

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ALBERTO PARADA MUÑETON

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ALBERTO PARADA MUÑETON

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

DIRECTOR:
MSC. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 29 de noviembre de 2021

AGRADECIMIENTOS

Agradezco primeramente a Dios por regalarme la salud, el conocimiento y la sabiduría para llevar a cabo cada uno de los proyectos de vida que me he trazado y permitirme culminar este diplomado CCNP, también porque ha proveído económicamente para poder cubrir los gastos que acarrearán mis estudios.

Un gran agradecimiento a mi hermosa esposa por su paciencia y ánimo que me dio ya que no es fácil trabajar y estudiar a la misma vez, pero ella con su admiración que tiene así mí me motiva a seguir para cumplir mis proyectos.

A mi familia como lo es mi madre Gloria Parada, porque ella hace parte de mis más grandes motivaciones para lograr cada uno de esos sueños que deseaba cumplir desde niño, mis hermanas porque ellas se sienten orgullosas de mí cuando ven como poco a poco he venido superando muchos obstáculos y cumpliendo metas que me he trazado.

Gracias a los tutores, por brindarnos todos los conocimientos que nos hacen ser mejores profesionales y nos preparan en conocimientos más sólidos para la ejecución de cada uno de ellos, es una tarea ardua para ellos ya que no es sencillo lidiar con diferentes personalidades, muchas gracias por querer hacer de estos estudiantes los mejores ingenieros que se graduarán de la universidad UNAD.

Doy también un agradecimiento a mis compañeros de grupo, porque compartieron de sus conocimientos y habilidades, no fue un proceso fácil ya que estamos adquiriendo muchos conocimientos de los cuales ellos aportaron de cierta forma para que yo los pusiera en práctica, mil gracias por su compañerismo.

A la universidad UNAD, por permitirnos ser parte de ella formando personas y profesionales humanos y con las mejores bases para emprender como profesionales en este proyecto de vida, porque a muchos de nuestros compañeros les dieron la forma económica para que no aplazaran sus estudios ya que la pandemia ha sido un obstáculo para muchos de aplazar sus proyectos, pero la UNAD con su humanismo ha hecho que muchos estudiantes hoy puedan decir se logró un objetivo más en mi vida.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO.....	5
LISTA DE TABLAS.....	7
LISTA DE FIGURAS	8
GLOSARIO.....	10
RESUMEN	11
ABSTRACT	12
INTRODUCCIÓN	13
DESARROLLO ESCENARIO PROPUESTO	14
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces.	14
Paso 1: Cablear la red como se muestra en la topología.....	14
Paso 2: Configurar los parámetros básicos para cada dispositivo	16
Configuración parámetros básicos router R1	16
Configuración parámetros básicos router R2	17
Configuración parámetros básicos router R3	17
Configuración parámetros básicos switch D1.....	18
Configuración parámetros básicos switch D2.....	20
Parte 2: Configurar la capa 2 de la red y el soporte de Host.....	25
2.1 Configuración enlaces troncales de switches.....	25
2.2 Configuración VLAN 999 como nativa en los enlaces troncales	26
2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP	27
2.4: Configurar los puentes raíz (root bridges)	27
2.5 Creacion de EtherChannel LACP en switch D1,D2 y A1.....	28
2.6 Configuración de los puertos de acceso en los switches para los PC.....	32
2.7 Verifique los servicios DHCP IPv4 para los PC.....	33
Parte 3: Configurar los protocolos de enrutamiento	39
3.1 Configuración OSPFv2 en área 0.....	39
3.2 Configuración OSPFv3.....	42
3.3 En R2 en la “Red ISP”, configure MP-BGP.	44
3.4 Configuración MP-BGP en la red ISP R1	45

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)	50
4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 fa0/0.	50
4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 fa0/0.	51
4.3 En D1 configure HSRPv2.	52
4.4 En D2 configure HSRPv2.	54
Parte 5: Seguridad	57
5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	57
5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	58
5.3 En todos los dispositivos (excepto R2), habilite AAA.	59
5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	59
5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	60
5.6 Verifique el servicio AAA en todos los dispositivos (except R2).	60
Parte 6: Configure las funciones de Administración de Red	62
6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.	62
6.2 Configure R2 como un NTP maestro.	64
6.3 Configure NTP en R1, R3, D1, D2, y A1.	64
6.4 Configure Syslog en todos los dispositivos excepto R2	65
6.5 Configure SNMPv2c en todos los dispositivos excepto R2	66
CONCLUSIONES.....	71
BIBLIOGRAFÍA	72

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento IP de los router, switches y PC	15
--	----

LISTA DE FIGURAS

Figura 1. Topología de red	14
Figura 2. Verificación de spanning-tree switch D1	27
Figura 3. Verificación de spanning-tree switch D2	28
Figura 4. verificación del LACP en D1	31
Figura 5. verificación del LACP en D2	31
Figura 6. verificación del LACP en A1	31
Figura 7. PC2 toma ip por dhcp	33
Figura 8. PC3 toma ip por dhcp	33
Figura 9. PC1 se configura con ip estática y hace ping a switch D1	34
Figura 10. PC1 hace ping a switch D2	34
Figura 11. Configuración IP estática a PC4	35
Figura 12. PC1 hace ping a PC4	35
Figura 13. PC2 hace ping a switch D1	36
Figura 14. PC2 hace ping a switch D2	36
Figura 15. PC3 hace ping a switch D1	37
Figura 16. PC3 hace ping a switch D2	37
Figura 17. PC4 hace ping a switch D1	38
Figura 18. PC4 hace ping a switch D2	38
Figura 19. PC4 hace ping a switch PC1	39
Figura 20. Verificación de la tabla de enrutamiento IPv4 router R1	47
Figura 21. Verificación de la tabla de enrutamiento IPv4 router R2	47
Figura 22. Verificación de la tabla de enrutamiento IPv4 router R3	48
Figura 23. Verificación de la tabla de enrutamiento IPv4 router D1	48
Figura 24. Verificación de la tabla de enrutamiento IPv4 router D2	49
Figura 25. Verificación de la tabla de enrutamiento IPv4 router A1	49
Figura 26. Ping desde switch D1 y switch D2 a Loopback 0	49
Figura 27. Verificación de las SLAs en switch D1	51
Figura 28. Verificación de las SLAs en switch D2	52
Figura 29. Verificación del standby en switch D1	56
Figura 30. Verificación del standby en switch D2	57
Figura 31. Verificación de usuario y contraseña creado en switch D1	58
Figura 32. Verificación de usuario y contraseña creado en switch D2	58
Figura 33. Verificación de usuario y contraseña creado en switch A1	58
Figura 34. Verificación de usuario y contraseña creado en switch R1	59
Figura 35. Verificación de usuario y contraseña creado en switch R2	59
Figura 36. Verificación de usuario y contraseña creado en switch R3	59
Figura 37. Verificación de autenticación en router R1	61
Figura 38. Verificación de autenticación en router R3	61
Figura 39. Verificación de autenticación en switch D1	61
Figura 40. Verificación de autenticación en switch D2	61
Figura 41. Verificación de autenticación en switch A1	62
Figura 42. validación configuración NTP en router R2	64
Figura 43. validación configuración NTP en router R1	64
Figura 44. validación configuración NTP en router R3	64
Figura 45. validación configuración NTP en switch D1	65

Figura 46. validación configuración NTP en switch A1	65
Figura 47. validación configuración NTP en switch D2	65
Figura 48. Verificación de la configuración SNMP en Router R1	68
Figura 49. Verificación de la configuración SNMP en Router R3	69
Figura 50. Verificación de la configuración SNMP en Switch D1	69
Figura 51. Verificación de la configuración SNMP en Switch D2	70
Figura 52. Verificación de la configuración SNMP en Switch A1	70

GLOSARIO

VLAN: Red de área local virtual, es un método para crear redes lógicas independientes dentro de una misma red física, su función principal es dividir de manera lógica una red física en varios grupos de redes usando el mismo medio físico de distribución, las VLAN son creadas en los switches.

SPANNING TREE: Protocolo que funciona en capa 2, su objetivo es controlar los enlaces redundantes a fin de evitar loop en la red.

ETHERCHANNEL: Protocolo que hace posible agregar o unificar enlaces físicos en un solo medio lógico, permitiendo sumar la velocidad de cada enlace físico en uno solo además de crear una redundancia entre los switches.

OSPF: Protocolo de enrutamiento dinámico para redes IP basado en algoritmos que facilitan la entrega de paquetes por el camino más corta.

ENRUTAMIENTO: El enrutamiento es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa y el ancho de banda

CNNP: (Cisco Certified Network Profesional) es el nivel Intermedio de Certificación de la compañía. Para obtener esta certificación.

OSPFv3: Open Shortest Path First, protocolo de enrutamiento dinámico que detecta cambios en la topología, fallas de enlace y converge en una nueva estructura rápidamente, específicamente para IPv6.

PACKET TRACER: Es un software de aprendizaje y simulación de redes de cisco, permite a los usuarios crear topologías de red y configurar dispositivos de red.

GNS3: Es un simulador grafico de red lanzado en 2008, que nos permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

RESUMEN

El presente trabajo contiene el desarrollo de las pruebas de habilidades prácticas del diplomado de profundización cisco CCNP que fueron desarrolladas en el simulador GNS3 de cisco, la actividad planteada consta de un escenario con 6 partes, la primera consiste en construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces, la segunda en configurar la capa 2 de la red y el soporte de Host, la tercera en configurar los protocolos de enrutamiento usados como fue OSPF y BGP, la cuarta en configurar la redundancia del primer salto, la quinta en configurar la seguridad y finalmente en configurar las características de administración de red a través de SNMP.

Por medio de los protocolos de enrutamiento usados entre ellos OSPF y BGP se logró la comunicación entre cada uno de los dispositivos de red implementados en el escenario propuesto y host finales.

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

ABSTRACT

The present work contains the development of the practical skills tests of the Cisco CCNP deepening diploma that were developed in the Cisco GNS3 simulator, the proposed activity consists of a scenario with 6 parts, the first one consists of building the network and configuring the settings of each device and the addressing of the interfaces, the second to configure the network layer 2 and Host support, the third to configure the routing protocols used such as OSPF and BGP, the fourth to configure the redundancy of the first jump, the fifth to configure security and finally to configure network management features through SNMP.

Through the routing protocols used, including OSPF and BGP, communication was achieved between each of the network devices implemented in the proposed scenario and the final hosts.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

Las redes de datos y de telecomunicaciones nos permiten estar comunicados en todo momento, a nivel personal con nuestros familiares y amigos, en entornos empresariales con los clientes y proveedores.

Los dispositivos de red y la información son vulnerables por los hacker y personas inescrupulosas que quieren atentar contra los activos de una organización y su información, por eso es importante que un administrador de red o ingeniero de telecomunicaciones egresado de la universidad UNAD cuente con las diferentes habilidades para asegurar la infraestructura de red, aplicando la seguridad en los dispositivos Core de la red como son los Router y Switches entre otros.

El presente diplomado nos permite como ingenieros tener la capacidad de planificar, implementar, verificar y solucionar problemas en redes empresariales a nivel LAN y WAN

En este escenario propuesto en el diplomado de profundización cisco CCNP realizaremos la configuración de 3 Router, 3 Switches y 4 Pc que brindara los servicios a una red empresarial de manera convergente, redundante, segura y de alto rendimiento en GNS3 con IOS reales de dispositivos cisco.

En el escenario propuesto fortaleceremos la estructura y diseño de una red corporativa, la configuración de los parámetros básicos de router y swiches, creación de VLAN, enlaces troncales, EtherChannel, configuración de protocolos de enrutamientos OSPF Y BGP, configuración de redundancia del primer salto, a nivel se seguridad encriptación de contraseña, autenticación radius, configuración de servidor NTP, syslog y la administración de la red a través de SNMP entre otros.

