

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

OSCAR MAURICIO GÓMEZ ALZATE

UNIVERSIDAD NACIONAL ABIERTA Y A MDISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
EL CARMEN DE VIBORAL  
2021

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

OSCAR MAURICIO GÓMEZ ALZATE

Diplomado de opción de grado presentado para optar el  
Título de INGENIERO ELECTRONICO

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A MDISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
EL CARMEN DE VIBORAL  
2021

NOTA DE ACEPTACIÓN:

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

El Carmen de Viboral, 29 de noviembre de 2021

## **AGRADECIMIENTOS**

En primer lugar agradezco a Dios por ser mi guía en este largo camino emprendido. A mi hija y a mi futura esposa que han sido el motor y el apoyo necesario para superar cada obstáculo que se me ha presentado en la búsqueda del tan anhelado título profesional. A mis padres y a mi hermanita por el apoyo emocional que me han brindado, demostrando su preocupación e interés no solo en mi formación académica, sino también en mi formación como persona, buscando que sea un profesional integro. Finalmente agradezco a la Universidad y a cada uno de los docentes que se involucraron en mi formación académica, brindándome todas las bases necesarias para así adquirir las competencias requeridas a un profesional en el campo de la ingeniería.

## CONTENIDO.

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	8
LISTA DE FIGURAS.....	9
GLOSARIO.....	10
RESUMEN.....	11
INTRODUCCION.....	12
DESARROLLO.....	13
ESCENARIO 1.....	13
PARTE 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.....	15
Paso 1: Cablear la red como se muestra en la topología.....	15
Paso 2: Configurar los parámetros básicos para cada dispositivo.....	15
Código configuración básica para switch D1:.....	15
Código configuración básica para switch D2:.....	17
Código configuración básica para switch A1:.....	20
Código configuración básica para Router R1:.....	20
Código configuración básica para Router R2:.....	21
Código configuración básica para Router R3:.....	22
Código configuración básica para PC1:.....	23
Código configuración básica para PC4:.....	23
PARTE 2: Configurar la capa 2 de la red y el soporte de host.....	23
Código configuración para switch D1:.....	25

Código configuración para Switch D2: .....	26
Código configuración para Switch A1:.....	27
Verificación de conectividad: .....	28
PARTE 3: Configurar los protocolos de enrutamiento. ....	32
Código configuración para Switch D1: .....	34
Código configuración para Switch D2: .....	36
Código configuración Para Router R1:.....	37
Código configuración Para Router R2:.....	38
Código configuración para Router R3: .....	39
PARTE 4: Configurar la redundancia del primer salto (first hop redundancy).....	40
Código configuración para Switch D1: .....	42
Código configuración para Switch D2: .....	43
PARTE 5: Seguridad.....	46
Código configuración para Router R1: .....	47
Código configuración para Router R2: .....	48
Código configuración para Router R3: .....	49
Código configuración para Switch D1: .....	50
Código configuración para Switch D2: .....	51
Código configuración para Switch A1:.....	52
PARTE 6: Configure las funciones de Administración de Red.....	56
Código configuración para Switch D1: .....	57
Código configuración para Switch D2: .....	59
Código configuración para Switch A2:.....	60
Código configuración para Router R1: .....	60

Código configuración para Router R2: .....	61
Código configuración para Router R3: .....	62
CONCLUSIONES .....	63
BIBLIOGRAFÍA.....	64

## LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento .....	14
Tabla 2. Tareas capa 2 de la red .....	24
Tabla 3. Tareas para protocolos de enrutamiento .....	32
Tabla 4. Tareas para la redundancia del primer salto .....	40
Tabla 5. Tareas para la seguridad de la red. ....	46
Tabla 6. Tareas para las funciones de administración de red.....	56

## LISTA DE FIGURAS

Figura 1. Escenario 1 .....	13
Figura 2. Simulación escenario1 .....	15
Figura 3. Servicios DHCP IPv4 PC2 .....	29
Figura 4. Servicios DHCP IPv4 PC3 .....	29
Figura 5. Conectividad PC1 .....	30
Figura 6. Conectividad PC2 .....	30
Figura 7. Conectividad PC3 .....	31
Figura 8. Conectividad PC4 .....	31
Figura 9. Verificación servicio AAA R1 .....	54
Figura 10. Verificación servicio AAA R3 .....	54
Figura 11. Verificación servicio AAA D1 .....	55
Figura 12. Verificación servicio AAA D2 .....	55
Figura 13. Verificación servicio AAA A1 .....	56

## GLOSARIO

**DIRECCIÓN IP:** Número que identifica de manera lógica una interfaz de red.

**OSPF:** Protocolo pensado para Internet y la pila TCP/IP como protocolo de routing interno (distribuye información entre routers que pertenecen al mismo Sistema autónomo).

**ROUTER:** Dispositivo que se encarga de distribuir la conexión a Internet a distintos ordenadores vinculados a una misma red local. Por tanto, actúa de intermediario entre el conjunto de equipos e Internet, como un puente entre nuestros dispositivos y la red de redes.

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

**VLAN:** También conocidas como redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física.

## **RESUMEN**

El presente documento contiene la prueba de habilidades prácticas del diplomado de profundización CISCO CCNP como opción de grado para la ingeniería electrónica y telecomunicaciones, en el cual se debe aplicar los conocimientos adquiridos con el fin de desarrollar un escenario propuesto. La configuración de cada uno de los dispositivos incidentes en la topología de la red, se lleva a cabo mediante el desarrollo de seis pasos, donde se configura el direccionamiento de las interfaces, las capas de la red, el soporte de los Host, los protocolos de enrutamiento tanto de IPv4 e IPv6, la redundancia, la seguridad y la administración de las redes incidentes en la topología. Posterior a la configuración se realiza una serie de chequeos que permite la verificación de la conectividad, la conmutación y la seguridad en la topología sea la deseada.

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

## **ABSTRACT**

This document contains the practical skills test of the CISCO CCNP in-depth diploma as a degree option for electronic engineering and telecommunications, in which the acquired knowledge must be applied in order to develop a proposed scenario. The configuration of each of the incident devices in the network topology is carried out through the development of six steps, where the addressing of the interfaces, the network layers, the host support, the protocols are configured. routing both IPv4 and IPv6, redundancy, security and management of incident networks in the topology. After the configuration, a series of checks is carried out that allows the verification of connectivity, switching and security in the topology as desired.

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

## **INTRODUCCION.**

El presente trabajo es la recopilación de habilidades y conocimientos adquiridos en Cisco, enfocados en la configuración y la arquitectura de diversos dispositivos de red presentes en el ámbito de las telecomunicaciones. Con el fin de consolidar conceptos, se implementa un escenario práctico donde se debe realizar el correcto conexionado y la debida configuración de cada uno de los dispositivos para que la topología de la red sea funcional.

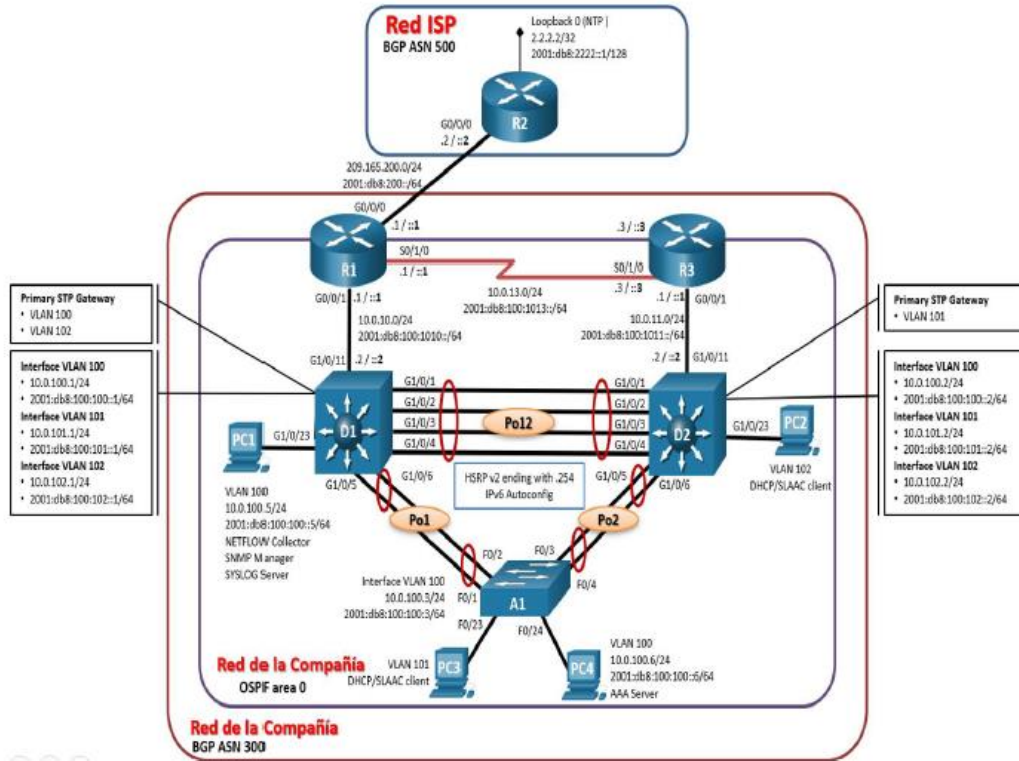
El escenario práctico es implementado en el software GNS3, el cual permite realizar diversas topologías y hacer su debida simulación con la mayor similitud a lo que se presenta en condiciones de la vida real.

