

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

FREDY ANDRÉS MÁRQUEZ MARÍN

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FREDY ANDRÉS MÁRQUEZ MARÍN

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

**NOTA DE ACEPTACIÓN**

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

Pereira, 29 de noviembre de 2021

## CONTENIDO

GLOSARIO.....	7
RESUMEN.....	8
ABSTRACT .....	9
INTRODUCCION .....	10
DESARROLLO ESCENARIO PROPUESTO .....	11
Escenario.....	13
Recursos necesarios .....	13
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces .....	14
Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	20
Parte 3: Configurar los protocolos de enrutamiento .....	27
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy) .....	34
Parte 5: Seguridad .....	41
Paso 6 Configure las funciones de Administración de Red.....	47
CONCLUSIONES.....	53
BIBLIOGRAFÍA.....	54

## LISTA DE TABLAS

Tabla 1 Direccionamiento IP .....	12
Tabla 2 Tareas a realizar paso 2 .....	21
Tabla 3 Tareas a realizar paso 3 .....	28
Tabla 4 Tareas a realizar paso 4 .....	37
Tabla 5 Tareas a realizar paso 5 .....	42
Tabla 6 Tareas a realizar paso 6 .....	48

## LISTA DE FIGURAS

Ilustración 1 Escenario propuesto .....	11
Ilustración 2 Prueba DHCP PC2.....	23
Ilustración 3 Prueba DHCP PC3.....	23
Ilustración 4 Prueba Ping PC1 .....	24
Ilustración 5 Prueba ping PC2 .....	25
Ilustración 6 Prueba Ping PC3.....	26
Ilustración 7 Prueba ping PC4 .....	27
Ilustración 8 Validación AAA en R1 .....	46
Ilustración 9 Validación AAA en R3.....	46
Ilustración 10 Validación AAA en D1.....	47
Ilustración 11 Validación AAA en D1.....	47

## GLOSARIO

**HSRP:** Hot Standby Router Protocol hace referencia a los protocolos de redundancia de primer salto, es un protocolo propietario de Cisco para permitir que varios routers o switches multicapa aparezcan como una única puerta de salida funcionando como gateway, Si se configuran grupos de HSRP en diferentes interfaces VLAN, suele ser útil hacer coincidir el número de grupo con el de VLAN.

**PROTOCOLO ENRUTAMIENTO:** Realizan el direccionamiento entre routers con el fin de establecer comunicación e intercambio de información de manera dinámica sobre las rutas que pueden alcanzar de acuerdo al número de saltos o routers para encontrar la ruta más corta, facilitando el proceso de enrutamiento enviando entre los routers periódicamente información del estado de las rutas.

**ROUTER:** Es un dispositivo de hardware para interconexión de red de datos que opera en la capa tres del nivel del red OSI, para la interconexión de redes informática que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

**TOPOLOGÍA DE RED:** Son las diferentes distribuciones de los dispositivos, tales como routers, computadoras, entre otros dispositivos que se conecten a la red, y las distintas conexiones que pueden haber en la red. Se pueden ilustrar gráficamente, cuando se refiere a una topología física refieren al diseño físico o lógico de una red de datos. Definiendo la forma en que se colocan los diferentes nodos y cómo se interconectan entre sí de igual manera, pueden describir cómo se transfieren los datos entre estos nodos.

**VLANs:** Redes de área local virtuales permite crear redes lógicas independientes dentro de la misma red física, su objetivo en redes domésticas o profesionales, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo de capa tres como lo son los Routers o switches multicapa.

## RESUMEN

Este trabajo consta de un escenario para la práctica de conocimientos adquiridos en el diplomado de profundización CISCO CCNP, ilustra mediante la realización de un laboratorio práctico con realizado en el ambiente virtual de simulación de redes de datos GNS3, se realiza las configuraciones propuestas en el escenario 1, permitiendo obtener el enrutamiento y conmutación entre los dispositivos como routers y switches de L3 que intervienen en las diferentes redes, permitiendo evaluar el nivel de conocimiento desarrollado, las habilidades, comprensión y solución de configuraciones a nivel de Networking que se emplean en los ambientes académicos y profesionales de la electrónica y las telecomunicaciones. Se explicara de manera detallada la solución del escenario propuesto, los códigos con los que se configuraron cada equipo en la red y el procedimiento de solución de enrutamiento de redes y segmentos, se usan para el escenario diferentes protocolos de enrutamiento entre ellos OSPF y MP-BGP, se realiza las configuraciones de redundancia de primer salto mediante HRSP versión 2, la configuración a nivel de seguridad y las funciones de administración de la red realizando las pruebas a las configuraciones de los routers y switches evidenciando mediante pruebas de conectividad ping, traceroute, show ip route, entre otros .

Palabras Clave en el RESUMEN: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.



## ABSTRACT

This work consists of a scenario for the practice of knowledge acquired in the CISCO CCNP deepening diploma, illustrated by conducting a practical laboratory with the virtual environment of simulation of GNS3 data networks, the configurations proposed in the scenario are carried out 1, allowing to obtain the routing and switching between the devices such as routers and L3 switches that intervene in the different networks, allowing to evaluate the level of knowledge developed, the skills, understanding and solution of Networking-level configurations that are used in the environments academics and professionals in electronics and telecommunications. The solution of the proposed scenario will be explained in detail, the codes with which each equipment in the network was configured and the procedure for the routing solution of networks and segments, different routing protocols are used for the scenario, including OSPF and MP-BGP, the first-hop redundancy configurations are carried out using HSRP version 2, the configuration at the security level and the network administration functions by testing the configurations of the routers and switches, evidencing through connectivity tests ping, traceroute, show ip route, among others.

Palabras Clave en el ABSTRACT: CISCO, CCNP, Routing, Switching, Networking, Electronics.

## INTRODUCCION

Las redes de datos y la ingeniería en telecomunicaciones contribuyen al desarrollo tecnológico del mundo otorgando un valor significativo al interconectar personas y objetos desde un nivel local hasta global, es por esto que aplicar conocimiento sobre Networking es fundamental para poder otorgar el engranaje que estas actividades requieren, configuraciones de equipos activos como enrutadores, switches, permiten que dispositivos finales de usuarios se conecten de la manera más sencilla a la red, esto es posible implementando una correcta administración de las redes de datos, mediante segmentación de subredes tanto físicas o virtuales las que mencionaremos como VLANS, administración de políticas de seguridad, configuraciones de protocolos de enrutamiento dinámicos, desarrollaremos en el contenido de este documento.

