

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS  
CCNP

JHOINER FAILER ANGARITA MONTIEL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
PROGRAMA INGENIERÍA TELECOMUNICACIONES  
TOLIMA  
2022

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS  
CCNP

JHOINER FAILER ANGARITA MONTIEL

Diplomado de opción de grado presentado para optar el título de ingeniero  
telecomunicaciones

PRESENTADO A:  
JUAN ESTEBAN TAPIAS BAENA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
PROGRAMA INGENIERÍA TELECOMUNICACIONES  
TOLIMA  
2022

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del Jurado

---

Firma del Jurado

Tolima 30 de noviembre de 2022

## **AGRADECIMIENTOS**

A mi familia quienes han sido siempre el motor que impulsa mis sueños y esperanzas, quienes estuvieron siempre a mi lado en los días y noches más difíciles durante mis horas de estudio. Siempre han sido mis mejores guías de vida.

A mis amigos que me apoyaron en este proyecto tan grande, quiero extender mi agradecimiento, no puedo evitar recordar mis tiempos en el colegio en donde apenas se formaban mis sueños, es muy reconfortante cada vez poder dar más pasos cerca a esas metas.

A mis instructores ya que fueron un apoyo fundamental en para lograr este objetivo en mi vida profesional y personal me motiva a seguir construyendo un futuro lleno de éxito.

## CONTENIDO

<b>NOTA DE ACEPTACION</b> .....	3
Lista de Ilustraciones .....	8
<b>RESUMEN</b> .....	10
Palabras Clave .....	10
<b>ABSTRACT</b> .....	11
Keywords .....	11
<b>INTRODUCCIÓN</b> .....	12
<b>1. DESARROLLO DEL PROYECTO</b> .....	13
1.1. Topología de la Red .....	13
<b>1. PASO 1: CABLEAR LA RED COMO SE MUESTRA EN LA TOPOLOGÍA</b> .....	18
1.1 Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces .....	18
1.2 Topología .....	18
<b>2.PASO 2: CONFIGURAR LOS PARÁMETROS BÁSICOS PARA CADA DISPOSITIVO</b> <b>19</b>	
2.1 Topología conectada .....	19
2.2 Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	28
<b>3. PASO 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO</b> .....	39
3.1 R3, .....	43
3.1.1 D2 .....	44
3.2 En R1 en la “Red ISP”, configure MP-BGP. ....	44

<b>4. PASO 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO (FIRST HOP REDUNDANCY)</b> .....	46
4.1 Topología.....	46
<b>5. PARTE 5: SEGURIDAD</b> .....	57
<b>6. PASO 6: CONFIGURE LAS FUNCIONES DE ADMINISTRACIÓN DE RED</b> .....	63
<b>CONCLUSIONES</b> .....	69
<b>REFERENCIAS BIBLIOGRÁFICAS</b> .....	70

## Lista de tablas

Tabla 1 Tabla de direccionamiento.....	14
Tabla 2 Tareas de configuración .....	28
Tabla 3 Interfaz de Vlan.....	39

## Lista de figuras

Figura 1 Topología de la Red Escenario 1 .....	13
Figura 2 Topología de Cablear la red .....	18
Figura 3 Topología conectada .....	19
Figura 4 Switch D1 .....	24
Figura 5 Switch D2 .....	25
Figura 6 running-config.....	26
Figura 7 Configuración del direccionamiento de los host PC 1 .....	26
Figura 8 Configuración del direccionamiento de los host PC4 .....	27
Figura 9 configuración de parámetros Vlan 02 .....	27
Figura 10 configuración de parámetros Vlan 01 .....	31
Figura 11 A1- Verificación .....	33
Figura 12 Topología .....	40
Figura 13 ip sla schedule 6 life forever start-time now.....	50
Figura 14 ip sla schedule 6 life forever start-time now.....	50
Figura 15-interface vlan 100.....	53
Figura 16 R1.....	58
Figura 17 R2.....	58
Figura 18 R3.....	58
Figura 19 D1.....	58
Figura 20 D2.....	58
Figura 21 A1 .....	58
Figura 22 authentication login default group radius local.....	60
Figura 23-aaa authentication login default group radius local.....	62
Figura 24-snmp-server host 10.0.100.5 version 2c ENCORSA.....	66



## GLOSARIO

**HOST:** Anfitrión que se usa para referirse a las computadoras u otros dispositivos (tablets, móviles, portátiles) conectados a una red.**NETWORK CORE:** Núcleo de red es la capa encargada de proporcionar conectividad entre los distintos puntos de acceso (router, switch, etc).

**PING:** Herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP.

**SWITCH:** Conmutador es un dispositivo de interconexión utilizado para conectar equipos en red.

**VTP: VLAN Trunking Protocol,** un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco

## RESUMEN

El diplomado de profundización CISCO, hace énfasis en realizar de manera correctas pruebas por medio de un simulador para un aprendizaje significativo por medio de lo práctico, usando herramientas de acceso remoto con el fin de establecer escenarios en redes como LAN/WAN, las cuales facilitan la realización de un análisis sobre la diversa aplicación de los protocolos y métrica de enrutamiento, es por esto que a través de la debida administración de las redes disponibles en la IOS para resolver los problemas de datos que se presentan en diversos tipos de redes, nos permite evaluar el desempeño de routers y switches, utilizando el uso de comandos especializados.

Durante el desarrollo del presente documento dará solución a los problemas planteados como parte de un examen final da habilidades prácticas, de acuerdo a lo requerido donde se puedan aplicar los conocimientos adquiridos durante este curso, al desarrollar la configuración de los dispositivos de una red, nos permiten llevar a cabo la alineación un dispositivo router, un dispositivo switch y los demás equipos que requieran la conectividad IPv4 como IPv6, para que los hosts soportados estén configurados de manera adecuada. Se configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security, todo con el fin de poder establecer que la conexión es transparente para el usuario, por lo que la práctica general de uso del acceso remoto es similar a la de trabajar en una estación de trabajo en una red local.

Así que podemos concluir la teoría y las habilidades que se han venido desarrollando con cada una de las prácticas realizadas y que han formado una capacidad técnica suficiente para desarrollar este proceso.

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

## ABSTRACT

The CISCO in-depth diploma emphasizes on carrying out correct tests by means of a simulator for a significant learning through the practical, using remote access tools in order to establish scenarios in networks such as LAN / WAN, which facilitate the realization of an analysis on the diverse application of the protocols and routing metrics, which is why through the proper administration of the networks available in the IOS to solve data problems that occur in various types of networks, it allows us to evaluate the performance of routers and switches, using the use of specialized commands.

During the development of this document, it will solve the problems raised as part of a final exam of practical skills, according to what is required where the knowledge acquired during this course can be applied, when developing the configuration of network devices, we They allow a router device, a switch device and other equipment that require IPv4 and IPv6 connectivity to carry out the alignment, so that the supported hosts are properly configured. Routing between VLANs, DHCP, Etherchannel and port-security will be configured, all in order to be able to establish that the connection is transparent to the user, so the general practice of using remote access is similar to working in a workstation on a local network.

So we can conclude the theory and the skills that have been developed with each of the practices carried out and that have formed a sufficient technical capacity to develop this process.

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

## INTRODUCCIÓN

En la actualidad los usuarios esperan tener acceso instantáneo a los recursos de una compañía, en cualquier momento y en cualquier lugar, es por esto que las redes modernas continúan evolucionando para adaptarse a las constantes demandas de la vida cotidiana; en estos recursos no solo repercuten los datos tradicionales, sino también de video y de voz. A su vez en las tecnologías se presentan necesidades que requieren de colaboración, en la que se reconocen el intercambio de recursos en tiempo real entre varias personas en sitios remotos como si estuvieran en la misma ubicación.

Cabe destacar que existen distintos dispositivos deben funcionar juntos sin problemas para proporcionar conexiones rápidas, seguras y confiables entre hosts. Un conmutador LAN proporciona el punto de conexión para los usuarios finales a la red corporativa y también es el principal controlador de información en el entorno LAN. Los enrutadores facilitan la transferencia de información entre LAN y en general, desconocen a los hosts individuales. Es por esto que los servicios avanzados dependen de la disponibilidad de una sólida infraestructura de routing y switching que se pueda construir; Esta infraestructura debe diseñarse, implementarse y administrarse cuidadosamente para proporcionar estabilidad a la plataforma.