Luego de la debida conexión de todos los dispositivos de la red propuesta, se procede a realizar la configuración de los protocolos direccionamientos y enrutamiento, las interfaces troncales, el soporte de los Host, la redundancia, la seguridad y la administración de la red, para cada uno de los dispositivos según sea el caso, y de esta forma lograr la correcta conectividad y operatividad de la red propuesta.

# DESARROLLO

## ESCENARIO 1

Figura 1. Escenario 1



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.

Tabla 1. Tabla de direccionamiento

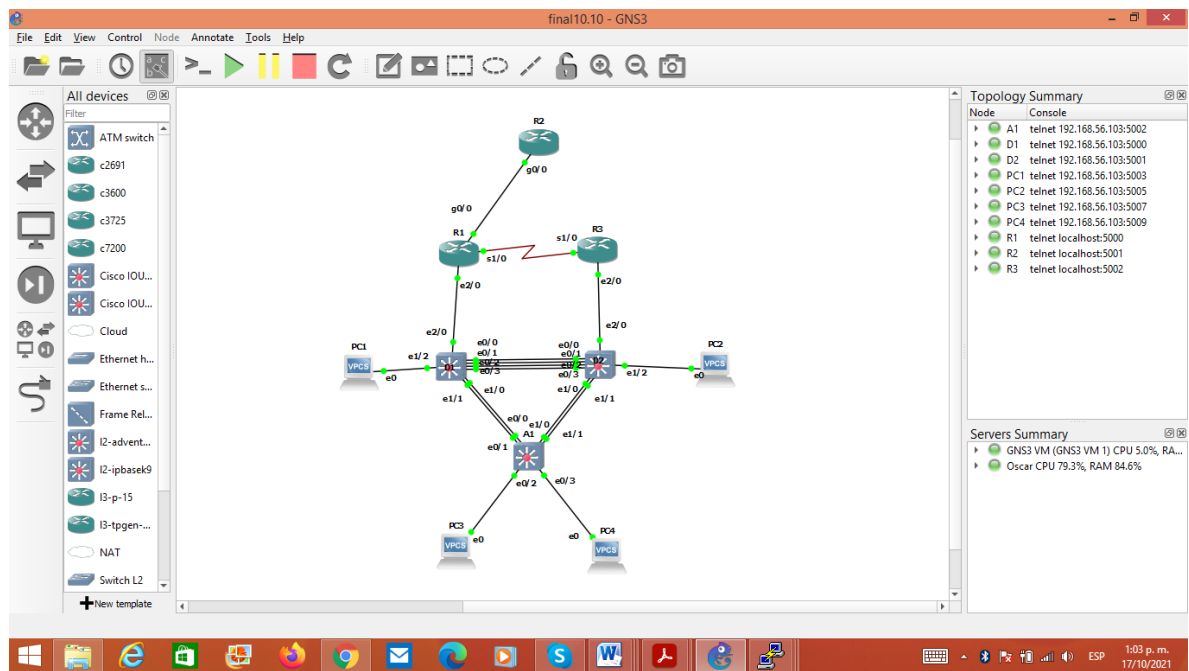
Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
R1	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
R1	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
R2	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
R3	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
D1	VLAN 100	10.0.100.1/24	2001:db8:100:1000::1/64	fe80::d1:2
D1	VLAN 101	10.0.101.1/24	2001:db8:100:1001::1/64	fe80::d1:3
D1	VLAN 102	10.0.102.1/24	2001:db8:100:1002::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
D2	VLAN 100	10.0.100.2/24	2001:db8:100:1000::2/64	fe80::d2:2
D2	VLAN 101	10.0.101.2/24	2001:db8:100:1001::2/64	fe80::d2:3
D2	VLAN 102	10.0.102.2/24	2001:db8:100:1002::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:1000::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:1000::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:1000::6/64	EUI-64

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

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

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

Figura 2. Simulación escenario1



### Paso 2: Configurar los parámetros básicos para cada dispositivo.

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:

#### Código configuración básica para switch D1:

```
D1#config t
```

```
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface e2/0
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 101
```

```
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range e0/0-3
D1(config-if-range)#shu
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#interface range e1/0-2
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1#copy running-config startup-config
```

### **Código configuración básica para switch D2:**

```
D2#configure terminal
```

```
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
D2(config)#interface e2/0
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 101
```

```
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shut
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shut
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range e0/0-3
D2(config-if-range)#shut
D2(config-if-range)#interface range e1/0-2
D2(config-if-range)#shut
D2(config-if-range)#
administratively
D2(config-if-range)#exit
D2(config)#exit
D2#exit
D2#copy running-config startup-config
```

### **Código configuración básica para switch A1:**

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

### **Código configuración básica para Router R1:**

```
R1#confi t
R1(config)#hostname R1
```

```
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface g0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shut
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface ethernet 2/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s1/1
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 shutd
R1(config-if)#exit
R1(config)#exit
R1# copy running-config startup-config
```

### **Código configuración básica para Router R2:**

```
R2#configu t
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
```

```
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutd
R2(config-if)#exit
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutd
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
R2# copy running-config startup-config
```

### **Código configuración básica para Router R3:**

```
R3#config t
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface ethernet 2/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
```

```
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s1/1
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:db8:100:1010::2/64
R3(config-if)#no shutd
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#exit
R3# copy running-config startup-config
```

#### **Código configuración básica para PC1:**

```
PC1> ip 10.0.100.5 10.0.100.254
PC1> save
```

#### **Código configuración básica para PC4:**

```
PC4> ip 10.0.100.6 10.0.100.254
PC4> save
```

### **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:

Tabla 2. Tareas capa 2 de la red

<b>Tarea#</b>	<b>Tarea</b>	<b>Especificación</b>
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: <ul style="list-style-type: none"> <li>• • D1 and D2</li> <li>• • D1 and A1</li> <li>• • D2 and A1</li> </ul>
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: <ul style="list-style-type: none"> <li>• • D1 a D2 – Port channel 12</li> <li>• • D1 a A1 – Port channel 1</li> <li>• • D2 a A1 – Port channel 2</li> </ul>
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	PC1 debería hacer ping con

	de la LAN local	<p>éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC4: 10.0.100.6</li> </ul> <p>PC2 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.102.1</li> <li>• D2: 10.0.102.2</li> </ul> <p>PC3 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.101.1</li> <li>• D2: 10.0.101.2</li> </ul> <p>PC4 debería hacer ping con éxito a:</p> <ul style="list-style-type: none"> <li>• D1: 10.0.100.1</li> <li>• D2: 10.0.100.2</li> <li>• PC1: 10.0.100.5</li> </ul>
--	-----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Se procede con la configuración de las interfaces troncales IEEE 802.1 Q y los puentes raíz RSTP en los 3 Switch, para permitir la interacción y la convergencia de toda la topología.

### Código configuración para switch D1:

```

D1(config)#interf
D1(config)#interface range e0/0-3
D1(config-if-range)#switchp
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trun
D1(config-if-range)#switchport trunk encapsulation dot1q           configuración
interfaces troncales.
D1(config-if-range)#switchport trunk native vlan 999               configuración
Vlan Nativa
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#no shut
D1(config-if-range)#exit

```

D1(config)#interface range e1/0-1	
D1(config-if-range)#switchport mode trunk	
D1(config-if-range)#switchport trunk encapsulation dot1q <i>interfaces troncales.</i>	<i>configuración</i>
D1(config-if-range)#switchport trunk native vlan 999 <i>Vlan Nativa</i>	<i>configuración</i>
D1(config-if-range)#switchport mode trunk	
D1(config-if-range)#channel-group 1 mode active	
D1(config-if-range)#no shut	
D1(config-if-range)#exit	
D1(config)#	
D1(config)#spanning	
D1(config)#spanning-tree mode rap	
D1(config)#spanning-tree mode rapid-pvst	<i>configuración Pvst</i>
D1(config)#spanning-tree vlan 100,102 root primary <i>Vlan primaria.</i>	<i>configuración prioridad</i>
D1(config)#spanning-tree vlan 101 root secondary <i>Vlan secundaria.</i>	<i>configuración prioridad</i>
D1(config)#interface e1/2	
D1(config-if)#switchport mode access	
D1(config-if)# switchport access vlan 100	
D1(config-if)#spanning-tree portfast	
D1(config-if)#no shutdown	
D1(config-if)#exit	