El presente trabajo se desarrollara con base al escenario propuesto en el cual la red de una compañía "red privada", se conectara a la Nube mediante la conexión de un router del ISP, dentro de la red de la compañía se encuentran dos switches de capa 3, los cuales admiten las configuraciones que permiten la segmentación de las redes en redes virtuales, se encuentran dos router R1 y R3 los cuales administraran el enrutamiento de paquetes haciendo uso del protocolo de enrutamiento dinámico de estado de enlace OSPF el cual es por hoy uno de los protocolos que más se utiliza dentro de las organizaciones a nivel empresarial institucional y gubernamental, implementado en redes medianas y de gran tamaño.

El protocolo OSPF mediante su arquitectura jerárquica facilita la escalabilidad, seguridad y administración de rutas, teniendo como gran fortaleza la métrica que usa, basada en la velocidad de los enlaces, y también cuenta con otras funciones que permite una óptima administración en el desempeño de la red, adicional además de las configuraciones básicas de los equipos de la red para su enrutamiento se realiza la configuración de Ethernet channel, entre los switches, configuración de interfaces troncales, habilitando el protocolo RSPT, configuramos la redundancia de primer salto haciendo uso de HSRP versión 2 en los switches L3, se protegen todos los dispositivos bajo administraciones de políticas de seguridad, al final se realizan pruebas de conectividad entre los diferentes actores de la topología para probar el funcionamiento del mismo.

## DESARROLLO ESCENARIO PROPUESTO

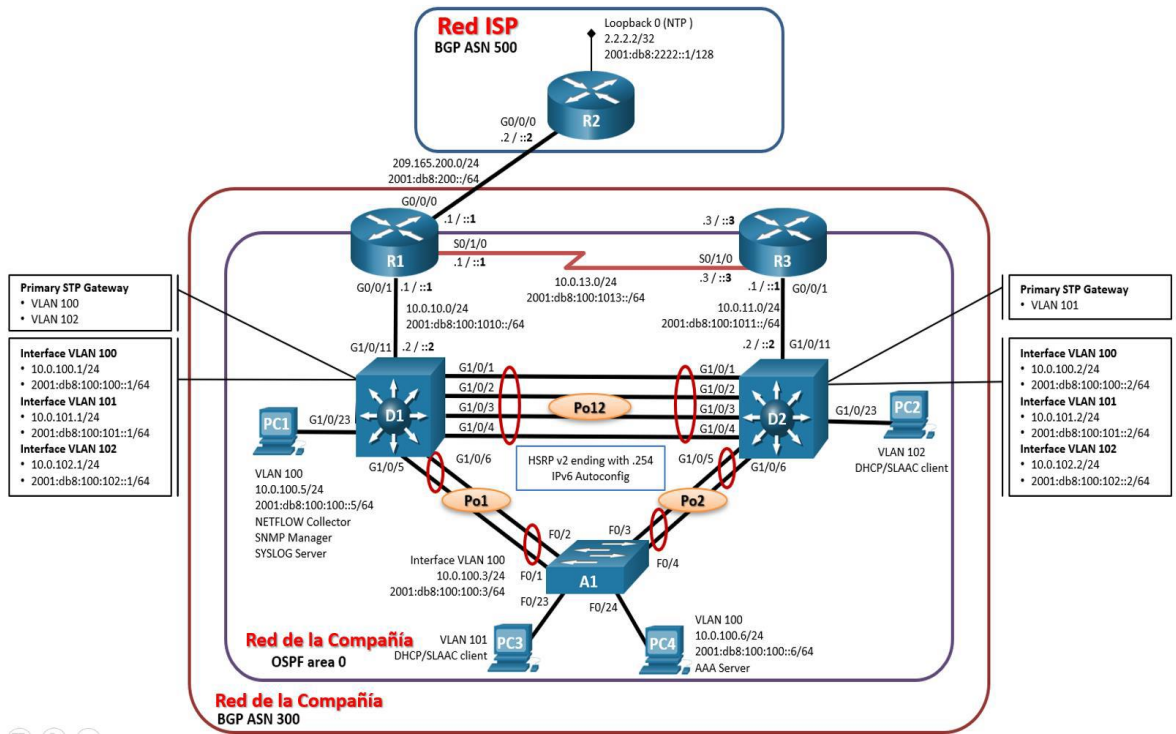


Ilustración 1 Escenario propuesto

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	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::1/28	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

Tabla 1 Direccionamiento IP

## Objetivos

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

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

**Parte 3:** Configurar los protocolos de enrutamiento

**Parte 4:** Configurar la redundancia del primer salto

**Parte 5:** Configurar la seguridad

**Parte 6:** Configurar las características de administración de red

### **Escenario**

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

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

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

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

### **Recursos necesarios**

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

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

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

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

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

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:

**Nota 1:** Para cada comando se comenta la acción que realiza en la configuración del router.

**Nota 2:** Las líneas de comandos recurrentes solo se comentan una sola vez.

**Nota 3:** No se comentan los comandos para **Router 2 y Router 3** que ya se describieron en **Router 1**

### Router R1

```
hostname R1 /Nombre del router
ipv6 unicast-routing /Enrutamiento IPV6
no ip domain lookup /Dominio IP
banner motd # R1, ENCOR Skills Assessment, Scenario 1 # /Mensaje en banner
motd
line con 0 /Configuración línea de consola
exec-timeout 0 0 /Tiempo de desconexión de consola
logging synchronous /Activamos acceso Sincrónico
exit /Salir de la configuración
interface g0/0/0 /Acceso a interface Giga Ethernet 0/0/0
ip address 209.165.200.225 255.255.255.224 /Configuración dirección IPV4
ipv6 address fe80::1:1 link-local /Configuración dirección link local
ipv6 address 2001:db8:200::1/64 /Configuración dirección IPV6
no shutdown /Activar Interface g0/0/0
exit
interface g0/0/1 /Acceso a interface g0/0/1
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 s0/1/0 /Acceso a interface Serial 0/1/0
ip address 10.0.13.1 255.255.255.0
```

```
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64
no shutdown
exit
```

### **Router R2**

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

### **Router R3**

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/1
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 s0/1/0
```

