

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

MANUEL ALBERTO ALDANA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA  
INGENIERIA DE TELECOMUNICACIONES  
BOGOTÁ  
2021

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRACTICAS CCNP

MANUEL ALBERTO ALDANA RODRIGUEZ

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

DIRECTOR:  
MSC. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA  
INGENIERIA DE TELECOMUNICACIONES  
BOGOTÁ  
2021

Nota de Aceptación

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Bogotá (20, noviembre, 2021)

## CONTENIDO

Lista de tablas .....	5
Lista de Figuras .....	6
GLOSARIO.....	8
ABSTRACT .....	9
INTRODUCCIÓN.....	10
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces .....	11
Parte 2: Configurar la capa 2 de la red y el soporte de Host .....	27
Parte 3: Configurar los protocolos de enrutamiento .....	41
Parte 4: Configurar la redundancia del primer salto .....	56
Parte 5: Seguridad.....	66
Parte 6: Configure las funciones de Administración de RED.....	71
CONCLUSIONES .....	80
BIBLIOGRAFIA.....	81

## Lista de tablas

Tabla 1. Tabla de Enrutamiento .....	10
--------------------------------------	----

## Lista de Figuras

Figura 1 Topología modelo para la implementación.....	11
Figura 2 Paso 1 Montaje topología en aplicativo GNS3.....	13
Figura 3 Paso 2 validación configuración R1.....	15
Figura 4 Paso 2 validación configuración R2.....	16
Figura 5 Paso 2 validación configuración R3.....	17
Figura 6 Paso 2 validación configuración D1.....	19
Figura 7 Paso 2 validación configuración D1.....	20
Figura 8 Paso 2 validación configuración D1.....	20
Figura 9 Paso 2 validación configuración D1.....	20
Figura 10 Paso 2 validación configuración D1.....	21
Figura 11 Parte1-Paso 2 validación configuración D2.....	23
Figura 12 Parte 1-Paso 2 validación configuración D2.....	23
Figura 13 Parte 1-Paso 2 validación configuración D2.....	24
Figura 14 Parte 1-Paso 2 validación configuración A1.....	25
Figura 15 Parte 1-Paso 2 configuración IP PC1.....	26
Figura 16 Parte 1-Paso 2 configuración IP PC4.....	26
Figura 17 Parte 2 validación interfaces troncales en D1.....	28
Figura 18 Parte 2 validación interfaces troncales en D1.....	28
Figura 19 Parte2 validación RSTP en D1.....	29
Figura 20 Parte2 validación RSTP en D1.....	29
Figura 21 Parte2 validación RSTP en D1.....	29
Figura 22 Parte2 validación RSTP en D2.....	30
Figura 23 Parte2 validación RSTP en D2.....	31
Figura 24 Parte2 validación RSTP en D2.....	31
Figura 25 Parte2 validación EtherChannel en D1.....	33
Figura 26 Parte2 validación EtherChannel en D2.....	34
Figura 27 Parte2 validación EtherChannel en D2.....	35
Figura 28 Parte2 Validación DHCP PC2.....	37
Figura 29 Parte2 Validación DHCP PC3.....	37
Figura 30 Parte2 Conectividad LAN PC1 D1.....	38
Figura 31 Parte2 Conectividad LAN PC1 hacia D2.....	38
Figura 32 Parte2 Conectividad LAN PC1 hacia PC4.....	38
Figura 33 Parte2 Conectividad LAN PC2 hacia D1.....	39
Figura 34 Parte2 Conectividad LAN PC2 hacia D2.....	39
Figura 35 Parte2 Conectividad LAN PC3 hacia D1.....	39
Figura 36 Parte2 Conectividad LAN PC3 hacia D2.....	39
Figura 37 Parte2 Conectividad LAN PC4 hacia D1.....	40
Figura 38 Parte2 Conectividad LAN PC4 hacia D2.....	40
Figura 39 Parte2 Conectividad LAN PC4 hacia PC1.....	40
Figura 40 Parte 3 Configuración OSPF v2 en R1.....	43
Figura 41 Parte 3 Configuración OSPF v2 en R1.....	43
Figura 42 Parte 3 Configuración OSPF v3 en R1.....	44
Figura 43 Parte 3 Validación OSPF en R1.....	44
Figura 44 Parte 3 Configuración BGP en R1.....	45
Figura 45 Parte 3 Validación BGP en R1.....	46
Figura 46 Parte 3 Configuración rutas estáticas en R2.....	46
Figura 47 Parte 3 Configuración BGP en R2.....	47
Figura 48 Parte 3 Validación BGP en R2.....	48
Figura 49 Parte 3 Validación enrutamiento en R2.....	48
Figura 50 Figura 49 Configuración OSPF v3 en R3.....	49
Figura 51 Validación OSPF v3 en R3.....	50

Figura 52 Validación OSPF v3 en R3 .....	50
Figura 53 Configuración OSPF v2 en D1 .....	51
Figura 54 Configuración OSPF v3 en D1 .....	51
Figura 55 Anuncio de redes OSPF en D1 .....	52
Figura 56 Validación OSPF v3 en D1 .....	52
Figura 57 Validación interfaces OSPF v3 en D1 .....	53
Figura 58 Configuración OSPF v2 en D2 .....	53
Figura 59 Configuración OSPF v3 en D2 .....	54
Figura 60 Anuncio de redes en D2 .....	55
Figura 61 Validación OSPF v3 en D2 .....	55
Figura 62 Validación Interfaces OSPF en D2 .....	55
Figura 63 Validación SLA D1 .....	59
Figura 64 Validación segmentos vlan D2 .....	61
Figura 65 Validación SLA D2 .....	63
Figura 66 Validación paso 4 D1 .....	64
Figura 67 Validación paso 4 D2 .....	65
Figura 68 Configuración SCRYPT D1 .....	66
Figura 69 Configuración SCRYPT D2 .....	66
Figura 70 Configuración SCRYPT A1 .....	67
Figura 71 Configuración SCRYPT R1 .....	67
Figura 72 Configuración SCRYPT R2 .....	67
Figura 73 Configuración SCRYPT R3 .....	67
Figura 74 Validación SCRYPT R3 .....	67
Figura 75 Implementación AAA D1 .....	69
Figura 76 Validación AAA R1 .....	69
Figura 77 Validación AAA R3 .....	69
Figura 78 Loggin verificación D1 .....	70
Figura 79 Validación reloj D1-D2 .....	71
Figura 80 Configuración NTP R2 .....	71
Figura 81 Validación NTP R2 .....	72
Figura 82 Validación NTP R1 .....	73
Figura 83 Syslog R1 .....	73
Figura 84 SNMP R1 .....	74
Figura 85 Sincronización NTP R3 .....	74
Figura 86 Syslog R3 .....	75
Figura 87 SNMP R3 .....	75
Figura 88 Syslog D1 .....	76
Figura 89 SNMP D1 .....	76
Figura 90 SNMP NMS D1 .....	76
Figura 91 Syslog D2 .....	77
Figura 92 SNMP D2 .....	77
Figura 93 SNMP NMS D2 .....	78
Figura 94 Syslog A1 .....	78
Figura 95 SNMP A1 .....	79
Figura 96 SNMP NMS A1 .....	79

## GLOSARIO

**OSPF (Open Shortest Path First):** Protocolo de enrutamiento que funciona a partir del principio de estado de enlace, establece una base de datos de los estados de conexión de la red y por medio del algoritmo Dijkstra y el envío de mensajes tipo "hello" a los routers vecinos se construye la ruta que determina óptima para la transmisión.

**BGP (Border Gateway Protocol):** Protocolo orientado al intercambio de información entre sistemas autónomos para establecer políticas de interconexión, el caso mas concreto de uso es la interacción de los diferentes ISP, los cuales son capaces de realizar intercambio de tablas de enrutamiento por medio de BGP aun cuando en su AS manejen protocolos totalmente diferentes, para su establecimiento se definen las sesiones internas (iBGP) y las sesiones externas (eBGP).

**VLAN:** Se conocen como redes de área local virtuales y permiten la creación de redes lógicas que funcionan de forma independiente dentro de un mismo segmento de red de un conmutador, el uso de estas permite una serie de beneficios en cuanto a temas de seguridad puesto que se pueden establecer parámetros específicos de comunicación, permitiendo o denegando la transmisión, optimización de la red con el uso de subredes y aprovechamiento de los recursos y escalamiento en cuanto a factores de intercambio de estado de la red.

**ETHERCHANNEL:** Corresponde a una tecnología desarrollada por Cisco que permite la agrupación de canales físicos en un único enlace lógico con capacidad de ancho de banda producto de la suma de los enlaces, de igual forma proporciona valores de tolerancia a fallos puesto que puede reajustar los parámetros del enlace si se produce alguna falla en uno de los enlaces físicos que lo componen.

**GNS3:** Es un simulador de redes muy potente y de licencia GNU para distribución gratuita que permite el uso de imágenes preconfiguradas de dispositivos de red para la realización de topologías de red en ambientes simulados, posee integración de máquinas virtuales y acepta un sin fin de sistemas operativos de diferentes fabricantes de dispositivos de res, adicionalmente su instalador es multiplataforma.

## **RESUMEN**

Por medio de la realización de la prueba de habilidades prácticas se aplicaran y representaran los conceptos adquiridos durante el diplomado Cisco CCNP de una forma directa con el desarrollo de un escenario puntual, se entrega una topología de red y una serie de parámetros de configuración en cada uno de los dispositivos para desarrollarse en un total de 6 pasos, para tal fin se utilizara el programa de simulación electrónica GNS3 y una conexión a la tarjeta virtual de red del aplicativo VMWARE, se mostrara un informe detallado de la serie de comandos ingresados en cada dispositivo y las pruebas de funcionamiento por medio de capturas de pantalla, se abordan temas de configuración de interfaces, creación de VLANs, segmentación de red, protocolos de enrutamiento y conmutación, parámetros de seguridad, acuerdos a nivel de servicio, y configuración de administración de la red.

Palabras clave: Cisco, CCNP, Enrutamiento, Conmutación, Redes, Electrónica.

## **ABSTRACT**

Through the realization of the practical skills test, the concepts acquired during the Cisco CCNP course will be applied in a direct way with the development of a specific scenario, a network topology and a series of configuration parameters are delivered in each of the devices to be developed in a total of 6 steps, for this purpose the GNS3 electronics simulation program and a connection to the virtual network card of the VMWARE application will be used, a detailed report of the series of commands entered in each device and performance tests by means of screenshots, Interface configuration, VLAN creation, network segmentation, routing and switching protocols, security parameters, service level agreements, and network management configuration are covered.

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

## INTRODUCCIÓN

Por medio del diplomado CCNP se adquiere una serie de conocimientos enfocados a fortalecer las competencias en el campo de la administración y configuración de dispositivos de red en el área de las telecomunicaciones, esto permite un mejor desenvolvimiento como profesional dado que en la prueba de habilidades prácticas se abordarán una serie de conceptos que son de vital importancia en nuestro sector laboral conforme a la demanda actual.

En el trabajo presentado a continuación se desarrollarán un total de 6 pasos orientados a completar el escenario propuesto, en una primera instancia se realizará la configuración básica de los dispositivos y el direccionamiento de sus interfaces validando cada uno de los componentes y dispositivos de la Topología dispuesta, después se procederá a realizar configuraciones de capa 2 para interacción de los switch y validación del correcto funcionamiento de la capa de red y soporte de host donde cada uno de los switch debe ser capaz de entregar servicios de DHCP y SLAAC a los PC clientes según corresponda esto con el fin de poder establecer la parametrización correcta de los protocolos de enrutamiento a trabajar que para nuestro escenario serán OSPF y BGP bajo la premisa de una red de sistema autónoma conectada hacia una red ISP permitiéndola interacción total de los dispositivos y brindando accesibilidad completa de extremo a extremo, por medio de HSRP se configuran aspectos de redundancia y monitoreo de estados de enlace mediante rastreo de objetos y ANS (acuerdos a nivel servicio), finalmente se establecen parámetros de seguridad para autenticación de usuarios en cada uno de los dispositivos y aspectos de administración como sincronización de zonas horarias entre otros.

Finalmente se entrega un informe detallado con los 6 pasos del escenario, donde se detalla paso a paso el proceso de configuración, las líneas de comandos aplicadas y las validaciones realizadas en cada uno de los dispositivos por medio de la ejecución de pruebas de conexión, establecimiento de servicio y respuesta de las interfaces configuradas.

## 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.

Para el montaje de la topología se utilizó las imágenes para los equipos Cisco L2 y L3 para el aplicativo GNS3. Se realiza redistribución de puertos conforme a los disponibles en las imágenes de los equipos a utilizar conforme a la siguiente topología.

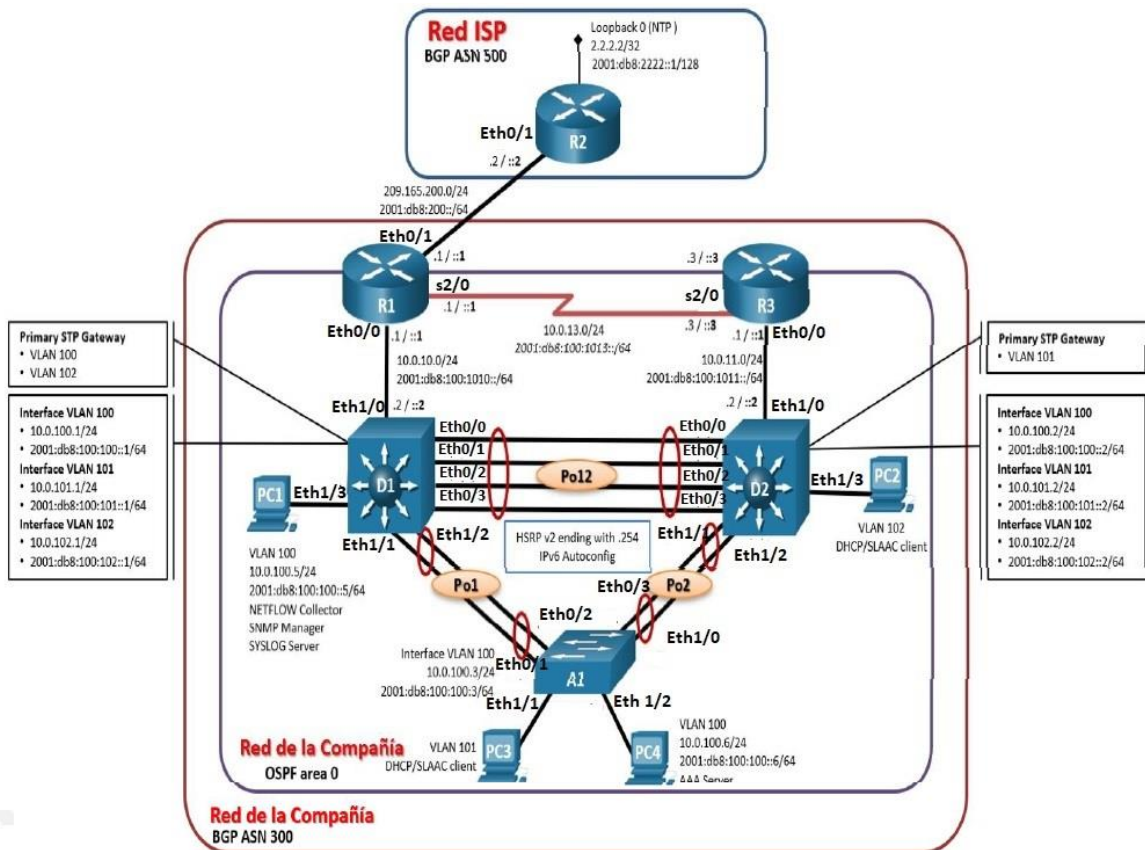


Figura 1 Topología modelo para la implementación.

**Tabla de enrutamiento.**

Dispositivo	Interfaz	Direccion IPv4	Direccion IPv6	Ipv6 Link-Local
R1	Eth0/1	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	Eth0/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	Eth0/1	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	Eth0/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	ETH1/0	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	ETH1/0	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

Montaje de la Topología propuesta mediante el aplicativo GNS3 y soporte de imágenes IOS de los dispositivos con VMWARE Workstation.