### **Código configuración para Switch D2:**

D2(config-if-range)#exit	
D2(config)#interface range e0/0-3	
D2(config-if-range)#switchport mode trunk	
D2(config-if-range)#switchport trunk encapsulation dot1q <i>interfaces troncales.</i>	<i>configuración</i>
D2(config-if-range)#switchport trunk native vlan 999 <i>Vlan Nativa</i>	<i>configuración</i>
D2(config-if-range)#switchport mode trunk	
D2(config-if-range)#channel-group 12 mode active	

```

D2(config-if-range)#no shut
D2(config-if-range)#exit
D2(config)#interface range e1/0-1
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk encapsulation dot1q
interfases troncales.
D2(config-if-range)#switchport trunk native vlan 999
Vlan Nativa
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#no shut
D2(config-if-range)#exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
prioridad Vlan primaria.
D2(config)#spanning-tree vlan 100,102 root secondary
prioridad Vlan secundaria.
D2(config)#interface e1/2
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)#no shut
D2(config-if)#exit

```

### **Código configuración para Switch A1:**

```

A1(config)#
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e0/0-1
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk encapsulation dot1q
interfases troncales.
A1(config-if-range)#switchport trunk native vlan 999
Vlan Nativa
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#channel-group 1 mode active

```

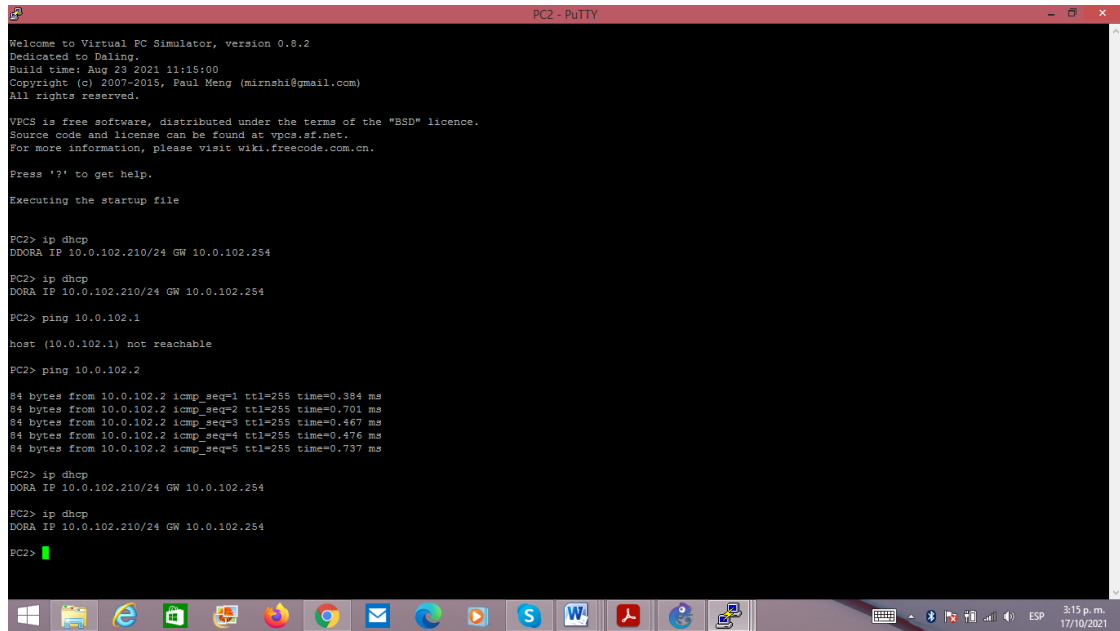
```

A1(config-if-range)#no shut
A1(config-if-range)#interface range e1/0-1
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk encapsulation dot1q      configuración
interfases troncales.
A1(config-if-range)#switchport trunk native vlan 999          configuración
Vlan Nativa
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#no shut
A1(config-if-range)#exit
A1(config)#interface e0/2
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config-if)#no shut
A1(config-if)#exit
A1(config)#interface e0/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shut
A1(config-if)#exit

```

**Verificación de conectividad:**

Figura 3. Servicios DHCP IPv4 PC2



```
PC2 - PuTTY
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Dalling.
Build time: Aug 29 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> ping 10.0.102.1

host (10.0.102.1) not reachable

PC2> ping 10.0.102.2

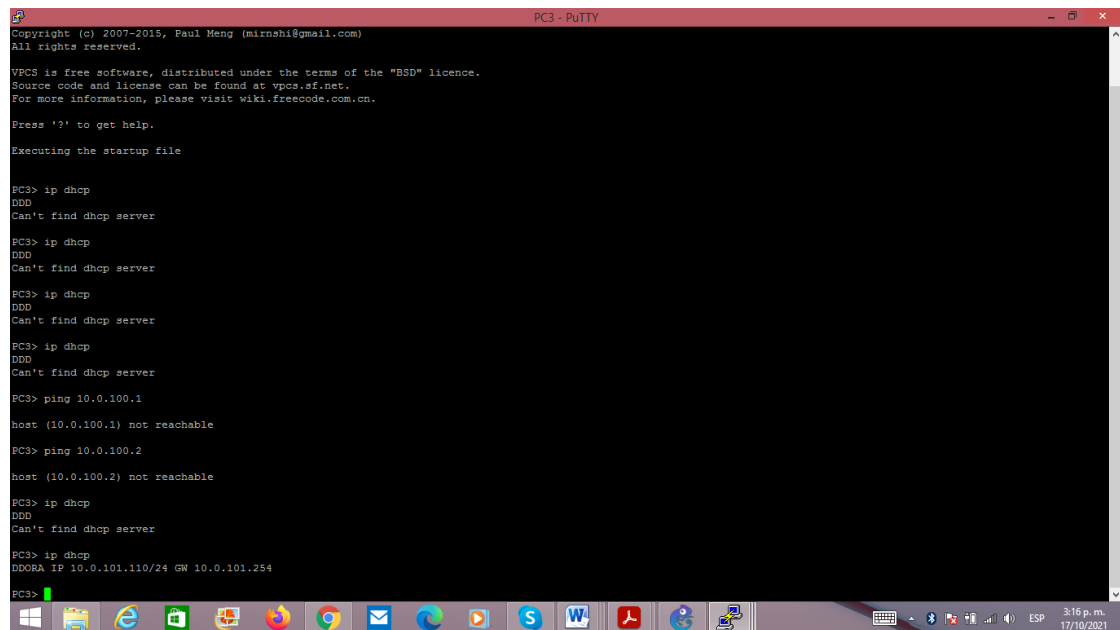
64 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.384 ms
64 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.701 ms
64 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.467 ms
64 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.476 ms
64 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.737 ms

PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254

PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254

PC2>
```