```
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

## Switch D1

```
hostname D1 /Nombre del switch
ip routing /Enrutamiento IPV4
ipv6 unicast-routing /Enrutamiento IPV6
no ip domain lookup /Dominio IP
banner motd # D1, ENCOR Skills Assessment, Scenario 1 # /Mensaje en Banner
Motd
line con 0 /Configuración consola
exec-timeout 0 0 /Tiempo desconexión consola
logging synchronous /Sincronismo en el acceso
exit /Salir de configuración
vlan 100 /Configuración VLAN 100
name Management /Asignar nombre a la VLAN 100
exit /Salir de configuración VLAN
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11 /Acceso interfaz g1/0/11
no switchport /Troncalización de VLANs
ip address 10.0.10.2 255.255.255.0 /Dirección ip de interface G1/0/11
ipv6 address fe80::d1:1 link-local /Configuración dirección link local
ipv6 address 2001:db8:100:1010::2/64 /Configuración IPV6I
no shutdown /Activar interface
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 /Exclusión de las direcciones de la VLAN 101
ip dhcp excluded-address 10.0.101.141 10.0.101.254 /Exclusión de las direcciones de la VLAN 101
ip dhcp excluded-address 10.0.102.1 10.0.102.109 /Exclusión de las direcciones de la VLAN 102
ip dhcp excluded-address 10.0.102.141 10.0.102.254 /Exclusión de las direcciones de la VLAN 102
ip dhcp pool VLAN-101 /Configuración de pool de direcciones VLAN 101
network 10.0.101.0 255.255.255.0 /Configuración de rango de direcciones de host
default-router 10.0.101.254 /Configuración de Gateway para VLAN101
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4 /Desactiva interfaces que no se utilizarán
shutdown
exit

```

## Switch D2

```

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

```

```
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11
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
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

### Switch A1

```
hostname A1 /Nombre del Switch A1
no ip domain lookup /Dominio IP
banner motd # A1, ENCOR Skills Assessment, Scenario 1 # /Mensaje en banner
Motd
line con 0 /Configuración consola
exec-timeout 0 0 /Tiempo desconexión consola
logging synchronous /acceso a sincronismo
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
interface range f0/5-22
shutdown
exit
```

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

Para cada uno de los dispositivos ingresamos al modo de configuración global, utilizamos el comando

```
R1#copy running-config startup-config / Graba el archivo de configuración actual
```

c. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

**Nota:**

Se utiliza el mismo comando de configuración de IP para PC1 y PC4, salvo que cambia la el direccionamiento IP

PC1> ip 10.0.100.5 255.255.255.0 10.0.100.254 / *Direccionamiento IPV4*

PC1> ip 2001:db8:100:100::5/64 /*Direccionamiento IPV6*

PC1 > save /*Guarda la configuración IP*

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

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

Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: <ul style="list-style-type: none"> <li>• D1 and D2</li> <li>• D1 and A1</li> <li>• D2 and A1</li> </ul>
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none"> <li>• D1 a D2 – Port channel 12</li> <li>• D1 a A1 – Port channel 1</li> <li>• D2 a A1 – Port channel 2</li> </ul>

2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6  PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2  PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2  PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

**Tabla 2 Tareas a realizar paso 2**

**Configuración tarea 2.1** En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches

**Nota:** Los comando realizados para D1, se replican en D2 y A1, teniendo presente la asignación de interfaces correspondientes

```
D1#configure terminal           /Configuración terminal
D1(config)# interface range e0/0-3, e1/0-1   /Interfaces troncales
D1(config-if-range)#switchport trunk encapsulation dot1q /Encapsulación dot1q
en el puerto
D1(config-if-range)#switchport mode trunk    /Activación puerto en modo troncal
D1(config-if-range)#no shutdown             /Activación puerto
```

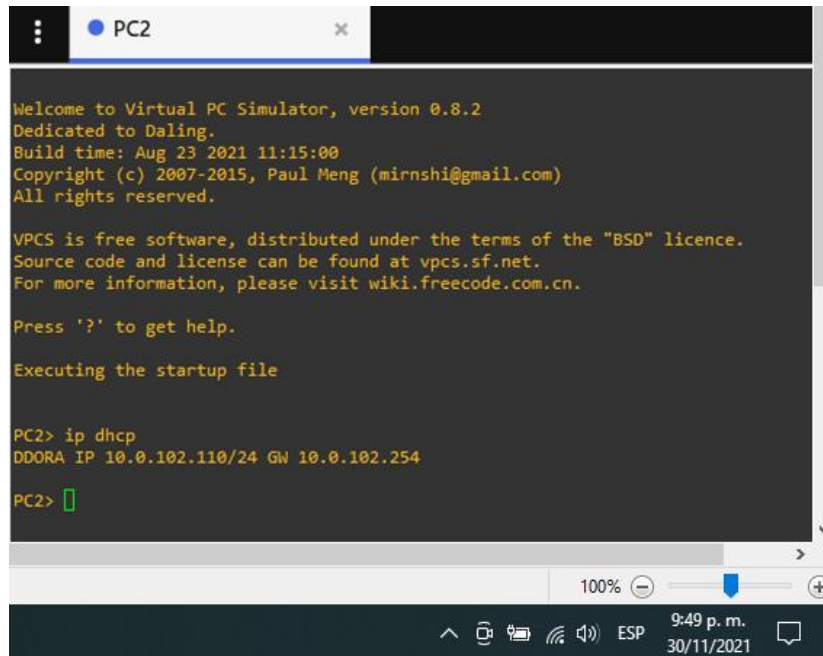
## Configuración tarea 2.2

```
D1(config-if-range)#switchport trunk native vlan 999 /Configuración de VLAN nativa
D1(config-if-range)#exit
```

## Configuración tarea 2.3 a 2.6

```
D1(config)#spanning-tree mode rapid-pvst /Activación de Rapid Spanning Tree en el switch
D1(config)#spanning-tree vlan 100,102 root primary /Configuración puente raíz
D1(config)#spanning-tree vlan 101 root secondary /Configuración puente respaldo
D1(config)#interface range e0/0-3 /Se seleccionan las interfaces
D1(config-if-range)#channel-group 12 mode active /configuración de canal y grupo
D1(config-if-range)#exit
D1(config)#interface range e1/0-1
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#exit
D1(config)#interface e2/1
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100 /Asignación VLAN al puerto
D1(config-if)#spanning-tree portfast /Activación portfast
D1(config-if)#no shutdown
D1(config-if)#exit
```

## Validación tarea 2.7



