# 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 TLEECOMUNICACIONES

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

## Lista de Figuras

## 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 envió 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 practicas 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 practicas 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 desarrollaran un total de 6 pasos orientados a completar el escenario propuesto, en una primera instancia se realizara la configuración básica de los dispositivos y el direccionamiento de sus interfaces validando cada uno de los componentes y dispositivos de la Topologia 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.

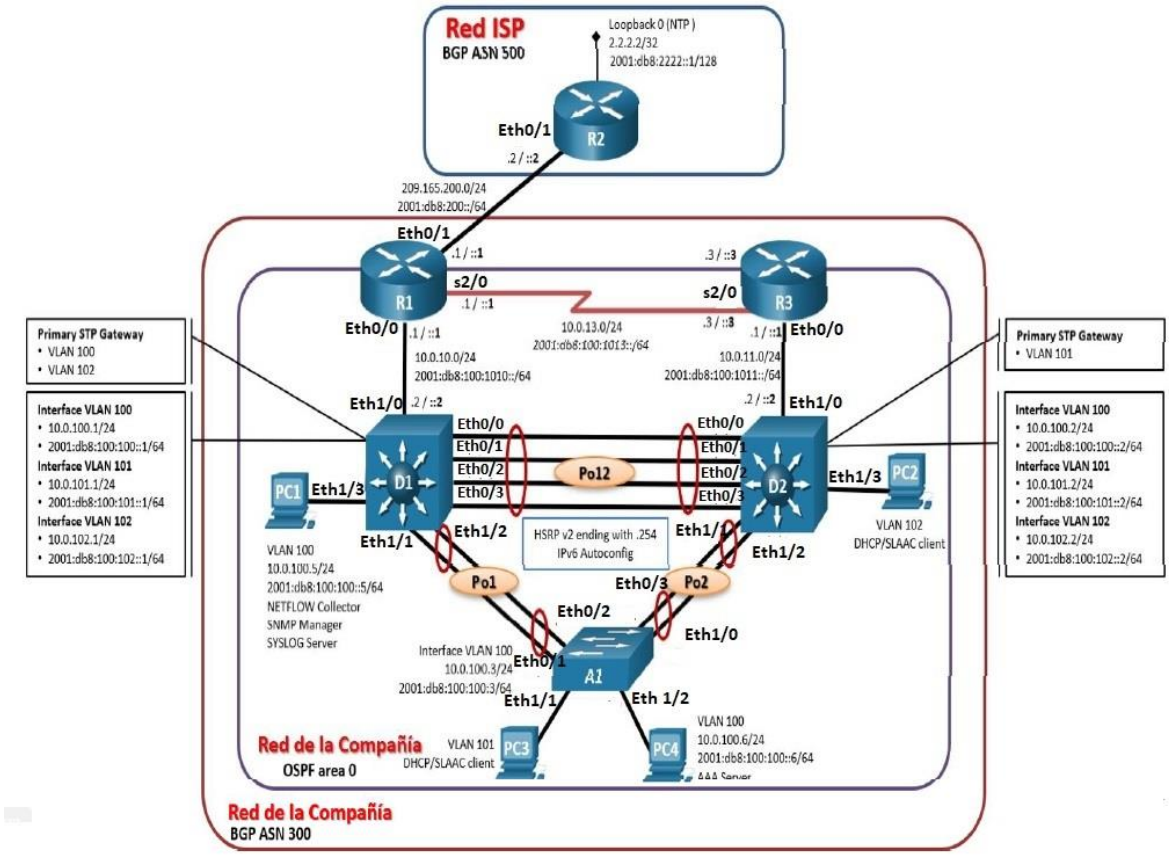


Figura 1 Topologia modelo para la implementación.

## Tabla de enrutamiento.

| Dispositivo | Interfaz | Direccion IPv4 | Direccion IPv6 | Ipv6 Link-Local |
|---|---|---|---|---|
| | 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 |
| R1 | S2/0 | 10.0.13.1/24 | 2001:db8:100:1013::1/64 | fe80::1:3 |
| | Eth0/1 | 209.165.200.226/27 | 2001:db8:200::2/64 | fe80::2:1 |
| R2 | Loopback0 | 2.2.2.2/32 | 2001:db8:2222::1/128 | fe80::2:3 |
| | Eth0/0 | 10.0.11.1/24 | 2001:db8:100:1011::1/64 | fe80::3:2 |
| R3 | S2/0 | 10.0.13.3/24 | 2001:db8:100:1013::3/64 | fe80::3:3 |
| | 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 |
| D1 | VLAN 102 | 10.0.102.1/24 | 2001:db8:100:102::1/64 | fe80::d1:4 |
| | 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 |
| D2 | 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 Topologia propuesta mediante el aplicativo GNS3 y soporte de imágenes IOS de los dispositivos con VMWARE Workstation.