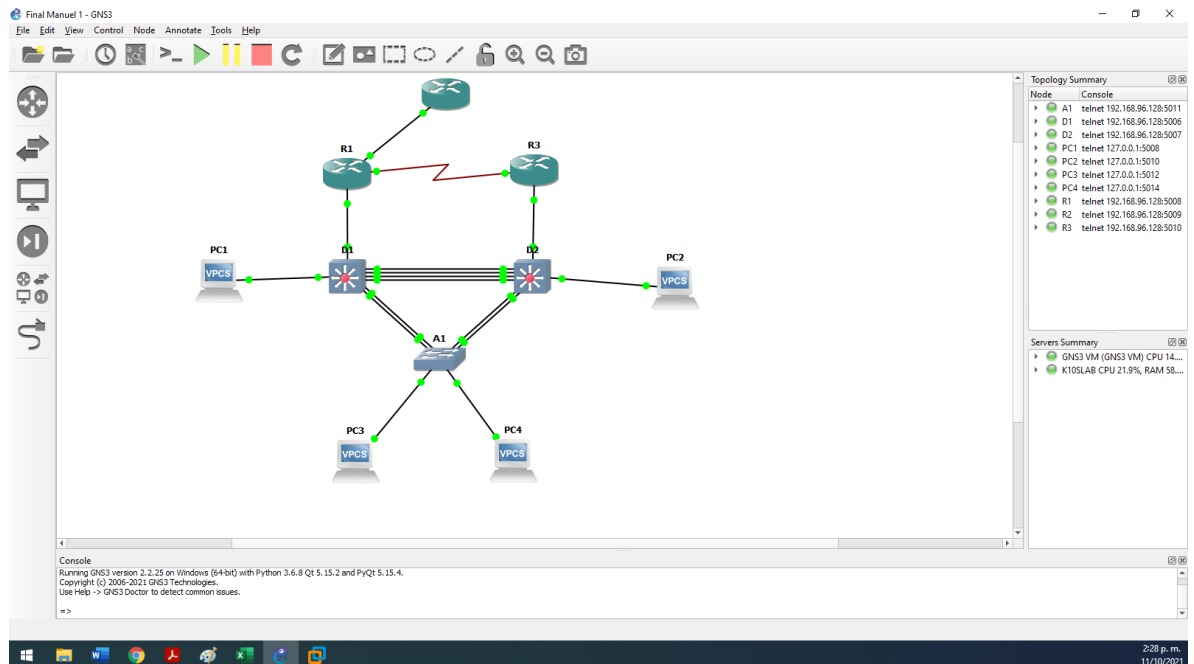


Figura 2 Paso 1 Montaje topología en aplicativo GNS3

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

### Configuraciones básicas en los router.

En los routers (R1,R2,R3) Se realiza configuración de única difusión por medio de protocolo ipv6, desactivación de la traducción de nombres del dispositivo lo cual evita problemas y traumatismos en los tiempos de configuración al momento de ingresar por error líneas de comando incorrectas, parametrización de direccionamiento en las interfaces de tal forma que se configure IPv4, IPv6 y la dirección IPv6 Link local para cada interfaz.

### **Comandos utilizados en R1**

```
hostname R1
ipv6 unicast-routing
no ip domain lookup
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface Eth0/1
ip address 209.165.200.225 255.255.255.224
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64
no shutdown
exit
interface Eth0/0
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s2/0
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
```

### **Validación configuración ingresada R1**

Comando utilizado: # Show ip interface brief

Este comando nos permite obtener un resumen de las interfaces del router, detallando información parametrizada como direccionamiento ip en cada interfaz y el estado de estas.

```
R1 - PuTTY
R1(config)#exit
R1#show
*Oct 11 19:38:44.816: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip interf
R1#show ip interface brief
Interface                IP-Address      OK? Method Status      Prot
ocol
Ethernet0/0              10.0.10.1       YES manual up          up
Ethernet0/1              209.165.200.225 YES manual up          up
Ethernet0/2              unassigned      YES NVRAM  administratively down down
Ethernet0/3              unassigned      YES NVRAM  administratively down down
Ethernet1/0              unassigned      YES NVRAM  administratively down down
Ethernet1/1              unassigned      YES NVRAM  administratively down down
Ethernet1/2              unassigned      YES NVRAM  administratively down down
Ethernet1/3              unassigned      YES NVRAM  administratively down down
Serial2/0                10.0.13.1       YES manual up          up
```

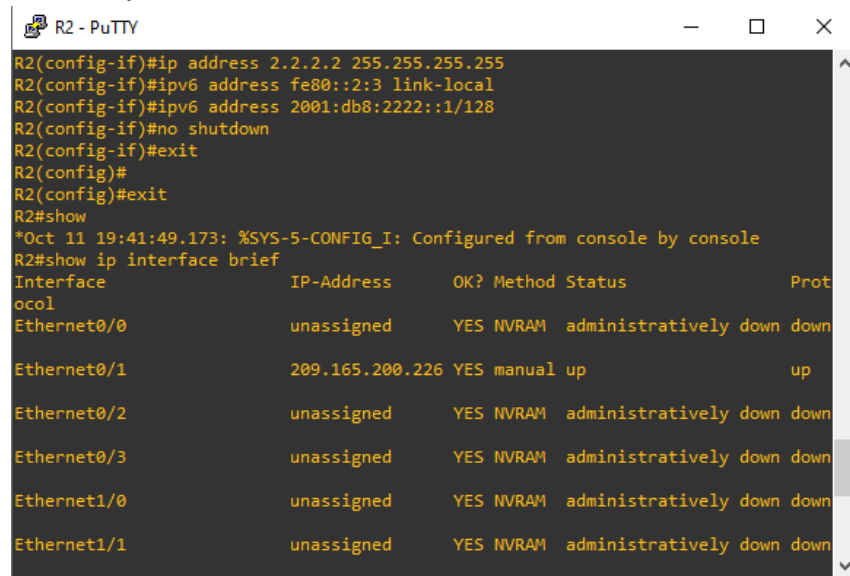
Figura 3 Paso 2 validación configuración R1

### Comandos utilizados en 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 Eth0/1
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
```

## Validación configuración ingresada R2

Comando: # Show ip interface brief



```
R2 - PuTTY
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#exit
R2#show
*Oct 11 19:41:49.173: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip interface brief
Interface                IP-Address      OK? Method Status        Prot
ocol
Ethernet0/0              unassigned     YES NVRAM   administratively down down
Ethernet0/1              209.165.200.226 YES manual   up            up
Ethernet0/2              unassigned     YES NVRAM   administratively down down
Ethernet0/3              unassigned     YES NVRAM   administratively down down
Ethernet1/0              unassigned     YES NVRAM   administratively down down
Ethernet1/1              unassigned     YES NVRAM   administratively down down
```

Figura 4 Paso 2 validación configuración R2

## Comandos utilizados en 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 Eth0/0

ip address 10.0.11.1 255.255.255.0

ipv6 address fe80::3:2 link-local

ipv6 address 2001:db8:100:1011::1/64

no shutdown

exit

interface s2/0

ip address 10.0.13.3 255.255.255.0

ipv6 address fe80::3:3 link-local

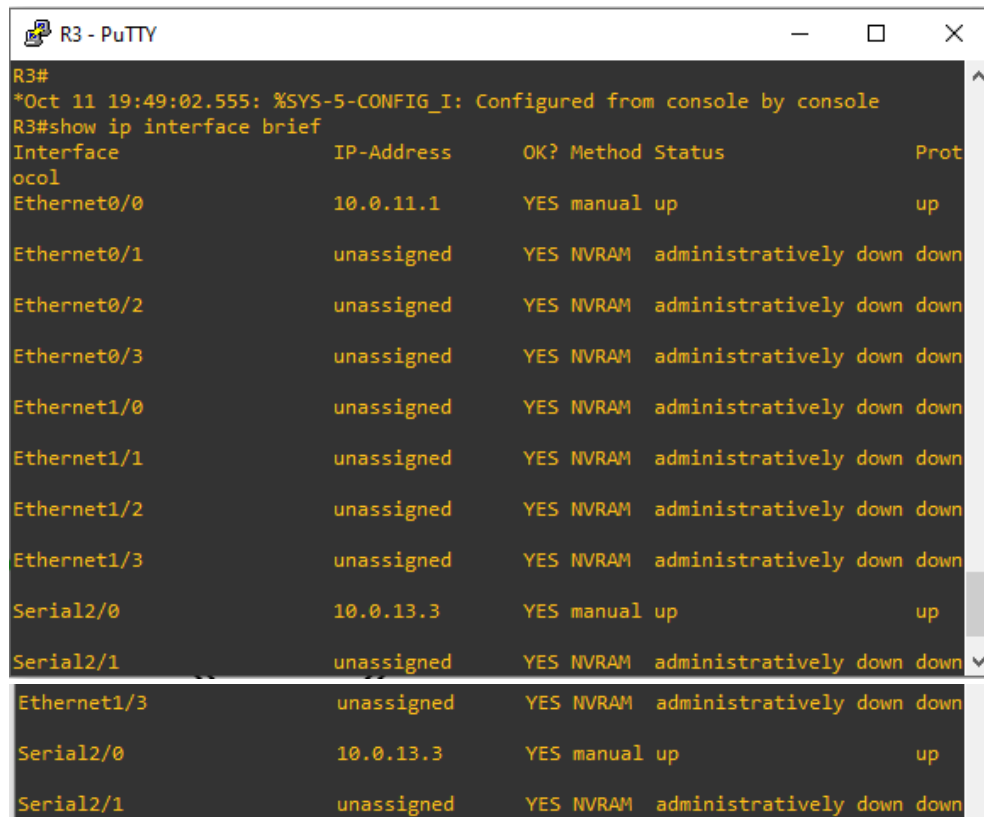
ipv6 address 2001:db8:100:1010::2/64

no shutdown

exit

## Validación configuración ingresada R3

Comando: # Show ip interface brief



```
R3#
*Oct 11 19:49:02.555: %SYS-5-CONFIG_I: Configured from console by console
R3#show ip interface brief
Interface                IP-Address      OK? Method Status      Prot
ocol
Ethernet0/0              10.0.11.1       YES manual up          up
Ethernet0/1              unassigned      YES NVRAM  administratively down down
Ethernet0/2              unassigned      YES NVRAM  administratively down down
Ethernet0/3              unassigned      YES NVRAM  administratively down down
Ethernet1/0              unassigned      YES NVRAM  administratively down down
Ethernet1/1              unassigned      YES NVRAM  administratively down down
Ethernet1/2              unassigned      YES NVRAM  administratively down down
Ethernet1/3              unassigned      YES NVRAM  administratively down down
Serial2/0                 10.0.13.3       YES manual up          up
Serial2/1                 unassigned      YES NVRAM  administratively down down
Ethernet1/3              unassigned      YES NVRAM  administratively down down
Serial2/0                 10.0.13.3       YES manual up          up
Serial2/1                 unassigned      YES NVRAM  administratively down down
```

Figura 5 Paso 2 validación configuración R3

## Configuraciones básicas para los Switch

Se realiza configuración de única difusión por medio de protocolo ipv6, desactivación de la traducción de nombres del dispositivo, creación de VLANs conforme a lo establecido en los lineamientos del escenario (vlan 100, vlan 101, vlan 102) y su respectiva configuración de interfaces con parametrización IPv4, IPv6 y exclusión de direcciones ip.

### Comandos utilizados en 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
```

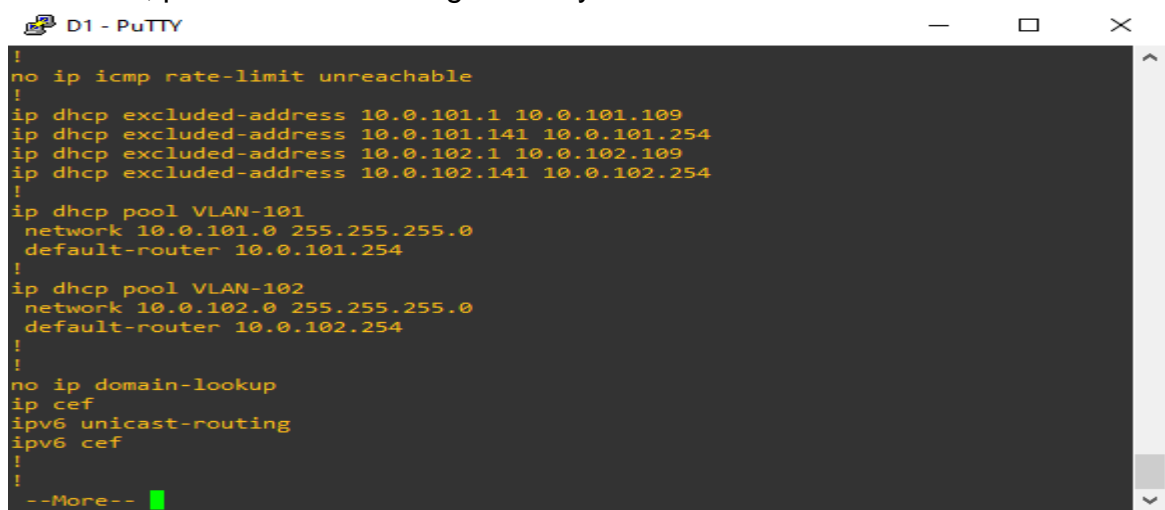
```
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface Eth1/0
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
```

```
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range Eth0/0-3 Eth2/0-3
shutdown
exit
```

### Validaciones en D1

Comando: #Show running-config

Este comando permite visualizar información general completa de la terminal como versiones, parámetros de configuración y direccionamiento de interfaces.



```
D1 - PuTTY
!
no ip icmp rate-limit unreachable
!
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
!
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
!
!
no ip domain-lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
--More--
```

Figura 6 Paso 2 validación configuración D1

```

D1 - PuTTY
shutdown
!
interface Ethernet0/3
shutdown
!
interface Ethernet1/0
no switchport
ip address 10.0.10.2 255.255.255.0
duplex auto
ipv6 address FE80::D1:1 link-local
ipv6 address 2001:DB8:100:1010::2/64
!
interface Ethernet1/1

```

Figura 7 Paso 2 validación configuración D1

```

D1 - PuTTY
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
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
!
interface Vlan101
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
!
interface Vlan102
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
!
ip forward-protocol nd
!
!
no ip http server

```

Figura 8 Paso 2 validación configuración D1

Comando: #show vlan brief

Este comando visualiza la asignación de puertos conforme a las vlan creadas y al conjunto de subredes ip configuradas.

```

D1 - PuTTY
!
end
D1#
D1#
D1#
D1#
D1#show vlan brief

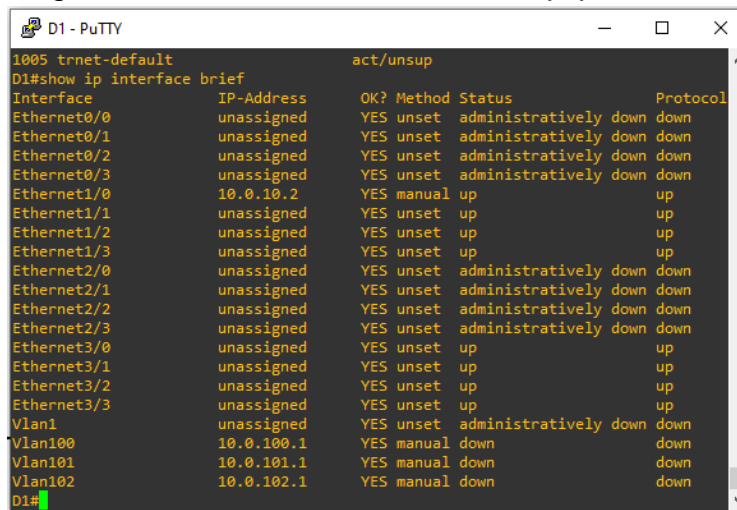
VLAN Name                Status    Ports
-----
1    default                 active    Et0/0, Et0/1, Et0/2, Et0/3
                                           Et1/1, Et1/2, Et1/3, Et2/0
                                           Et2/1, Et2/2, Et2/3, Et3/0
                                           Et3/1, Et3/2, Et3/3
100  Management              active
101  UserGroupA              active
102  UserGroupB              active
999  NATIVE                  active
1002 fddi-default            act/unsup
1003 token-ring-default     act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup
D1#

```

Figura 9 Paso 2 validación configuración D1

Comando: #show ip interface brief

Resumen de configuración en las interfaces de los equipos.



```
D1 - PuTTY
1005 trnet-default act/unsup
D1#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
Ethernet0/0        unassigned      YES unset  administratively down  down
Ethernet0/1        unassigned      YES unset  administratively down  down
Ethernet0/2        unassigned      YES unset  administratively down  down
Ethernet0/3        unassigned      YES unset  administratively down  down
Ethernet1/0        10.0.10.2       YES manual  up              up
Ethernet1/1        unassigned      YES unset  up              up
Ethernet1/2        unassigned      YES unset  up              up
Ethernet1/3        unassigned      YES unset  up              up
Ethernet2/0        unassigned      YES unset  administratively down  down
Ethernet2/1        unassigned      YES unset  administratively down  down
Ethernet2/2        unassigned      YES unset  administratively down  down
Ethernet2/3        unassigned      YES unset  administratively down  down
Ethernet3/0        unassigned      YES unset  up              up
Ethernet3/1        unassigned      YES unset  up              up
Ethernet3/2        unassigned      YES unset  up              up
Ethernet3/3        unassigned      YES unset  up              up
Vlan1              unassigned      YES unset  administratively down  down
Vlan100            10.0.100.1      YES manual  down            down
Vlan101            10.0.101.1      YES manual  down            down
Vlan102            10.0.102.1      YES manual  down            down
D1#
```

Figura 10 Paso 2 validación configuración D1

### Comandos utilizados en 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 Eth1/0

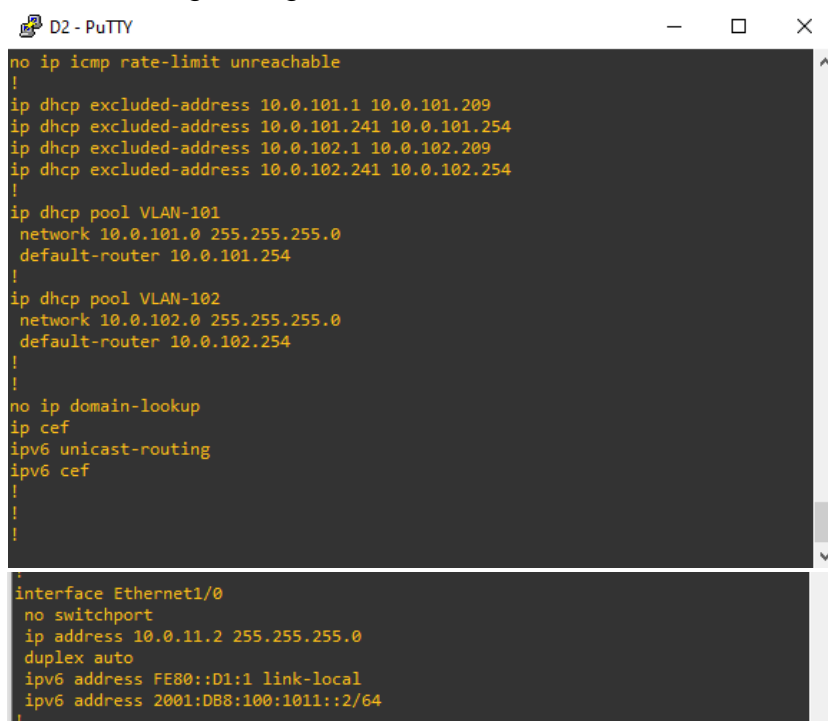
```

no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range Eth2/0-3
shutdown
exit