```
PC2
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

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

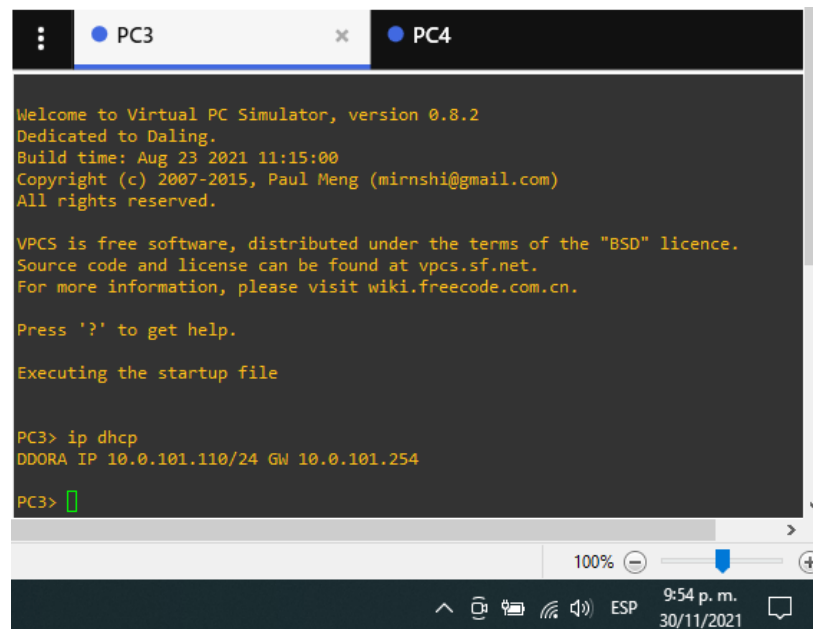
Press '?' to get help.

Executing the startup file

PC2> ip dhcp
DDORA IP 10.0.102.110/24 GW 10.0.102.254

PC2> 
```

Ilustración 2 Prueba DHCP PC2



```
PC3
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

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

Press '?' to get help.

Executing the startup file

PC3> ip dhcp
DDORA IP 10.0.101.110/24 GW 10.0.101.254

PC3> 
```

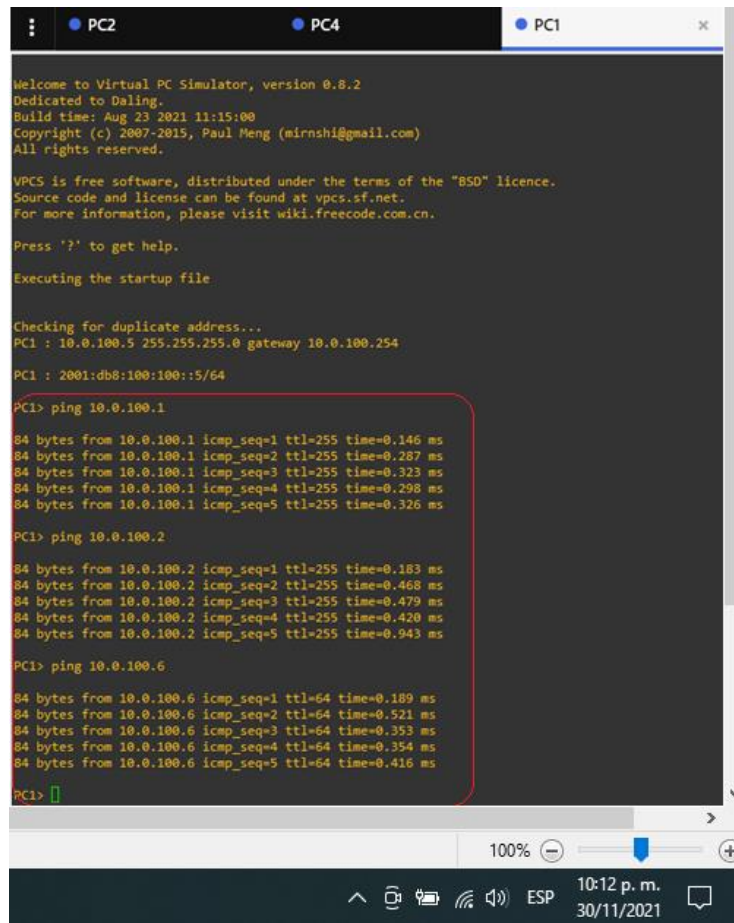
Ilustración 3 Prueba DHCP PC3

## Configuración Tarea 2.8

Pruebas de conectividad de la LAN local

PC1 debería hacer ping con éxito a:

D1: 10.0.100.1, D2: 10.0.100.2 y PC4: 10.0.100.6



```
PC2 PC4 PC1
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

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

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
PC1 : 2001:db8:100:100::5/64

PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.146 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.287 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.323 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.298 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.326 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.183 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.468 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.479 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.420 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.943 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=0.189 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=0.521 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=0.353 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=0.354 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=0.416 ms

PC1> █
```

Ilustración 4 Prueba Ping PC1

PC2 debería hacer ping con éxito a:

D1: 10.0.102.1

D2: 10.0.102.2



```
PC2 PC4 PC1 PC3
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "B50" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip dhcp
000RA IP 10.0.102.110/24 GW 10.0.102.254

PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=0.221 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=0.497 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=0.562 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=0.546 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=0.735 ms

PC2> ping 10.0.100.2

84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.183 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.468 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.479 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.420 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.943 ms
```

Ilustración 5 Prueba ping PC2

**PC3 debería hacer ping con éxito a:**

D1: 10.0.101.1

D2: 10.0.101.2

The image shows a terminal window from a virtual PC simulator. The window title bar includes tabs for PC3, PC4, and PC1. The terminal text is as follows:

```
welcome to Virtual PC Simulator, version 0.8.2
dedicated to Dalling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

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

Press '?' to get help.

Executing the startup file.

PC3> ip dhcp
DHCPA IP 10.0.101.110/24 GW 10.0.101.254

PC3> ping 10.0.101.1
64 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.324 ms
64 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.531 ms
64 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=0.621 ms
64 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=0.431 ms
64 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.832 ms

PC3> ping 10.0.101.2
64 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.439 ms
64 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.442 ms
64 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=0.444 ms
64 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=0.454 ms
64 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.574 ms
```

The terminal window also shows a system tray at the bottom right with the time 10:25 p.m. and date 30/11/2021.

Ilustración 6 Prueba Ping PC3

**PC4 debería hacer ping con éxito a:**

D1: 10.0.100.1

D2: 10.0.100.2

PC1: 10.0.100.5

```
Welcome to Virtual PC Simulator, version 0.8.2.
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BS0" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC1 : 2001:db8:100:100::6/64

PC4> ping 10.0.100.1

64 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=0.197 ms
64 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=0.372 ms
64 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=0.346 ms
64 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=0.413 ms
64 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=0.648 ms

PC4> ping 10.0.100.2

64 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=0.243 ms
64 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=0.606 ms
64 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=0.585 ms
64 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=0.476 ms
64 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=0.571 ms

