

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JESUS EDWIN ROJAS FIERRO

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JESUS EDWIN ROJAS FIERRO

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Pitalito Huila 29 de noviembre 2021

## **AGRADECIMIENTOS**

El presente trabajo va dedicado a Dios, quien como guía ha estado presente en cada una de las decisiones tomadas en mi vida, bendiciéndome y dándome fuerzas para continuar con mis metas trazadas sin desfallecer. A mis padres, hermanas y familiares que con apoyo incondicional, amor y confianza permitieron que logre culminar mi carrera profesional.

A mis tutores que con su gran conocimiento y compromiso fueron una guía y pieza clave para el desarrollo de cada una de las estancias del proyecto

A la universidad Nacional Abierta y a Distancia UNAD que gracias a la metodología y mediaciones tecnológicas me permitieron avanzar en mi proceso educativo y al mismo tiempo poder desempeñar mi actividad laboral.

## CONTENIDO

LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	9
RESUMEN.....	10
ABSTRACT.....	10
INTRODUCCION .....	11
DESARROLLO .....	12
Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	25
Parte 3: Configurar los protocolos de enrutamiento.....	33
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy) .....	42
Parte 5: Seguridad .....	49
Parte 6: Configure las funciones de Administración de Red .....	54
CONCLUSIONES .....	61
BIBLIOGRAFÍA .....	62

## LISTA DE TABLAS

Tabla 1. Direccionamiento topologia.....	13
Tabla 2. Tareas Parte 2.....	25
Tabla 3. Tareas Parte 3.....	33
Tabla 4. Tareas Parte 4.....	42
Table 5. Tareas Parte 5.....	49
Table 6. Tareas Parte 6.....	55

## LISTA DE FIGURAS

Figura 1 Escenario 1 .....	12
Figura 2 Simulación de escenario 1 .....	15
Figura 3 Verificación configuración R1 .....	16
Figura 4 Verificación configuración R2 .....	17
Figura 5 Verificación configuración R3 .....	18
Figura 6 Verificación configuración D1 .....	20
Figura 7 Verificación configuración D2 .....	21
Figura 8 Verificación Vlan A1 .....	22
Figura 9 Copiado archivo running-config en R1 .....	23
Figura 10 Copiado archivo running-config en R2 .....	23
Figura 11 Copiado archivo running-config en R3 .....	23
Figura 12 Copiado archivo running-config en D1 .....	23
Figura 13 Copiado archivo running-config en D2 .....	24
Figura 14 Copiado archivo running-config en A1 .....	24
Figura 15 Verificación configuración PC1 .....	24
Figura 16 Verificación configuración PC4 .....	25
Figura 17 Verificación troncales, vlan nativa y etherchannels en D1 .....	28
Figura 18 Verificación troncales, vlan nativa y etherchannels en D2 .....	29
Figura 19 Verificación configuración puertos de acceso del host en D1 .....	29
Figura 20 Verificación configuración puertos de acceso del host en D2 .....	30
Figura 21 Verificación troncales, vlan nativa y etherchannels en A1 .....	30
Figura 22 Verificación configuración puertos de acceso del host en A1 .....	31
Figura 23 Verificación ping desde PC1 .....	31
Figura 24 Verificación ping desde PC2 .....	32
Figura 25 Verificación ping desde PC3 .....	32
Figura 26 Verificación ping desde PC4 .....	32
Figura 27 Verificación OSPFv2 en R1 .....	37
Figura 28 Verificación OSPFv2 en R3 .....	38
Figura 29 Verificación OSPFv2 en D1 .....	38
Figura 30 Verificación OSPFv2 en D2 .....	38
Figura 31 Verificación OSPFv3 en R1 .....	39
Figura 32 Verificación OSPFv3 en R3 .....	39

Figura 33 Verificación MP-BGP en R2 .....	39
Figura 34 Verificación MP-BGP en R1 .....	40
Figura 35 Verificación OSPF y BGP en R1 .....	40
Figura 36 Verificación OSPFv3 para IPv6 en R1 .....	41
Figura 37 Verificación OSPF y OSPFv3 en R3.....	41
Figura 38 configuración IP SLAs para D1 .....	47
Figura 39 configuración Vlans para D1 .....	48
Figura 40 configuración IP SLAs para D2 .....	48
Figura 41 configuración Vlans para D2 .....	49
Figura 42 validación de encriptación SCRYPT y usuario R1 .....	51
Figura 43 validación de encriptación SCRYPT y usuario R2 .....	51
Figura 44 validación de encriptación SCRYPT y usuario R3 .....	51
Figura 45 validación de encriptación SCRYPT y usuario D1 .....	52
Figura 46 validación de encriptación SCRYPT y usuario D2 .....	52
Figura 47 validación de encriptación SCRYPT y usuario A1 .....	52
Figura 48 validación de configuraciones puntos 5.3 al 5.5 R1 .....	53
Figura 49 validación de configuraciones puntos 5.3 al 5.5 R3 .....	53
Figura 50 validación de configuraciones puntos 5.3 al 5.5 D1 .....	53
Figura 51 validación de configuraciones puntos 5.3 al 5.5 D2 .....	54
Figura 52 validación de configuraciones puntos 5.3 al 5.5 A1 .....	54
Figura 53 validación de hora local R2 .....	58
Figura 54 validación de hora local R1 .....	58
Figura 55 validación master R2 .....	58
Figura 56 validación de Syslog R1 .....	59
Figura 57 validación de Syslog D1 .....	59
Figura 58 validación de SNMPv2c R1 .....	59
Figura 59 validación de SNMPv2c D1 .....	60
Figura 60 validación Limitación del acceso SNMP R1 .....	60
Figura 61 validación Limitación del acceso SNMP D1 .....	60



## GLOSARIO

**Topología de red:** La topología de red se define como un mapa físico o lógico de una red para intercambiar datos.

**Protocolo de red:** es el encargado de actuar en la llamada capa de mediación o de red, el nivel 3 en el modelo OSI y establecen una serie de acuerdos para el intercambio de datos, regulando, así, las condiciones para el transporte, el direccionamiento, el enrutamiento (camino del paquete) y el control de fallos

**Direccionamiento ip:** El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. El Protocolo de Internet versión 4 (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos

**Red de área local LAN:** es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio

**VPN:** Una VPN (Virtual Private Network) es una red privada que se extiende a través de una red pública, como Internet, permitiendo que los dispositivos conectados puedan enviar y recibir datos como si estuvieran conectados a una red local.

**OSPF (Open Shortest Path First):** es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP)

**Border Gateway Protocol (BGP):** es un protocolo escalable de dynamic routing usado en la Internet por grupos de enrutadores para compartir información de enrutamiento

## **RESUMEN**

El presente proyecto documenta la implementación y simulación de una red muy completa la cual puede ser aplicada a nivel profesional en el área de las telecomunicaciones y enfocada a empresas que requieran sistemas robustos tanto de enrutamiento como a nivel de seguridad, la cual cuenta con la aplicación de protocolos de tipo enlace- estado con lo es OSPF (Open Shortest Path First) y protocolos de puerta de enlace como lo es BGP (Border Gateway Protocol).

El diseño de la red está enfocado en lograr mediante cada uno de los pasos propuestos la correcta aplicación de los conocimientos adquiridos durante todo nuestro proceso formativo, mostrando las configuraciones realizadas y el posterior funcionamiento de cada uno de los direccionamientos y protocolos implementados, mediante la evidencia de imágenes y archivos de simulación.

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

## **ABSTRACT**

This project documents the implementation and simulation of a very complete network which can be applied at a professional level in the telecommunications area and focused on companies that require robust systems both routing and security level, which has the application of protocols such as link-state type OSPF (Open Shortest Path First) and gateway protocols such as BGP (Border Gateway Protocol).

The network design is focused on achieving through each of the proposed steps the correct application of the knowledge acquired throughout our training process, showing the configurations made and the subsequent operation of each of the implemented addressing and protocols, through the evidence of images and simulation files.

Keywords: CISCO, CCNP, commutation, routing, Networking, Electronics

## INTRODUCCION

El presente proyecto busca dar a conocer mediante la prueba de habilidades prácticas de CCNP la aplicación de los conocimientos adquiridos durante la experiencia académica, la implementación y simulación de un escenario de red en donde mediante la configuración de cada uno de los escenarios propuestos por la rúbrica y haciendo uso de software o plataformas especializadas en la virtualización de cada uno de los protocolos como lo es spanning-tree, OSPF, BGP entre otros.

En primera medida se muestra la configuración inicial de cada uno de los Routers y switch con el direccionamiento entregado, junto con la demostración mediante el uso de imágenes tomadas directamente de las consolas de los equipos de red evidenciando las configuraciones realizadas y el correcto funcionamiento de cada uno de los protocolos establecidos, dando como resultado una red que trabaja en armonía, brindando eficiencia en cada uno de los procesos que se ejecutan simultáneamente.

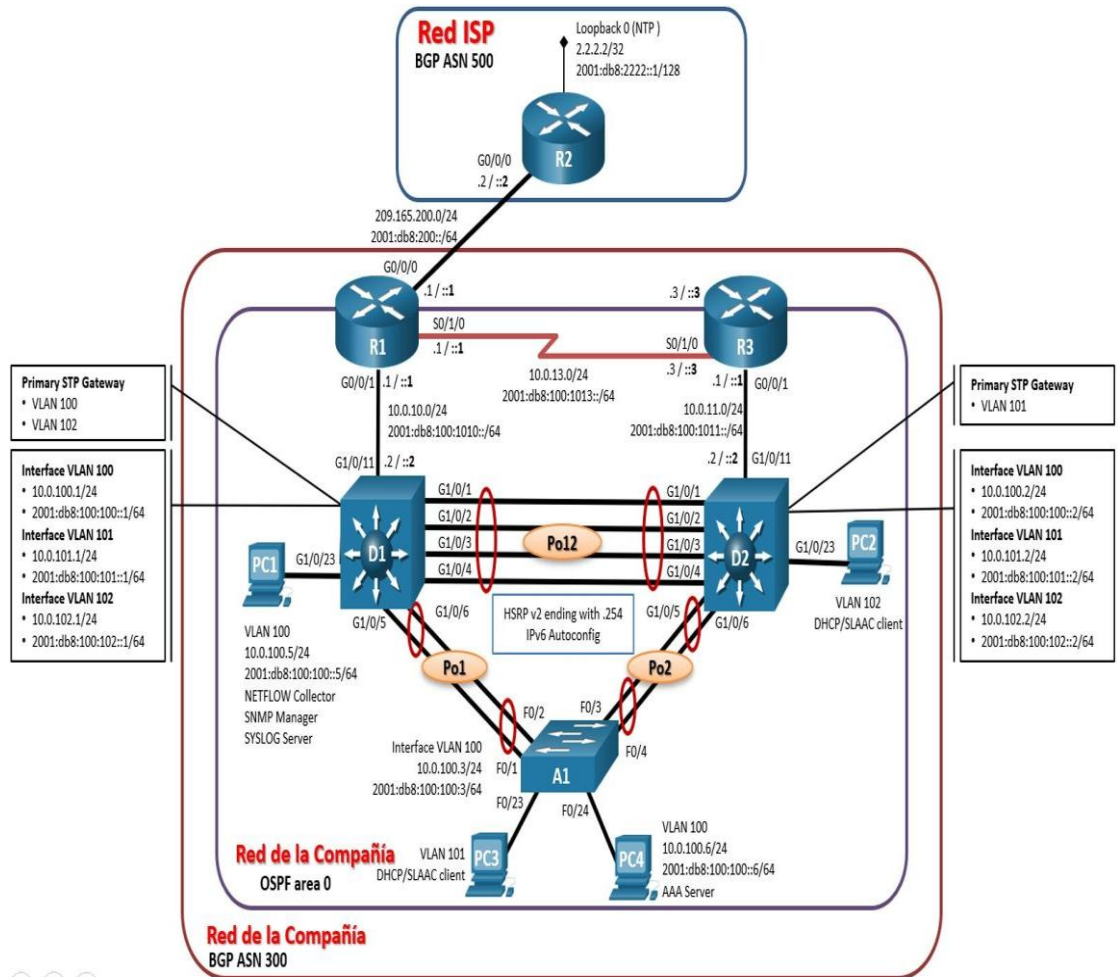
Es importante resaltar que cada una de las configuraciones y protocolos aplicados están estrechamente relacionadas y dependen directamente del anterior, es por esto la importancia de la buena planificación a la hora de realizar implementaciones de escenarios de este tipo

Para la simulación se utiliza el software GNS3 junto con VMware Workstation la cual cuenta con equipos cisco los cuales brindan una experiencia realista y características muy completas que otro software no ofrece.

## DESARROLLO

Topología de la Red:

Figura 1. Escenario 1



## Direccionamiento

Tabla 1. Direccionamiento topologia

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

## Objetivos

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

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

Part 3: Configurar los protocolos de enrutamiento

Part 4: Configurar la redundancia del primer salto

Part 5: Configurar la seguridad

Part 6: Configurar las características de administración de red

### Escenario

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

### Recursos necesarios

3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)

1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)

4 PCs (utilice el programa de emulación de terminal)

Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola

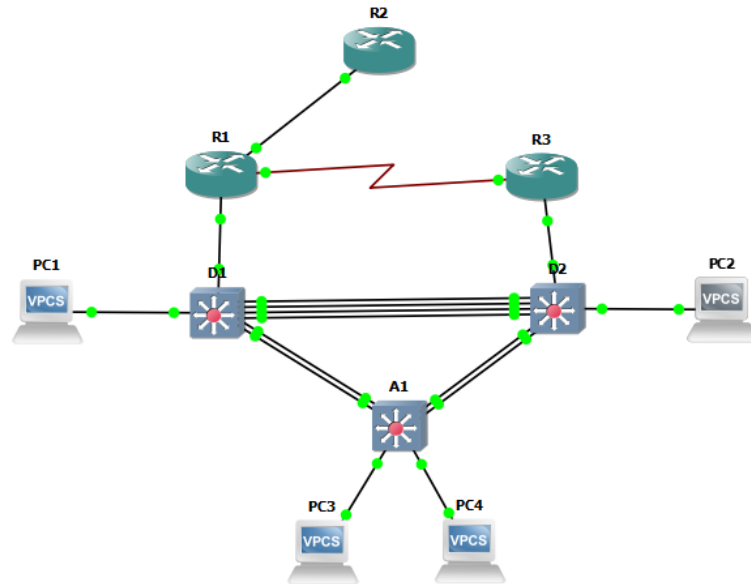
Los cables Ethernet y seriales van como se muestra en la topología

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

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

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

Figura 2. Simulación de escenario 1



Paso 2: Configurar los parámetros básicos para cada dispositivo.

