DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NELSON HERNANDO FARFÁN RIVEROS

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NELSON HERNANDO FARFÁN RIVEROS

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 27 de noviembre de 2021

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por haberme dado los recursos el tiempo y la salud para poder concluir con mis estudios.
Un gran agradecimiento al tutor Gerardo Granados Acuña quien me oriento para llevar acabo el desarrollo de este curso de Diplomado.
También quiero agradecer a mi familia por apoyarme con sus buenos pensamientos; en especial a mis padres los que siempre han estado ahí para darme voz de aliento, a mis hijos a los cuales instó a salir adelante y decirles que, si se puede, y por último y no menos importante a mi esposa que me demuestra cada día que el esfuerzo da frutos.
Por ultimo agradecerle a la UNAD, tutores y demás por el apoyo que me han brindado a través de los años que estuve en la institución.

CONTENIDO

Pág.

LISTA DE IMÁGENES

Pág.

GLOSARIO

ACL — Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios accedan los recursos específicos. Un ACL contiene los hosts se permiten que o acceso negado al dispositivo de red. El router o el Switch examina cada paquete para determinar si remitir o caer el paquete, en base de los criterios especificados dentro de las Listas de acceso. Los criterios de lista de acceso podían ser la dirección de origen del tráfico, la dirección destino del tráfico, el Upper-Layer Protocol, o la otra información.

IPv4 — El IPv4 es un sistema direccional de 32 bits usado para identificar un dispositivo en una red. Es el sistema direccional usado en la mayoría de las redes informáticas, incluyendo Internet.

IPv6 — El IPv6 es un sistema direccional del 128-bit usado para identificar un dispositivo en una red. Es el sucesor al IPv4 y a la mayoría de la versión reciente del sistema direccional usado en las redes informáticas. El IPv6 se está desarrollando actualmente en todo el mundo. Un direccionamiento del IPv6 se representa en ocho campos de los números hexadecimales, cada campo que contiene 16 bits. Un direccionamiento del IPv6 se divide en dos porciones, cada parte integrada por 64 bits. La primera parte que es la dirección de red, y la segunda parte la dirección de host.

MSTP — El protocolo multiple spanning-tree (MSTP) es un protocolo que crea los árboles de expansión múltiple (casos) para cada Virtual LAN (VLAN) en una sola red física. Esto permite para que cada VLA N tenga una topología configurada del Root Bridge y de la expedición. Esto reduce el número de las Unidades (BPDU) a través de la red y reduce la tensión en las unidades de procesamiento central (CPU) de los dispositivos de red.

VLA N basado en protocolos — Los grupos basados en protocolos pueden ser definidos y estar limitados a un puerto; por lo tanto, cada paquete que origina de los grupos de protocolos se asigna al VLAN configurado en la página. El VLA N basado en protocolos divide la red física en los grupos VLAN lógicos para cada protocolo requerido. En el paquete de entrada, se marca la trama y la calidad de miembro de VLAN se puede determinar sobre la base del Tipo de protocolo. Los grupos basados en protocolos a la asignación del VLA N ayudan a asociar a un grupo de protocolos a un puerto único.

RESUMEN

Este documento presenta un escenario el cual se debe desarrollar en una plataforma de simulación, con este se pretende que el grupo de estudiantes presenten una solución de implementación, el documento sirve como apoyo para todo aquel que quiera aprender sobre configuraciones de equipos cisco, se construyó desarrollando el paso a paso propuesto por la guía, el laboratorio se implementó en la plataforma gns3 que es la que soporta todos los comandos necesarios para llevar a cabo todas las configuraciones solicitadas.

En los equipos se implementaron configuraciones en IPv4 e IPv6 para comprobar que las dos condiciones se pueden configurar en los equipos que se implementaron en la solución del escenario, se aplicaron protocolo bgp y ospf para poder probar las conexiones de todos los equipos.

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

ABSTRACT

This document presents a scenario which must be developed in a simulation platform, with this it is intended that the group of students present an implementation solution, the document serves as support for anyone who wants to learn about Cisco equipment configurations, it was built developing the step by step proposed by the guide, the laboratory was implemented on the gns3 platform, which is the one that supports all the necessary commands to carry out all the requested configurations.

In the computers configurations in IPv4 and IPv6 were implemented to verify that the two conditions can be configured in the computers that were implemented in the solution of the scenario, bgp and ospf protocols were applied to be able to test the connections of all the computers.

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

INTRODUCCIÓN

El diplomado CCNP tiene como finalidad, introducir a los estudiantes en los entornos de redes complejas, es vital si se habla del desarrollo laboral de TI, este trabajo se realiza como guía de configuración de diferentes protocolos necesarios para el funcionamiento de una red, a través de la construcción paso a paso de la configuración de cada uno de los equipos, se realizó con el apoyo continuo del instructor, se tomó como base la guía propuesta por el curso diplomado CCNP para construir cada una de las partes del documento y la configuración de los equipos.

El laboratorio se desarrolló en la plataforma gns3, se realizaron configuraciones de puertos troncales en los equipos principales, se construyó un sistema redundante de comunicación para evitar pérdidas de conexión si llegara a fallar alguno de los enlaces propuestos.

En la fase inicial se tenía que hacer la construcción del escenario propuesto por la guía, fue necesario hacer las conexiones entre equipos, se agregó la configuración propuesta por la guía realizando adaptaciones, no se tenían las mismas interfaces. En la segunda fase se configuraron los enlaces troncales, se definieron las vlans necesarias de conexión entre equipos, se crearon los Port channel. En la tercera fase se configuro el OSPFv2 y OSPFv3 según fue necesario, después se configuro el BGP para IPv4 e IPv6. En la cuarta fase se configuro el HSRPv2 en lo SW D1 y D2, mediante estos comandos se pudo rastrear objetos, definir los grupos y VLAN que intervinieron en las configuraciones. En la quinta fase se configuro toda la parte de seguridad en cada uno de los dispositivos. En la sexta fase se configuro el NTP y SNMPv2c, se establecieron las comunidades.

1 PRIMER PASO DE LA GUÍA

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

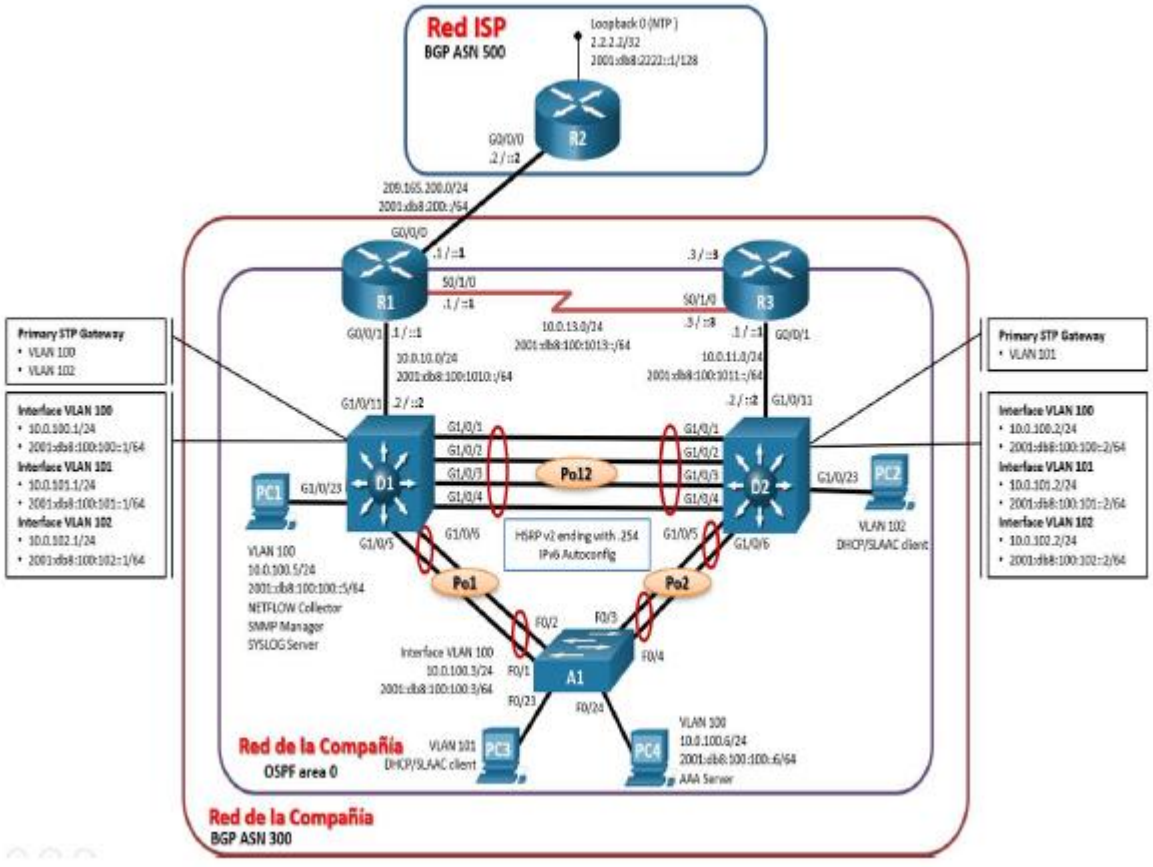
1.1 CABLEAR LA RED COMO SE MUESTRA EN LA TOPOLOGÍA.

