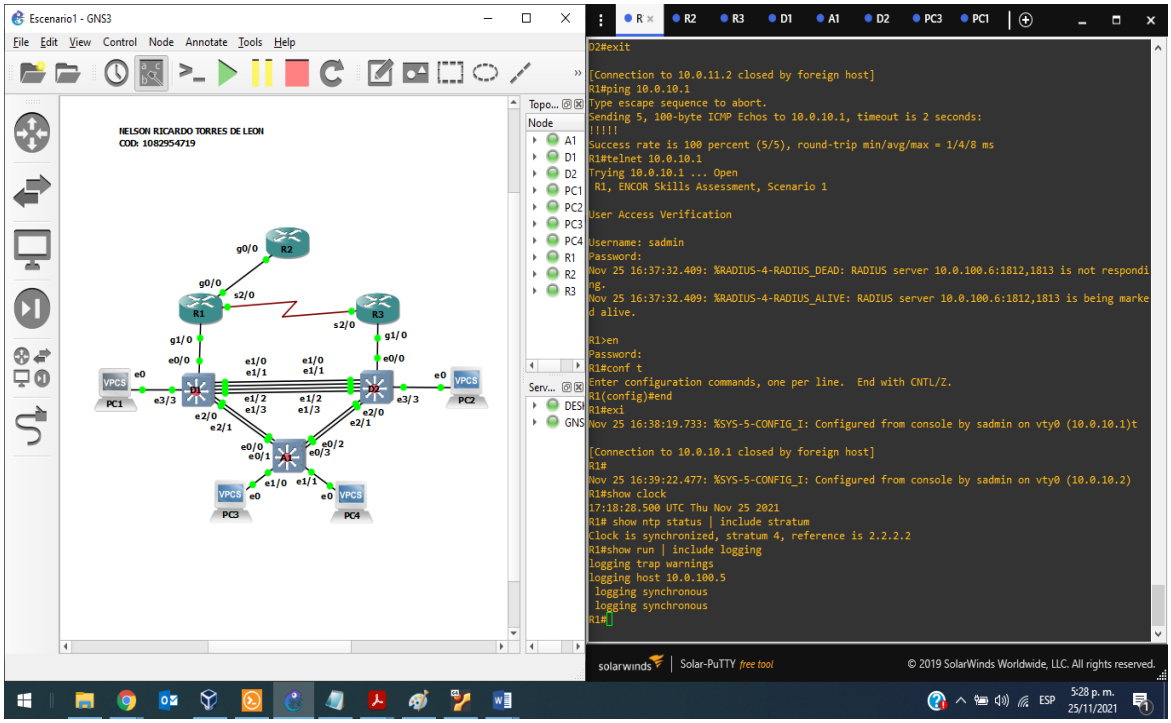


*Figura 24 - Evidencia 6b*

La configuración SNMPv2c en D1 se puede verificar con el comando “show ip access-list SNMP-NMS”, con esto se da solución al punto 6.5:

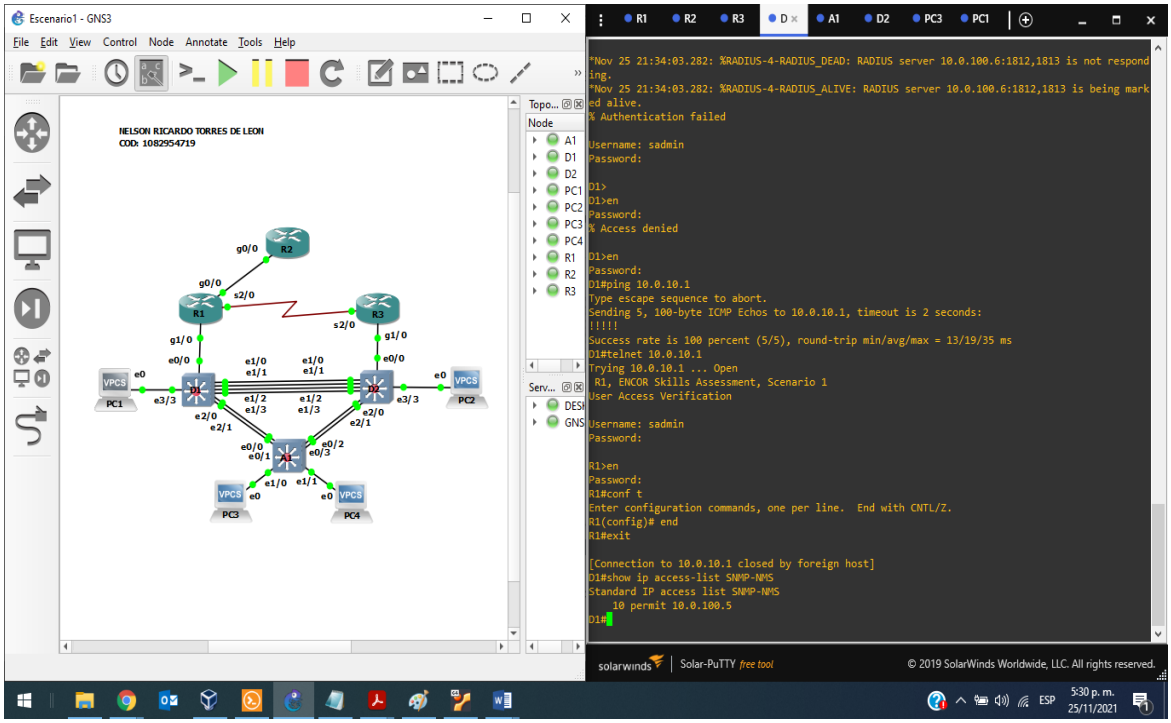


*Figura 25 - Evidencia 6c*

En cualquier dispositivo, excepto en R2, podemos corroborar la configuración SNMPv2c mediante el comando “show run | include snmp”, con esto damos solución al punto 6.5

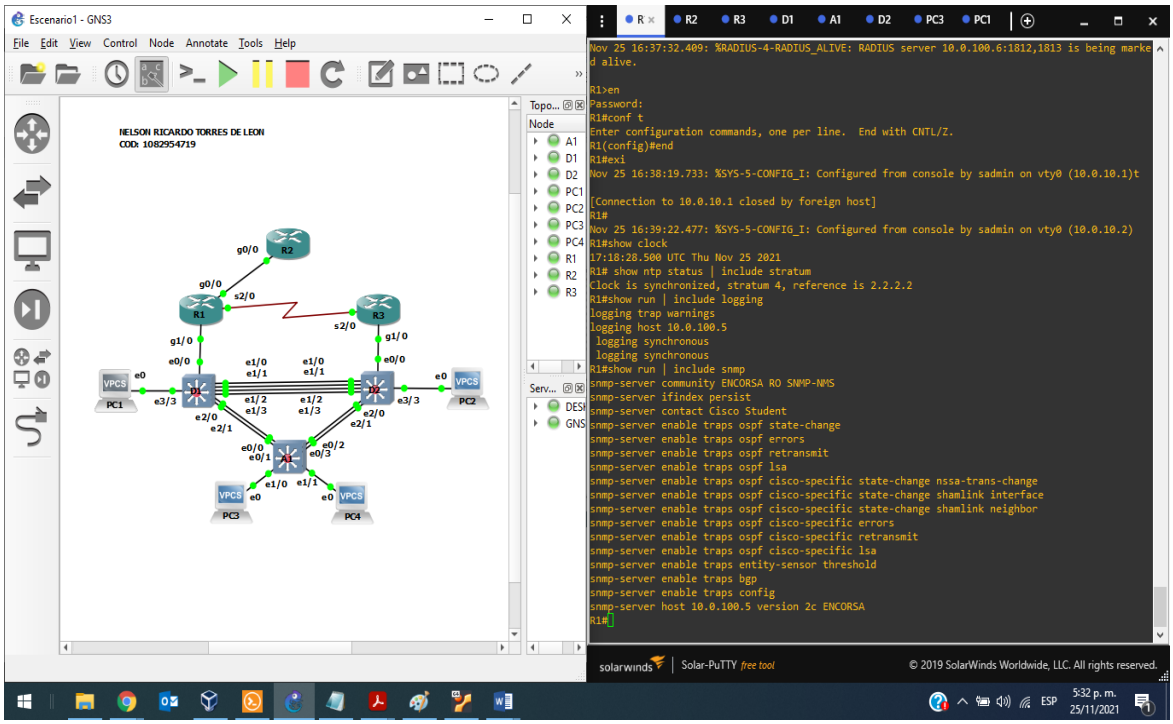


*Figura 26 - Evidencia 6d*

## CONCLUSIONES

De las anteriores actividades podemos concluir que es muy importante conocer la topología de la red y su configuración, ya que al momento de implementar el direccionamiento ip y las VLANs, podemos caer en el error de equivocarnos en alguna dirección y por ende crear conflictos al momento de ejecutar las conexiones.

Hay que reconocer la importancia de los sistemas de información, como estos operan y los diferentes protocolos y directrices que implementan estos sistemas, ya que hoy en día es un aspecto muy importante en el desarrollo de las comunicaciones.

Es de resaltar la manera como se establecen conexiones de datos entre dispositivos que físicamente no están cercanos, pero mediante el enrutamiento correspondiente, se pueden manipular y configurar entre sí, con los conocimientos requeridos, por eso se hace importante la implementación de un buen sistema de Ciberseguridad que permita reducir las vulnerabilidades de la red.

Por otra parte, el uso de los softwares de simulación de Packet Tracer y GNS3 ha sido mucha ayuda, debido a la facilidad de simular el escenario de una manera eficiente, con todas las funciones que se han requerido y por la facilidad de entender como están configuradas las redes.

## BIBLIOGRÁFIA

(S/f). Gns3.com. Recuperado el 26 de noviembre de 2021, de https://gns3.com/software

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

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