Mediante una conexión de consola ingresamos en cada dispositivo, en el modo de configuración global y aplicamos los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

### R1

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0
ip address 209.165.200.225 255.255.255.224
```

```

ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown
exit
interface g1/0
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s3/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit

```

Verificamos la configuración

El siguiente comando nos brinda un resumen de la información de todas las interfaces de la red y las ip asignadas a cada una del dispositivo

Figura 3. Verificación configuración R1

```

R1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Proto
Ethernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	209.165.200.225	YES	manual	up	up
GigabitEthernet1/0	10.0.10.1	YES	manual	up	up
Serial3/0	10.0.13.1	YES	manual	up	down
Serial3/1	unassigned	YES	unset	administratively down	down
Serial3/2	unassigned	YES	unset	administratively down	down
Serial3/3	unassigned	YES	unset	administratively down	down

```

R1#

```

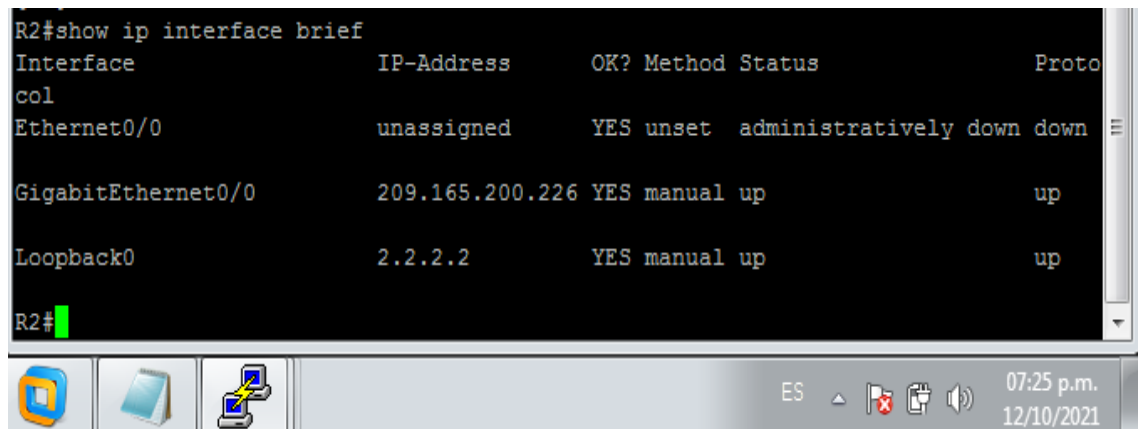


## R2

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

Verificamos la configuración

Figura 4. Verificación configuración R2



## R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

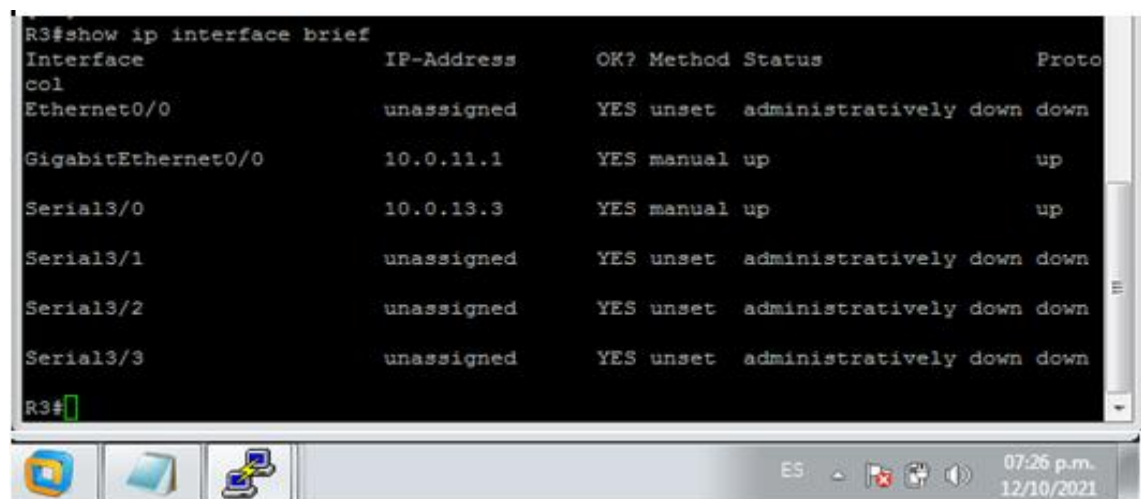
```

interface g0/0
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit
interface s3/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit

```

Verificamos configuración

Figura 5. Verificación configuración R3



## D1

```

hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit

```

```

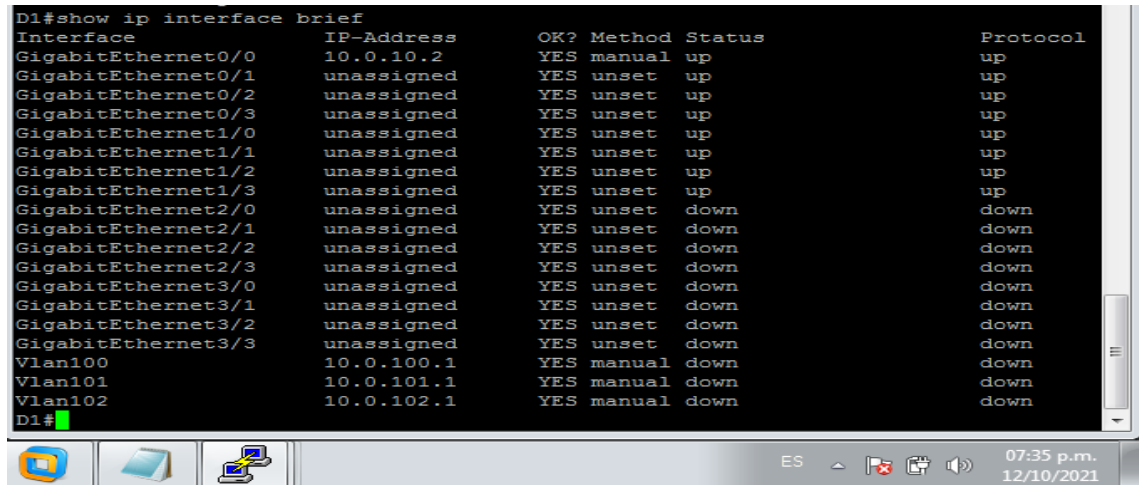
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g0/0
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit

```

Verificamos configuración

Figura 6. Verificación configuración D1

```
D1#show ip interface brief
Interface                IP-Address      OK? Method Status Protocol
GigabitEthernet0/0       10.0.10.2       YES manual up      up
GigabitEthernet0/1       unassigned      YES unset up      up
GigabitEthernet0/2       unassigned      YES unset up      up
GigabitEthernet0/3       unassigned      YES unset up      up
GigabitEthernet1/0       unassigned      YES unset up      up
GigabitEthernet1/1       unassigned      YES unset up      up
GigabitEthernet1/2       unassigned      YES unset up      up
GigabitEthernet1/3       unassigned      YES unset up      up
GigabitEthernet2/0       unassigned      YES unset down    down
GigabitEthernet2/1       unassigned      YES unset down    down
GigabitEthernet2/2       unassigned      YES unset down    down
GigabitEthernet2/3       unassigned      YES unset down    down
GigabitEthernet3/0       unassigned      YES unset down    down
GigabitEthernet3/1       unassigned      YES unset down    down
GigabitEthernet3/2       unassigned      YES unset down    down
GigabitEthernet3/3       unassigned      YES unset down    down
Vlan100                  10.0.100.1      YES manual down    down
Vlan101                  10.0.101.1      YES manual down    down
Vlan102                  10.0.102.1      YES manual down    down
D1#
```



## D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g0/0
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
```

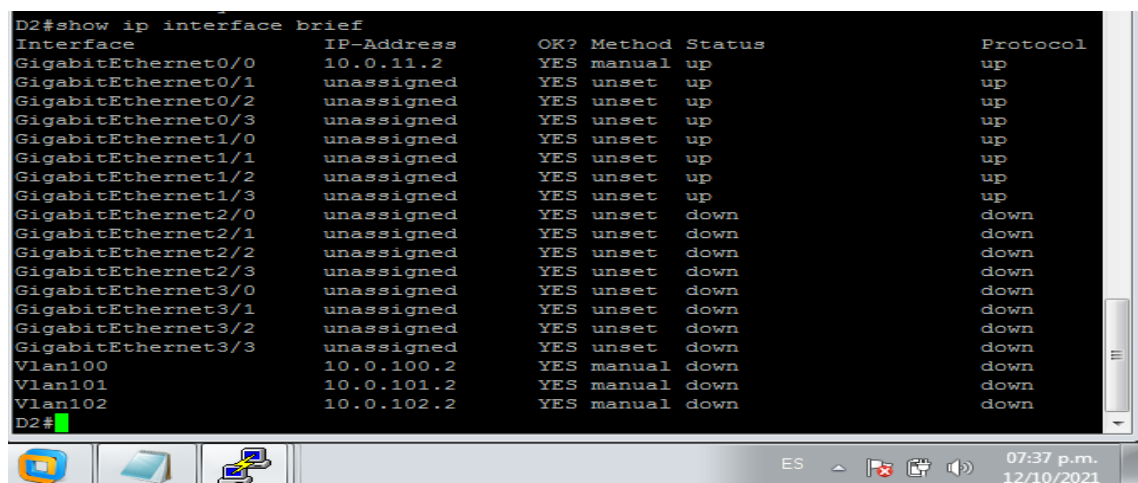
```

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

```

Verificamos configuración

Figura 7. Verificación configuración D2



```

D2#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.0.11.2	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	up	up
GigabitEthernet0/3	unassigned	YES	unset	up	up
GigabitEthernet1/0	unassigned	YES	unset	up	up
GigabitEthernet1/1	unassigned	YES	unset	up	up
GigabitEthernet1/2	unassigned	YES	unset	up	up
GigabitEthernet1/3	unassigned	YES	unset	up	up
GigabitEthernet2/0	unassigned	YES	unset	down	down
GigabitEthernet2/1	unassigned	YES	unset	down	down
GigabitEthernet2/2	unassigned	YES	unset	down	down
GigabitEthernet2/3	unassigned	YES	unset	down	down
GigabitEthernet3/0	unassigned	YES	unset	down	down
GigabitEthernet3/1	unassigned	YES	unset	down	down
GigabitEthernet3/2	unassigned	YES	unset	down	down
GigabitEthernet3/3	unassigned	YES	unset	down	down
Vlan100	10.0.100.2	YES	manual	down	down
Vlan101	10.0.101.2	YES	manual	down	down
Vlan102	10.0.102.2	YES	manual	down	down

```

D2#

```

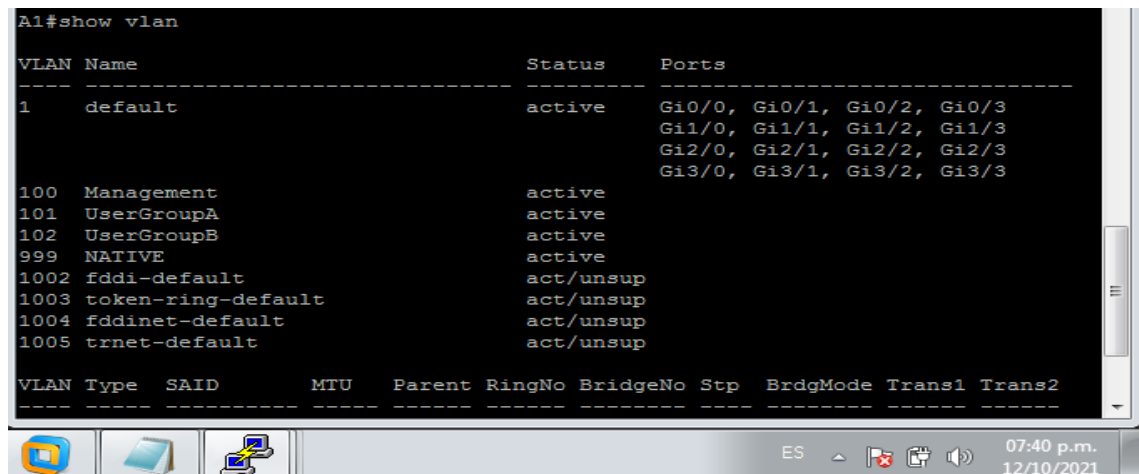
## A1

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

Validamos las vlan

El siguiente comando nos muestra las vlan configuradas y los puertos que pertenecen a cada una de estas

Figura 8. Verificación Vlan A1



```
A1#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                           Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                           Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                           Gi3/0, Gi3/1, Gi3/2, Gi3/3

100  Management              active
101  UserGroupA              active
102  UserGroupB              active
999  NATIVE                   active
1002 fddi-default             act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    eth  100000000 1500    0      0      0      0    0          0      0
100  eth  100000000 1500    0      0      0      0    0          0      0
101  eth  100000000 1500    0      0      0      0    0          0      0
102  eth  100000000 1500    0      0      0      0    0          0      0
999  eth  100000000 1500    0      0      0      0    0          0      0
1002 eth  100000000 1500    0      0      0      0    0          0      0
1003 eth  100000000 1500    0      0      0      0    0          0      0
1004 eth  100000000 1500    0      0      0      0    0          0      0
1005 eth  100000000 1500    0      0      0      0    0          0      0
```

