DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS YESID CORTÉS LOMBANA

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS YESID CORTÉS LOMBANA

Diplomado de opción de grado presentado para optar el título de INGENIERO ELECTRÓNICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 29 de noviembre de 2021

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

IP SLa: Se trata de una herramienta incluida en Cisco IOS que nos permite analizar niveles de servicios de aplicaciones y servicios IP. Es una tecnología de monitoreo continuo activo de tráfico en la red que nos brinda un método confiable de análisis de performance de la red.

IPv4: El Protocolo de Internet versión 4 (en inglés, Internet Protocol version 4, IPv4) es la cuarta versión del Internet Protocol (IP), un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET.

IPV6: Es la versión 6 del Protocolo de Internet (Internet Protocol), es decir, es la sexta versión del protocolo que hace posible conectar dispositivos en Internet, identificándolos con una dirección unívoca.

OSPFv2: Es un protocolo de routing de estado de enlace para IPv4 que se presentó en 1991. OSPF se diseñó como alternativa a otro protocolo de routing IPv4, RIP.

Switch: Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

VLAN: Nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soporten VLANs para segmentar adecuadamente la red.

RESUMEN

Este trabajo argumenta la ejecución de diferentes temáticas expuestas en el diplomado de profundización CCNP competente para la carrera de Ingeniería electrónica.

Las habilidades se encaminan en el desarrollo de la completa configuración de red logrando una accesibilidad satisfactoria en todos los extremos requeridos y que los equipos de cómputo obtengan un soporte eficaz en el desarrollo de las actividades solicitadas. Para generar el cumplimiento del trabajo se instituye el enrutamiento de ipv4 e ipv6 de las redes y subredes, el intercambio de protocolos de comunicación.

Inicialmente se ejecuta la configuración de la topología en el simulador de GNS3 que permite diseñar y poner en marcha las respectivas simulaciones permitiendo la combinación de dispositivos reales y virtuales. Las imágenes que se utilizaron para realizar el enrutamiento fueron los Router 7200 los cuales soportan todas las características de los protocolos, fue escogido por el bajo consumo de RAM, se utiliza la imagen virtual IOS L3 teniendo en cuenta que resiste todos los comandos de un switch de capa 3. En cada imagen se configuran los Slots de los puertos fastEthernet, gigabitEthernet y serial para poder realizar la interconexión dentro de los Routers y los switchs, posterior a ello se ejecuta la topología e inicia la configuración en consola de cada uno de estos.

Posteriormente se establecen las funciones de administración de la red, y así se da efectivo cumplimiento al escenario planteado, exponiendo el paso a paso del debido procedimiento en la línea de comandos o códigos usados para la configuración.

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

ABSTRACT

This work argues the execution of different themes exposed in the CCNP deepening diploma competent for the Electronic Engineering career.

The skills are directed in the development of the complete network configuration, achieving satisfactory accessibility at all the required ends and the computer equipment obtaining effective support in the development of the requested activities. To generate the fulfillment of the work, the routing of ipv4 and ipv6 of the networks and subnets is instituted, the exchange of communication protocols.

Initially, the topology configuration is executed in the GNS3 simulator, which allows the design and implementation of the respective simulations, allowing the combination of real and virtual devices. The images that were used to carry out the routing were the 7200 Router which support all the characteristics of the protocols, it was chosen due to the low consumption of RAM, the IOS L3 virtual image is used taking into account that it resists all the commands of a switch of layer 3. In each image, the slots of the fastEthernet, gigabitEthernet and serial ports are configured to be able to perform the interconnection within the routers and switches, after that the topology is executed and the console configuration of each of these begins .

Subsequently, the network administration functions were carried out, and thus the proposed scenario is effectively fulfilled, exposing the step by step of the due procedure in the command line or codes used for the configuration.

Key words: CISCO, CCNP, Routing, Swicthing, Networking, Electronics

INTRODUCCIÓN

Las redes de datos permiten intercambiar información entre equipos de cómputo o dispositivos conectados en red, para esto se requieren diferentes medios de comunicación tanto físicos como lógicos (cables, señales y medios de transmisión) que permiten compartir recursos.