1.2 CONECTE LOS DISPOSITIVOS COMO SE MUESTRA EN EL DIAGRAMA DE TOPOLOGÍA Y CONECTE LOS CABLES SEGÚN SEA NECESARIO.

1.3 CONFIGURAR LOS PARÁMETROS BÁSICOS PARA CADA DISPOSITIVO.

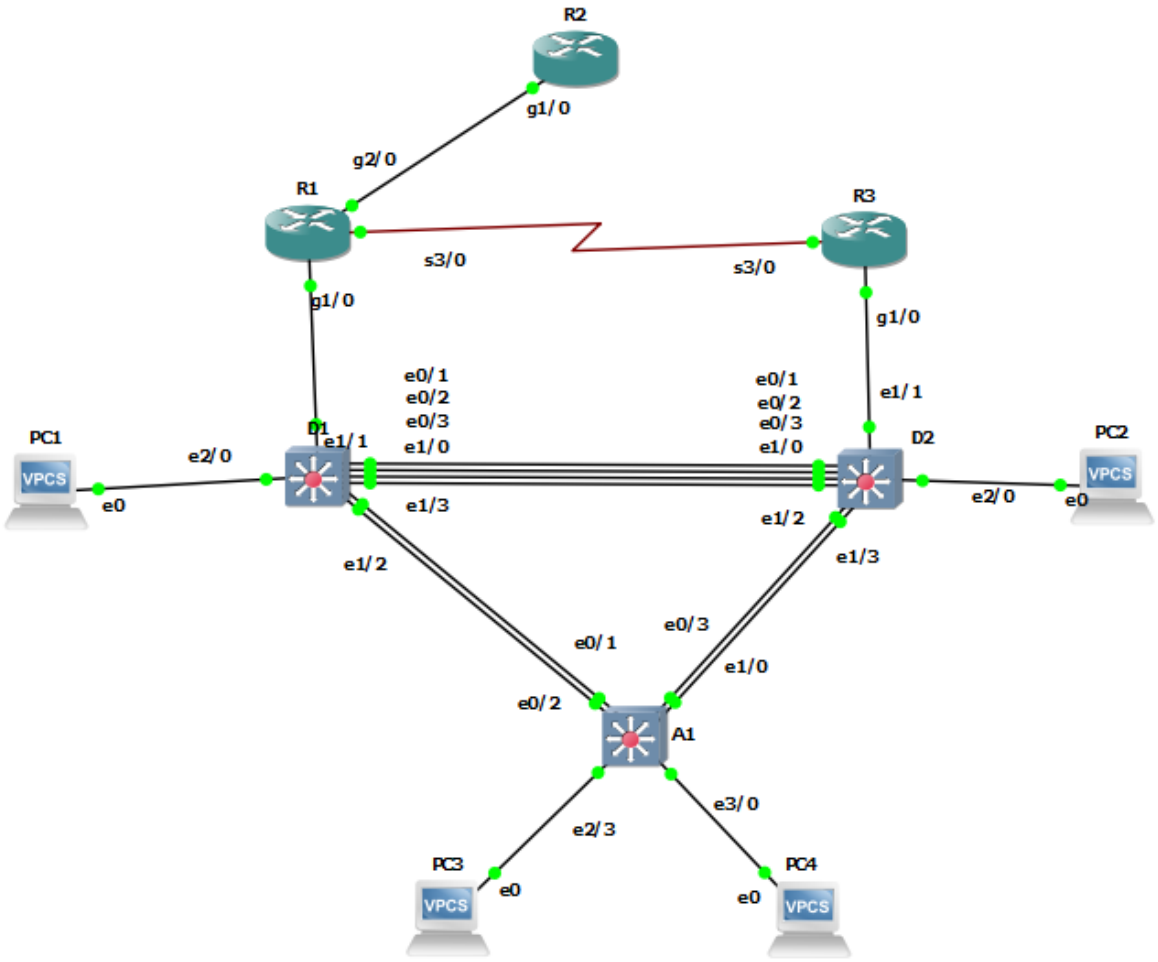
1.4 MEDIANTE UNA CONEXIÓN DE CONSOLA INGRESE EN CADA DISPOSITIVO, ENTRE AL MODO DE CONFIGURACIÓN GLOBAL Y APLIQUE LOS PARÁMETROS BÁSICOS. LAS CONFIGURACIONES DE INICIO PARA CADA DISPOSITIVO SON SUMINISTRADAS A CONTINUACIÓN:

Imagen 1. Escenario Propuesto por la Guía CCNP



Tomado de la guía del curso

Imagen 2. Escenario propuesto por el estudiante



1.5 CONFIGURACIÓN INICIAL DE DISPOSITIVOS

Se realizó la configuración del enrutador R1, se adaptó las interfaces del equipo para poder aplicar la configuración.

1.5.1 Configuración de R1

```
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 GigabitEthernet2/0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
R1(config-if)# negotiation auto
R1(config-if)# ipv6 address FE80::1:1 link-local
R1(config-if)# ipv6 address 2001:DB8:200::1/64
R1(config-if)#end

R1(config)#interface GigabitEthernet1/0
R1(config-if)# ip address 10.0.10.1 255.255.255.0
R1(config-if)# negotiation auto
R1(config-if)# ipv6 address FE80::1:2 link-local
R1(config-if)# ipv6 address 2001:DB8:100:1010::1/64
R1(config-if)#end

R1(config)#interface Serial3/0
R1(config-if)# ip address 10.0.13.1 255.255.255.0
R1(config-if)# ipv6 address FE80::1:3 link-local
R1(config-if)# ipv6 address 2001:DB8:100:1013::1/64
R1(config-if)# serial restart-delay 0
R1(config-if)#end
```

Se realizó la configuración del enrutador R2, se adaptó las interfaces del equipo para poder aplicar la configuración.

1.5.2 Configuración R2

```
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 GigabitEthernet1/0
R2(config-if)# ip address 209.165.200.226 255.255.255.224
R2(config-if)# negotiation auto
R2(config-if)# ipv6 address FE80::2:1 link-local
R2(config-if)# ipv6 address 2001:DB8:200::2/64
R2(config-if)#end

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 shutdown
R2(config-if)#exit
R2(config)#
```

Se realizó la configuración del enrutador R3, se adaptó las interfaces del equipo para poder aplicar la configuración.

1.5.3 Configuración R3

```
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 GigabitEthernet1/0
R3(config-if)# ip address 10.0.11.1 255.255.255.0
R3(config-if)# negotiation auto
R3(config-if)# ipv6 address FE80::3:2 link-local
R3(config-if)# ipv6 address 2001:DB8:100:1011::1/64
R3(config-if)#end

R3(config)#interface Serial3/0
R3(config-if)# ip address 10.0.13.3 255.255.255.0
R3(config-if)# ipv6 address FE80::3:3 link-local
R3(config-if)# ipv6 address 2001:DB8:100:1010::2/64
R3(config-if)# serial restart-delay 0
R3(config-if)#end
R3#
```

Se realizó la configuración del enrutador D1, se adaptó las interfaces del equipo para poder aplicar la configuración.

1.5.4 Configuración D1

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

D1(config)#inter ethernet 1/1
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-if)#exit
D1(config)#

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)#

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
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)#

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)#

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)#

D1(config)#interface range ethernet 2/0-2
D1(config-if-range)#shutdown
D1(config-if-range)#interface range ethernet 3/0-3
D1(config-if-range)#shutdown
D1(config-if-range)#
```

Se realizó la configuración del enrutador D2, se adaptó las interfaces del equipo para poder aplicar la configuración.

1.5.5 Configuración D2

```
D2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

```
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)#

D2(config)#interface ethernet 1/1
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)#

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 shutdown
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 shutdown
D2(config-if)#exit
D2(config)#
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)#inter range ethernet 2/0-2
D2(config-if-range)#sh
D2(config-if-range)#shutdown
D2(config-if-range)#inter range ethernet 3/0-3
D2(config-if-range)#shutdown
```

Se realizó la configuración del enrutador A1, se adaptó las interfaces del equipo para poder aplicar la configuración.

1.5.6 Configuración A1

```
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)#
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)#
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 shutdown
A1(config-if)#exit

A1(config)#inter range ethernet 1/1-3
A1(config-if-range)# shutdown
A1(config-if-range)#exit
A1(config)#inter range ethernet 2/0-2
A1(config-if-range)# shutdown
A1(config-if-range)#exit
A1(config)#inter range ethernet 3/1-3
A1(config-if-range)# shutdown
A1(config-if-range)#exit
A1(config)#
```

1.6 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.

Imagen 3. Configuración PC1

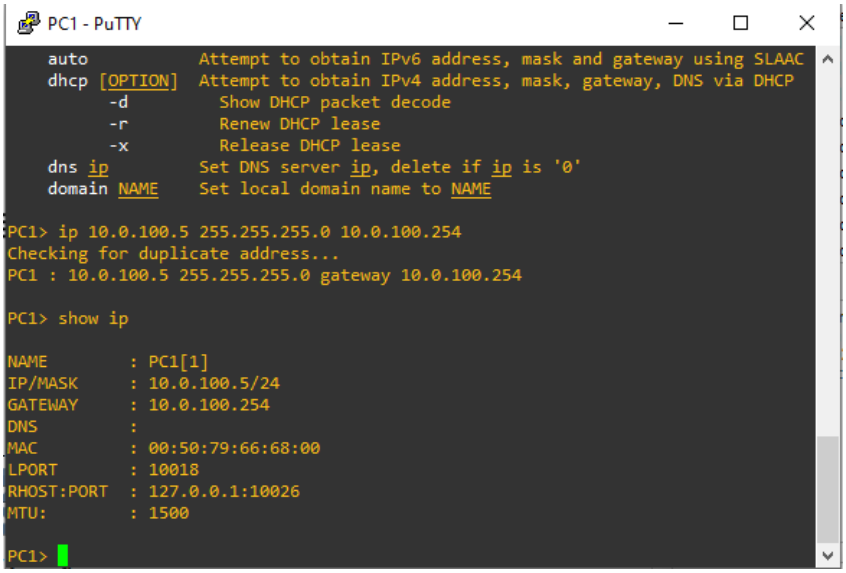
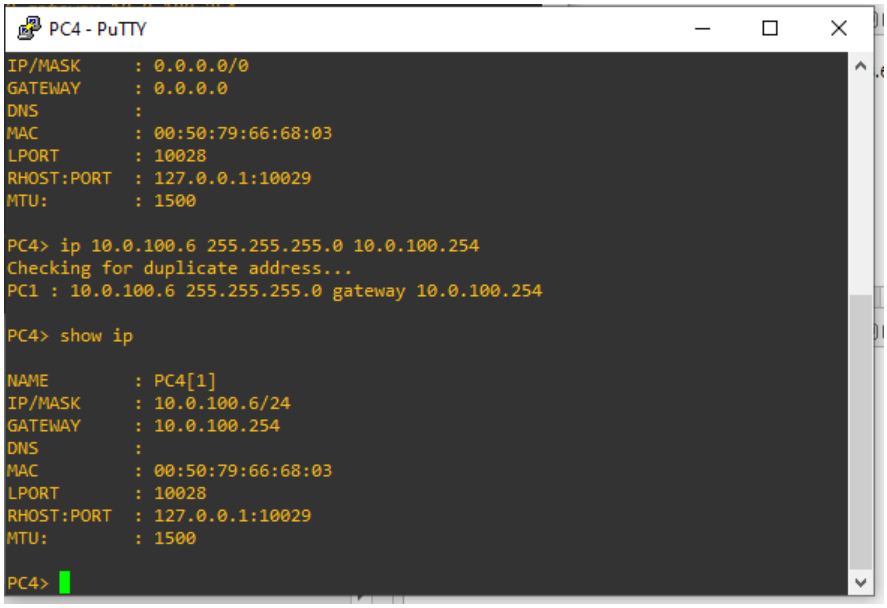


Imagen 4. Configuración PC4



2 SEGUNDO PASO DE LA GUÍA

2.1 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.