DESARROLLO ESCENARIO PROPUESTO

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

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

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

Figura 1. Topología de red

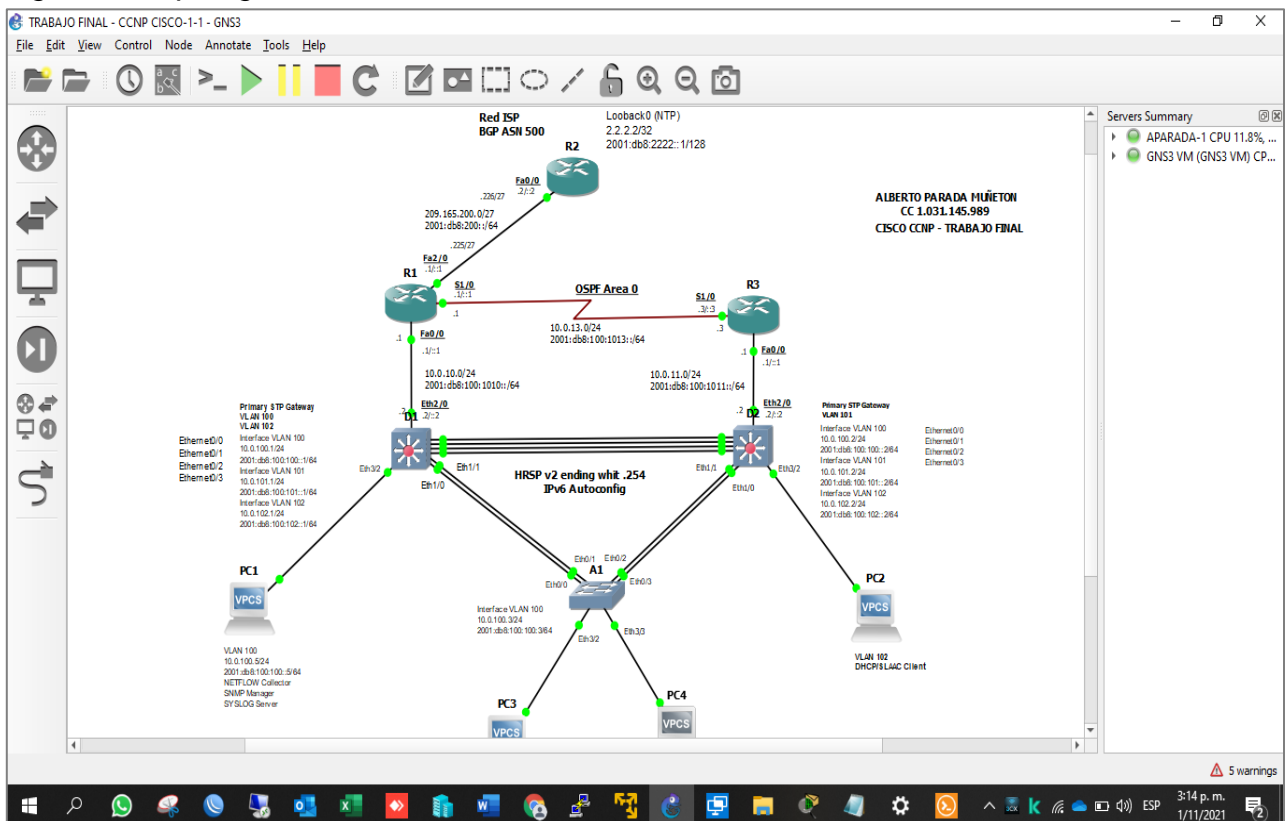


TABLA DE DIRECCIONAMIENTO

Tabla 1. Tabla de direccionamiento ip de los router, switches y PC

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	Fa2/0	209.165.200.29/27	2001:db8:200::1/64	fe80::1:1
R1	Fa0/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
R1	S1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	Fa0/0	209.165.200.30/27	2001:db8:200::2/64	fe80::2:1
R2	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	Fa0/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
R3	S1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	Eth2/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
D1	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
D1	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
D2	Eth2/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
D2	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
D2	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

Paso 2: Configurar los parámetros básicos para cada dispositivo

Configuración parámetros básicos router R1

Se realiza configuración para cambiar nombre del router R1, se habilita Ipv6 en el router, desactivo la traducción de nombres a dirección del dispositivo, configuro el mensaje del día “banner motd”, configuración de la línea de consola y configuro un tiempo de espera ilimitado para la sesión.

```
Router1(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit
```

Se realizo la configuración de las ip de las interfaces de red Fa2/0, Fa0/0 y s1/0 del router R1.

```
R1(config)#interface Fa2/0
R1(config-if)#ip address 209.165.200.29 255.255.255.224
R1(config-if)#ipv6 address fe80::1:1 link-local
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface Fa0/0
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s1/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
```

Configuración parámetros básicos router R2

Se realiza configuración para cambiar nombre del router R2, se habilita Ipv6 en el router, desactivo la traducción de nombres a dirección del dispositivo, configuro el mensaje del día "banner motd", configuración de la línea de consola y configuro un tiempo de espera ilimitado para la sesión.

```
Router2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config-line)#exit
```

Configuración de la IP de la interfaz de red Fa0/0 del router R2.

```
R2(config)#interface Fa0/0
R2(config-if)#ip address 209.165.200.30 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)#ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)#exit
```

Configuración de la IP de la interfaz loopback del router R2.

```
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::f:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
```

Configuración parámetros básicos router R3

Se realiza configuración para cambiar nombre del router R1, se habilita Ipv6 en el router, desactivo la traducción de nombres a dirección del dispositivo, configuro el mensaje del día "banner motd", configuración de la línea de consola y configuro un tiempo de espera ilimitado para la sesión.

```
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
```

```
R3(config-line)#logging synchronous
R3(config-line)#exit
```

Se realiza la configuración de las IP de las interfaces de red Fa0/0 y s1/0 del router R3.

```
R3(config)#interface Fa0/0
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
```

Configuración parámetros básicos switch D1

Se realiza configuración para cambiar nombre del switch D1, se habilita Ipv6 en el router, habilito enrutamiento ip en el switch, desactivo la traducción de nombres a dirección del dispositivo, configure el mensaje del día "banner motd", configuración de la línea de consola y configure un tiempo de espera ilimitado para la sesión.

```
Switch(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
```

Se realiza la creación de las VLAN 100, VLAN 101, VLAN 102, VLAN 999 con su nombre.

```
D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
```

```
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
```

Se configura el puerto ethernet2/0 con el comando no switchport para que brinde la capacidad de capa 3 al puerto y se configura la ipv4 e ipv6 asignada al puerto.

```
D1(config)#interface Eth2/0
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 100 y se enciende la interfaz.

```
D1(config)#interface vlan 100
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 101 y se enciende la interfaz.

```
D1(config)#interface vlan 101
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 102 y se enciende la interfaz.

```
D1(config)#interface vlan 102
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
```

Se configura el pool DHCP de las VLAN 101 y VLAN 102, además se excluyen el rango de direcciones ip por cada VLAN.

```
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
```

Se realiza el apagado de las interfaces del switch D1 que no se usan:

```
D1(config)#interface range Eth1/2-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#interface range Eth2/1-3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#interface range Eth3/0-1
D1(config-if-range)#shutdown
D1(config-if-range)#exit
D1(config)#
D1(config)#interface Eth3/3
D1(config-if-range)#shutdown
D1(config-if-range)#exit
```

Configuración parámetros básicos switch D2

Se realiza configuración para cambiar nombre del switch D2, se habilita Ipv6 en el router, desactivo la traducción de nombres a dirección del dispositivo, configuro el mensaje del día "banner motd", configuración de la línea de consola y configuro un tiempo de espera ilimitado para la sesión.

```
Switch(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
```

Se realiza la creación de las VLAN 100, VLAN 101, VLAN 102, VLAN 999 con su nombre.

```
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
```

Se configura el puerto ethernet2/0 con el comando no switchport para que brinde la capacidad de capa 3 al puerto y se configura la ipv4 e ipv6 asignada al puerto.

```
D2(config)#interface Eth2/0
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 100 y se enciende la interfaz.

```
D2(config)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 101 y se enciende la interfaz.

```
D2(config)#interface vlan 101
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 102 y se enciende la interfaz.

```
D2(config)#interface vlan 102
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
```

Se configura el pool DHCP de las VLAN 101 y VLAN 102, además se excluyen el rango de direcciones ip por cada VLAN.

```
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
```

Se realiza el apagado de las interfaces del switch D2 que no se usan:

```
D2(config)#interface range Eth1/2-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface range Eth2/1-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#interface range Eth3/0-1
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#
D2(config)#interface Eth3/3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2(config)#
```

Configuración Parámetros Básicos Switch A1

Se realiza configuración para cambiar nombre del swicth D2, se habilita Ipv6 en el router, desactivo la traducción de nombres a dirección del dispositivo, configuro el mensaje del día "banner motd", configuración de la línea de consola y configuro un tiempo de espera ilimitado para la sesión.

```
A1(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
```

Se realiza la creación de las VLAN 100, VLAN 101, VLAN 102, VLAN 999 con su nombre.

```
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
```

Se configura la ip de administración ipv4 e ipv6 a la vlan 100 y se enciende la interfaz.

```
A1(config)#interface vlan 100
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
```

Se realiza el apagado de las interfaces del switch A1 que no se usan:

```
A1(config)#interface range Eth1/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#
A1(config)#interface range Eth2/0-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#
A1(config)#interface range Eth3/0-1
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#
```

Guardar configuración de los router y Swiches (R1,R2,R3,D1,D2 y A1)

Guardando la configuración del router R1

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Guardando la configuración del router R2

```
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

Guardando la configuración del router R3

```
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#
```

Guardando la configuración del switch D1

```
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
D1#
```

Guardando la configuración del switch D2

```
D2#copy running-config startup-config
Destination filename [startup-config]?
```

Building configuration...

[OK]

D2#

Guardando la configuración del switch A1

A1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A1#

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

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

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

2.1 Configuración enlaces troncales de switches

Habilite enlaces trunk 802.1Q entre :

Switch D1 and D2

D1(config)#interface range Eth0/0-3

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

D1(config-if-range)# switchport mode trunk

D1(config-if-range)# no shutdown

D1(config-if-range)#

Switch D2 a D1

D2(config)#interface range Eth0/0-3

D2(config-if-range)#switchport trunk encapsulation dot1q

D2(config-if-range)#switchport mode trunk

D2(config-if-range)#no sh

Switch D1 a A1

D1(config)#interface range Eth1/0-1

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

D1(config-if-range)# switchport mode trunk

D1(config-if-range)# no shutdown

D1(config-if-range)#

Switch A1 a D1

```
A1(config)#interface range Eth0/0-1
A1(config-if-range)# switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#no shutdown
A1(config-if-range)# exit
A1(config)#
```

Switch D2 a A1

```
D2(config)#interface range Eth1/0-1
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#no sh
```

Switch A1 a D2

```
A1(config)#interface range Eth0/2-3
A1(config-if-range)# switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#no shutdown
A1(config-if-range)# exit
A1(config)#
```

En todos los switches cambie la VLAN nativa en los enlaces troncales.
Use VLAN 999 como la VLAN nativa.

2.2 Configuración VLAN 999 como nativa en los enlaces troncales

Switch D1

```
D1(config)#interface range Eth0/0-3
D1(config-if-range)#switchport trunk native vlan 999
```

```
D1(config)#interface range Eth1/0-1
D1(config-if-range)#switchport trunk native vlan 999
```

Switch D2

```
D2(config)#interface range Eth0/0-3
D2(config-if-range)#switchport trunk native vlan 999
```

```
D2(config)#interface range Eth1/0-1
D2(config-if-range)#switchport trunk native vlan 999
```

Switch A1

```
A1(config)#interface range Eth0/0-3
A1(config-if-range)#switchport trunk native vlan 999
```

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

Switch D1

```
D1(config)#spanning-tree mode rapid-pvst  
D1(config)#
```

Switch D2

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

Switch A1

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

2.4: Configurar los puentes raíz (root bridges)

En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología, D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

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

Switch D1

```
D1(config)#spanning-tree vlan 100 root primary  
D1(config)#spanning-tree vlan 102 root primary  
D1(config)#spanning-tree vlan 101 root secondary
```

Switch D2