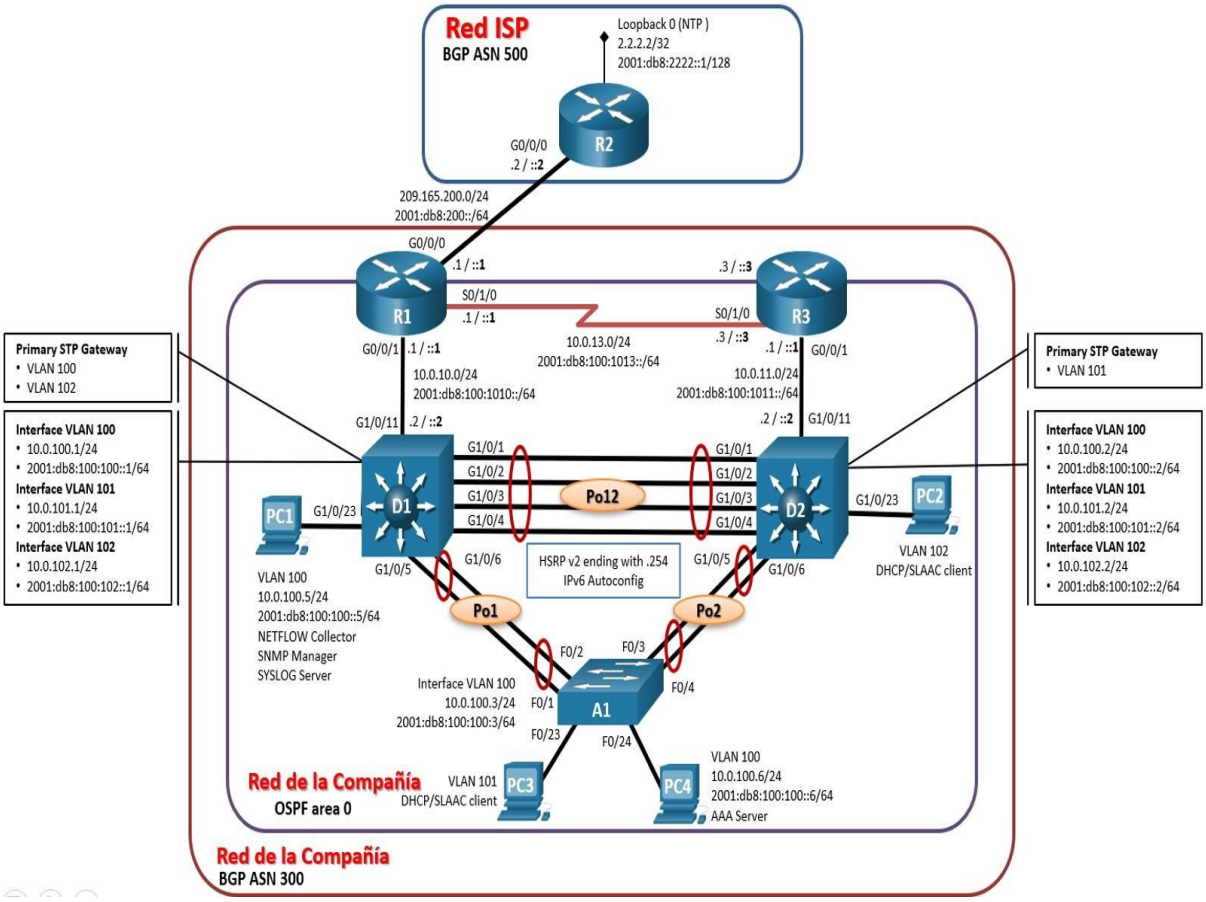
Actualmente, las redes de datos se han convertido en una necesidad para los seres humanos y su continua evolución, ha llevado a desarrollar soluciones en busca de mejoras en cuanto a la estabilidad y rapidez de las redes; cada día se busca mayor optimización de los recursos para minimizar los costos. Detrás de cada uno de estos procesos existen un sin número de componentes para poder garantizar la confiabilidad, escalabilidad y administración de la red.

Con este proyecto se busca desarrollar las habilidades de los futuros diseñadores de redes viendo de forma detallada cada proceso involucrado en la construcción de una red, permitiendo afianzar los conocimientos mediante la aplicación simulada para tener mejor dominio y comprensión de los funcionamientos de los dispositivos que conforman una red; desde la conexión hasta la configuración de estos.

DESARROLLO

1. ESCENARIO 1.

Figura 1 Topología del escenario



1.1. Direccionamiento de la topología

Tabla 1. Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Parte1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

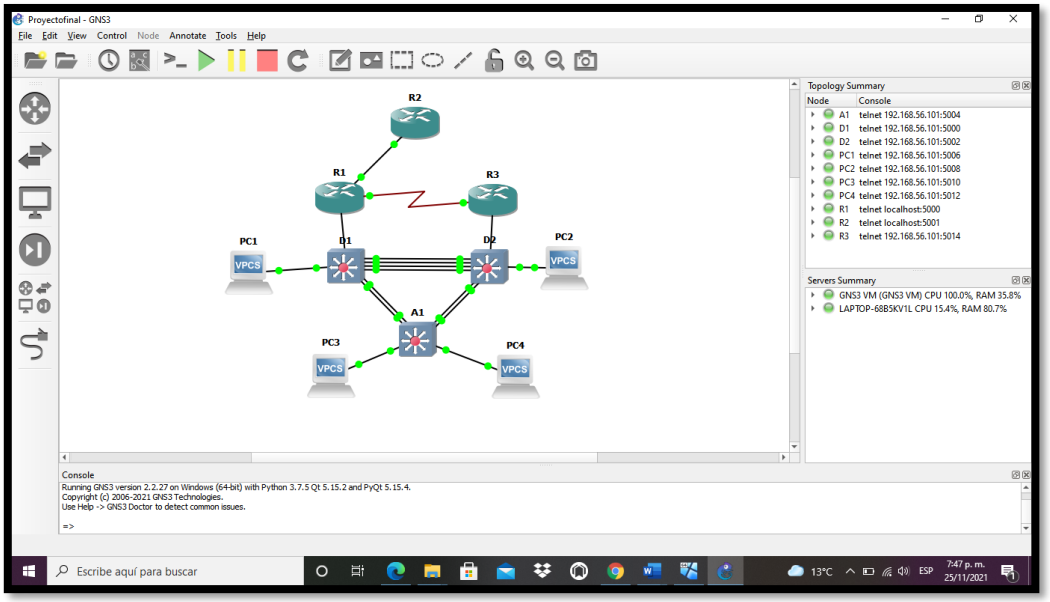
1.2. Paso 1: Cablear la red como se muestra en la topología.

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

El escenario propuesto es realizado en el software GNS3 y las imágenes que fueron descargadas y utilizadas para el montaje son: imagen c3725 para los

router R1 y R2, para el Router 3 la imagen utilizadas fue la c7200 y finalmente para los switch D1, D2 y A1 fue la IOS L2 la cual soporta todas las configuraciones para CCNP

Figura 2 Simulación del escenario propuesto



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

1.3.1 Mediante una conexión de consola ingrese en cada dispositivo, entre al modo de configuración global y aplique los parámetros básicos. Las configuraciones de inicio para cada dispositivo son suministradas a continuación:

A continuación, se presenta la configuración del Router paso a paso según las características del programa GNS3, se da una explicación del código línea por línea para identificar la configuración que conlleva cada una de estas.