Figura 4. Servicios DHCP IPv4 PC3



```
PC3 - PuTTY
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC3> ip dhcp
DDD
Can't find dhcp server

PC3> ip dhcp
DDD
Can't find dhcp server

PC3> ip dhcp
DDD
Can't find dhcp server

PC3> ip dhcp
DDD
Can't find dhcp server

PC3> ping 10.0.100.1

host (10.0.100.1) not reachable

PC3> ping 10.0.100.2

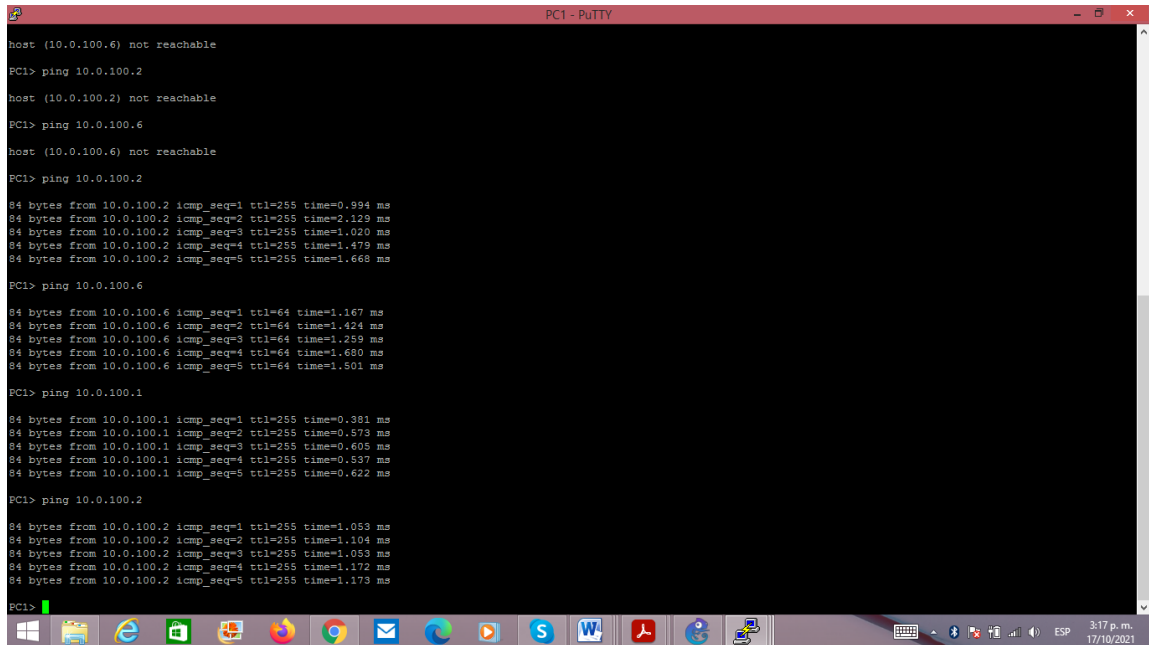
host (10.0.100.2) not reachable

PC3> ip dhcp
DDD
Can't find dhcp server

PC3> ip dhcp
DDORA IP 10.0.101.110/24 GW 10.0.101.254

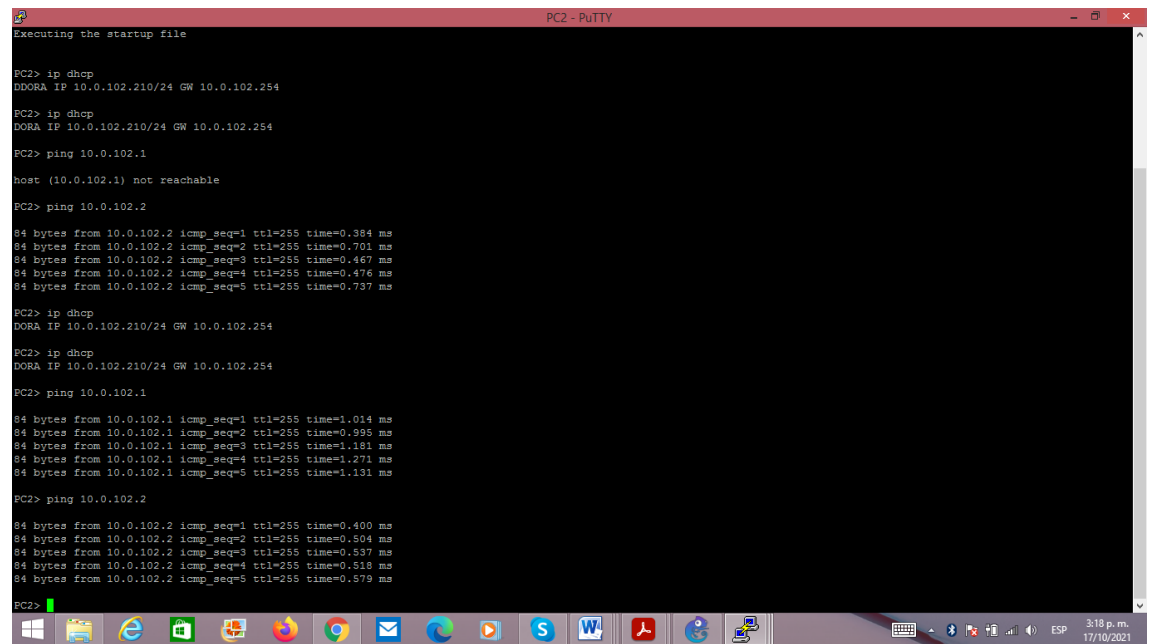
PC3>
```

Figura 5. Conectividad PC1



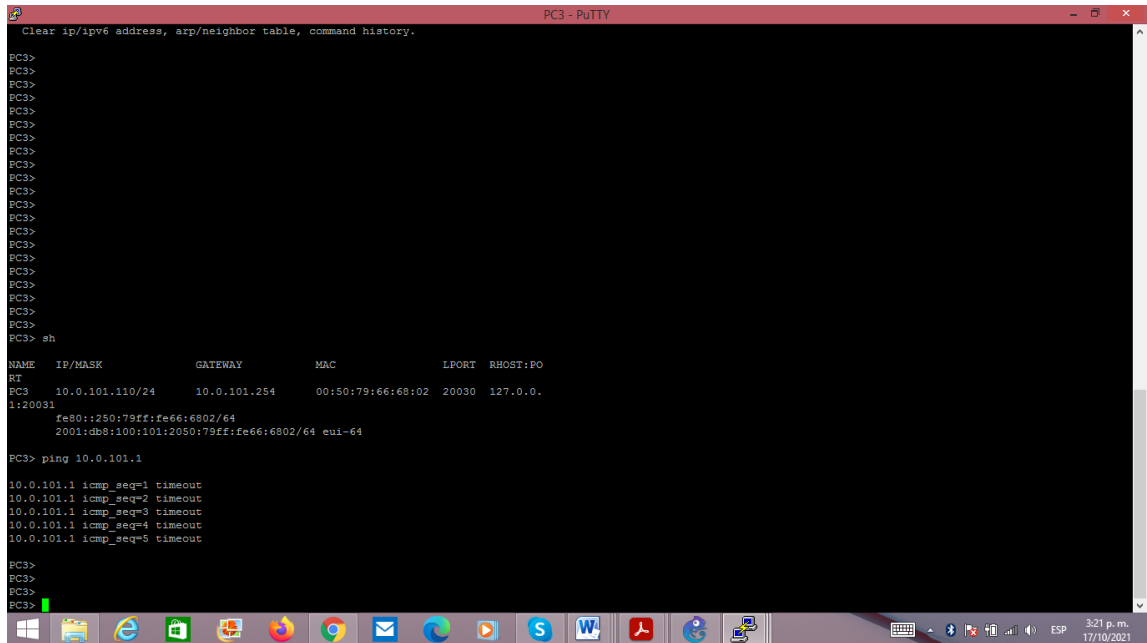
```
host (10.0.100.6) not reachable
PC1> ping 10.0.100.2
host (10.0.100.2) not reachable
PC1> ping 10.0.100.6
host (10.0.100.6) not reachable
PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.994 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=2.129 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.020 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.479 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.668 ms
PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=1.167 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=1.424 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=1.259 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=1.680 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=1.501 ms
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.381 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.573 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.605 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.537 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.622 ms
PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=1.053 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=1.104 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=1.053 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=1.192 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=1.173 ms
PC1>
```

Figura 6. Conectividad PC2



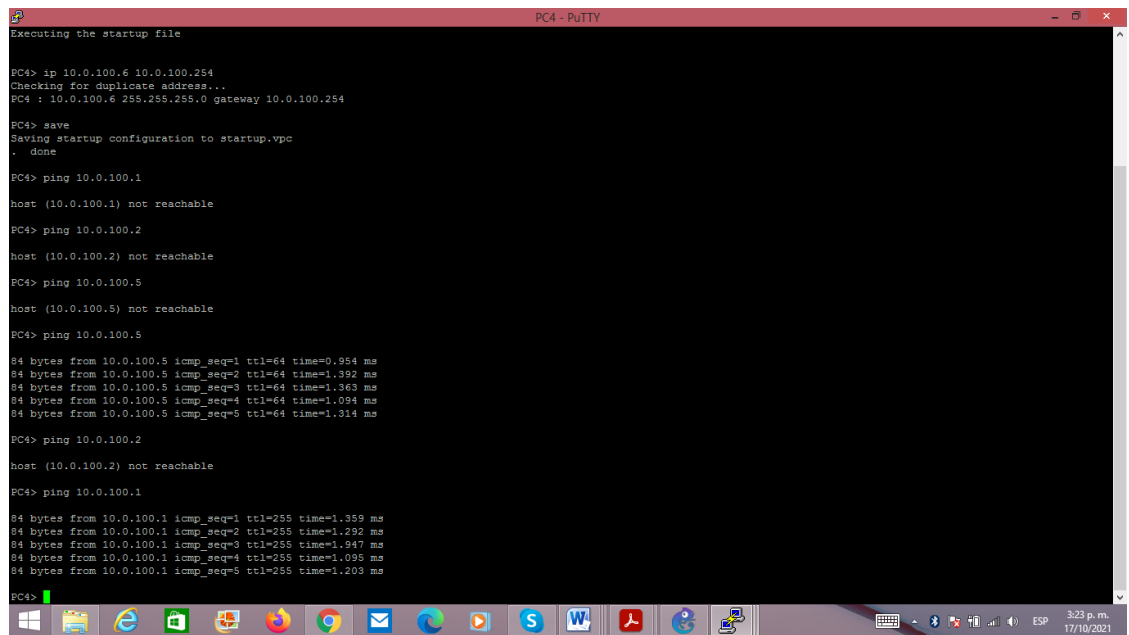
```
Executing the startup file
PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254
PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254
PC2> ping 10.0.102.1
host (10.0.102.1) not reachable
PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.384 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.701 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.467 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.476 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.737 ms
PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254
PC2> ip dhcp
DORA IP 10.0.102.210/24 GW 10.0.102.254
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=1.014 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.995 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=1.181 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=1.271 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.191 ms
PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.400 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.594 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.537 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.518 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.579 ms
PC2>
```