```
D2(config)#spanning-tree vlan 101 root primary  
D2(config)#spanning-tree vlan 100 root secondary  
D2(config)#spanning-tree vlan 102 root secondary
```

Figura 2. Verificación de spanning-tree switch D1

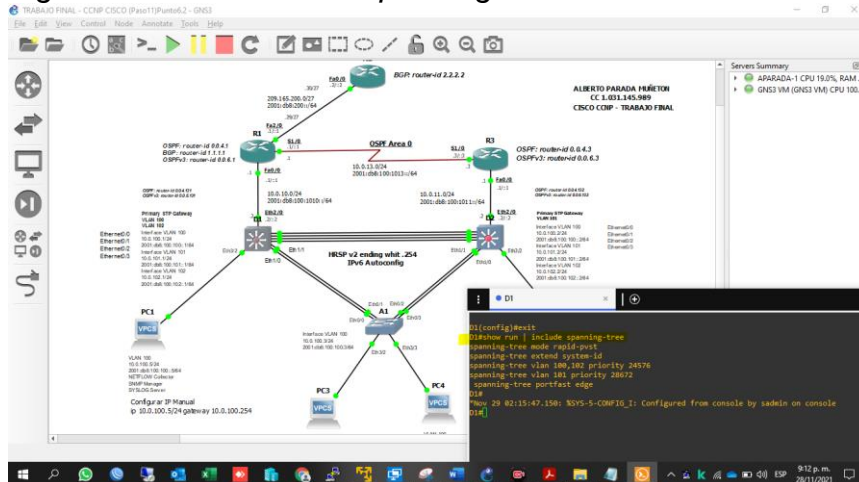
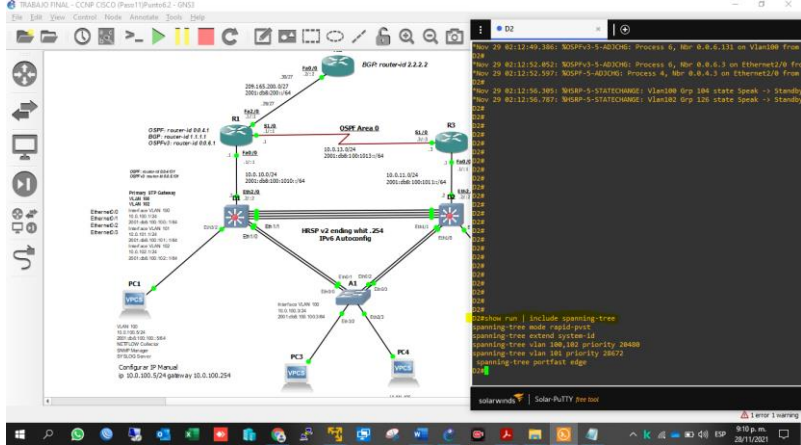


Figura 3. Verificación de spanning-tree switch D2



2.5 Creacion de EtherChannel LACP en switch D1,D2 y A1

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

Use los siguientes números de canales:

- D1 a D2 – Port channel 12
- D1 a A1 – Port channel 1
- D2 a A1 – Port channel 2

Switch D1 a D2

```

D1#configure terminal
D1(config)#interface range Eth0/0-3
D1(config-if-range)# shutdown
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface Port-channel12
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#switchport trunk allowed vlan all
D1(config-if)#
  
```

Switch D1 a A1

```
D1#configure terminal
D1(config)#interface range Eth1/0-1
D1(config-if-range)# shutdown
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface Port-channel1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#switchport trunk allowed vlan all
D1(config-if)#
```

Switch D2 a D1

```
D2#configure terminal
D2(config)#interface range Eth0/0-3
D2(config-if-range)# shutdown
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface Port-channel12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#switchport trunk allowed vlan all
D2(config-if)#
```

Switch D2 a A1

```
D2#configure terminal
D2(config)#interface range Eth1/0-1
D2(config-if-range)# shutdown
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface Port-channel2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#switchport trunk allowed vlan all
```

D2(config-if)#

Switch A1 a D1

A1#configure terminal

A1(config)#interface range Eth0/0-1

A1 (config-if-range)# shutdown

A1 (config-if-range)#channel-protocol lacp

A1 (config-if-range)#channel-group 1 mode active

A1 (config-if-range)#no shutdown

A1 (config-if-range)#exit

A1 (config)#interface Port-channel1

A1 (config-if)#switchport trunk encapsulation dot1q

A1 (config-if)#switchport mode trunk

A1 (config-if)#switchport trunk native vlan 999

A1 (config-if)#switchport trunk allowed vlan all

A1 (config-if)#

Switch A1 a D2

A1#configure terminal

A1(config)#interface range Eth0/2-3

A1 (config-if-range)# shutdown

A1 (config-if-range)#channel-protocol lacp

A1 (config-if-range)#channel-group 2 mode active

A1 (config-if-range)#no shutdown

A1 (config-if-range)#exit

A1 (config)#interface Port-channel2

A1 (config-if)#switchport trunk encapsulation dot1q

A1 (config-if)#switchport mode trunk

A1 (config-if)#switchport trunk native vlan 999

A1 (config-if)#switchport trunk allowed vlan all

A1 (config-if)#

Figura 4. verificación del LACP en D1

```
D1#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 1 neighbors
Partner's information:

Port    Flags    LACP port    Dev ID    Age    Admin Oper  Port    Port
      Priority Dev ID    Age    key    Key    Number State
Et1/0   SA      32768      aabb.cc80.0300 26s    0x0  0x1  0x1    0x3D
Et1/1   SA      32768      aabb.cc80.0300 2s     0x0  0x1  0x2    0x3D

Channel group 12 neighbors
Partner's information:

Port    Flags    LACP port    Dev ID    Age    Admin Oper  Port    Port
      Priority Dev ID    Age    key    Key    Number State
Et0/0   SA      32768      aabb.cc80.0200 17s    0x0  0xC  0x1    0x3D
Et0/1   SA      32768      aabb.cc80.0200 23s    0x0  0xC  0x2    0x3D
Et0/2   SA      32768      aabb.cc80.0200 23s    0x0  0xC  0x3    0x3D
Et0/3   SA      32768      aabb.cc80.0200 26s    0x0  0xC  0x4    0x3D
D1#
D1#
```

Figura 5. verificación del LACP en D2

```
D2#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 2 neighbors
Partner's information:

Port    Flags    LACP port    Dev ID    Age    Admin Oper  Port    Port
      Priority Dev ID    Age    key    Key    Number State
Et1/0   SA      32768      aabb.cc80.0300 23s    0x0  0x2  0x4    0x3D
Et1/1   SA      32768      aabb.cc80.0300 5s     0x0  0x2  0x3    0x3D

Channel group 12 neighbors
Partner's information:

Port    Flags    LACP port    Dev ID    Age    Admin Oper  Port    Port
      Priority Dev ID    Age    key    Key    Number State
Et0/0   SA      32768      aabb.cc80.0100 8s     0x0  0xC  0x1    0x3D
Et0/1   SA      32768      aabb.cc80.0100 22s    0x0  0xC  0x2    0x3D
Et0/2   SA      32768      aabb.cc80.0100 4s     0x0  0xC  0x3    0x3D
Et0/3   SA      32768      aabb.cc80.0100 8s     0x0  0xC  0x4    0x3D
D2#
D2#
```

Figura 6. verificación del LACP en A1

```
A1#show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 1 neighbors
Partner's information:

Port    Flags    LACP port    Dev ID    Age    Admin Oper  Port    Port
      Priority Dev ID    Age    key    Key    Number State
Et0/0   SA      32768      aabb.cc80.0100 12s    0x0  0x1  0x101  0x3D
Et0/1   SA      32768      aabb.cc80.0100 20s    0x0  0x1  0x102  0x3D

Channel group 2 neighbors
Partner's information:

Port    Flags    LACP port    Dev ID    Age    Admin Oper  Port    Port
      Priority Dev ID    Age    key    Key    Number State
Et0/2   SA      32768      aabb.cc80.0200 9s     0x0  0x2  0x102  0x3D
Et0/3   SA      32768      aabb.cc80.0200 12s    0x0  0x2  0x101  0x3D
A1#
A1#
```

2.6 Configuración de los puertos de acceso en los switches para los PC.

En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

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

Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).

Switch D1

```
D1(config)#interface Eth3/2
D1(config-if)#switchport mode Access
D1(config-if)#switchport access vlan 100
D1(config-if)#spanning-tree portfast
D1(config-if)# no shutdown
D1(config-if)#exit
```

Switch D2

```
D2(config)#interface Eth3/2
D2(config-if)#switchport mode Access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)# no shutdown
D2(config-if)#exit
```

Switch A1

```
A1(config)#interface Eth3/2
A1(config-if)#switchport mode Access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config-if)# no shutdown
A1(config-if)#exit
```

```
A1(config)#interface Eth3/3
A1(config-if)#switchport mode Access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)# no shutdown
A1(config-if)#exit
```

2.7 Verifique los servicios DHCP IPv4 para los PC.

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

Equipo **PC2 y PC3** va a tomar direccionamiento IP por DHCP, para que el equipo tome direccionamiento ip se ejecuta el comando **ip dhcp**.

- El **PC2** toma la ip por DHCP : **10.0.102.210/24**

Figura 7. PC2 toma ip por dhcp

The screenshot shows a network simulator interface with a terminal window on the left and a network topology diagram on the right. The terminal window displays the following output:

```
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build times: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

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

Press '?' to get help.

Executing the startup file

PC2> ip dhcp
DORA IP 10.0.102.210/24 Gw 10.0.102.254

PC2> show ip

NAME       : PC2[1]
IP/MASK    : 10.0.102.210/24
GATEWAY    : 10.0.102.254
VCS       :
DHCP SERVER : 10.0.102.2
DHCP LEASE  : 86380, 86400/43200/75600
MAC        : 00:50:79:66:68:01
LPORT     : 10004
RHOST-PORT : 127.0.0.1:10005
MTU       : 1500
```

The network topology diagram shows a central switch (Primary STP Gateway) connected to several interfaces. PC2 is connected to the switch via a VPCS client. The switch has interfaces for VLAN 100, VLAN 101, and VLAN 102. The terminal window shows that PC2 has successfully received an IP address of 10.0.102.210/24 via DHCP.

El **PC3** toma la ip por dhcp : **10.0.101.110/24**

Figura 8. PC3 toma ip por dhcp

The screenshot shows a network simulator interface with a terminal window on the right and a network topology diagram on the left. The terminal window displays the following output:

```
Dedicated to Daling.
Build times: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

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

Press '?' to get help.

Executing the startup file

PC3> show ip

NAME       : PC3[1]
IP/MASK    : 0.0.0.0/0
GATEWAY    : 0.0.0.0
VCS       :
DHCP SERVER : 10.0.101.1
DHCP LEASE  : 86388, 86400/43200/75600
MAC        : 00:50:79:66:68:00
LPORT     : 10002
RHOST-PORT : 127.0.0.1:10003
MTU       : 1500