Router 1

Se ingresa a modo configuración

Router#Config terminal

Se indica el nombre del router
Router(config)#hostname R1

Tipo de direccionamiento IPV6 unidifisión
R1(config)# ipv6 unicast-routing no ip domain lookup

Mensaje cuando se conecta a consola
R1(config)# banner motd # R1, ENCOR Skills Assessment, Scenario 1 #

Configuración de la línea de consola
R1(config)# line con 0

Se retira el límite de tiempo
R1(config-line)# exec-timeout 0 0

Depuración de mensajes no solicitados
R1(config-line)# logging synchronous

Salida modo de configuración de la línea de consola
R1(config-line)# exit

Configuración de la interfaz f1/0
R1(config)# interface f1/0

Asignación dirección IP
R1(config-if)# ip address 209.165.200.225 255.255.255.224

Asignación dirección IPV6
R1(config-if)# ipv6 address fe80::1:1 link-local ipv6 address 2001:db8:200::1/64

Reinicia la interfaz
R1(config-if)# no shutdown

Salida de configuración de la interfaz f1/0
R1(config-if)# Exit

Configuración de la interfaz f0/1
R1(config)#   interface f0/1

Asignación dirección IP
R1(config-if)# ip address 10.0.10.1 255.255.255.0

Asignación dirección IPV6
R1(config-if)# ipv6 address fe80::1:2 link-local
R1(config-if)# ipv6 address 2001:db8:100:1010::1/64

Reinicia la interfaz

R1(config-if)# no shutdown

Salida de configuración de la interfaz f0/1
R1(config-if)# exit

Configuración de la interfaz f2/0
R1(config)# interface s2/0

Asignación dirección IP
R1(config- if)# ip address 10.0.13.1 255.255.255.0

Asignación dirección IPV6
R1(config- if)# ipv6 address fe80::1:3 link-local
R1(config- if)# ipv6 address 2001:db8:100:1013::1/64 no shutdown
R1(config- if)# exit

Para los Router 2 y 3, se realiza la misma configuración con las direcciones IP correspondientes.

Router 2

Config terminal
hostname R2
ipv6 unicast-routing no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0 logging synchronous
exit
interface f1/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local ipv6 address 2001:db8:2222::1/128
no shutdown
exit

Router 3

Config terminal
hostname R3
ipv6 unicast-routing no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0 logging synchronous
exit
interface f1/0
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
no shutdown
exit

```
interface s2/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

Respecto al Switch multicapa se realiza el cambio de nombre según corresponda (D1), asignación de nombres Vlan, direccionamiento IPV6 e IPV4 para las interfaces g1/1, Vlan 100, Vlan 101, Vlan 102 y Vlan 999, reinicio de las interfaces y estado bajo para las interfaces g0/1-3 , g1/0-3 , g2/1-2 , g3/0.

Switch D1

Modo configuración

```
Enable
Config terminal
```

Asignación de nombre

```
hostname D1
```

Habilitación de enrutamiento

```
ip routing
ipv6 unicast-routing
```

Desactivación busqueda de dominio

```
no ip domain lookup
```

Mensaje cuando se conecta a consola

```
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
```

Configuración de la línea de consola

```
line con 0
```

Se retira el límite de tiempo

```
exec-timeout 0 0
```

sincronización de logeo

```
logging synchronous
exit
```

Asignación de nombre de las vlan

```
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
```

se accede a la interfaz

```
interface g1/1
no switchport
```

Asignación de dirección IP

```
ip address 10.0.10.2 255.255.255.0
```

Asignación de dirección link

```
ipv6 address fe80::d1:1 link-local
```

Asignación de dirección IPV6

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

Se inicializa la interfaz

```
no shutdown
exit
```

Se accede a las interfaces vlan 100, 101, 102, se configuran las derecciones IP, dirección lik y dirección IPV6

```
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
```

```
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
```

Se excluyen direcciones de vlan 101 y 102

```
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
```

Se crea un pool de direcciones IP

```
ip dhcp pool VLAN-102
```

Asignación del rango

```
network 10.0.102.0 255.255.255.0
```

Definición de puerta de enlace

```
default-router 10.0.102.254
exit
```

Se inactivan el rango de interfaces

```
interface range g0/1-3 , g1/0-3 , g2/1-2 , g3/0
shutdown
exit
```

Para el switch D2, se realiza la misma configuración con las direcciones IP correspondientes.

Switch D2

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

```
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/1
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range g0/1-3 , g1/0-3 , g2/1-2 , g3/0
shutdown
exit
```

Para el switch A1 se utiliza la imagen IOS L2, es la que soporta todas las características y se representa como una switch de capa 3 en la topología realizada, en esta configuración se realiza la misma configuración que se

realizó en la etapa anterior

Switch A1

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

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

Para esto se realiza la copia de configuración de la Ram a NVram en cada dispositivo.

Router 1 2 y 3

```
Copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK].
```

Switch D1 D2 y A1

```
Enable
Copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
Compressed configurations from 3770 bytes to 1762 bytes [OK]
*Nov 26 03:24:15.369: GRUB-5-CONFIG WRITING: GRUB configuration is being update
d on disk. Please wait...
*Nov 26 03:24:16.178: GRUB-5-CONFIG WRITTEN: GRUB configuration was written to disk
successfully.
24:15.369; GRUB-5-CONFIG_WRITING: GRUB configuration is being update
```

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

Se ingresa la dirección IP 10.0.100.5/24 seguida del enlace de puerta de enlace 10.0.100.254:

PC 1

```
PC1> IP 10.0.100.5/24 10.0.100.254
Chcking for duplicate address…
PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254
```

PC4