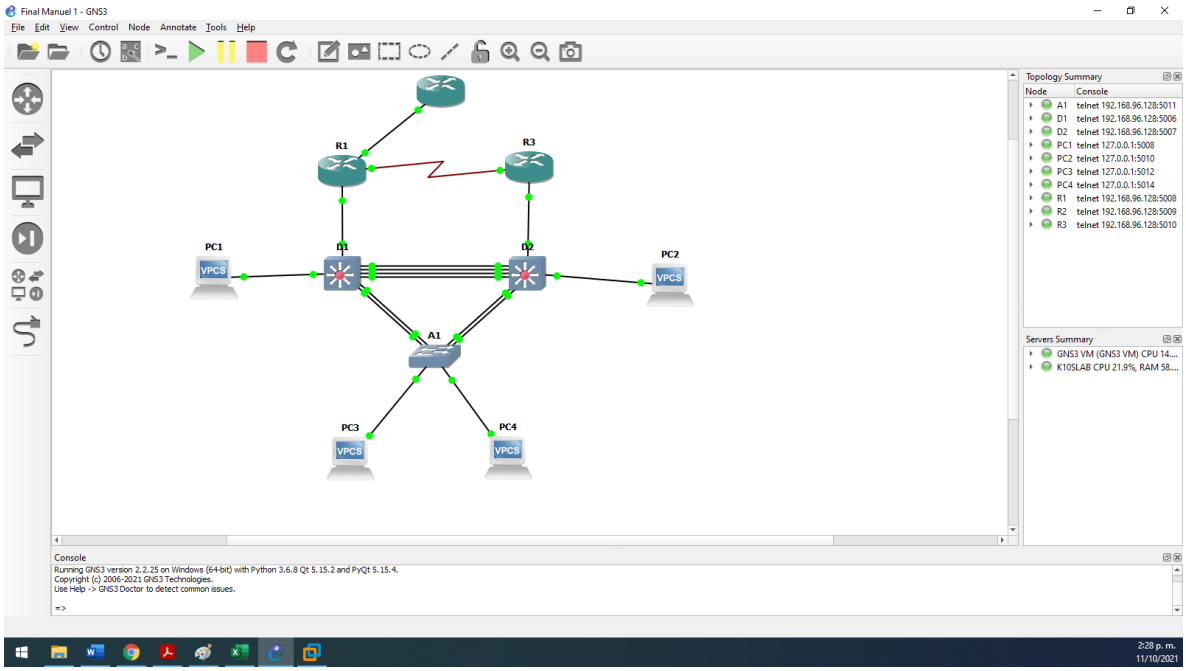


Figura 2 Paso 1 Montaje topología en aplicativo GNS3

**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.

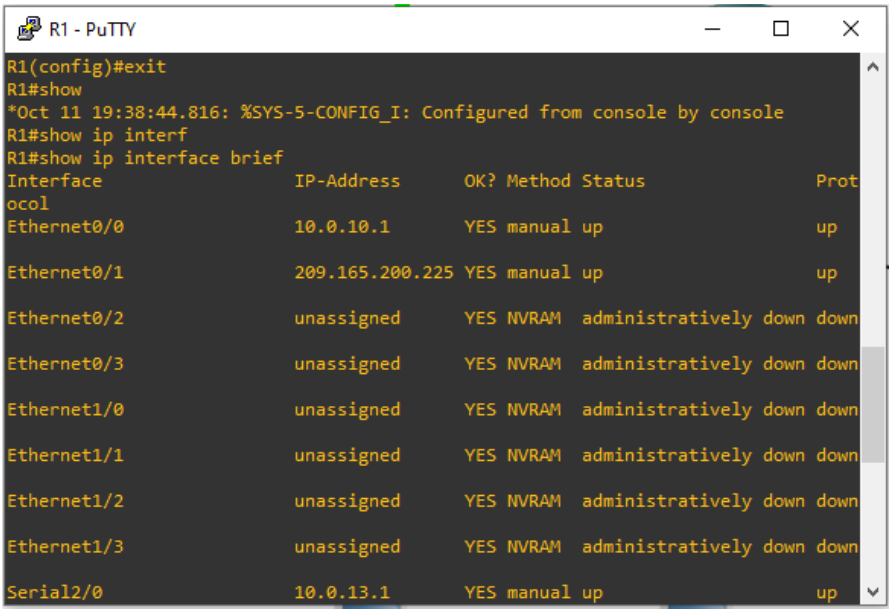


*Figura 3 Paso 2 validación configuración R1*

**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

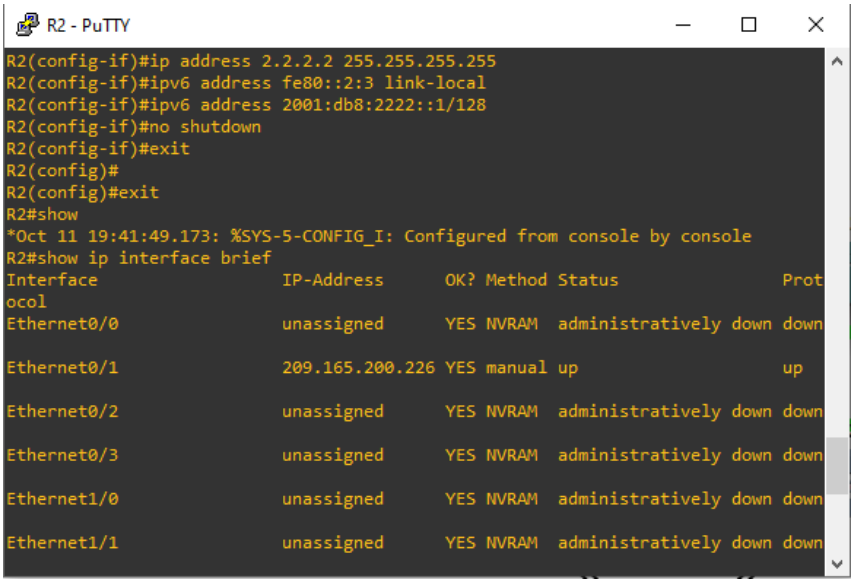


*Figura 4 Paso 2 validación configuración R2*

**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

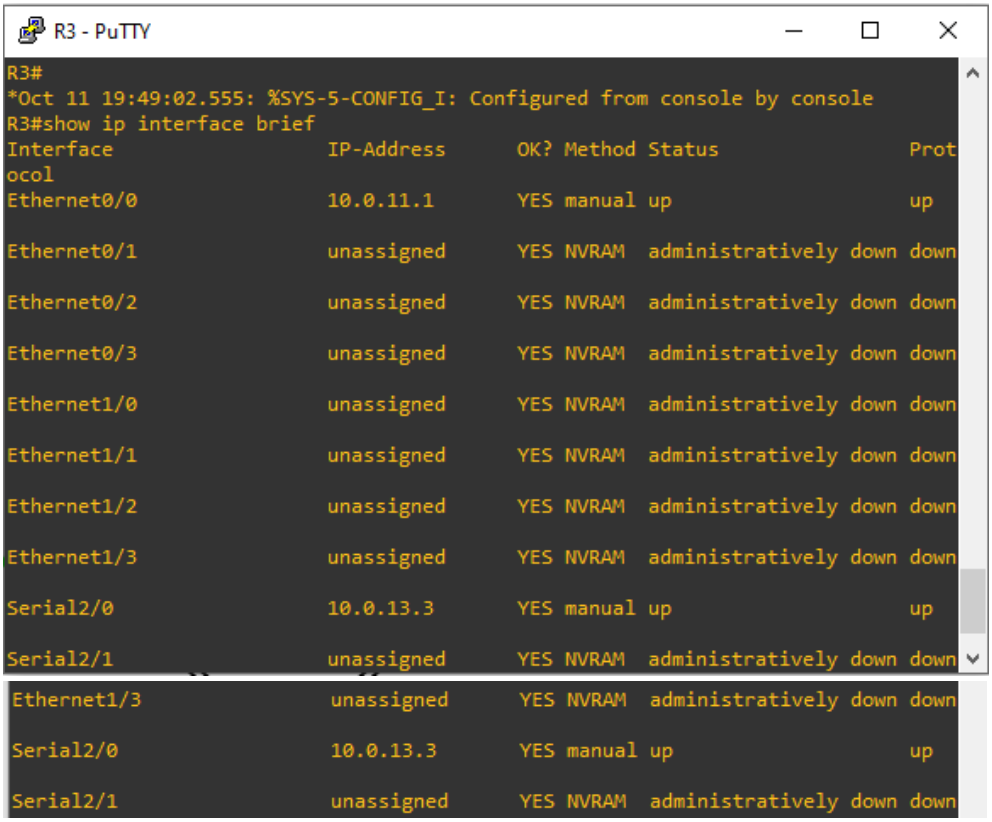


*Figura 5 Paso 2 validación configuración R3*

**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.

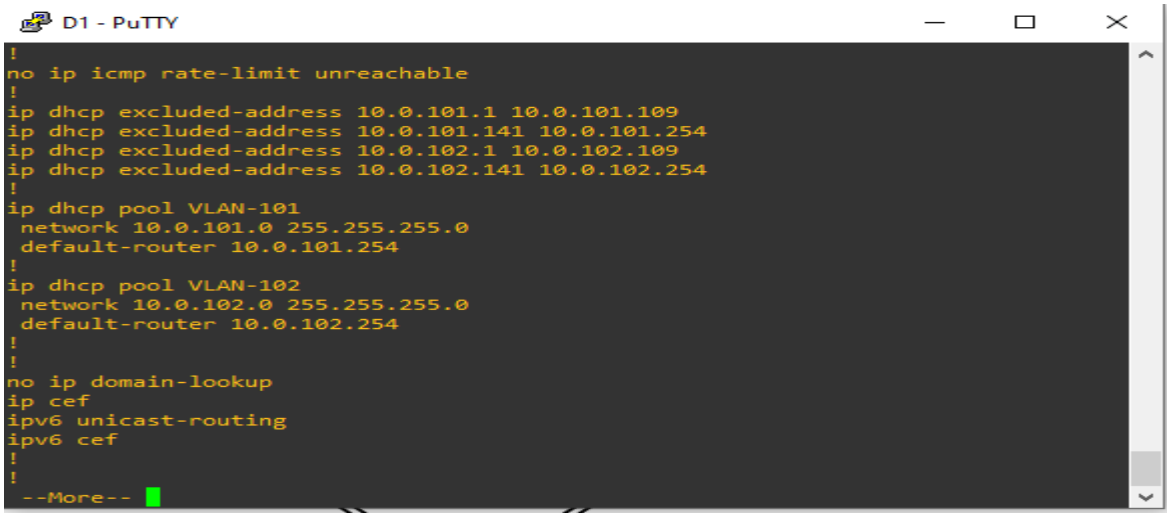


*Figura 6 Paso 2 validación configuración D1*

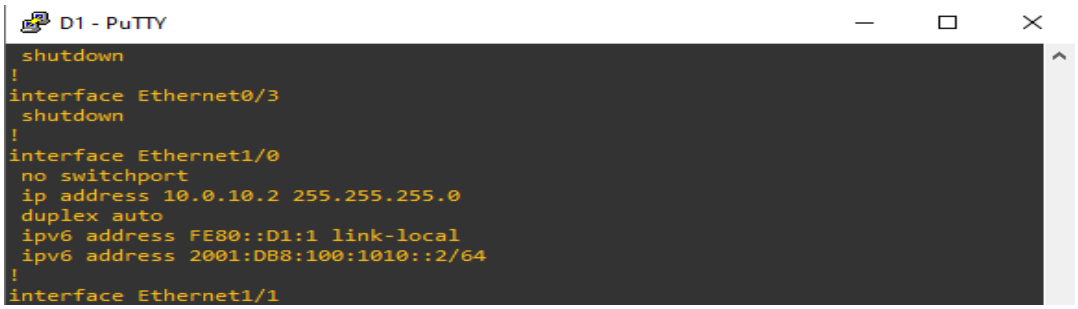


*Figura 7 Paso 2 validación configuración D1*

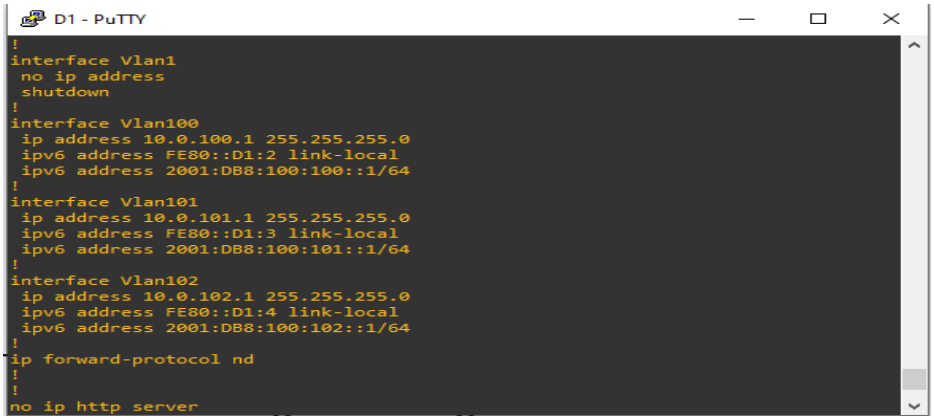


*Figura 8 Paso 2 validación configuración D1*

Comando: #show vlan brief

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

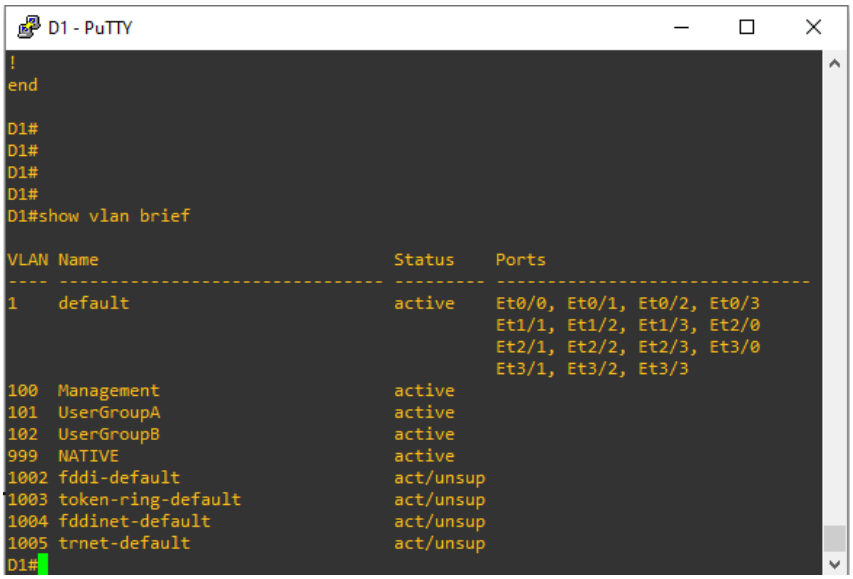


*Figura 9 Paso 2 validación configuración D1*

Comando: #show ip interface brief
Resumen de configuración en las interfaces de los equipos.