PC4> ping 10.0.100.5

64 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=0.424 ms
64 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=0.300 ms
64 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=0.470 ms
64 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=0.390 ms
64 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=0.372 ms
```

Ilustración 7 Prueba ping PC4

### Parte 3: Configurar los protocolos de enrutamiento

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

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

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>

**Tabla 3 Tareas a realizar paso 3**

**Configuración Tarea 3.1 y 3.2** En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0. En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.

**Nota 1:** Los comando que ya se mencionan en configuraciones anteriores, no se describen en esta configuración.

Las configuraciones para R1 son:

```
R1#configure terminal
R1(config)#router ospf 4           //Se configura protocolo OSPF y process ID 4
R1(config-router)#router-id 0.0.4.1 //Se establece identificador para R1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 //Se configura la red
en área 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate //Ruta predeterminada OSPF
R1(config-router)#exit
R1(config)#
R1(config)#ipv6 router ospf 6 //Configuración de IPV6 en OSPF V3 R1
R1(config-rtr)#router-id 0.0.6.1 //Se establece identificador para R1
R1(config-rtr)#default-information originate //Ruta predeterminada OSPF V3
R1(config-rtr)#exit
R1(config)#interface gi2/0
R1(config-if)#ipv6 ospf 6 area 0 //Se habilita OSPV v3, y se configura área 0
R1(config-if)#exit
R1(config)#interface se1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0 //Ruta predeterminada a interface
salida OSPV V2
R1(config)#ipv6 route 2001:db8:100::/48 null0 //Ruta predeterminada a interface
salida OSPV V3
R1(config)#router bgp 300 //Se configura y activa BGP
R1(config-router)# bgp router-id 1.1.1.1 //Identificador BGP
R1(config-router)# neighbor 209.165.200.226 remote-as 500 //relación con
R2 en ASN 500
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500Se //relación con R2
en ASN 500
R1(config-router)# address-family ipv4 unicast //Configuración Unicast
R1(config-router-af)# neighbor 209.165.200.226 activate //relación con el vecino
activa
R1(config-router-af)# no neighbor 2001:db8:200::2 activate
```

```

R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)# exit-address-family
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)# no neighbor 209.165.200.226 activate //desactivación
relación con el vecino
R1(config-router-af)# neighbor 2001:db8:200::2
R1(config-router-af)# network 2001:db8:100::/48 //configuración IPV6
R1(config-router-af)# exit-address-family
R1(config-router)#exit
R1(config)# exit
R1#copy-running-config startup-config

```

### Configuración Tarea 3.3

#### Las configuraciones para R2 son:

```

R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 //ruta predeterminada con interfaz
de salida loopback
R2(config)#ipv6 route ::/0 loopback 0 //ruta IPv6 predeterminada con
interfaz de salida loopback
R2(config)#router bgp 500 // BGP 500
R2(config-router)# bgp router-id 2.2.2.2 //Identificador BGP
R2(config-router)# neighbor 209.165.200.225 remote-as 300 //relación con
R1 en ASN 300
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300 //relación con R2 en
ASN 500
R2(config-router)# address-family ipv4
R2(config-router-af)# neighbor 209.165.200.225 activate // relación con el
vecino activa
R2(config-router-af)# no neighbor 2001:db8:200::1 activate //Se excluye la
dirección IPv6
R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255 // relación con la
interface loopback de R2
R2(config-router-af)# network 0.0.0.0 // Redes predeterminadas
R2(config-router-af)# exit-address-family
R2(config-router)# address-family ipv6
R2(config-router-af)# no neighbor 209.165.200.225 activate //relación con el
vecino activa
R2(config-router-af)# neighbor 2001:db8:200::1 activate // Se incluye la
dirección IPv6
R2(config-router-af)# network 2001:db8:2222::/128 // Se excluye la dirección
IPv6
R2(config-router-af)# network ::/0 //Redes predeterminadas

```

```
R2(config-router-af)# exit-address-family
R2(config-router)#
R2#copy-running-config startup-config
```

### Las configuraciones para R3 son:

```
R3#configure terminal
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)#exit
R3(config)#
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface gi2/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#interface se1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3#copy-running-config startup-config
```

### Configuración Tarea 3.4

```
R1#configure terminal
R1(config)#router ospf 4 //Se configura protocolo OSPF y process ID 4
R1(config-router)#router-id 0.0.4.1 //Se establece identificador para R1
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 //Se configura la red
en área 0
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate //Ruta predeterminada OSPF
R1(config-router)#exit
R1(config)#
R1(config)#ipv6 router ospf 6 //Configuración de IPV6 en OSPF V3 R1
R1(config-rtr)#router-id 0.0.6.1 //Se establece identificador para R1
R1(config-rtr)#default-information originate //Ruta predeterminada OSPF V3
R1(config-rtr)#exit
R1(config)#interface gi2/0
R1(config-if)#ipv6 ospf 6 area 0 //Se habilita OSPF v3, y se configura área 0
R1(config-if)#exit
```

```

R1(config)#interface se1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#ip route 10.0.0.0 255.0.0.0 null0 //Ruta predeterminada a interface
salida OSPV V2
R1(config)#ipv6 route 2001:db8:100::/48 null0 //Ruta predeterminada a interface
salida OSPV V3
R1(config)#router bgp 300 //Se configura y activa BGP
R1(config-router)# bgp router-id 1.1.1.1 //Identificador BGP
R1(config-router)# neighbor 209.165.200.226 remote-as 500 //relación con
R2 en ASN 500
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500 Se //relación
con R2 en ASN 500
R1(config-router)# address-family ipv4 unicast //Configuración Unicast
R1(config-router-af)# neighbor 209.165.200.226 activate //relación con el vecino
activa
R1(config-router-af)# no neighbor 2001:db8:200::2 activate
R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)# exit-address-family
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)# no neighbor 209.165.200.226 activate //desactivación
relación con el vecino
R1(config-router-af)# neighbor 2001:db8:200::2
R1(config-router-af)# network 2001:db8:100::/48 //configuración IPV6
R1(config-router-af)# exit-address-family
R1(config-router)#exit
R1(config)# exit
R1#copy-runing-config startup-config

```

## Las configuraciones para D1 son:

### Switch D1

```

D1#configure terminal
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#passive-interface default //interfaces como pasivas
D1(config-router)#no passive-interface e2/0 //Excluye la interfaz pasiva
D1(config-router)#exit

```



```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface e2/0
D1(config-rtr)#exit
D1(config)#interface e2/0
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#
D1#copy-running-config startup-config
```

### **Las configuraciones para D2 son:**

```
D2#configure terminal
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface e2/0
D2(config-router)#exit
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 e2/0
D2(config-rtr)#exit
D2(config)#interface e2/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 101
```