PC3> ip dhcp
DORA IP 10.0.101.110/24 Gw 10.0.101.254

PC3> show ip

NAME       : PC3[1]
IP/MASK    : 10.0.101.110/24
GATEWAY    : 10.0.101.254
VCS       :
DHCP SERVER : 10.0.101.1
DHCP LEASE  : 86388, 86400/43200/75600
MAC        : 00:50:79:66:68:00
LPORT     : 10002
RHOST-PORT : 127.0.0.1:10003
MTU       : 1500
```

The network topology diagram shows a central switch (Primary STP Gateway) connected to several interfaces. PC3 is connected to the switch via a VPCS client. The switch has interfaces for VLAN 100, VLAN 101, and VLAN 102. The terminal window shows that PC3 has successfully received an IP address of 10.0.101.110/24 via DHCP.

2.8 Verificación de la conectividad de la red LAN local.

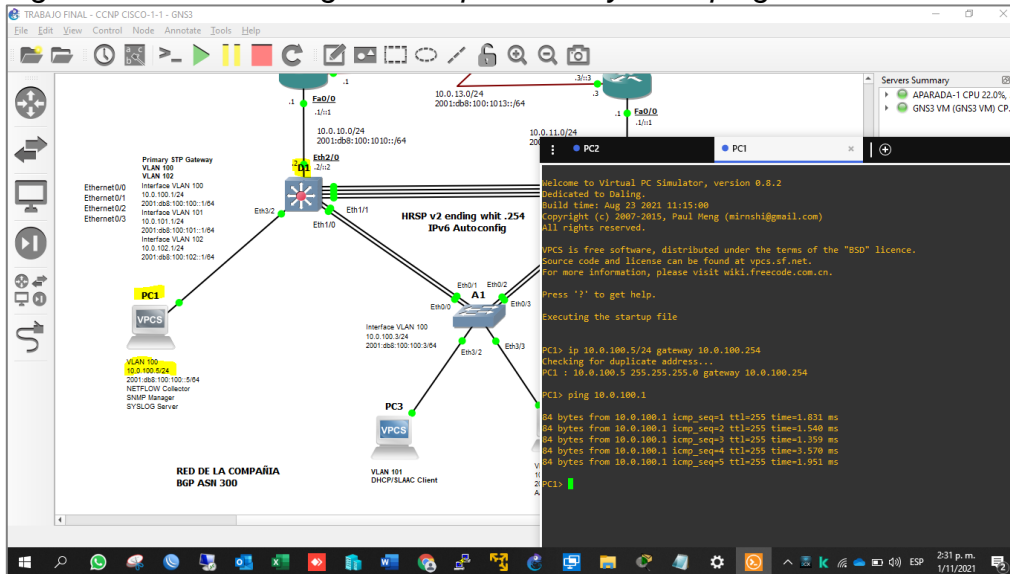
PC1 debería hacer ping con éxito a:

- D1: 10.0.100.1

Configurar la ip Estática al PC1 en GNS3.

Comando: ip 10.0.100.5/24 gateway 10.0.100.254

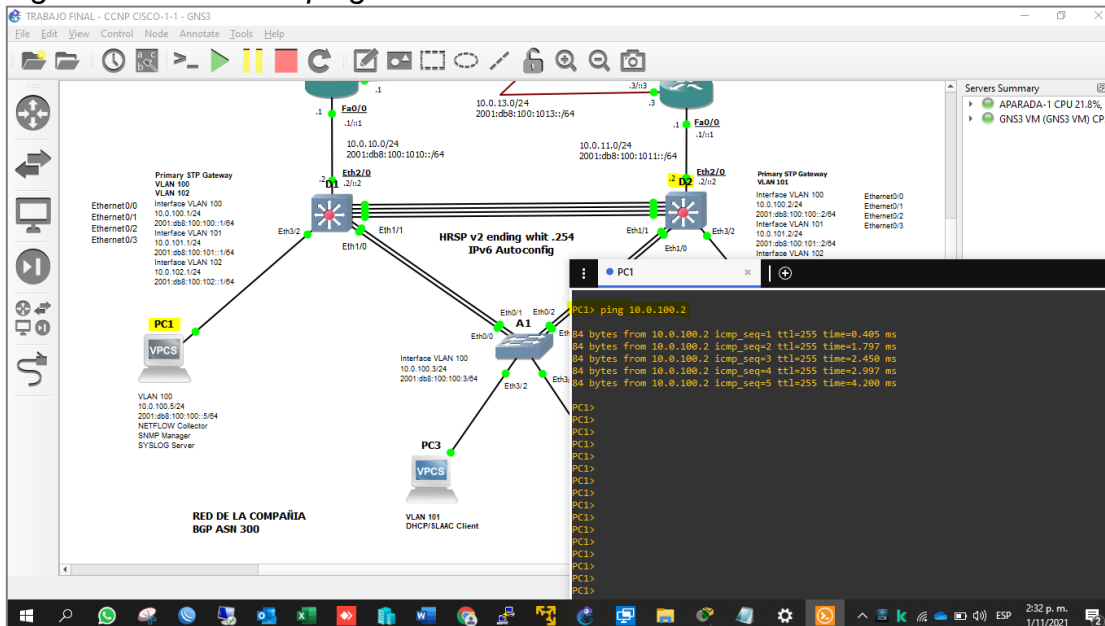
Figura 9. PC1 se configura con ip estática y hace ping a switch D1



PC1 debería hacer ping con éxito a:

- D2: 10.0.100.2

Figura 10. PC1 hace ping a switch D2



PC1 debería hacer ping con éxito a:

- PC4: 10.0.100.6

Configurar la ip Estática al PC4 en GNS3.

Comando: ip 10.0.100.6/24 gateway 10.0.100.254

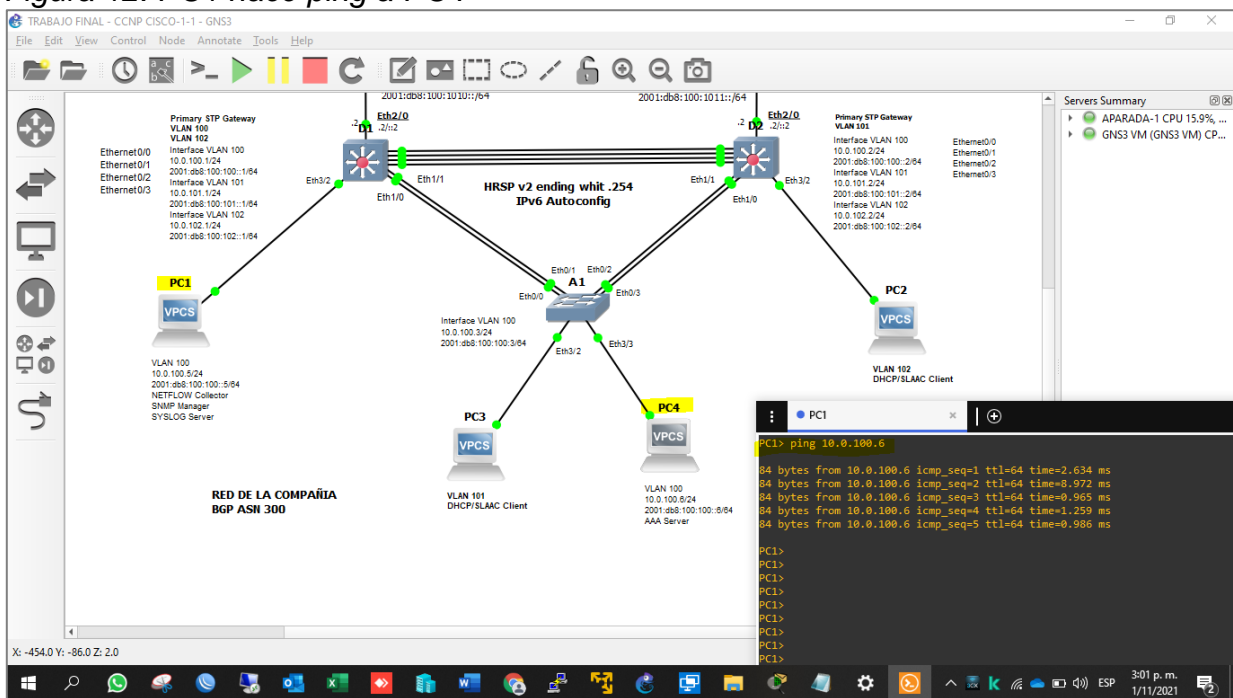
Comando: save (Guarda la configuración)

Figura 11. Configuración IP estática a PC4

```
PC4> ip 10.0.100.6/24 gateway 10.0.100.254
Checking for duplicate address...
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254

PC4> █
```

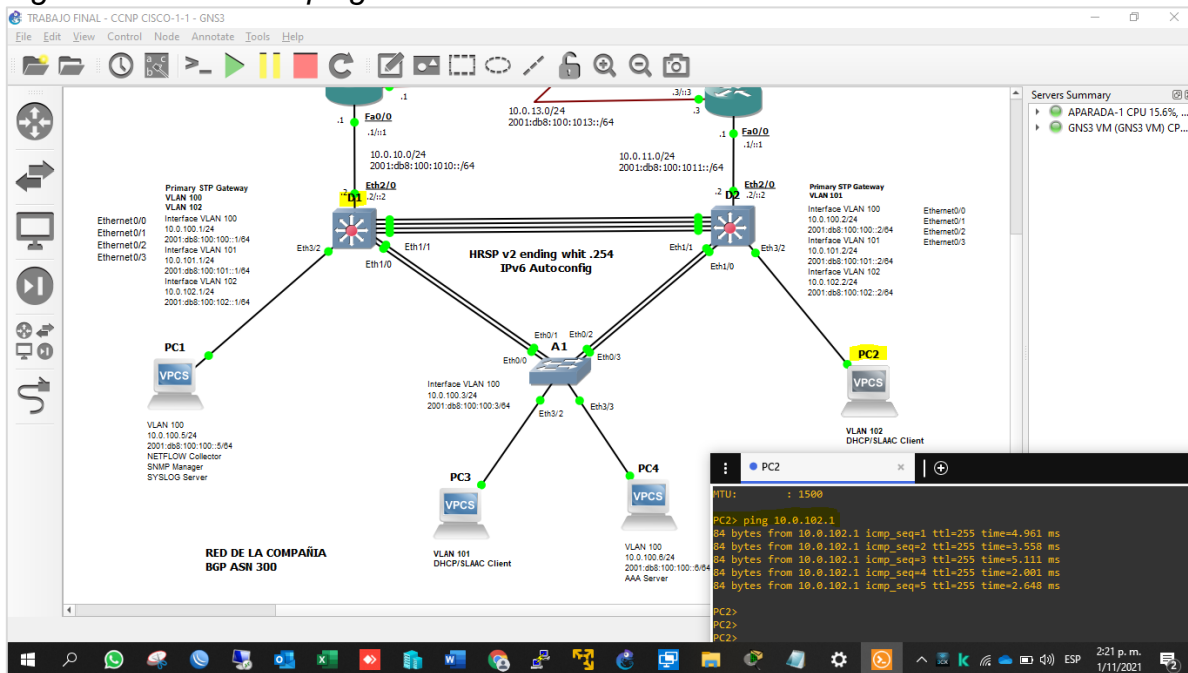
Figura 12. PC1 hace ping a PC4



PC2 debería hacer ping con éxito a:

- D1: 10.0.102.1

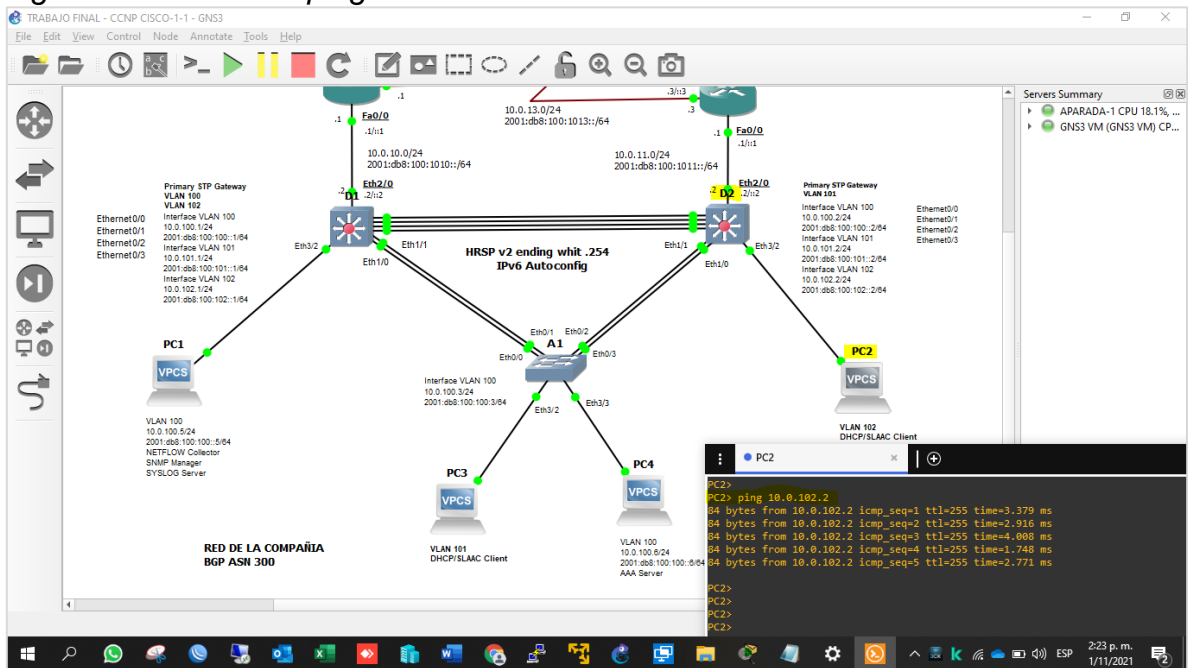
Figura 13. PC2 hace ping a switch D1



PC2 debería hacer ping con éxito a:

- D2: 10.0.102.2

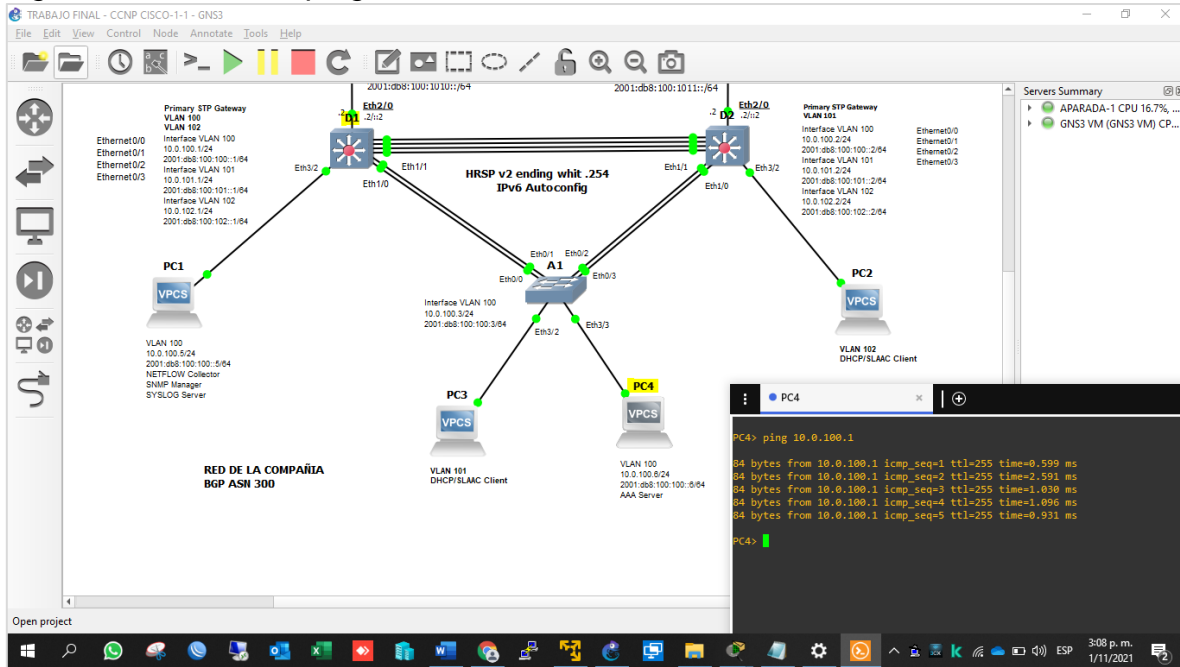
Figura 14. PC2 hace ping a switch D2



PC4 debería hacer ping con éxito a:

- D1: 10.0.100.1

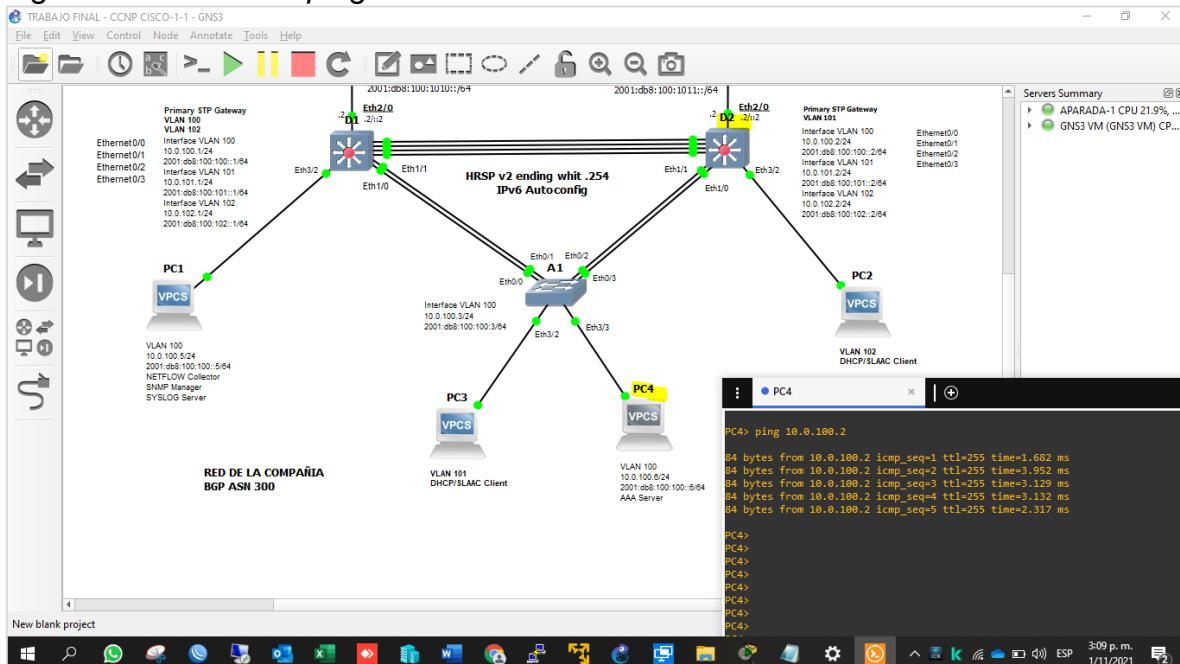
Figura 17. PC4 hace ping a switch D1



PC4 debería hacer ping con éxito a:

- D2: 10.0.100.2

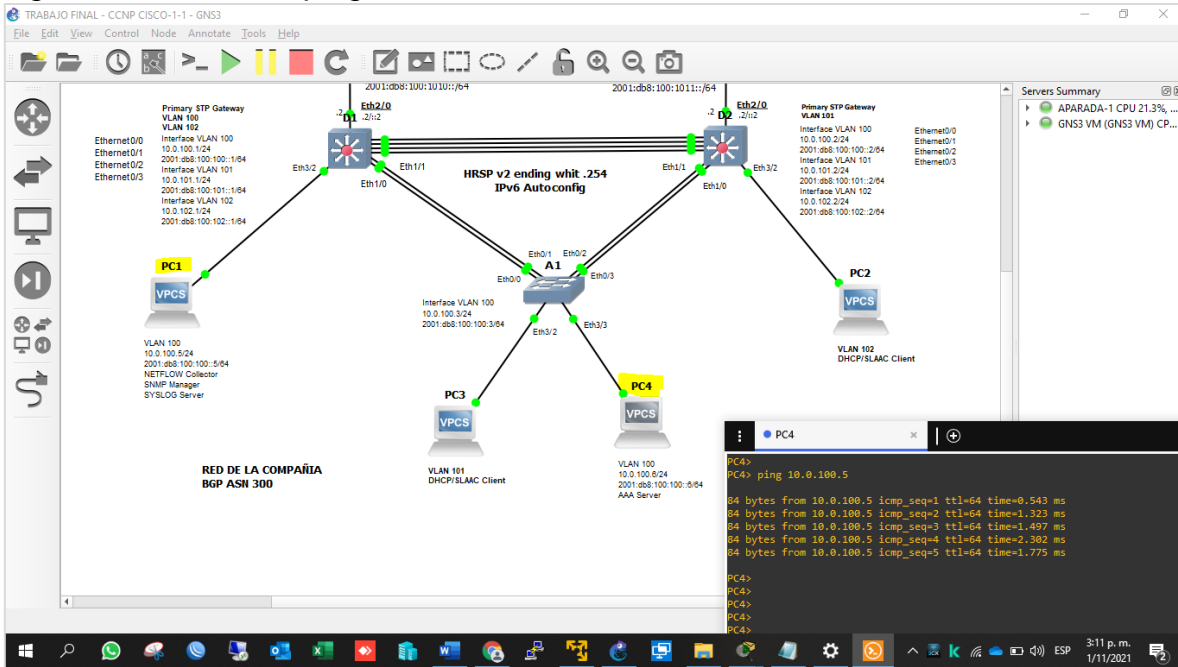
Figura 18. PC4 hace ping a switch D2



PC4 debería hacer ping con éxito a:

- PC1: 10.0.100.5

Figura 19. PC4 hace ping a switch PC1



Parte 3: Configurar los protocolos de enrutamiento

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

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

3.1 Configuración OSPFv2 en área 0

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

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

- R1: 0.0.4.1
- R3: 0.0.4.3
- D1: 0.0.4.131
- D2: 0.0.4.132

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

- En R1, no publique la red R1 – R2.

Router R1

Se anuncian las redes directamente conectadas, menos la red que esta entre **R1** y **R2**.