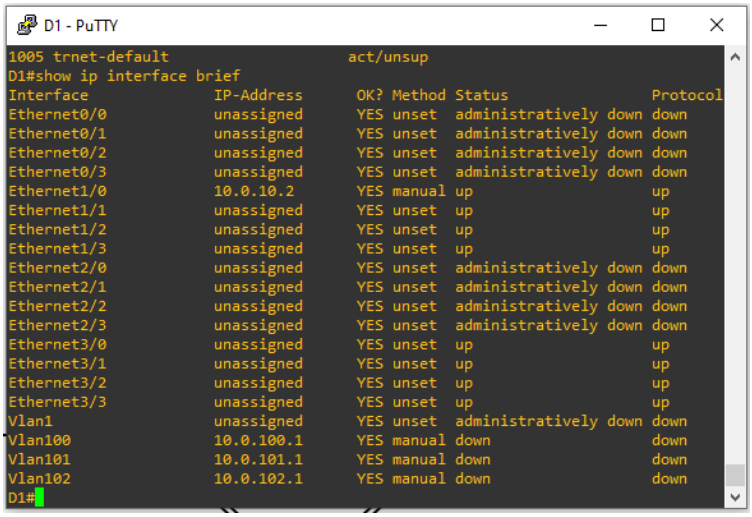


*Figura 10 Paso 2 validación configuración D1*

**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

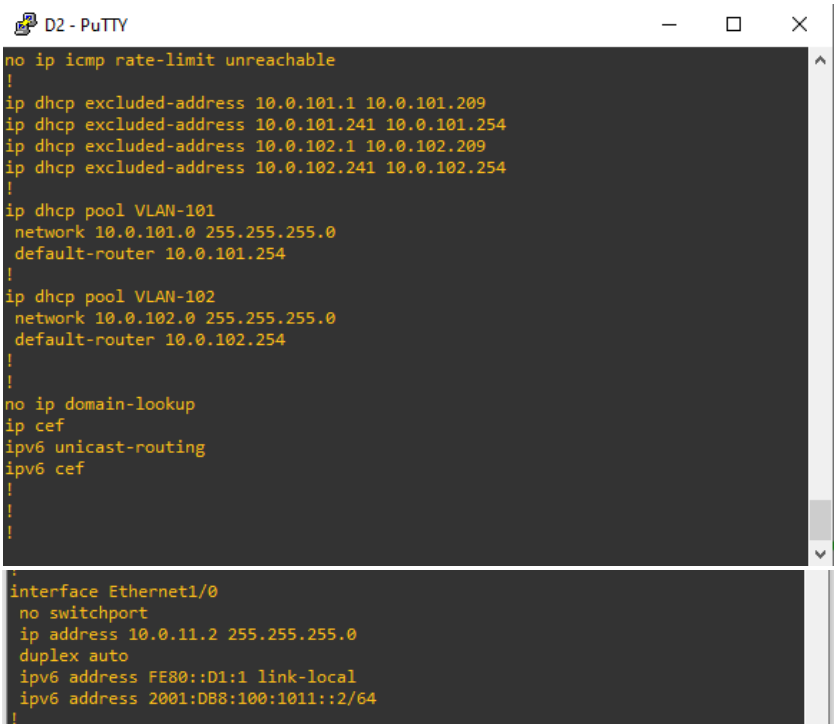


*Figura 11 Parte1-Paso 2 validación configuración D2*

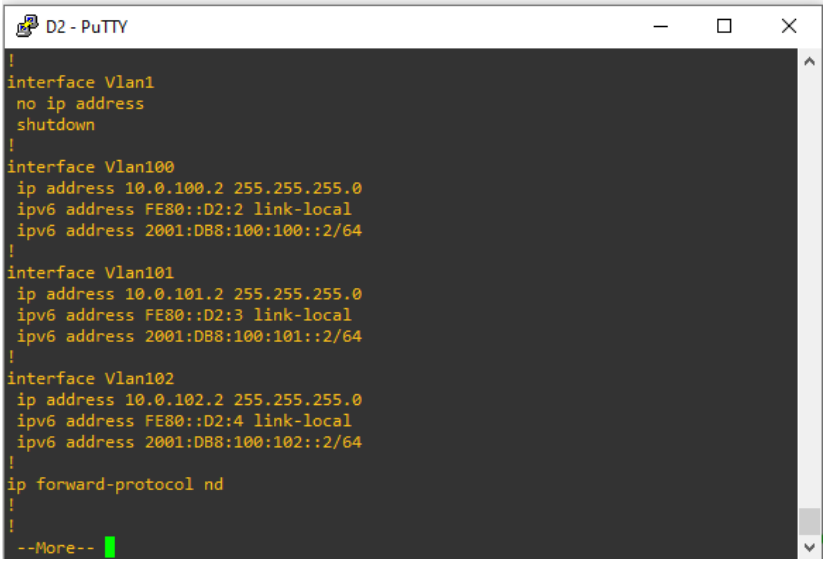


*Figura 12 Parte 1-Paso 2 validación configuración D2*

Comando: #show vlan brief

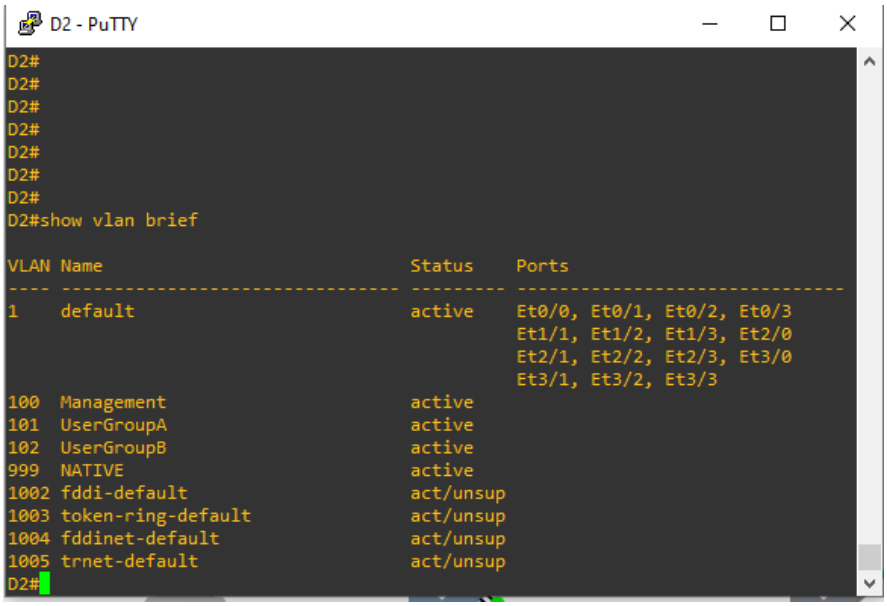


*Figura 13 Parte 1-Paso 2 validación configuración D2*

**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

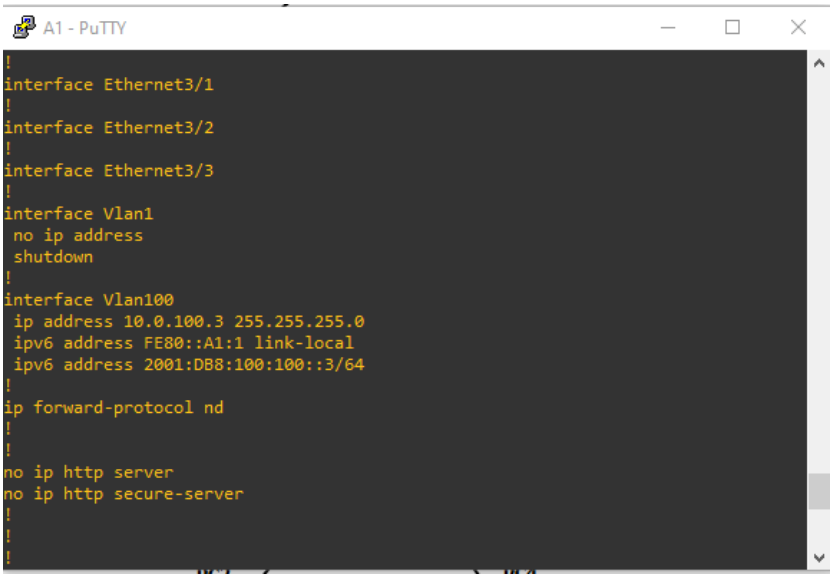

*Figura 14 Parte 1-Paso 2 validación configuración A1*

**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

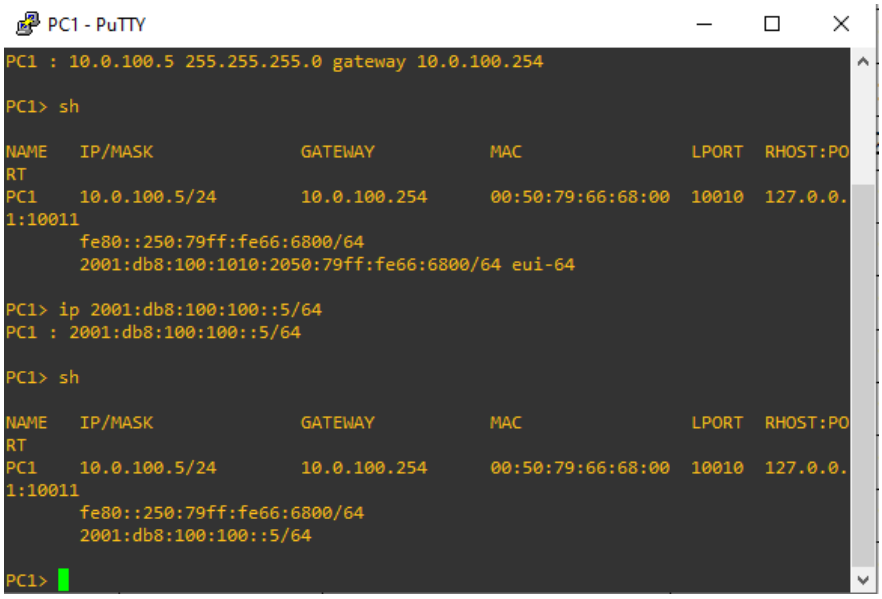


*Figura 15 Parte 1-Paso 2 configuración IP PC1*

**Configuración equipos PC4**

Ip 10.0.100.6 255.255.255.0 10.0.100.254

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

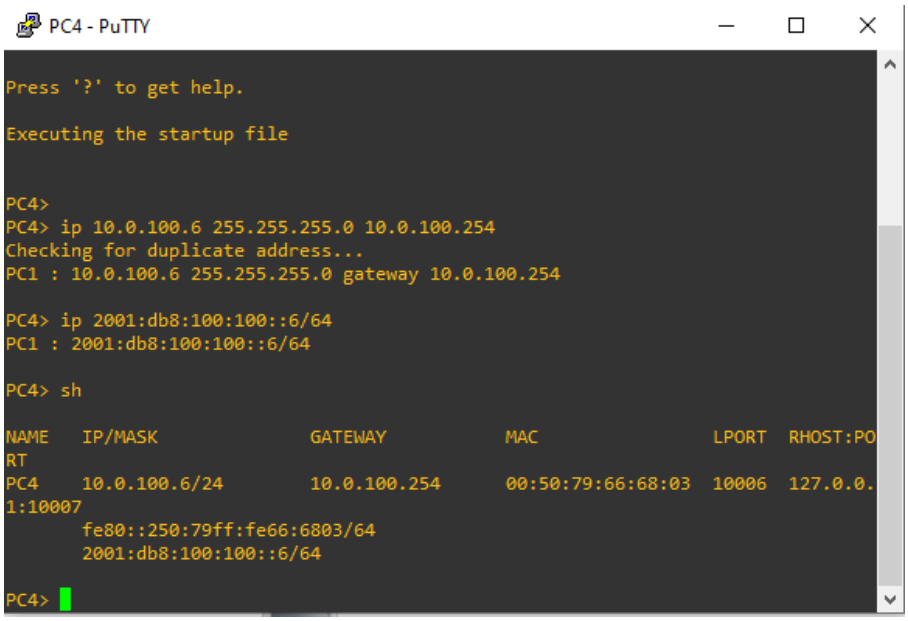


*Figura 16 Parte 1-Paso 2 configuración IP PC4*

## 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 Topologia 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.