2.2 EN TODOS LOS SWITCHES CONFIGURE INTERFACES TRONCALES IEEE 802.1Q SOBRE LOS ENLACES DE INTERCONEXIÓN ENTRE SWITCHES.

Habilite enlaces trunk 802.1Q entre:
D1 and D2
D1 and A1
D2 and A1

2.2.1 Configuración de puertos en modo troncal en D1

```
D1(config)#inter range ethernet 0/1-3, ethernet 1/0, ethernet 1/2-3
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#
```

2.2.2 Configuración de puertos en modo troncal en D2

```
D2(config)#inter range ethernet 0/1-3, ethernet 1/0, ethernet 1/2-3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#
```

2.2.3 Configuración de puertos en modo troncal en A1

```
A1(config)#inter range et
A1(config)#inter range ethernet 0/1-3, et
A1(config)#inter range ethernet 0/1-3, ethernet 1/0
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#exit
A1(config)#
```

2.3 EN TODOS LOS SWITCHES CAMBIE LA VLAN NATIVA EN LOS ENLACES TRONCALES. USE VLAN 999 COMO LA VLAN NATIVA.

2.3.1 Configuración de la vlan nativa en D1

```
D1(config)#inter range ethernet 0/1-3, ethernet 1/0, ethernet 1/2-3
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#
```

2.3.2 Configuración de la vlan nativa en D2

```
D2(config)#inter range ethernet 0/1-3, ethernet 1/0, ethernet 1/2-3
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#
```

2.3.3 Configuración de la vlan nativa en A1

```
A1(config)#inter range ethernet 0/1-3, ethernet 1/0
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#
```

2.4 EN TODOS LOS SWITCHES HABILITE EL PROTOCOLO RAPID SPANNING-TREE (RSTP) USE RAPID SPANNING TREE (RSPT).

2.4.1 Configuración de spanning-tree en D1

```
D1(config)#spanning-tree mo
D1(config)#spanning-tree mode ra
D1(config)#spanning-tree mode rapid-pvst
D1(config)#
```

2.4.2 Configuración de spanning-tree en D2

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

2.4.3 Configuración de spanning-tree en A1

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

2.5 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.

2.5.1 Configuración de las vlan en D1

```
D1(config)#spanning-tree vlan 100 root primary
D1(config)#spanning-tree vlan 102 root primary
D1(config)#
```

2.5.2 Configuración de las vlan en D2

```
D2(config)#
D2(config)#spanning-tree vlan 101 root primary
D2(config)#
```

2.6 EN TODOS LOS SWITCHES, CREE ETHERCHANNELS LACP COMO SE MUESTRA EN EL DIAGRAMA DE TOPOLOGÍA

Use los siguientes números de canales:

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

2.6.1 Creación de port cannel en D1

```
D1(config)#interface range ethernet 0/1-3, ethernet 1/0
D1(config-if-range)#channel-group 12 mo
D1(config-if-range)#channel-group 12 mode on
Creating a port-channel interface Port-channel 12
D1(config-if-range)#

D1(config)#interface range ethernet 1/2-3
D1(config-if-range)#channel-group 1 mode on
D1(config-if-range)#
```

2.6.2 Creación de port cannel en D2

```
D2(config)#inter range ethernet 0/1-3, ethernet 1/0
D2(config-if-range)#channel-group 12 mode on
Creating a port-channel interface Port-channel 12
```

```
D2(config-if-range)#
```

2.6.3 Creación de port cannel en A1

```
A1(config)#interface range ethernet 0/1-2
A1(config-if-range)#cha
A1(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
A1(config-if-range)#

A1(config)#interface range ethernet 0/3, ethernet 1/0
A1(config-if-range)#channel-group 2 mode on
Creating a port-channel interface Port-channel 2
A1(config-if-range)#
```

2.7 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)

2.7.1 Configuración de los puertos en modo acceso en D1

```
D1(config)#inter ethernet 2/0
D1(config-if)#switchport access vlan 100
D1(config-if)#switchport mode access
D1(config-if)#spanning-tree portfast
D1(config-if)#
```

2.7.2 Configuración de los puertos en modo acceso en D2

```
D2(config)#interface ethernet 2/0
D2(config-if)#switchport access vlan 102
D2(config-if)#switchport mode access
D2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on Ethernet2/0 but will only
 have effect when the interface is in a non-trunking mode.
D2(config-if)#
```

2.7.3 Configuración de los puertos en modo acceso en A1

```
A1(config)#interface ethernet 2/3
A1(config-if)#sw
A1(config-if)#switchport acc
A1(config-if)#switchport access vla
A1(config-if)#switchport access vlan 101
A1(config-if)#switchport mode access
A1(config-if)#spanning-tree portfast
A1(config-if)#

A1(config)#interface ethernet 3/0
A1(config-if)#switchport access vlan 100
A1(config-if)#switchport mode access
A1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on Ethernet3/0 but will only
 have effect when the interface is in a non-trunking mode.
A1(config-if)#
```

2.8 VERIFIQUE LOS SERVICIOS DHCP IPV4. PC2 Y PC3 SON CLIENTES DHCP Y DEBEN RECIBIR DIRECCIONES IPV4 VÁLIDAS

Imagen 5. Configuración DHCP PC2

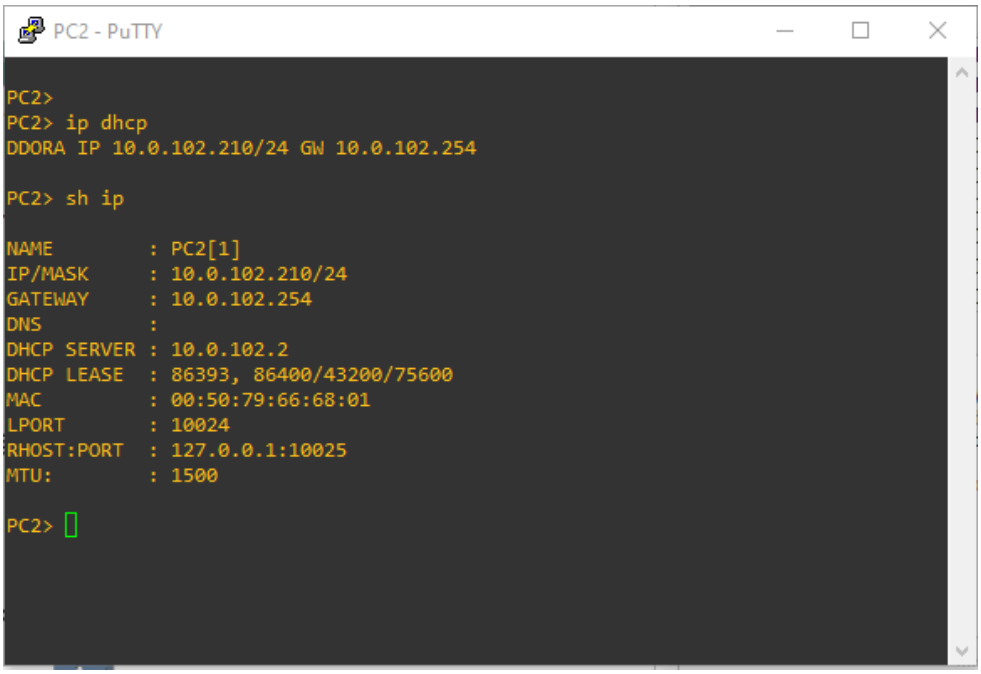
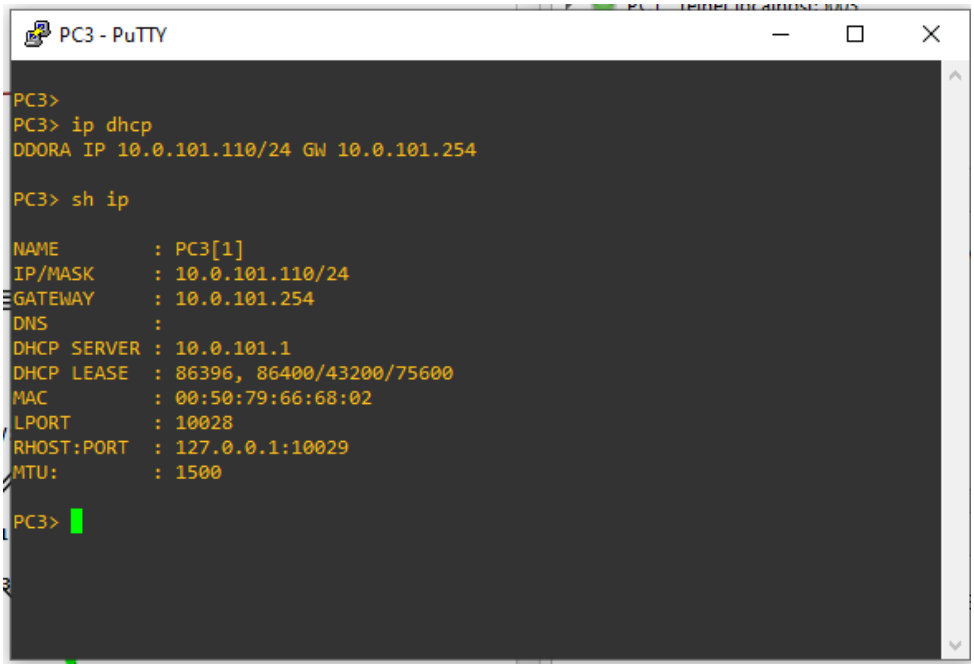