```

D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config)#
D21#copy-running-config startup-config

```

#### 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:

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. 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.</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. 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.</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 version 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> <ul style="list-style-type: none"> <li>• Configure IPv4 HSRP grupo <b>124</b> para la VLAN 102:</li> </ul> <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 150.</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 150.</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> <li>• Rastree el objeto 6 y decremente en 60.</li> </ul>
-----	-------------------------	---

	<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. Configure HSRP version 2.  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 150.</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 150.</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> <li>• Rastree el objeto 6 para disminuir en 60.</li> </ul>
--	---------------------------------	---

Tabla 4 Tareas a realizar paso 4

## Configuraciones para D1 parte 4.1

```
D1#configure terminal
D1(config)#ip sla 4 //Configuración de SLA
D1(config-ip-sla)#icmp-echo 10.0.10.1 //Interfaz para el SLA4
D1(config-ip-sla-echo)#frequency 5 //Se configura la frecuencia
D1(config-ip-sla-echo)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 D1(config-ip-sla-
echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now //Se activa la
operación SLA 4
D1(config)#ip sla schedule 6 life forever start-time now //Se activa la
operación SLA 6
D1(config)#track 4 ip sla 4 //Configuración de verificador de estado IP SLA 4
D1(config-track)#delay down 10 up 15 //Cambia de estado Dw-Up >10s o
Up-Dw >15s
D1(config-track)#exit
D1(config)#track 6 ip sla 6 //Configuración de verificador de estado IP SLA 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#
D1(config)#interface vlan 100 //Ingreso interfaz VLAN100
D1(config-if)#standby version 2 //Se habilita HSRPv2
D1(config-if)#standby 104 ip 10.0.100.254 //Se asigna IPV4 a grupo
D1(config-if)#standby 104 priority 150 //prioridad del grupo en 150
D1(config-if)#standby 104 preempt //Se habilita la preferencia
D1(config-if)#standby 104 track 4 decrement 60 //Rastre de objeto y
decrementa en 60
D1(config-if)#standby 106 ipv6 autoconfig //Asignación IP virtual para el
respectivo grupo
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
```

```
D1(config)#interface vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 priority 150
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 6 decrement 60
D1(config-if)#exit
```

## **Configuraciones para D2 parte 4.2**

```
D2#configure terminal
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now
D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#track 6 ip sla 6
D2(config-track)#delay down 10 up 15
D2(config-track)#exit
D2(config)#
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60
D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
D2(config-if)# standby 106 track 6 decrement 60
D2(config-if)# exit
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)# 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)# standby 116 track 6 decrement 60
D2(config-if)# exit
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)# standby 124 track 4 decrement 60
D2(config-if)# standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60
D2(config-if)# exit

```

### Configuración Tarea 4.3

```

D1(config)#
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)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 6 decrement 60
D1(config-if)#exit
D1(config)#interface vlan 102
D1(config-if)#standby version 2

```

*//Ingreso interfaz VLAN100*

*//Se habilita HSRPv2*

*//Se asigna IPV4 a grupo*

*//prioridad del grupo en 150*

*//Se habilita la preferencia*

*//Rastre de objeto y decrementa en 60*

*//Asignación IP virtual para el respectivo grupo*



```

D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 priority 150
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 6 decrement 60
D1(config-if)#exit

```

### Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología.

Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: <b>cisco12345cisco</b>
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: <b>sadmin</b> • Nivel de privilegio 15 • Contraseña: <b>cisco12345cisco</b>
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.

5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <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> .

Tabla 5 Tareas a realizar paso 5

### Configuración tarea 5.1

#### Para Router R1

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco //Se activa algoritmo SCRYPT en EXEC

#### Para Router R2

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

#### Para Router R3

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

### **Para Switch D1**

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

### **Para Switch D2**

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

### **Para Switch A1**

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

## **Configuración tarea 5.2**

### **Para Router R1**

```
R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret  
cisco12345cisco //Se crea usuario local y credencial del usuario
```

### **Para Router R2**

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

### **Para Router R3**

```
R3(config)#username sadmin privilege 15 algorithm-type SCRYPT secret  
cisco12345cisco
```

### **Para Switch D1**

```
D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret  
cisco12345cisco
```

### **Para Switch D2**

```
D2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret  
cisco12345cisco
```

### **Para Switch A1**

```
A1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret  
cisco12345cisco
```

### **Configuración tarea 5.3**

#### **Para Router R1**

```
R1(config)#aaa new-model //Se habilita AAA
```

#### **Para Router R3**

```
R3(config)#aaa new-model
```

#### **Para Switch D1**

```
D1(config)#aaa new-model
```

#### **Para Switch D2**

```
D2(config)#aaa new-model
```

#### **Para Switch A1**

```
A1(config)#aaa new-model
```

### **Configuración tarea 5.4**

#### **Para Router R1**

```
R1(config)#radius server RADIUS //Servidor radius
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
//Dirección RADIUS y puertos lógicos
R1(config-radius-server)#key $strongPass //Contraseña de RADIUS
R1(config-radius-server)#exit
```

#### **Para Router R3**

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

#### **Para Switch D1**

```
D1(config)#radius server RADIUS
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)#key $strongPass
D1(config-radius-server)#exit
```

### Para Switch D2

```
D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 18
13
D2(config-radius-server)#key $strongPass
D2(config-radius-server)#exit
```

### Para Switch A1

```
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 $strongPass
A1(config-radius-server)# exit
```

## Configuración tarea 5.5

### Para Router R1

```
R1(config)#aaa authentication login default group radius local //Listas
autenticación AAA
```

### Para Router R3

```
R3(config)#aaa authentication login default group radius local
```

### Para Switch D1

```
D1(config)#aaa authentication login default group radius local
```

### Para Switch D2