En este proceso podemos analizar que el escenario inicial corresponde a CCNP Router, para los cuales trataremos dos protocolos básicos, EIGRP y OSPF. En cuanto al protocolo OSPF, podemos decir que se refiere al primer protocolo de estado de enlace de ruta más corta, desarrollado por el Grupo de trabajo de ingeniería de Internet para corregir las limitaciones de los protocolos de enrutamiento, en el escenario dos, el protocolo relevante utilizado es el protocolo BGP (Protocolo de Gateway de frontera) un protocolo ampliamente utilizado en entornos entre SA para permitir el enrutamiento de información entre los mismos

# 1. DESARROLLO DEL PROYECTO

## 1.1. Topología de la Red

Fig. 1 Topología de la Red Escenario 1

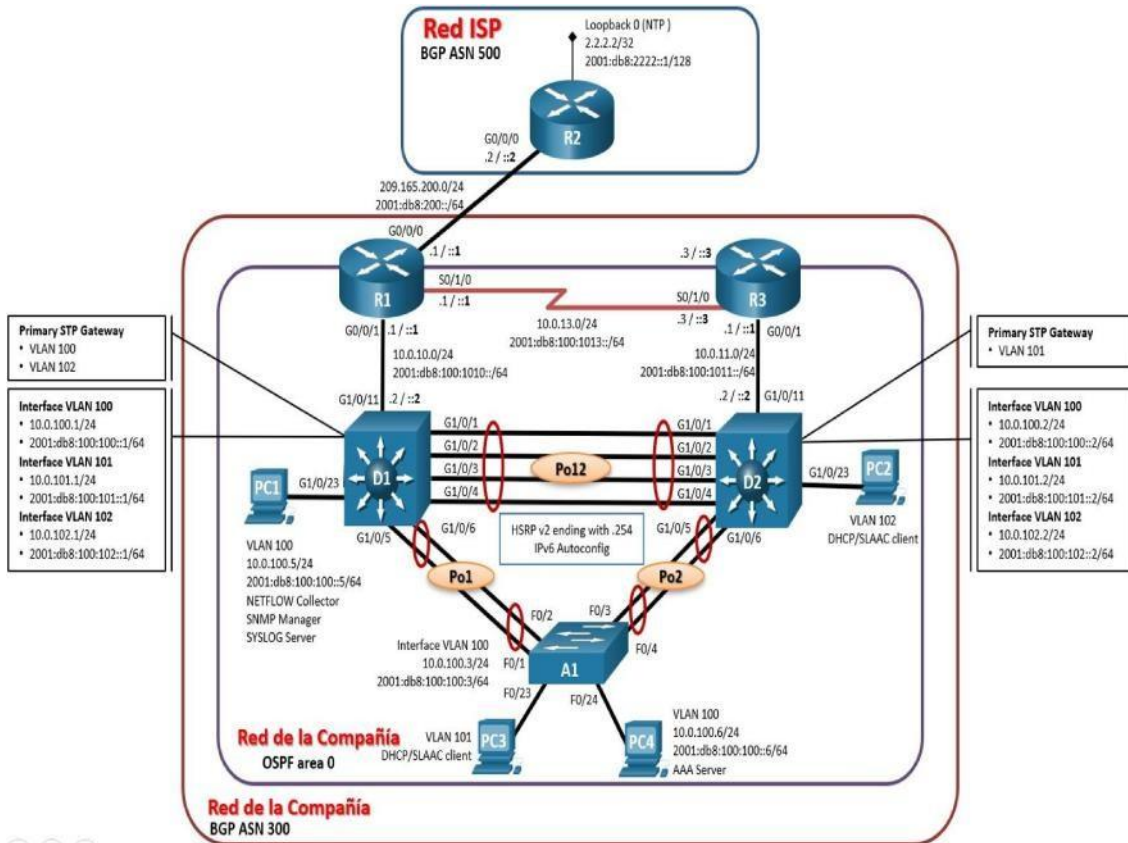


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Local	Link-
R1	G0/0/0	209.165.200.22 5/27	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	209.165.200.22 6/27	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	

Tabla 1 Tabla de direccionamiento

## Objetivos

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

Part 2: Configurar la capa 2 de la red y el soporte de Host Part 3: Configurar los protocolos de enrutamiento.

Part 4: Configurar la redundancia del primer salto (\*\*no se entrega aún)

Part 5: Configurar la seguridad (\*\*no se entrega aún).

Part 6: Configurar las características de administración de red (\*\* no se entrega aún)

## Escenario

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "**Red de la 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 version 16.9.4 (imagen universalk9). Los switches usados son Cisco Catalyst 3650 con Cisco IOSXE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variar de lo que se muestra en las prácticas de laboratorio.

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

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

## Recursos necesarios

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

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

1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)  
4 PCs (utilice el programa de emulación de terminal)

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



delos puertos de consola.

Los cables Ethernet y serales van como se muestra en la topología.

## 1. PASO 1: CABLEAR LA RED COMO SE MUESTRA EN LA TOPOLOGÍA

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

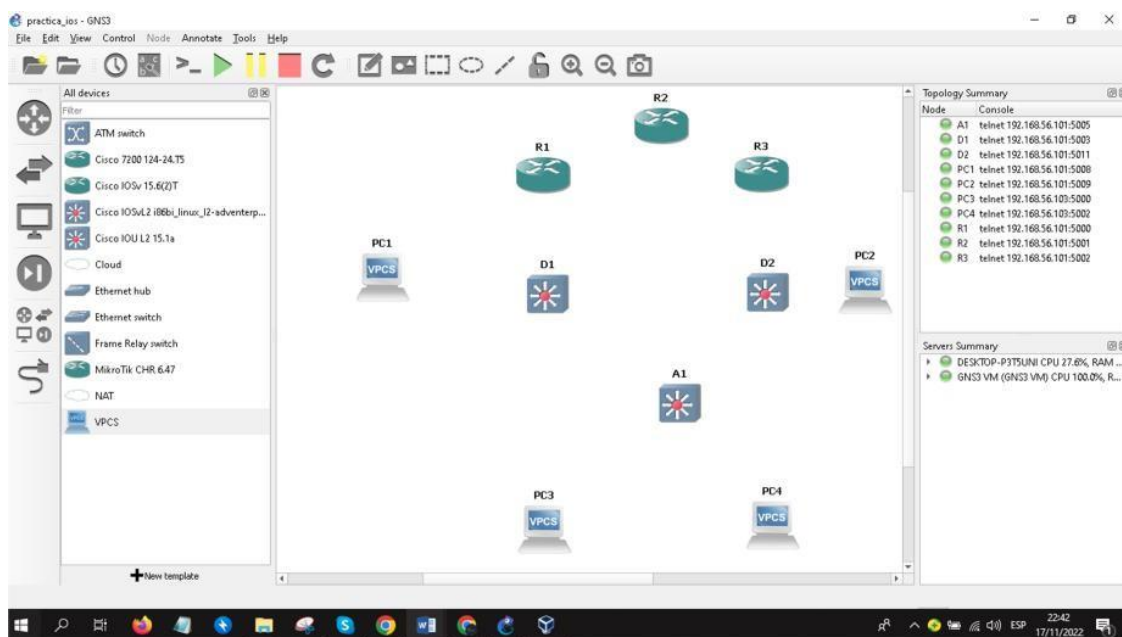
Conecte los dispositivos como se muestra en el diagrama de topología y conéctelos cables según sea necesario.

Adaptacion Tarjeta de expansion Routers 4321 (a packet tracer no hay disposicion del Router 4221)

The NIM-2T is a 2 port multi-protocol Synchronous Serial NIM

### 1.2 Topología.

Fig. 2 Topología de Cablear la red



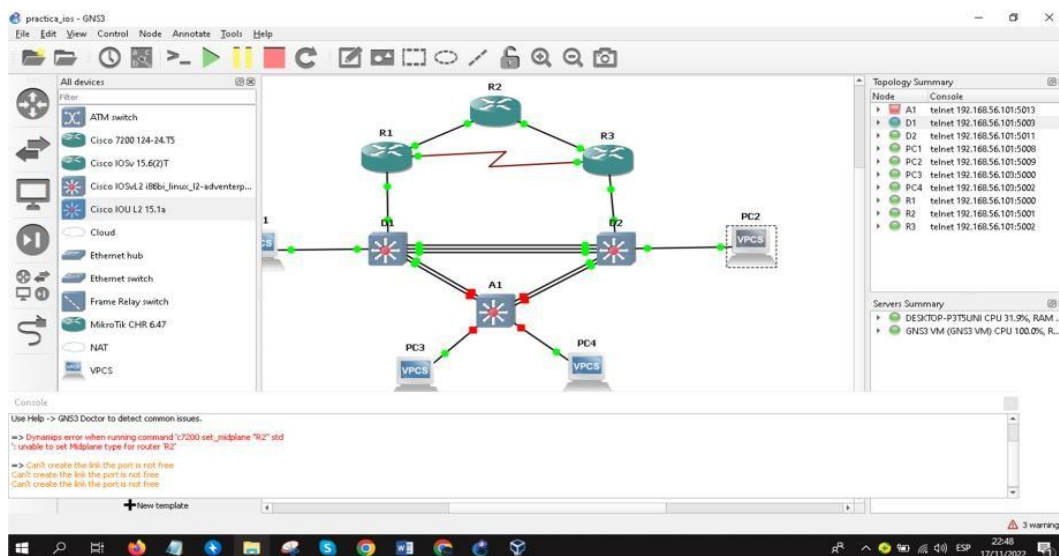
El cableado estructurado establecido en la topología propuesta corresponde al tipo de puertos conectados entre los dispositivos sea cable cruzado, cable serial y cable de red.

## 2. 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 aplicar parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

### 2.1 Topología conectada.

Fig. 3 Topología conectada



### Router R1

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

Se ingresa al modo privilegiado En el modo de configuración global se asigna el nombre al router R1 Se habilita router como router IPv6 Se habilita la traducción de nombre a dirección basado en DNS del host. Se crea un mensaje de aviso Se ingresa al modo de configuración de línea de la consola 0.