Imagen 6. Configuración DHCP PC3

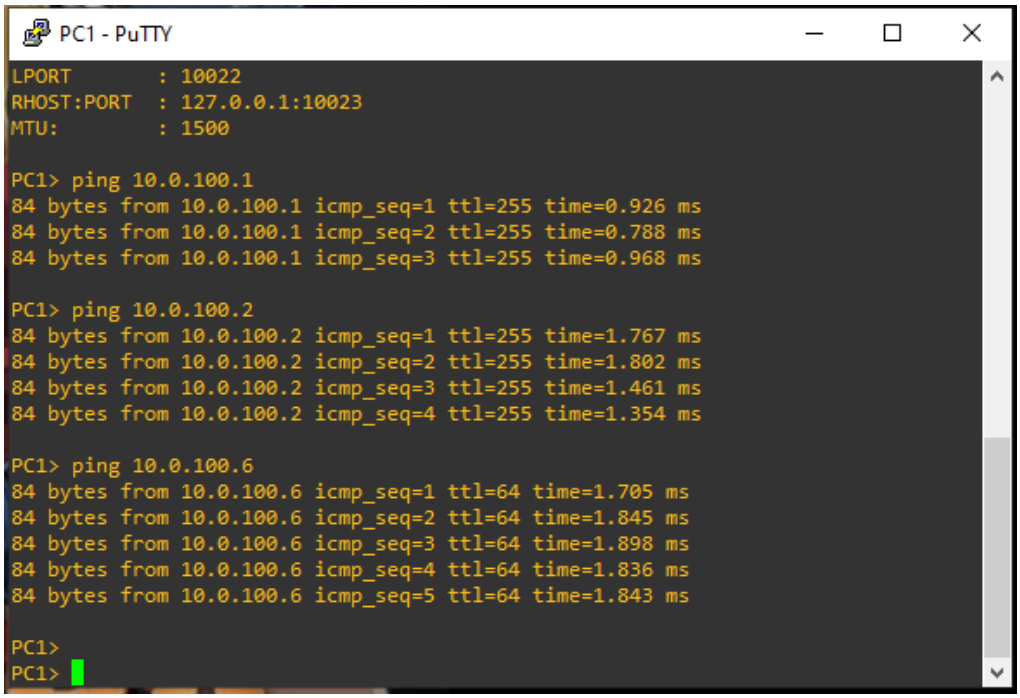


2.9 VERIFIQUE LA CONECTIVIDAD DE LA LAN LOCAL

2.9.1 PC1 debería hacer ping con éxito a:

D1: 10.0.100.1
D2: 10.0.100.2
PC4: 10.0.100.6

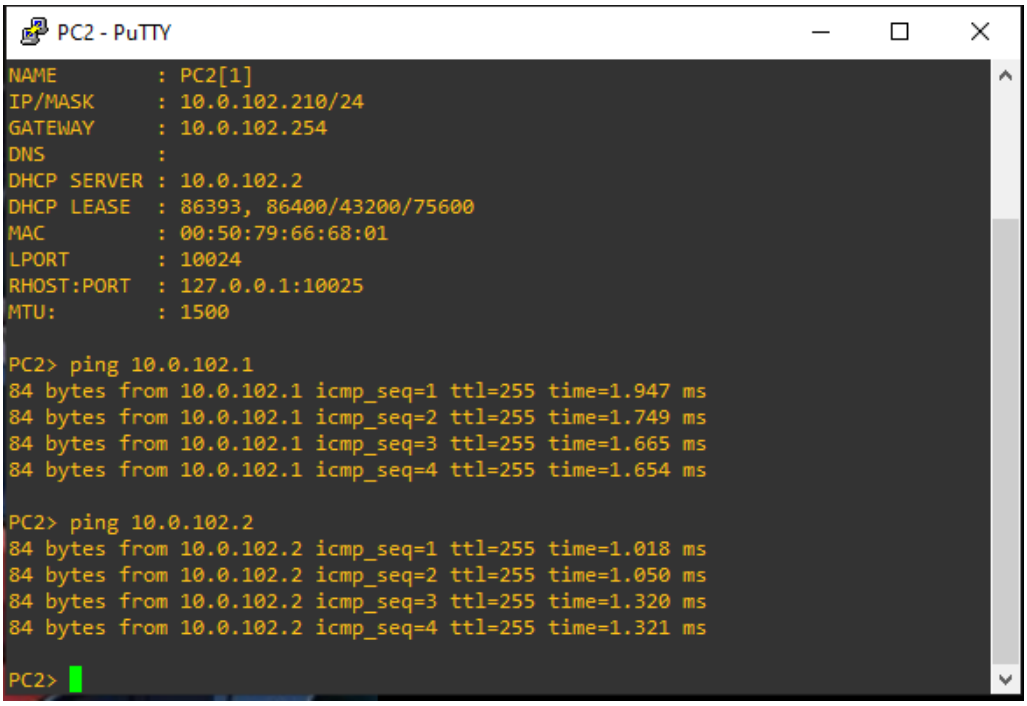
Imagen 7. Pruebas de ping del PC1



2.9.2 PC2 debería hacer ping con éxito a:

D1: 10.0.102.1
D2: 10.0.102.2

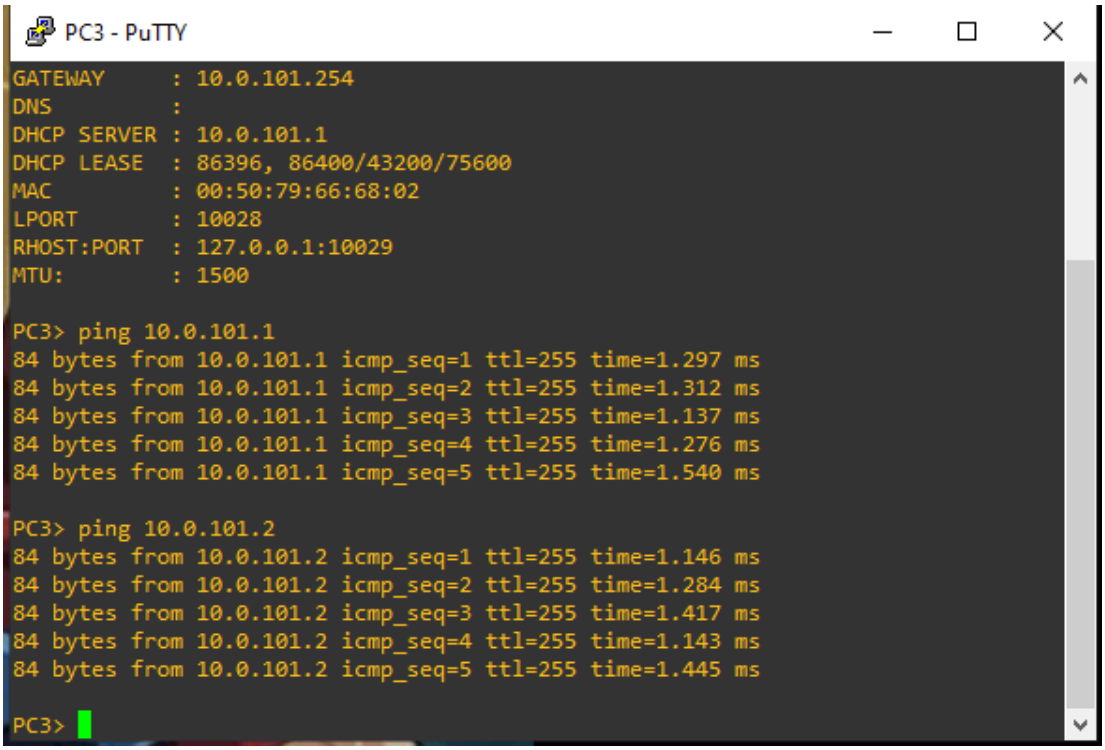
Imagen 8. Pruebas de ping del PC2



2.9.3 PC3 debería hacer ping con éxito a:

D1: 10.0.101.1
D2: 10.0.101.2

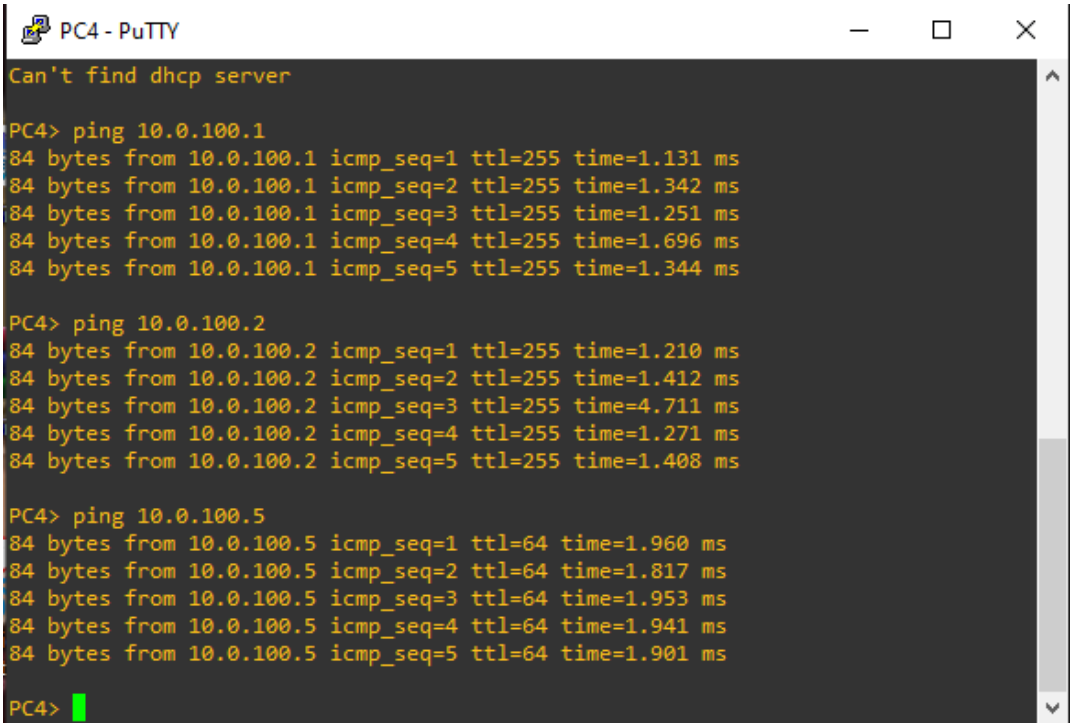
Imagen 9. Pruebas de ping del PC3



2.9.4 PC4 debería hacer ping con éxito a:

D1: 10.0.100.1
D2: 10.0.100.2
PC1: 10.0.100.5

Imagen 10. Pruebas de ping del PC4



3 TERCER PASO DE LA GUÍA

3.1 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:

3.2 EN LA "RED DE LA COMPAÑIA" (ES DECIR, R1, R3, D1, Y D2), CONFIGURE SINGLE-AREA OSPFV2 EN AREA 0

Use OSPF Process ID 4 y asigne los siguientes router-IDs:

R1: 0.0.4.1
R3: 0.0.4.3
D1: 0.0.4.131
D2: 0.0.4.132

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.
En R1, no publique la red R1 – R2.
En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Deshabilite las publicaciones OSPFv2 en:

D1: todas las interfaces excepto G1/0/11
D2: todas las interfaces excepto G1/0/11

3.2.1 Asignación de IDs y OSPFv2 en R1

```
R1(config)#router osp
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#
```

3.2.2 Asignación de IDs y OSPFv2 en R3

```
R3(config)#router osp
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)#
```

3.2.3 Asignación de IDs y OSPFv2 en D1

```
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
D1(config-router)# passive-interface default
D1(config-router)#no passive-interface ethernet 1/1
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)# network 10.0.100.0 0.0.0.255 area 0
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0
D1(config-router)# network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#exit
```

3.2.4 Asignación de IDs y OSPFv2 en D2

```
D2(config)#router ospf 4
D2(config-router)# router-id 0.0.4.132
D2(config-router)# passive-interface default
D2(config-router)#no passive-interface ethernet 1/1
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)# network 10.0.100.0 0.0.0.255 area 0
D2(config-router)# network 10.0.101.0 0.0.0.255 area 0
D2(config-router)# network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#
```

3.3 EN LA “RED DE LA COMPAÑÍA” (ES DECIR, R1, R3, D1, Y D2), CONFIGURE CLASSIC SINGLE-AREA OSPFV3 EN AREA 0

Use OSPF Process ID 6 y asigne los siguientes router-IDs:

R1: 0.0.6.1
R3: 0.0.6.3
D1: 0.0.6.131
D2: 0.0.6.132

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

En R1, no publique la red R1 – R2.
On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Deshabilite las publicaciones OSPFv3 en:

D1: todas las interfaces excepto G1/0/11
D2: todas las interfaces excepto G1/0/11

3.3.1 Asignación de IDs 6 y OSPFv2 en R1

```
R1(config)#ipv6 router osp
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#default-information originate
R1(config-rtr)#
```

3.3.2 Asignación de IDs 6 y OSPFv2 en R3

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

3.3.3 Asignación de IDs 6 y OSPFv2 en D1

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface ethernet 1/1
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#
```

Asignación de IDs 6 y OSPFv2 en D2

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#passive-interface default
D2(config-rtr)#no passive-interface et
D2(config-rtr)#no passive-interface ethernet 1/1
D2(config-rtr)#
```

3.4 EN R2 EN LA “RED ISP”, CONFIGURE MP-BGP. CONFIGURE DOS RUTAS ESTÁTICAS PREDETERMINADAS

A través de la interfaz Loopback 0:

Una ruta estática predeterminada IPv4.
Una ruta estática predeterminada IPv6.

Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.
Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

En IPv4 address family, anuncie:

La red Loopback 0 IPv4 (/32).
La ruta por defecto (0.0.0.0/0).

En IPv6 address family, anuncie:

La red Loopback 0 IPv4 (/128).
La ruta por defecto (::/0).

3.4.1 Configuración de bgp, router id, loopback en R2

```
R2(config)#router bgp 500
R2(config-router)# bgp router-id 2.2.2.2
R2(config-router)# bgp log-neighbor-changes
R2(config-router)# neighbor 2001:DB8:200::1 remote-as 300
R2(config-router)# neighbor 209.165.200.225 remote-as 300

R2(config-router)#
R2(config)#router bgp 500
R2(config-router)#address-family ipv4
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#  network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#  no neighbor 2001:DB8:200::1 activate
R2(config-router-af)#  neighbor 209.165.200.225 activate
R2(config-router-af)# exit-address-family
R2(config-router)#address-family ipv6
R2(config-router-af)#  network ::/0
R2(config-router-af)#  network 2001:DB8:2222::/128
R2(config-router-af)#  neighbor 2001:DB8:200::1 activate
R2(config-router-af)# exit-address-family
R2(config-router)#
R2(config)#router bgp 500
R2(config-router)#bg
```

```
R2(config-router)#bgp ro
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#ip ro
R2(config-router)#ip rou
R2(config-router)#ip route 0.0.0.0 0.0.0.0 loopback0
R2(config)#ipv6 route ::/0 Loopback0
R2(config)#
```

3.5 EN R1 EN LA “RED ISP”, CONFIGURE MP-BGP

Configure dos rutas resumen estáticas a la interfaz Null 0:

Una ruta resumen IPv4 para 10.0.0.0/8.
Una ruta resumen IPv6 para 2001:db8:100::/48.
Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.
Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

Deshabilite la relación de vecino IPv6.
Habilite la relación de vecino IPv4.
Anuncie la red 10.0.0.0/8.

En IPv6 address family:

Deshabilite la relación de vecino IPv4.
Habilite la relación de vecino IPv6.
Anuncie la red 2001:db8:100::/48.
Configuración de bgp, router id en

3.5.1 Configuración de bgp, router id en R1

```
R1(config)#router bgp 300
R1(config-router)# bgp router-id 1.1.1.1
R1(config-router)# bgp log-neighbor-changes
R1(config-router)# neighbor 2001:DB8:200::2 remote-as 500
R1(config-router)# neighbor 209.165.200.226 remote-as 500
R1(config-router)#
```

```
R1(config-router)#address-family ipv4
R1(config-router-af)#  network 10.0.0.0
R1(config-router-af)#  no neighbor 2001:DB8:200::2 activate
R1(config-router-af)#  neighbor 209.165.200.226 activate
R1(config-router-af)# exit-address-family
R1(config-router)#
```

```
R1(config-router)#address-family ipv6
R1(config-router-af)#  network 2001:DB8:100::/48
R1(config-router-af)#  neighbor 2001:DB8:200::2 activate
R1(config-router-af)# exit-address-family
R1(config-router)#
```

4 CUARTO PASO DE LA GUÍA

4.1 PARTE 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO (FIRST HOP REDUNDANCY)

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

Las tareas de configuración son las siguientes:

4.2 4.1 EN D1, CREE IP SLAS QUE PRUEBEN LA ACCESIBILIDAD DE LA INTERFAZ R1 G0/0/1

Cree dos IP SLAs.

• Use la SLA número 4 para IPv4.

• Use la SLA número 6 para IPv6.

Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

Programe la SLA para una implementación inmediata sin tiempo de finalización.

Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.

• Use el número de rastreo 4 para la IP SLA 4.

• Use el número de rastreo 6 para la IP SLA 6.

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

4.2.1 Configuración pasos 4.2 en D1

```
D1(config)#track 4 ip sla 4
D1(config-track)#delay down 10 up 15
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config)#ip sla 4
D1(config-ip-sla)#icmp-echo 10.0.10.1
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:DB8:100:1010::1
D1(config-ip-sla-echo)#frequency 5
```

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

4.2.2 4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

Cree IP SLAs.

• Use la SLA número 4 para IPv4.

• Use la SLA número 6 para IPv6.

Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.

Programe la SLA para una implementación inmediata sin tiempo de finalización.

Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.

• Use el número de rastreo 4 para la IP SLA 4.

• Use el número de rastreo 6 para la SLA 6.

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

4.2.3 Configuración pasos 4.2 en D2

Configuración y pruebas con SLA en IPV4 e IPV6 en D2.

```
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)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:DB8:100:1011::1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
```

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

4.3 EN D1 4.3 CONFIGURE HSRPV2

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

Configure HSRP version 2.

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

4.3.1 Configuración pasos 4.3 en D1

```
D1(config)#interface vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#
*Nov  8 15:02:16.913: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby
-> Active
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#
*Nov  8 15:02:33.665: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby
-> Active
D1(config-if)#

D1(config)#interD1(config)#interface vlan 101
D1(config-if)#standby ver
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)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60

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)#
*Nov  8 15:17:12.605: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Standby
-> Active
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 priority 150
```

```
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 6 decrement 60
D1(config-if)#
*Nov  8 15:17:44.672: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Standby
-> Active
D1(config-if)#
```

4.3.2 Configuración pasos 4.3 en D1. En D2, configure HSRPv2

```
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)#standby 104 track 4 decrement 60
D2(config-if)#standby 106 ipv6 autoconfig
*Nov  8 15:23:47.983: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Speak -
> Standby
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 track 6 decrement 60
D2(config-if)#exit
D2(config)#
*Nov  8 15:24:04.872: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered
on Ethernet1/1 (not full duplex), with R3 GigabitEthernet1/0 (full duplex).
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)#
*Nov  8 15:27:58.154: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -
> Active
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)#
*Nov  8 15:28:24.729: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -
> Active
D2(config-if)#standby 116 track 6 decrement 60
```

```
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)#standby 124 track 4 decrement 60
D2(config-if)#standby 126 ipv6 autoconfig
*Nov  8 15:30:26.642: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Speak -
> Standby
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 6 decrement 60
D2(config-if)#exit
D2(config)#
```

5 QUINTO PASO DE LA GUÍA

5.1 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:

5.2 5.1 EN TODOS LOS DISPOSITIVOS, PROTEJA EL EXEC PRIVILEGIADO USANDO EL ALGORITMO DE ENCRIPCIÓN SCRYPT

5.2.1 Configuración de seguridad en R1

```
R1(config)#ena
R1(config)#enable se
R1(config)#enable secret cisco12345cisco
```

5.2.2 Configuración de seguridad en R2

```
R2(config)#ena secr
R2(config)#ena secret cisco12345cisco
R2(config)#
```

5.2.3 Configuración de seguridad en R3

```
R3(config)#enable se
R3(config)#enable secret cisco12345cisco
R3(config)#
```

Nota: El comando debería ser enable algorithm-type SCRYPT secret cisco12345cisco; pero para la versión que se tiene de ios no se aplica, se deja el que se pudo aplicar.