```

## Validaciones en D2

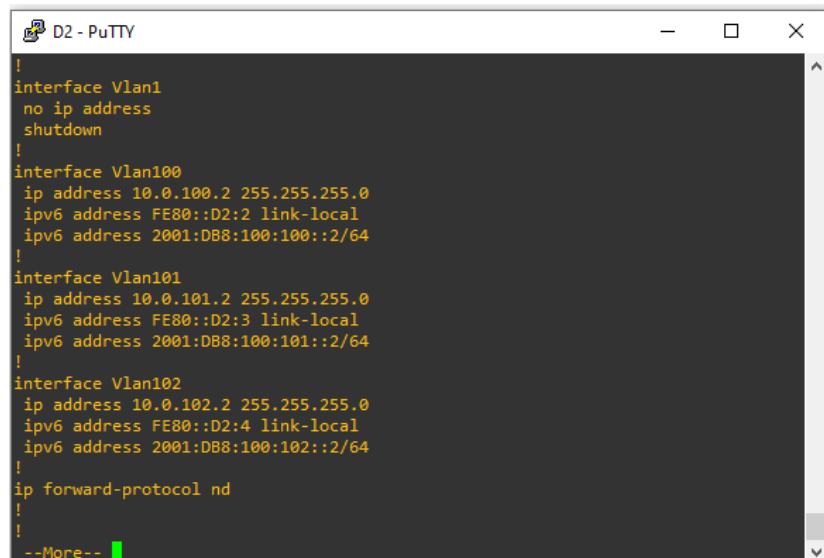
Comando: #Show running-config



```
D2 - PuTTY
no ip icmp rate-limit unreachable
!
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
!
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
!
!
no ip domain-lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
!
!

interface Ethernet1/0
no switchport
ip address 10.0.11.2 255.255.255.0
duplex auto
ipv6 address FE80::D1:1 link-local
ipv6 address 2001:DB8:100:1011::2/64
!
```

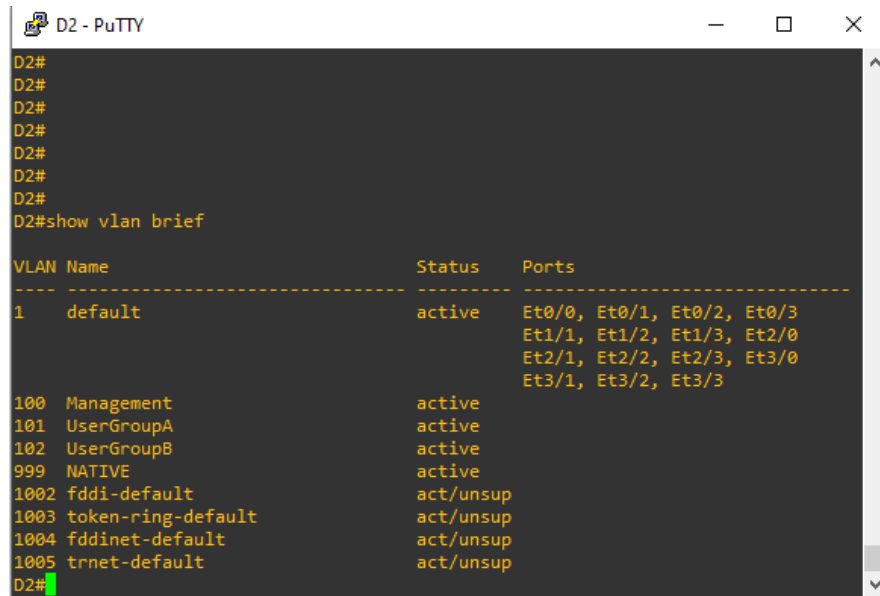
Figura 11 Parte1-Paso 2 validación configuración D2



```
D2 - PuTTY
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
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
!
interface Vlan101
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
!
interface Vlan102
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
!
ip forward-protocol nd
!
!
--More--
```

Figura 12 Parte 1-Paso 2 validación configuración D2

Comando: #show vlan brief



```
D2#
D2#
D2#
D2#
D2#
D2#
D2#
D2#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Et0/0, Et0/1, Et0/2, Et0/3
                                           Et1/1, Et1/2, Et1/3, Et2/0
                                           Et2/1, Et2/2, Et2/3, Et3/0
                                           Et3/1, Et3/2, Et3/3
100  Management              active
101  UserGroupA              active
102  UserGroupB              active
999  NATIVE                   active
1002 fddi-default             act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default         act/unsup
1005 trnet-default         act/unsup
D2#
```

Figura 13 Parte 1-Paso 2 validación configuración D2

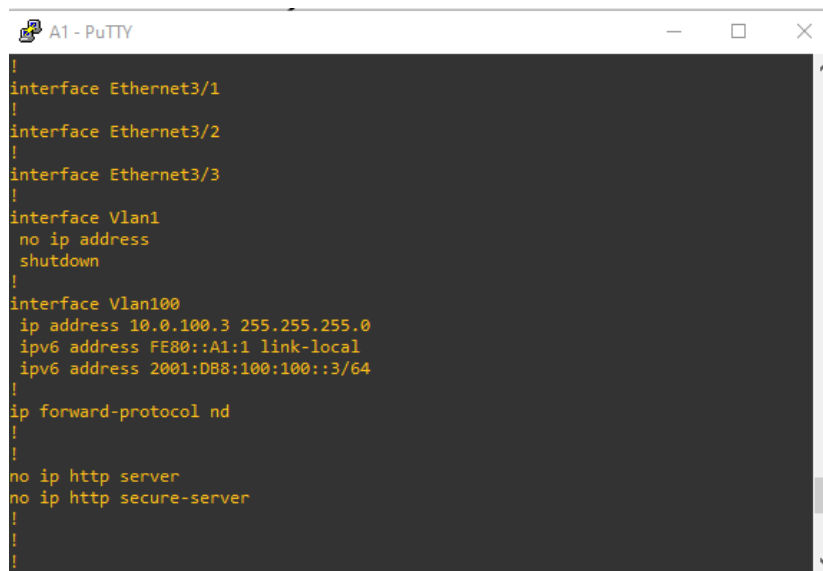
### Comandos utilizados en Switch A1

```
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 eth2/0-3
shutdown
exit
```

## Validaciones en A1

```
#show running-config
```



```
A1 - PuTTY
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
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
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
```

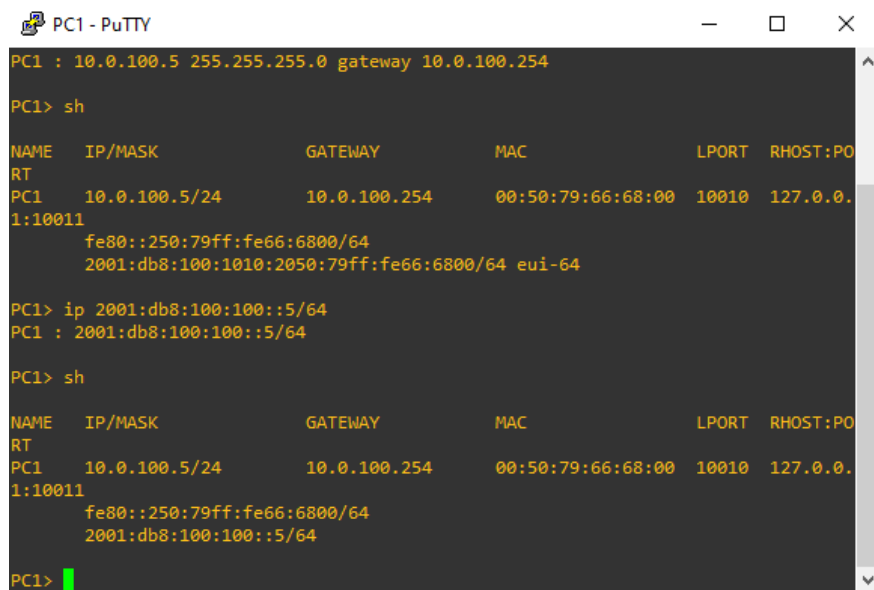
Figura 14 Parte 1-Paso 2 validación configuración A1

## Configuración equipos PC1

Comandos en terminal PC1:

```
Ip 10.0.100.5 255.255.255.0 10.0.100.254
ip 2001:db8:100:100::5/64
```

## Verificación, comando sh Terminal PC1



```
PC1 - PuTTY
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
RT
PC1 10.0.100.5/24 10.0.100.254 00:50:79:66:68:00 10010 127.0.0.1:10011
fe80::250:79ff:fe66:6800/64
2001:db8:100:1010:2050:79ff:fe66:6800/64 eui-64

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

PC1> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
RT
PC1 10.0.100.5/24 10.0.100.254 00:50:79:66:68:00 10010 127.0.0.1:10011
fe80::250:79ff:fe66:6800/64
2001:db8:100:100::5/64

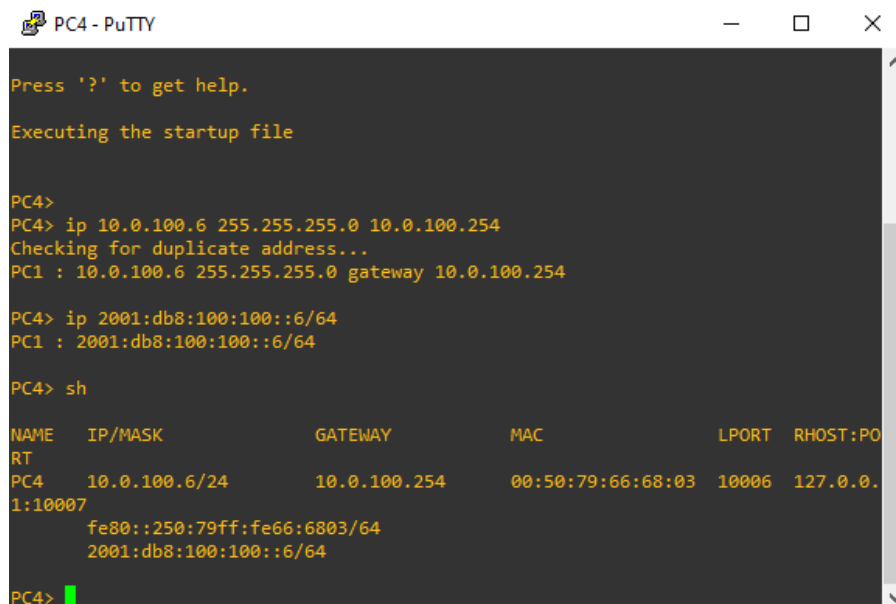
PC1>
```

Figura 15 Parte 1-Paso 2 configuración IP PC1

## Configuración equipos PC4

Ip 10.0.100.6 255.255.255.0 10.0.100.254

ip 2001:db8:100:100::6/64



```
PC4 - PuTTY

Press '?' to get help.
Executing the startup file

PC4>
PC4> ip 10.0.100.6 255.255.255.0 10.0.100.254
Checking for duplicate address...
PC1 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> ip 2001:db8:100:100::6/64
PC1 : 2001:db8:100:100::6/64

PC4> sh

NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
RT
PC4 10.0.100.6/24 10.0.100.254 00:50:79:66:68:03 10006 127.0.0.1:10007
fe80::250:79ff:fe66:6803/64
2001:db8:100:100::6/64

PC4>
```

Figura 16 Parte 1-Paso 2 configuración IP PC4

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

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

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

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).

Se procede a parametrizar el protocolo de encapsulamiento **IEEE 802.1q** el cual permite la interacción de diversas redes por un mismo medio físico, de igual manera se realiza la configuración del protocolo **RSTP** en busca de obtener un mejor tiempo de respuesta para enlace de convergencia de la Topología de red.

### Configuración en D1

Comandos utilizados en D1:

Enable

Config t

spanning-tree mode rapid-pvst

spanning-tree vlan 100 root primary

spanning-tree vlan 102 root primary

spanning-tree vlan 101 root secondary

exit

interface range Eth0/0-3, Eth1/1-2

switchport trunk encapsulation dot1q

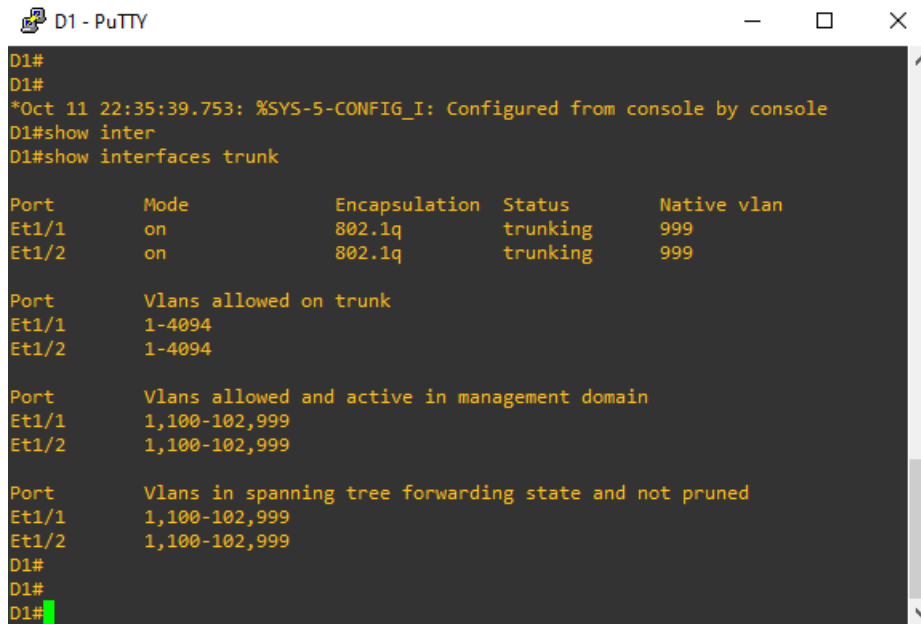
switchport mode trunk

switchport trunk native vlan 999

## Validaciones en D1

Comando: show interfaces trunk

interfaces troncales, modo de encapsulación y vlan nativa D1.



```
D1#
D1#
*Oct 11 22:35:39.753: %SYS-5-CONFIG_I: Configured from console by console
D1#show inter
D1#show interfaces trunk

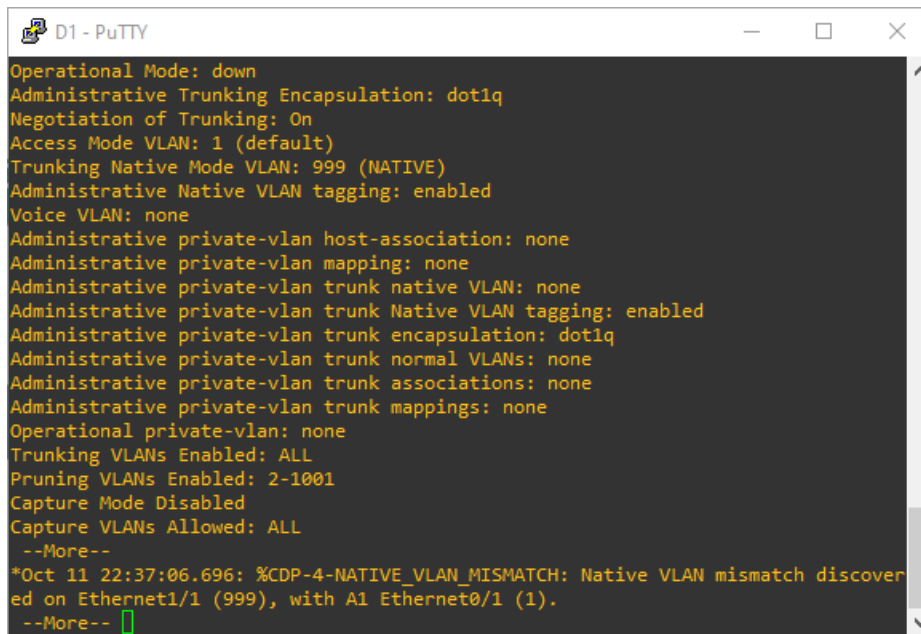
Port      Mode           Encapsulation  Status        Native vlan
Et1/1     on             802.1q         trunking      999
Et1/2     on             802.1q         trunking      999

Port      Vlans allowed on trunk
Et1/1     1-4094
Et1/2     1-4094

Port      Vlans allowed and active in management domain
Et1/1     1,100-102,999
Et1/2     1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Et1/1     1,100-102,999
Et1/2     1,100-102,999
D1#
D1#
D1#
```

Figura 17 Parte 2 validación interfaces troncales en D1



```
D1#
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 999 (NATIVE)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
--More--
*Oct 11 22:37:06.696: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet0/1 (1).
--More--
```