```
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)#ip route 0.0.0.0 0.0.0.0 Fa2/0
R1(config)#router ospf 4
R1(config-router)#default-information originate always
```

Router R3

Se anuncian todas las redes directamente conectadas, para ver las redes directamente conectadas se ejecuta el comando **do show ip route connected**.

```
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
```

Switch D1

Se anuncian todas las redes directamente conectadas y redes de las Vlan.

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
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
```

Switch D2

Se anuncian todas las redes directamente conectadas y redes de las Vlan.

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
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
```

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

```
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#no bgp default ipv4-unicast
R1(config-router)#neighbor 209.165.200.30 remote-as 500
R1(config-router)#network 209.165.200.0 mask 255.255.255.224
```

```
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)#no bgp default ipv4-unicast
R2(config-router)#neighbor 209.165.200.29 remote-as 300
R2(config-router)#network 209.165.200.0 mask 255.255.255.224
```

Deshabilite las publicaciones OSPFv2 en:

D1: todas las interfaces excepto Eth2/0
D2: todas las interfaces excepto Eth2/0

Switch D1: todas las interfaces excepto Eth2/0

```
D1(config)#router ospf 4
D1(config-router)#passive-interface vlan 100
D1(config-router)#passive-interface vlan 101
D1(config-router)#passive-interface vlan 102
D1(config-router)#passive-interface Eth0/0
D1(config-router)#passive-interface Eth0/1
D1(config-router)#passive-interface Eth0/2
D1(config-router)#passive-interface Eth0/3
D1(config-router)#passive-interface Eth1/0
D1(config-router)#passive-interface Eth1/1
```

Switch D2: todas las interfaces excepto Eth2/0

```
D2(config)#router ospf 4
D2(config-router)#passive-interface vlan 100
D2(config-router)#passive-interface vlan 101
D2(config-router)#passive-interface vlan 102
D2(config-router)#passive-interface Eth0/0
D2(config-router)#passive-interface Eth0/1
D2(config-router)#passive-interface Eth0/2
D2(config-router)#passive-interface Eth0/3
D2(config-router)#passive-interface Eth1/0
D2(config-router)#passive-interface Eth1/1
D2(config-router)#
```

3.2 Configuración OSPFv3

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

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

Router R1

Se anuncian las redes directamente conectadas, **menos la red que esta entre R1 y R2**

```
R1(config)#
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#do show ip route connected
    209.165.200.0/24 is subnetted, 1 subnets
C    209.165.200.0 is directly connected, FastEthernet2/0
    10.0.0.0/24 is subnetted, 6 subnets
C    10.0.10.0 is directly connected, FastEthernet0/0
C    10.0.13.0 is directly connected, Serial1/0
R1(config-rtr)#
R1(config-rtr)#interface Fa0/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#interface s1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#exit
R1(config)#ipv6 route ::/0 fa0/0
R1(config)#ipv6 router ospf 6
R1(config-rtr)#default-information originate
```

Router R3

Se anuncian todas las redes directamente conectadas

```
R3#configure terminal
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)#do show ip route connected
    10.0.0.0/24 is subnetted, 6 subnets
C    10.0.11.0 is directly connected, FastEthernet0/0
C    10.0.13.0 is directly connected, Serial1/0
```

```
R3(config-rtr)#interface Fa0/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#interface s1/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#
```

Switch D1

Se anuncian todas las redes directamente conectadas y redes Vlans

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#do show ip route connected
C 10.0.10.0/24 is directly connected, Ethernet2/0
C 10.0.100.0/24 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
```

```
D1(config-rtr)#interface Eth2/0
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface Vlan100
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface Vlan101
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#interface Vlan102
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#
```

Switch D2

Se anuncian todas las redes directamente conectadas y redes Vlans

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#router-id 0.0.6.132
D2(config-rtr)#do show ip route connected
C 10.0.11.0/24 is directly connected, Ethernet2/0
C 10.0.100.0/24 is directly connected, Vlan100
C 10.0.101.0/24 is directly connected, Vlan101
C 10.0.102.0/24 is directly connected, Vlan102
D2(config-rtr)#interface Eth2/0
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface Vlan100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface Vlan101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface Vlan102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#
```

Deshabilite las publicaciones OSPFv3 en:

- D1: todas las interfaces excepto G1/0/11
- D2: todas las interfaces excepto G1/0/11

D1: todas las interfaces excepto Eth2/0

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#passive-interface Eth0/0
D1(config-rtr)#passive-interface Eth0/1
D1(config-rtr)#passive-interface Eth0/2
D1(config-rtr)#passive-interface Eth0/3
D1(config-rtr)#passive-interface Eth1/0
D1(config-rtr)#passive-interface Eth1/1
D1(config-rtr)#
```

D2: todas las interfaces excepto Eth2/0

```
D2(config)#ipv6 router ospf 6
D2(config-rtr)#passive-interface Eth0/0
D2(config-rtr)#passive-interface Eth0/1
D2(config-rtr)#passive-interface Eth0/2
D2(config-rtr)#passive-interface Eth0/3
D2(config-rtr)#passive-interface Eth1/0
D2(config-rtr)#passive-interface Eth1/1
D2(config-rtr)#
```

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

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:
Una ruta estática predeterminada IPv4.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback0
R2(config)#
```

Una ruta estática predeterminada IPv6.

```
R2(config)#ipv6 route ::/0 loopback0
R2(config)#
```

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

```
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
R2(config-router)# no bgp default ipv4-unicast
```

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).

```
R2(config)#router bgp 500
R2(config-router)# no bgp default ipv4-unicast
R2(config-router)#address-family ipv4 unicast
R2(config-router-af)#neighbor 209.165.200.29 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0 mask 0.0.0.0
```

En IPv6 address family, anuncie:

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

```
R2(config)#router bgp 500
R2(config-router)#address-family ipv6 unicast
R2(config-router-af)#network 2001:db8:2222::1/128
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network ::/0
R2(config-router-af)#exit
```

3.4 Configuración MP-BGP en la red ISP R1

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

```
R1(config)#ip route 10.0.0.0 255.0.0.0 null 0
R1(config)#ipv6 route 2001:db8:100::/48 null 0
```

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

```
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#
```

**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.
- Deshabilite la relación de vecino IPv6.

```
R1(config)#router bgp 300
R1(config-router)#address-family ipv4 unicast
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-af)#no neighbor 2001:db8:200::2 activate
```

Habilite la relación de vecino IPv4.