```
D2(config)#aaa authentication login default group radius local
```

### Para Switch A1

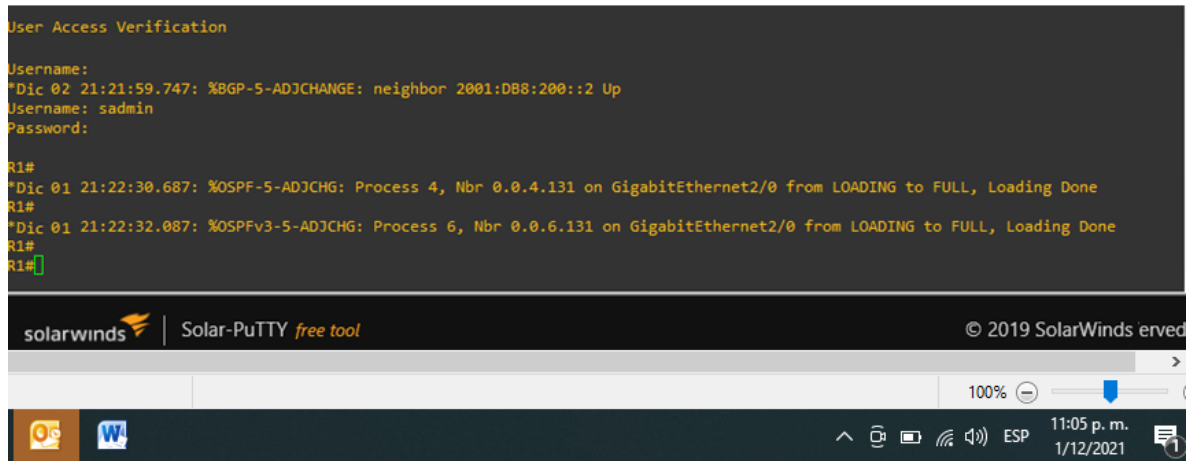
```
A1(config)#aaa authentication login default group radius local
```

## Configuración tarea 5.6

## Configuraciones parte 5.6 Validación de AAA

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

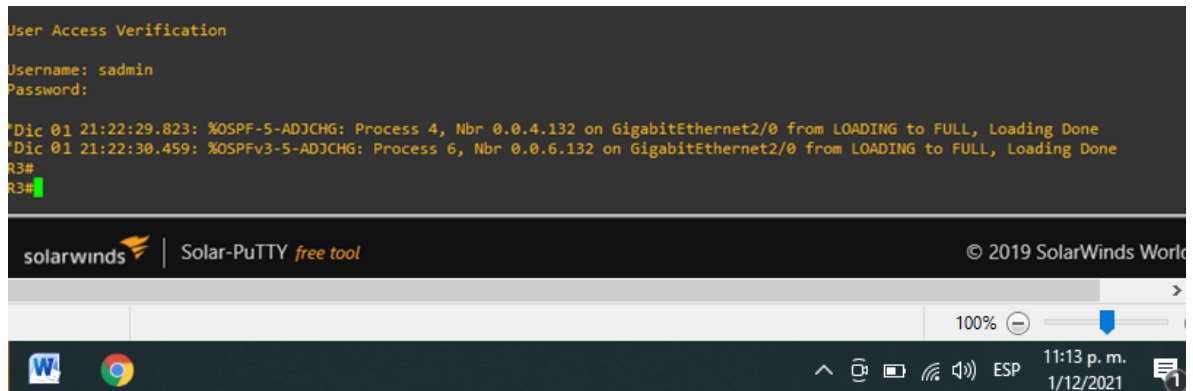
### Para Router R1



```
User Access Verification
Username:
*Dic 02 21:21:59.747: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::2 Up
Username: sadmin
Password:
R1#
*Dic 01 21:22:30.687: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.131 on GigabitEthernet2/0 from LOADING to FULL, Loading Done
R1#
*Dic 01 21:22:32.087: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.131 on GigabitEthernet2/0 from LOADING to FULL, Loading Done
R1#
R1#
```

Ilustración 8 Validación AAA en R1

### Para Router R3



```
User Access Verification
Username: sadmin
Password:
*Dic 01 21:22:29.823: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.132 on GigabitEthernet2/0 from LOADING to FULL, Loading Done
*Dic 01 21:22:30.459: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.132 on GigabitEthernet2/0 from LOADING to FULL, Loading Done
R3#
R3#
```

Ilustración 9 Validación AAA en R3

## Para Switch D1

```
User Access Verification
Username:
*Dic 01 21:22:40.927: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet2/0 from LOADING to FULL, Loading Done
Username: ci
*Dic 01 21:22:42.324: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Ethernet2/0 from LOADING to FULL, Loading Done
Username: sadmin
Password:
D1#
```

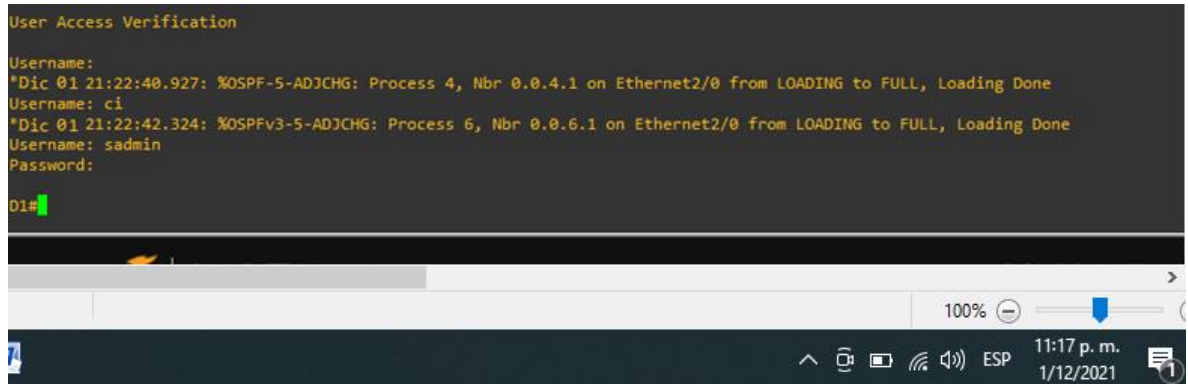


Ilustración 10 Validación AAA en D1

## Para Switch D2