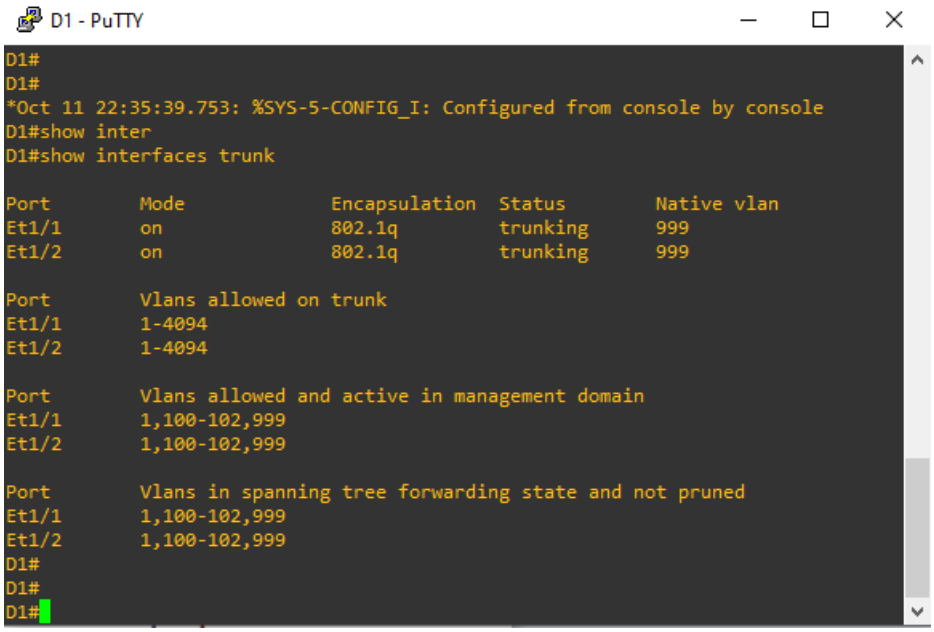


*Figura 17 Parte 2 validación interfaces troncales en D1*

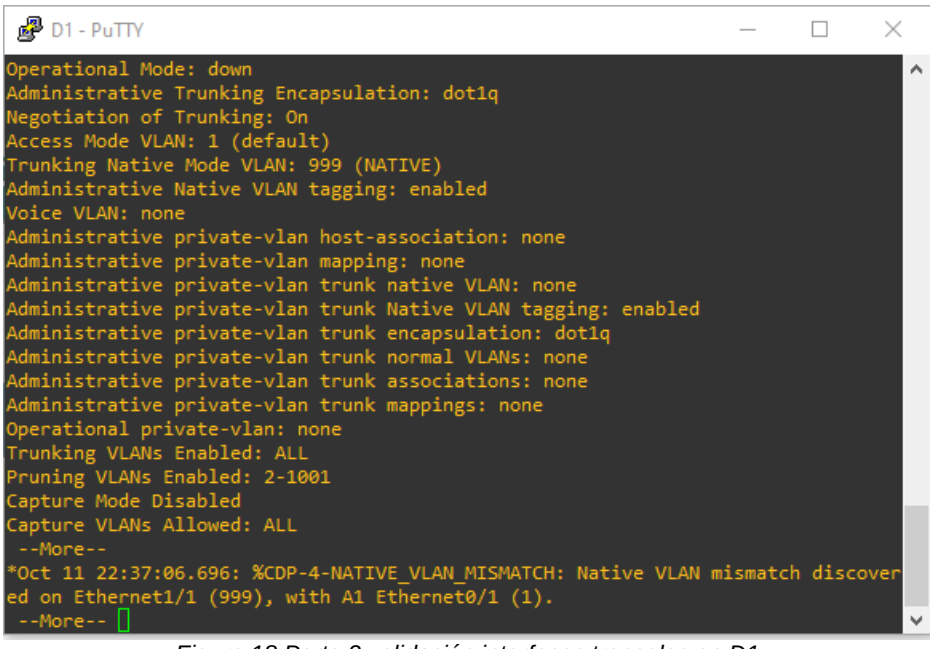


*Figura 18 Parte 2 validación interfaces troncales en D1*

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

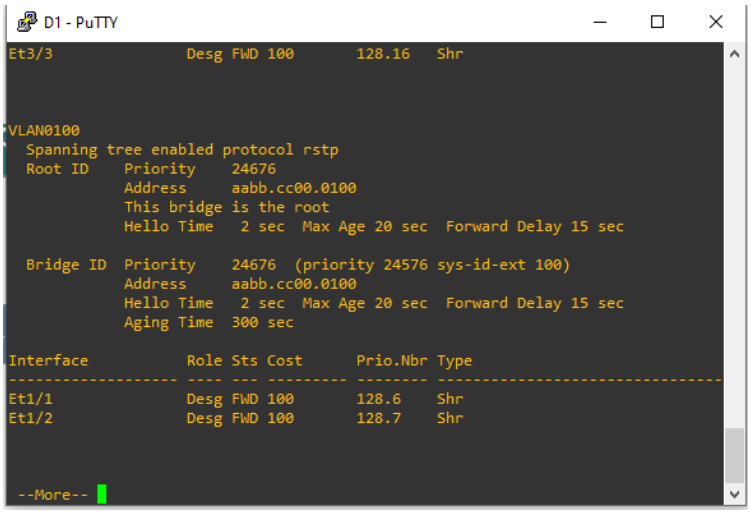


*Figura 19 Parte2 validación RSTP en D1*

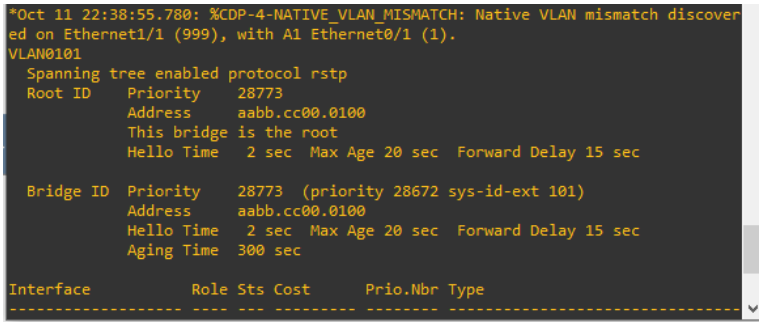


*Figura 20 Parte2 validación RSTP en D1*

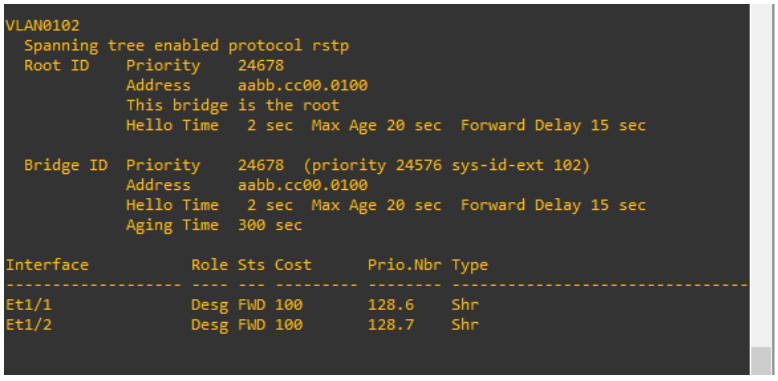


*Figura 21 Parte2 validación RSTP en D1*

**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

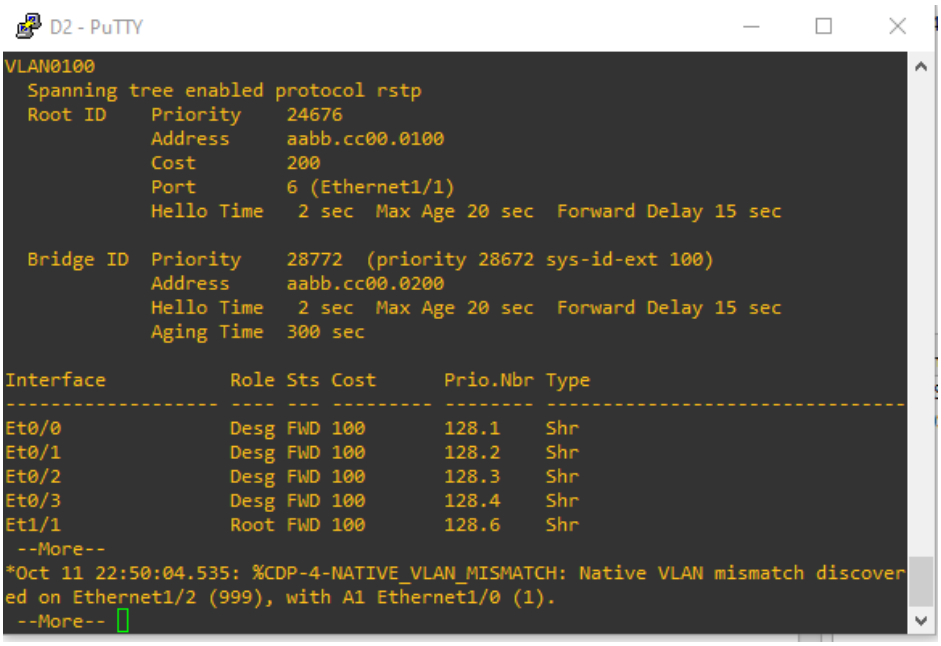


*Figura 22 Parte2 validación RSTP en D2*

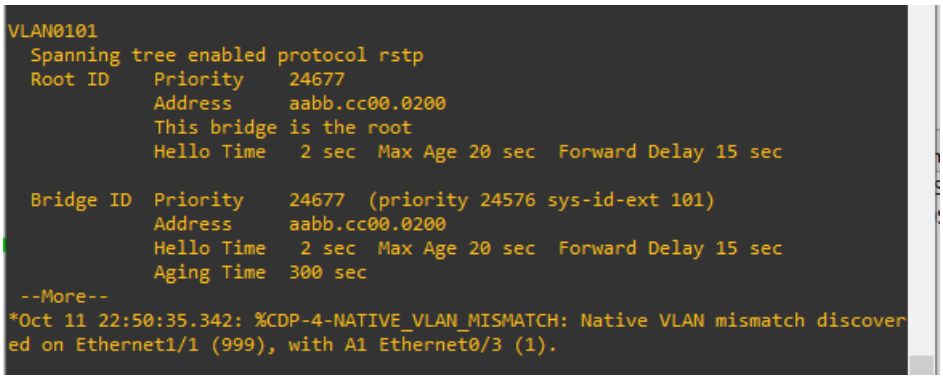


*Figura 23 Parte2 validación RSTP en D2*

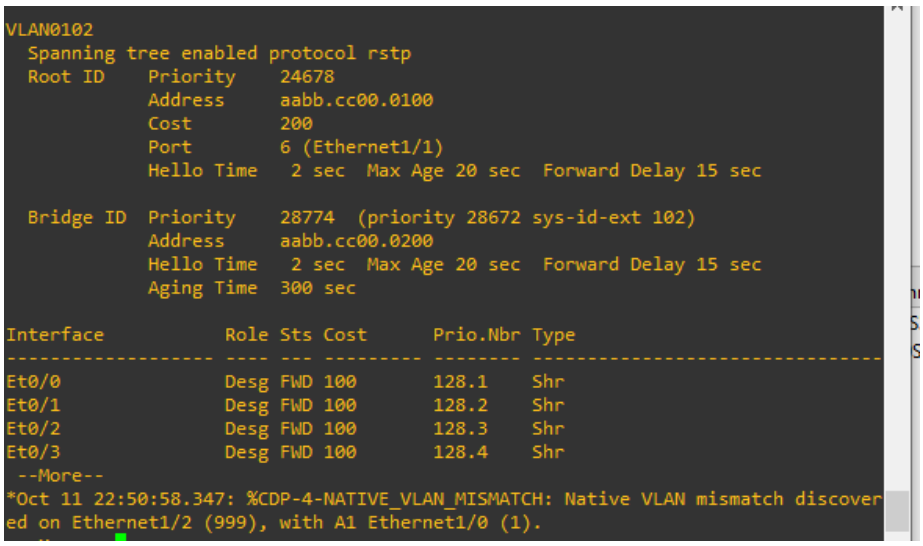


*Figura 24 Parte2 validación RSTP en D2*

**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 Topologia 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

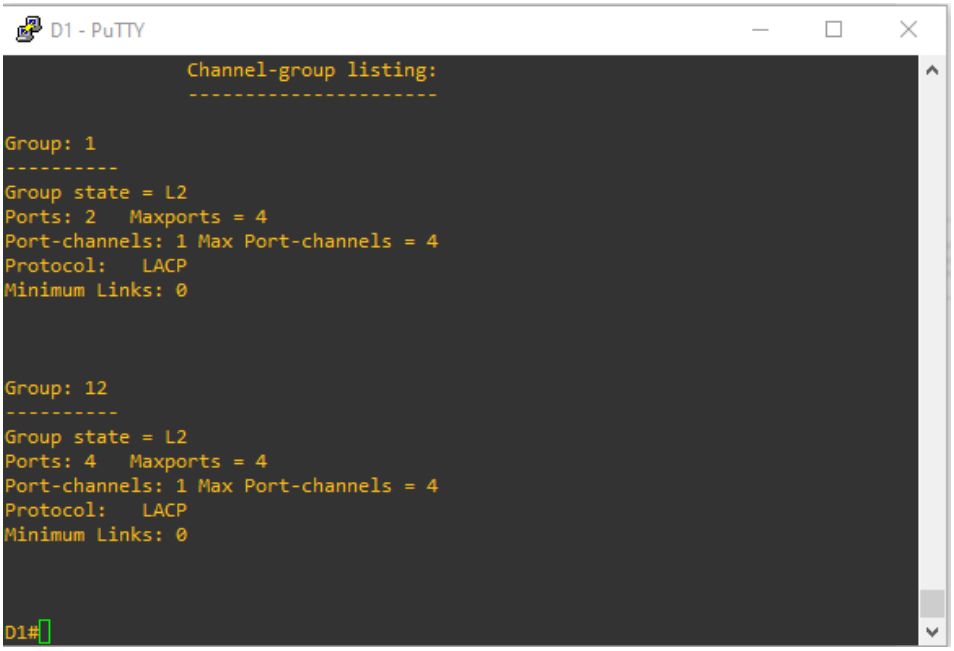


*Figura 25 Parte2 validación EtherChannel en D1*

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

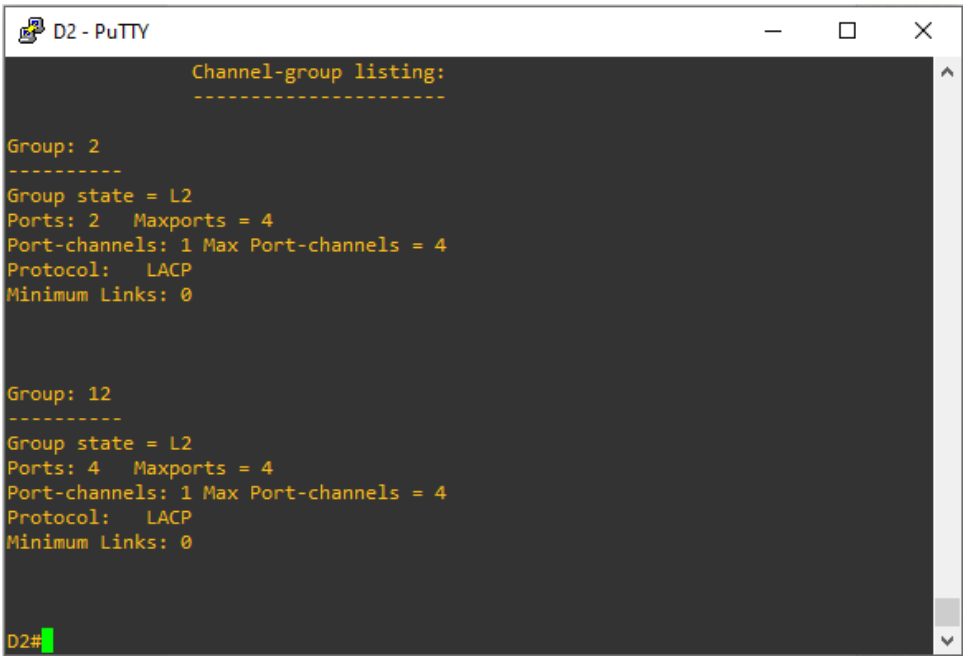


*Figura 26 Parte2 validación EtherChannel en D2*

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

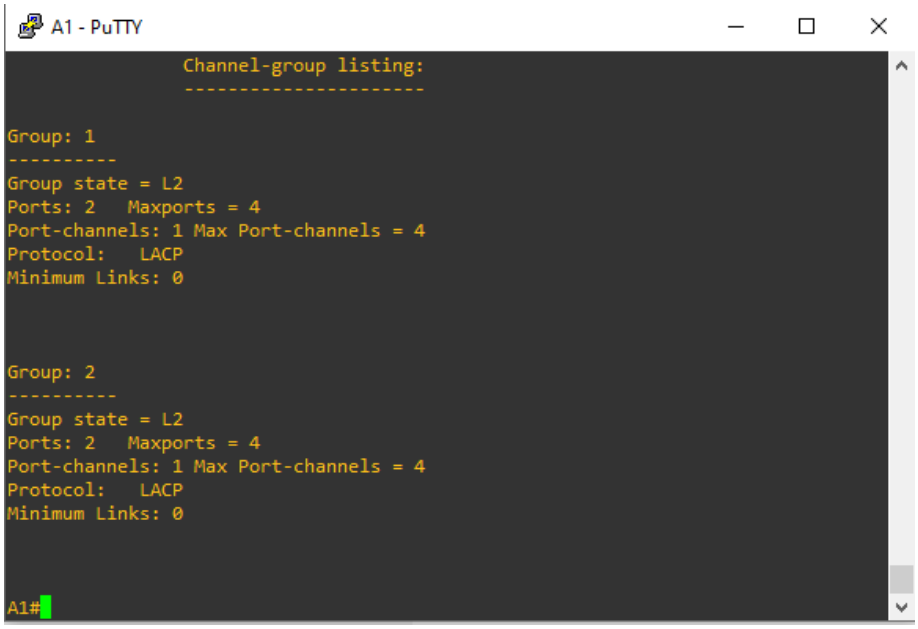


*Figura 27 Parte2 validación EtherChannel en D2*

**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

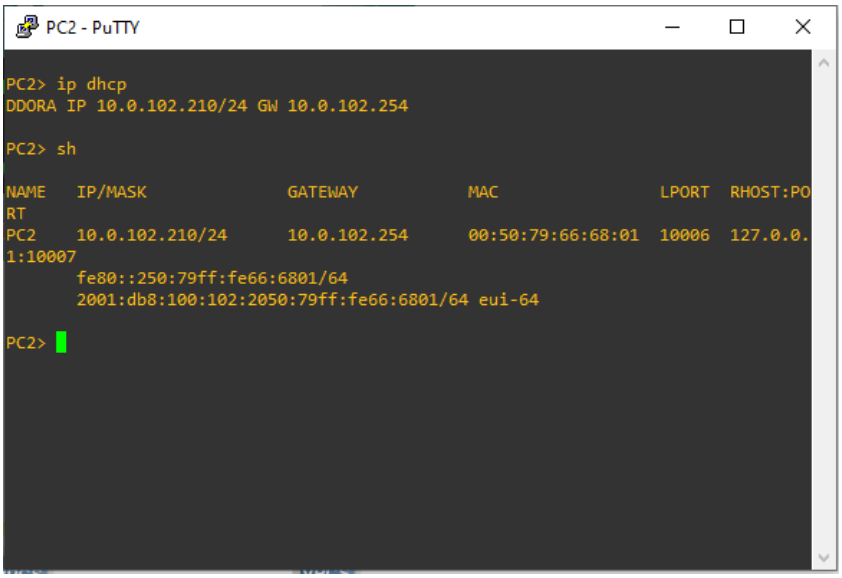


*Figura 28 Parte2 Validación DHCP PC2*

**Validación de correcto direccionamiento Dhcp desde PC3**

Comando para asignación ip: Ip dhcp

Comando validación: sh

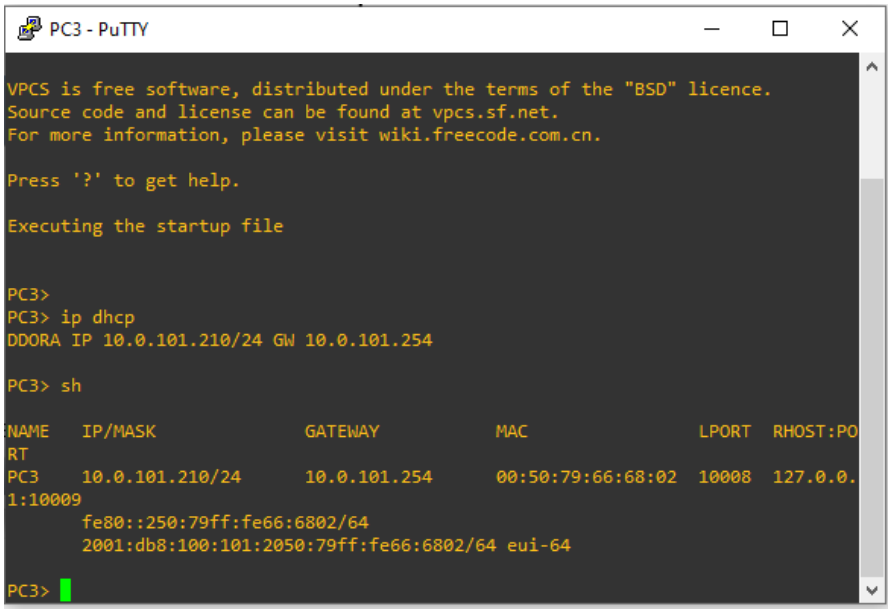