A continuación copiamos el archivo **running-config** al archivo **startup-config** en todos los dispositivos el cual nos permite guardar las configuraciones realizadas

## Routers

Figura 9. Copiado archivo running-config en R1

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#
```

Figura 10. Copiado archivo running-config en R2

```
R2#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R2#
```

Figura 11. Copiado archivo running-config en R3

```
R3#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R3#
```

## Switches

Figura 12. Copiado archivo running-config en D1

```
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 4505 bytes to 2103 bytes[OK]
D1#
*Oct 17 17:00:24.505: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated
on disk. Please wait...
*Oct 17 17:00:25.358: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to d
isk successfully.
D1#
```

Figura 13. Copiado archivo running-config en D2

```
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 4505 bytes to 2097 bytes[OK]
D2#
*Oct 17 17:00:14.456: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated
  on disk. Please wait...
*Oct 17 17:00:15.310: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to d
isk successfully.
D2#
```

Figura 14. Copiado archivo running-config en A1

```
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 3743 bytes to 1737 bytes[OK]
A1#
*Oct 17 16:58:24.632: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated
  on disk. Please wait...
*Oct 17 16:58:25.522: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to d
isk successfully.
A1#
```

A continuación configuramos el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asignamos 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.

PC 1

Figura 15. Verificación configuración PC1

```
PC1> show ip

NAME           : PC1[1]
IP/MASK        : 10.0.100.5/24
GATEWAY        : 10.0.100.254
DNS            :
MAC            : 00:50:79:66:68:00
LPORT         : 20044
RHOST:PORT     : 127.0.0.1:20045
MTU            : 1500
```



PC 4

Figura 16. Verificación configuración PC4

```
PC4> show ip

NAME       : PC4[1]
IP/MASK    : 10.0.100.6/24
GATEWAY    : 10.0.100.254
DNS        :
MAC        : 00:50:79:66:68:03
LPORT      : 20046
RHOST:PORT : 127.0.0.1:20047
MTU        : 1500
```

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

En esta parte de la prueba de habilidades, se 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 Parte 2

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <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	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

	en caso de falla del puente raíz (root bridge).	
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 de la LAN local	PC1 debería hacer ping con éxito a: <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> PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> <li>• D1: 10.0.102.1</li> <li>• D2: 10.0.102.2</li> </ul> PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> <li>• D1: 10.0.101.1</li> <li>• D2: 10.0.101.2</li> </ul> PC4 debería hacer ping con éxito a: <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>

## Solución

A continuación se describe los comandos usados en cada uno de los puntos de la parte dos por cada uno de los switch, los cuales nos permiten realizar la habilitación de los enlaces trunk 802.1Q, configurar la Vlan 999 con Vlan native, los números de canal asignados y los puertos de acceso

### D1

```
interface range g0/1-3,g1/0
switchport trunk encapsulation dot1q
switchport mode trunk
```

```

switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
interface g1/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end

```

## **D2**

```

interface range g0/1-3,g1/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 12 mode active
no shutdown
exit
interface range g1/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
interface g1/3
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
end

```

## **A1**

```

spanning-tree mode rapid-pvst
interface range g0/0-1
switchport trunk encapsulation dot1q
switchport mode trunk

```

```

switchport trunk native vlan 999
channel-group 1 mode active
no shutdown
exit
interface range g0/2-3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 999
channel-group 2 mode active
no shutdown
exit
interface g1/0
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface g1/1
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end

```

Ahora vamos a realizar las respectivas validaciones en cada switch

## D1 y D2

Con el siguiente comando podemos verificar varios elementos de la operación de los enlaces troncales, como el modo en el que este se establece como troncal, protocolo de etiquetado de Vlans, estado del puerto, la vlan nativa entre otros. Con esto validamos los puntos 2.1, 2.2 y 2.5

Figura 17. Verificación troncales, vlan nativa y etherchannels en D1

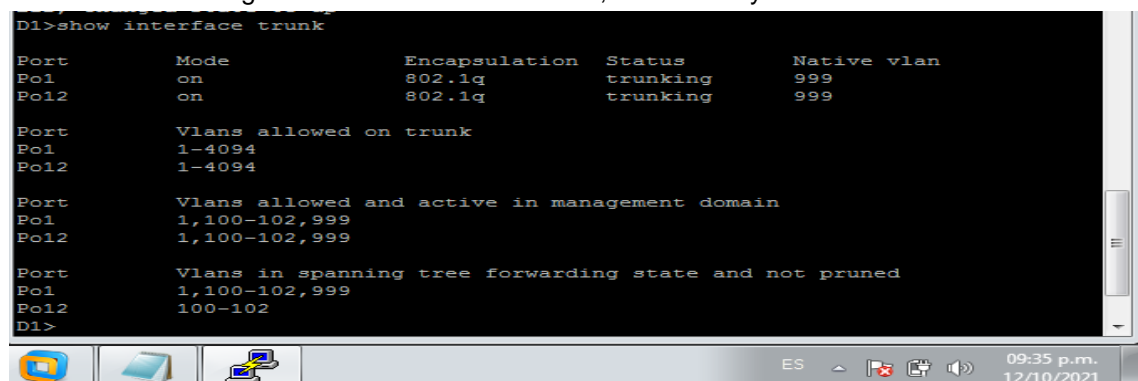


Figura 18. Verificación troncales, vlan nativa y etherchannels en D2

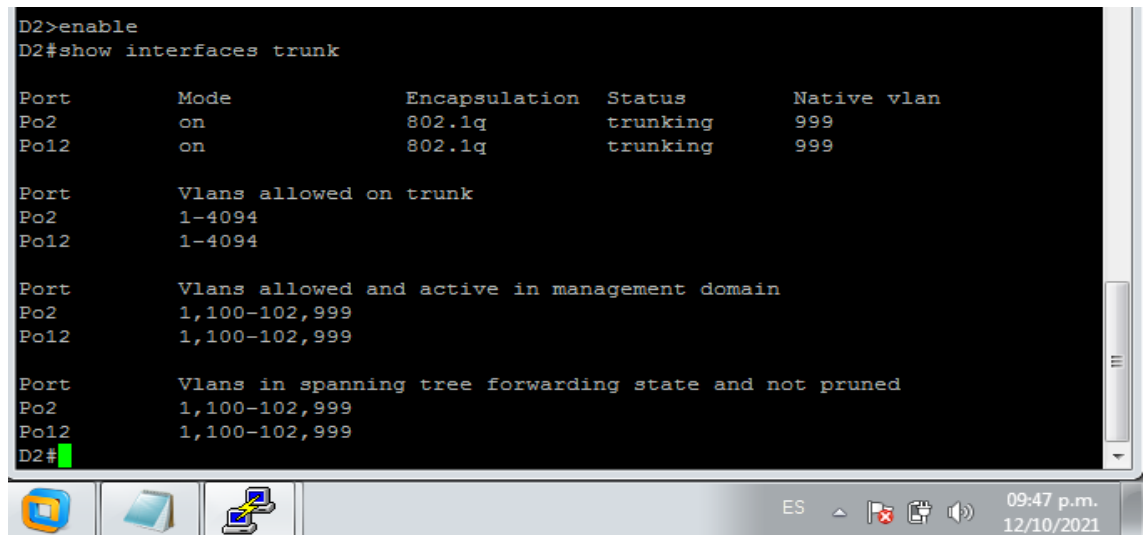
```
D2>enable
D2#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Po2       on        802.1q         trunking      999
Po12      on        802.1q         trunking      999

Port      Vlans allowed on trunk
Po2       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
Po2       1,100-102,999
Po12      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,100-102,999
Po12      1,100-102,999
D2#
```



Con el siguiente comando podemos validar los puertos de acceso del host

Figura 19. Verificación configuración puertos de acceso del host en D1

```
D1#show run interface g1/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/3
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
D1#
```

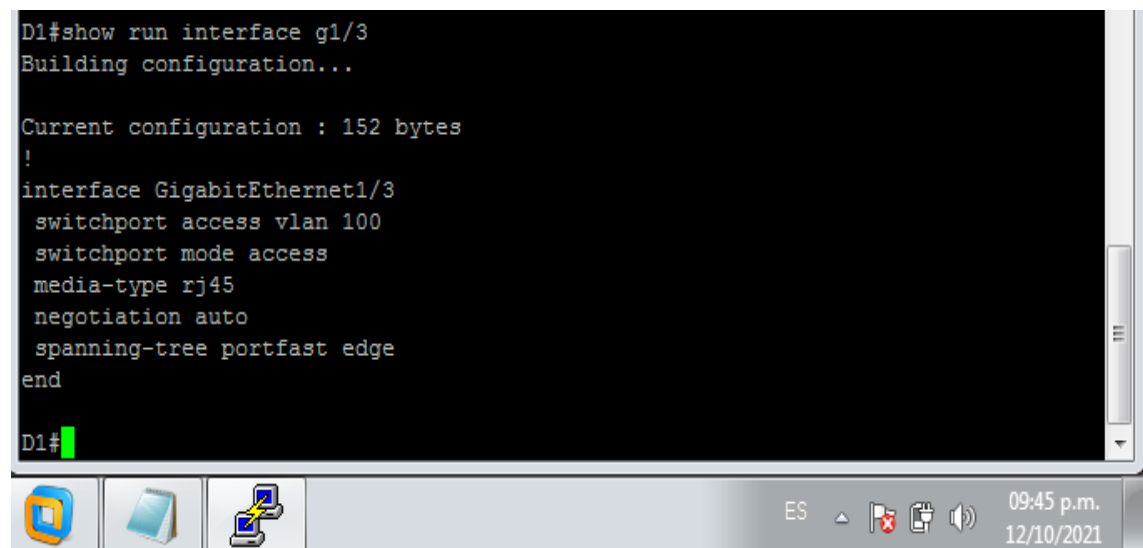
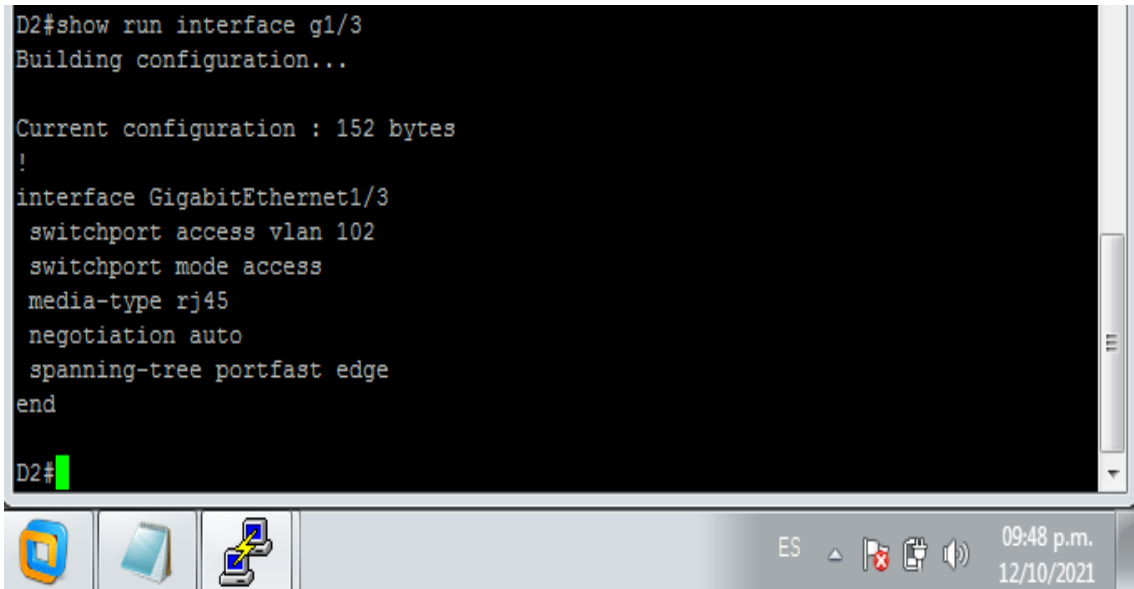


Figura 20. Verificación configuración puertos de acceso del host en D2

```
D2#show run interface g1/3
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/3
  switchport access vlan 102
  switchport mode access
  media-type rj45
  negotiation auto
  spanning-tree portfast edge
end

D2#
```



A1

Figura 21. Verificación troncales, vlan nativa y etherchannels en A1

```
A1#show interface trunk

Port      Mode      Encapsulation  Status        Native vlan
Po1       on        802.1q         trunking      999
Po2       on        802.1q         trunking      999