Figura 18 Parte 2 validación interfaces troncales en D1

Validación protocolo rapid spanning tree en D1  
 Comando: show spanning-tree

```

D1 - PuTTY
Et3/3          Desg FWD 100      128.16 Shr

VLAN0100
Spanning tree enabled protocol rstp
Root ID      Priority    24676
             Address    aabb.cc00.0100
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority    24676 (priority 24576 sys-id-ext 100)
             Address    aabb.cc00.0100
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300 sec

Interface    Role Sts Cost      Prio.Nbr Type
-----
Et1/1        Desg FWD 100      128.6 Shr
Et1/2        Desg FWD 100      128.7 Shr

--More--
  
```

Figura 19 Parte2 validación RSTP en D1

```

*Oct 11 22:38:55.780: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discover
ed on Ethernet1/1 (999), with A1 Ethernet0/1 (1).
VLAN0101
Spanning tree enabled protocol rstp
Root ID      Priority    28773
             Address    aabb.cc00.0100
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority    28773 (priority 28672 sys-id-ext 101)
             Address    aabb.cc00.0100
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300 sec

Interface    Role Sts Cost      Prio.Nbr Type
-----
  
```

Figura 20 Parte2 validación RSTP en D1

```

VLAN0102
Spanning tree enabled protocol rstp
Root ID      Priority    24678
             Address    aabb.cc00.0100
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority    24678 (priority 24576 sys-id-ext 102)
             Address    aabb.cc00.0100
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
             Aging Time 300 sec

Interface    Role Sts Cost      Prio.Nbr Type
-----
Et1/1        Desg FWD 100      128.6 Shr
Et1/2        Desg FWD 100      128.7 Shr
  
```

Figura 21 Parte2 validación RSTP en D1

## Configuración en D2

Comandos utilizados:

Enable

Config t

spanning-tree mode rapid-pvst

spanning-tree vlan 101 root primary

spanning-tree vlan 100,102 root secondary

interface range Eth0/0-3, Eth1/1-2

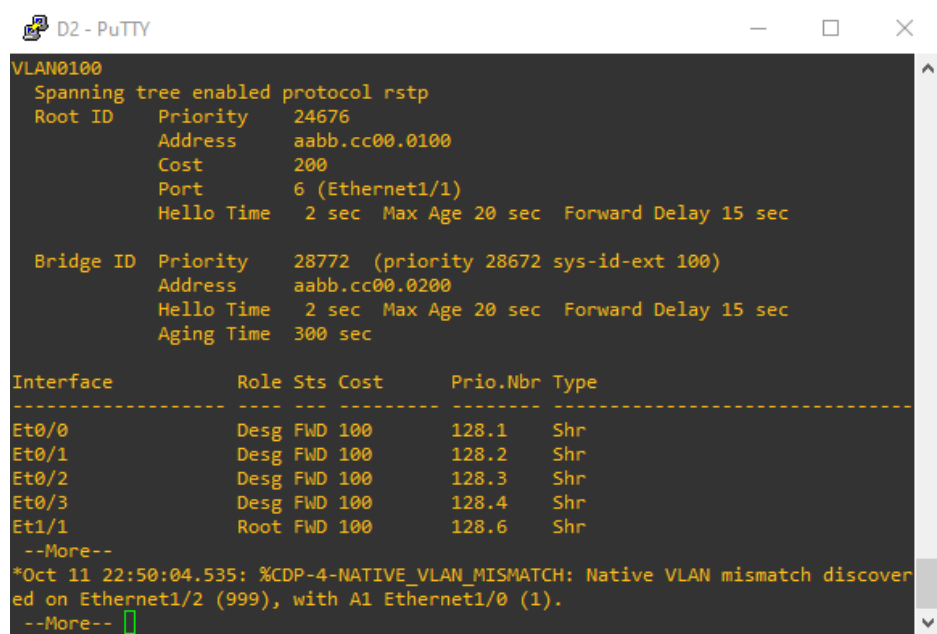
switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk native vlan 999

## Validación de configuración en D2

Comando: show spanning-tree



```
D2 - PuTTY
VLAN0100
Spanning tree enabled protocol rstp
Root ID    Priority    24676
Address    aabb.cc00.0100
Cost       200
Port       6 (Ethernet1/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    28772 (priority 28672 sys-id-ext 100)
Address    aabb.cc00.0200
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Et0/0          Desg FWD 100       128.1   Shr
Et0/1          Desg FWD 100       128.2   Shr
Et0/2          Desg FWD 100       128.3   Shr
Et0/3          Desg FWD 100       128.4   Shr
Et1/1          Root FWD 100       128.6   Shr
--More--
*Oct 11 22:50:04.535: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered
on Ethernet1/2 (999), with A1 Ethernet1/0 (1).
--More--
```

Figura 22 Parte2 validación RSTP en D2

```

VLAN0101
Spanning tree enabled protocol rstp
Root ID    Priority    24677
           Address    aabb.cc00.0200
           This bridge is the root
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    24677 (priority 24576 sys-id-ext 101)
           Address    aabb.cc00.0200
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300 sec

--More--
*Oct 11 22:50:35.342: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/1 (999), with A1 Ethernet0/3 (1).

```

Figura 23 Parte2 validación RSTP en D2

```

VLAN0102
Spanning tree enabled protocol rstp
Root ID    Priority    24678
           Address    aabb.cc00.0100
           Cost        200
           Port        6 (Ethernet1/1)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    28774 (priority 28672 sys-id-ext 102)
           Address    aabb.cc00.0200
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Et0/0          Desg FWD 100       128.1   Shr
Et0/1          Desg FWD 100       128.2   Shr
Et0/2          Desg FWD 100       128.3   Shr
Et0/3          Desg FWD 100       128.4   Shr

--More--
*Oct 11 22:50:58.347: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on Ethernet1/2 (999), with A1 Ethernet1/0 (1).

```

Figura 24 Parte2 validación RSTP en D2

## Configuración en A1

Comandos utilizados:

Enable

Config t

spanning-tree mode rapid-pvst

interface range Eth0/1-3, Eth1/0

switchport mode trunk

switchport trunk native vlan 999

## **2.5 En todos los switches, cree EtherChannel LACP como se muestra en el diagrama de topología.**

La creación de EtherChannel en nuestra Topología nos permite agrupar una serie de enlaces físicos entre los Switch en un solo enlace lógico con el fin de permitir una velocidad de transmisión mayor, para este caso se utiliza el protocolo de negociación LACP (Link aggregation control protocol) el cual es de uso libre y registrado bajo la IEEE.

Creacion PortChannel #12 y #1 en switch D1

### **Configuración portchannel 12 D1**

```
Enable
Config t
Interface range Eth0/0-3
Switchport mode trunk
channel-protocol LACP
channel-group 12 mode active
no shutdown
exit
```

### **Configuración portchannel 1 D1**

```
Interface range Eth1/1-2
Switchport mode trunk
channel-protocol LACP
channel-group 1 mode active
no shutdown
exit
```

### **Validacion EtherChannel creados en D1**

Comando: show Etherchannel



```
Channel-group listing:
-----
Group: 1
-----
Group state = L2
Ports: 2  Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:  LACP
Minimum Links: 0

Group: 12
-----
Group state = L2
Ports: 4  Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:  LACP
Minimum Links: 0

D1#
```

Figura 25 Parte2 validación EtherChannel en D1

Creacion PortChannel #12 y #2 en switch D2

### **Configuración port channel 12 en D2**

Config t

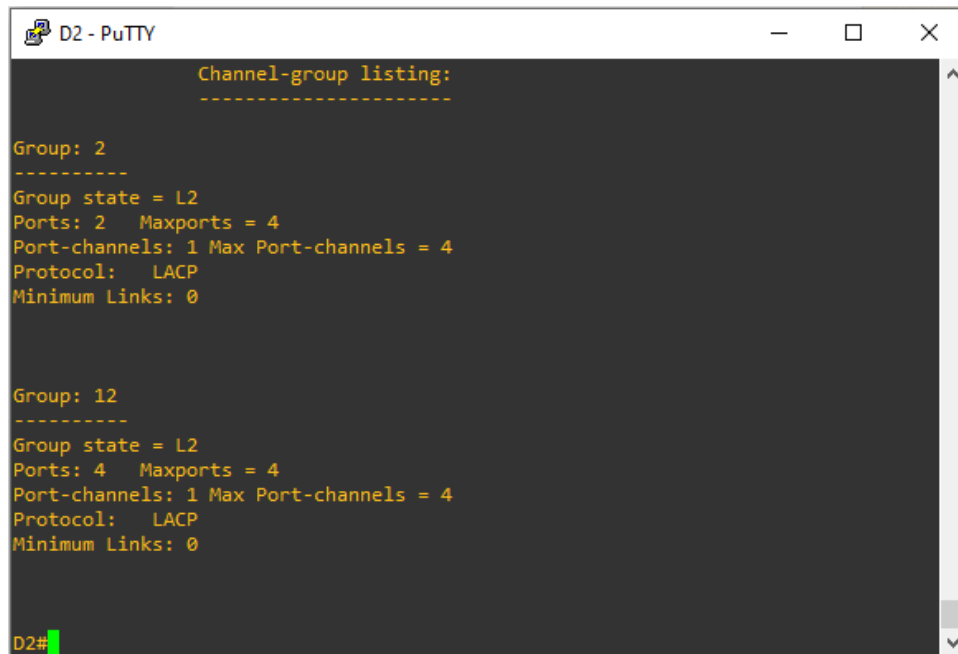
```
interface range Eth0/0-3
channel-protocol LACP
channel-group 12 mode passive
no shutdown
exit
```

### **Configuración portchannel 2 D2**

```
Interface range Eth1/1-2
Switchport mode trunk
channel-protocol LACP
channel-group 2 mode active
no shutdown
exit
```

## Validación EtherChannel creados en D2

Comando: show EtherChannel



```
D2 - PuTTY
Channel-group listing:
-----
Group: 2
-----
Group state = L2
Ports: 2   Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:  LACP
Minimum Links: 0

Group: 12
-----
Group state = L2
Ports: 4   Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:  LACP
Minimum Links: 0

D2#
```

Figura 26 Parte2 validación EtherChannel en D2

Creacion PortChannel #1 y #2 en switch A1

### Configuración portchannel 1 A1

```
Interface range Eth0/1-2
Switchport mode trunk
channel-protocol LACP
channel-group 1 mode passive
no shutdown
exit
```

### Configuración portchannel 2 A1

```
Interface range Eth0/3, Eth1/0
Switchport mode trunk
channel-protocol LACP
channel-group 2 mode passive
no shutdown
exit
```

## Validación Etherchannels creados en A1

Comando: show EtherChannel



```
A1 - PuTTY
Channel-group listing:
-----
Group: 1
-----
Group state = L2
Ports: 2  Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:  LACP
Minimum Links: 0

Group: 2
-----
Group state = L2
Ports: 2  Maxports = 4
Port-channels: 1 Max Port-channels = 4
Protocol:  LACP
Minimum Links: 0

A1#
```

Figura 27 Parte2 validación EtherChannel en D2

### 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.

Se realiza configuración de puertos de acceso para las conexiones que tienen como equipo final dispositivos PC dando permisos de acceso por medio de las vlan correspondientes, de igual forma por medio del comando spanning-tree portfast se permite acceso directo a la red de capa 2 a los equipos finales desde el estado forwarding.

#### Comandos utilizados en D1

```
Enable
Config t
interface Eth1/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
```

### **Comandos utilizados en D2**

```
Enable
Config t
interface Eth1/3
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
```

### **Comandos utilizados en A1**

```
Enable
Config t
interface Eth1/1
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
interface Eth1/2
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
```

### **2.7 Verifique los servicios DHCP IPv4.**

#### **validación de correcto direccionamiento Dhcp desde PC2**

Comando para asignación ip: Ip dhcp

```
PC2 - PuTTY
PC2> ip dhcp
DDORA IP 10.0.102.210/24 GW 10.0.102.254
PC2> sh
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC2      10.0.102.210/24  10.0.102.254  00:50:79:66:68:01  10006  127.0.0.
1:10007
          fe80::250:79ff:fe66:6801/64
          2001:db8:100:102:2050:79ff:fe66:6801/64 eui-64
PC2>
```

Figura 28 Parte2 Validación DHCP PC2

### Validación de correcto direccionamiento Dhcp desde PC3

Comando para asignación ip: Ip dhcp

Comando validación: sh

```
PC3 - PuTTY
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

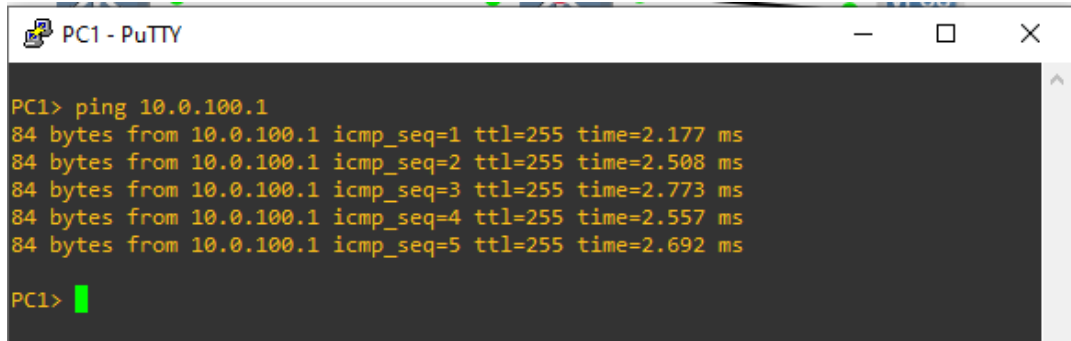
PC3>
PC3> ip dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254
PC3> sh
NAME      IP/MASK      GATEWAY      MAC          LPORT  RHOST:PO
RT
PC3      10.0.101.210/24  10.0.101.254  00:50:79:66:68:02  10008  127.0.0.
1:10009
          fe80::250:79ff:fe66:6802/64
          2001:db8:100:101:2050:79ff:fe66:6802/64 eui-64
PC3>
```

Figura 29 Parte2 Validación DHCP PC3

## 2.8 Verifique la conectividad de la LAN local

### Validaciones de conectividad desde PC1

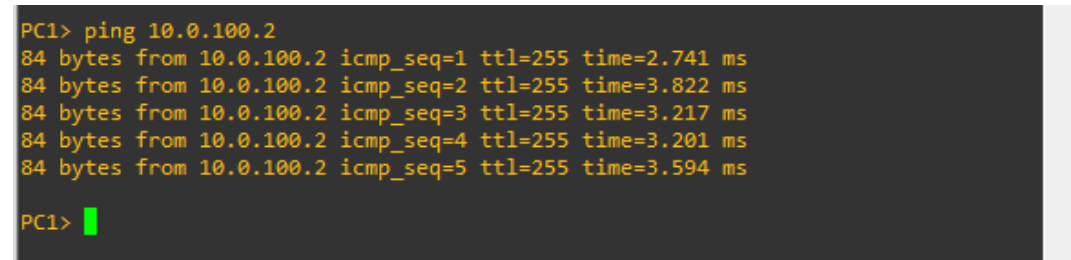
Ping hacia D1 IP 10.0.100.1



```
PC1 - PuTTY
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=2.177 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=2.508 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=2.773 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=2.557 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=2.692 ms
PC1>
```

Figura 30 Parte2 Conectividad LAN PC1 D1

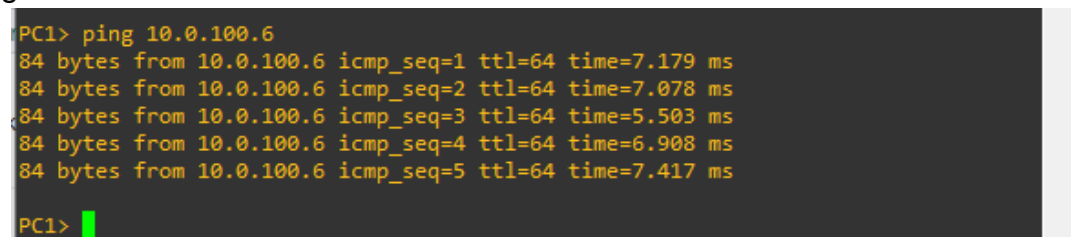
Ping hacia D2 IP 10.0.100.2



```
PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=2.741 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=3.822 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=3.217 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=3.201 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=3.594 ms
PC1>
```

Figura 31 Parte2 Conectividad LAN PC1 hacia D2

Ping hacia PC4 IP 10.0.100.6



```
PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=7.179 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=7.078 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=5.503 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=6.908 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=7.417 ms
PC1>
```

Figura 32 Parte2 Conectividad LAN PC1 hacia PC4

## Validaciones de conectividad desde PC2

Ping hacia D1 IP 10.0.102.1

```
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=3.444 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=3.419 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=3.698 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=3.696 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=3.926 ms
PC2> █
```

Figura 33 Parte2 Conectividad LAN PC2 hacia D1

Ping hacia D2 IP 10.0.102.2

```
PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=2.511 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=3.491 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=2.854 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=2.604 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=3.069 ms
PC2> █
```

Figura 34 Parte2 Conectividad LAN PC2 hacia D2

## Validaciones de conectividad desde PC3

Ping hacia D1 IP 10.0.101.1

```
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=4.065 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=5.305 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=4.501 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=4.467 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=4.342 ms
PC3> █
```