*Figura 29 Parte2 Validación DHCP PC3*

## 2.8 Verifique la conectividad de la LAN local

### Validaciones de conectividad desde PC1

Ping hacia D1 IP 10.0.100.1

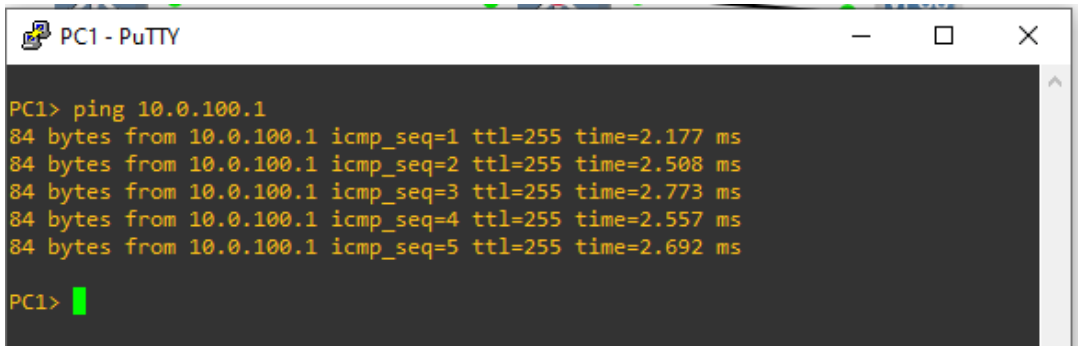


*Figura 30 Parte2 Conectividad LAN PC1 D1*

Ping hacia D2 IP 10.0.100.2

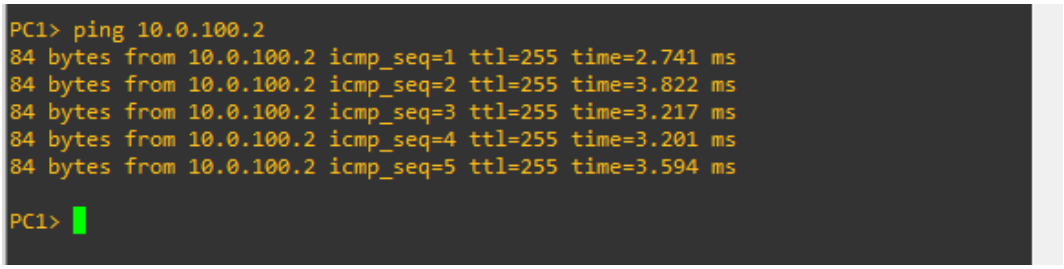


*Figura 31 Parte2 Conectividad LAN PC1 hacia D2*

Ping hacia PC4 IP 10.0.100.6

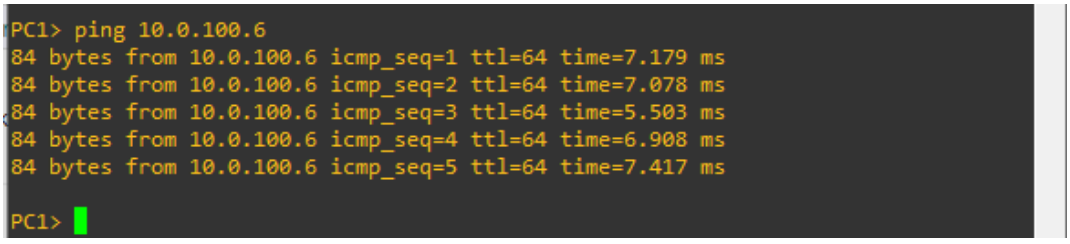


*Figura 32 Parte2 Conectividad LAN PC1 hacia PC4*

**Validaciones de conectividad desde PC2**

Ping hacia D1 IP 10.0.102.1

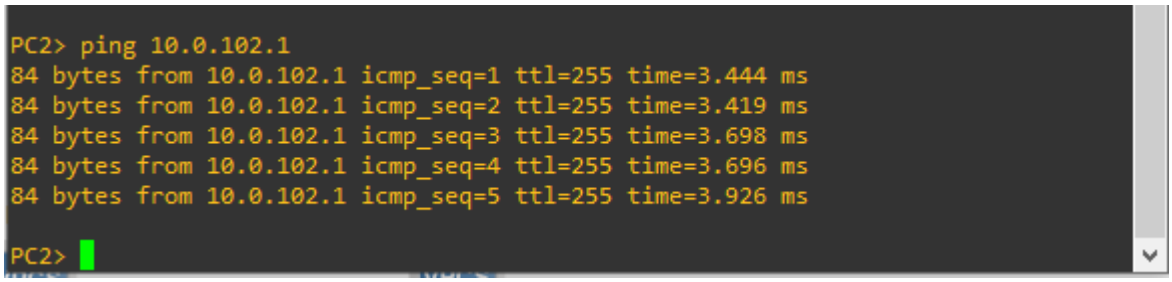


*Figura 33 Parte2 Conectividad LAN PC2 hacia D1*

Ping hacia D2 IP 10.0.102.2

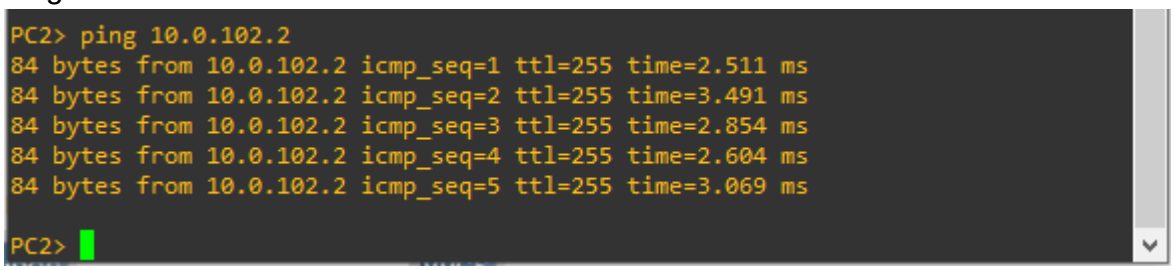


*Figura 34 Parte2 Conectividad LAN PC2 hacia D2*

**Validaciones de conectividad desde PC3**

Ping hacia D1 IP 10.0.101.1

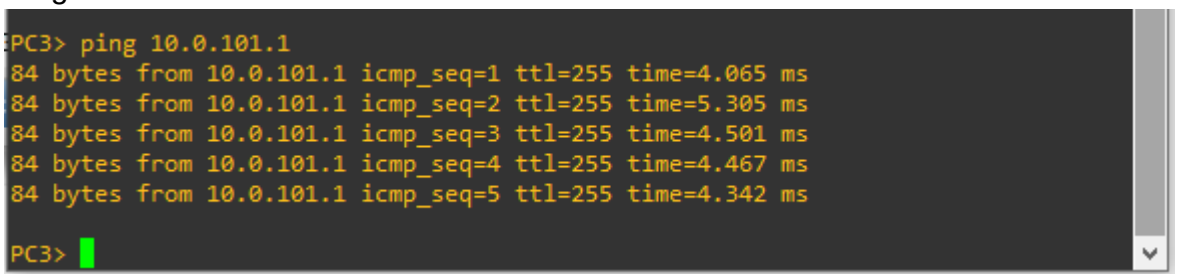


*Figura 35 Parte2 Conectividad LAN PC3 hacia D1*

Ping hacia D2 IP 10.0.101.2

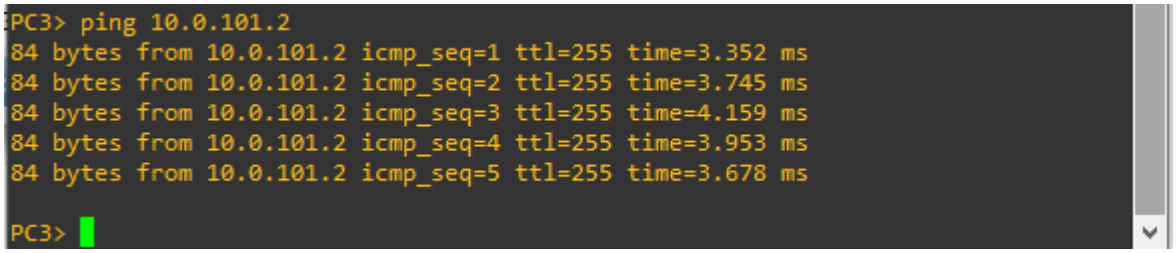


*Figura 36 Parte2 Conectividad LAN PC3 hacia D2*

## Validaciones de conectividad desde PC4

Ping hacia D1 IP 10.0.100.1

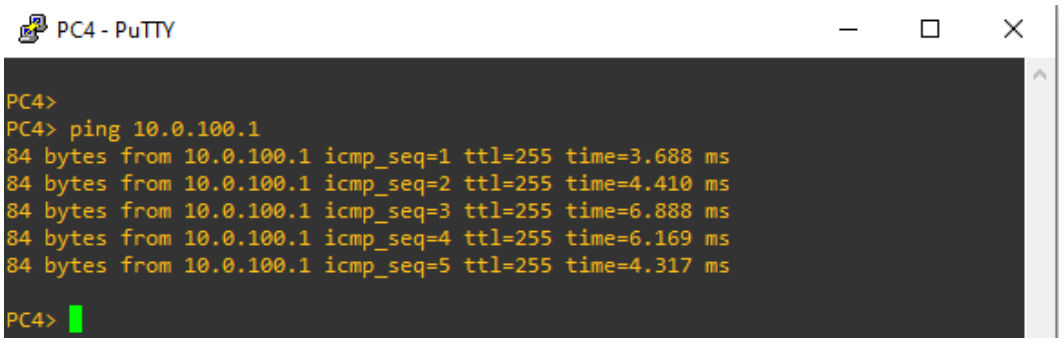


*Figura 37 Parte2 Conectividad LAN PC4 hacia D1*

Ping hacia D2 IP 10.0.100.2

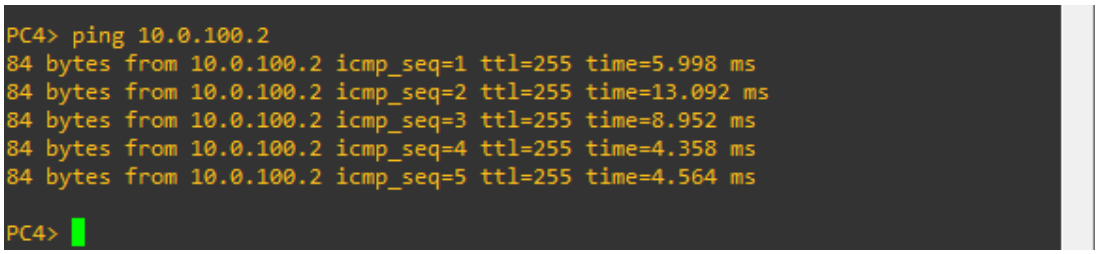


*Figura 38 Parte2 Conectividad LAN PC4 hacia D2*

Ping hacia PC1 IP 10.0.100.5

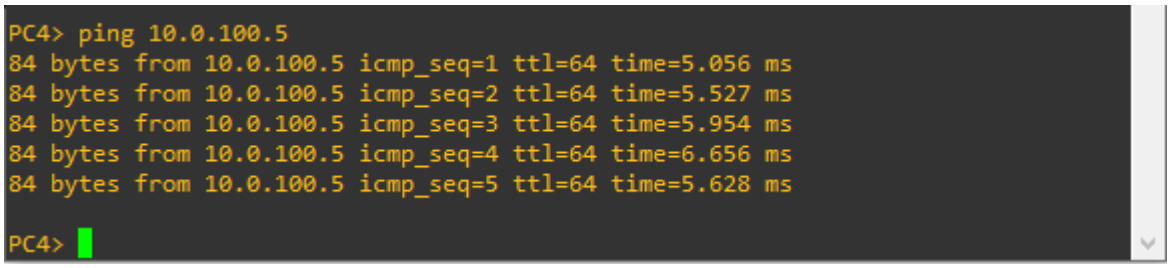


*Figura 39 Parte2 Conectividad LAN PC4 hacia PC1*

## 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 Compañia” (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