En el puerto de la consola 0 nunca se agotará el tiempo de espera. Evita que los mensajes inesperados que aparecen en pantalla, desplacen los comandos que estamos escribiendo en el momento. Se procede a configurar la interface g0/0 de R1. Se asigna la dirección ipv4 y la máscara de subred. Se asigna la dirección link local ala interface. Se asigna la dirección ipv6.

Exit

```
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 noshutdown
exit
interface s0/1/0
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 noshutdown
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 noshutdown
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 noshutdown
exit.
```

## Switch D1

```
hostname D1 ip routing
ipv6 unicast-routing no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 # line con 0 exec-timeout 0 0
logging synchronous exit
vlan 100
name Management exit vlan 101
name UserGroupA exit vlan 102
name UserGroupB exit
vlan 999 name NATIVE exit interface g1/0/11 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::2/64no
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
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4 shutdown exit.
```

En el modo de configuración global se asigna el nombre al Switch D1. Se habilita el routing ipv4.

Se habilita routing IPv6.

Se habilita la traducción de nombre a dirección basado en DNS del host.

Se crea un mensaje de aviso.

Se ingresa al modo de configuración de línea de la consola 0.

En el puerto de la consola 0 nunca se agotará el tiempo de espera.

Evita que los mensajes inesperados que aparecen en pantalla desplacen los comandos que estamos escribiendo en el momento.

Se configura la vlan 100 en D1. Se le asigna nombre.

Se configura la vlan 101 en D1. Se le asigna nombre.

Se configura la vlan 102 en D1.

Se le asigna nombre. Se configura la vlan 999.

Se le asigna nombre como la vlan nativa.

Se procede a configurar la interface.

E0/0 de D1.

Se aporta a la interface capacidad de capa3.

Se asigna la dirección ipv4 y la máscara de subred.

Se asigna la dirección link local a la interface.

Se asigna la dirección ipv6. Se habilita la interface E0/0. Se sale de la interfaz E0/0.  
Se procede a configurar la interface vlan 100 de D1.

## 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

```

Se asigna el nombre al Switch D2. Se habilita el routing ipv4.

Se habilita routing IPv6.

Se habilita la traducción de nombre a dirección basado en DNS del host. Se crea un mensaje de aviso.

Se ingresa al modo de configuración de línea de la consola 0.

En el puerto de la consola 0 nunca se agotará el tiempo de espera.

Evita que los mensajes inesperados que aparecen en pantalla, desplacen los comandos que estamos escribiendo en el momento.

Se configura la vlan 100 en D2. Se le asigna nombre.

Se configura la vlan 101 en D2. Se le asigna nombre.

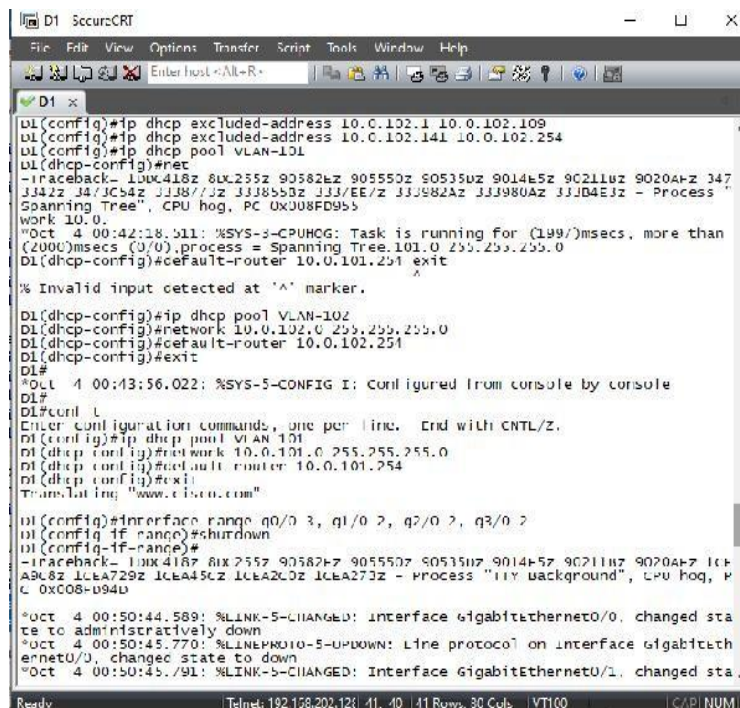
Se configura la vlan 102. Se le asigna nombre.

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 # line con 0 exec-timeout 0 0
logging synchronous exit
vlan 100
name Management exit
vlan 101
name UserGroupA exit
vlan 102
name UserGroupB exit
vlan 999 name NATIVE exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local ipv6 address 2001:db8:100:100::3/64 no
shutdown
exit
interface range f0/5-22 shutdown
exit
```

Fig.4 Switch D1

D1



```
D1 SccurCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt-R>
D1 x
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#net
-traceback- 10X418z 8X235z 90582Ez 905550z 905350z 9014E5z 902110z 9020A7z 347
J342z J4/JC54z J3J8/Jz J3J8550z J3J/EE/z J3J982Az J3J980Az J3J04EJz - Process "
Spanning Tree", CPU hog, PC 0x008FD955
work 10.0.
*Oct 4 00:42:18.511: %SYS-3-CPUHOG: Task is running for (199/)msecs, more than
(200)msecs (0/0), process = Spanning Tree.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.251 exit
% Invalid input detected at '^' marker.
D1(dhcp-config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.251
D1(dhcp-config)#exit
D1#
*Oct 4 00:43:56.022: %SYS-5-CONFIG I: Configured from console by console
D1#
D1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip dhcp pool VLAN 101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(dhcp-config)#exit
Translating "www.cisco.com"
D1(config)#interface range g0/0 3, g1/0 2, g2/0 2, g3/0 2
D1(config-if-range)#shutdown
D1(config-if-range)#
-traceback- 10X418z 8X235z 90582Ez 905550z 905350z 9014E5z 902110z 9020A7z 1c
A9C8z 1cEA729z 1cEA45Cz 1cEA2C0z 1cEA273z - Process "tty background", CPU hog, P
C 0x008D94D
*Oct 4 00:50:44.589: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed sta
te to administratively down
*Oct 4 00:50:45.770: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEt
ernet0/0, changed state to down
*Oct 4 00:50:45.791: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed sta
Ready Telnet: 192.168.202.12: 41, 40 41 Rows, 30 Cols VTI00 CAP NUM
```



En el modo de configuración global se asigna el nombre al Switch A1. Se habilita la traducción de nombre a dirección basado en DNS del host.

Se crea un mensaje de aviso

Se ingresa al modo de configuración de línea de la consola 0.

En el puerto de la consola 0 nunca se agotará el tiempo de espera, evita que los mensajes inesperados que aparecen en pantalla, desplacen los comandos que estamos escribiendo en el momento.

Se configura la vlan 100 en A1. Se le asigna nombre.

Se configura la vlan 101 en A1. Se le asigna nombre.

Se configura la vlan 102 en A1. Se le asigna nombre.

<pre>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</pre>	<p>En el modo de configuración global se asigna el nombre al Switch D2. Se habilita el routing ipv4 Se habilita routing IPv6 Se habilita la traducción de nombre a dirección basado en DNS del host. Se crea un mensaje de aviso. Se ingresa al modo de configuración de línea de la consola 0. En el puerto de la consola 0 nunca se agotará el tiempo de espera. Evita que los mensajes inesperados que aparecen en pantalla, desplacen los comandos que estamos escribiendo en el momento. Se configura la vlan 100 en D2. Se le asigna nombre.  Se configura la vlan 101 en D2. Se le asigna nombre.  Se configura la vlan 102. Se le asigna nombre.</p>
--	--

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

Fig. 6 *running-config*

```
PC1> save
Saving startup configuration to startup.vpc
. done

PC1> show

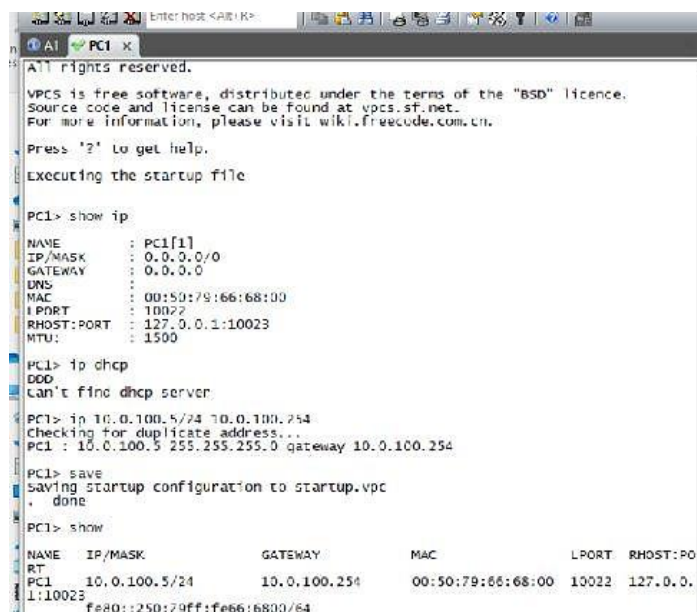
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC1      10.0.100.5/24  10.0.100.254  00:50:79:66:68:00  10022  127.0.0.
1:10023
          fe80::250:79ff:fe66:6800/64

PC1>
```

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.