Figura 35 Parte2 Conectividad LAN PC3 hacia D1

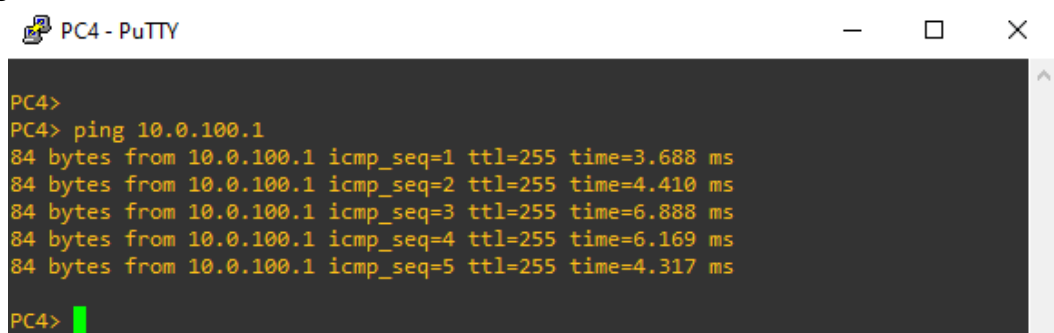
Ping hacia D2 IP 10.0.101.2

```
PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=3.352 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=3.745 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=4.159 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=3.953 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=3.678 ms
PC3> █
```

Figura 36 Parte2 Conectividad LAN PC3 hacia D2

## Validaciones de conectividad desde PC4

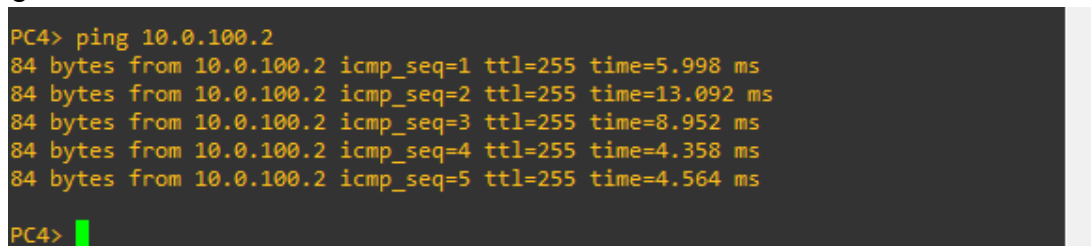
Ping hacia D1 IP 10.0.100.1



```
PC4 - PuTTY
PC4>
PC4> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=3.688 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=4.410 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=6.888 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=6.169 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=4.317 ms
PC4> █
```

Figura 37 Parte2 Conectividad LAN PC4 hacia D1

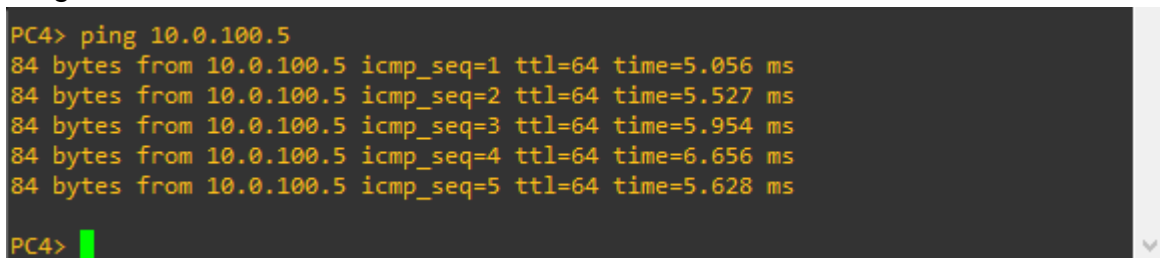
Ping hacia D2 IP 10.0.100.2



```
PC4> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=5.998 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=13.092 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=8.952 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=4.358 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=4.564 ms
PC4> █
```

Figura 38 Parte2 Conectividad LAN PC4 hacia D2

Ping hacia PC1 IP 10.0.100.5



```
PC4> ping 10.0.100.5
84 bytes from 10.0.100.5 icmp_seq=1 ttl=64 time=5.056 ms
84 bytes from 10.0.100.5 icmp_seq=2 ttl=64 time=5.527 ms
84 bytes from 10.0.100.5 icmp_seq=3 ttl=64 time=5.954 ms
84 bytes from 10.0.100.5 icmp_seq=4 ttl=64 time=6.656 ms
84 bytes from 10.0.100.5 icmp_seq=5 ttl=64 time=5.628 ms
PC4> █
```

Figura 39 Parte2 Conectividad LAN PC4 hacia PC1

## Parte 3: Configurar los protocolos de enrutamiento

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

Especificaciones.

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

R1: 0.0.4.1

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

En R1, no publique la red R1 – R2.

En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

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

Especificaciones

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

- R1: 0.0.6.1

- R3: 0.0.6.3

- D1: 0.0.6.131

- D2: 0.0.6.132

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

- En R1, no publique la red R1 – R2.

- On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

Deshabilite las publicaciones OSPFv3 en:

- D1: todas las interfaces excepto ETH0/01

- D2: todas las interfaces excepto ETH0/01

### 3.3 En R2 en la “Red ISP”, configure MP-BGP.

Especificaciones

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada IPv4.

- Una ruta estática predeterminada IPv6.

Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2.

Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

En IPv4 address family, anuncie:

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

En IPv6 address family, anuncie:

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

### **3.4 En R1 en la “Red ISP”, configure MP-BGP.**

Especificaciones

Configure dos rutas resumen estáticas a la interfaz Null 0:

- Una ruta resumen IPv4 para 10.0.0.0/8.
- Una ruta resumen IPv6 para 2001:db8:100::/48.

Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1.

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

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

En IPv6 address family:

- Deshabilite la relación de vecino IPv4.
- Habilite la relación de vecino IPv6.
- Anuncie la red 2001:db8:100::/48.

### **Configuración en R1 utilizando process ID 4 y con la asignación 0.0.4.1 y asignación de ruta por defecto.**

Se configura el protocolo de enrutamiento OSPF v2 a partir de un process ID el cual es un valor entre 1 y 65535 que actúa como identificador local y el cual puede ser el mismo que los de los routers vecinos, de igual forma se parametriza el router id el cual se representa como una dirección IPv4 y el cual permite identificar un router OSPF dentro de un dominio de enrutamiento determinado.

## Configuración en R1

Comandos utilizados.

enable

config t

router ospf 4

router-id 0.0.4.1

network 10.0.10.0 0.0.0.255 area 0

network 10.0.13.0 0.0.0.255 area 0

default-information originate

exit

```
R1#
R1#enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)# network 10.0.10.0 0.0.0.255 area 0
R1(config-router)# network 10.0.13.0 0.0.0.255 area 0
R1(config-router)#default-information originate
R1(config-router)#exit
R1(config)#
```

Figura 40 Parte 3 Configuración OSPF v2 en R1

Verificamos los parámetros ingresados por medio del comando: show run | section ^router ospf

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

Figura 41 Parte 3 Configuración OSPF v2 en R1

Configuración OSPF v3 en R1 para process ID 6 con asignación 0.0.6.1, anuncio de interfaces exceptuando conexión entre R1-R2

Comandos utilizados.

ipv6 router ospf 6

router-id 0.0.6.1

default-information originate

```
exit
interface Eth0/0
ipv6 ospf 6 area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
```

```
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface eth0/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#interface s2/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#
```

Figura 42 Parte 3 Configuración OSPF v3 en R1

Validación configuración OSPF en R1

comando: show ipv6 ospf interface brief

```
R1#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State  Nbrs F/C
Se2/0     6    0         11       64   P2P    1/1
Et0/0     6    0         3        10   DR     0/0
R1#
```

Figura 43 Parte 3 Validación OSPF en R1

Configuración de rutas resumen tanto para ipv4 como para ipv6

Comandos utilizados.

Enable

Config t

ip route 10.0.0.0 255.0.0.0 null0

ipv6 route 2001:db8:100::/48 null0

Definición de proceso en r1 para protocolo BGP y configuración de numero ASN identificativo 300 con router-id: 1.1.1.1.

Comandos utilizados:

```
router bgp 300  
bgp router-id 1.1.1.1
```

Establecimiento de redes vecinas hacia R2 numero identificativo ASN 500.

Comandos utilizados:

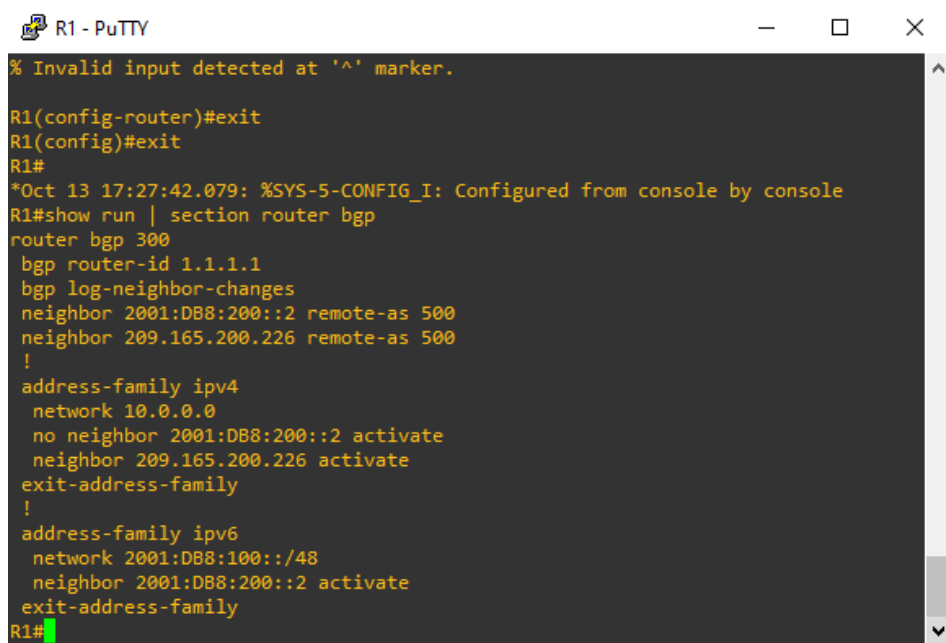
```
neighbor 2001:db8:200::2 remote-as 500  
address-family ipv4 unicast  
neighbor 209.165.200.226 activate  
no neighbor 2001:db8:200::2 activate  
network 10.0.0.0 mask 255.0.0.0  
exit-address-family  
address-family ipv6 unicast  
no neighbor 209.165.200.226 activate  
neighbor 2001:db8:200::2 activate  
network 2001:db8:100::/48  
exit-address-family
```

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

Figura 44 Parte 3 Configuración BGP en R1

## Validación de parámetros ingresados en R1

comando: show run | section router bgp.



```
R1 - PuTTY
% Invalid input detected at '^' marker.

R1(config-router)#exit
R1(config)#exit
R1#
*Oct 13 17:27:42.079: %SYS-5-CONFIG_I: Configured from console by console
R1#show run | section router bgp
router bgp 300
  bgp router-id 1.1.1.1
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::2 remote-as 500
  neighbor 209.165.200.226 remote-as 500
  !
  address-family ipv4
    network 10.0.0.0
    no neighbor 2001:DB8:200::2 activate
    neighbor 209.165.200.226 activate
  exit-address-family
  !
  address-family ipv6
    network 2001:DB8:100::/48
    neighbor 2001:DB8:200::2 activate
  exit-address-family
R1#
```

Figura 45 Parte 3 Validación BGP en R1

## Configuración en R2

Configuración de rutas estáticas por medio de interfaz loopback.

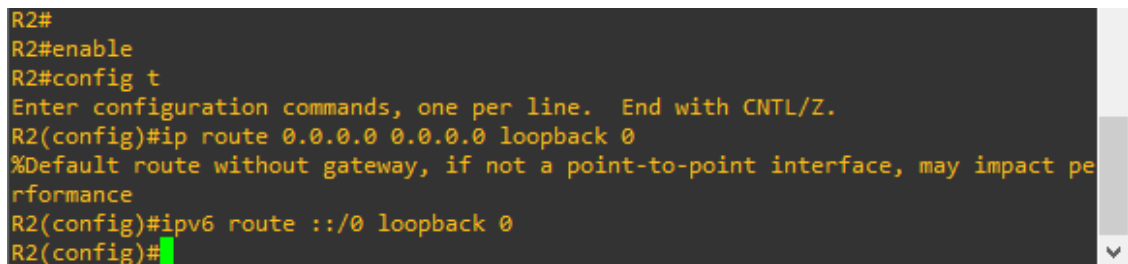
Comandos utilizados.

Enable

Config t

ip route 0.0.0.0 0.0.0.0 loopback 0

ipv6 route ::/0 loopback 0



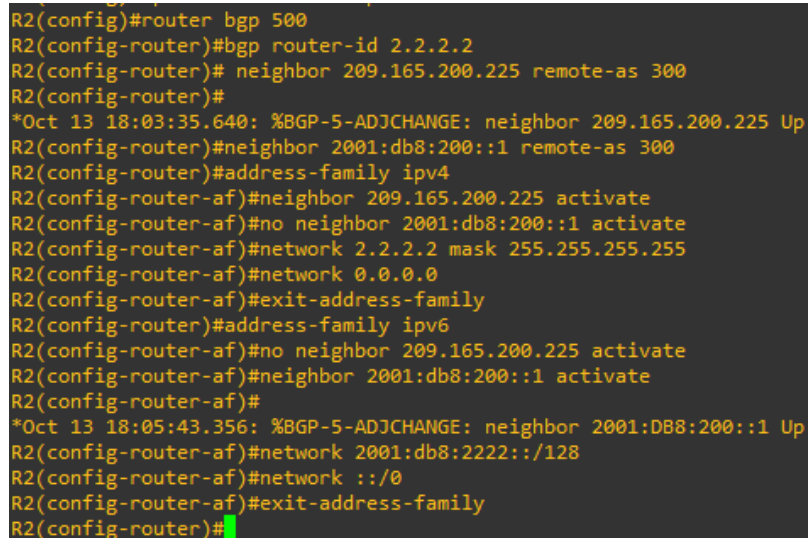
```
R2#
R2#enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0
R2(config)#
```

Figura 46 Parte 3 Configuración rutas estáticas en R2

Configuración de proceso BGP en R2 mediante número ASN 500 y router id 2.2.2.2, establecimiento de redes vecinas mediante interfaz tcp conectada a R1 y anuncio de redes familia para protocolo IPV4 y IPV6.

Comandos utilizados:

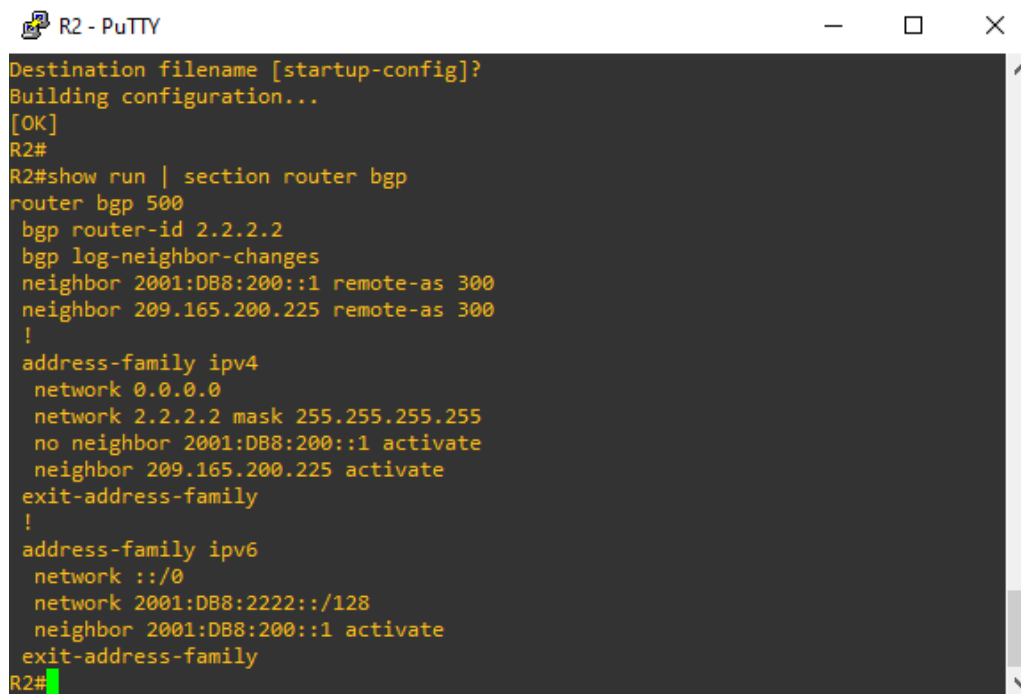
```
router bgp 500
bgp router-id 2.2.2.2
neighbor 209.165.200.225 remote-as 300
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate
no neighbor 2001:db8:200::1 activate
network 2.2.2.2 mask 255.255.255.255
network 0.0.0.0
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family
```



```
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)# neighbor 209.165.200.225 remote-as 300
R2(config-router)#
*Oct 13 18:03:35.640: %BGP-5-ADJCHANGE: neighbor 209.165.200.225 Up
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.225 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
R2(config-router-af)#exit-address-family
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.225 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#
*Oct 13 18:05:43.356: %BGP-5-ADJCHANGE: neighbor 2001:DB8:200::1 Up
R2(config-router-af)#network 2001:db8:2222::/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit-address-family
R2(config-router)#
```