```
R1(config-router-af)#neighbor 209.165.200.30 activate
```

Anuncie la red 10.0.0.0/8.

```
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0
```

En IPv6 address family:

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

Deshabilite la relación de vecino IPv4.

```
R1(config)#router bgp 300
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)#no neighbor 209.165.200.30 activate
```

Habilite la relación de vecino IPv6.

```
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#network 2001:db8:100::/48
```

Anuncie la red 2001:db8:100::/48.

```
R1(config-router-af)#network 2001:db8:100::/48
```

Figura 20. Verificación de la tabla de enrutamiento IPv4 router R1

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, FastEthernet2/0
   2.0.0.0/32 is subnetted, 1 subnets
   B 2.2.2.2 [20/0] via 209.165.200.30, 02:12:03
   B 10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
   S 10.0.0.0/8 is directly connected, Null0
   C 10.0.10.0/24 is directly connected, FastEthernet0/0
   L 10.0.10.1/32 is directly connected, FastEthernet0/0
   O 10.0.11.0/24 [110/65] via 10.0.13.3, 00:01:59, Serial1/0
   C 10.0.13.0/24 is directly connected, Serial1/0
   L 10.0.13.1/32 is directly connected, Serial1/0
   O 10.0.100.0/24 [110/2] via 10.0.10.2, 00:01:59, FastEthernet0/0
   O 10.0.101.0/24 [110/2] via 10.0.10.2, 00:01:59, FastEthernet0/0
   O 10.0.102.0/24 [110/2] via 10.0.10.2, 00:01:59, FastEthernet0/0
   C 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
   C 209.165.200.0/27 is directly connected, FastEthernet2/0
   L 209.165.200.29/32 is directly connected, FastEthernet2/0
R1#
R1#
```

Figura 21. Verificación de la tabla de enrutamiento IPv4 router R2

```
R2#show ip route
Nov 29 04:26:22.227: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Loopback0
   2.0.0.0/32 is subnetted, 1 subnets
   C 2.2.2.2 is directly connected, Loopback0
   B 10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
   B 10.0.0.0/8 [20/0] via 209.165.200.29, 00:13:31
   B 10.0.10.0/24 [20/0] via 209.165.200.29, 02:17:21
   B 10.0.11.0/24 [20/65] via 209.165.200.29, 02:17:21
   B 10.0.13.0/24 [20/0] via 209.165.200.29, 02:17:21
   B 10.0.100.0/24 [20/2] via 209.165.200.29, 00:04:26
   B 10.0.101.0/24 [20/2] via 209.165.200.29, 00:04:26
   B 10.0.102.0/24 [20/2] via 209.165.200.29, 00:04:26
   C 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
   C 209.165.200.0/27 is directly connected, FastEthernet0/0
   L 209.165.200.30/32 is directly connected, FastEthernet0/0
R2#
R2#
```

Figura 22. Verificación de la tabla de enrutamiento IPv4 router R3

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 02:16:43, Serial1/0
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O     10.0.10.0/24 [110/65] via 10.0.13.1, 00:05:15, Serial1/0
C     10.0.11.0/24 is directly connected, FastEthernet0/0
C     10.0.11.1/32 is directly connected, FastEthernet0/0
C     10.0.13.0/24 is directly connected, Serial1/0
L     10.0.13.3/32 is directly connected, Serial1/0
O     10.0.100.0/24 [110/2] via 10.0.11.2, 00:05:25, FastEthernet0/0
O     10.0.101.0/24 [110/2] via 10.0.11.2, 00:05:25, FastEthernet0/0
O     10.0.102.0/24 [110/2] via 10.0.11.2, 00:05:25, FastEthernet0/0
R3#
R3#
R3#
```

Figura 23. Verificación de la tabla de enrutamiento IPv4 router D1

```
D1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C     10.0.10.0/24 is directly connected, Ethernet2/0
L     10.0.10.2/32 is directly connected, Ethernet2/0
C     10.0.100.0/24 is directly connected, Vlan100
L     10.0.100.1/32 is directly connected, Vlan100
C     10.0.101.0/24 is directly connected, Vlan101
L     10.0.101.1/32 is directly connected, Vlan101
C     10.0.102.0/24 is directly connected, Vlan102
L     10.0.102.1/32 is directly connected, Vlan102
D1#
D1#
*Nov 29 04:38:43.908: %HSRP-5-STATECHANGE: Vlan100 Grp 106 state Speak -> Standby
*Nov 29 04:38:44.032: %HSRP-5-STATECHANGE: Vlan101 Grp 116 state Speak -> Standby
D1#
```

Figura 24. Verificación de la tabla de enrutamiento IPv4 router D2

```
D2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.0.11.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.0.11.1, 00:00:40, Ethernet2/0
      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O      10.0.10.0/24 [110/75] via 10.0.11.1, 00:00:40, Ethernet2/0
C      10.0.11.0/24 is directly connected, Ethernet2/0
L      10.0.11.2/32 is directly connected, Ethernet2/0
O      10.0.13.0/24 [110/74] via 10.0.11.1, 00:00:40, Ethernet2/0
C      10.0.100.0/24 is directly connected, Vlan100
L      10.0.100.2/32 is directly connected, Vlan100
C      10.0.101.0/24 is directly connected, Vlan101
L      10.0.101.2/32 is directly connected, Vlan101
C      10.0.102.0/24 is directly connected, Vlan102
L      10.0.102.2/32 is directly connected, Vlan102
D2#
D2#
```

Figura 25. Verificación de la tabla de enrutamiento IPv4 router A1

```
A1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.0.100.0/24 is directly connected, Vlan100
L      10.0.100.3/32 is directly connected, Vlan100
A1#
A1#
A1#
A1#
```

Figura 26. Ping desde switch D1 y switch D2 a Loopback 0

```
D1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/32/39 ms
D1#

D2#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 125/150/178 ms
D2#
```

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 fa0/0.

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.

Switch D1

Crea el SLA

```
D1(config)#ip sla 4
```

Define el destino y la fuente

```
D1(config-ip-sla)#icmp-echo 10.0.10.1 source-ip 10.0.10.2
```

Prueba la disponibilidad cada 5 segundos

```
D1(config-ip-sla-echo)#frequency 5
```

```
D1(config-ip-sla-echo)#exit
```

Programación del SLA para una implementación inmediata sin tiempo de finalización

```
D1(config)#ip sla schedule 4 start-time now life forever
```

```
D1(config)#track 4 ip sla 4 reachability
```

Configuración de notificación de los estados Up a Down después de 15 segundos

```
D1(config-track)#delay up 10 down 15
```

```
D1(config-track)#exit
```

```
D1(config)#ip sla 6
```

```
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-interface eth2/0
```

```
D1(config-ip-sla-echo)#frequency 5
```

```
D1(config-ip-sla-echo)#exit
```

```
D1(config)#ip sla schedule 6 start-time now life forever
```

```
D1(config)#track 6 ip sla 6 reachability
```

```
D1(config-track)#delay up 10 down 15
```

```
D1(config-track)#exit
```

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 fa0/0.

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.
Programar 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.

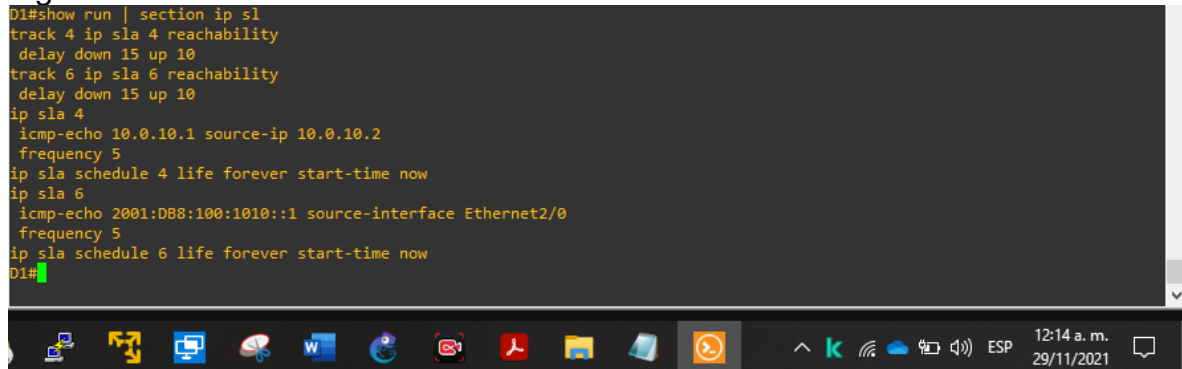
Use el número de rastreo 4 para la IP SLA 4.

Use el número de rastreo 6 para la SLA 6.

Switch D2

```
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1 source-interface eth2/0
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 start-time now life forever
D2(config)#track 4 ip sla 4 reachability
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-interface eth2/0
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 6 start-time now life forever
D2(config)#track 6 ip sla 6 reachability
D2(config-track)# delay up 10 down 15
D2(config-track)#exit
```

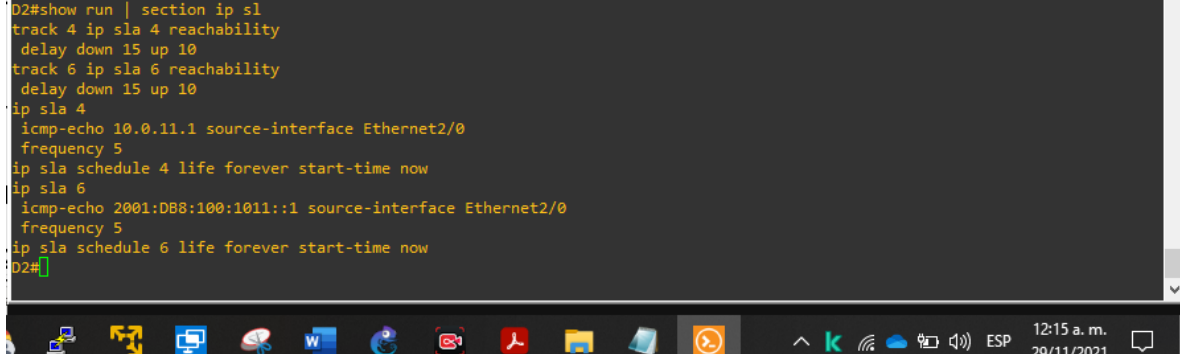
Figura 27. Verificación de las SLAs en switch D1



```
D1#show run | section ip sla
track 4 ip sla 4 reachability
  delay down 15 up 10
track 6 ip sla 6 reachability
  delay down 15 up 10
ip sla 4
  icmp-echo 10.0.10.1 source-ip 10.0.10.2
  frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
  icmp-echo 2001:DB8:100:1010::1 source-interface Ethernet2/0
  frequency 5
ip sla schedule 6 life forever start-time now
D1#
```

Figura 28. Verificación de las SLAs en switch D2

```
D2#show run | section ip sl
track 4 ip sla 4 reachability
delay down 15 up 10
track 6 ip sla 6 reachability
delay down 15 up 10
ip sla 4
icmp-echo 10.0.11.1 source-interface Ethernet2/0
frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
icmp-echo 2001:DB8:100:1011::1 source-interface Ethernet2/0
frequency 5
ip sla schedule 6 life forever start-time now
D2#
```



4.3 En D1 configure HSRPv2.

En D1 configure HSRPv2, D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150, Configure HSRP versión 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

En D1 Asigne la dirección IP virtual 10.0.100.254.

```
D1(config)#interface vlan 100
D1(config)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#standby 104 ip 10.0.100.254
```

Establezca la prioridad del grupo en 150.

```
D1(config-if)#standby 104 priority 150
```

Habilite la preferencia (preemption).

```
D1(config-if)# standby 104 preempt
```

Rastree el objeto 4 y decremente en 60.

```
D1(config-if)# standby 104 track 4 decrement 60
```

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254

```
D1(config)#interface vlan 101
D1(config)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#standby 114 ip 10.0.101.254
```

Establezca la prioridad del grupo en 150.

```
D1(config-if)#standby 114 priority 150
```

Habilite la preferencia (preemption).

```
D1(config-if)# standby 114 preempt
```

Rastree el objeto 4 para disminuir en 60.

```
D1(config-if)# standby 114 track 4 decrement 60
```

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

```
D1(config)#interface vlan 102
```

```
D1(config)#ip address 10.0.102.1 255.255.255.0
```

```
D1(config-if)#standby 124 ip 10.0.102.254
```

Habilite la preferencia (preemption).

```
D1(config-if)# standby 124 preempt
```

Rastree el objeto 4 para disminuir en 60.

```
D1(config-if)# standby 124 track 4 decrement 60
```

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

```
D1(config)#interface vlan 100
```

```
D1(config-if)# standby version 2
```

```
D1(config-if)# standby 106 ipv6 autoconfig
```

Habilite la preferencia (preemption).