5.2.4 Configuración de seguridad en D1

```
D1(config)#enable algorithm-type scrypt se
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D1(config)#
```

5.2.5 Configuración de seguridad en D2

```
D2(config)#enable algorithm-type SCRYPT secr
```

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

5.2.6 Configuración de seguridad en A1

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

5.3 EN TODOS LOS DISPOSITIVOS, CREE UN USUARIO LOCAL Y PROTÉJALO USANDO EL ALGORITMO DE ENCRIPCIÓN SCRYPT

Detalles de la cuenta encriptada SCRYPT:

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

5.3.1 Configuración de privilegios de seguridad en R1

R1(config)#username sadmin privilege 15 secret cisco12345cisco
R1(config)#

5.3.2 Configuración de privilegios de seguridad en R2

R2(config)#username sadmin privilege 15 se
R2(config)#username sadmin privilege 15 secret cisco12345cisco
R2(config)#

5.3.3 Configuración de privilegios de seguridad en R3

R3(config)#username sadmin privilege 15 se
R3(config)#username sadmin privilege 15 secret cisco12345cisco
R3(config)#

Nota: El comando debería ser username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco; pero para la versión que se tiene de ios no se aplica, se deja el que se pudo aplicar.

5.3.4 Configuración de privilegios de seguridad en D1

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

D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco1234$
D1(config)#

5.3.5 Configuración de privilegios de seguridad en D2

D2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco1234$
D2(config)#

5.3.6 Configuración de privilegios de seguridad en A1

A1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco1234$

5.4 EN TODOS LOS DISPOSITIVOS (EXCEPTO R2), HABILITE AAA. HABILITE AAA

5.5 EN TODOS LOS DISPOSITIVOS (EXCEPTO R2), CONFIGURE LAS ESPECIFICACIONES DEL SERVIDOR RADIUS

Especificaciones del servidor RADIUS:

• Dirección IP del servidor RADIUS es 10.0.100.6.
• Puertos UDP del servidor RADIUS son 1812 y 1813.
• Contraseña: $trongPass

5.6 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.

5.6.1 Configuración AAA, RADIUS en R1

R1(config)#aaa new-model
R1(config)#aaa authentication login default group radius local
R1(config)#aaa session-id common

```
R1(config)#radius server RADIUS
R1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)#key $trongPass
R1(config-radius-server)#
```

5.6.2 Configuración AAA, RADIUS en R3

```
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#aaa session-id common
R3(config)#aaa session-id common
R3(config)#radius server RADIUS
R3(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)#key $trongPass
R3(config-radius-server)#
```

5.6.3 Configuración AAA, RADIUS en D1

```
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#
D1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)#key $trongPass
D1(config-radius-server)#EXIT
D1(config)#aaa authentication login default group radius local
D1(config)#
```

5.6.4 Configuración AAA, RADIUS en D2

```
D2(config)#aaa new-model
D2(config)#aaa authentication login default group radius local
D2(config)#aaa session-id common
D2(config)#radius server RADIUS
D2(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)#key $trongPass
D2(config-radius-server)#
```

5.6.5 Configuración AAA, RADIUS en A1

```
A1(config)#aaa new-model
A1(config)#aaa authentication login default group radius local
A1(config)#aaa session-id common
```

A1(config)#radius server RADIUS
A1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)#key $trongPass
A1(config-radius-server)#

5.7 VERIFIQUE EL SERVICIO AAA EN TODOS LOS DISPOSITIVOS (EXCEPT R2)

Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: sadmin y la contraseña: cisco12345cisco.