Port      Vlans allowed on trunk
Po1       1-4094
Po2       1-4094

Port      Vlans allowed and active in management domain
Po1       1,100-102,999
Po2       1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,100,102,999
Po2       1,101,999
A1#
```

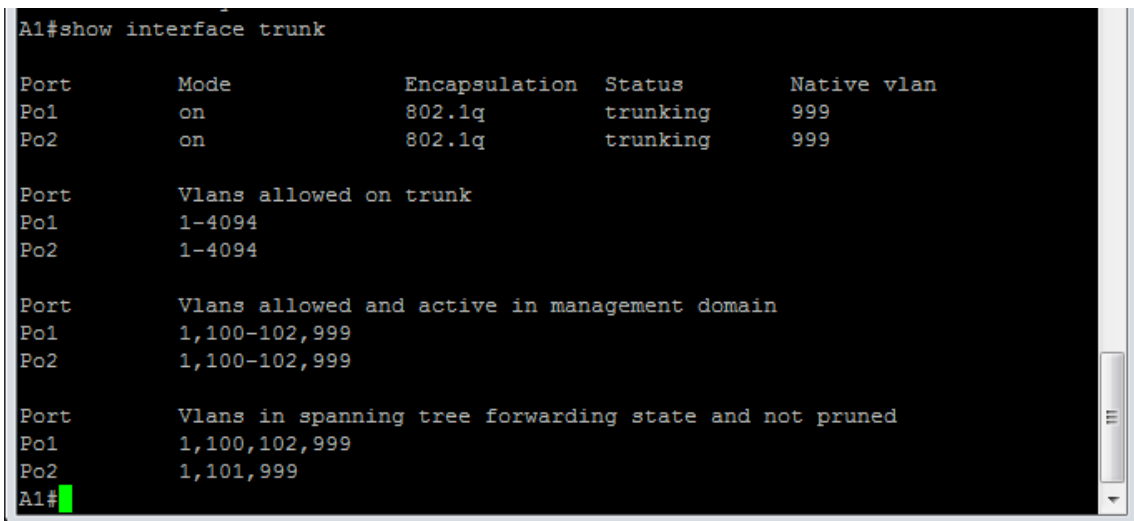
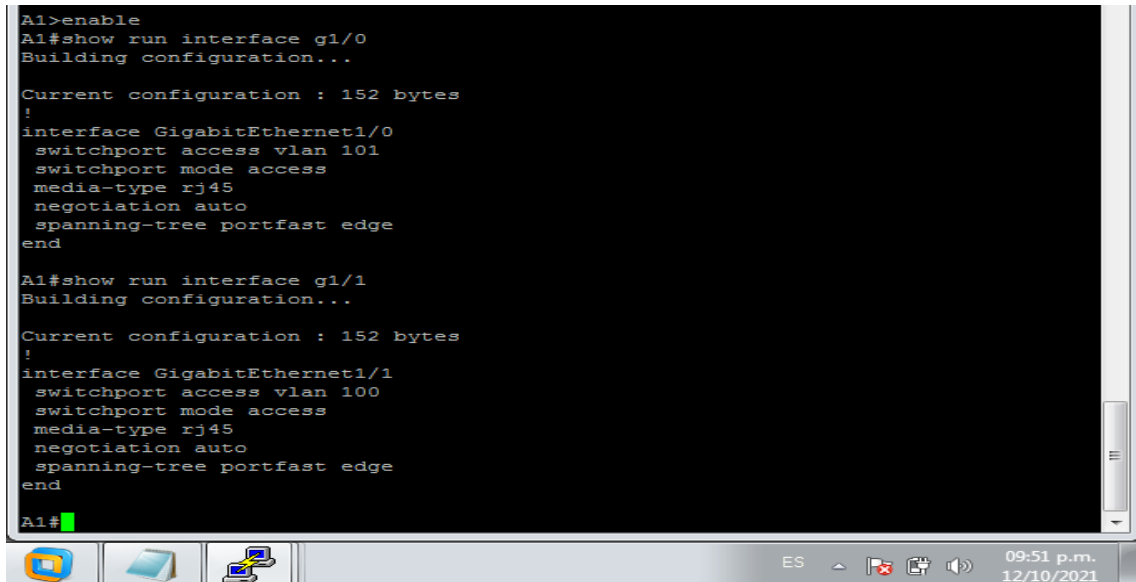


Figura 22. Verificación configuración puertos de acceso del host en A1



```
A1>enable
A1#show run interface g1/0
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/0
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end

A1#show run interface g1/1
Building configuration...

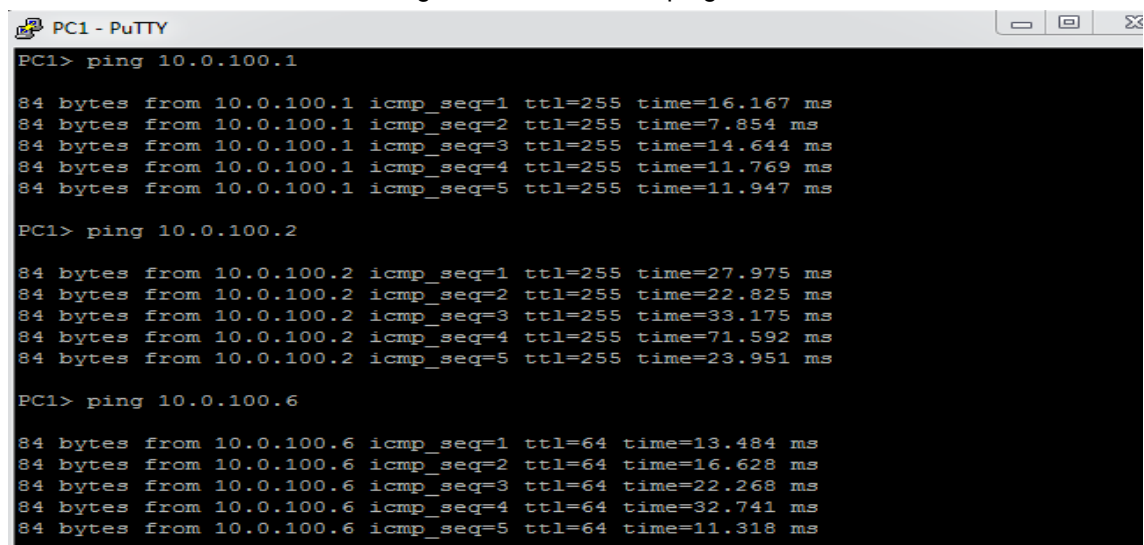
Current configuration : 152 bytes
!
interface GigabitEthernet1/1
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
 spanning-tree portfast edge
end
A1#
```

Con el anterior comando podemos validar los puertos de acceso del host

Ahora vamos a validar la conectividad de la red LAN utilizando el comando Ping el cual nos permite validar la respuesta del equipo destino y los tiempos

## PC1

Figura 23. Verificación ping desde PC1



```
PC1 - PuTTY
PC1> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=16.167 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=7.854 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=14.644 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=11.769 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=11.947 ms

PC1> ping 10.0.100.2

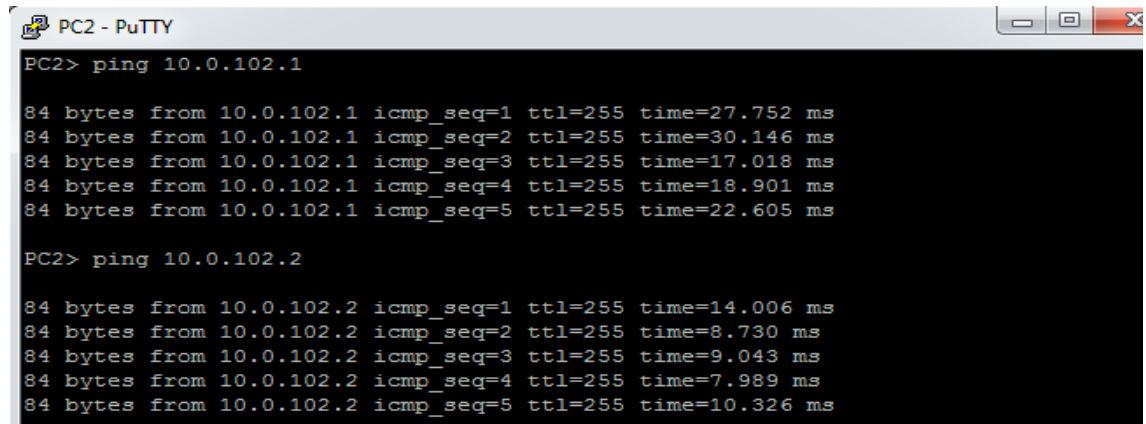
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=27.975 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=22.825 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=33.175 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=71.592 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=23.951 ms

PC1> ping 10.0.100.6

84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=13.484 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=16.628 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=22.268 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=32.741 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=11.318 ms
```

## PC2

Figura 24. Verificación ping desde PC2



```
PC2 - PuTTY
PC2> ping 10.0.102.1

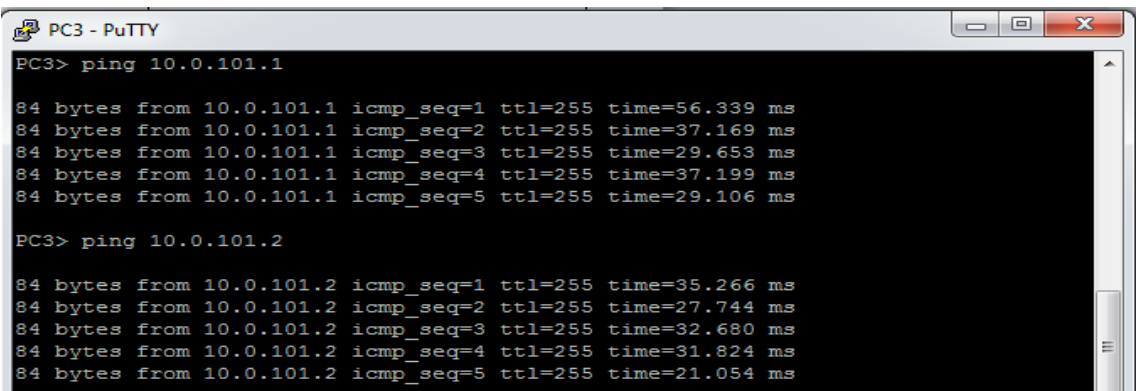
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=27.752 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=30.146 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=17.018 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=18.901 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=22.605 ms

PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=14.006 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=8.730 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=9.043 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=7.989 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=10.326 ms
```

## PC3

Figura 25. Verificación ping desde PC3



```
PC3 - PuTTY
PC3> ping 10.0.101.1

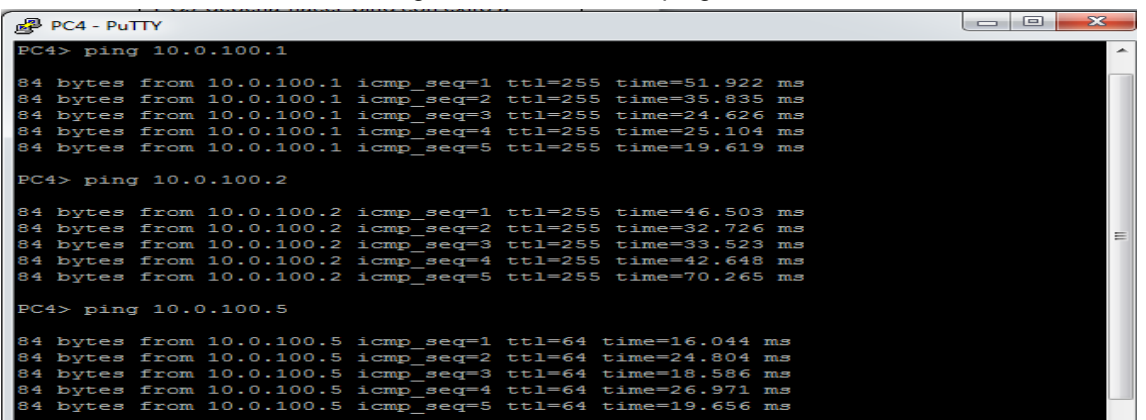
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=56.339 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=37.169 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=29.653 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=37.199 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=29.106 ms

PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=35.266 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=27.744 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=32.680 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=31.824 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=21.054 ms
```

## PC4

Figura 26. Verificación ping desde PC4



```
PC4 - PuTTY
PC4> ping 10.0.100.1

84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=51.922 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=35.835 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=24.626 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=25.104 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=19.619 ms

PC4> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=46.503 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=32.726 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=33.523 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=42.648 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=70.265 ms

PC4> ping 10.0.100.5

84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=16.044 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=24.804 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=18.586 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=26.971 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=19.656 ms
```



### Parte 3: Configurar los protocolos de enrutamiento

En esta parte, se 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 Parte 3

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en 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 <b>500</b> y use el router-id 2.2.2.2.</p> <p>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. Configure R1 en BGP ASN <b>300</b> y use el router-id 1.1.1.1. <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>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. En IPv6 address family:</li> </ul> <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> </li></ul>

## Solución

A continuación se describe los comandos usados en cada uno de los puntos de la parte tres por cada uno de los dispositivos, esto nos permite realizar la configuración de OSPFv2 y OSPFv3 de área única para los equipos de la red de la compañía y asignar router-id a cada equipo, así como la configuración de MP-BGP en los router de la red ISP al cual permite el transporte de la información de enrutamiento de varias capas de red y familias de direcciones

## R1

```
router ospf 4
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface g1/0
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
exit
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family
exit
```

## R2

```
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
```

```
network 2001:db8:2222::/128
network ::/0
exit-address-family
exit
```

### **R3**

```
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface g0/0
ipv6 ospf 6 area 0
exit
interface s3/0
ipv6 ospf 6 area 0
exit
end
```

### **D1**

```
router ospf 4
router-id 0.0.4.131
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface g0/0
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface g0/0
exit
interface g0/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

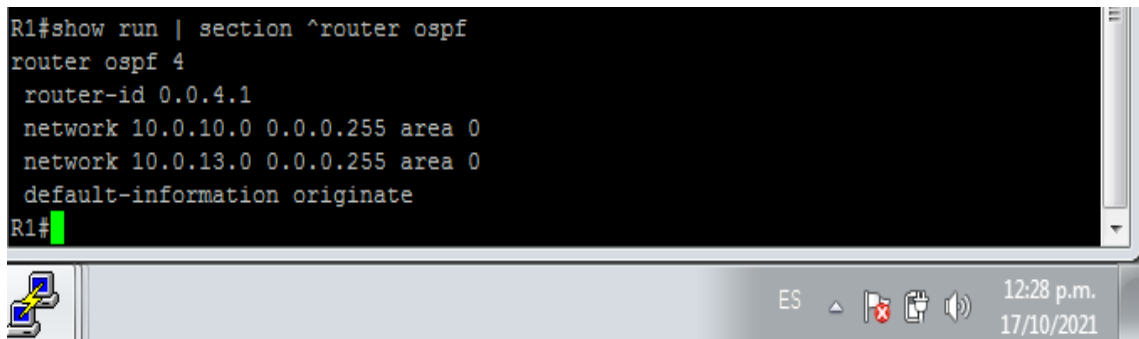
## D2

```
router ospf 4
router-id 0.0.4.132
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface g0/0
exit
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g0/0
exit
interface g0/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

Ahora vamos a realizar las respectivas validaciones en cada dispositivo para la configure single- area OSPFv2 en area 0 en cada uno de los dispositivos utilizando el comando **show run | section ^router ospf**

## R1

Figura 27. Verificación OSPFv2 en R1

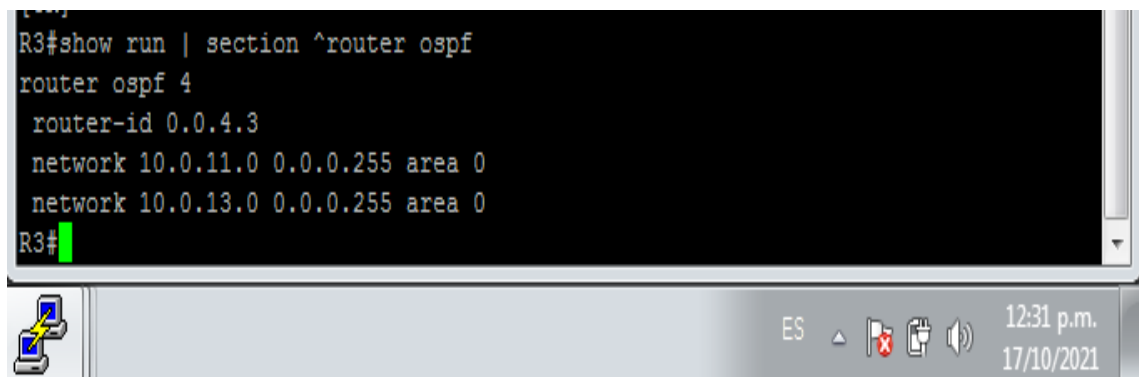