Figura 47 Parte 3 Configuración BGP en R2

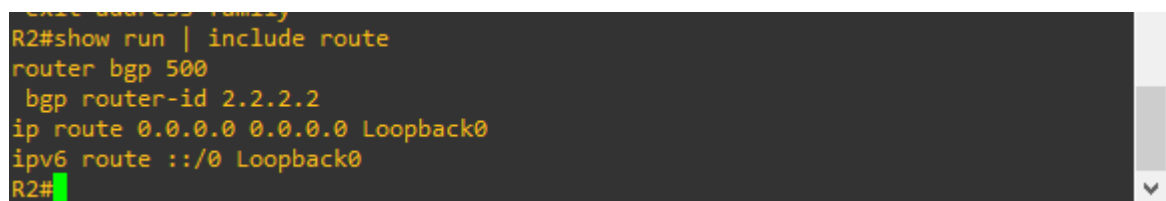
Validación de configuración en R2  
comandos: show run | section router bgp



```
R2 - PuTTY
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
R2#show run | section router bgp
router bgp 500
  bgp router-id 2.2.2.2
  bgp log-neighbor-changes
  neighbor 2001:DB8:200::1 remote-as 300
  neighbor 209.165.200.225 remote-as 300
  !
  address-family ipv4
    network 0.0.0.0
    network 2.2.2.2 mask 255.255.255.255
    no neighbor 2001:DB8:200::1 activate
    neighbor 209.165.200.225 activate
  exit-address-family
  !
  address-family ipv6
    network ::/0
    network 2001:DB8:2222::/128
    neighbor 2001:DB8:200::1 activate
  exit-address-family
R2#
```

Figura 48 Parte 3 Validación BGP en R2

Comando: show run | include route



```
exit address-family
R2#show run | include route
router bgp 500
  bgp router-id 2.2.2.2
ip route 0.0.0.0 0.0.0.0 Loopback0
ipv6 route ::/0 Loopback0
R2#
```

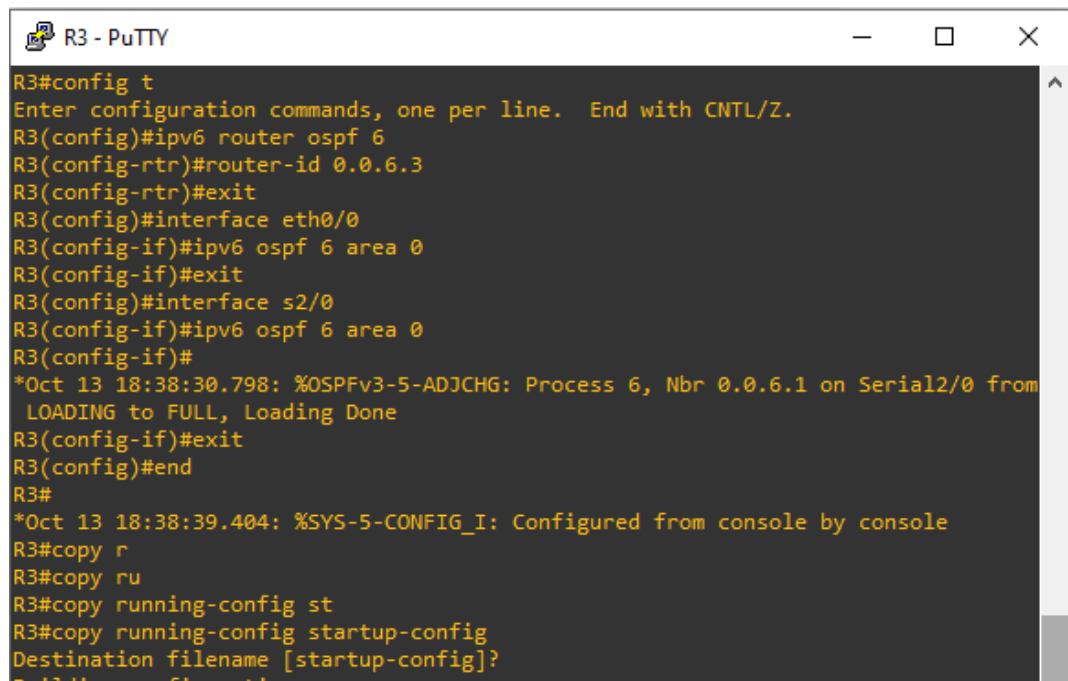
Figura 49 Parte 3 Validación enrutamiento en R2

### Configuraciones en R3

Configuración en R3 utilizando process ID 4 y con la asignación 0.0.4.3 para redes vecinas mediante protocolo OSPF por salida de rutas en las interfaces Eth0/0 y S2/0, Configuración classic single-area OSPF V3 mediante ID6 y router ID 0.0.6.3. y asignación de protocolo.

### Comandos utilizados:

```
Enable
Config t
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface eth0/0
ipv6 ospf 6 area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
```



```
R3 - PuTTY
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface eth0/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#interface s2/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#
*Oct 13 18:38:30.798: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Serial2/0 from
LOADING to FULL, Loading Done
R3(config-if)#exit
R3(config)#end
R3#
*Oct 13 18:38:39.404: %SYS-5-CONFIG_I: Configured from console by console
R3#copy r
R3#copy ru
R3#copy running-config st
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Figura 50 Figura 49 Configuración OSPF v3 en R3

## Validación de configuraciones en R3

comando: show ipv6 ospf interface brief

```
R3#show ipv6 ospf interface brief
Interface  PID  Area      Intf ID  Cost  State Nbrs F/C
Se2/0      6   0         11       64   P2P   1/1
Et0/0      6   0         3        10   DR    0/0
R3#
```

Figura 51 Validación OSPF v3 en R3

Comando: show run | section ^ipv6 router

```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.3
R3#
```

Figura 52 Validación OSPF v3 en R3

## Configuraciones en D1

Configuración protocolo OSPF v2 EN AREA 0, con asignación de process ID 4 y router ID 0.0.4.131 para el Switch D1, proceso para deshabilitar las publicaciones de rutas en todas las interfaces exceptuando la interfaz Eth1/0.

Comandos utilizados.

Enable

Config t

router ospf 4

router-id 0.0.4.131

network 10.0.100.0 0.0.0.255 area 0

network 10.0.101.0 0.0.0.255 area 0

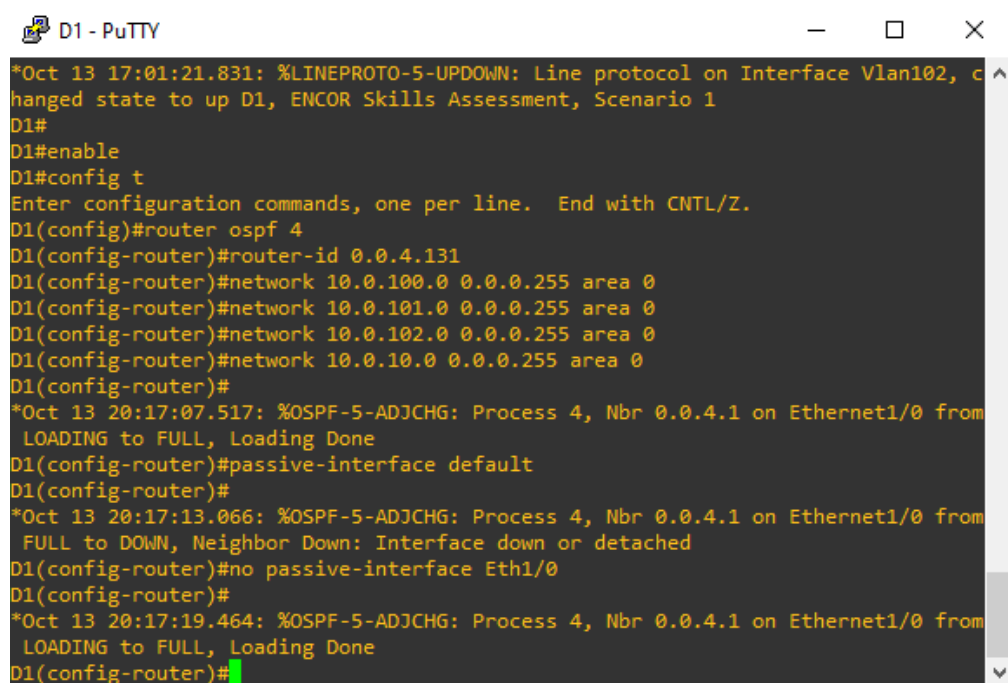
network 10.0.102.0 0.0.0.255 area 0

network 10.0.10.0 0.0.0.255 area 0

passive-interface default

no passive-interface Eth1/0

exit



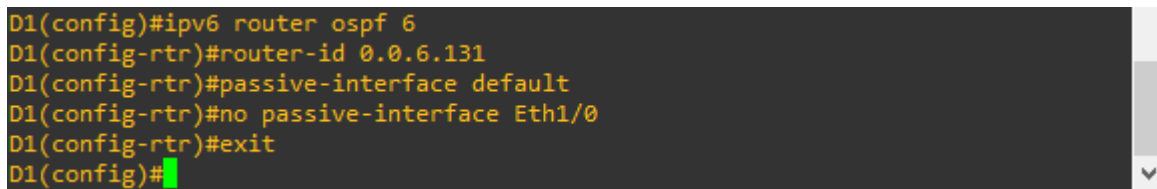
```
D1 - PuTTY
*Oct 13 17:01:21.831: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, c
hanged state to up D1, ENCOR Skills Assessment, Scenario 1
D1#
D1#enable
D1#config t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
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)#
*Oct 13 20:17:07.517: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/0 from
LOADING to FULL, Loading Done
D1(config-router)#passive-interface default
D1(config-router)#
*Oct 13 20:17:13.066: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
D1(config-router)#no passive-interface Eth1/0
D1(config-router)#
*Oct 13 20:17:19.464: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/0 from
LOADING to FULL, Loading Done
D1(config-router)#
```

Figura 53 Configuración OSPF v2 en D1

Configuración Ospf V3 Process ID 6, router ID 0.0.6.131, deshabilitado de publicaciones en interfaces diferentes a Eth1/0.

Comandos utilizados:

```
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Eth1/0
exit
```



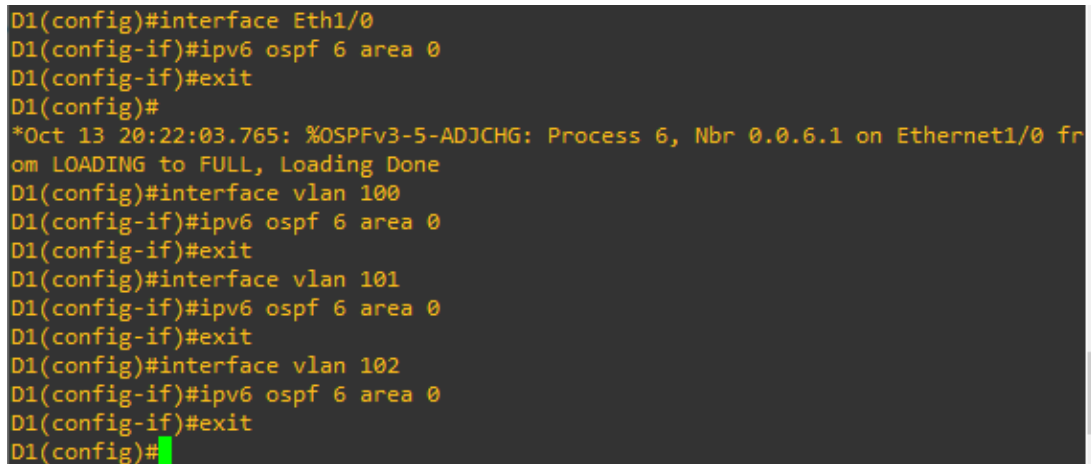
```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface Eth1/0
D1(config-rtr)#exit
D1(config)#
```

Figura 54 Configuración OSPF v3 en D1

anuncio de las redes conectadas, incluidas las vlan número 100, 101 y 102 conectadas en Área 0 Ospf.

### Comandos utilizados.

```
interface Eth1/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

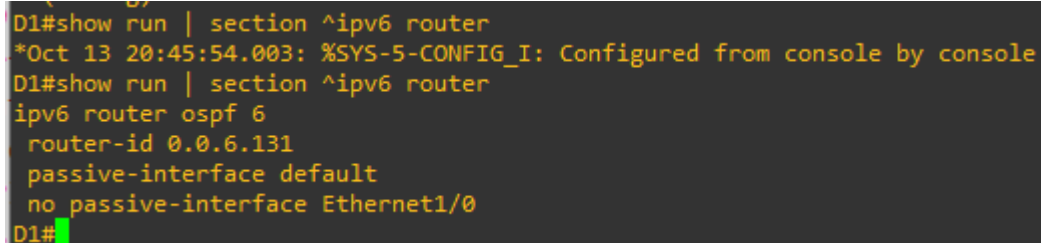


```
D1(config)#interface Eth1/0
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#
*Oct 13 20:22:03.765: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.1 on Ethernet1/0 fr
om LOADING to FULL, Loading Done
D1(config)#interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#interface 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)#
```

Figura 55 Anuncio de redes OSPF en D1

### Validación configuración en D1

Comando: show run | section ^ipv6 router



```
D1#show run | section ^ipv6 router
*Oct 13 20:45:54.003: %SYS-5-CONFIG_I: Configured from console by console
D1#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Ethernet1/0
D1#
```

Figura 56 Validación OSPF v3 en D1

Comando: show ipv6 ospf interface brief

```
D1#show ipv6 ospf interface brief
Interface      PID      Area      Intf ID    Cost    State Nbrs F/C
Vl102          6        0         25         1      DR    0/0
Vl101          6        0         24         1      DR    0/0
Vl100          6        0         23         1      DR    0/0
Et1/0         6        0         21        10     BDR    1/1
D1#
```

Figura 57 Validación interfaces OSPF v3 en D1

## Configuraciones en D2

Configuración protocolo OSPF v2 EN AREA 0, con asignación de process ID 4 y router ID 0.0.4.132 para el Switch D2, proceso para deshabilitar las publicaciones de rutas en todas las interfaces exceptuando la interfaz Eth1/0.

Comandos utilizados:

Enable

Config t

router ospf 4

router-id 0.0.4.132

network 10.0.100.0 0.0.0.255 area 0

network 10.0.101.0 0.0.0.255 area 0

network 10.0.102.0 0.0.0.255 area 0

network 10.0.11.0 0.0.0.255 area 0

passive-interface default

no passive-interface Eth1/0

exit

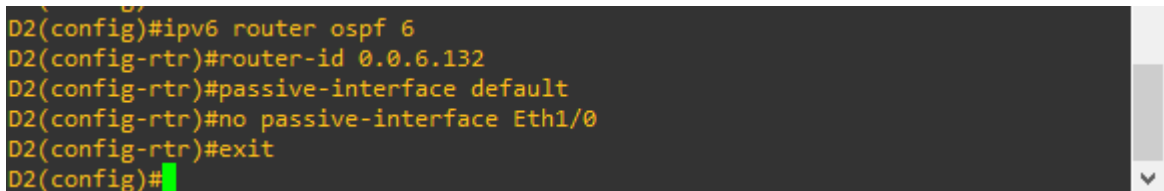
```
D2 - PuTTY
*Oct 13 17:00:51.824: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel112, changed state to up
*Oct 13 17:00:51.831: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up
*Oct 13 17:01:19.178: %LINK-3-UPDOWN: Interface Vlan101, changed state to up
*Oct 13 17:01:20.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up
D2#
D2#enable
D2#config t
Enter configuration commands, one per line. End with CNTL/Z.
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 Eth1/0
D2(config-router)#exit
*Oct 13 20:32:18.549: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.3 on Ethernet1/0 from LOADING to FULL, Loading Done
D2(config-router)#exit
D2(config)#
```

Figura 58 Configuración OSPF v2 en D2

Configuración Ospf V3 Process ID 6, router ID 0.0.6.132, deshabilitado de publicaciones en interfaces diferentes a Eth1/0.

Comandos utilizados:

```
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface Eth1/0
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 Eth1/0
D2(config-rtr)#exit
D2(config)#
```

Figura 59 Configuración OSPF v3 en D2

anuncio de las redes conectadas, incluidas las vlan número 100, 101 y 102 conectadas en Area 0 Ospf.

**Comandos utilizados:**

```
interface Eth1/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
```

```

D2(config)#interface Eth1/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#
*Oct 13 20:33:46.806: %OSPFv3-5-ADJCHG: Process 6, Nbr 0.0.6.3 on Ethernet1/0 fr
om LOADING to FULL, Loading Done
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)#

```

Figura 60 Anuncio de redes en D2

## Validación configuración en D2

Comando: show run | section ^ipv6 router

```

D2#show run | section ^ipv6 router
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface Ethernet1/0
D2#

```

Figura 61 Validación OSPF v3 en D2

Comando: show ipv6 ospf interface brief

```

D2#show ipv6 ospf interface brief
Interface    PID    Area          Intf ID    Cost    State Nbrs F/C
Vl102        6      0              25         1      DR    0/0
Vl101        6      0              24         1      DR    0/0
Vl100        6      0              23         1      DR    0/0
Et1/0        6      0              21         10     BDR   1/1
D2#

```

Figura 62 Validación Interfaces OSPF en D2

## Parte 4: Configurar la redundancia del primer salto

### 4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

Especificaciones:

Cree dos IP SLAs.

- Use la SLA número 4 para IPv4.
- Use la SLA número 6 para IPv6.

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

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

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

- Use el número de rastreo 4 para la IP SLA 4.
- Use el número de rastreo 6 para la IP SLA 6.