Imagen 11. Prueba de configuración de seguridad en R1

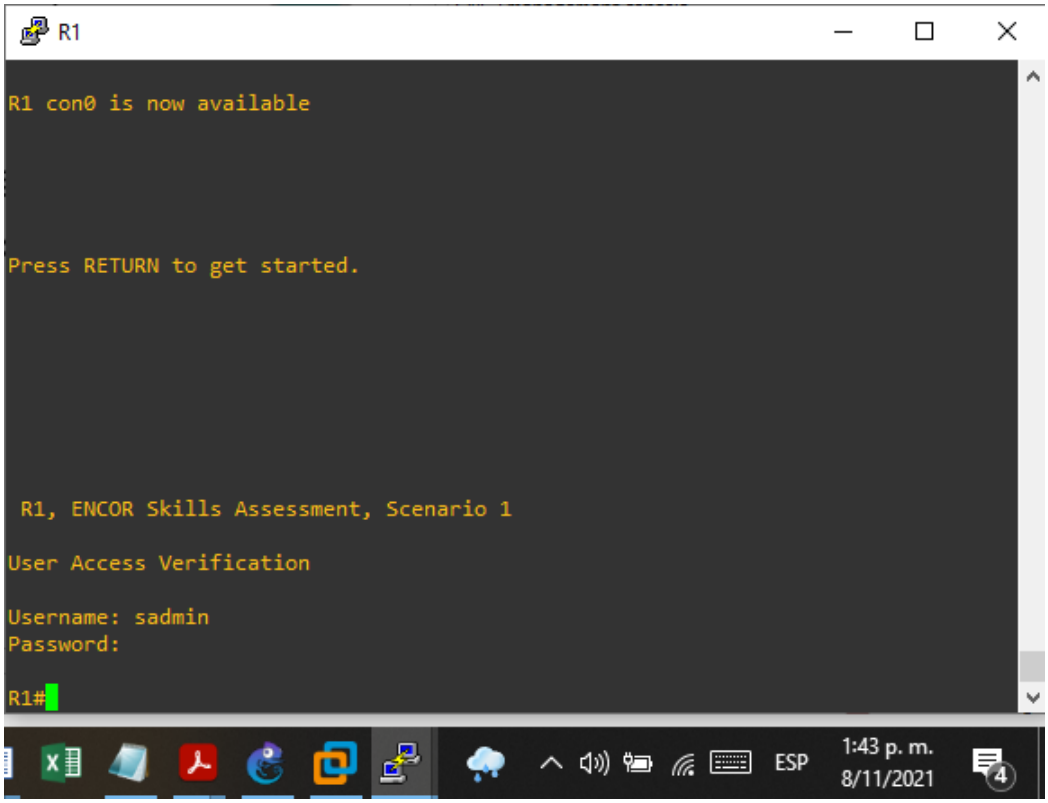


Imagen 12. Prueba de configuración de seguridad en R3

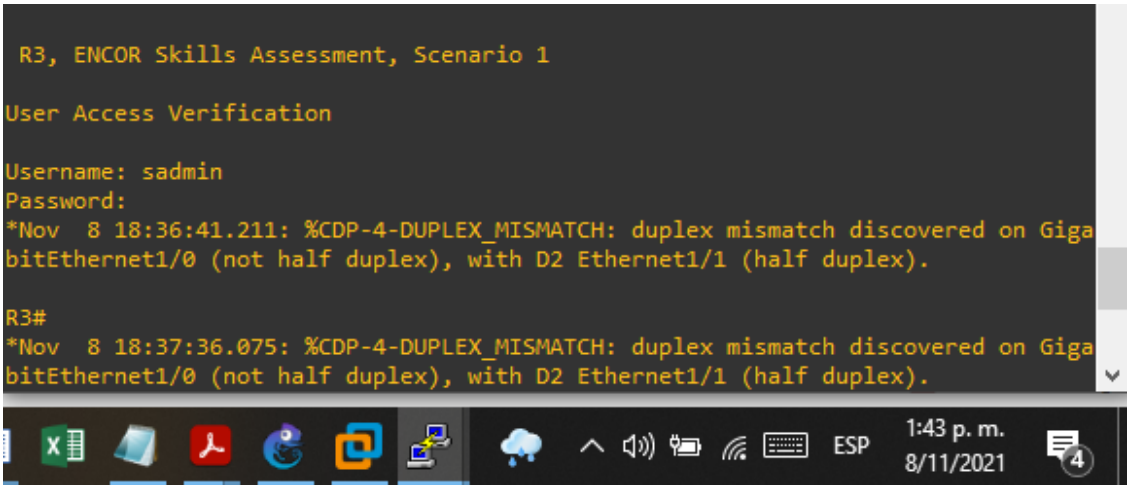


Imagen 13. Prueba de configuración de seguridad en D1

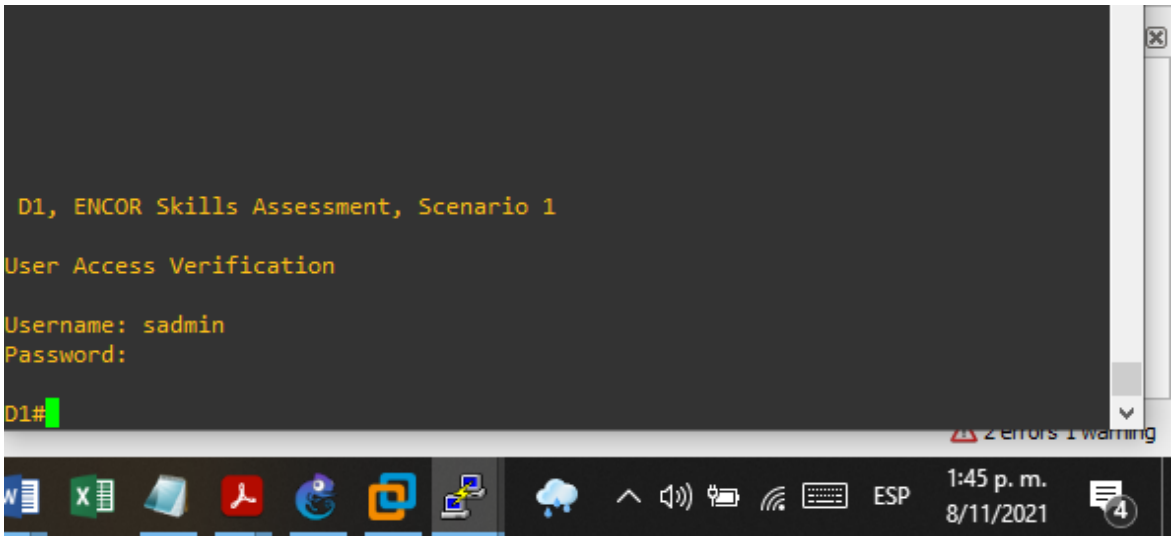


Imagen 14. Prueba de configuración de seguridad en D2

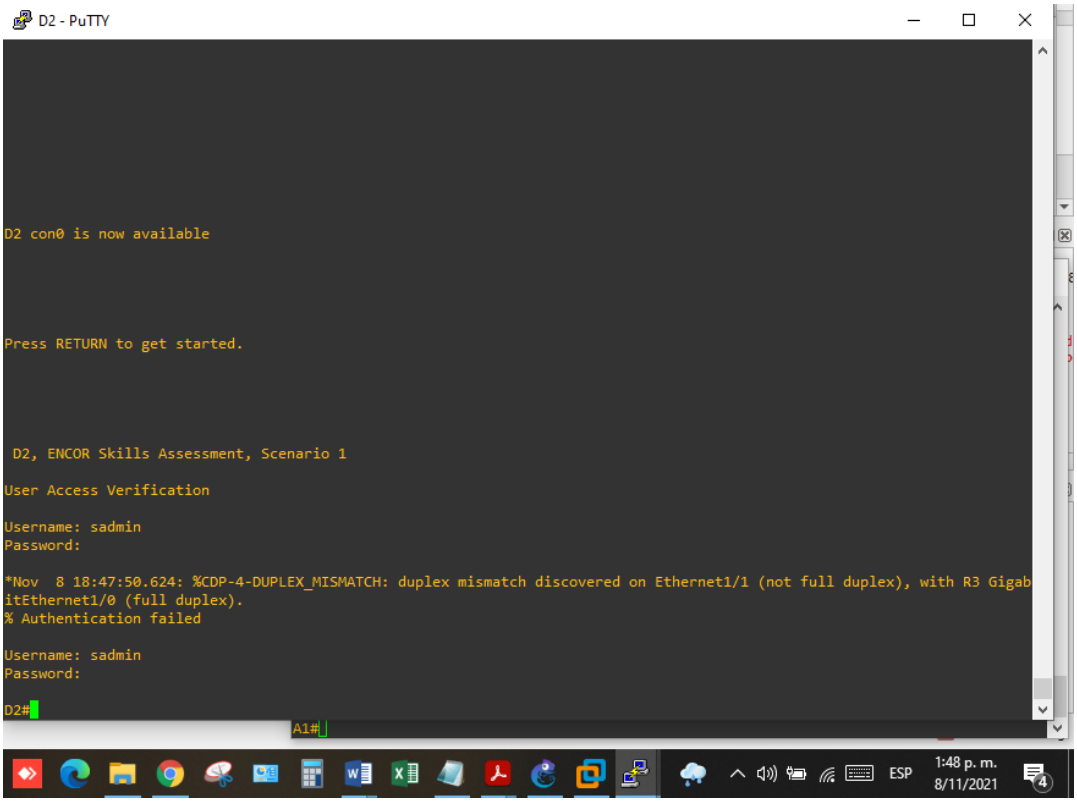
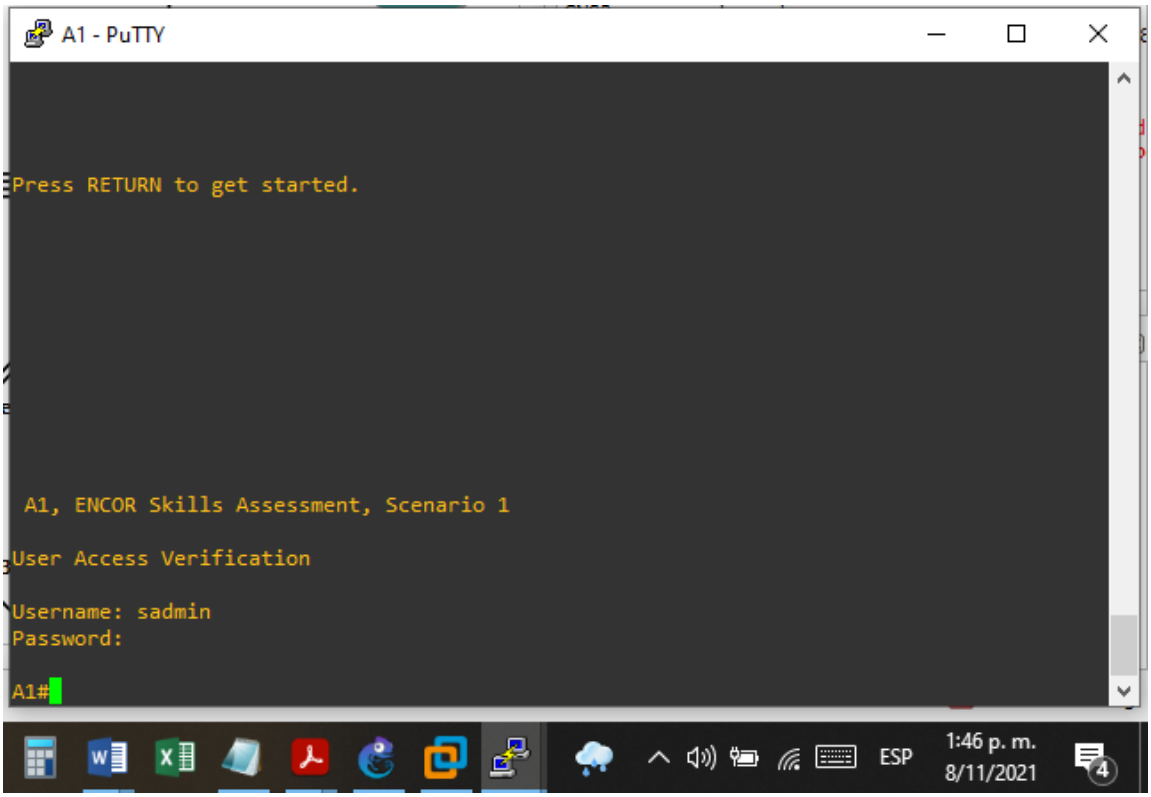


Imagen 15. Prueba de configuración de seguridad en A1



6 SEXTO PASO DE LA GUÍA

6.1 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:

6.2 EN TODOS LOS DISPOSITIVOS, CONFIGURE EL RELOJ LOCAL A LA HORA UTC ACTUAL

Configure el reloj local a la hora UTC actual.

Nota: Para este caso se configuro la hora de Colombia CTS 5.

6.2.1 Configuración de la Hora en R1

```
R1(config)#clock timezone CTS -5
R1(config)#
*Nov  8 18:58:04.331: %SYS-6-CLOCKUPDATE: System clock has been updated
from 18:    58:04 UTC Mon Nov 8 2021 to 13:58:04 CTS Mon Nov 8 2021, configured
from console      by sadmin on console.
R1(config)#
```

6.2.2 Configuración de la Hora en R2

```
R2(config)#CLOck timezone CTS -5
R2(config)#
*Nov  8 19:00:13.811: %SYS-6-CLOCKUPDATE: System clock has been updated
from 19:00:13 UTC Mon Nov 8 2021 to 14:00:13 CTS Mon Nov 8 2021, configured
from console by console.
R2(config)#
```

6.2.3 Configuración de la Hora en R3

```
R3(config)#clock timezone CTS -5
R3(config)#
*Nov  8 19:01:01.567: %SYS-6-CLOCKUPDATE: System clock has been updated
from 19:01:01 UTC Mon Nov 8 2021 to 14:01:01 CTS Mon Nov 8 2021, configured
from console by sadmin on console.
R3(config)#
```

6.2.4 Configuración de la Hora en D1

```
D1(config)#clock ti
D1(config)#clock timezone CTS -5
D1(config)#
```

6.2.5 Configuración de la Hora en D2

```
D2(config)#clo
D2(config)#clock ti
D2(config)#clock timezone CTS -5
D2(config)#
```

6.2.6 Configuración de la Hora en A1

```
A1(config)#clock ti
A1(config)#clock timezone CTS -5
A1(config)#
```

6.3 CONFIGURE R2 COMO UN NTP MAESTRO

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

6.3.1 Configuración de R2 como maestro

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

6.3.2 Configure NTP en R1, R3, D1, D2, y A1

Configure NTP de la siguiente manera:

- R1 debe sincronizar con R2.
- R3, D1 y A1 para sincronizar la hora con R1.
- D2 para sincronizar la hora con R3.

6.4 CONFIGURE SYSLOG EN TODOS LOS DISPOSITIVOS EXCEPTO R2

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

6.4.1 Configuracion Syslogs de R1

```
R1(config)#ntp server 2.2.2.2
R1(config)#logging trap warning
R1(config)#logging host 10.0.100.5    Este es el host donde debe apuntar el servicio
R1(config)#logging on
R1(config)#
```

6.4.2 Configuración Syslogs en R3

```
R3(config)#ntp server 10.0.10.1          Servidor NTP
R3(config)#logging trap warning
R3(config)#logging host 10.0.100.5       Syslogs
R3(config)#logging on
```

6.4.3 Configuración Syslogs en D1

```
D1(config)#ntp server 10.0.10.1          Servidor NTP
D1(config)#logging trap warning
D1(config)#logging host 10.0.100.5       Syslogs
D1(config)#logging on
D1(config)#
```

6.4.4 Configuración Syslogs en D2

```
D2(config)#ntp server 10.0.10.1          Servidor NTP
D2(config)# logging trap warning
D2(config)# logging host 10.0.100.5      Syslogs
D2(config)# logging on
D2(config)#
```

6.4.5 Configuración Syslogs en A1

```
A1(config)#ntp server 10.0.10.1          Servidor NTP
A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5      Syslogs
A1(config)# logging on
A1(config)#
```

6.5 CONFIGURE SNMPV2C EN TODOS LOS DISPOSITIVOS EXCEPTO R2

Especificaciones de SNMPv2:

• Unicamente se usará SNMP en modo lectura (Read-Only).
• Limite el acceso SNMP a la dirección IP de la PC1.
• Configure el valor de contacto SNMP con su nombre.
• Establezca el community string en ENCORSA.
• En R3, D1, y D2, habilite el envío de traps config y ospf.
• En R1, habilite el envío de traps bgp, config, y ospf.
• En A1, habilite el envío de traps config.