```
R1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.1
  network 10.0.10.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
  default-information originate
R1#
```

R3

Figura 28. Verificación OSPFv2 en R3

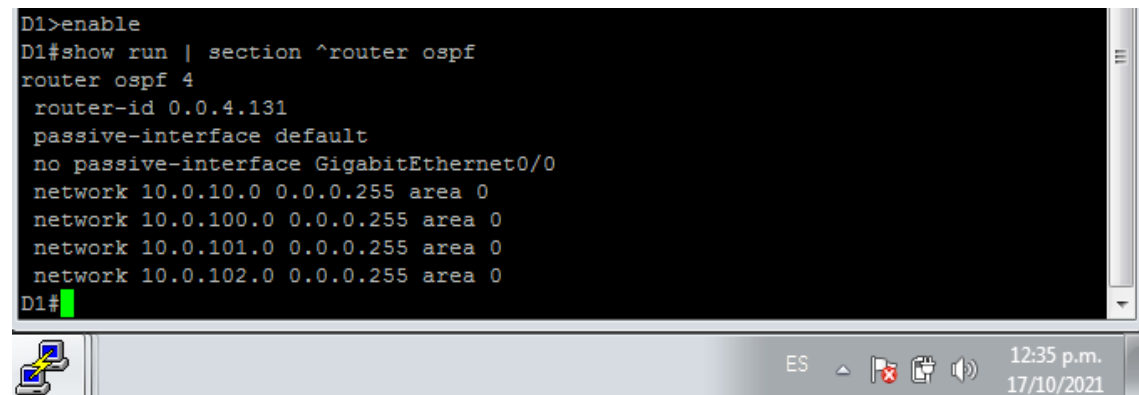
```
R3#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.3
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.13.0 0.0.0.255 area 0
R3#
```



D1

Figura 29. Verificación OSPFv2 en D1

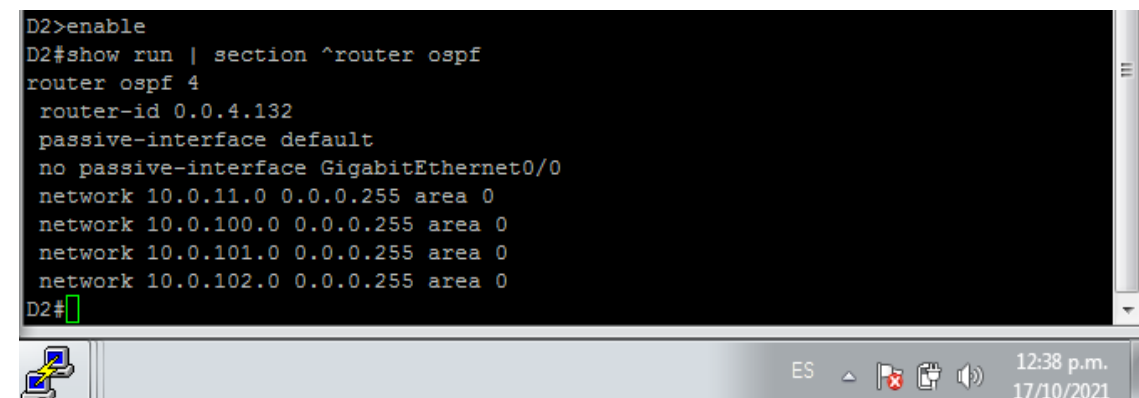
```
D1>enable
D1#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.131
  passive-interface default
  no passive-interface GigabitEthernet0/0
  network 10.0.10.0 0.0.0.255 area 0
  network 10.0.100.0 0.0.0.255 area 0
  network 10.0.101.0 0.0.0.255 area 0
  network 10.0.102.0 0.0.0.255 area 0
D1#
```



D2

Figura 30. Verificación OSPFv2 en D2

```
D2>enable
D2#show run | section ^router ospf
router ospf 4
  router-id 0.0.4.132
  passive-interface default
  no passive-interface GigabitEthernet0/0
  network 10.0.11.0 0.0.0.255 area 0
  network 10.0.100.0 0.0.0.255 area 0
  network 10.0.101.0 0.0.0.255 area 0
  network 10.0.102.0 0.0.0.255 area 0
D2#
```

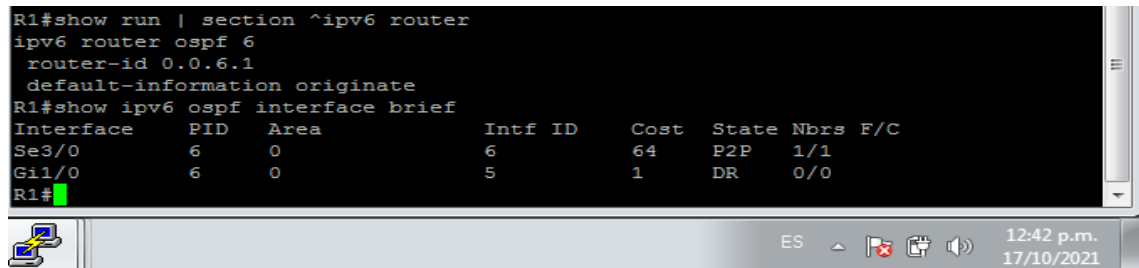


Ahora vamos a realizar las respectivas validaciones en cada dispositivo para configure classic single-area OSPFv3 en area 0 utilizando el comando **show run | section ^ipv6 router**

R1

Figura 31. Verificación OSPFv3 en R1

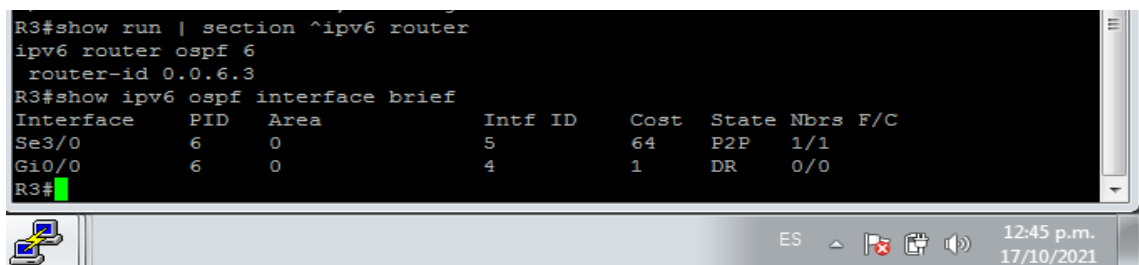
```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.1
  default-information originate
R1#show ipv6 ospf interface brief
Interface      PID    Area      Intf ID    Cost    State Nbrs F/C
Se3/0          6      0          6          64      P2P    1/1
Gi1/0          6      0          5          1       DR     0/0
R1#
```



R3

Figura 32. Verificación OSPFv3 en R3

```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
  router-id 0.0.6.3
R3#show ipv6 ospf interface brief
Interface      PID    Area      Intf ID    Cost    State Nbrs F/C
Se3/0          6      0          5          64      P2P    1/1
Gi0/0          6      0          4          1       DR     0/0
R3#
```

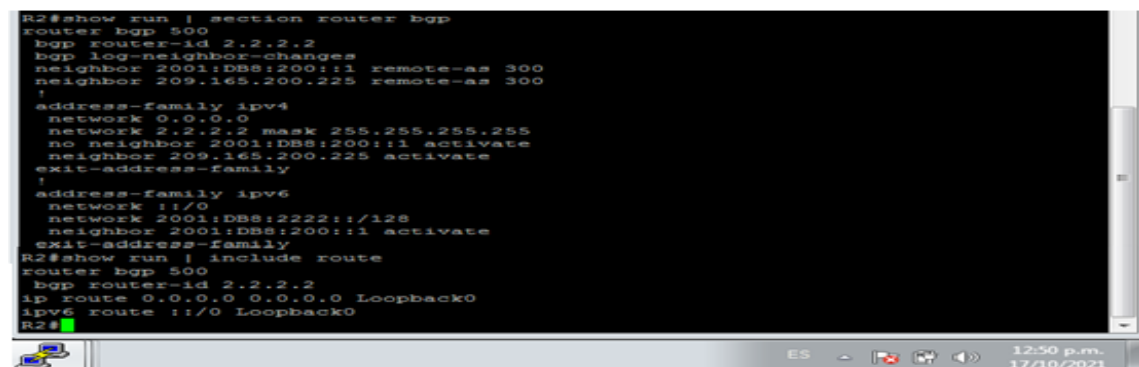


Ahora vamos a realizar las respectivas validaciones en cada dispositivo para R2 en la “Red ISP”, configure MP- BGP mediante el comando **show run | section router bgp**

R2

Figura 33. Verificación MP-BGP en R2

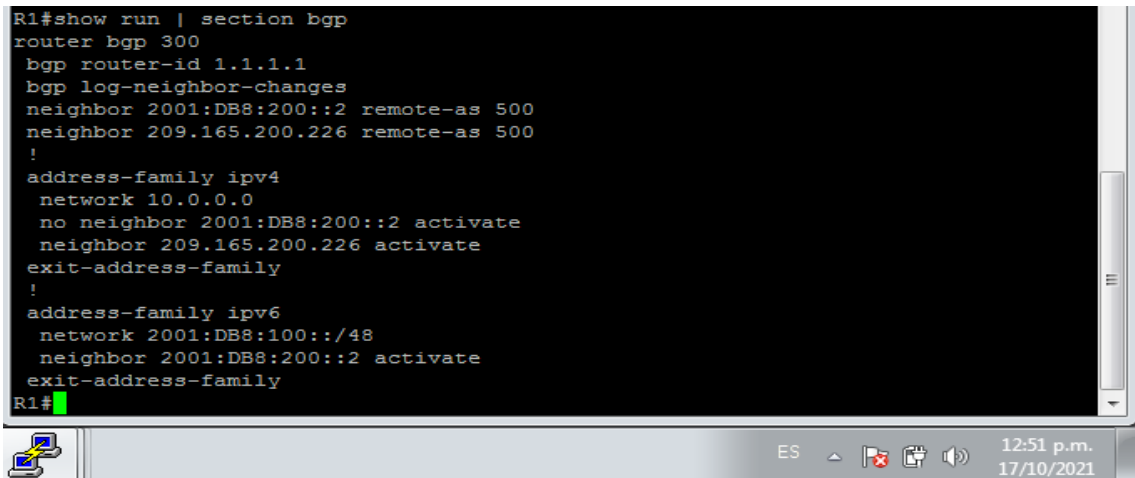
```
R2#show run | section router bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.225 remote-as 300
  !
  address-family ipv4
    network 0.0.0.0
    network 2.2.2.2 mask 255.255.255.255
    no neighbor 2001:DB8:200::1 activate
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:222::/128
    neighbor 2001:DB8:200::1 activate
  exit-address-family
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
  ip route 0.0.0.0 0.0.0.0 Loopback0
  ipv6 route ::/0 Loopback0
R2#
```



Ahora vamos a realizar las respectivas validaciones en cada dispositivo para R1 en la “Red ISP”, configure MP- BGP mediante el comando **show run | section bgp**

R1

Figura 34. Verificación MP-BGP en R1

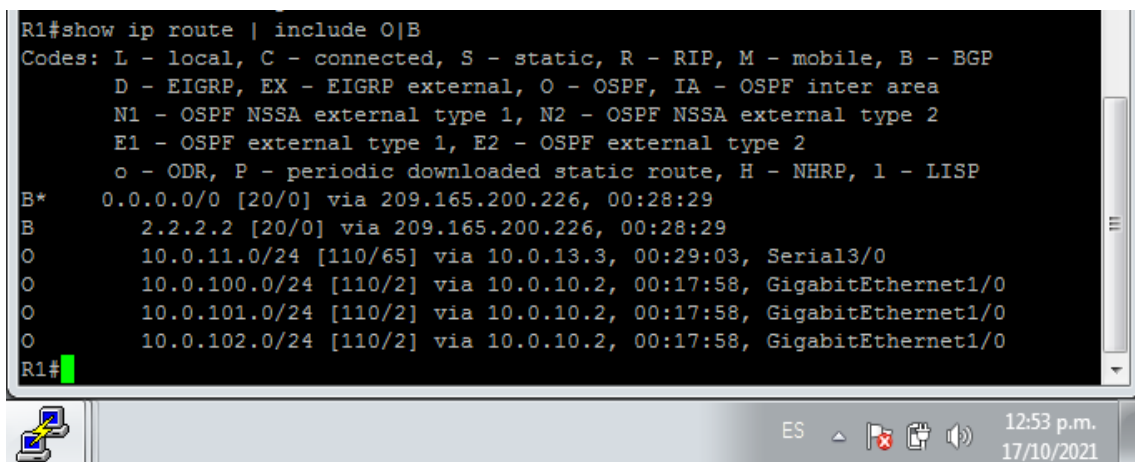