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

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

Especificaciones:

Cree IP SLAs.

- Use la SLA número 4 para IPv4.
- Use la SLA número 6 para IPv6.

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

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

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

- Use el número de rastreo 4 para la IP SLA 4.
- Use el número de rastreo 6 para la SLA 6.

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

### 4.3 En D1 configure HSRPv2.

Especificaciones:

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

Configure HSRP version 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

Configure IPv6 HSRP grupo 106 para la VLAN 100:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 y decremente en 60.

Configure IPv6 HSRP grupo 116 para la VLAN 101:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Habilite la preferencia (preemption).
- Registre el objeto 6 y decremente en 60.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 y decremente en 60.

#### **4.4 En D2, configure HSRPv2.**

Especificaciones:

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 104 para la VLAN 100:

- Asigne la dirección IP virtual 10.0.100.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 y decremente en 60.

Configure IPv4 HSRP grupo 114 para la VLAN 101:

- Asigne la dirección IP virtual 10.0.101.254.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

Configure IPv4 HSRP grupo 124 para la VLAN 102:

- Asigne la dirección IP virtual 10.0.102.254.
- Habilite la preferencia (preemption).
- Rastree el objeto 4 para disminuir en 60.

Configure IPv6 HSRP grupo 106 para la VLAN 100:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

Configure IPv6 HSRP grupo 116 para la VLAN 101:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Establezca la prioridad del grupo en 150.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

Configure IPv6 HSRP grupo 126 para la VLAN 102:

- Asigne la dirección IP virtual usando ipv6 autoconfig.
- Habilite la preferencia (preemption).
- Rastree el objeto 6 para disminuir en 60.

### **Configuraciones en D1**

Configuración de protocolo ICMP para establecer SLA (Acuerdo nivel de servicio) definiendo SLA 4 para IPV4 y SLA 6 para IPV6, se parametriza enlace salida por medio de las interfaces Eth0/0 de conexión hacia R1 conforme a la interfaz y frecuencia 5 esto último para definir la velocidad en que se repite la operación del SLA.

### **Comandos utilizados en D1**

```
enable
config t
ip sla 4
icmp-echo 10.0.10.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
```

Ejecución del sondeo por medio del protocolo ICMP y parametrización de los objetos SLA para reporte hacia D1 cuando se presente cambio de estado Down/Up tiempo 10 segundos y Up/Down con un tiempo de 15 segundos.

### Comandos utilizados en D1

Enable

Config t

```
ip sla schedule 4 life forever start-time now
```

```
track 4 ip sla 4
```

```
delay down 10 up 15
```

```
exit
```

```
ip sla schedule 6 life-forever start-time now
```

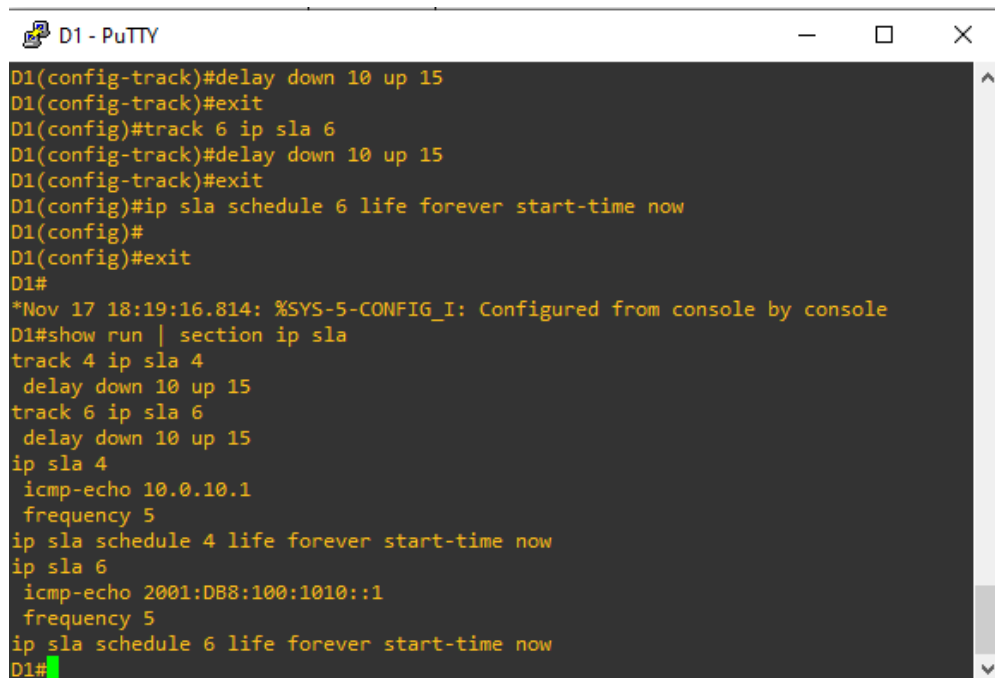
```
track 6 ip sla 6
```

```
delay down 10 up 15
```

```
exit
```

### Validación en D1

Comando utilizado: show run | section ip sla



```
D1 - PuTTY
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#track 6 ip sla 6
D1(config-track)#delay down 10 up 15
D1(config-track)#exit
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#
D1(config)#exit
D1#
*Nov 17 18:19:16.814: %SYS-5-CONFIG_I: Configured from console by console
D1#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.10.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

Figura 63 Validación SLA D1

Configuración del protocolo HSRP en D1 para establecimiento de diferentes Gateway alternativos mediante configuración de prioridad conforme a las VLAN relacionadas (100,101,102) que genere redundancia en la transmisión, por medio del comando **preempt** se habilita el protocolo de ruteo de reserva en modo activo y por medio del comando **track** estableceremos el rastreo del objeto para la reducción de prioridad.

### **Comandos utilizados:**

```
enable
config t
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

```

Validación de configuración realizada en D1 en cada uno de los segmentos VLAN Standby no reconocido, puesto que se encuentra faltante la configuración en D2.

Comando utilizado: show standby brief

```

D1 - PuTTY
ip sla 4
 icmp-echo 10.0.10.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1010::1
 frequency 5
ip sla schedule 6 life forever start-time now
D1#show stand
D1#show standby brie
D1#show standby brief
P indicates configured to preempt.
|
Interface  Grp  Pri P State  Active      Standby      Virtual IP
V1100      104 150 P Active local    unknown     10.0.100.254
V1100      106 150 P Active local    unknown     FE80::5:73FF:FEA0
:6A
V1101      114 100 P Active local    unknown     10.0.101.254
V1101      116 100 P Active local    unknown     FE80::5:73FF:FEA0
:74
V1102      124 150 P Active local    unknown     10.0.102.254
V1102      126 150 P Active local    unknown     FE80::5:73FF:FEA0
:7E
D1#

```

Figura 64 Validación segmentos vlan D2

### Configuraciones en D2

Configuración de protocolo ICPM para establecer SLA (Acuerdo nivel de servicio) definiendo SLA 4 para IPV4 y SLA 6 para IPV6, se parametriza enlace salida por medio de las interfaces Eth0/0 de conexión hacia R3 conforme a la interfaz y frecuencia 5 esto último para definir la velocidad en que se repite la operación del SLA.

**Comandos utilizados:**

```
enable
config t
ip sla 4
icmp-echo 10.0.11.1
frequency
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency
exit
```

ejecución del sondeo por medio del protocolo ICMP y parametrización de los objetos SLA para reporte hacia D2 cuando se presente cambio de estado Down/Up tiempo 10 segundos y Up/Down con un tiempo de 15 segundos.

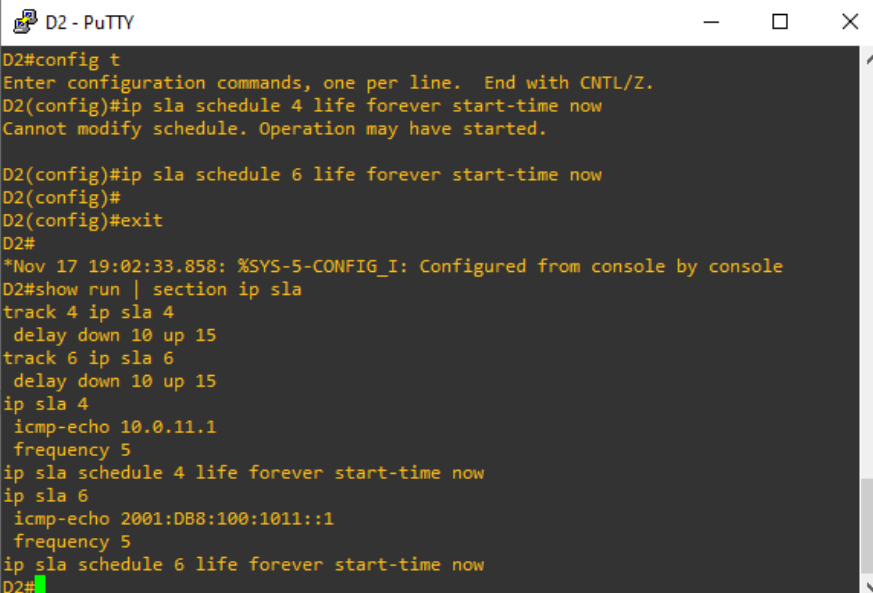
**Comandos utilizados en D2**

```
Enable
Config t
ip sla schedule 4 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
```

```
ip sla schedule 6 life forever start-time now
track 6 ip sla 6
delay down 10 up 15
exit
```

## Validación en D2

Comando utilizado: show run | section ip sla



```
D2-PuTTY
D2#config t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ip sla schedule 4 life forever start-time now
Cannot modify schedule. Operation may have started.

D2(config)#ip sla schedule 6 life forever start-time now
D2(config)#
D2(config)#exit
D2#
*Nov 17 19:02:33.858: %SYS-5-CONFIG_I: Configured from console by console
D2#show run | section ip sla
track 4 ip sla 4
  delay down 10 up 15
track 6 ip sla 6
  delay down 10 up 15
ip sla 4
  icmp-echo 10.0.11.1
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1011::1
  frequency 5
ip sla schedule 6 life forever start-time now
D2#
```

Figura 65 Validación SLA D2

Configuración del protocolo HSRP en D2 para establecimiento de diferentes Gateway alternativos mediante configuración de prioridad conforme a las VLAN relacionadas (100,101,102) que genere redundancia en la transmisión, por medio del comando **preempt** se habilita el protocolo de ruteo de reserva en modo activo y por medio del comando **track** estableceremos el rastreo del objeto para la reducción de prioridad.

### Comandos utilizados:

```
enable
config t
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
```

```

interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit

```

```

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

```

## Validaciones realizadas una vez se ha configurado D2

Comando utilizado en D1-D2: show standby brief

```

D1 - PuTTY
D1#
*Nov 17 19:07:04.014: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Active -> Speak
D1#
*Nov 17 19:07:16.001: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby
D1#
*Nov 17 19:07:23.142: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Active -> Speak
D1#
*Nov 17 19:07:33.812: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -> Standby
D1#show standby brief
          P indicates configured to preempt.
          |
Interface   Grp  Pri  P State  Active      Standby      Virtual IP
Vl100      104  150  P Active local      10.0.100.2   10.0.100.254
Vl100      106  150  P Active local      FE80::D2:2   FE80::5:73FF:FEA0
:6A
Vl101       114  100  P Standby 10.0.101.2  local        10.0.101.254
Vl101       116  100  P Standby FE80::D2:3  local        FE80::5:73FF:FEA0
:74
Vl102       124  150  P Active local      10.0.102.2   10.0.102.254
Vl102       126  150  P Active local      FE80::D2:4   FE80::5:73FF:FEA0
:7E
D1#

```

Figura 66 Validación paso 4 D1

```
D2#copy ru
D2#copy running-config st
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 4981 bytes to 2471 bytes[OK]
D2#
D2#
*Nov 17 19:08:22.195: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Speak -> Standby
D2#show standby brief
          P indicates configured to preempt.
          |
Interface Grp Pri P State Active Standby Virtual IP
V1100     104 100 P Standby 10.0.100.1 local 10.0.100.254
V1100     106 100 P Standby FE80::D1:2 local FE80::5:73FF:FEA0
:6A
V1101     114 150 P Active local 10.0.101.1 10.0.101.254
V1101     116 150 P Active local FE80::D1:3 FE80::5:73FF:FEA0
:74
V1102     124 100 P Standby 10.0.102.1 local 10.0.102.254
V1102     126 100 P Standby FE80::D1:4 local FE80::5:73FF:FEA0
:7E
D2#
```

Figura 67 Validación paso 4 D2

## Parte 5: Seguridad

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

Especificaciones:

Contraseña: cisco12345cisco

### 5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.

Especificaciones:

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

Configuración realizada en todos los dispositivos de la topología (D1,D2,R1,R2,R3)

Por medio de la habilitación del algoritmo para almacenamiento de contraseñas en el modo privilegiado de encriptado SCRYPT, posteriormente se genera la creación de usuarios por dispositivo y la protección de este mediante el empleo de una contraseña.

Comandos utilizados:

```
enable algorithm-type SCRYPT secret cisco12345cisco
```

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

Configuración en dispositivos

```
D1#enable
D1#config t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D1(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D1(config)#
```

Figura 68 Configuración SCRYPT D1

```
D2#enable
D2#config t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
D2(config)#sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D2(config)#
```

Figura 69 Configuración SCRYPT D2

```

A1#enable
A1#config t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
A1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
A1(config)#

```

Figura 70 Configuración SCRYPT A1

```

R1#
R1#enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R1(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R1(config)#

```

Figura 71 Configuración SCRYPT R1

```

R2#
R2#enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R2(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R2(config)#

```

Figura 72 Configuración SCRYPT R2

```

R3#enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R3(config)#

```

Figura 73 Configuración SCRYPT R3

Validación de la configuración de seguridad en todos los dispositivos (ejemplo D1-R3)

Comando utilizado: show run | include secret

```

R3#enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco
R3(config)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
R3(config)#
R3(config)#EXIT
R3#
*Nov 17 22:41:59.403: %SYS-5-CONFIG_I: Configured from console by console
R3#show run | include secret
enable secret 9 $9$S174Xaua..ZrN1$yB70.6bELwFMCT0Z7YvrgINmhxGbp04lh65TgfpAtqY
username sadmin privilege 15 secret 9 $9$jobqwcVA380E3n$6PP3t39zaZANwgOTvcfKiD6.
8p7L.QGExc3JukUwytS
R3#

```

Figura 74 Validación SCRYPT R3

### **5.3 En todos los dispositivos (excepto R2), habilite AAA.**

### **5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.**

Especificaciones:

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

### **5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA**

Especificaciones:

- Use la lista de métodos por defecto
- Valide contra el grupo de servidores RADIUS
- De lo contrario, utilice la base de datos local.

Se realiza habilitación en todos los equipos exceptuando R2 del protocolo AAA (Authentication, Authorization, Accounting) para la implementación de la herramienta de validación contra los servidores RADIUS, orientado a establecer parámetros más fiables de autenticación de los usuarios que se conectan a la red.

Comandos utilizados:

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

## Implementación AAA en los dispositivos (D1, D2, A1, R1, R3)

```
D1#config t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#aaa new-model
D1(config)#radius server RADIUS
D1(config-radius-server)#$4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)#key $trongPass
D1(config-radius-server)#exit
D1(config)#aaa authentication login default group radius local
D1(config)#exit
D1#
*Nov 17 23:56:28.905: %SYS-5-CONFIG_I: Configured from console by console
D1#copy ru
D1#copy running-config star
D1#copy running-config startup-config
Destination filename [startup-config]?
```

Figura 75 Implementación AAA D1

## Validación configuración AAA desde R1 y R3

Comando utilizado: R1# show run aaa | exclude !