```
PC4> IP 10.0.100.6/24 10.0.100.254
Chcking for duplicate address…
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
```

Posterior a ello se ingresa la dirección IPV6 como se encuentra a continuación:

PC1

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

PC4

```
PC4>  ip 2001:db8:100:100::6/64 2001:db8:100:100::6
PC4 : 2001:db8:100:100::5/64
```

Parte2: 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.

2. Las tareas de configuración son las siguientes:

Tabla 2. Tarea de configuración parte 2

Tarea#	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: D1 and D2 D1 and A1 D2 and A1
2.2	En todos los switches cambie la VLAN nativaen los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocoloRapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en casode falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades deapoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannelsLACP como se muestra en el diagrama detopología.	Use los siguientes números de canales: D1 a D2 – Port channel 12 D1 a A1 – Port channel 1 D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, comose muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: D1: 10.0.100.1 D2: 10.0.100.2 PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: D1: 10.0.102.1 D2: 10.0.102.2 PC3 debería hacer ping con éxito a: D1: 10.0.101.1 D2: 10.0.101.2 PC4 debería hacer ping con éxito a: D1: 10.0.100.1 D2: 10.0.100.2 PC1: 10.0.100.5

En este paso se especificaran los direccionamientos de la IPV4 e IPV6 a fin de establecer comunicación entre los switch y los router de la topología que se ha venido trabajando en la parte anterior; para ellos se configura es el D1 para el encapsulamiento de las interfaces troncales, se utilizan las interconexiones de g0/1, g0/2, g0/3 y g1/0 que van al D2, posterior a ello, se le asigna al switch la VLAN nativa 999; luego se crean los puertos según la topología propuesta, luego se habilita la interfaz.

2.1. se configura las interfaces IEEE 802.1Q sobre los enlaces de interconexión de los switches

Switch D1

```
Enable
config t
interface range g0/1-3 , g1/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

Switch D2

```
Enable
Config t
interface range g0/1-3 , g1/0 , g2/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown
```

Switch A1

Enable
Config t
interface range g1/1-3 , g2/1-2
switchport trunk encapsulation dot1q
switchport mode trunk
no shutdown

2.2 Configuración vlan nativa interfaces g0/1-3 , g1/0

Switch D1

interface range g0/1-3 , g1/0
switchport mode trunk
switchport trunk native vlan 999

Switch D2

interface range g2/1-2
switchport mode trunk
switchport trunk native vlan 999

Switch A1

Enable
Config t
interface range g2/1-2
switchport mode trunk
switchport trunk native vlan 999

2.3 Se habilitan todos los protocolos RSTP

Switch D1

Enable
Config t
spanning-tree mode rapid-pvst

Switch D2

Enable
Config t
spanning-tree mode rapid-pvst

Switch A1

Enable
Config t
spanning-tree mode rapid-pvst

2.4 Configuración de puertos raíz con prioridades en las VLAN 100 y 102

Switch D1

```
Enable
Config t
spanning-tree vlan 100,102 root primary      //configuración Puente de raiz
spanning-tree vlan 101 root secondary        //configuración Puente de respaldo
```

Switch D2

```
Enable
Config t
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
```

Switch A1

```
Enable
Config t
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
```

2.5 Se crean los EtherChannels en las intefaces g0/1-3, g1/0

Switch D1

```
Enable
Config t
Int range g0/1-3 , g1/0              //configuración interfaz
channel-group 12 mode active   //configuración del canal del grupo 12 en modo activo
exit
int range g1/2-3
channel-group 1 mode active     //configuración del canal del grupo 1 en modo activo
```

Switch D2

```
Enable
Config t
Int range g0/1-3 , g1/0
channel-group 12 mode active
exit
int range g2/1 , g2/2
channel-group 2 mode active
```

Switch A1

```
Enable
Config t
Int range g1/2-3
channel-group 1 mode active
exit
```

```
int range g2/1-2
channel-group 2 mode active
exit
```

2.6. En la interconexión del switch con el PC g3/0 se configuran los puertos de acceso

```
interface g3/0                  //asignación de la interfaz
switchport mode access          //configuración modo de acceso
switchport access vlan 100      //asignación vlan al puerto
spanning-tree portfast          //se habilita el portfast
no shutdown                     //se inicializa la interfaz
exit
end
```