```
R1#show run | section bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
    neighbor 2001:DB8:200::2 activate
  exit-address-family
R1#
```

Luego de esto procedemos a verificar que OSPF y BGP funcionen de forma correcta para IPv4, para esto implementamos el comando **show ip route | include O|B**

R1

Figura 35. Verificación OSPF y BGP en R1



```
R1#show ip route | include O|B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
B*    0.0.0.0/0 [20/0] via 209.165.200.226, 00:28:29
B     2.2.2.2 [20/0] via 209.165.200.226, 00:28:29
O     10.0.11.0/24 [110/65] via 10.0.13.3, 00:29:03, Serial3/0
O     10.0.100.0/24 [110/2] via 10.0.10.2, 00:17:58, GigabitEthernet1/0
O     10.0.101.0/24 [110/2] via 10.0.10.2, 00:17:58, GigabitEthernet1/0
O     10.0.102.0/24 [110/2] via 10.0.10.2, 00:17:58, GigabitEthernet1/0
R1#
```



Ahora verificamos si las redes IPv6 y las direcciones específicas de la interfaz IPv6 se instalaron en la tabla de enrutamiento IPv6, esto lo hacemos mediante el comando **show ipv6 route** el cual muestra solamente redes IPv6, no redes IPv4.

R1

Figura 36. Verificación OSPFv3 para IPv6 en R1

```
R1#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDR - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
B ::0 [20/0]
  via FE80::2:1, GigabitEthernet0/0
S 2001:DB8:100::1/48 [1/0]
  via Null0, directly connected
C 2001:DB8:100:1010::/64 [0/0]
  via GigabitEthernet1/0, directly connected
L 2001:DB8:100:1010::1/128 [0/0]
  via GigabitEthernet1/0, receive
O 2001:DB8:100:1011::/64 [110/65]
  via FE80::3:3, Serial3/0
C 2001:DB8:100:1013::/64 [0/0]
  via Serial3/0, directly connected
L 2001:DB8:100:1013::1/128 [0/0]
  via Serial3/0, receive
C 2001:DB8:200::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:200::1/128 [0/0]
  via GigabitEthernet0/0, receive
L FE00::/8 [0/0]
  via Null0, receive
R1#
```

Finalmente realizamos las validaciones de OSPF para IPv4 y OSPFv3 para IPv6 mediante el comando **show ip route ospf** el cual nos muestra solo las rutas OSPF descubiertas en la tabla de routing.

Figura 37. Verificación OSPF y OSPFv3 en R3

```
R3#show ip route ospf | begin Gateway
Gateway of last resort is 10.0.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 00:36:36, Serial3/0
  10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O    10.0.10.0/24 [110/65] via 10.0.13.1, 00:37:13, Serial3/0
O    10.0.100.0/24 [110/2] via 10.0.11.2, 00:22:51, GigabitEthernet0/0
O    10.0.101.0/24 [110/2] via 10.0.11.2, 00:22:51, GigabitEthernet0/0
O    10.0.102.0/24 [110/2] via 10.0.11.2, 00:22:51, GigabitEthernet0/0
R3#
R3#show ipv6 route ospf
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
ND - ND Default, NDp - ND Prefix, DCE - Destination, NDR - Redirect
O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, 1 - LISP
OE2 ::0 [110/1], tag 6
  via FE80::1:3, Serial3/0
O 2001:DB8:100:1013::/64 [110/128]
  via FE80::1:3, Serial3/0
R3#
```

#### 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 Parte 4

Tarea#	Tarea	Especificación
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 rastreo <b>4</b> para la IP SLA 4.</li><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>

4.3	En D1 configure HSRPv2	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP versión 2.</p> <p>Configure IPv4 HSRP grupo <b>104</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.100.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 y decremente en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>114</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.101.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>124</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.102.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>106</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>116</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Registre el objeto 6 y decremente en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>126</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> </ul> <p>Rastree el objeto 6 y decremente en 60</p>
-----	------------------------	---

	<p>En D2, configure HSRPv2</p>	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure HSRP versión 2.</p> <p>Configure IPv4 HSRP grupo <b>104</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.100.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 y decremente en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>114</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.101.254</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv4 HSRP grupo <b>124</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual <b>10.0.102.254</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 4 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>106</b> para la VLAN 100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>116</b> para la VLAN 101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Establezca la prioridad del grupo en <b>150</b>.</li> <li>• Habilite la preferencia (preemption).</li> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul> <p>Configure IPv6 HSRP grupo <b>126</b> para la VLAN 102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6 autoconfig</b>.</li> <li>• Habilite la preferencia (preemption).</li> </ul> <p>Rastree el objeto 6 para disminuir en 60</p>
--	--------------------------------	---

## Solución

A continuación se describe los comandos usados en cada uno de los puntos de la parte cuatro por cada uno de los dispositivos, lo cual nos permitirá la creación de IP SLAs para D1 y D2, los cual permitirá 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, también permitirán la configuración de HSRPv2 en ambos switch asignando IPv4 HSRP grupos a cada una de las Vlan, estableciendo prioridades de 150

### D1

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

```

exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
end

```

## D2

```

ip sla 4
icmp-echo 10.0.11.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102

```

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

Ahora vamos a realizar las respectivas validaciones en cada dispositivo para cada uno de los puntos del paso 4

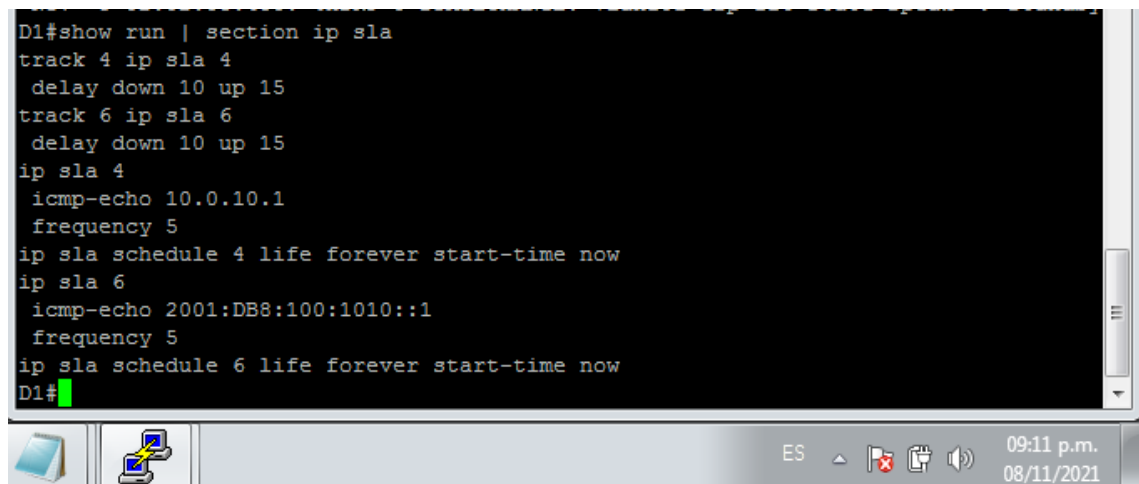
Configuraciones para D1 de los pasos 4.1 y 4.3

Para ello ejecutamos el siguiente comando

**show run | section ip sla**

a continuación se muestra la configuración para IP SLAs

Figura 38 configuración IP SLAs para D1

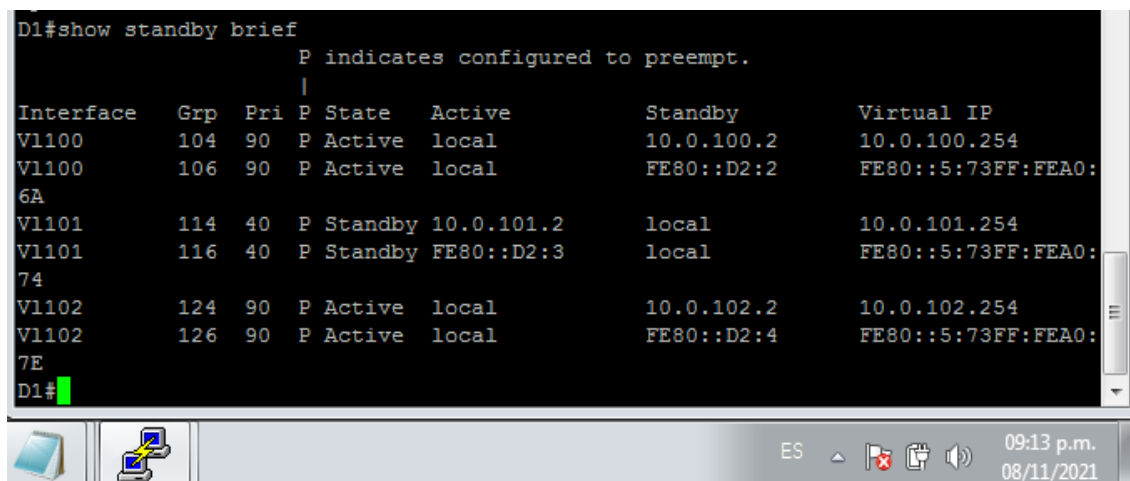


```
D1#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

A continuación validamos las configuraciones para cada una de las vlan con el comando **show standby brief** el cual nos brinda una descripción breve de el grupo, prioridad, estado e ip virtual.

Figura 39 configuración Vlans para D1

```
D1#show standby brief
P indicates configured to preempt.
|
Interface    Grp  Pri  P State    Active        Standby        Virtual IP
Vl100        104  90   P Active   local         10.0.100.2    10.0.100.254
Vl100        106  90   P Active   local         FE80::D2:2    FE80::5:73FF:FEA0:
6A
Vl101        114  40   P Standby  10.0.101.2    local         10.0.101.254
Vl101        116  40   P Standby  FE80::D2:3    local         FE80::5:73FF:FEA0:
74
Vl102        124  90   P Active   local         10.0.102.2    10.0.102.254
Vl102        126  90   P Active   local         FE80::D2:4    FE80::5:73FF:FEA0:
7E
D1#
```



Configuraciones para D2 de los pasos 4.2 y 4.3

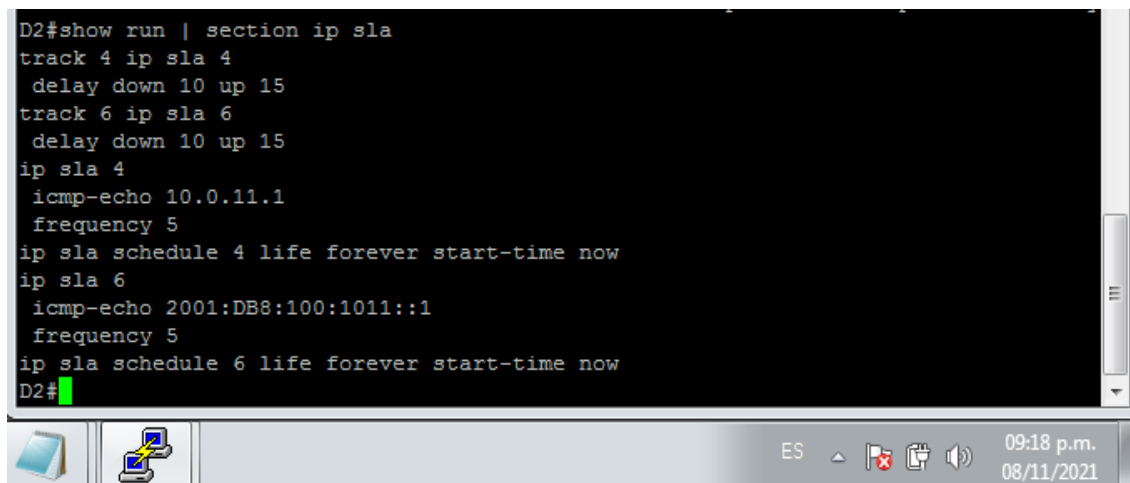
Para ello ejecutamos el siguiente comando

**show run | section ip sla**

a continuación se muestra la configuración para IP SLAs

Figura 40 configuración IP SLAs para D2

```
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
D2#
```





A continuación validamos las configuraciones para cada una de las vlan

Figura 41 configuración Vlans para D2

```

D2#show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri  P State   Active        Standby        Virtual IP
Vl100          104  40   P Standby 10.0.100.1    local          10.0.100.254
Vl100          106  40   P Standby FE80::D1:2    local          FE80::5:73FF:FEA0:
6A
Vl101          114  90   P Active  local         10.0.101.1     10.0.101.254
Vl101          116  90   P Active  local         FE80::D1:3     FE80::5:73FF:FEA0:
74
Vl102          124  40   P Standby 10.0.102.1    local          10.0.102.254
Vl102          126  40   P Standby FE80::D1:4    local          FE80::5:73FF:FEA0:
7E
D2#

```

## 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 Parte 5

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: <ul style="list-style-type: none"> <li>Nombre de usuario Local: <b>admin</b></li> <li>Nivel de privilegio <b>15</b></li> <li>Contraseña: <b>cisco12345cisco</b></li> </ul>
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.: <ul style="list-style-type: none"> <li>Dirección IP del servidor RADIUS es 10.0.100.6.</li> <li>Puertos UDP del servidor RADIUS son 1812 y 1813.</li> <li>Contraseña: <b>\$strongPass</b></li> </ul>

5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: <ul style="list-style-type: none"> <li>• Use la lista de métodos por defecto</li> <li>• Valide contra el grupo de servidores RADIUS</li> <li>• De lo contrario, utilice la base de datos local.</li> </ul>
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> .

## Solucion

A continuación se describe los comandos usados en cada uno de los puntos de la parte cinco por cada uno de los dispositivos, lo cual nos permitirá crear privilegios de encriptación con nivel de seguridad 15 usando usuario y contraseña, la habilitación de AAA y configuración de servidor RADIUS, los cuales permite el acceso de los usuarios legítimos a los activos conectados a la red e impide el acceso no autorizado.