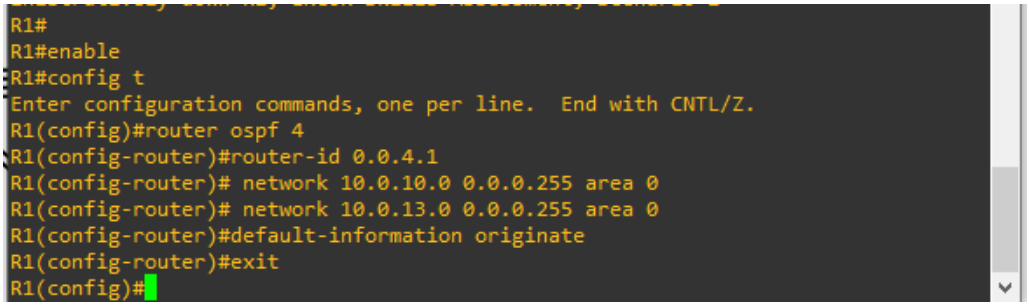


*Figura 40 Parte 3 Configuración OSPF v2 en R1*

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

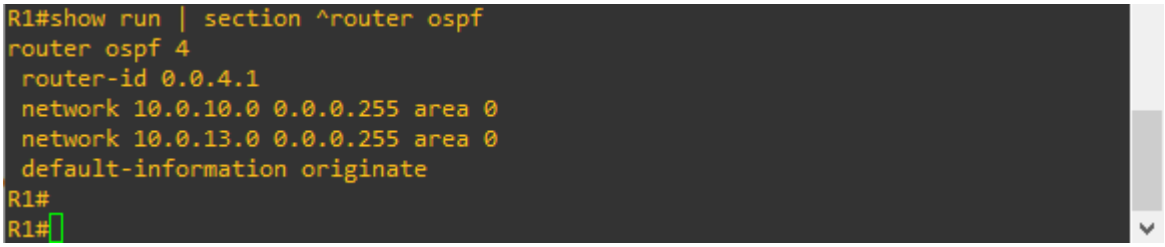


*Figura 41 Parte 3 Configuración OSPF v2 en R1*

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

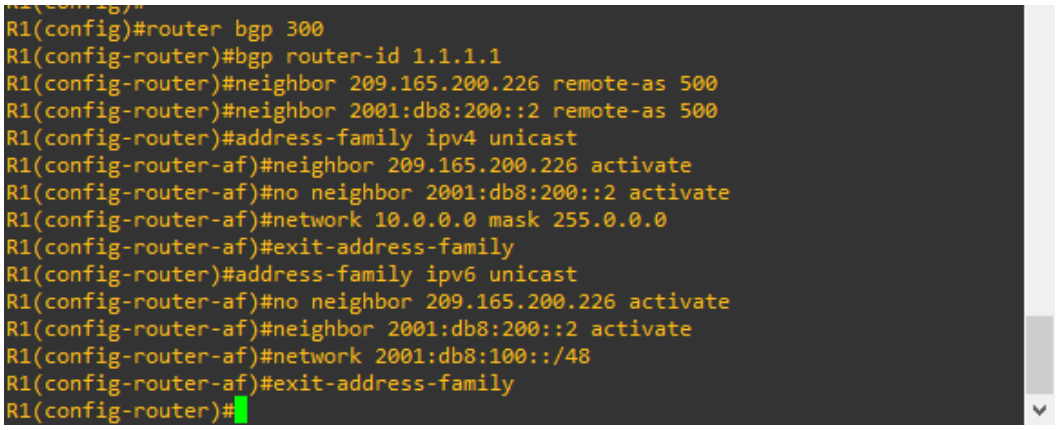


*Figura 44 Parte 3 Configuración BGP en R1*

**Validación de parámetros ingresados en R1**
comando: show run | section router bgp.

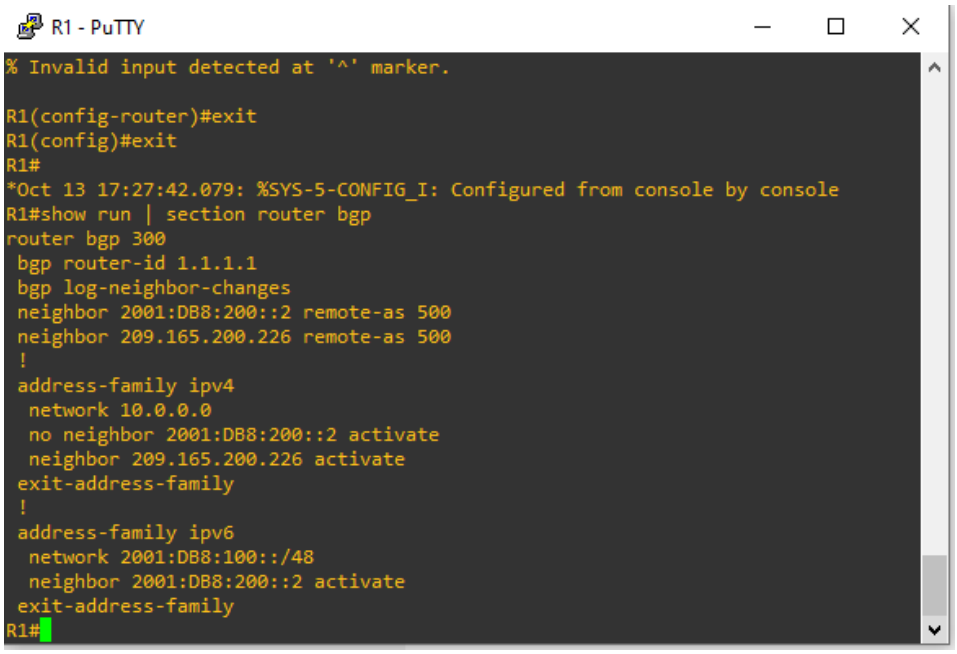


*Figura 45 Parte 3 Validación BGP en R1*

**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

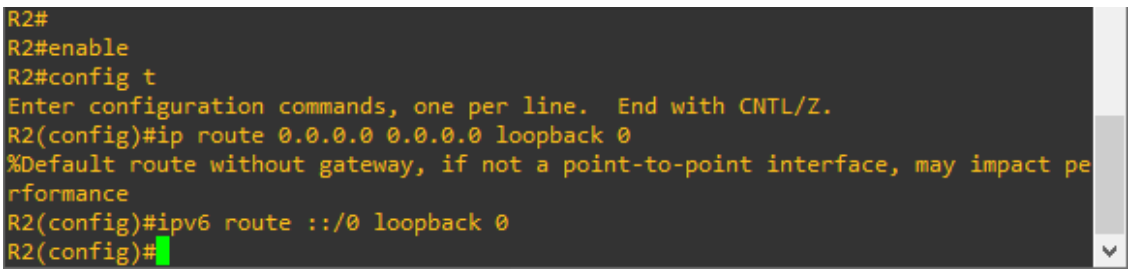


*Figura 46 Parte 3 Configuración rutas estáticas en R2*

Configuración de proceso BGP en R2 mediante número ASN 500 y router id 2.2.2.2, establecimiento de redes vecinas mediate 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

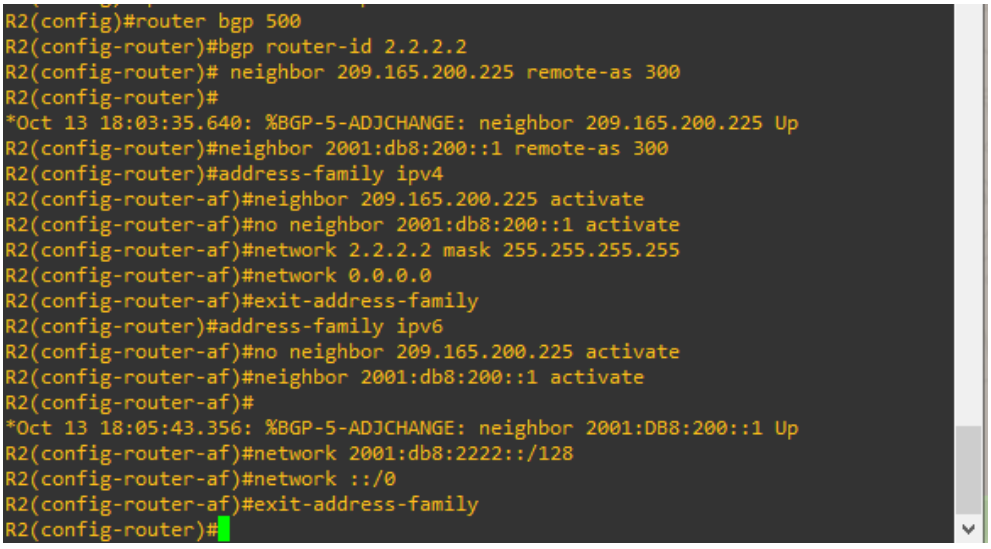


*Figura 47 Parte 3 Configuración BGP en R2*

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

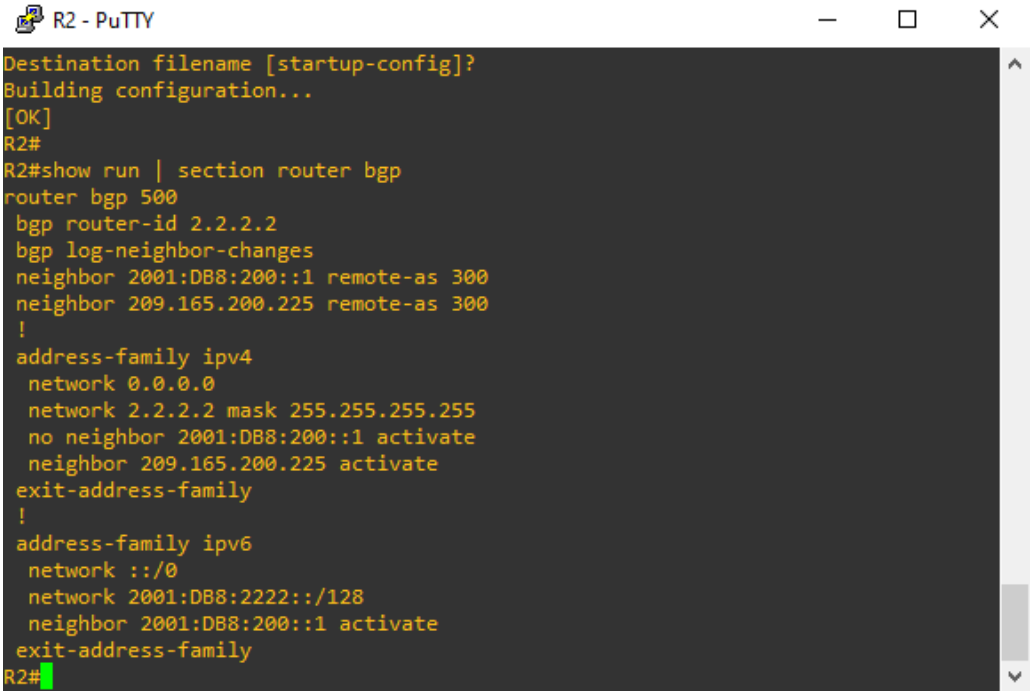


*Figura 48 Parte 3 Validación BGP en R2*

Comando: show run | include route


*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, Configracion classic single-area OSPF V3 mediante ID6 y router ID 0.0.6.3. y asinacion 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