2.7. Verificación conectividad Paso 2

Figura 3 configuración interfaces globales, troncales y LACP

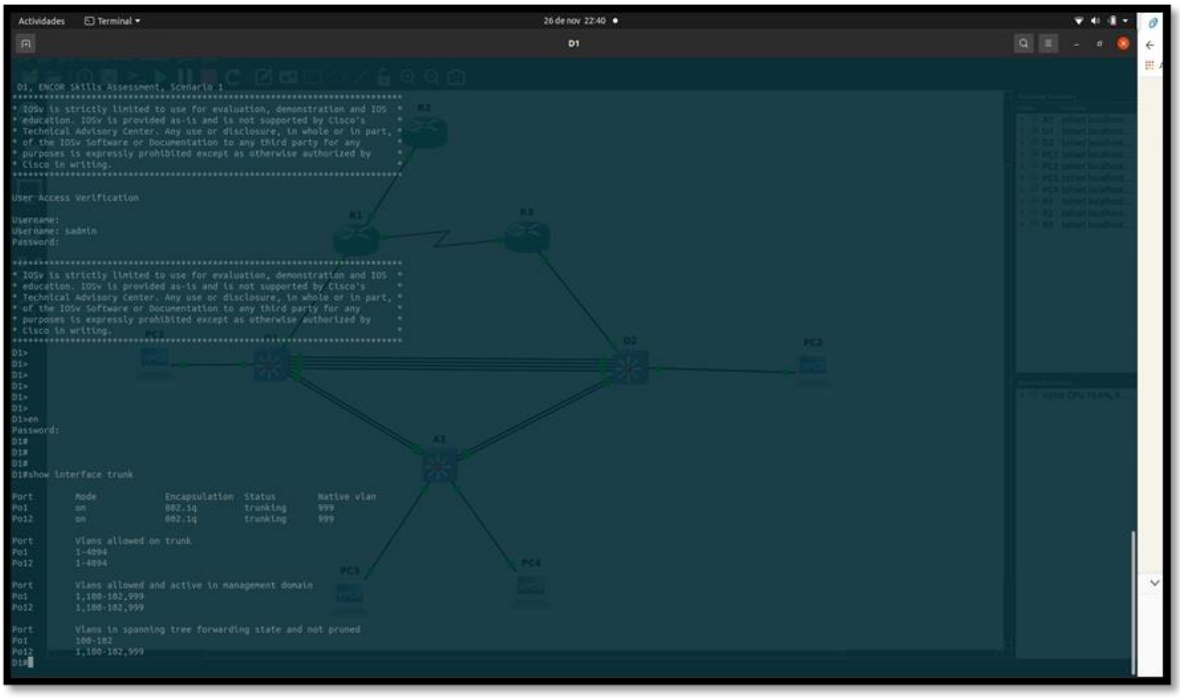


Figura 4 habilitación RSTP y puente raíz

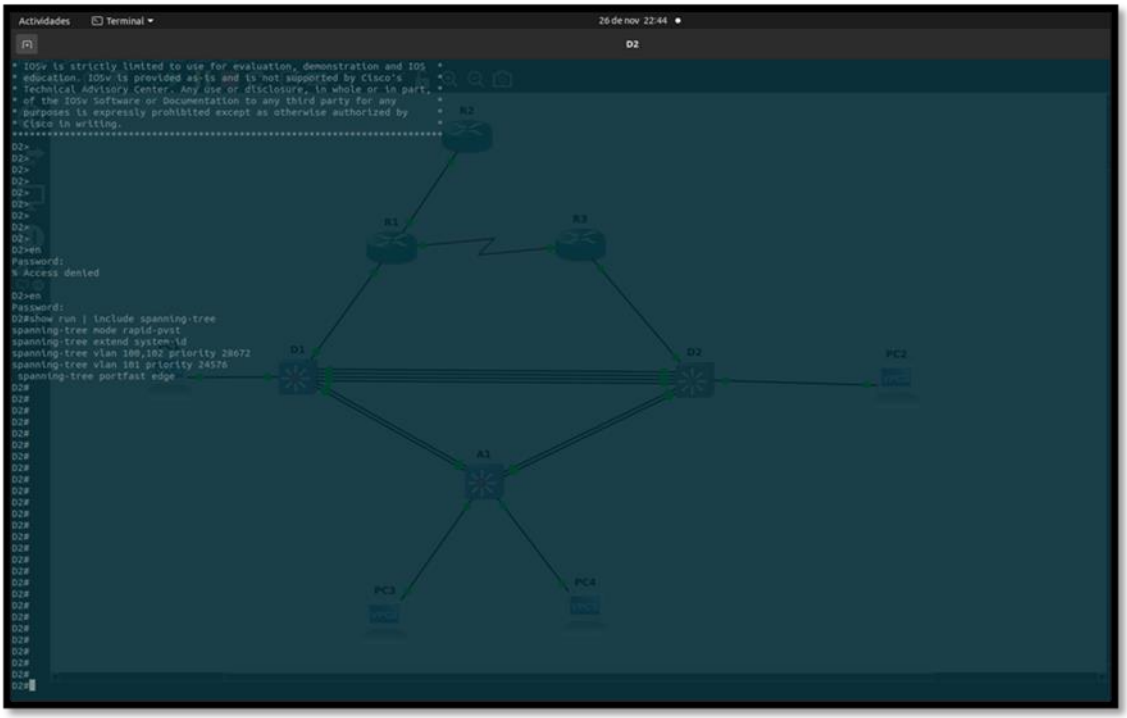