Pc1

Fig.7 Configuración del direccionamiento de los host PC 1



```
PC1 X
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

PC1> show ip
NAME      : PC1[1]
IP/MASK   : 0.0.0.0/0
GATEWAY   : 0.0.0.0
DNS       :
MAC       : 00:50:79:66:68:00
LPORT    : 10022
RHOST:PORT : 127.0.0.1:10023
MTU       : 1500

PC1> ip dhcp
DDP
Can't find dhcp server

PC1> ip 10.0.100.5/24 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> save
Saving startup configuration to startup.vpc
. done

PC1> show

NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC1      10.0.100.5/24  10.0.100.254  00:50:79:66:68:00  10022  127.0.0.
1:10023
          fe80::250:79ff:fe66:6800/64
```

Configuración de PC1

```
PC1> ip 10.0.100.5/24 10.0.100.254
```

```
Checking for duplicate address... PC1 : 10.0.100.5
```

```
255.255.255.0 gateway 10.0.100.254
```

```
PC1> ip 2001:db8:100:100::5/64
```

```
PC1 : 2001:db8:100:100::5/64
```

Se configura la dirección ipv4 y el Gateway predeterminado.

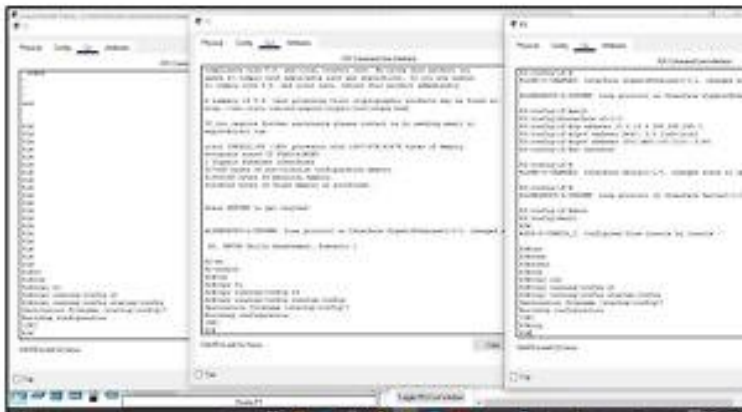
Se configura la dirección ipv6.

### Ilustración 8 Configuración del direccionamiento de los host PC4

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

Se emplea el comando: `copy running-config startup-config` en R1, R2 y R3.

Figura 9. Copia al archivo `starup-config` en R1, R2 y R3.



En esta parte del escenario 1 todos los routers se comunican con el vecino R1 con R2 y R2 con R3, y R1 se comunica con D1, y R3 se comunica con D2, La comunicación entre los switchts esta desconectada y los puertos están apagados.

## Topología

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

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

Las tareas de configuración son las siguientes:

Tabla 2 Tareas de configuración

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).

Habilite enlaces trunk 802.1Q entre:

```
D1 and D2 D1(config)#interface range g1/0/1-4
```

```
D1(config-if-range)#switchport trunk encapsulation dot1q D1(config-if-range)#switchport mode trunk
```

```
D1(cnofig-if-range)#exit
```

D1 and A1

```
D1(cnofig)#interface range g1/0/5-6
```

```
D1(cnofig-if-range)#switchport trunk encapsulation dot1q D1(cnofig-if-range)#switchport mode trunk
```

```
D1(cnofig-if-range)#exit
```

```
D1(config)#
```

D2 and A1

Se selecciona el rango de interfaces ethernet 1/0-3, ethernet 0/1-2.

Se configuran como interfaces troncales.

Se permiten solo las vlan 100,101,102 y 999 para estas interfaces troncales. Se asigna la vlan 999 como nativa.

Se activan las interfaces.  
Se activa el protocolo RSPT.

```
D2(config)#interface range g1/0/5-6
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#exit
D2(config)#
```

Use VLAN 999 como la VLAN nativa.

```
D1 a D2
D1(config)#interface range g1/0/1-4
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#exit
D1(config)#
```

D1 a A1

```
D1(config)#interface range g1/0/5-6
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#exit
```

D2 a A1

```
D2(config)#interface range g1/0/5-6
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#exit
D2(config)#
```

Use Rapid Spanning Tree (RSPT).

D1

```
D1(config)#spanning-tree mode rapid-pvst
D1(config)#end
D1#
%SYS-5-CONFIG_I: Configured from console by console
D2
```

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

D2#

Se selecciona el rango de interfaces ethernet 1/0-3, ethernet 0/1-2.  
Se configuran como interfaces troncales.

Se permiten solo las vlan 100,101,102 y  
999 para estas interfaces troncales. Se asigna la vlan 999 como nativa.

Se activan las interfaces.  
Se activa el protocolo RSPT.

%SYS-5-CONFIG\_I: Configured from console by console

```
D2#wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
D2#
```

A1

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

```
A1#wr
Building configuration...
[OK]
A1#
D1
```

Se configura D1 para usar mst.

Se acomoda la información de VLAN adicional, tomando prestados 12 bits de la prioridad de puente original.

Se ingresa al modo de configuración mst.

Se asigna un nombre de región mst.

Se configura un número de revisión de configuración de MST.

Se configura la instancia 1 donde se incluyen las vlan 100 y 102.

Se configura la instancia 2 donde se incluye la vlan 101.

Se estable mst0 y mst1 como raíz (para las vlan 100 y 102).

Se establece mst2 como secundario (para la vlan 101).

Fig. 10 configuración de parámetros Vlan 01

```
D1 x D2 A1
VLAN0102
Spanning tree enabled protocol ieee
Root ID Priority 32870
Address 0c1b.3809.0000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32870 (priority 32768 sys-id-ext 102)
Address 0c1b.3809.0000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FwD 4 128.2 P2p
Gi0/2 Desg FwD 4 128.3 P2p
Gi0/3 Desg FwD 4 128.4 P2p
Gi1/0 Desg FwD 4 128.5 P2p
Gi3/0 Desg FwD 4 128.13 P2p
Gi3/1 Desg FwD 4 128.14 P2p
Gi3/2 Desg FwD 4 128.15 P2p

VLAN0999
Spanning tree enabled protocol ieee
Root ID Priority 33767
Address 0c1b.3809.0000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 33767 (priority 32768 sys-id-ext 999)
Address 0c1b.3809.0000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FwD 4 128.2 P2p
Gi0/2 Desg FwD 4 128.3 P2p
Gi0/3 Desg FwD 4 128.4 P2p
Gi1/0 Desg FwD 4 128.5 P2p
Gi3/0 Desg FwD 4 128.13 P2p
```

## D2

Se ingresa a configurar OSPFv3 indicando el id del proceso (6). Se asigna el router id a R1. Se ordena a R1 para que de origen a la información de la ruta predeterminada y para que la ruta estática predeterminada se propague al actualizarse OSPF. Se accede a la interface gi1/0. Se habilita OSPFv6 para la interface en el área 0. Se accede a la interface se2/0. Se habilita OSPFv6 para la interface. La interface entre R1 y R2 (G0/0) no se habilitó.

Se coloca en modo trunk.

Se evita generar tramas DPT.

Se activa el protocolo LACP de forma incondicional.

Se accede a configurar la interface

E1/2.

Se coloca en modo trunk.

Se evita generar tramas DPT.

Se activa el protocolo LACP de forma incondicional.  
 Se accede a configurar la interface E1/3.  
 Se coloca en modo trunk.  
 Se evita generar tramas DPT.

Tarea #	Tarea	Especificación
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 de números canales: D1 a D2 – Port channel 12 D1 a A1 – Port channel 1 D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Ver los servicios DHCP que se configuren en los switches para que los hosts reciban direcciones 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
-----	---	--

A1

Fig. 11 A1- Verificacion

```

D1 D2 A1 x
enterprisek9-m' passed code signing verification
A1(config)#
-Traceback= 1DDC418z 8DC255z 90582Ez 905550z 90535Dz 9014E5z 90211Bz 9020AFz 8F2
304z - Process "IOSv e1000", CPU hog, PC 0x008F6E41

*Oct 10 15:11:44.317: %SYS-3-CPUHOG: Task is running for (1998)msecs, more than
(2000)msecs (0/0),process = IOSv e1000.
A1(config)#
-Traceback= 1DDC418z 8DC255z 90582Ez 905550z 90535Dz 9014E5z 90211Bz 9020AFz 347
EE85z 347EDB7z 7EALDFz - Process "Per-minute Jobs", CPU hog, PC 0x03E0A5A7

*Oct 10 15:20:21.225: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than
(2000)msecs (0/0),process = Per-minute Jobs.
A1(config)#exit
A1#
*Oct 10 15:22:39.045: %SYS-5-CONFIG_I: Configured from console by console
A1#show spanning-tree

VLAN0001
Spanning tree enabled protocol rstp
Root ID Priority 32769
Address 0cf9.aa6d.0000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0cf9.aa6d.0000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Gi2/3 Desg FWD 4 128.12 P2p
Gi3/0 Desg FWD 4 128.13 P2p
Gi3/1 Desg FWD 4 128.14 P2p
Gi3/2 Desg FWD 4 128.15 P2p
Gi3/3 Desg FWD 4 128.16 P2p

A1#

```

- Se accede a configurar la interface E1/0.
- Se coloca en modo trunk.
- Se evita generar tramas DPT.
- Se activa el protocolo LACP de forma incondicional.