Primero vamos a ejecutar el comando algoritmo de encriptación SCRYPT con la Contraseña: cisco12345cisco y crear un usuario local protegiéndolo con el algoritmo de encriptación.

Para ello ejecutamos los siguientes comandos en todos los dispositivos

```
enable algorithm-type SCRYPT secret cisco12345cisco
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
```

Una vez ejecutados los comandos procedemos a realizar las configuraciones de los puntos 5.3 a 5.6 con los siguientes comandos en todos los dispositivos a excepción de R2

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

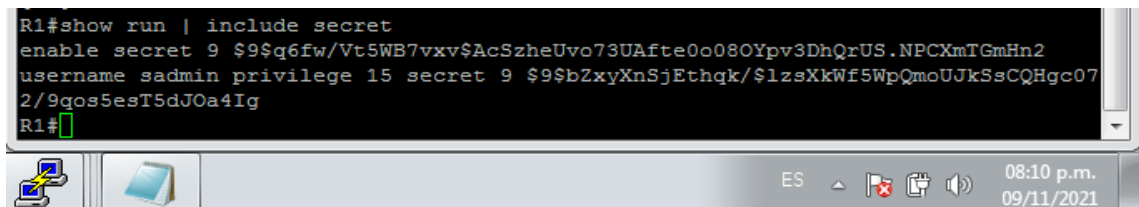
Ahora vamos a realizar las respectivas validaciones en cada dispositivo para cada uno de los puntos del paso 5

### Paso 5.1 y 5.2

Para este paso ejecutamos el comando **show run | include secret** para validar la encriptación, usuario y nivel de privilegio, este lo aplicamos para cada uno de los dispositivos.

#### R1

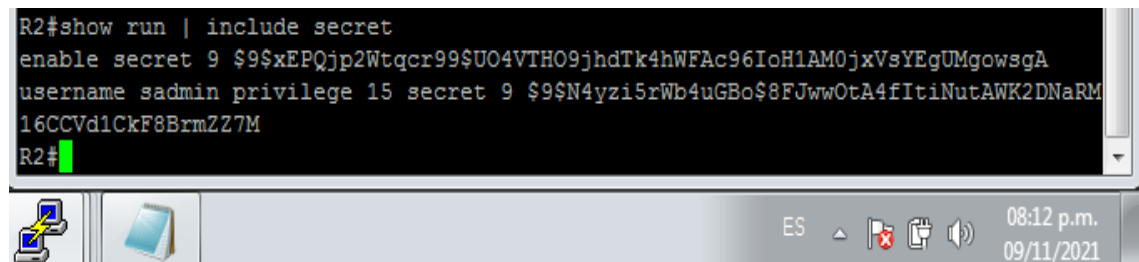
Figura 42 validación de encriptación SCRYPT y usuario R1



```
R1#show run | include secret
enable secret 9 $9$q6fw/Vt5WB7vxv$AcSzheUvo73UAfte0o08OYpv3DhQrUS.NPCXmTGMHn2
username sadmin privilege 15 secret 9 $9$bZxyXnSjEthqk/$1zsXkWf5WpQmoUJkSsCQHgc07
2/9qosSesT5dJOa4Ig
R1#
```

#### R2

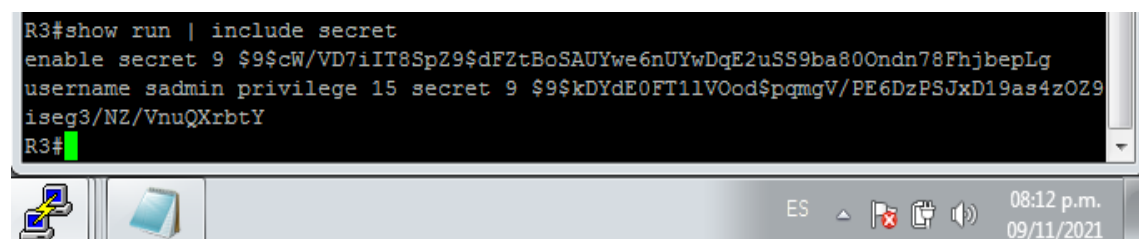
Figura 43 validación de encriptación SCRYPT y usuario R2



```
R2#show run | include secret
enable secret 9 $9$xEPQjp2Wtqcr99$UO4VTH09jhdTk4hWFAc96IoH1AM0jxVsYEgUMgowsgA
username sadmin privilege 15 secret 9 $9$N4yzi5rWb4uGBo$8FJwwOtA4fItiNutAWK2DNaRM
16CCVd1CkF8BrmZZ7M
R2#
```

#### R3

Figura 44 validación de encriptación SCRYPT y usuario R3

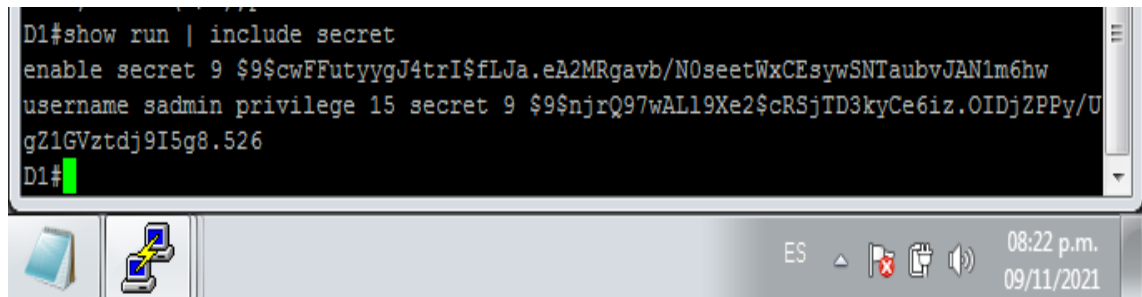


```
R3#show run | include secret
enable secret 9 $9$cW/VD7iIT8SpZ9$dFZtBoSAUYwe6nUYwDgE2uSS9ba80Ondn78Fhjbeplg
username sadmin privilege 15 secret 9 $9$kDYdE0FT11VOod$pmgV/PE6DzPSJxD19as4zOZ9
iseg3/NZ/VnuQXrbtY
R3#
```

D1

Figura 45 validación de encriptación SCRYPT y usuario D1

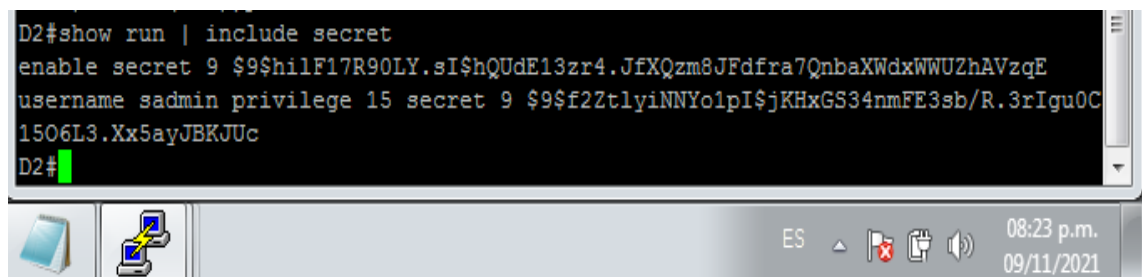
```
D1#show run | include secret
enable secret 9 $9$cwFFutygJ4trI$fLJa.eA2MRgavb/N0seetWxCEsywSNTaubvJAN1m6hw
username sadmin privilege 15 secret 9 $9$njrQ97wAL19Xe2$cRSjTD3kyCe6iz.OIDj2PPy/U
gZ1GVztdj9I5g8.526
D1#
```



D2

Figura 46 validación de encriptación SCRYPT y usuario D2

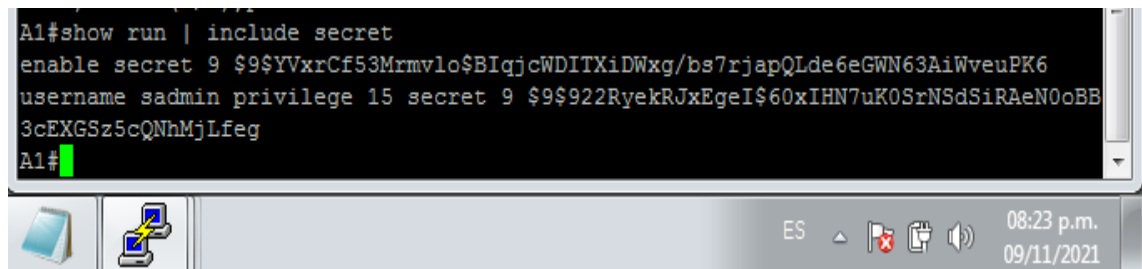
```
D2#show run | include secret
enable secret 9 $9$h1lF17R90LY.sI$hQUdE13zr4.JfXQzm8JFdfra7QnbaXWdxWWUZhAVzqE
username sadmin privilege 15 secret 9 $9$f2ZtlyiNNYo1pI$jKHxGS34nmFE3sb/R.3rIguOC
1506L3.Xx5ayJBKJUc
D2#
```



A1

Figura 47 validación de encriptación SCRYPT y usuario A1

```
A1#show run | include secret
enable secret 9 $9$YVxrCf53Mrmvlo$BIqjcWDITXiDWxg/bs7rjapQLde6eGWN63AiWveuPK6
username sadmin privilege 15 secret 9 $9$922RyekRJxEgeI$60xIHN7uK0SrNSdSiRAeN0oBB
3cEXGSz5cQNhmJLfeg
A1#
```

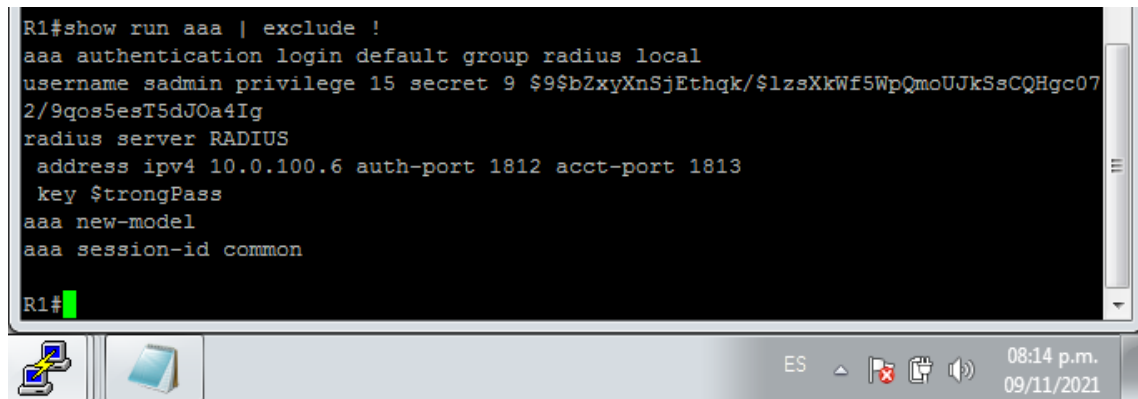


Ahora realizamos las validaciones para verificar la configuración de los puntos 5.3 al 5.5 mediante el comando **show run aaa | exclude !** el cual nos permite validar la habilitación de AAA, las especificaciones del servidor RADIUS como lo son ip, puerto y contraseña, este lo aplicamos a todos los dispositivos a excepción de R2

R1

Figura 48 validación de configuraciones puntos 5.3 al 5.5 R1

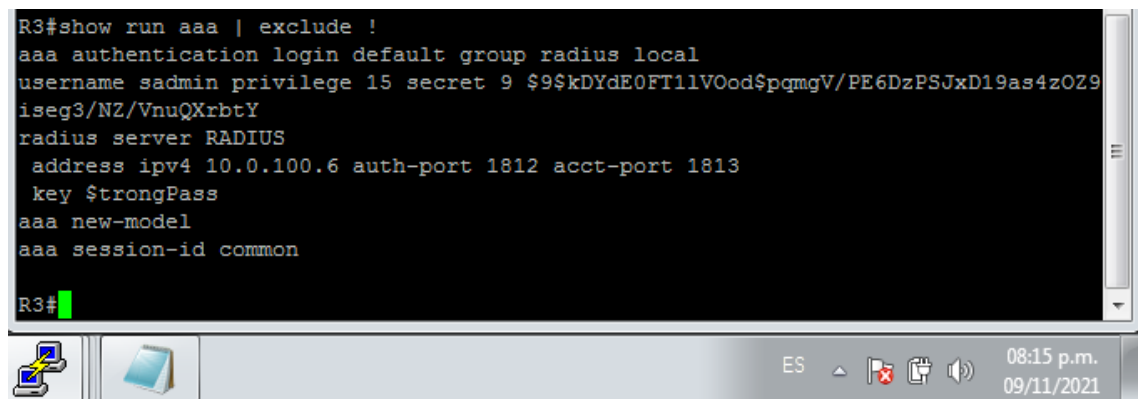
```
R1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$bZxyXnSjEthqk/$1zsXkWf5WpQmoUJkSsCQHgc07
2/9qos5esT5dJOa4Ig
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
R1#
```



R3

Figura 49 validación de configuraciones puntos 5.3 al 5.5 R3

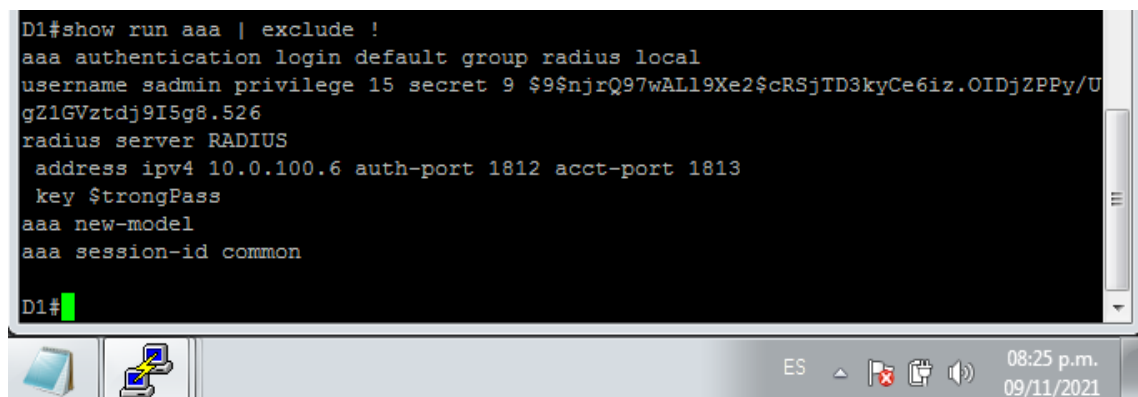
```
R3#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$kDYdE0FT1lVOod$pmgV/PE6DzPSJxD19as4zOZ9
iseg3/NZ/VnuQXrbtY
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
R3#
```