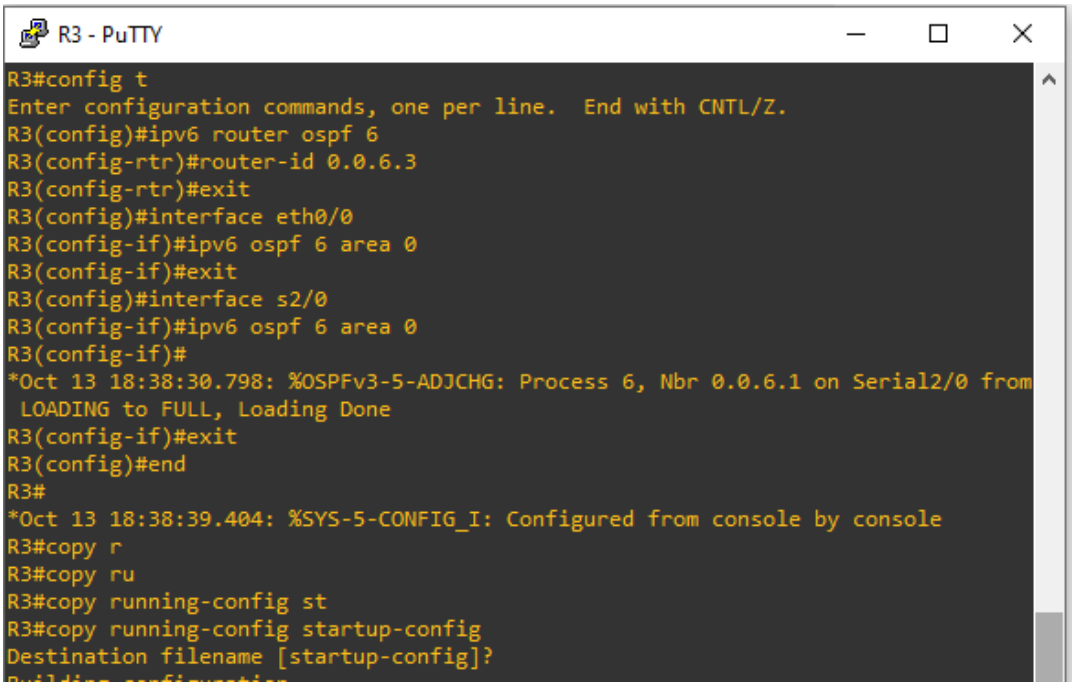


*Figura 50 Figura 49 Configuración OSPF v3 en R3*

**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

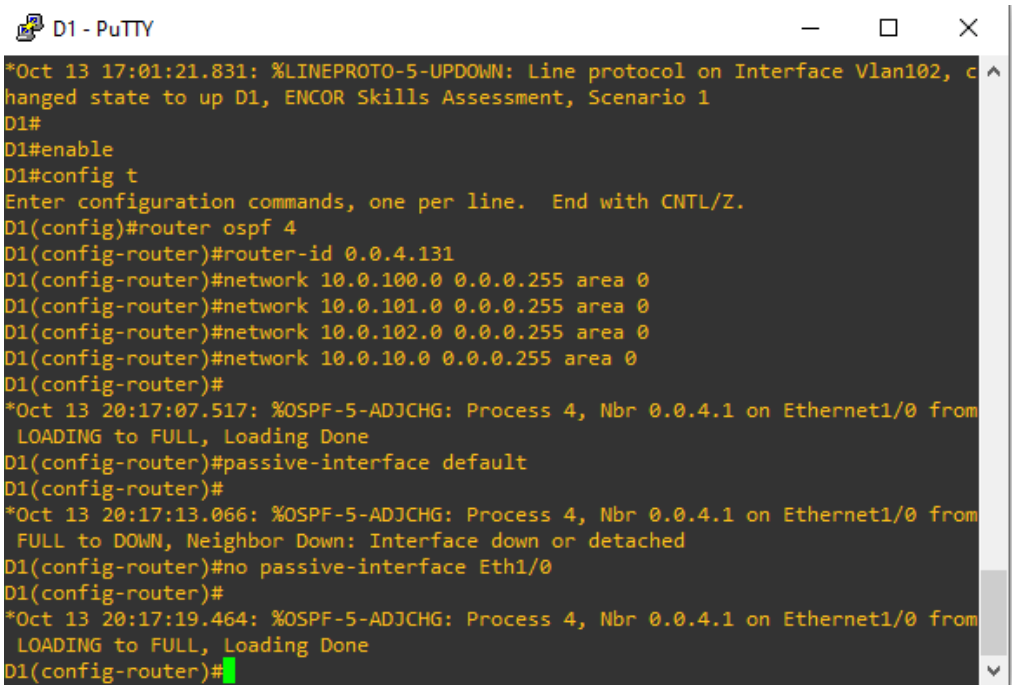


*Figura 53 Configuración OSPF v2 en D1*

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

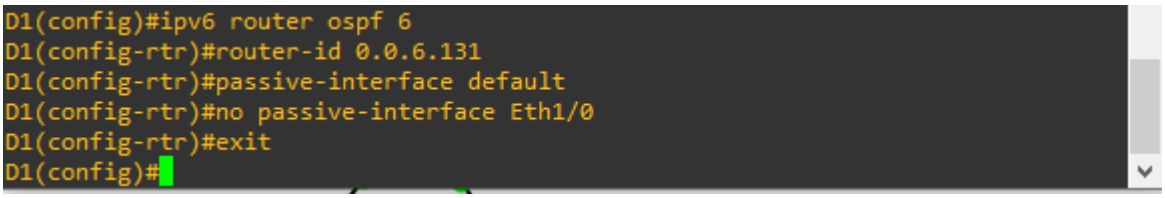


*Figura 54 Configuración OSPF v3 en D1*

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

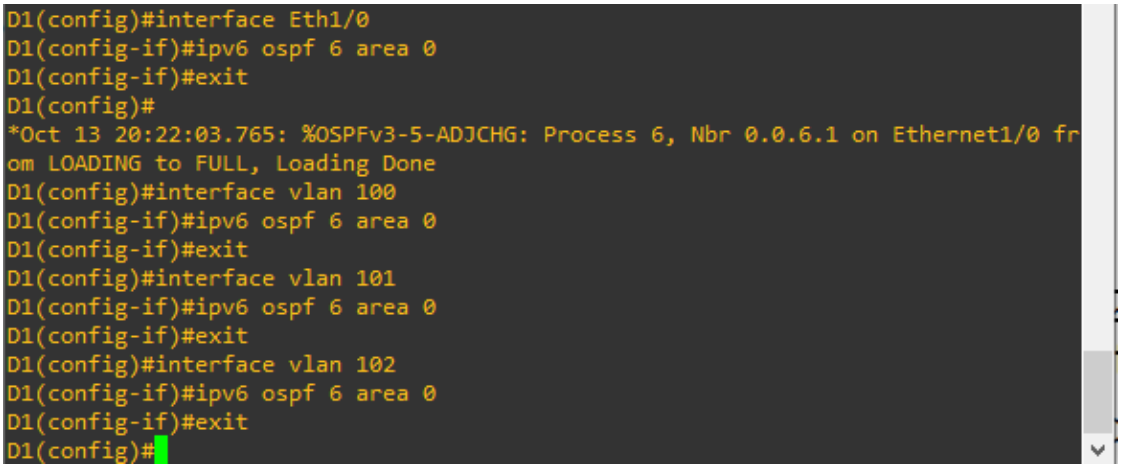


*Figura 55 Anuncio de redes OSPF en D1*

**Validación configuración en D1**

Comando: show run | section ^ipv6 router

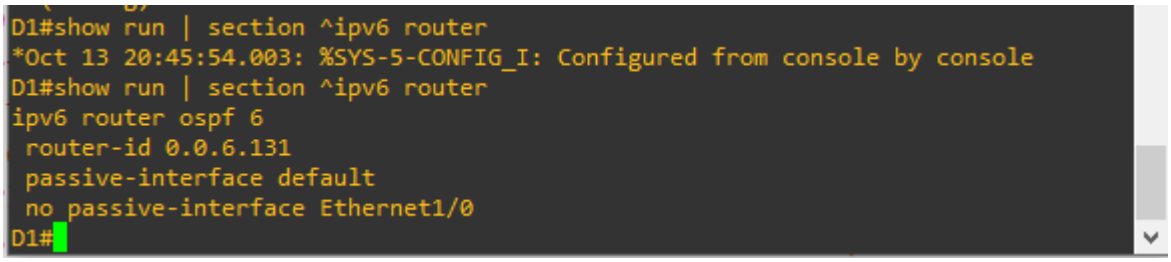


*Figura 56 Validación OSPF v3 en D1*

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

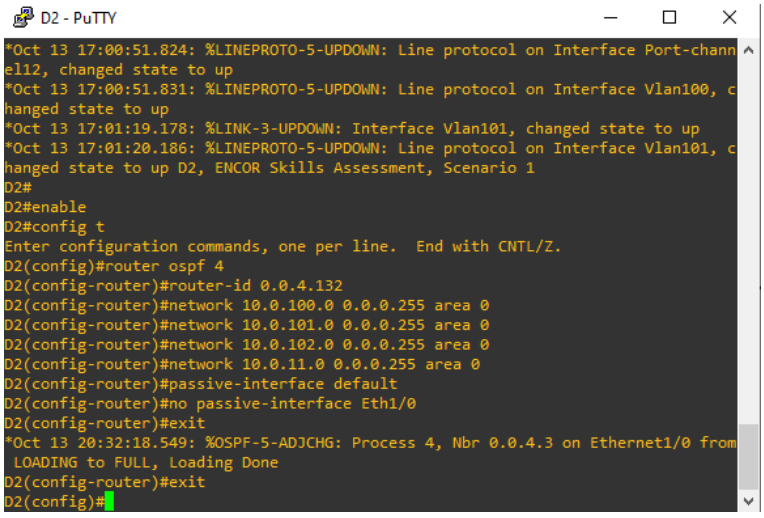


*Figura 58 Configuración OSPF v2 en D2*

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.

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

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

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

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

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

**4.2 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.

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

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

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

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

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

**4.3 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 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 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