Se accede a configurar la interface E1/1.  
Se coloca en modo trunk.  
Se evita generar tramas DPT.  
Se activa el protocolo LACP de forma incondicional.  
Se accede a configurar la interface  
E1/2.  
Se coloca en modo trunk.  
Se evita generar tramas DPT.  
Se activa el protocolo LACP de forma incondicional.  
Se accede a configurar la interface  
E1/3.  
Se coloca en modo trunk.  
Se evita generar tramas DPT.  
Se activa el protocolo LACP de forma incondicional.

Se accede a configurar la interface E0/0. Se indica que se va a configurar el modo de acceso. Se asigna la vlan 101. Se activa la interface. Se accede a configurar la interface E0/3. Se indica que se va a configurar el modo de acceso. Se asigna la vlan 100. Se activa la interface.

Se accede a configurar la interface E0/3. Se indica que se va a configurar el modo de acceso. Se asigna la vlan 102. Se activa la interface.

Se accede a configurar la interface E0/0.

Se indica que se va a configurar el modo de acceso.

Se asigna la vlan 101.

Se activa la interface.

Se accede a configurar la interface

E0/3.

Se indica que se va a configurar el modo de acceso.

Se asigna la vlan 100.

Se activa la interface

2.3 Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.

D1 root primary a la vlan 100

```
D1(config)#spanning-tree vlan 1 root primary
D1(config)#exit
D1#
%SYS-5-CONFIG_I: Configured from console by console
```

D2 root secondary a la vlan 100

```
D2(config)#spanning-tree vlan 1 root secondary
D2(config)#exit
D2#
%SYS-5-CONFIG_I: Configured from console by console
```

D2#

En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

### **D1 a D2 – Port channel 12**

```
D1(config)#interface range g1/0/1-4
D1(config-if-range)#no switchport
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/5 (999), with A1 FastEthernet0/1 (1).
```

```
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#
Creating a port-channel interface Port-channel 12
```

```
%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po12 and will be suspended
(native vlan of Gig1/0/1 is 999, Po12 id 1)
```

```
%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po12 and will be suspended
(native vlan of Gig1/0/2 is 999, Po12 id 1)
```

```
%EC-5-CANNOT_BUNDLE2: Gig1/0/3 is not compatible with Po12 and will be suspended
(native vlan of Gig1/0/3 is 999, Po12 id 1)
```

```
%EC-5-CANNOT_BUNDLE2: Gig1/0/4 is not compatible with Po12 and will be suspended
```

(native vlan of Gig1/0/4 is 999, Po12 id 1)

```
D1(config-if-range)#no shutdown
```

```
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to down
```

```
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to down
```

```
%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to down
```

```
%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to down D1(config-if-range)#exit
```

```
D1(config)#
```

### **D1 a A1 – Port channel 1**

```
D1(config)#interface range g1/0/5-6
```

```
D1(config-if-range)#no switchport
```

```
D1(config-if-range)#
```

```
D1(config-if-range)#channel-protocol lacp
```

```
D1(config-if-range)#channel-group 1 mode active
```

```
D1(config-if-range)#
```

```
Creating a port-channel interface Port-channel 1
```

```
%EC-5-CANNOT_BUNDLE2: Gig1/0/5 is not compatible with Po1 and will be suspended  
(native vlan of Gig1/0/5 is 999, Po1 id 1)
```

```
%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po1 and will be suspended  
(native vlan of Gig1/0/6 is 999, Po1 id 1)
```

```
D1(config-if-range)#no shutdown
```

```
D1(config-if-range)#
```

```
D1(config-if-range)#exit
```

Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.

```
D1(config)#
```

## D2 a A1 – Port channel 2

```
D2(config)#interface range g1/0/5-6
D2(config-if-range)#no switchport
D2(config-if-range)#
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
  Creating a port-channel interface Port-channel 2
D2(config-if-range)#no shu
D2(config-if-range)#no shutdown
D2(config-if-range)#
D2(config-if-range)#exit
```

En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

D1

```
D1(config)#interface gigabitEthernet 1/0/23
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
  D1(config-if)#no shutdown
D1(config-if)#no shutdown
```

D2

```
D2(config)#interface gigabitEthernet 1/0/23
D2(config-if)#switchport mode a
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan
D2(config-if)#switchport access vlan 102
D2(config-if)#no shut
```

A1

```
A1(config)#interface fastEthernet 0/24

A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#no shutdown
A1(config-if)#exit
```

```
A1(config)#interface fastEthernet 0/23
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
```

```
A1(config-if)#no shutdown  
A1(config-if)#exit  
A1(config)#
```

Verifique los servicios DHCP IPv4.  
PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

```
PC2 DHCP VLAN 102  
PC3 DHCP VLAN 101
```

### 3. PASO 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO

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

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

Las tareas de configuración son las siguientes:

*Tabla 3 Interfaz*

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.	Use OSPF Process ID 4 y asigne los siguientes router-IDs: R1: 0.0.4.1 R3: 0.0.4.3 D1: 0.0.4.131 D2: 0.0.4.132  En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.

		<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	<p>En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.</p>	<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>
	<p>En R2 en la “Red ISP”, configure MP-BGP.</p>	<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>



3.3		<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</p>
-----	--	---

		<p>vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie: La red Loopback 0 IPv4 (/32). La ruta por defecto (0.0.0.0/0).</p> <p>En IPv6 address family, anuncie: La red Loopback 0 IPv4 (/128). La ruta por defecto (::/0).</p>
3.4	<p>En R1 en la "Red ISP", configure MP-BGP.</p>	<p>Configure dos rutas resumen estáticas a la interfaz Null 0: Una ruta resumen IPv4 para 10.0.0.0/8. Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: Deshabilite la relación de vecino IPv6. Habilite la relación de vecino IPv4. Anuncie la red 10.0.0.0/8. En IPv6 address family: Deshabilite la relación de vecino IPv4. Habilite la relación de vecino IPv6. Anuncie la red 2001:db8:100::/48.</p>

En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.

```
R1,  
R1(config)#router ospf 1  
R1(config-router)#router-id 0.0.4.1  
R1(config-router)#do show ip route connected
```

Se ingresa a configurar OSPF indicando el id del proceso (4). Se asigna el router id a R1.

Se anuncian las redes directamente conectadas a R1 a excepción de la red 209.165.200.224 que está entre R1 – R2, para definir las interfaces que van a participar en OSPF, delimitando el área. Se ordena a R1 para que de origen a la información de la ruta predeterminada y para que la ruta estática predeterminada se propague al actualizarse OSPF.

Se ingresa a configurar OSPF indicando el id del proceso (4). Se asigna el router id a R3. Se anuncian las redes directamente conectadas a R3, para definir las interfaces que van a participar en OSPF, delimitando el área.

```
C 10.0.10.0/24 is directly connected, GigabitEthernet0/0/1  
C 10.0.13.0/24 is directly connected, Serial0/1/0  
C 209.165.200.224/27 is directly connected, GigabitEthernet0/0/0  
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0  
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0  
R1(config-router)#network 209.165.200.224 0.0.0.31 area 0  
R1(config-router)#exit  
R1(config)#
```

### 3.1 R3,

```
R3(cnfig)#router ospf 1
R3(cnfig-router)#router-id 0.0.4.3
```

```
R1(cnfig)#interface serial 0/1/0
R1(cnfig-if)#ip ospf 1 area 0
R1(cnfig-if)#exit
R1(cnfig)#
```

```
R3(cnfig-router)#do show ip route connected
C 10.0.11.0/24 is directly connected, GigabitEthernet0/0/1
C 10.0.13.0/24 is directly connected, Serial0/1/0
R3(cnfig-router)#network 10.0.11.0 0.0.0.255 area 0
R3(cnfig-router)#network 10.0.13.0 0.0.0.255 area 0
R3(cnfig-router)#exit
R3(cnfig)#interface serial 0/1/0
R3(cnfig-if)#ip ospf 1 area0
R3(cnfig-if)#exit
R3(cnfig)#
```

```
D1,
D1(cnfig)#router ospf 1
D1(cnfig-router)#router-id 0.0.4.131
D1(cnfig-router)#do show ip route connected
C 10.0.10.0/24 is directly connected, GigabitEthernet1/0/11
C 10.0.100.0/24 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
```

Se ingresa a configurar OSPF indicando el id del proceso (4). Se asigna el router id a D1. Se anuncian las redes directamente conectadas a D1, para definir las interfaces que van a participar en OSPF, delimitando el área.

```
D1(cnfig-router)#network 10.0.0.0 0.0.0.255 area 0
D1(cnfig-router)#exit
D1(cnfig)#interface range gigabitEthernet 1/0/1-6
D1(cnfig-if-range)#ip ospf 1 area 0
D1(cnfig-if-range)#interface range gigabitEthernet 1/0/11
D1(cnfig-if-range)#ip ospf 1 area 0
D1(cnfig-if-range)#exit
D1(cnfig)#
```

### 3.1.1 D2

```
D2(config)#router ospf 1
D2(config-router)#router-id 0.0.4.132
D2(config-router)#do show ip route connected
C 10.0.11.0/24 is directly connected, GigabitEthernet1/0/11
C 10.0.100.0/24 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
D2(config-router)#network 10.0.0.0 0.0.0.255 area 0
D2(config-router)#exit
```

Se ingresa a configurar OSPF indicando el id del proceso (4). Se asigna el router id a D2.