```
D1(config-if)# standby 106 preempt
```

Rastree el objeto 6 para disminuir en 60.

```
D1(config-if)# standby 106 track 6 decrement 60
```

Configure IPv6 HSRP grupo 116 para la VLAN 101:

Asigne la dirección IP virtual usando ipv6 autoconfig.

```
D1(config)#interface vlan 101
```

```
D1(config-if)# standby version 2
```

```
D1(config-if)# standby 116 ipv6 autoconfig
```

Establezca la prioridad del grupo en 150.

```
D1(config-if)#standby 116 priority 150
```

Habilite la preferencia (preemption).
D1(config-if)# standby 116 preempt

Rastree el objeto 6 para disminuir en 60.
D1(config-if)# standby 116 track 6 decrement 60

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6 autoconfig.
D1(config)#interface vlan 102
D1(config-if)# standby version 2
D1(config-if)# standby 126 ipv6 autoconfig

Establezca la prioridad del grupo en 150.
D1(config-if)#standby 126 priority 150

Habilite la preferencia (preemption).
D1(config-if)# standby 126 preempt

Rastree el objeto 6 para disminuir en 60.
D1(config-if)# standby 126 track 6 decrement 60

4.4 En D2 configure HSRPv2.

D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.
Configure HSRP versión 2.

Configure IPv4 HSRP grupo 104 para la VLAN 100:

Asigne la dirección IP virtual 10.0.100.254.
D2(config)#interface vlan 100
D2(config)#ip address 10.0.100.2 255.255.255.0 (IP ya configurada en Pasos Anteriores)
D2(config-if)#standby 104 ip 10.0.100.254

Habilite la preferencia (preemption).
D2(config-if)# standby 104 preempt

Rastree el objeto 4 y decremente en 60.
D2(config-if)# standby 104 track 4 decrement 60

Configure IPv4 HSRP grupo 114 para la VLAN 101:

Asigne la dirección IP virtual 10.0.101.254.

```
D2(config)#interface vlan 101
D2(config)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#standby 114 ip 10.0.101.254
```

Establezca la prioridad del grupo en 150.

```
D2(config-if)#standby 114 priority 150
```

Habilite la preferencia (preemption).

```
D2(config-if)# standby 114 preempt
```

Rastree el objeto 4 para disminuir en 60.

```
D2(config-if)# standby 114 track 4 decrement 60
```

Configure IPv4 HSRP grupo 124 para la VLAN 102:

Asigne la dirección IP virtual 10.0.102.254.

```
D2(config)#interface vlan 102
D2(config)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#standby 124 ip 10.0.102.254
```

Habilite la preferencia (preemption).

```
D2(config-if)# standby 124 preempt
```

Rastree el objeto 4 para disminuir en 60.

```
D2(config-if)# standby 124 track 4 decrement 60
```

Configure IPv6 HSRP grupo 106 para la VLAN 100:

Asigne la dirección IP virtual usando ipv6 autoconfig.

```
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 106 ipv6 autoconfig
```

Habilite la preferencia (preemption).

```
D2(config-if)# standby 106 preempt
```

Rastree el objeto 6 para disminuir en 60.

```
D2(config-if)# standby 106 track 6 decrement 60
```

Configure IPv6 HSRP grupo 116 para la VLAN 101:

Asigne la dirección IP virtual usando ipv6 autoconfig.

```
D2(config)#interface vlan 101
D2(config-if)# standby version 2
D2(config-if)# standby 116 ipv6 autoconfig
```

Establezca la prioridad del grupo en 150.

```
D2(config-if)#standby 116 priority 150
```

Habilite la preferencia (preemption).

```
D2(config-if)# standby 116 preempt
```

Rastree el objeto 6 para disminuir en 60.

```
D2(config-if)# standby 116 track 6 decrement 60
```

Configure IPv6 HSRP grupo 126 para la VLAN 102:

Asigne la dirección IP virtual usando ipv6 autoconfig.

```
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 126 ipv6 autoconfig
```

Habilite la preferencia (preemption).

```
D2(config-if)# standby 126 preempt
```

Rastree el objeto 6 para disminuir en 60.

```
D2(config-if)# standby 126 track 6 decrement 60
```

Figura 29. Verificación del standby en switch D1

```
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  100 P Standby FE80::D2:2      local            FE80::5:73FF:FEA0:6A
Vl101      114  150 P Standby 10.0.101.2     local            10.0.101.254
Vl101      116  150 P Standby FE80::D2:3      local            FE80::5:73FF:FEA0:74
Vl102      124  100 P Standby 10.0.102.2     local            10.0.102.254
Vl102      126  150 P Active  local           FE80::D2:4       FE80::5:73FF:FEA0:7E
D1#
```

Figura 30. Verificación del standby en switch D2

```
D2#Show standby brief
*Nov 2 04:44:44.138: %SYS-5-CONFIG_I: Configured from console by console
D2#Show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Vl100      104 100 P Standby 10.0.100.1      local            10.0.100.254
Vl100      106 100 P Active  local           FE80::D1:2      FE80::5:73FF:FEA0:6A
Vl101      114 150 P Active  local           10.0.101.1      10.0.101.254
Vl101      116 150 P Active  local           FE80::D1:3      FE80::5:73FF:FEA0:74
Vl102      124 100 P Active  local           10.0.102.1      10.0.102.254
Vl102      126 100 P Standby FE80::D1:4      local            FE80::5:73FF:FEA0:7E
D2#
```

Parte 5: Seguridad

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

Las tareas de configuración son las siguientes:

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

Contraseña: **cisco12345cisco**

Router R1

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

Router R2

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

Router R3

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

Switch D1

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

Switch D2

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

Switch A1

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

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

Detalles de la cuenta encriptada SCRYPT:

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

Router R1

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

Router R2

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

Router R3

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

Switch D1

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

Switch D2

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

Switch A1

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

Figura 31. Verificación de usuario y contraseña creado en switch D1

```
D1#show run | include secret
enable secret 9 $9$gqJ.zMUpeicgHi$CWnDBAgoJ1ms9L.iK74nK10NmNSC6hctcZpSRfWI24U
username sadmin privilege 15 secret 9 $9$F1m7ZkuUwsZEcS$6qPA.A0ULqTMNfn4UdQRDI7Q6Zrgyxq2IyJy18o1xYg
D1#
```

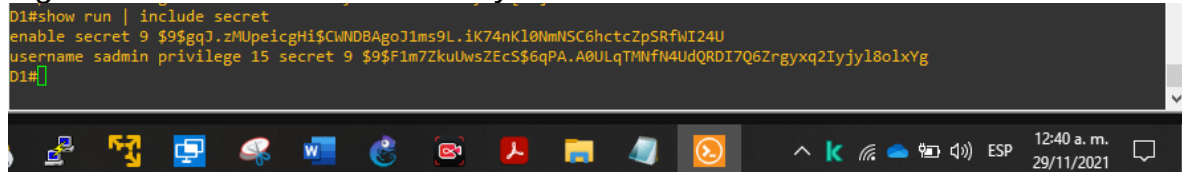


Figura 32. Verificación de usuario y contraseña creado en switch D2

```
D2#show run | include secret
enable secret 9 $9$gLS6SKjv.9erUi$rL4.Yb4hxfcPnRI.SDbES8N.9mmh7MOXiDTfU3gkRv2
username sadmin privilege 15 secret 9 $9$zD5kFFEqJWAlRy$/wrXaOQVYwL0.0AJYfvDV0sBnd1247GhwJzyfnGYsD6
D2#
```

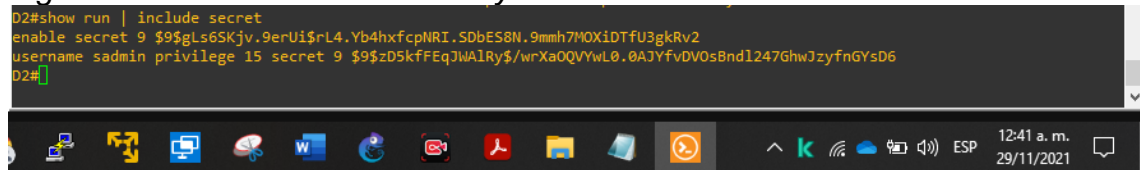


Figura 33. Verificación de usuario y contraseña creado en switch A1

```
A1#show run | include secret
enable secret 9 $9$JzEUBVUgNoopwy$cyYK1Y69v.ktorV3DKXMKfrmIs4oAWxqjJr2jGsEjDc
username sadmin privilege 15 secret 9 $9$tuPKmHP7nbsFZC$.DHS8qw.Rx83T2/N0AvbgNFKkv.TQq1DUvpoEvEJeaK
A1#
```

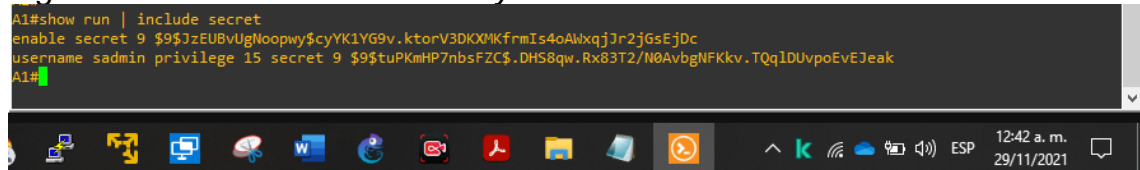


Figura 34. Verificación de usuario y contraseña creado en switch R1

```
R1#show run | include secret
enable secret 9 $9$7/3uLGxhTvLxoR$MSfE50qT8VFjoPq0d1njboFMHTFHlwyx5VoVhAONNJo
username sadmin privilege 15 secret 9 $9$i/Ewqd.B91yb.k$ZrUrsEQHbRixfEj0ZJmqNWFsc1w07y8W4wEhM1FBGcE
R1#
```

Figura 35. Verificación de usuario y contraseña creado en switch R2

```
R2#show run | include secret
enable secret 9 $9$RXw2N0IgxPlZ2h$nx2rPsDLIxy2PZqsh6Hqubw56ilb0ph1Bgu59fnaKCo
username sadmin privilege 15 secret 9 $9$XD.hiiG8k2KPXF$D2wbxD0tRkWI9EUz/68wPKnnfEPKceFQ3oL38CLos
R2#
```

Figura 36. Verificación de usuario y contraseña creado en switch R3

```
R3#show run | include secret
enable secret 9 $9$AF0YiZutkm97SR$abjqtRt36cUNIwsbNPS5w2L46ugPTnnk4YwmpFfjy0.
username sadmin privilege 15 secret 9 $9$JF24J1iVMijfVp$91Z0.ObFcZDPM9BxG0JRI5bRMvR2.K7a6PUBfZYBSYQ
R3#
```

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

```
R1(config)# aaa new-model
R3(config)# aaa new-model

D1(config)# aaa new-model
D2(config)# aaa new-model
A1(config)# aaa new-model
```

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

Especificaciones del servidor RADIUS.:

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

```
R1(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
R1(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
```

```
R3(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
R3(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
```

```
D1(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
D1(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
```

```
D2(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
D2(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
```

```
A1(config)# radius-server host 10.0.100.6 auth-port 1812 key $strongPass
A1(config)# radius-server host 10.0.100.6 auth-port 1813 key $strongPass
```

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

Especificaciones de autenticación AAA:

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

```
R1 (config)# aaa authentication login default group radius local
R1(config)#line console 0
R1(config-line)#login authentication default
```

```
R3 (config)# aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
```

```
D1 (config)# aaa authentication login default group radius local
D1(config)#line console 0
D1(config-line)#login authentication default
```

```
D2 (config)# aaa authentication login default group radius local
D2(config)#line console 0
D2(config-line)#login authentication default
```

```
A1 (config)# aaa authentication login default group radius local
A1(config)#line console 0
A1(config-line)#login authentication default
```

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

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

Acceso Router R1

R1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: admin

Password:

R1#

Figura 37. Verificación de autenticación en router R1

```
R1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
R1#
```

Acceso Router R3

R3, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: sadmin

Password:

R3#

Figura 38. Verificación de autenticación en router R3

```
R3, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
R3#
```

Acceso Switch D1

D1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: sadmin

Password:

D1#

Figura 39. Verificación de autenticación en switch D1

```
D1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
D1#
```

Acceso Switch D2

D2, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: sadmin

Password:

D2#

Figura 40. Verificación de autenticación en switch D2

```
Username: sadmin
Password:
*Nov 13 02:42:27.902: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.0.100.6:1812,1646 is not responding.
*Nov 13 02:42:27.902: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.0.100.6:1812,1646 is being marked alive.
*Nov 13 02:42:48.041: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.0.100.6:1813,1646 is not responding.
*Nov 13 02:42:48.041: %RADIUS-4-RADIUS_ALIVE: RADIUS server 10.0.100.6:1813,1646 is being marked alive.
D2#
```

Acceso Switch A1

A1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: sadmin

Password:

A1#

Figura 41. Verificación de autenticación en switch A1