Figura 5 puertos de acceso PC1, PC2, PC3, PC4

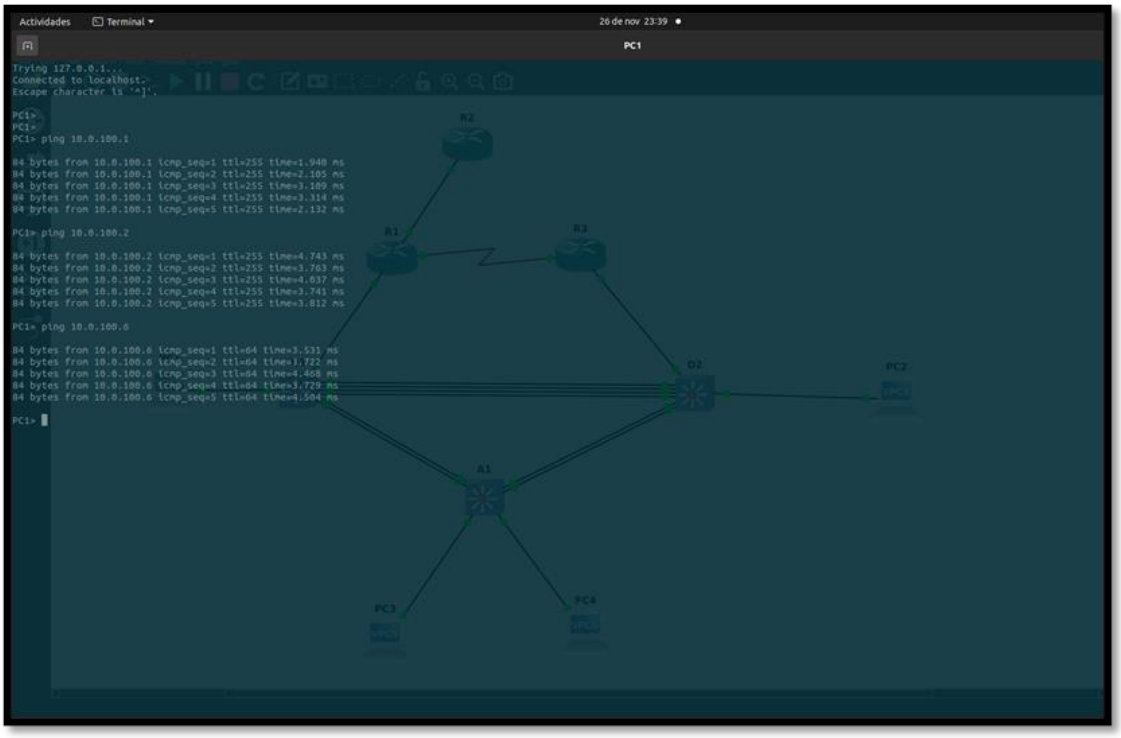


Figura 6 conectividad PC1 – D1, D2, PC4

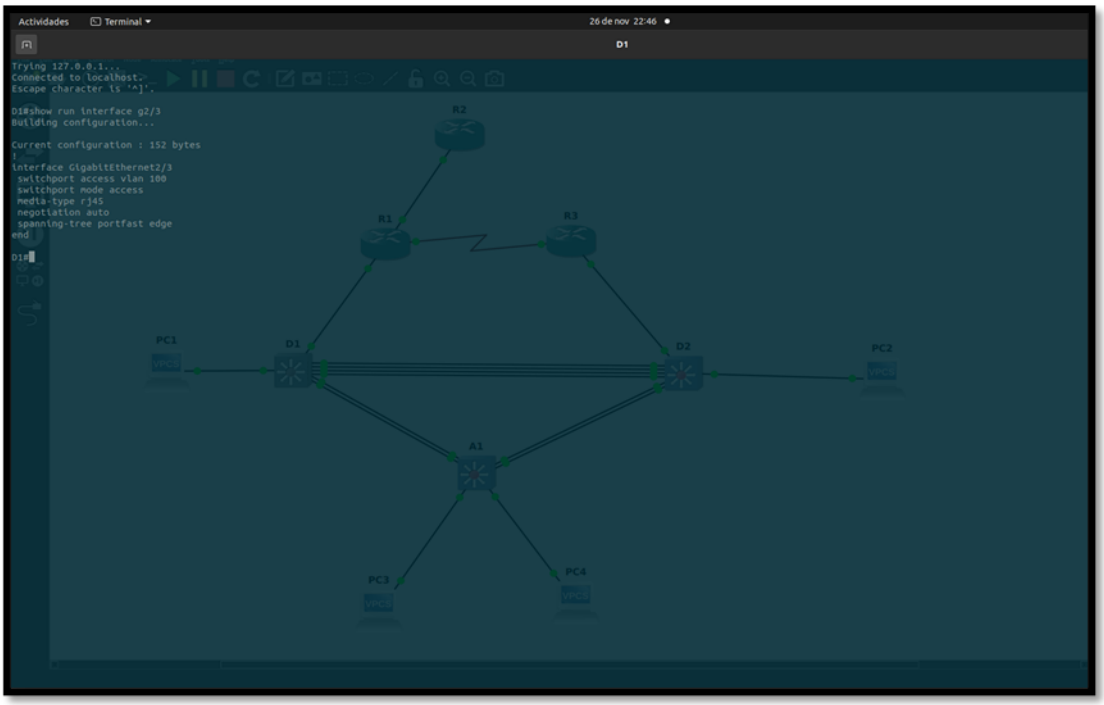


Figura 7 conectividad PC2 – D1, D2

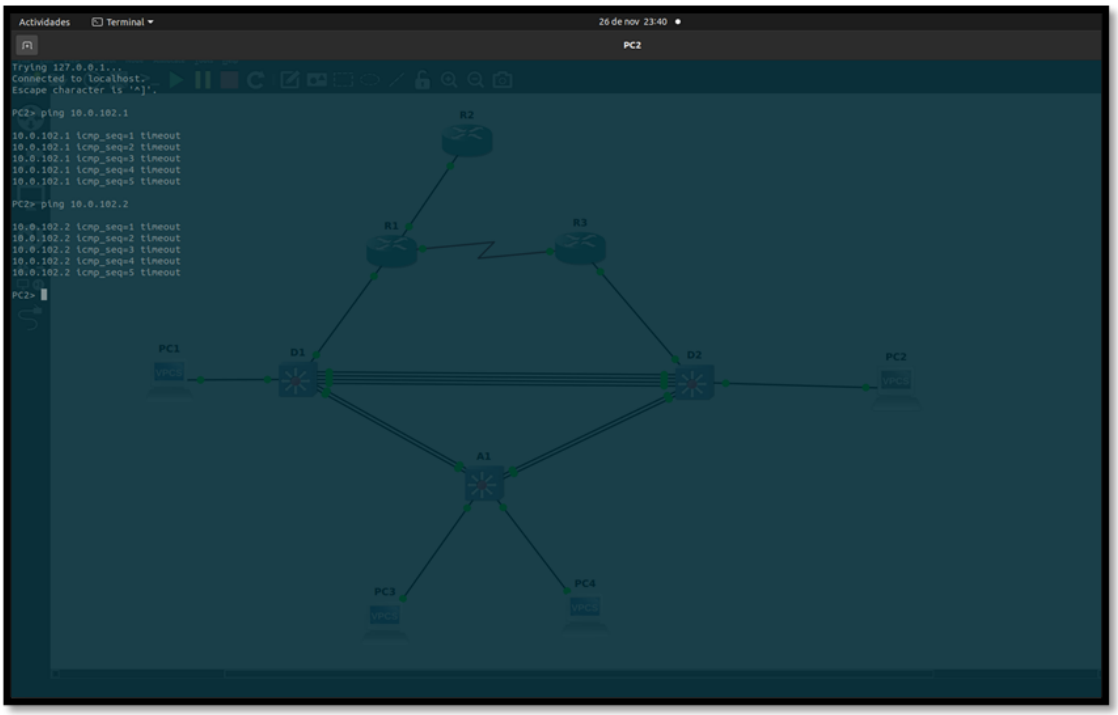