Figura 7. Conectividad PC3



```
PC3 - PuTTY
Clear ip/ipv6 address, arp/neighbor table, command history.
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3>
PC3> #h
NAME IP/MASK GATEWAY MAC LPORT RHOST:PO
RT
PC3 10.0.101.110/24 10.0.101.254 00:50:79:66:68:02 20030 127.0.0.
1:20031
fe80::250:79ff:fe66:6802/64
2001:db8:100:101:2050:79ff:fe66:6802/64 eui-64
PC3> ping 10.0.101.1
10.0.101.1 icmp_seq=1 timeout
10.0.101.1 icmp_seq=2 timeout
10.0.101.1 icmp_seq=3 timeout
10.0.101.1 icmp_seq=4 timeout
10.0.101.1 icmp_seq=5 timeout
PC3>
PC3>
PC3>
PC3>
```

Figura 8. Conectividad PC4



```
PC4 - PuTTY
Executing the startup file
PC4> ip 10.0.100.6 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC4> save
Saving startup configuration to startup.vpc
. done
PC4> ping 10.0.100.1
host (10.0.100.1) not reachable
PC4> ping 10.0.100.2
host (10.0.100.2) not reachable
PC4> ping 10.0.100.5
host (10.0.100.5) not reachable
PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.954 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=1.392 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=1.363 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=1.094 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=1.314 ms
PC4> ping 10.0.100.2
host (10.0.100.2) not reachable
PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=1.359 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=1.292 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=1.947 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=1.095 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=1.203 ms
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. Tareas para protocolos de enrutamiento

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	<p>Use OSPF Process ID <b>4</b> y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"><li>• R1: 0.0.4.1</li><li>• R3: 0.0.4.3</li><li>• D1: 0.0.4.131</li><li>• D2: 0.0.4.132</li></ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"><li>• En R1, no publique la red R1 – R2.</li><li>• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li></ul> <p>Deshabilite las publicaciones OSPFv2 en:</p> <ul style="list-style-type: none"><li>• D1: todas las interfaces excepto G1/0/11</li><li>• D2: todas las interfaces excepto G1/0/11</li></ul>

3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	<p>Use OSPF Process ID <b>6</b> y asigne los siguientes router-IDs:</p> <ul style="list-style-type: none"> <li>• R1: 0.0.6.1</li> <li>• R3: 0.0.6.3</li> <li>• D1: 0.0.6.131</li> <li>• D2: 0.0.6.132</li> </ul> <p>En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.</p> <ul style="list-style-type: none"> <li>• En R1, no publique la red R1 – R2.</li> <li>• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.</li> </ul> <p>Deshabilite las publicaciones OSPFv3 en:</p> <ul style="list-style-type: none"> <li>• D1: todas las interfaces excepto G1/0/11</li> <li>• D2: todas las interfaces excepto G1/0/11</li> </ul>
3.3	En R2 en la “Red ISP”, configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> <li>• Una ruta estática predeterminada IPv4.</li> <li>• Una ruta estática predeterminada IPv6.</li> </ul> <p>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.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/32).</li> <li>• La ruta por defecto (0.0.0.0/0).</li> </ul> <p>En IPv6 address family, anuncie:</p>

		<ul style="list-style-type: none"> <li>• La red Loopback 0 IPv4 (/128).</li> <li>• La ruta por defecto (::/0).</li> </ul>
3.4	En R1 en la “Red ISP”, configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> <li>• Una ruta resumen IPv4 para 10.0.0.0/8.</li> <li>• Una ruta resumen IPv6 para 2001:db8:100::/48.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>• Deshabilite la relación de vecino IPv6.</li> <li>• Habilite la relación de vecino IPv4.</li> <li>• Anuncie la red 10.0.0.0/8.</li> </ul> <p>En IPv6 address family:</p> <ul style="list-style-type: none"> <li>• Deshabilite la relación de vecino IPv4.</li> <li>• Habilite la relación de vecino IPv6.</li> <li>• Anuncie la red 2001:db8:100::/48.</li> </ul>

Se configuran los protocolos de enrutamiento IPv4 e IPv6, el single- área OSPFv2, OSPFv3, con el fin de que la red sea totalmente convergente.

#### Código configuración para Switch D1:

```
D1(config)#
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
router ID OSPF4
```

*Configuración de la*

D1(config-router)#netwo	
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0 <i>la ruta del área 0.</i>	<i>Asignación de la red a</i>
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0 <i>la ruta del área 0.</i>	<i>Asignación de la red a</i>
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0 <i>la ruta del área 0.</i>	<i>Asignación de la red a</i>
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0 <i>la ruta del área 0.</i>	<i>Asignación de la red a</i>
D1(config-router)#passive-interface default	
D1(config-router)# no passive-interface e2/0	
D1(config-router)#exit	
D1(config)#	
D1(config)#ipv6 router ospf 6	
D1(config-rtr)#router-id 0.0.6.131 <i>router ID OSPF6</i>	<i>Configuración de la</i>
D1(config-rtr)#passive-interface default	
D1(config-rtr)# no passive-interface e2/0	
D1(config-rtr)#exit	
D1(config)#	
D1(config)#interface e2/0	
D1(config-if)#ipv6 ospf 6 area 0 <i>OSPF6 en área 0</i>	<i>Configuración del</i>
D1(config-if)#exit	
D1(config)#interface vlan 100	
D1(config-if)#ipv6 ospf 6 area 0 <i>OSPF6 en área 0</i>	<i>Configuración del</i>
D1(config-if)#exit	
D1(config)#interface vlan 101	
D1(config-if)#ipv6 ospf 6 area 0 <i>OSPF6 en área 0</i>	<i>Configuración del</i>
D1(config-if)#exit	
D1(config)#interface vlan 102	
D1(config-if)#ipv6 ospf 6 area 0 <i>OSPF6 en área 0</i>	<i>Configuración del</i>
D1(config-if)#exit	

## Código configuración para Switch D2:

```
D2#confi t
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132          Configuración de la
router ID OSPF4
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0  Asignación de la red a
la ruta del área 0.
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0  Asignación de la red a
la ruta del área 0.
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0  Asignación de la red a
la ruta del área 0.
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0   Asignación de la red a
la ruta del área 0.
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface e2/0
D2(config-router)#exit
D2(config)#
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132              Configuración de la
router ID OSPF6
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface e2/0
D2(config-rtr)#exit
D2(config)#interface e2/0
D2(config-if)#ipv6 ospf 6 area 0               Configuración del
OSPF6 en área 0
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0              Configuración del
OSPF6 en área 0
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0              Configuración del
OSPF6 en área 0
D2(config-if)#exit
D2(config)#interface vlan 102
```

```
D2(config-if)#ipv6 ospf 6 area 0
OSPF6 en área 0
D2(config-if)#exit
```

*Configuración del*

### **Código configuración Para Router R1:**

```
R1(config)# router osp
R1(config)#router ospf 4
R1(config-router)# router-id 0.0.4.1
router ID OSPF4.
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
la ruta del área 0.
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
la ruta del área 0.
R1(config-router)#default-
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
router ID OSPF6
R1(config-rtr)#default-information originate
R1(config-rtr)#exit
R1(config)#interfac
R1(config)#interface e2/0
R1(config-if)#ipv6 ospf 6 area 0
OSPF6 en área 0
R1(config-if)#exit
R1(config)#
R1(config)#interface s1/0
R1(config-if)#ipv6 osp
R1(config-if)#ipv6 ospf 6 area 0
OSPF6 en área 0
R1(config-if)#exit
R1(config)#
```

*Configuración de la*

*Asignación de la red a*

*la ruta del área 0.*

*Configuración de la*

*Configuración del*

*Configuración del*

```

R1(config)#ip route 10.0.0.0 255.0.0.0 null0
R1(config)#ipv6 route 2001:db8:100::/48 null0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neigh
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)#neighbor 209.165.200.226 activate
R1(config-router-af)#no neighbor 2001:db8:200::2 activate
R1(config-router-af)#netwo
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit-address-family
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.226 activate
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#exit-address-family
R1(config-router)#exit
R1(config)#exit
R1#

```

*Configuración de la dirección bgp*

*Configuración de la dirección de vecino*

*Configuración de la dirección de vecino*

*Configuración de la dirección de vecino*

*Configuración de la dirección de vecino*

*Configuración de la dirección de vecino*

*Configuración de la dirección de vecino*

*Configuración de la dirección de vecino*

### **Código configuración Para Router R2:**

```

R2#
R2#config t
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R2(config)#ipv6 route ::/0 loopback 0

```

*Configuración de las rutas estáticas a través de la interfaz Loopback 0*

*Configuración de las rutas estáticas a través de la interfaz Loopback 0*

```

R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2           Configuración de la
dirección bgp
R2(config-router)#neighbor 209.165.200.225 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300   Configuración
de la dirección de vecino
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate     Configuración
de la dirección de vecino
R2(config-router-af)#no neighbor 2001:db8:200::1 activate  Configuración
de la dirección de vecino
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate  Configuración
de la dirección de vecino
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#exit
R2(config)#exit
R2#

```

### **Código configuración para Router R3:**

```

R3#config t
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3           Configuración de la
router ID OSPF4
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0       Asignación de la red a
la ruta del área 0.
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0       Asignación de la red a
la ruta del área 0.
R3(config-router)#exit

```