```
A1, ENCOR Skills Assessment, Scenario 1
User Access Verification
Username: sadmin
Password:
A1#
```

Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red.

Las tareas de configuración son las siguientes:

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

Configure el reloj local a la hora UTC actual.

Configuración hora UTC -5 en R1

```
R1(config)#clock timezone UTC -5
```

```
*Nov 13 03:04:56.423: %SYS-6-CLOCKUPDATE: System clock has been updated
from 03:04:56 UTC Sat Nov 13 2021 to 22:04:56 UTC Fri Nov 12 2021, configured
from console by sadmin on console.
```

Consultar Hora UTC -5 Configurada

(Validación de la configuración de la hora realizada (Colombia -5 Horas)

```
R1#show clock detail
```

```
*22:05:29.579 UTC Fri Nov 12 2021
```

```
Time source is hardware calendar
```

```
R1#
```

Configuración hora UTC -5 en R2

```
R2(config)#clock timezone UTC -5
```

```
*Nov 13 03:04:56.423: %SYS-6-CLOCKUPDATE: System clock has been updated
from 03:04:56 UTC Sat Nov 13 2021 to 22:04:56 UTC Fri Nov 12 2021, configured
from console by sadmin on console.
```

Consultar Hora UTC -5 Configurada
(Validación de la configuración de la hora realizada (Colombia -5 Horas))
R2#show clock detail
*22:05:29.579 UTC Fri Nov 12 2021
Time source is hardware calendar

Configuración hora UTC -5 en R3

R3(config)#clock timezone UTC -5
*Nov 13 03:04:56.423: %SYS-6-CLOCKUPDATE: System clock has been updated
from 03:04:56 UTC Sat Nov 13 2021 to 22:04:56 UTC Fri Nov 12 2021, configured
from console by sadmin on console.

Consultar Hora UTC -5 Configurada
(Validación de la configuración de la hora realizada (Colombia -5 Horas))
R3#show clock detail
*22:05:29.579 UTC Fri Nov 12 2021
Time source is hardware calendar

Configuración hora UTC -5 en D1

D1(config)#clock timezone UTC -5
*Nov 13 03:04:56.423: %SYS-6-CLOCKUPDATE: System clock has been updated
from 03:04:56 UTC Sat Nov 13 2021 to 22:04:56 UTC Fri Nov 12 2021, configured
from console by sadmin on console.

Consultar Hora UTC -5 Configurada
(Validación de la configuración de la hora realizada (Colombia -5 Horas))
D1#show clock detail
*22:05:29.579 UTC Fri Nov 12 2021
Time source is hardware calendar

Configuración hora UTC -5 en D2

D2(config)#clock timezone UTC -5
*Nov 13 03:04:56.423: %SYS-6-CLOCKUPDATE: System clock has been updated
from 03:04:56 UTC Sat Nov 13 2021 to 22:04:56 UTC Fri Nov 12 2021, configured
from console by sadmin on console.

Consultar Hora UTC -5 Configurada
(Validación de la configuración de la hora realizada (Colombia -5 Horas))
D2#show clock detail
*22:05:29.579 UTC Fri Nov 12 2021
Time source is hardware calendar

Configuración hora UTC -5 en A1

A1(config)#clock timezone UTC -5

*Nov 13 03:04:56.423: %SYS-6-CLOCKUPDATE: System clock has been updated from 03:04:56 UTC Sat Nov 13 2021 to 22:04:56 UTC Fri Nov 12 2021, configured from console by sadmin on console.

Consultar Hora UTC -5 Configurada

(Validación de la configuración de la hora realizada (Colombia -5 Horas)

A1#show clock detail

*22:05:29.579 UTC Fri Nov 12 2021

Time source is hardware calendar

6.2 Configure R2 como un NTP maestro.

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

R2(config)#ntp master 3

Figura 42. validación configuración NTP en router R2

```
R2#sh run | i ntp
ntp master 3
R2#
R2#
```

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

Configure NTP de la siguiente manera:

R1 debe sincronizar con R2.

R1(config)#ntp server 209.165.200.30

Figura 43. validación configuración NTP en router R1

```
R1#sh run | i ntp
ntp server 209.165.200.30
R1#
```

R3, D1 y A1 para sincronizar la hora con R1.

R3(config)#ntp server 10.0.13.1

Figura 44. validación configuración NTP en router R3

```
R3#show run | i ntp
ntp server 10.0.13.1
R3#
```

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

Figura 45. validación configuración NTP en switch D1

```
D1#sh run | i ntp
ntp server 10.0.10.1
D1#
```

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

Figura 46. validación configuración NTP en switch A1

```
A1#sh run | i ntp
ntp server 10.0.10.1
A1#
```

D2 para sincronizar la hora con R3.

```
D2(config)#ntp server 10.0.11.1
```

Figura 47. validación configuración NTP en switch D2

```
D2#sh run | i ntp
ntp server 10.0.11.1
D2#
```

6.4 Configure Syslog en todos los dispositivos excepto R2

Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

Configuración del servidor syslog en los dispositivos de red (R1,R3,D1,D2 y A1) estos dispositivos envían los mensajes del sistema al servidor de syslog configurado.

Configuración Syslog en Router R1

```
R1(config)#logging 10.0.100.5
R1(config)#logging trap warning
R1(config)#exit
```

Configuración Syslog en Router R3

```
R3(config)#logging 10.0.100.5
R3(config)#logging trap warning
R3(config)#exit
```

Configuración Syslog en Switch D1

```
D1(config)#logging 10.0.100.5
D1(config)#logging trap warning
D1(config)#exit
```

Configuración Syslog en Switch D2

```
D2(config)#logging 10.0.100.5
D2(config)#logging trap warning
D2(config)#exit
```

Configuración Syslog en Switch A1

```
A1(config)#logging 10.0.100.5
A1(config)#logging trap warning
A1(config)#exit
```

6.5 Configure SNMPv2c en todos los dispositivos excepto R2

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.

Configuración SNMP en Router R1:

```
R1(config)#snmp-server community ENCORSA ro ACL_SNMP
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)#snmp-server location NETFLOW Collector
R1(config)#snmp-server contact ALBERTO PARADA
R1(config)#ip access-list standard ACL_SNMP
R1(config-std-nacl)#permit 10.0.100.5
R1(config-std-nacl)#
```

Configuración SNMP en Router R3:

```
R3(config)#snmp-server community ENCORSA ro ACL_SNMP
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server location NETFLOW Collector
R3(config)#snmp-server contact ALBERTO PARADA
R3(config)#ip access-list standard ACL_SNMP
R3(config-std-nacl)#permit 10.0.100.5
R3(config-std-nacl)#
```

Configuración SNMP en Switch D1:

```
D1(config)#snmp-server community ENCORSA ro ACL_SNMP
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server location NETFLOW Collector
D1(config)#snmp-server contact ALBERTO PARADA
D1(config)#ip access-list standard ACL_SNMP
D1(config-std-nacl)#permit 10.0.100.5
D1(config-std-nacl)#
```

Configuración SNMP en Switch D2:

```
D2(config)#snmp-server community ENCORSA ro ACL_SNMP
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server location NETFLOW Collector
D2(config)#snmp-server contact ALBERTO PARADA
D2(config)#ip access-list standard ACL_SNMP
D2(config-std-nacl)#permit 10.0.100.5
D2(config-std-nacl)#
```

Configuración SNMP en Switch A1:

```
A1(config)#snmp-server community ENCORSA ro ACL_SNMP
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server location NETFLOW Collector
A1(config)#snmp-server contact ALBERTO PARADA
A1(config)#ip access-list standard ACL_SNMP
A1(config-std-nacl)#permit 10.0.100.5
A1(config-std-nacl)#
```

En R3, D1, y D2, habilite el envío de traps config y ospf. Configuración envío de traps config y ospf en Router R3:

```
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#exit
```

Configuración envío de traps config y ospf en Switch D1:

```
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
D1(config)#exit
```

Comando snmp-server enable traps Config no soportado en el switch al momento de realizar la configuración, solo soporto el snmp-server enable traps ospf.

Figura 49. Verificación de la configuración SNMP en Router R3

The screenshot shows a Packet Tracer workspace with a network diagram and a terminal window for Router R3. The network diagram includes:

- Red ISP BGP ASN 500:** R2 (BGP router-id 2.2.2.2) with Loopback0 (10.0.0.2/32) and interface Fa0/0/24 (200.145.200.0/27).
- OSPF Area 0:** R1 (router-id 0.0.4.1) and R3 (router-id 0.0.4.3) connected via S1/0/1 and S1/0/24.
- Primary RTP Gateway:** A switch with VLAN 100 (10.0.100.1/24) and VLAN 102 (10.0.102.1/24).
- PC1:** Connected to the switch with IP 10.0.100.5/24.

The terminal window on R3 shows the following configuration:

```

R3# show run | include snmp
snmp-server community ENCORSA RO ACL_SNMP
snmp-server location NETFLOW Collector
snmp-server contact ALBERTO PARADA
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 retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
R3#
    
```

Figura 50. Verificación de la configuración SNMP en Switch D1

The screenshot shows a Packet Tracer workspace with a network diagram and a terminal window for Switch D1. The network diagram is identical to Figure 49.

The terminal window on Switch D1 shows the following configuration:

```

D1# show run | include snmp
snmp-server community ENCORSA RO ACL_snmp
snmp-server location NETFLOW Collector
snmp-server contact ALBERTO PARADA
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps cdp
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 ethernet cfa cc wdg-up wdg-down cross-connect loop-config
snmp-server enable traps ethernet cfa crosscheck wdg-missing wdg-unknown service-up
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps energywise
snmp-server enable traps pm vc
snmp-server enable traps litmus session
snmp-server enable traps litmus pseudowire status
snmp-server enable traps ether-nac
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps ethernet evc status create delete
D1#
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 10.0.100.5 version 2c ENCORSA
D1#
D1#
    
```

Figura 51. Verificación de la configuración SNMP en Switch D2

The screenshot shows a network diagram with several routers (R1, R2, R3) and switches (A1, D2). The network is configured with OSPF Area 0 and BGP. A terminal window on Switch D2 displays the following configuration:

```

D2#show run | include snmp
snmp-server community ENCORSA RO ACL_SNMP
snmp-server location NETFLOW Collector
snmp-server contact ALBERTO PARADA
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf iso
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 lia
snmp-server host 10.0.100.5 version 2c ENCORSA
D2#
    
```

The interface shows the user 'ALBERTO PARADA' with 'CC 1.031.145.989' and 'CISCO CCNP - TRABAJO FINAL'.

Figura 52. Verificación de la configuración SNMP en Switch A1

The screenshot shows the same network diagram as Figure 51. A terminal window on Switch A1 displays the following configuration:

```

A1#show run | include snmp
snmp-server community ENCORSA RO ACL_SNMP
snmp-server location NETFLOW Collector
snmp-server contact ALBERTO PARADA
snmp-server host 10.0.100.5 version 2c ENCORSA
A1#
    
```

The interface shows the user 'ALBERTO PARADA' with 'CC 1.031.145.989' and 'CISCO CCNP - TRABAJO FINAL'.

CONCLUSIONES

El simulador de red de cisco GNS3 nos permitió realizar el desarrollo de la red propuesta con router y switches reales capa 3, en donde se pudo ejecutar cada uno del comando para llevar a cabo el laboratorio del diplomado CCNP, a diferencia de Packet Tracer muchos comandos no son soportados.

Los protocolos de enrutamiento como OSPF y BGP nos permite comunicar diferentes segmentos de red, en donde cada dispositivo anuncia las redes directamente conectadas y así permitir intercomunicarse los demás dispositivos entre sí.

Las VLAN nos permitió realizar segmentaciones de redes lógicas en los switches, así crear enlaces troncales y enlaces EtherChannel para la creación de una red robusta, convergente y de alta disponibilidad.

Los servidores NTP nos permiten tener los dispositivos de red sincronización en su hora para así tener un control y monitoreo de la red segura y eficiente.

El diplomado realizado me permitió fortalecer mas mis conocimiento en diseño y solución de problemas en dispositivos de red, realizar la configuración mas sencilla en un router y switch, como también implementar la seguridad y monitoreo de los dispositivos activos de red.

BIBLIOGRAFÍA

UNAD (2017). **Configuración de Switches y Routers [OVA]**. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC>

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

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

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

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

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **OSPF v3**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **Advanced BGP**. 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). **Multicast**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **QoS**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUqUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **IP Services**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de <https://1drv.ms/b/s!AAIGg5JUqUBthk8>