```
User Access Verification
Username:
*Dic 01 21:22:40.927: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet2/0 from LOADING to FULL, Loading Done
Username: ci
*Dic 01 21:22:42.324: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Ethernet2/0 from LOADING to FULL, Loading Done
Username: sadmin
Password:
D2#
```

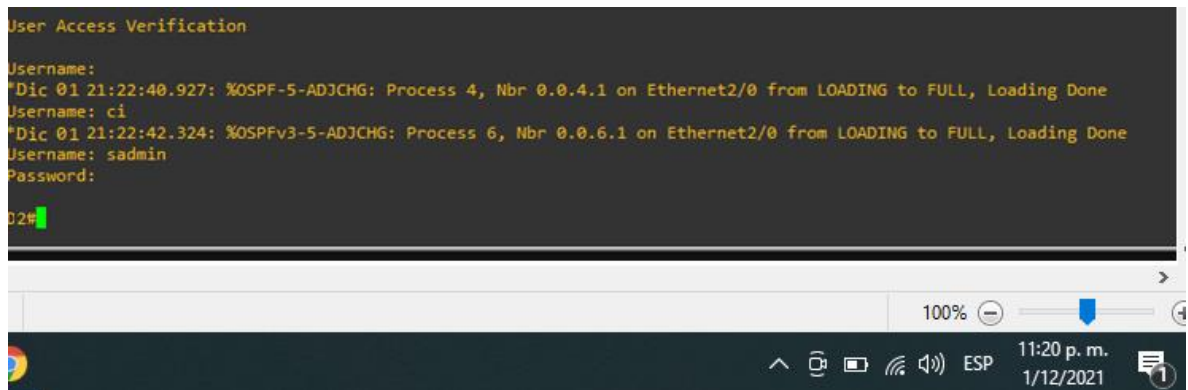


Ilustración 11 Validación AAA en D1

## Paso 6 Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel 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>

Tabla 6 Tareas a realizar paso 6

### Configuración tarea 6.1

#### Para Router 1

R1(config)#clock timezone utc -5 //Reloj actual de acuerdo a UTC

#### Para Router 2



R2(config)#clock timezone utc -5

**Para Router 3**

R3(config)#clock timezone utc -5

**Para Switch D1**

D1(config)#clock timezone utc -5

**Para Switch D2**

D2(config)#clock timezone utc -5

**Para Switch A1**

A1(config)#clock timezone utc -5

**Configuración tarea 6.2**

**Para Router R2**

R2(config)#ntp master 3                    *//Se configura R2 como maestro NTP*

**Configuración tarea 6.3**

**Para Router R1**

R1(config)#ntp server 2.2.2.2            *//Sincronizar NTP server*

**Para Router R3**

R3(config)#ntp server 10.0.10.1

**Para Switch D1**

D1(config)#ntp server 10.0.10.1

**Para Switch D2**

D2(config)#ntp server 10.0.10.1

**Para Switch A1**

A1(config)#ntp server 10.0.10.1        *//Se sincroniza NTP*

## Configuración tarea 6.4

### Para Router R1

```
R1(config)#logging trap warning //Se configura Syslog
R1(config)#logging host 10.0.100.5 //Envío a PC1 de eventos Syslog
R1(config)#logging on //Se habilita la funcionalidad de syslog
```

### Para Router R3

```
R3(config)#logging trap warning
R3(config)#logging host 10.0.100.5
R3(config)#logging on
```

### Para Switch D1

```
D1(config)#logging trap warning // Syslog de peligro
D1(config)#logging host 10.0.100.5
D1(config)#logging on
```

### Para Switch D2

```
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
```

### Para Switch A1

```
A1(config)#logging trap warning
A1(config)#logging host 10.0.100.5
A1(config)#logging on
```

## Configuración tarea 6.5

### Para Router R1

```
R1(config)#ip access-list standard SNMP //Configuración de lista de acceso
estandar
R1(config-std-nacl)#permit host 10.0.100.5 //SNMP a la dirección del PC1
R1(config-std-nacl)#exit
R1(config)#snmp-server contact Fredy_Marquez //Se configura contacto
R1(config)#snmp-server community ENCORSA ro SNMP /Se configura
comunidad y acceso de solo lectura
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA /Dirección de
envío traps
R1(config)# snmp-server ifindex persist //Se activa preexistencia
```

```
R1(config)# snmp-server enable traps bgp //Envío de traps BGP
R1(config)# snmp-server enable traps config //Envío de traps config
R1(config)# snmp-server enable traps ospf //Envío de traps OSPF
```

### **Para Router R3**

```
R3(config)#ip access-list standard SNMP
R3(config-std-nacl)#permit host 10.0.100.5
R3(config-std-nacl)#exit
R3(config)# snmp-server contact Fredy_Marquez
R3(config)#snmp-server community ENCORSA ro SNMP
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)#
```

### **Para Switch D1**

```
D1(config)#ip access-list standard SNMP
D1(config-std-nacl)#permit host 10.0.100.5
D1(config-std-nacl)#exit
D1(config)# snmp-server contact Fredy_Marquez
D1(config)#snmp-server community ENCORSA ro SNMP
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps config
D1(config)# snmp-server enable traps ospf
```

### **Para Switch D2**

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

### **Para Switch A1**

```
A1(config)#ip access-list standard SNMP
A1(config-std-nacl)#permit host 10.0.100.5
A1(config-std-nacl)# exit
```

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

## CONCLUSIONES

Con el desarrollo del taller propuesto en el escenario 1 en la primeros tres pasos se realizan las configuraciones básicas de los routers y switches de capa 3, en donde la segmentación de redes mediante el uso de redes virtuales VLAN permite tener una administración acorde a los escenarios reales que se puedan desempeñar en el campo de la ingeniería en telecomunicaciones, adicional se tiene clientes DHCP y SLAAC, se realiza con los protocolos de direccionamiento IPV4 e IPV6, y como protocolo interno de la compañía se tiene OSPF que permite enrutar hacia la red ISP a la interfaz Loopback en mediante R2, se presenta inconvenientes con el software de simulación de Packet tracer al no aceptar la compatibilidad con algunos comandos en la configuración de los switches es por esto que se realiza de nuevo la simulación utilizando el software GNS3.

El protocolo OSPF es un protocolo adecuado para el funcionamiento de redes heterogéneas de gran tamaño, este protocolo presta su funcionalidad al realizar cálculos de rutas a gran velocidad determinado su métrica, ofreciendo rendimiento a la redes, dinamismo en su forma de actualizar las tablas de enrutamiento con los próximos saltos cuando cambia la topología de la red, es el protocolo por excelencia que elegir el camino más corto entre redes, converge dentro sistemas autónomos (AS) a la vez permitiendo la administración para el tráfico de datos entre segmentos.

La implementación de los escenarios haciendo uso de ambientes virtuales de simulación como GNS3 permite identificar, configurar y realizar pruebas de ensayo y error de cómo se podría dimensionar, desempeñar y comportarse al encontrarse configurados los equipos en un entorno laboral real donde sea necesario una comunicación y transmisión de datos, permitiendo también los accesos a los segmentos de red de los switches, configuración de las VLANs y troncales para poder establecer la adecuada administración de los equipos de la red.

Al finalizar la construcción del documento con la elaboración de las simulaciones propuestas en el escenario correspondiente a la práctica de conocimientos del diplomado de profundización de CISCO CCNP logramos definir los conceptos de redes avanzadas para la administración y configuración de la Networking, que serán utilizados en el desarrollo de las etapas productivas en el campo laboral de la ingeniería en telecomunicaciones, logramos reconocer la importancia disciplinar de la administración de la redes aplicada en diversos escenarios reales en donde exista la necesidad de dar solución aplicando conocimientos propios de la disciplina en este caso la ingeniería en telecomunicaciones.

## BIBLIOGRAFÍA

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

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

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

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

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

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

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhqL9QChD1m9EuGqC>