Se anuncian las redes directamente conectadas a D2, para definir las interfaces que van a participar en OSPF, delimitando el área.

Todas las interfaces de D2 se colocan en estado pasivo para OSPF y así no se tienen publicaciones OSPFv2.

La única interface que se habilita para OSPFv2 es la ethernet 0/0.

### 3.2 En R1 en la "Red ISP", configure MP-BGP.

```
R1(config-router)#do show ip route
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, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is 10.0.10.2 to network 0.0.0.0
O* 0.0.0.0/0 [110/2] via 10.0.10.2, 00:38:31, GigabitEthernet0/0/1
10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C 10.0.10.0/24 is directly connected, GigabitEthernet0/0/1
L 10.0.10.1/32 is directly connected, GigabitEthernet0/0/1
```

O 10.0.11.0/24 [110/65] via 10.0.13.3, 00:48:26, Serial0/1/0  
C 10.0.13.0/24 is directly connected, Serial0/1/0  
L 10.0.13.1/32 is directly connected, Serial0/1/0  
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks  
C 209.165.200.224/27 is directly connected, GigabitEthernet0/0/0  
L 209.165.200.225/32 is directly connected, GigabitEthernet0/0/0

R1(config-router)#NEIghbor 10.0.13.0 remote-as 30  
R1(config-router)#NEIghbor 10.0.10.0 remote-as 30  
R1(config-router)#NEIghbor 10.0.11.0 remote-as 30

## 4. PASO 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 hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

### 4.1 Topología.

Fig.12 Topología

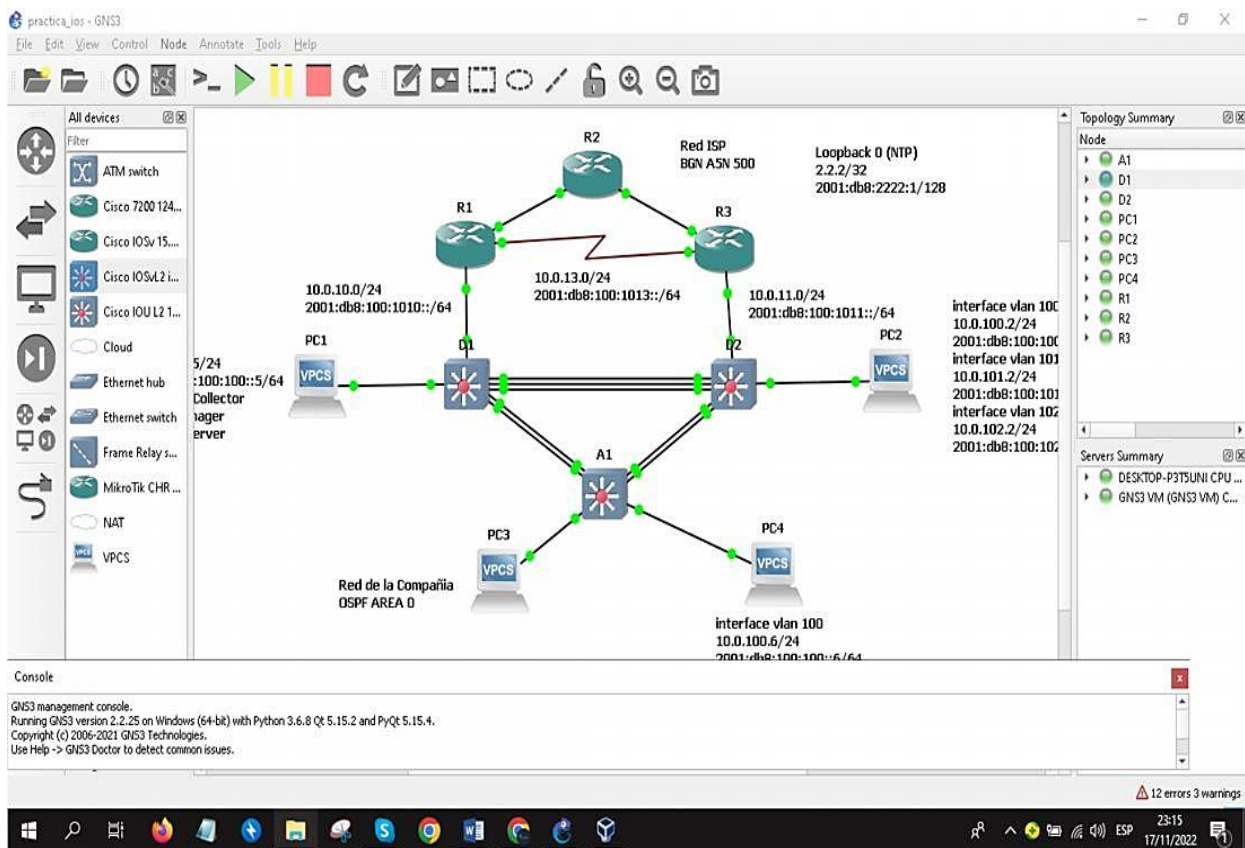


Tabla 4 Tareas de Configurar de los protocolos de enrutamiento

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 R1G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sintiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 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 R3G0/0/1 cada 5 segundos.</p> <p>Programe la SLA para una implementación inmediata sintiempo de finalización.</p> <p>Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 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	<p>En D1 configure HSRPv2.</p>	<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 VLAN100:</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 VLAN101:</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 VLAN102:</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 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 VLAN100:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6autoconfig</b>.</li> </ul>



		<ul style="list-style-type: none"> <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 VLAN101:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6autoconfig</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 VLAN102:</p> <ul style="list-style-type: none"> <li>• Asigne la dirección IP virtual usando <b>ipv6autoconfig</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>
--	--	--

Se define el número de sesión 4 del SLA

Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv4 G1/0 de R1.

Se prueba la disponibilidad de la interfaz G1/0 de R1 cada 5 segundos. Se define el número de sesión 6 del SLA.

Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv6 G1/0 de R1.

Se prueba la disponibilidad de la interfaz G1/0 de R1 cada 5 segundos

Se programa la SLA 4 para una implementación inmediata sin tiempo de finalización. Se programa la SLA 6 para una implementación inmediata sin tiempo de finalización. Se crea el número de rastreo 4 y se asocia al IP SLA 4.

Cada 10 segundos se debe notificar el:

```

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

```

*Fig.13 ip sla schedule 6 life forever start-time now*

```

D1(config)#track 4 ip sla 4
D1(config-track)# delay down 10 up 15
D1(config-track)#track 6 ip sla 6
D1(config-track)# delay down 10 up 15
D1(config-track)#ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)#ip sla schedule 4 life forever start-time now
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)#ip sla schedule 6 life forever start-time now
D1(config)#

```

```

4.2
D2
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

```

cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando para de up a down. Se crea el número de rastreo 6 y se asocia al IP SLA 6.

Cada 10 segundos se debe notificar el cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando pasa de up a down

```

ip sla 6
icmp-echo 2001:DB8:100:1011::1
frequency 5
ip sla schedule 6 life forever start-time now

```

*Fig. 14-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)#track 6 ip sla 6
D2(config-track)# delay down 10 up 15
D2(config-track)#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)#ip sla schedule 4 life forever start-time now
D2(config)#
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)#ip sla schedule 6 life forever start-time now
D2(config)#

```

### 4.3

D1

```
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.
```

Se define el número de sesión 4 del SLA.

Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv4 G0/0 de R3.

Se prueba la disponibilidad de la interfaz G0/0 de R3 cada 5 segundos. Se define el número de sesión 6 del SLA.

Se inicia la configuración IP SLA ICMP

Echo con destino a la interfaz ipv6 G0/0 de R3.

Se prueba la disponibilidad de la interfaz G1/0 de R1 cada 5 segundos. Se programa la SLA 4 para una implementación inmediata sin tiempo de finalización.

Se programa la SLA 6 para una implementación inmediata sin tiempo de finalización.

Se crea el número de rastreo 4 y se asocia al IP SLA 4.

Cada 10 segundos se debe notificar el cambio de estado de la IP SLA cuando pasa de down a up.

Cada 15 segundos cuando pasa de up a down. Se crea el número de rastreo 6 y se asocia al IP SLA 6. Cada 10 segundos se debe notificar el cambio de estado de la IP SLA cuando pasa de down a up.

Se accede a la interfaz VLAN 100.

Se configura el HSRP para usar la versión 2.

Se inicia la configuración IPv4 HSRP grupo 104 para la VLAN 100, asignando la ip virtual 10.0.100.254.

Se establece la prioridad del grupo 124 en 150.

Se habilita la preferencia al grupo 124.

Se rastrea el objeto 4 y se decrementa en 60.

Se inicia la configuración IPv6 HSRP grupo 106 para la VLAN 100.

Se asigna la dirección IP virtual usando ipv6 autoconfig.

Se establece la prioridad del grupo en 150.

Se habilita la preferencia al grupo 106

Se rastrea el objeto 6 y se decrementa en 60.

*Fig. 15-interface vlan 100*