Figura 8 conectividad PC3 – D1, D2

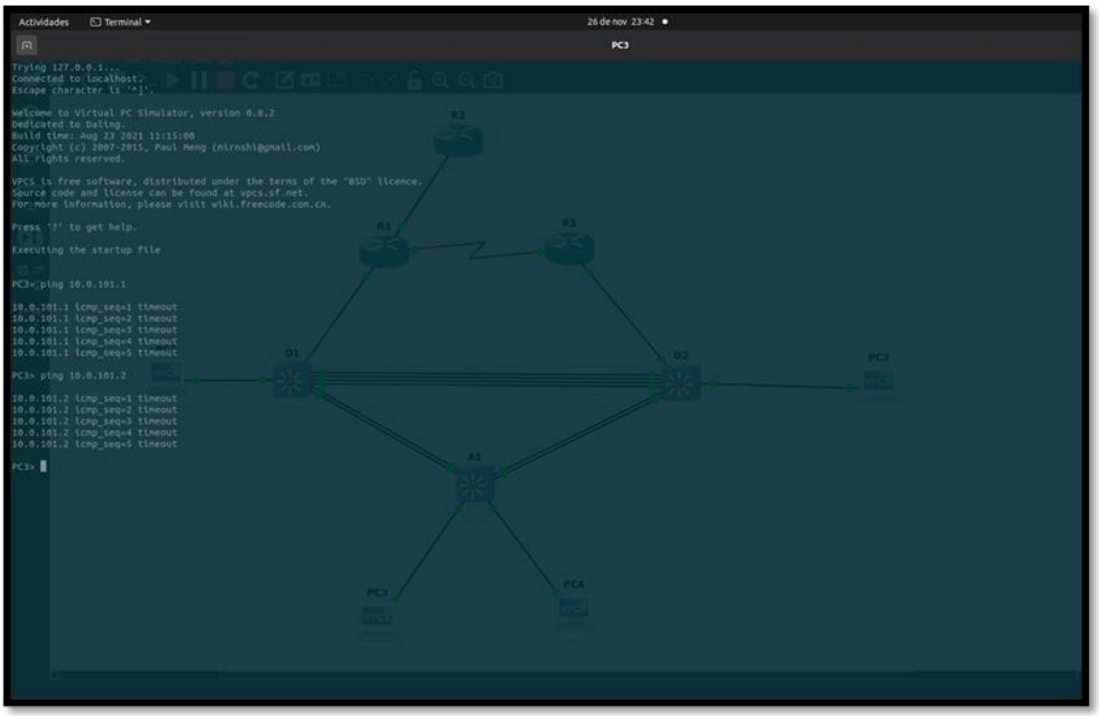
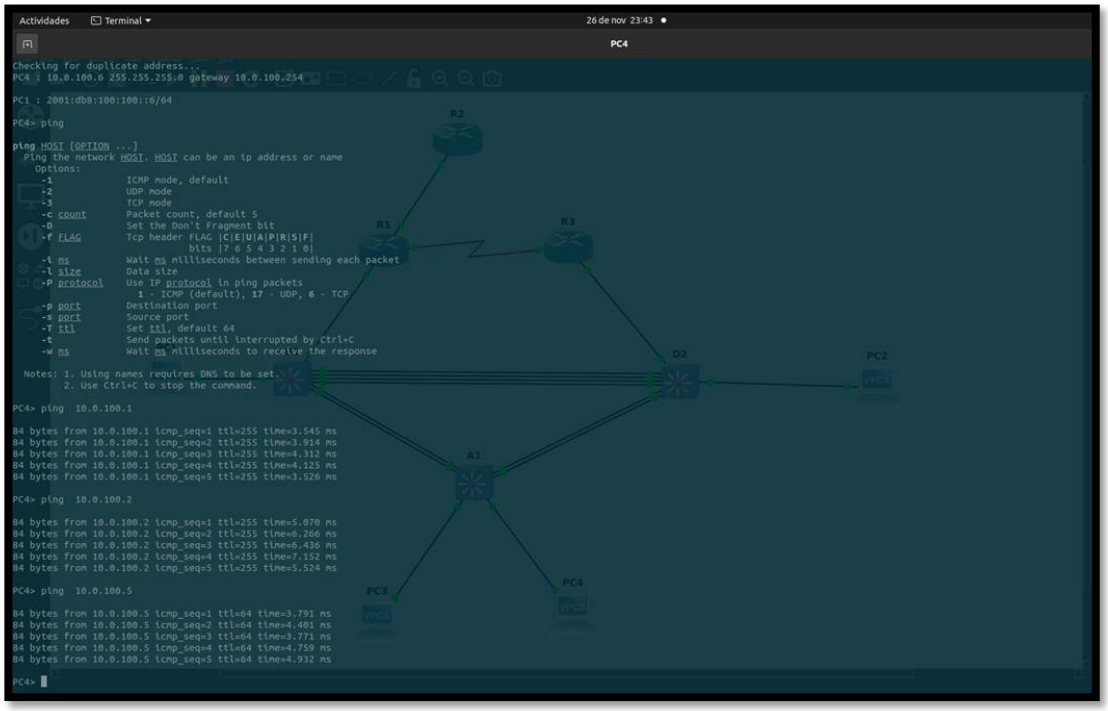


Figura 9 conectividad PC4 – D1, D2



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.