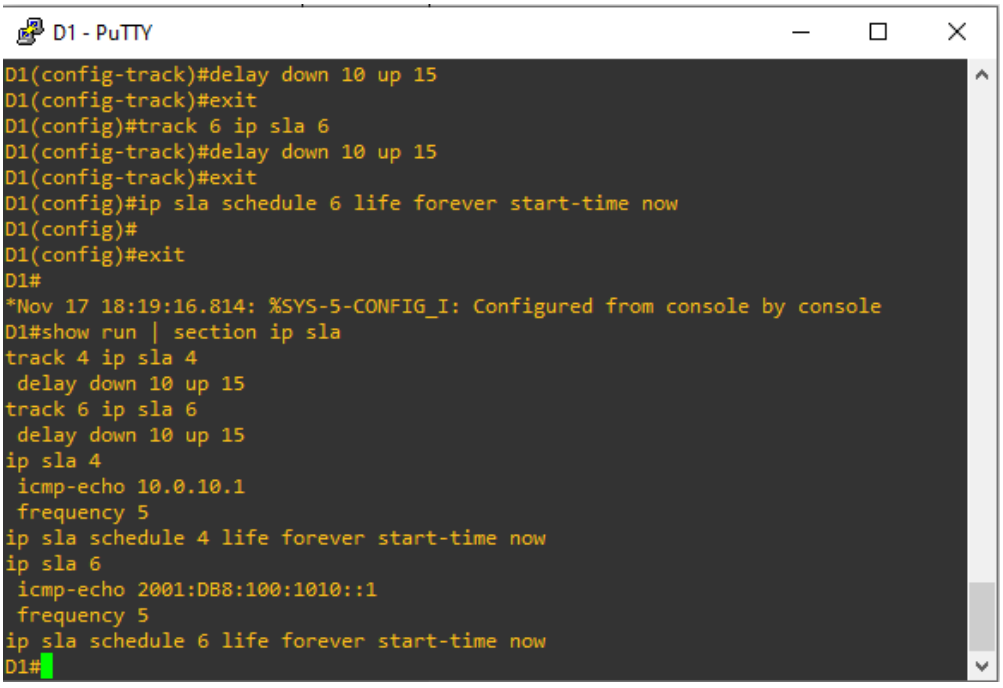


*Figura 63 Validación SLA D1*

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

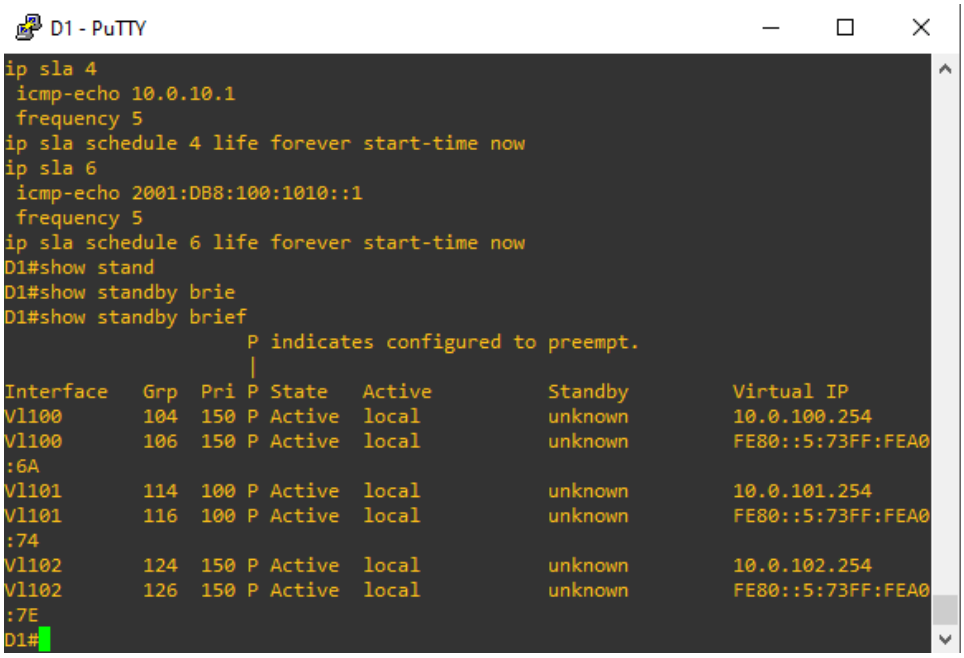


*Figura 64 Validación segmentos vlan D2*

**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

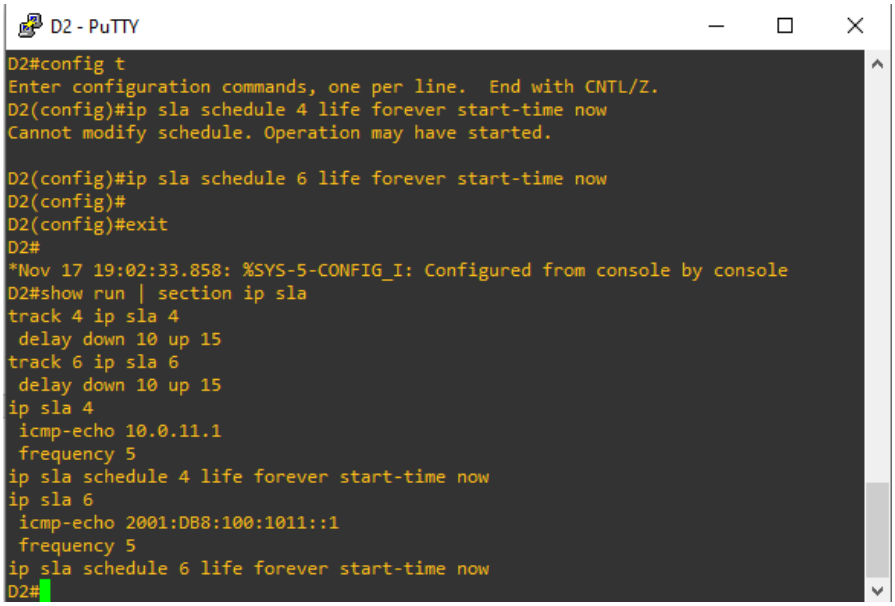

*Figura 65 Validación SLA D2*

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

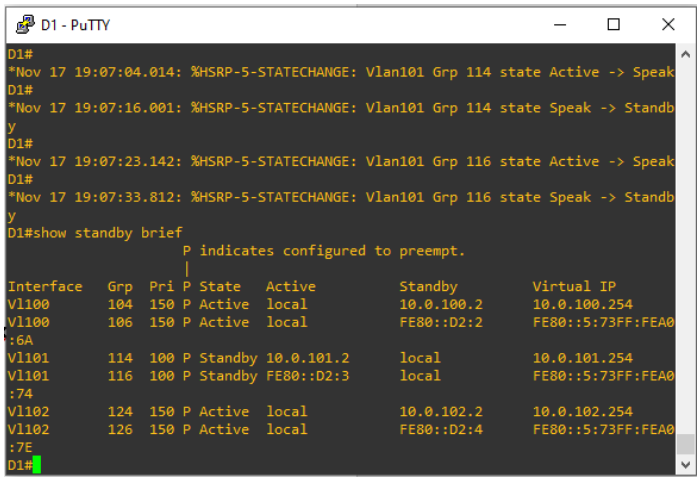


*Figura 66 Validación paso 4 D1*

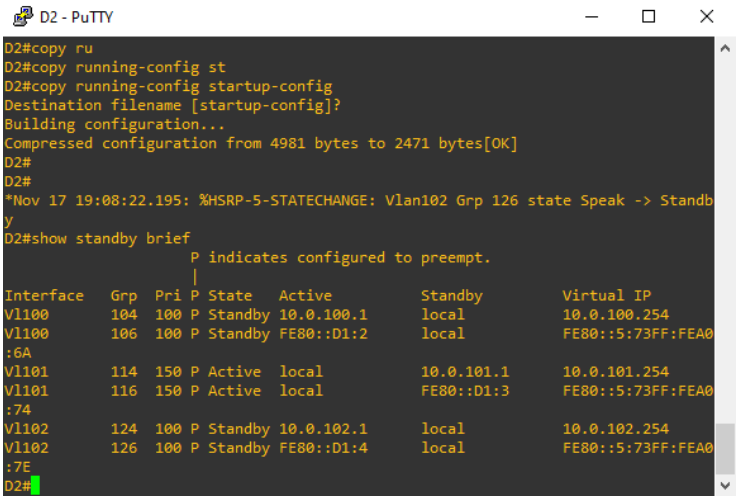


*Figura 67 Validación paso 4 D2*

## Parte 5: Seguridad

**5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción 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)#$dmin 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)#$dmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco
D2(config)#
```

*Figura 69 Configuración SCRYPT D2*

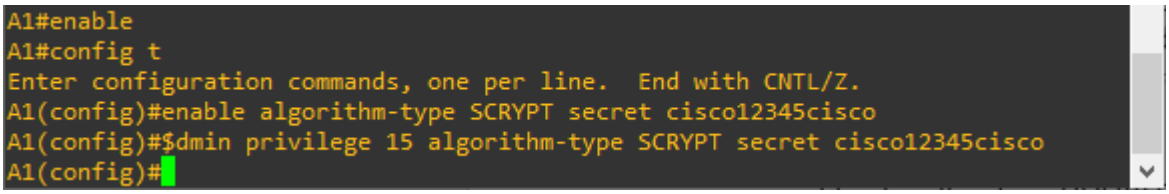


*Figura 70 Configuración SCRYPT A1*

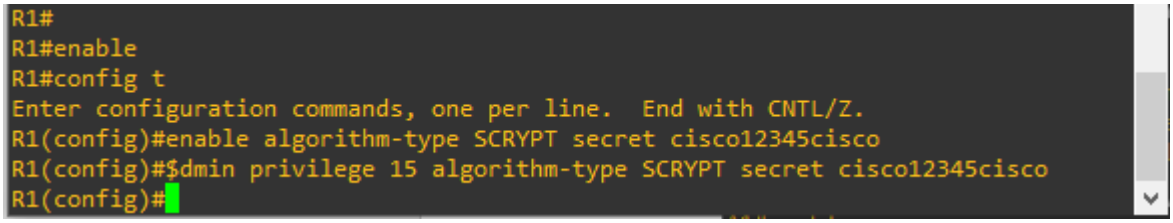


*Figura 71 Configuración SCRYPT R1*

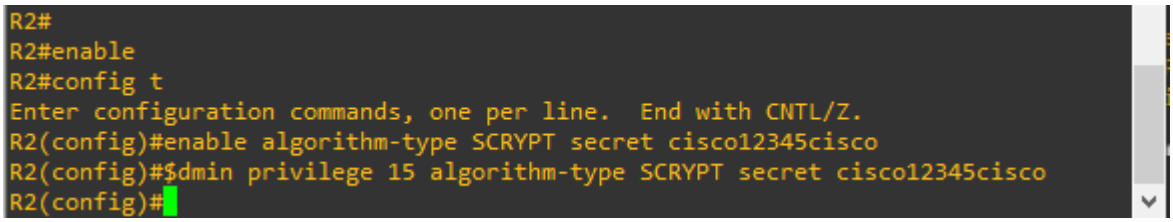


*Figura 72 Configuración SCRYPT R2*

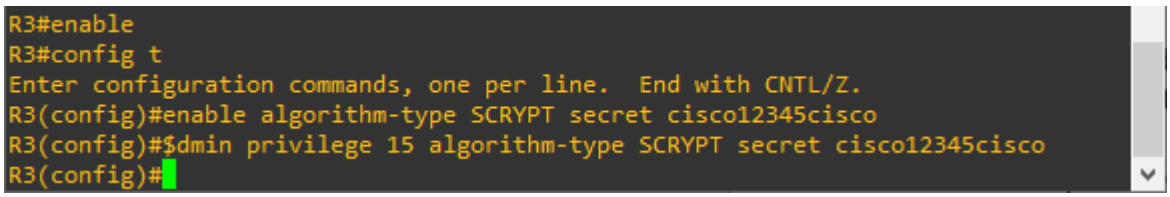


*Figura 73 Configuración SCRYPT R3*

Validación de la configuración de seguridad en todos los dispositivos (ejemplo D1-R3)
Comando utilizado: show run | include secret

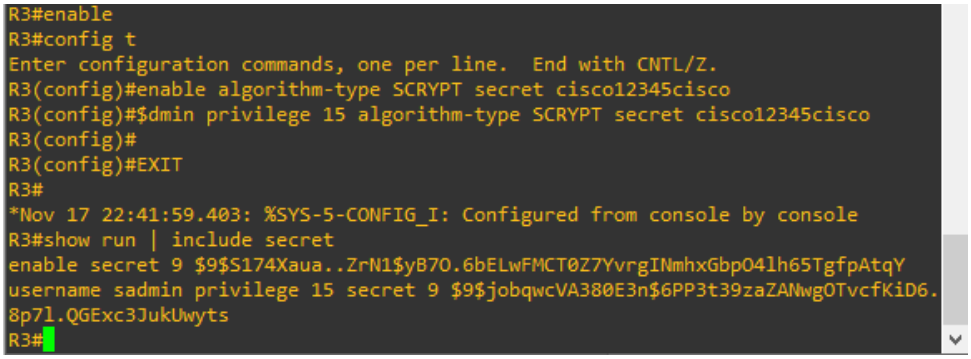


*Figura 74 Validación SCRYPT R3*

**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 $9$Sg3OrQU06bC/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

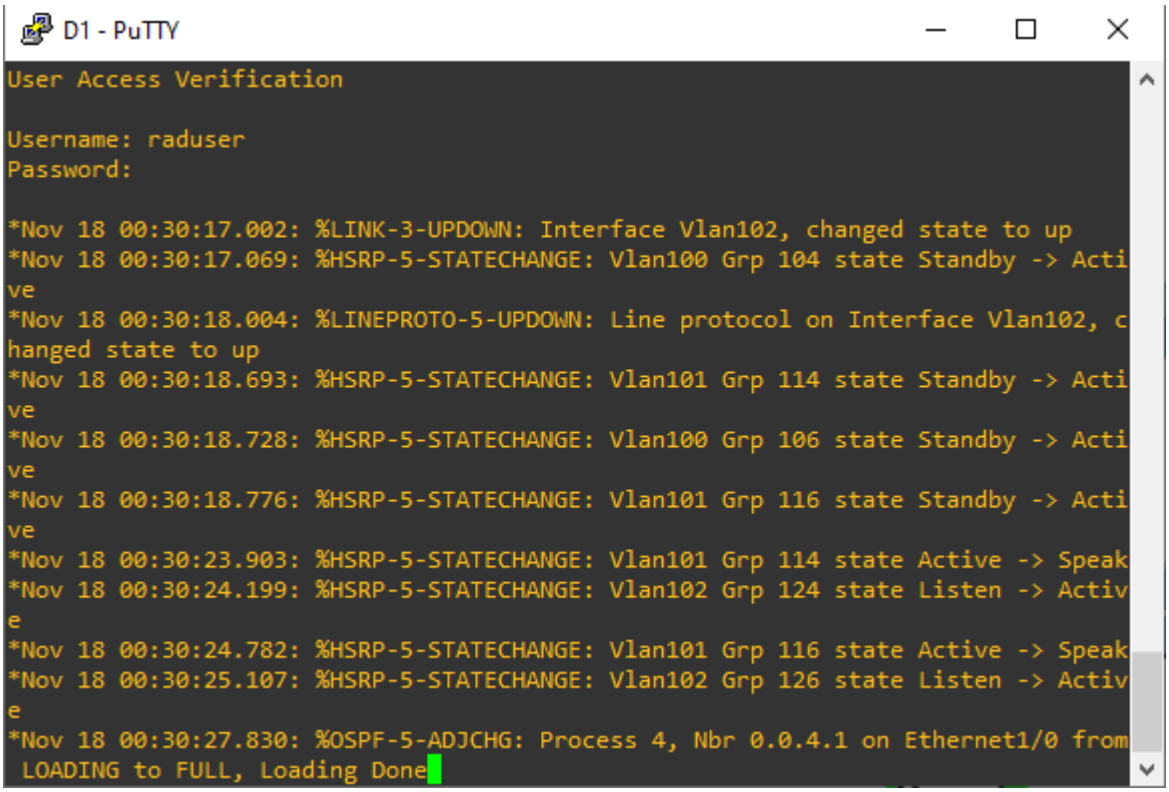


*Figura 78 Loggin verificación D1*

## 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


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

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 Topologia 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

**Validacion sincronización NTP en R1 hacia R2**

Comando utilizado: show ntp status | include stratum

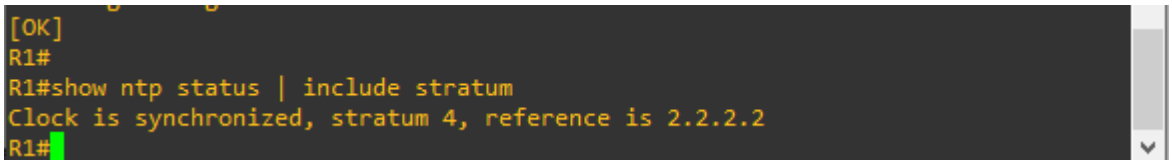


*Figura 82 Validación NTP R1*

**Validacion estado de registro syslog en R1**

Comando utilizado: show run | include logging


*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


*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

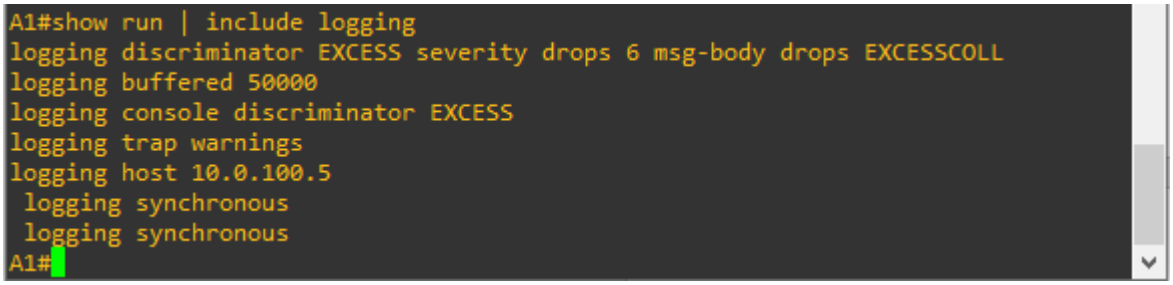


*Figura 94 Syslog A1*

### 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 configuraciónes, 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 fisico sin que se presenten interferencias, esto se orienta siempre que deseemos trabajar con VLANs.

La implementacion de EtherChannel permite el aprovechamiento de las conexiones fisicas entre dispositivos con el fin de crear canales logicos con una velocidad mayor, tolerante a fallos mediante balanceo de cargas y redireccion de trafico en caso de presentarse caida de algun canal, el escenario propuesto representa una fiel imagen del tipo de problematicas en temrinos de uso de ancho de banda que encontraremos en el entorno laboral y que con una parametrizacion sencilla por medio de esta tecnologia podemos solventar y optimizar.

El protocolo OSPF dado que funciona partir de un principío de estado de enlace, garantiza un manejo de transferencia optimo orientado al establecimiento e interpretacion de las rutas mas cortas posibles, su adecuacion a trabajo por medio de areas facilita la interpretacion del enrutamiento y se adapta facilmente a la topologia palnteada 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!AmIJYeiNT1llnWR0hoMxgBNv1CJ

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