```

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

```

*Configuración de la*

*Configuración del*

#### **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. Tareas para la redundancia del primer salto

<b>Tarea#</b>	<b>Tarea</b>	<b>Especificación</b>
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> <li>• Use la SLA número <b>4</b> para IPv4.</li> <li>• Use la SLA número <b>6</b> para IPv6.</li> </ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.</p> <ul style="list-style-type: none"> <li>• Use el número de</li> </ul>

		<p>rastreo <b>4</b> para la IP SLA 4.</p> <ul style="list-style-type: none"> <li>• Use el número de rastreo <b>6</b> para la IP SLA 6.</li> </ul> <p>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.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> <li>• Use la SLA número <b>4</b> para IPv4.</li> <li>• Use la SLA número <b>6</b> para IPv6.</li> </ul> <p>Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sin tiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.</p> <ul style="list-style-type: none"> <li>• Use el número de rastreo <b>4</b> para la IP SLA 4.</li> <li>• Use el número de rastreo <b>6</b> para la SLA 6.</li> </ul> <p>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.</p>

Se configuran los SLAs, las prioridades, el protocolo HSRP en versión 2 para IPV4, y para IPV6:

## Código configuración para Switch D1:

```
D1(config)#ip sla 4
D1(config-ip-sla)#icmp-echo 10.0.10.1
mensaje de control para verificar conectividad
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1
de mensaje de control para verificar conectividad
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#
D1(config)#ip sla schedule 4 life forever start-time now
SLA, e indica su actividad
D1(config)#ip sla schedule 6 life forever start-time now
SLA, e indica su actividad
D1(config)#track 4 ip sla 4
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#tra
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#interface vlan 100
D1(config-if)#stand
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#
D1(config-if)# standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 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 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#
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
D1(config)#
D1(config)#
D1(config)#
```

### **Código configuración para Switch D2:**

```
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1
mensaje de control para verificar conectividad
```

*Configuración de*

```

D2(config-ip-sla-echo)#frecu
D2(config-ip-sla-echo)#frecuen
D2(config-ip-sla-echo)#freq
D2(config-ip-sla-echo)#frequency
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#ip sla 6
D2(config-ip-sla)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1
de mensaje de control para verificar conectividad
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
SLA, e indica su actividad
D2(config)#ip sla schedule 6 life forever start-time now
SLA, e indica su actividad
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
D2(config)#
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt
D2(config-if)#
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 preempt
D2(config-if)#
D2(config-if)#standby 106 track 6 decrement 60

```

*Configuración*

*Habilita el IP*

*Habilita el IP*

```
D2(config-if)#
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#
D2(config-if)#standby 116 track 6 decrement 60
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 preempt
D2(config-if)#
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit
D2(config)#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. Tareas para la seguridad de la red.

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: <b>cisco12345cisco</b>
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: <b>sadmin</b> • Nivel de privilegio 15 • Contraseña: <b>cisco12345cisco</b>
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: <b>\$strongPass</b>
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: <b>raduser</b> y la contraseña: <b>upass123</b> .

Se configura en todos los dispositivos un usuario y una contraseña de autenticación, y se habilita el modo privilegiado de encriptado scrypt para encriptar y guardar dicha protección creada.

### **Código configuración para Router R1:**

```
R1#conf t
R1(config)#enab
R1(config)#enable alg
R1(config)#enable algorithm-type sc
R1(config)#enable algorithm-type scrypt
R1(config)#enable algorithm-type scrypt sec
R1(config)#enable algorithm-type scrypt secret cisco12345cisco Configuración de la protección al acceso a EXEC privilegiado
R1(config)#
R1(config)#
R1#conf t
R1(config)#user
R1(config)#usern
R1(config)#username sadmin privi
R1(config)#username sadmin privilege 15 algo
R1(config)#username sadmin privilege 15 algorithm-type scr
R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R1(config)#exit
R1#
R1#conf t
R1(config)#aaa new-model Configuración de la autenticación
R1(config)#exit
R1#
R1#conf t
R1(config)#radius ser
R1(config)#radius server RADIUS Configuración de la IP del servidor Radius y los puertos
```

```

R1(config-radius-server)#addr
R1(config-radius-server)#address ipv4 10.0.100.6 aut
R1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)#key $strongPass Configuración de la
contraseña.
R1(config-radius-server)#exit
R1(config)#exit
R1#
R1#
R1#conf t
R1(config)#aaa authe
R1(config)#aaa authentication log
R1(config)#aaa authentication login def
R1(config)#aaa authentication login default gr
R1(config)#aaa authentication login default group r
R1(config)#aaa authentication login default group radius loc
R1(config)#aaa authentication login default group radius local Configuración
de la autenticación
R1(config)#exit
R1#

```

### **Código configuración para Router R2:**

```

R2#
R2#conf t
R2(config)#enable alg
R2(config)#enable algorithm-type scr
R2(config)#enable algorithm-type script secret cisco12345cisco
R2(config)#
R2(config)#exit
R2#
R2#conf t
R2(config)#usern
R2(config)#username sadmin priv
R2(config)#username sadmin privilege 15 alg

```

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

### **Código configuración para Router R3:**

```
R3#
R3#conf t
R3(config)#enab
R3(config)#enable alg
R3(config)#enable algorithm-type scr
R3(config)#enable algorithm-type scrypt sec
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
R3(config)#
R3(config)#exit
R3#
R3#conf t
R3(config)#user
R3(config)#usern
R3(config)#username sadmin priv
R3(config)#username sadmin privilege 15 alg
R3(config)#username sadmin privilege 15 algorithm-type scr
R3(config)#username sadmin privilege 15 algorithm-type scrypt cisco12345cisco
R3(config)#username sadmin privilege 15 algorithm-type scrypt secret
cisco12345cisco
R3(config)#
R3(config)#exit
R3#
R3#conf t
R3(config)#aaa new-model
autenticación
R3(config)#exit
```

*Configuración de la*

```

R3#
R3#conf t
R3(config)#radius server RADIUS Configuración de la IP
del servidor Radius y los puertos
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)#key $strongPass Configuración de la
contraseña.
R3(config-radius-server)#exit
R3(config)#exit
R3#
R3#conf t
R3(config)#aaa authentication login default group radius local Configuración
de la autenticación
R3(config)#exit

```

### **Código configuración para Switch D1:**

```

D1#conf t
D1(config)#enabl
D1(config)#enable algo
D1(config)#enable algorithm-type scr
D1(config)#enable algorithm-type scrypt secr
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D1(config)#
D1(config)#exit
D1#conf t
D1(config)#usern
D1(config)#username sadmin pri
D1(config)#username sadmin privilege 15 algo
D1(config)#username sadmin privilege 15 algorithm-type scr
D1(config)#username sadmin privilege 15 algorithm-type scrypt secret
cisco12345cisco
D1(config)#
D1(config)#exit
D1#conf t

```

```

D1(config)#aaa new-model
autenticación
D1(config)#
D1(config)#exit
D1#
D1#conf t
D1(config)#radius server RADIUS
Configuración de la IP
del servidor Radius y los puertos
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)#key $strongPass
Configuración de la
contraseña.
D1(config-radius-server)#exit
D1(config)#end
D1#
D1#conf t
D1(config)#
D1(config)#aaa authentication login default group radius local
Configuración
de la autenticación
D1(config)#exit
D1#

```

### **Código configuración para Switch D2:**

```

D2#
D2#conf t
D2(config)#enable alg
D2(config)#enable algorithm-type scr
D2(config)#enable algorithm-type scrypt sec
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
D2(config)#
D2(config)#exit
D2#
D2#conf t
D2(config)#username sad
D2(config)#username sadmin pri

```

```

D2(config)#username sadmin privilege 15
D2(config)#username sadmin privilege 15 al
D2(config)#username sadmin privilege 15 algorithm-type scr
D2(config)#username sadmin privilege 15 algorithm-type scrypt secret
cisco12345cisco
D2(config)#exit
D2#
D2#conf t
D2(config)#aaa new-model Configuración de la
autenticación
D2(config)#
D2(config)#end
D2#
D2#conf t
D2(config)#radius server RADIUS Configuración de la IP del
servidor Radius y los puertos
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $strongPass Configuración de la
contraseña.
D2(config-radius-server)#e
D2(config-radius-server)#exit
D2(config)#end
D2#conf t
D2(config)#aaa authentication login default group radius local Configuración
de la autenticación
D2(config)#exit

```

### **Código configuración para Switch A1:**

```

A1#conf t
A1(config)#enable algo
A1(config)#enable algorithm-type scry
A1(config)#enable algorithm-type scrypt secret cisco12345cisco
A1(config)#
A1(config)#exit
A1#

```

```

A1#conf t
A1(config)#usern
A1(config)#username sadmin privilege 15 algorithm-type scrypt secret
cisco12345cisco
A1(config)#exit
A1#conf t
A1(config)#aaa new-model Configuración de la
autenticación
A1(config)#
A1(config)#exit
A1#conf t
A1(config)#radius server RADIUS Configuración de la IP del
servidor Radius y los puertos
A1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)#
A1(config-radius-server)#key $strongPass Configuración de la
contraseña.
A1(config-radius-server)#exit
A1(config)#end
A1#
A1#conf t
A1(config)#
A1(config)#aaa authentication login default group radius local
A1(config)#exit