6.5.1 Configuración de SNMPv2c en R1

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

6.5.2 Configuración de SNMPv2c en R3

```
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 Nelson-Farfan
R3(config)#snmp-server community ENCORSA ro SNMP-NMS
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server ifindex persist
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#
```

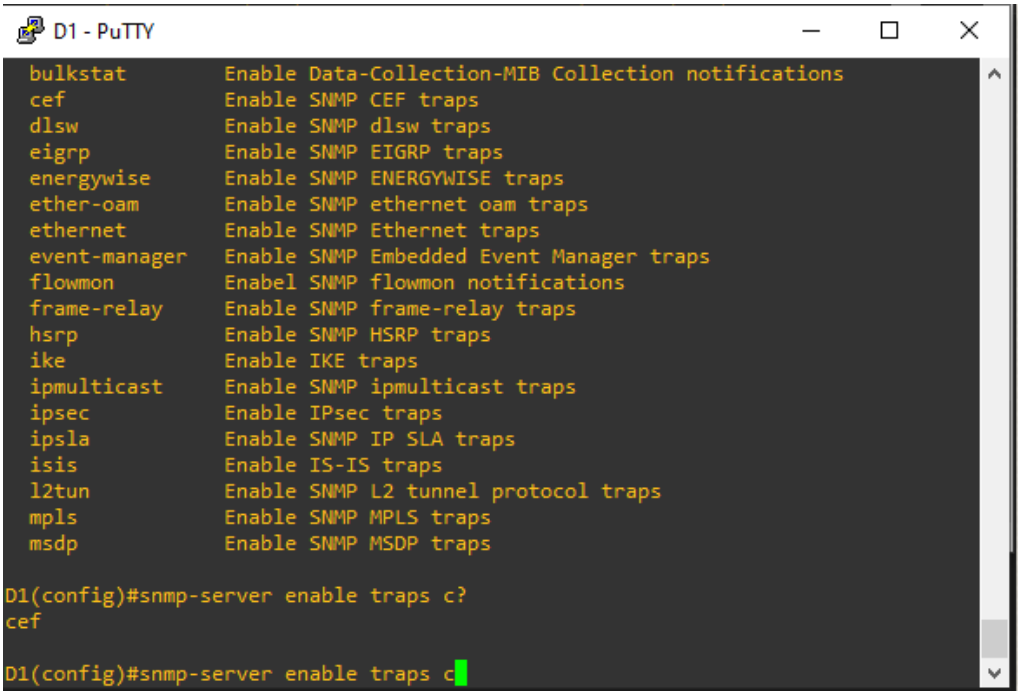
6.5.3 Configuración de SNMPv2c en D1

```
D1(config)#ip access-list standard SNMP-NMS
```

D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Cisco Nelson-Farfan
D1(config)#snmp-server community ENCORSA ro SNMP-NMS
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server ifindex persist
D1(config)#snmp-server enable traps ospf

Nota: No se pudo configurar snmp-server enable traps config por que el Sw D1 no cuenta con la opción se adjunta las pruebas, se pregunta los comandos por C.

Imagen 16. Prueba de que el equipo implementado no tenía la opción para poder configurar en SW D1

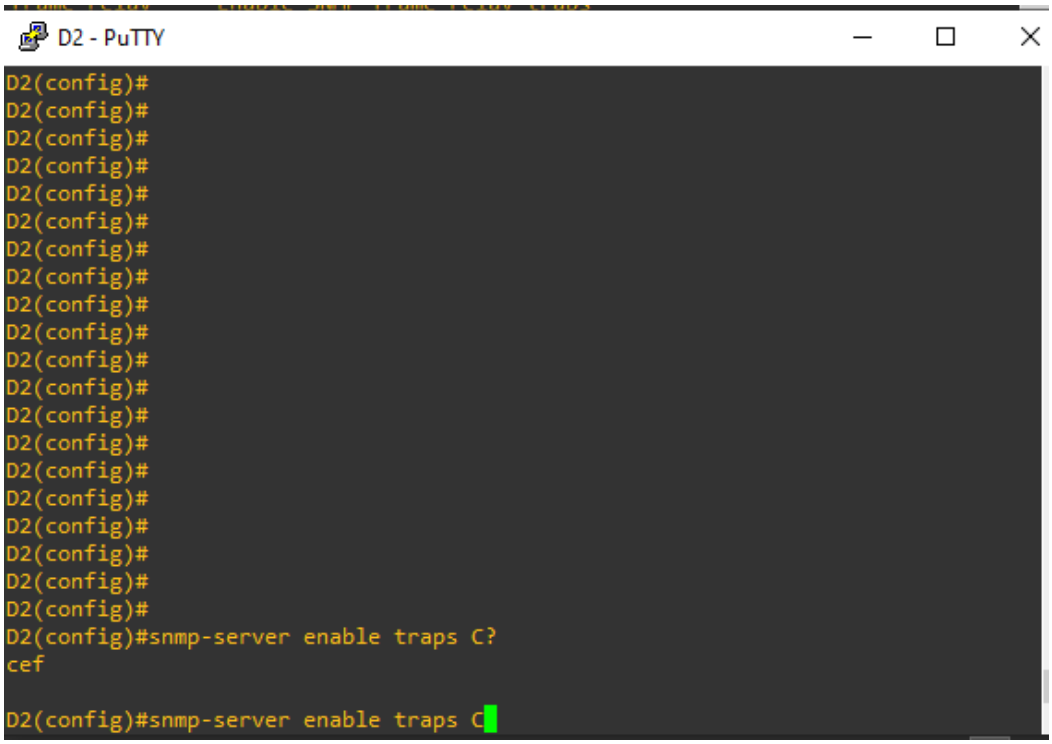


6.5.4 Configuración de SNMPv2c en D2

D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config)#snmp-server contact Cisco Nelson-Farfan
D2(config)#snmp-server community ENCORSA ro SNMP-NMS
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server enable traps ospf

Nota: No se pudo configurar snmp-server enable traps config por que el Sw D2 no cuenta con la opción se adjunta las pruebas, se pregunta los comandos por C.

Imagen 17. Prueba de que el equipo implementado no tenía la opción para poder configurar en SW D2

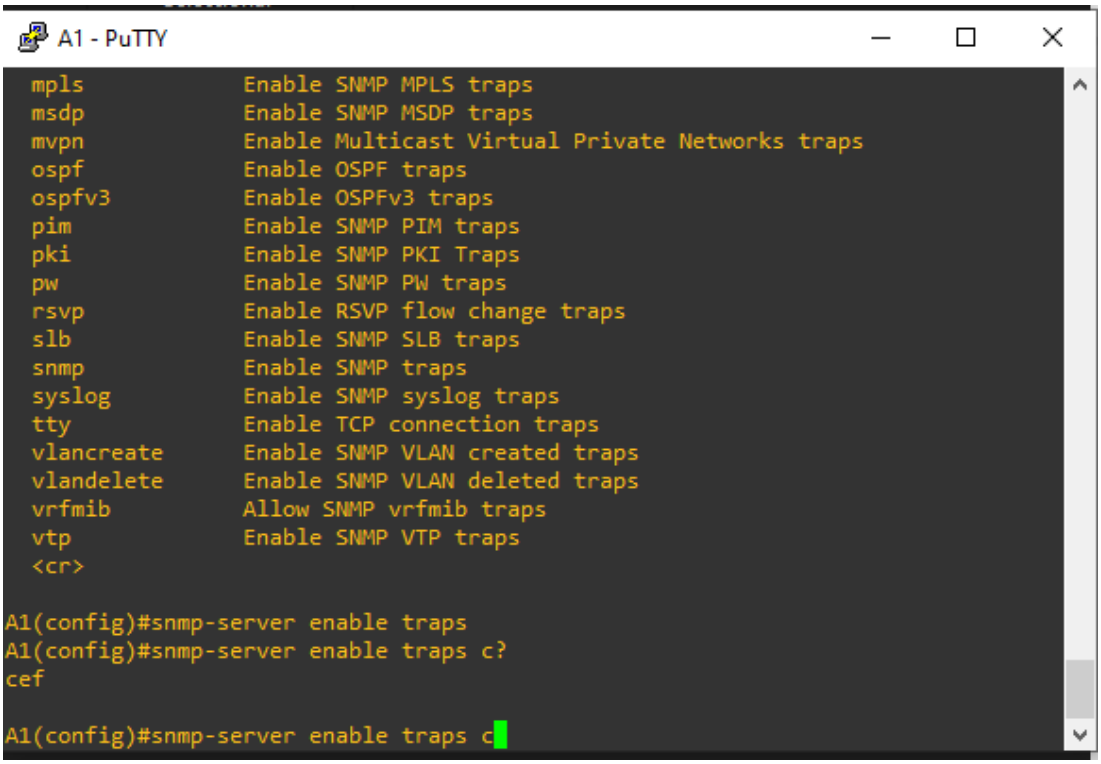


6.5.5 Configuración de SNMPv2c en A1

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 Nelson-Farfan
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

Nota: No se pudo configurar snmp-server enable traps config por que el Sw A1 no cuenta con la opción se adjunta las pruebas, se pregunta los comandos por C.

Imagen 18. Prueba de que el equipo implementado no tenía la opción para poder configurar en SW A1



7 CONCLUSIONES

Al momento de implementar el escenario en packet tracer se identificó que varios de los comandos no estaban habilitados; se consultó con el tutor quien indico que lo mejor era implementar en GNS3, se tomó esta opción.

Cuando se implementó la solución en gns3 se presentó un inconveniente con las imágenes de los SW que se tenían, estas no servían; se consultó y se obtuvieron unas imágenes que soportaran todos los comandos, pero al final de la configuración fue necesario ampliar la memoria para seguir trabajando sobre el escenario.

Con los enlaces troncal se garantizan enlaces redundantes para evitar perdida de comunicaciones, también se optimizan los recursos porque solo se utilizan puertos en los mismos equipos, se debe aclarar que los enlaces en modo troncal se configuran en pares.

Con OSPF se garantiza la mejora en los tiempos de conexión se eligen las rutas con la menor cantidad de saltos, este protocolo garantiza que se tenga alta escalabilidad, no se tiene problemas con el crecimiento de la red, el ospf recalcula la rutas y adyacencias para garantizar la menor cantidad de saltos.

Los enlaces troncales se pueden configurar localmente en data center y cuartos de cableado, con la instalación de fibra óptica estos enlaces ahora no necesariamente tienen que estar en el mismo lugar físico, hoy en día los clientes pueden tener más de un centro de cableado.

BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Packet Forwarding. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Fabric Technologies. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Network Assurance. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Enterprise Network Architecture. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Network Device Access Control and Infrastructure Security. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. CISCO Press (Ed). Virtualization. CCNP and CCIE Enterprise Core ENCOR 350-401p. {2020}. {En línea}. {15 de septiembre 2021} Disponible en : (https://1drv.ms/b/s!AAIGg5JUgUBthk8)