D1

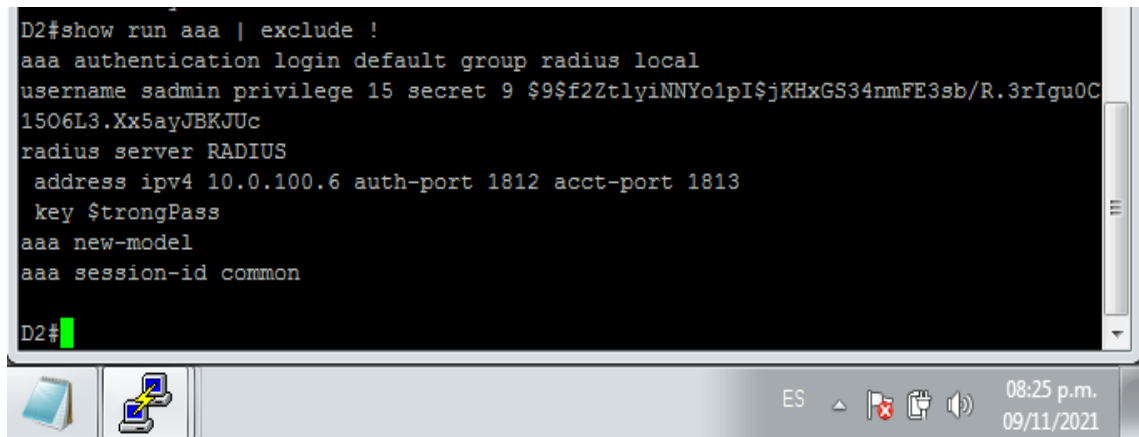
Figura 50 validación de configuraciones puntos 5.3 al 5.5 D1

```
D1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$njrQ97wALl9Xe2$cRSjTD3kyCe6iz.OIDjZPPy/U
gZlGVztdj9I5g8.526
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
D1#
```



D2

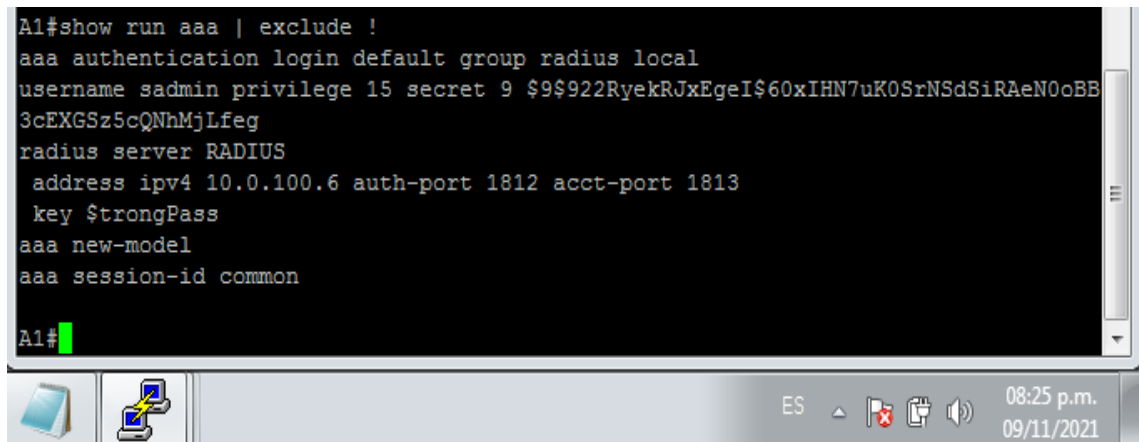
Figura 51 validación de configuraciones puntos 5.3 al 5.5 D2



```
D2#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$f22tlyiNNYolpI$jKHxGS34nmFE3sb/R.3rIgu0C
1506L3.Xx5ayJBKJUc
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
D2#
```

A1

Figura 52 validación de configuraciones puntos 5.3 al 5.5 A1



```
A1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$922RyekRJxEgeI$60xIHN7uK0SrNSdSiRAeN0oBB
3cEXGSz5cQNhMjLfeg
radius server RADIUS
  address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
  key $strongPass
aaa new-model
aaa session-id common
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 Parte 6

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un 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	Especificaciones de SNMPv2: <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 <i>community string</i> en <b>ENCORSA</b>.</li> <li>• En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i>.</li> <li>• En R1, habilite el envío de <i>traps bgp</i>, <i>config</i>, y <i>ospf</i>.</li> <li>• En A1, habilite el envío de <i>traps config</i>.</li> </ul>

## Solucion

A continuación se describe los comandos usados en cada uno de los puntos de la parte seis por cada uno de los dispositivos, esto nos permitirá realizar la configuración de la hora local, NTP el cual permite que los dispositivos de red

sincronicen la configuración de la hora con un servidor NTP, Syslog para el envío de mensajes de eventos y SNMP que permite administrar y monitorizar elementos de la red.

Primero ejecutamos el siguiente comando para configurar la zona horaria local en cada uno de los dispositivos

```
clock timezone UTC -5
```

Posterior a esto configuramos R2 como un NTP maestro ejecutando la siguiente línea de comando

```
ntp master 3  
end
```

Finalmente en cada uno de los dispositivos a excepción de R2 ejecutamos las líneas de comando para configurar los pasos 6.3, 6.4 y 6.5

## **R1**

```
ntp server 2.2.2.2  
logging trap warning  
logging host 10.0.100.5  
logging on  
ip access-list standard SNMP-NMS  
permit host 10.0.100.5  
exit  
snmp-server contact Cisco Student  
snmp-server community ENCORSA ro SNMP-NMS  
snmp-server host 10.0.100.5 version 2c ENCORSA  
snmp-server ifindex persist  
snmp-server enable traps bgp  
snmp-server enable traps config  
snmp-server enable traps ospf  
end
```

## **R3**

```
ntp server 10.0.10.1  
logging trap warning  
logging host 10.0.100.5  
logging on  
ip access-list standard SNMP-NMS
```



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

## **D1**

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server ifindex persist
snmp-server enable traps config
snmp-server enable traps ospf
end
```

## **D2**

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp-server enable traps config
snmp-server enable traps ospf
end
```

## **A1**

```
ntp server 10.0.10.1
logging trap warning
logging host 10.0.100.5
logging on
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
```

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

Ahora vamos a realizar las respectivas validaciones en cada dispositivo para cada uno de los puntos del paso 6

Primero vamos a validar la hora local en cada uno de los dispositivos con el comando **Show clock**

Figura 53 validación de hora local R2



Figura 54 validación de hora local R1



Este paso se repite con los demás dispositivos

Ahora validamos la configuración del R2 como master mediante el comando **show run | include ntp**

Figura 55 validación master R2



Ahora validamos la configuración NTP en los dispositivos a excepción de R2

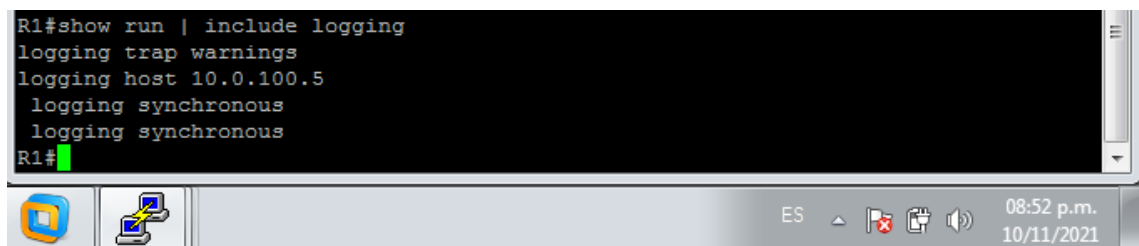
```
R1# show ntp status | include stratum  
Clock is synchronized, stratum 4, reference is 2.2.2.2
```

```
A1# show ntp status | include stratum  
Clock is synchronized, stratum 5, reference is 10.0.10.1
```

Esto lo hacemos con cada dispositivo

Ahora vamos a validar la Configuración de Syslog en todos los dispositivos excepto R2 mediante el comando **show run | include logging**

Figura 56 validación de Syslog R1



```
R1#show run | include logging  
logging trap warnings  
logging host 10.0.100.5  
logging synchronous  
logging synchronous  
R1#
```

Figura 57 validación de Syslog D1



```
D1#show run | include logging  
logging trap warnings  
logging host 10.0.100.5  
logging synchronous  
D1#
```

Esto se aplica para cada dispositivo a excepción de R2

Por ultimo vamos a validar la configuración del punto 6.5 SNMPv2c en todos los dispositivos excepto R2 mediante el comando **show ip access-list SNMP-NMS**

R1

Figura 58 validación de SNMPv2c R1



```
R1#show ip access-list SNMP-NMS  
Standard IP access list SNMP-NMS  
10 permit 10.0.100.5  
R1#
```

D1

Figura 59 validación de SNMPv2c D1

```
D1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
D1#
```



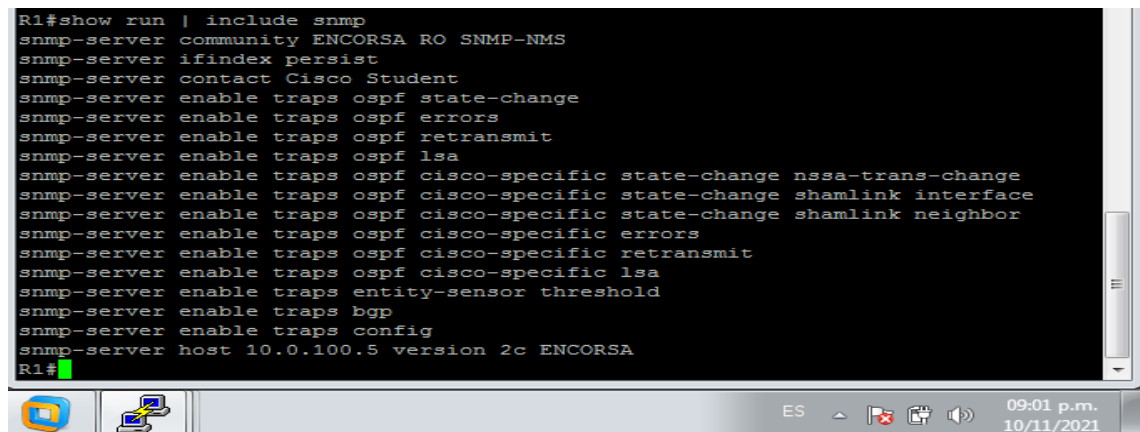
Esto lo aplicamos a cada dispositivo

Finalmente ejecutamos la línea de comandos para validar la segunda parte del punto 6.5 mediante el comando **show run | include snmp**

R1

Figura 60 validación Limitación del acceso SNMP R1

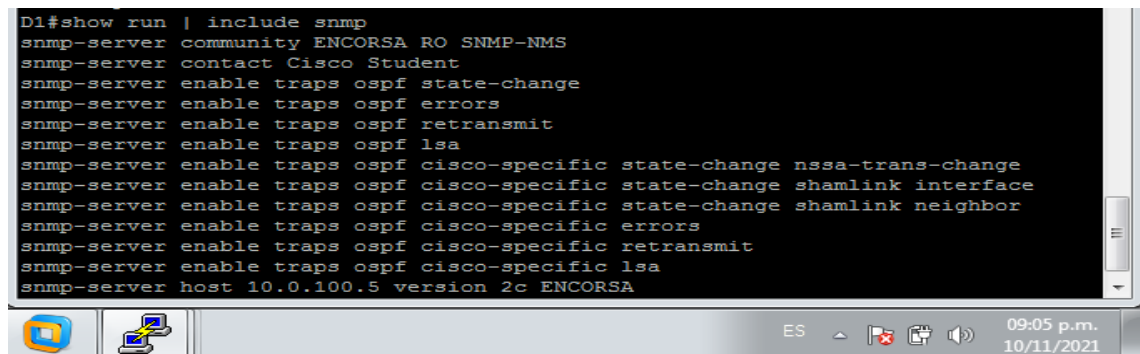
```
R1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
R1#
```



D1

Figura 61 validación Limitación del acceso SNMP D1

```
D1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
D1#
```



De igual manera se aplica para cada dispositivo

## **CONCLUSIONES**

El proyecto se centra en la implementación de un escenario de red para una empresa, poniendo en práctica los conocimientos adquiridos durante el desarrollo del diplomado, con el manejo de herramientas de simulación y aplicando las configuraciones de los enrutamientos y diferentes protocolos vistos en las diferentes etapas.

Para cada una de las etapas se realiza la adaptación y configuración de cada uno de los comandos previstos y de esta manera poder implementar cada uno de los protocolos, vlan y enrutamientos solicitados, dando así como resultado una red que se comporta según lo esperado en cada etapa.

Mediante el uso de software de simulación GNS3 el cual nos permite utilizar imágenes de dispositivos reales y mediante el acoplamiento de este con una maquina virtualizada mediante el uso de VMware podemos contar con un escenario que se comporta de la misma manera que lo haría un sistema de administración de red de una empresa.

Como futuros ingenieros debemos contar con un amplio conocimiento en la estructuración e implementación de redes y como estas pueden variar en su configuración y adaptación de acuerdo a las necesidades de cada empresa o institución como lo son soluciones para el fortalecimiento de la seguridad de la información

## BIBLIOGRAFÍA

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). **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). **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). **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). **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). **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). **BGP**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>