```

**Verificación de los servicios AAA en los dispositivos:**

Figura 9. Verificación servicio AAA R1

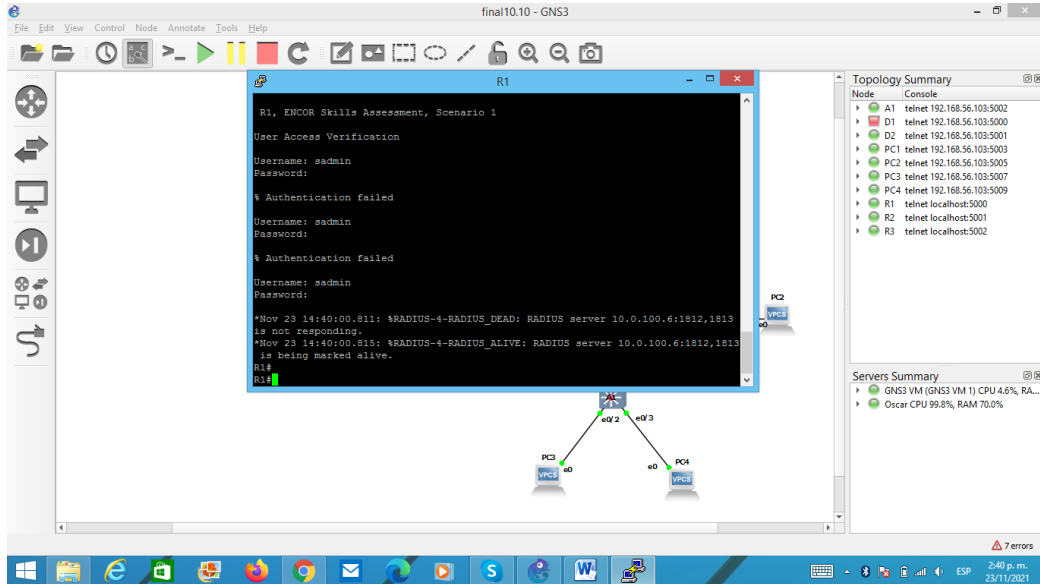


Figura 10. Verificación servicio AAA R3

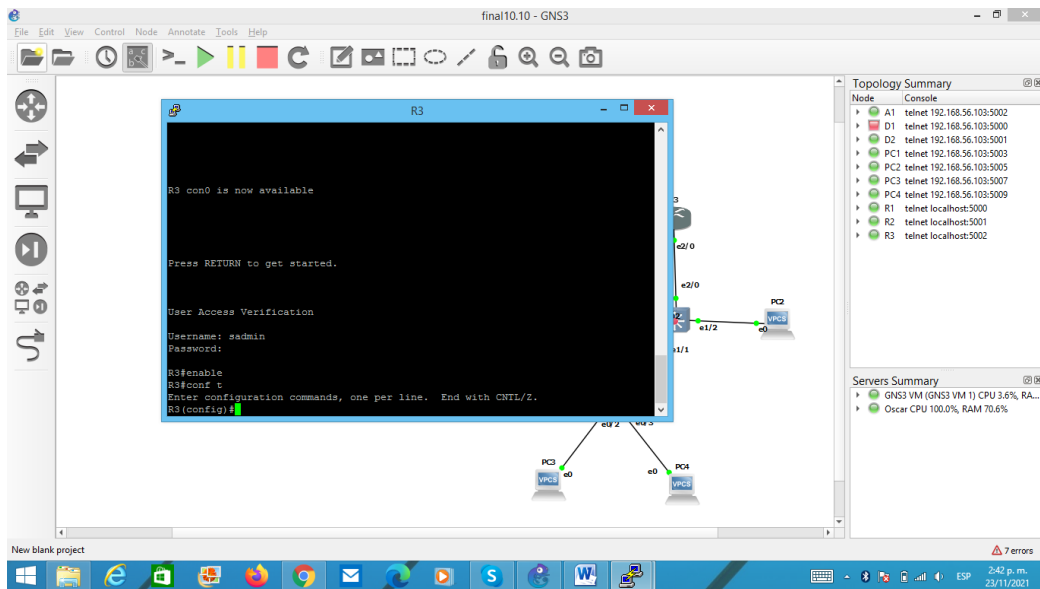


Figura 11. Verificación servicio AAA D1

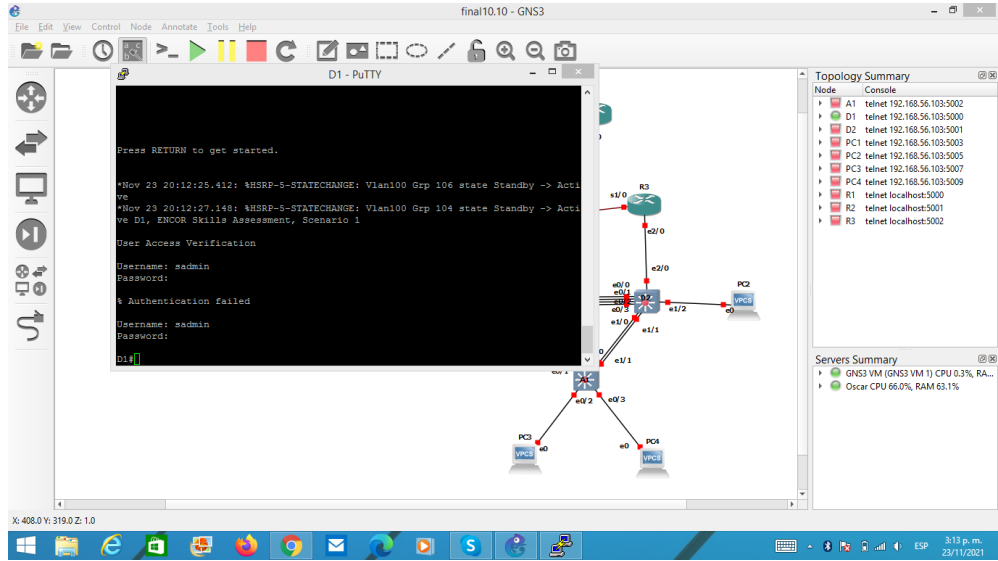


Figura 12. Verificación servicio AAA D2

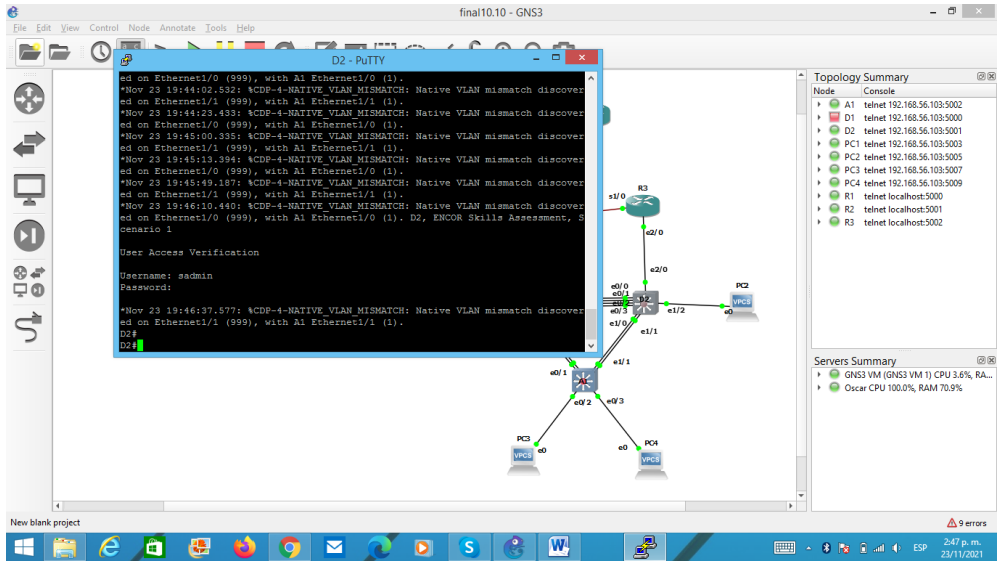
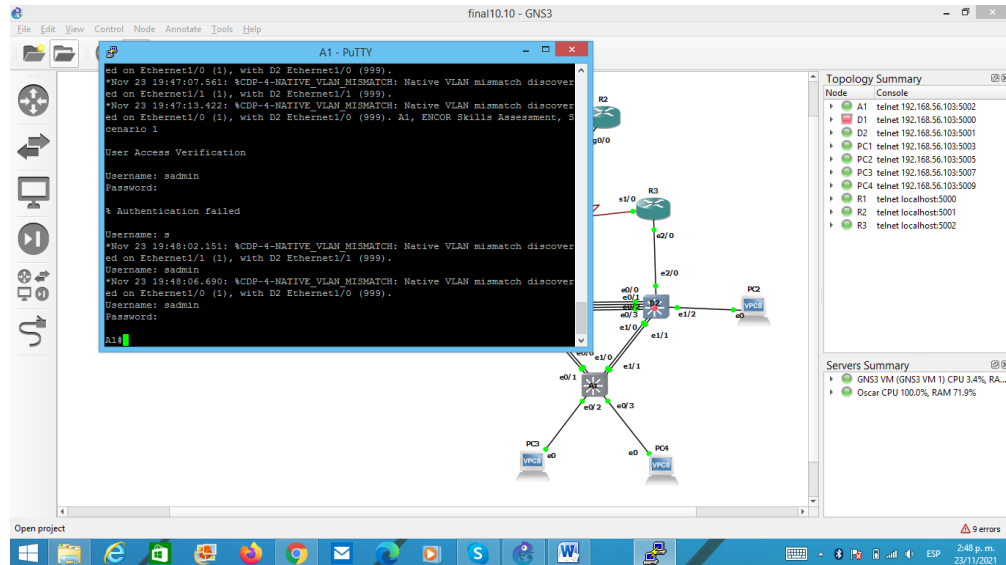