```
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
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
D1(config)#end
D1#
```

D2

interface vlan 100

standby version 2

standby 104 ip 10.0.100.254

standby 104 preempt

standby 104 track 4 decrement 60

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

Se habilita la preferencia al grupo 114.

Se rastrea el objeto 4 y se decrementa en 60.

Se inicia la configuración IPv6 HSRP grupo 116 para la VLAN 101.

Se asigna la dirección IP virtual usando ipv6 autoconfig.

Se establece la prioridad del grupo en 150.

Se habilita la preferencia al grupo 116. Se rastrea el objeto 6 y se decrementa en 60.

Se accede a la interfaz VLAN 102.

Se configura el HSRP para usar la versión 2.

Se inicia la configuración IPv4 HSRP grupo 124 para la VLAN 102, asignando la ip virtual 10.0.102.254.

Se habilita la preferencia al grupo 124.

Se rastrea el objeto 4 y se decrementa en 60.

Se inicia la configuración IPv6 HSRP grupo 126 para la VLAN 102.

Se asigna la dirección IP virtual usando ipv6 autoconfig.

Se habilita la preferencia al grupo 126.

Se rastrea el objeto 6 y se decrementa en 60.

```
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
D2(config)#
```



## 5. 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 de configuración de seguridad en los dispositivos*

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: sadmin Nivel de privilegio 15 Contraseña: cisco12345cisco
5.3	En todos los dispositivos(excepto R2),habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: <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: \$trongPass</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: raduser y la contraseña: upass123.
-----	--	---

## 5.1

En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.

Para R1: R1(config)#enable algorithm-type scrypt secret cisco12345cisco

Para R2: R2(config)#enable algorithm-type scrypt secret cisco12345cisco

Para R3: R3(config)#enable algorithm-type scrypt secret cisco12345cisco

En todos los dispositivos, cree un usuario localy protéjalo usando el algoritmo de encriptación SCRYPT. Para R1: Para R2: Para R3: Para D1: Para D2: Para A1

*Fig. 16, 17, 18, 19, 20, 21*

```
R1(config)# username sadmin privilege 15 algorithm-type SCRYPT
secret cisco12345cisco
```

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

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

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

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

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

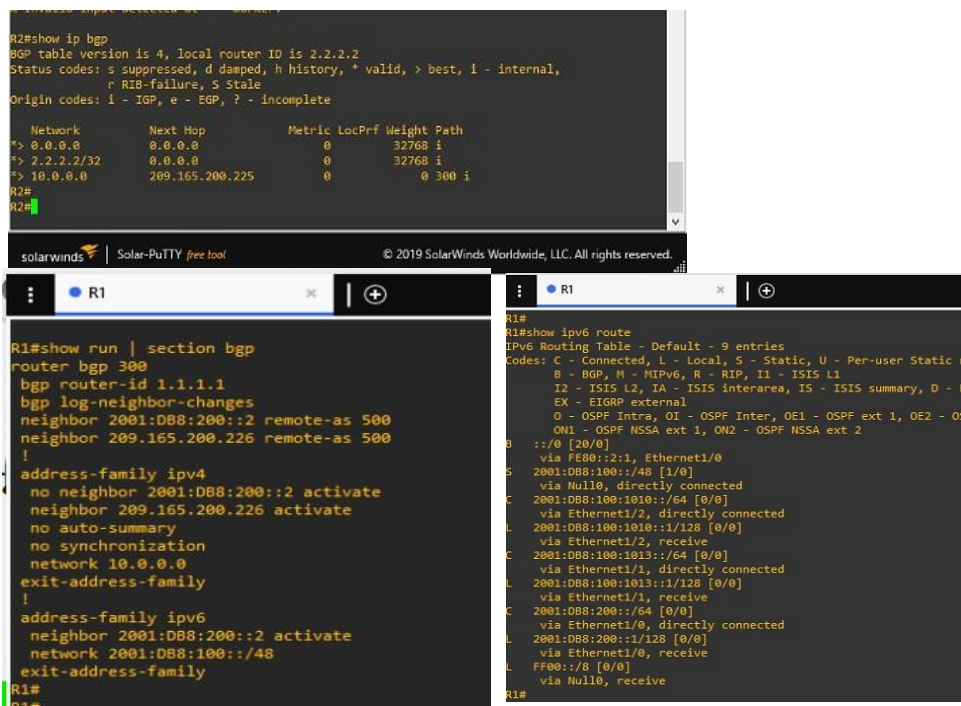
En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS. R1(config)#radius server RADIUS R1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813.

R1(config-radius-server)# key \$strongPass R1(config-radius-server)# exit 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 D1(config)#radius server RADIUS

Se inicia la configuración del servidor RADIUS en R1. Se especifica la dirección IP y los puertos UDP para R1. Se asigna la contraseña al servidor RADIUS para R1. Se inicia la configuración del servidor RADIUS en R3. Se especifica la dirección IP y los puertos UDP para R3. Se asigna la contraseña al servidor RADIUS para R3. Se inicia la configuración del servidor RADIUS en D1.

### Verificación De Configuración BGP EN R2

El comando utilizado que me permite revisar BGP en el Router, se muestra la tabla de routing en BGP en el dispositivo R2,



5.4  
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

Utiliza la base de datos local del router (el segundo método). Se configura la lista de métodos de autenticación AAA en D2. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método). Se configura la lista de métodos de autenticación AAA en A1. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método).

D1#

*Fig. 22 authentication login default group radius local*

R1

```
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $strongPass
D1(config-radius-server)# exit
D1(config)#aaa authentication login default group radius local
D1(config)#
```

R3

```
R1(config)#aaa new-model
R1(config)#radius server RADIUS
R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $strongPass
R1(config-radius-server)# exit
R1(config)#aaa authentication login default group radius local
R1(config)#
```

D2

```
R3(config)#aaa new-model
R3(config)#radius server RADIUS
R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $strongPass
R3(config-radius-server)# exit
R3(config)#aaa authentication login default group radius local
R3(config)#
```

A1

```
D2(config)#aaa new-model
D2(config)#radius server RADIUS
D2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)# key $strongPass
D2(config-radius-server)# exit
D2(config)#aaa authentication login default group radius local
D2(config)#
```

```
A1(config)#aaa new-model
A1(config)#radius server RADIUS
A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813
A1(config-radius-server)# key $strongPass
A1(config-radius-server)# exit
A1(config)#aaa authentication login default group radius local
A1(config)#
```

## 5.5

aaa authentication login default group radius local

Utiliza la base de datos local del router (el segundo método). Se configura la lista de métodos de autenticación AAA en D2. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método). Se configura la lista de métodos de autenticación AAA en A1. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método).

Local D2(config)#aaa authentication login default group radius local  
A1(config)#aaa authentication login default group radius local.

aaa session-id common

Verificación enrutamiento OSPF

show run | section router ospf

este Comando se utiliza para verificar las redes conectadas con enrutamiento OSPF, el área y el sector, se puede corroborar en R1 y R3, en D1 y D2 En R1

```
R1#show run | section router ospf
router ospf 4
  router-id 0.0.4.1
  log-adjacency-changes
  network 10.8.10.0 0.0.0.255 area 0
  network 10.8.13.0 0.0.0.255 area 0
  network 209.165.200.224 0.0.0.31 area 0
  default-information originate
  ipv6 router ospf 6
    router-id 0.0.6.1
    log-adjacency-changes
    default-information originate
R1#

R3#show run | section ospf
ip ospf 1 area 0
router ospf 1
  router-id 0.0.4.3
  log-adjacency-changes
  network 10.8.11.0 0.0.0.255 area 0
  network 10.8.13.0 0.0.0.255 area 0
R3#

D1#show run | section ospf
ipv6 ospf 6 area 0
ipv6 ospf 6 area 0
ipv6 ospf 6 area 0
ipv6 ospf 6 area 0
router ospf 4
  router-id 0.0.4.131
  passive-interface default
  no passive-interface Ethernet1/2
  network 10.8.10.0 0.0.0.255 area 0
  network 10.8.100.0 0.0.0.255 area 0
  network 10.8.101.0 0.0.0.255 area 0
  network 10.8.102.0 0.0.0.255 area 0
  ipv6 router ospf 6
    router-id 0.0.6.131
    passive-interface default
    no passive-interface Ethernet1/2
D1#

D2#show run | section ospf
router ospf 1
  router-id 0.0.4.132
  passive-interface default
  no passive-interface Ethernet1/0
  network 10.8.11.0 0.0.0.255 area 0
  network 10.8.100.0 0.0.0.255 area 0
  network 10.8.101.0 0.0.0.255 area 0
  network 10.8.102.0 0.0.0.255 area 0
  ipv6 router ospf 6
    router-id 0.0.6.132
    passive-interface default
    no passive-interface Ethernet1/0
D2#
```

**Fig.23**