```
R1#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$5g30rQU06bC/4X$VgwDV6AnpJUXJjQ8ogQpBYJg
5G807bb9LxGFtuz0urY
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
aaa new-model
aaa session-id common
```

Figura 76 Validación AAA R1

```
% Invalid input detected at ... marker.
R3(config)#exit
R3#
*Nov 18 00:19:19.290: %SYS-5-CONFIG_I: Configured from console by console
R3#show run aaa | exclude !
aaa authentication login default group radius local
username sadmin privilege 15 secret 9 $9$jobqwcVA380E3n$6PP3t39zaZANwgOTvcfKiD6.
8p7l.QGExc3JukUwyts
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
aaa new-model
aaa session-id common
```

Figura 77 Validación AAA R3

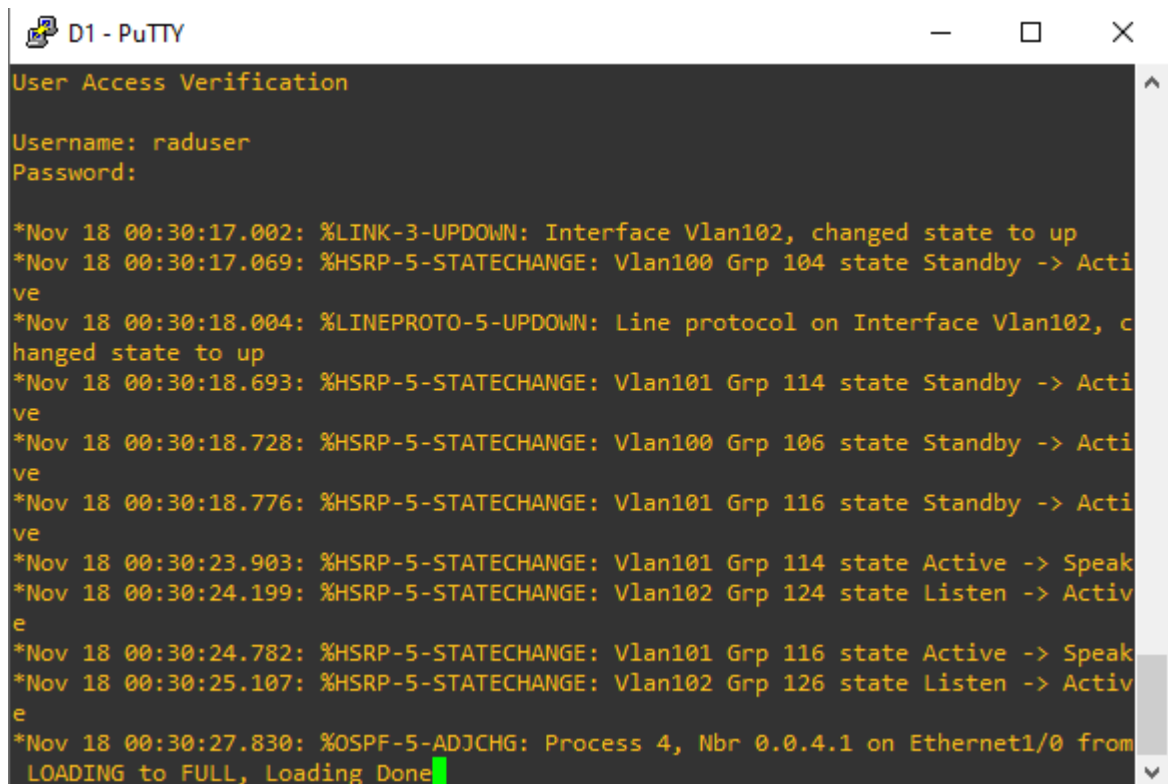
## 5.6 Verifique el servicio AAA en todos los dispositivos (except R2).

Especificaciones:

Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.

Username: raduser

Pass: upass123



```
D1 - PuTTY
User Access Verification
Username: raduser
Password:

*Nov 18 00:30:17.002: %LINK-3-UPDOWN: Interface Vlan102, changed state to up
*Nov 18 00:30:17.069: %HSRP-5-STATECHANGE: Vlan100 Grp 104 state Standby -> Active
*Nov 18 00:30:18.004: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up
*Nov 18 00:30:18.693: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
*Nov 18 00:30:18.728: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Standby -> Active
*Nov 18 00:30:18.776: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Standby -> Active
*Nov 18 00:30:23.903: %HSRP-5-STATECHANGE: Vlan101 Grp 114 state Active -> Speaking
*Nov 18 00:30:24.199: %HSRP-5-STATECHANGE: Vlan102 Grp 124 state Listen -> Active
*Nov 18 00:30:24.782: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Active -> Speaking
*Nov 18 00:30:25.107: %HSRP-5-STATECHANGE: Vlan102 Grp 126 state Listen -> Active
*Nov 18 00:30:27.830: %OSPF-5-ADJCHG: Process 4, Nbr 0.0.4.1 on Ethernet1/0 from
LOADING to FULL, Loading Done
```

Figura 78 Loggin verificación D1

## Parte 6: Configure las funciones de Administración de RED.

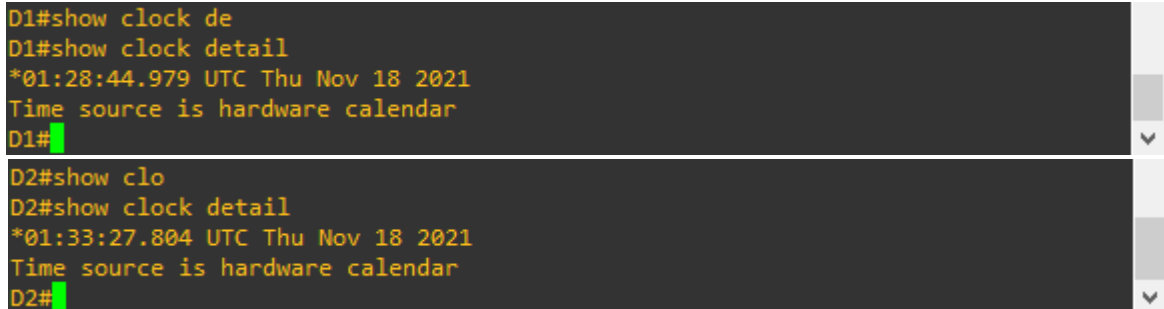
### 6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.

Especificaciones:

Configure el reloj local a la hora UTC actual.

Validación de parámetros de reloj en los dispositivos

Comando utilizado: show clock detail



```
D1#show clock de
D1#show clock detail
*01:28:44.979 UTC Thu Nov 18 2021
Time source is hardware calendar
D1#

D2#show clo
D2#show clock detail
*01:33:27.804 UTC Thu Nov 18 2021
Time source is hardware calendar
D2#
```

Figura 79 Validación reloj D1-D2

### 6.2 Configure R2 como un NTP maestro.

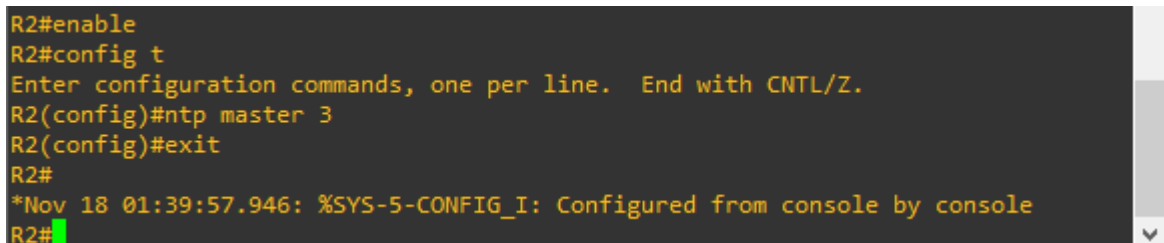
Especificaciones:

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

Se procede a realizar configuración del servicio NTP para que los dispositivos mantengan una sincronización de reloj, se configura R2 como maestro.

#### Comandos utilizados en R2:

```
enable
config t
ntp master 3
exit
```



```
R2#enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 3
R2(config)#exit
R2#
*Nov 18 01:39:57.946: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

Figura 80 Configuración NTP R2

## Validación configuración en R2.

Comando utilizado: show run | include ntp

```
R2#  
R2#show run | include ntp  
ntp master 3  
R2#
```

Figura 81 Validación NTP R2

## 6.3 Configure NTP en R1, R3, D1, D2, y A1.

Especificaciones:

Configure NTP de la siguiente manera:

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

## 6.4 Configure Syslog en todos los dispositivos excepto R2

Especificaciones:

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:

Especificaciones de SNMPv2:

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

Configuración de sincronización de reloj en los dispositivos, R1 sincronizara hacia R2 que se encuentra como maestro, y habilitación de protocolo SNMP para intercambio de administración entre los dispositivos de la Topología y los correspondientes mensajes de trap que permita sondear la información que se transmite en la red.

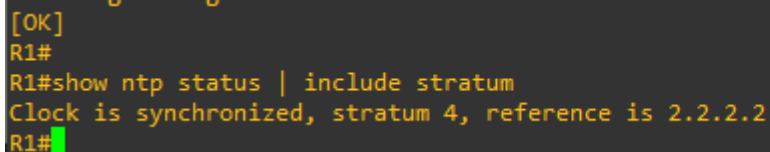
## Configuraciones en R1

Comandos utilizados:

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

## Validación sincronización NTP en R1 hacia R2

Comando utilizado: show ntp status | include stratum




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

Figura 82 Validación NTP R1

## Validación estado de registro syslog en R1

Comando utilizado: show run | include logging



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

Figura 83 Syslog R1

## Validacion SNMP en R1

Comando utilizado: show run | include snmp

```
R1#show run | include snmp
mmi snmp-timeout 180
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
R1#
```

Figura 84 SNMP R1

## Configuraciones en R3

Comandos utilizados:

enable

config t

ntp server 10.0.10.1

logging trap warning

logging host 10.0.100.5

logging on

ip access-list standard SNMP-NMS

permit host 10.0.100.5

exit

snmp-server contact Cisco Student

snmp-server community ENCORSA ro SNMP-NMS

snmp-server host 10.0.100.5 version 2c ENCORSA

snmp-server ifindex persist

snmp-server enable traps config

snmp-server enable traps ospf

end

## Validación sincronización NTP en R3

Comando utilizado: show ntp status | include stratum

```
from LOADING to FULL, Loading Done
R3#show ntp status | include stratum
Clock is synchronized, stratum 5, reference is 10.0.10.1
R3#
```

Figura 85 Sincronización NTP R3

## Validación estado de registro syslog en R3

Comando utilizado: show run | include logging

```
R3#show ntp status | include stratum
Clock is synchronized, stratum 5, reference is 10.0.10.1
R3#show run | include logging
cts logging verbose
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
R3#
```

Figura 86 Syslog R3

## Validación SNMP en R3

Comando utilizado: show run | include snmp

```
R3#show run | include snmp
mmi snmp-timeout 180
snmp-server community ENCORSA RO SNMP-NMS
snmp-server ifindex persist
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
R3#
```

Figura 87 SNMP R3

## Configuraciones en D1

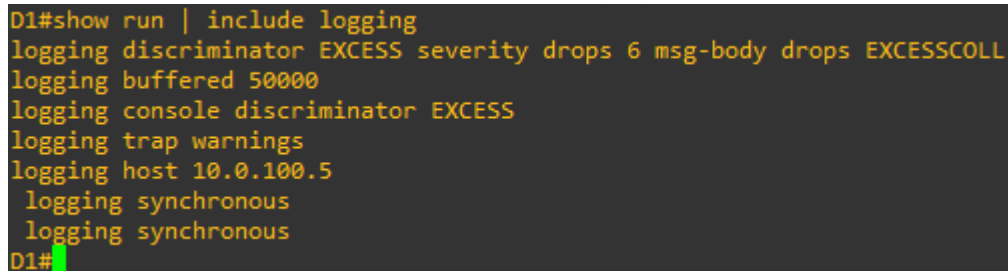
### Comandos utilizados:

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

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

### Validación estado de registro syslog en D1

Comando utilizado: show run | include logging

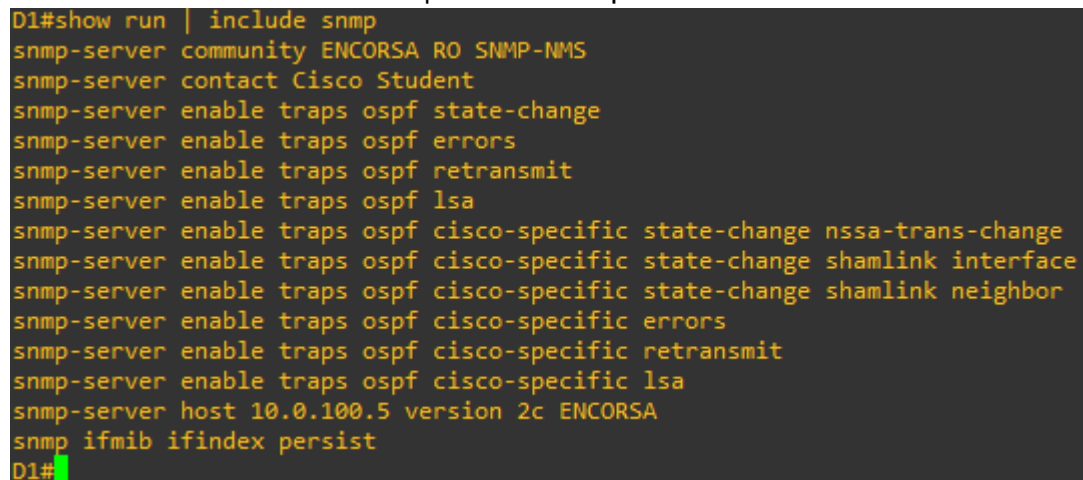


```
D1#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
D1#
```

Figura 88 Syslog D1

### Validación SNMP en D1

Comando utilizado: show run | include snmp

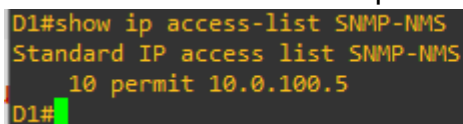


```
D1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific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

Figura 89 SNMP D1

### Validación listas de acceso SNMP NMS en D1

Comando utilizado: show ip access-list SNMP-NMS



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

Figura 90 SNMP NMS D1

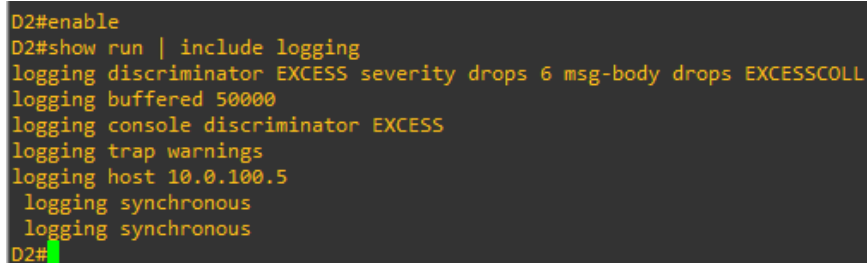
## Configuraciones en D2

### Comandos utilizados:

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

## Validación estado de registro syslog en D2

Comando utilizado: show run | include logging

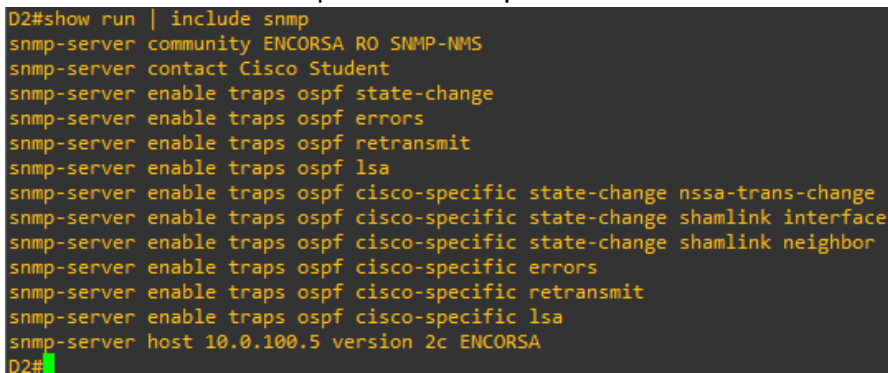


```
D2#enable
D2#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
  logging synchronous
  logging synchronous
D2#
```

Figura 91 Syslog D2

## Validación SNMP en D2

Comando utilizado: show run | include snmp



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

Figura 92 SNMP D2

## Validación listas de acceso SNMP NMS en D2

Comando utilizado: show ip access-list SNMP-NMS

```
D2#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
D2#
```

Figura 93 SNMP NMS D2

## Configuraciones en A1

### Comandos utilizados:

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

## Validación estado de registro syslog en A1

Comando utilizado: show run | include logging

```
A1#show run | include logging
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
logging trap warnings
logging host 10.0.100.5
logging synchronous
logging synchronous
A1#
```

Figura 94 Syslog A1

## Validación SNMP en A1

Comando utilizado: show run | include snmp

```
A1#show run | include snmp
snmp-server community ENCORSA RO SNMP-NMS
snmp-server contact Cisco Student
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
A1#
```

Figura 95 SNMP A1

## Validaciones listas de acceso SNMP NMS en A1

Comando utilizado: show ip access-list SNMP-NMS

```
A1#show ip access-list SNMP-NMS
Standard IP access list SNMP-NMS
 10 permit 10.0.100.5
A1#
```

Figura 96 SNMP NMS A1

## CONCLUSIONES

El uso del software GNS3 y VMWARE Workstation es obligatorio para llevar a cabo la totalidad de pasos que solicita el escenario de la prueba práctica, esto sustentado en las imágenes de los dispositivos de red a trabajar (L2, L3) y las líneas de comando para sus configuraciones, las cuales no son soportadas en su totalidad en otros simuladores menos robustos como Cisco Packet tracer.

Para el manejo de interfaces en estado troncal se debe habilitar el protocolo IEEE 8021q, el cual permite que diversas redes compartan un medio físico sin que se presenten interferencias, esto se orienta siempre que deseemos trabajar con VLANs.

La implementación de EtherChannel permite el aprovechamiento de las conexiones físicas entre dispositivos con el fin de crear canales lógicos con una velocidad mayor, tolerante a fallos mediante balanceo de cargas y redirección de tráfico en caso de presentarse caída de algún canal, el escenario propuesto representa una fiel imagen del tipo de problemáticas en términos de uso de ancho de banda que encontraremos en el entorno laboral y que con una parametrización sencilla por medio de esta tecnología podemos solventar y optimizar.

El protocolo OSPF dado que funciona partir de un principio de estado de enlace, garantiza un manejo de transferencia óptimo orientado al establecimiento e interpretación de las rutas más cortas posibles, su adecuación a trabajo por medio de áreas facilita la interpretación del enrutamiento y se adapta fácilmente a la topología planteada y su salida hacia las redes ISP por medio de BGP.

## BIBLIOGRAFIA

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

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

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

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

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: <https://1drv.ms/b/s!AmIJYeiNT1lnWR0hoMxgBNv1CJ>

The bryantadvantage.com. (2017). CCNP SWITCH Tutorial: EtherChannel Fundamentals. Recuperado de: <https://www.thebryantadvantage.com/videos-and-tutorials/ccnp-switch-tshoot-tutorials/etherchannel-fundamentals/>