Figura 13. Verificación servicio AAA A1



## 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. Tareas para las funciones de administración de red.

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"> <li>• R1 debe sincronizar con R2.</li> <li>• R3, D1 y A1 para sincronizar la hora con R1.</li> <li>• D2 para sincronizar la hora con R3.</li> </ul>
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel

		WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	<p>Especificaciones de SNMPv2:</p> <ul style="list-style-type: none"> <li>• Únicamente se usará SNMP en modo lectura (Read-Only).</li> <li>• Limite el acceso SNMP a la dirección IP de la PC1.</li> <li>• Configure el valor de contacto SNMP con su nombre.</li> <li>• Establezca el community string en ENCORSA.</li> <li>• En R3, D1, y D2, habilite el envío de traps config y ospf.</li> <li>• En R1, habilite el envío de traps bgp, config, y ospf.</li> <li>• En A1, habilite el envío de traps config.</li> </ul>

Se configura en todos los dispositivos los parámetros de administración de red como son la sincronización de fecha y hora, y el protocolo simple de administración de red SNMPv2c.

### **Código configuración para Switch D1:**

```

D1#conf t
D1(config)#cloc
D1(config)#clock tim
D1(config)#clock timezone
D1(config)#clock timezone CO -5
D1(config)#exit
D1#
D1#conf t
D1(config)#ntp ser
D1(config)#ntp server 10.0.10.1
D1(config)#exit
D1#conf t
D1(config)#logg

```

```
D1(config)#logging tr
D1(config)#logging trap war
D1(config)#logging trap warning
D1(config)#logging hos
D1(config)#logging host 10.0.100.5
D1(config)#logging on
D1(config)#exit
D1#
D1#conf t
D1(config)#ip acce
D1(config)#ip access-list stan
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)#permit
D1(config-std-nacl)#permit ho
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#
D1(config)#sn
D1(config)#snmp-
D1(config)#snmp-server c
D1(config)#snmp-server conta
D1(config)#snmp-server contact Cisc
D1(config)#snmp-server contact Cisco OSCAR
D1(config)#sn
D1(config)#snmp-
D1(config)#snmp-server comm
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server hos
D1(config)#snmp-server host 10.0.100.5 vers
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server if
D1(config)#snmp-server ifindex pe
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server ena
D1(config)#snmp-server enable tr
```

```

D1(config)#snmp-server enable traps os
D1(config)#snmp-server enable traps ospf
D1(config)#snmp-server enable traps confi
D1(config)#snmp-server enable traps config                               Comando    no
reconocido por el dispositivo
D1(config)#exit
D1#

```

### **Código configuración para Switch D2:**

```

D2(config)#
D2(config)#clock timezone CO -5
D2(config)#exit
D2#conf t
D2(config)#ntp server 10.0.10.1
D2(config)#
D2(config)#exit
D2#conf t
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#
D2(config)#logging on
D2(config)#exit
D2#conf t
D2(config)#
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#exit
D2(config)#snmp-server contact Cisco OSCAR
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server enable traps ospf
D2(config)#snmp-server enable traps config                               Comando    no
reconocido por el dispositivo

```

D2(config)#exit

### **Código configuración para Switch A2:**

A1#

A1#conf t

A1(config)#clock timezone CO -5

A1(config)#exit

A1#conf t

A1(config)#

A1(config)# ntp server 10.0.10.1

A1(config)#exit

A1#conf t

A1(config)#logging trap warning

A1(config)#logging host 10.0.100.5

A1(config)#logging on

A1(config)#exit

A1#conf t

A1(config)#ip access-list standard SNMP-NMS

A1(config-std-nacl)#permit host 10.0.100.5

A1(config-std-nacl)#exit

A1(config)#snmp-server contact Cisco Oscar

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 ospf

A1(config)#snmp-server enable traps config  
*reconocido por el dispositivo*

*Comando no*

A1(config)#exit

### **Código configuración para Router R1:**

R1#conf t

R1(config)#clock timezone CO -5

R1(config)#

```
R1(config)#exit
R1#conf t
R1(config)#ntp ser
R1(config)#ntp server 2.2.2.2
R1(config)#exit
R1#conf t
R1(config)#logg
R1(config)#logging tr
R1(config)#logging trap war
R1(config)#logging trap warning
R1(config)#logging hos
R1(config)#logging host 10.0.100.5
R1(config)#logging on
R1(config)#exit
R1#conf t
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)#permit host 10.0.100.5
R1(config-std-nacl)#exit
R1(config)#snmp-server contact Cisco OSCAR
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 ospf
R1(config)#snmp-server enable traps config
R1(config)#exit
R1#
```

### **Código configuración para Router R2:**

```
R2#conf t
R2(config)#clock timezone CO -5
R2(config)#exit
R2#conf t
```

```
R2(config)#ntp
R2(config)#ntp mas
R2(config)#ntp master 3
R2(config)#exit
R2#
```

### **Código configuración para Router R3:**

```
R3#conf t
R3(config)#clock timezone CO -5
R3(config)#exit
R3#conf t
R3(config)#ntp server 10.0.10.1
R3(config)#exit
R3#conf t
R3(config)#logging trap warning
R3(config)#logging host 10.0.100.5
R3(config)#logging on
R3(config)#exit
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip access-list standard SNMP-NMS
R3(config-std-nacl)#permit host 10.0.100.5
R3(config-std-nacl)#exit
R3(config)#snmp-server contact Cisco OSCAR
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 ospf
R3(config)#snmp-server enable traps config
R3(config)#exit
R3#
```

## CONCLUSIONES

La correcta programación de los enlaces troncales y los puertos de acceso de los dispositivos en capa 2, permite la conectividad de estos y el flujo confiable de los datos en la red.

Con el fin de tener seguridad sobre cualquier red, y evitar que personas ajenas ingresen y puedan realizar algún tipo de ataque, se deben configurar varios mecanismos de seguridad en los dispositivos incidentes en la topología, donde se debe incluir como mínimo usuario y contraseña para los diferentes modos de configuración, y encriptación de contraseñas para evitar que sea descifrada fácilmente.

Se debe tener en cuenta que en toda red se pueden presentar diversos fallos que pueden afectar la conectividad de los dispositivos, por esto es conveniente el diseño de una topología donde se pueda realizar una configuración de rutas redundantes para aislar el dispositivo en falla de la red y de este modo no afectar la conectividad de los demás dispositivos.

El uso de software especiales para simular la topología de una red es de gran ayuda para los estudiantes de las asignaturas de telecomunicaciones, puesto que estos ayudan a la interpretación y mayor entendimiento del comportamiento de todos los dispositivos dentro de una red en la vida real. No obstante de las grandes ventajas que presentan estos software, también hay que mencionar que presentan desventajas puntualmente con el software GNS3, puesto que este requiere de un equipo con buen nivel de procesamiento y con buena memoria de almacenamiento para su correcto funcionamiento.

## BIBLIOGRAFÍA

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Authenticating Wireless Clients. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8> 57

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). BGP. 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). EIGRP. 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). Enterprise Network Architecture. 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). Fabric Technologies. 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). Foundational Network Programmability Concepts. 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). Introduction to Automation Tools. 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). IP Routing Essentials. 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). 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). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Network Assurance. 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). Network Device Access Control and Infrastructure Security. 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). OSPF. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8> 56

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF v3. 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). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Troubleshooting Wireless Connectivity. 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). Understanding Wireless Roaming and Location 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). Virtualization. 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). VLAN Trunks and EtherChannel Bundles. 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). Wireless Signals and Modulation. 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). Wireless Infrastructure. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Mejia, O. A. (2011). Migración del protocolo IPv4 a IPv6. *ContactoS*, 79, 55-60.

Muñoz-Gallego, A. (2018). Protocolos RIP y OSPF. *Arquitectura de Redes y Servicios*.