```
D2#sh run aaa
|
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$XC04pzqbRT.3EP$ymouL0QI5/o0F0kYDtA1ztejFra67!nkJJ5Y3bhyQe6
|
```

Como se observa en la figura , se ha cerrado e iniciado sesión en R1, R3, D1, D2 y A1. En R1, D1 y D2 respondió el servidor RADIUS; en R3 y A1 respondió el servidor local.

A1  
show run aaa

```
A1#sh run aaa
|
aaa authentication login default group radius local
username admin privilege 15 secret 9 $9$XC04pzqbRT.3EP$ymouL0QI5/o0F0kYDtA1ztejFra67!nkJJ5Y3bhyQe6
username sadmin privilege 15 secret 9 $9$XC04pzqbRT.3EP$ymouL0QI5/o0F0kYDtA1ztejFra67!nkJJ5Y3bhyQe6
|
```

## 6. 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:

Tabla 6 Funciones de la red

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"> <li>• R1 debe sincronizar con R2.</li> <li>• R3, D1 y A1 para sincronizar la hora con R1.</li> <li>• D2 para sincronizar la hora con R3.</li> </ul>
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	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 un 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>

## 6.1

```
R1# ntp server 2.2.2.2
```

```
R3# ntp server 10.0.10.1 A1# ntp server 10.0.10.1 D1# ntp server 10.0.10.1 D2# ntp server 10.0.10.1
```

## 6.2

```
R2
```

```
ntp master 3
```

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

## 6.3

```
R1# ntp server 2.2.2.2
```

```
R1(config)#ntp server 2.2.2.2
```

```
R3# ntp server 10.0.10.1
```

```
R3(config)#ntp server 10.0.10.1
```

```
D1# ntp server 10.0.10.1
```

```
D1(config)#ntp server 10.0.10.1
```

```
D2# ntp server 10.0.10.1
```

```
D2(config)#ntp server 10.0.10.1  
D2(config)#
```

```
A1# ntp server 10.0.10.1
```

```
A1(config)#ntp server 10.0.10.1  
A1(config)#
```

```
R1(config)#ntp server 2.2.2.2
```

```
R3(config)#ntp server 10.0.10.1
```

```
D1(config)#ntp server
```

Se configura el reloj local de R1 a la hora UTC actual. Para ello se configura NTP para que R1 se sincronice por medio de la interfaz loopback 0 de R2.

Se configura el reloj local de R3 a la hora UTC actual. Para ello se configura NTP para que R3 se sincronice por medio de la interfaz G1/0 de R1.



Se configura el reloj local de D3 a la hora UTC actual.

6.4

logging host 10.0.100.5 logging trap warning logging on

R1

```
R1(config)#logging host 10.0.100.5
R1(config)#logging trap warning
R1(config)#logging on
```

R3

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

D1

```
D1(config)#logging host 10.0.100.5
D1(config)#logging trap warning
D1(config)#logging on
```

D2

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

A1

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

Para ello se configura NTP para que R3 se sincronice por medio de la interfaz G1/0 de R1.

Se configura el reloj local de A1 a la hora UTC actual. Para ello se configura NTP para que R3 se sincronice por medio de la interfaz G1/0 de R1.

Se configura el reloj local de D2 a la hora UTC actual. Para ello se configura NTP para que D2 se sincronice por medio de la interfaz G0/0 de R3.

Se configura R2 como NTP maestro en el nivel de estrato 3.

Se configura el host PC1 para que sea el host de registro de destino para R1.

Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.

Se habilita el registro para que los mensajes puedan ser enviados.

Se configura el host PC1 para que sea el host de registro de destino para R3.

Se establece el nivel de prioridad del “trap” en el nivel 4 (warning)

## 6.5

### R1

```
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
```

*Fig. 24-snmp-server host 10.0.100.5 version 2c ENCORSA*

```
R1(config)#snmp-server community ENCORSA RO SNMP-NMS
R1(config)#snmp-server contact Cisco Student
R1(config)#snmp-server enable traps ospf state-change
R1(config)#snmp-server enable traps ospf errors
R1(config)#snmp-server enable traps ospf retransmit
R1(config)#snmp-server enable traps ospf lsa
R1(config)# enable traps ospf cisco-specific state-change nssa-trans-change
R1(config)# enable traps ospf cisco-specific state-change shamlink interface
R1(config)# enable traps ospf cisco-specific state-change shamlink neighbor
R1(config)#snmp-server enable traps ospf cisco-specific errors
R1(config)#snmp-server enable traps ospf cisco-specific retransmit
R1(config)#snmp-server enable traps ospf cisco-specific lsa
R1(config)#snmp-server enable traps config
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)#
```

### R3.

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

Se habilita el registro para que los mensajes puedan ser enviados.

Se configura el host PC1 para que sea el host de registro de destino para D1.

Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.

Se habilita el registro para que los mensajes puedan ser enviados.

Se configura el host PC1 para que sea el host de registro de destino para D2.

Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.

Se habilita el registro para que los mensajes puedan ser enviados.

Se configura el host PC1 para que sea el host de registro de destino para A1.

Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.

Se habilita el registro para que los mensajes puedan ser enviados

```
R3(config)#snmp-server community ENCORSA RO SNMP-NMS
R3(config)#snmp-server contact Cisco Student
R3(config)#snmp-server enable traps ospf state-change
R3(config)#snmp-server enable traps ospf errors
R3(config)#snmp-server enable traps ospf retransmit
R3(config)#snmp-server enable traps ospf lsa
R3(config)#$ enable traps ospf cisco-specific state-change nssa-trans-change
R3(config)#$ enable traps ospf cisco-specific state-change shamlink interface
R3(config)#$ enable traps ospf cisco-specific state-change shamlink neighbor
R3(config)#snmp-server enable traps ospf cisco-specific errors
R3(config)#snmp-server enable traps ospf cisco-specific retransmit
R3(config)#snmp-server enable traps ospf cisco-specific lsa
R3(config)#snmp-server enable traps config
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
```

D2

```
D2(config)#snmp-server community ENCORSA RO SNMP-NMS
D2(config)#snmp-server contact Cisco Student
D2(config)#snmp-server enable traps ospf state-change
D2(config)#snmp-server enable traps ospf errors
D2(config)#snmp-server enable traps ospf retransmit
D2(config)#snmp-server enable traps ospf lsa
D2(config)#$ enable traps ospf cisco-specific state-change nssa-trans-change
D2(config)#$ enable traps ospf cisco-specific state-change shamlink interface
D2(config)#$ enable traps ospf cisco-specific state-change shamlink neighbor
D2(config)#snmp-server enable traps ospf cisco-specific errors
D2(config)#snmp-server enable traps ospf cisco-specific retransmit
D2(config)#snmp-server enable traps ospf cisco-specific lsa
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#
```

Se establece el "community string" en ENCORSA y se especifica el uso de SNMPv2 como solo lectura. Se limita el acceso SNMP a la dirección IP de PC1. Se configura el valor de contacto SNMP con mi nombre. Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP. En R1, se habilita el envío de traps: bgp, config, y ospf. Se establece el "community string" en ENCORSA y se especifica el uso de SNMPv2 como solo lectura. Se limita el acceso SNMP a la dirección IP de PC1. Se configura el valor de contacto SNMP con mi nombre. Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP. En R3, se habilita el envío de traps: config, y ospf.. Se establece el "community string" en ENCORSA y se especifica el uso de SNMPv2 como solo lectura. Se limita el acceso SNMP a la dirección IP.

Se establece el "community string" en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.

Se limita el acceso SNMP a la dirección IP de PC1.

Se configura el valor de contacto SNMP con mi nombre.

Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.

En R1, se habilita el envío de traps: bgp, config, y ospf.

Se establece el "community string" en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.

Se limita el acceso SNMP a la dirección IP de PC1.

## CONCLUSIONES

- Inicialmente cabe destacar que el desarrollo del ejercicio en el escenario posibilita evidenciar que no todos los dispositivos comercializados son apropiados para realizar las tareas requeridas para la configuración de interfaces troncales, y la habilitación del servicio del servidor.
- Es importante realizar un análisis y diseño de la red, de esta manera se puede determinar qué tipo de equipos son los adecuados que se adapten a las necesidades del sistema.
- La presente actividad permite la aplicación de los conocimientos adquiridos durante el diplomado, por medio de la herramienta de simulación GNS3 como solución al problema planteado, en la cual dispone de todos los dispositivos requeridos para el desarrollo y configuración adecuada para el diseño de la red; Lo cual es un aprendizaje importante ya que los escenarios estudiados, se presentan en la vida cotidiana.

## REFERENCIAS BIBLIOGRÁFICAS

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

Guía De Actividades Prueba De Habilidades Practicas  
[Https://Static-Course-Assets.S3.Amazonaws.Com/Rse503/Es/Index.Html#3.2](https://Static-Course-Assets.S3.Amazonaws.Com/Rse503/Es/Index.Html#3.2) Laboratorios Smarlab

Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1Im3L74BZ3bpMiXRx0>

Modulo Ccna 2 Exploración 5.0 Cisco  
Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de <http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/> Cisco-ICND2.pdf

Temática: OSPF de una sola área

Temática: Traducción de direcciones IP para IPv4