3 Las tareas de configuración son las siguientes:

Tabla 3. Tarea de configuración parte 3

Tarea#	Tarea	Especificaciones
3.1	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	Use OSPF Process ID **4** y asigne los siguientes router-IDs: R1: 0.0.4.1 R3: 0.0.4.3 D1: 0.0.4.131 D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. En R1, no publique la red R1 – R2. En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: D1: todas las interfaces excepto G1/0/11 D2: todas las interfaces excepto G1/0/11

3.2	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 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 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. En R1, no publique la red R1 – R2. On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: D1: todas las interfaces excepto G1/0/11 D2: todas las interfaces excepto G1/0/11
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. Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6con R1 en ASN 300. En IPv4 address family, anuncie: La red Loopback 0 IPv4 (/32). La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: La red Loopback 0 IPv4 (/128). La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MP-BGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: Deshabilite la relación de vecino IPv6. Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8.En IPv6 address family: Deshabilite la relación de vecino IPv4. Habilite la relación de vecino IPv6. Anuncie la red 2001:db8:100::/48.

Se configura en los protocolos en los Router 1 y 3 los estados de enlace para IPV4 con el protocolo OSPFv2 (Open Shortest Path First), Seguidamente se definen para la red IPV6 (OSPFv3) en las interfaces f0/1 y s2/0, posterior a ello, se declaran los protocolos de la puerta de enlace marginal (BGP). En los Switch D1 y D2 se realizan las mismas configuraciones y adicional a ello inhabilitan los protocolos OSPFv3 para la interfaz g1/1.

3.1 Configuración OSPv2

Router R1

```
Enable
Config t
router ospf 4                          //se habilita el OSPF con el indicador
router-id 0.0.4.1
network 10.0.10.0 0.0.0.255 area 0     //se configural las redes en el area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate          //se genera la ruta por default
exit
```

Router 3

```
Enable
Config t
router ospf 4
router-id 0.0.4.3
network 10.0.11.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
exit
```

Switch D1

```
Enable
Config t
router ospf 4
router-id 0.0.4.131
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface g1/0/11
exit
```

Switch D2

```
Enable
Config t
router ospf 4
router-id 0.0.4.132
network 10.0.100.0 0.0.0.255 area 0
network 10.0.101.0 0.0.0.255 area 0
network 10.0.102.0 0.0.0.255 area 0
network 10.0.11.0 0.0.0.255 area 0
passive-interface default
no passive-interface g1/1
exit
```

3.2 Configuración OSPv3

Router R1

```
Enable
Config t
Ipv6 router ospf 6              //se habilita el OSPF con el indicador
router-id 0.0.6.1
default-information originate   //se genera una ruta por default
exit
interface f0/1                  //configuración de la interfaz
ipv6 ospf 6 area 0              //se habilita OSPF6 en el area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
```

Router R3

```
Enable
Config t
ipv6 router ospf 6
Router-id 0.0.6.3
exit
interface f1/0
ipv6 ospf 6 area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
end
```

Switch D1

```
Enable
Config t
ipv6 router ospf 6
```

```
router-id 0.0.6.131
passive-interface default          //configuración como interfaz pasiva
no passive-interface g1/1          //se excluye la interfaz
exit
interface g1/1                     //configuración de la interfaz
ipv6 ospf 6 area 0                 //se habilita OSPFv6 en la interfazen el area 0
exit
interface vlan 100                 //configuración de la interfaz
ipv6 ospf 6 area 0                 //se habilita OSPFv6 en la interfazen el area 0
exit
interface vlan 101                 //configuración de la interfaz
ipv6 ospf 6 area 0                 //se habilita OSPFv6 en la interfazen el area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

Switch D1

```
Enable
Config t
ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface g1/1
exit
interface g1/1
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

3.3 Configuración de protocolos de la puerta de enlace marginal (BGP) para el Router 2

Configuración MP-BGP en la red ISP

Router R2

```
Enable
config t
ip route 0.0.0.0 0.0.0.0 loopback 0     // interfaz de salida se configura una ruta por default
ipv6 route ::/0 loopback 0              //configuración  IPV6
router bgp 500                          //configuración BGP 500
```

```
bgp router-id 2.2.2.2                          //asignación BGP
neighbor 209.165.200.225 remote-as 300         //configuración ASN con relación a R1
neighbor 2001:db8:200::1 remote-as 300
address-family ipv4
neighbor 209.165.200.225 activate              //configuración en relación con el vecino
no neighbor 2001:db8:200::1 activate           //se excluye la IPV6
network 2.2.2.2 mask 255.255.255.255          //configuración en relación con R2
network 0.0.0.0                                //Red predeterminada
exit-address-family
address-family ipv6
no neighbor 209.165.200.225 activate
neighbor 2001:db8:200::1 activate
network 2001:db8:2222::/128
network ::/0
exit-address-family
```

3.4 Configuración MP-BGP en la red ISP R2

Router R1

```
Enable
Config t
ip route 10.0.0.0 255.0.0.0 null0              //ruta predeterminada
ipv6 route 2001:db8:100::/48 null0             //configuración de ruta IPV6
router bgp 300                                 //configuración BGP
bgp router-id 1.1.1.1                          //Asignación de identificador
neighbor 209.165.200.226 remote-as 500         //configuración en relación R2
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-familyguración
```

3.5. Verificaciones de conectividad punto 3

Figura 10 verificación OSFv2

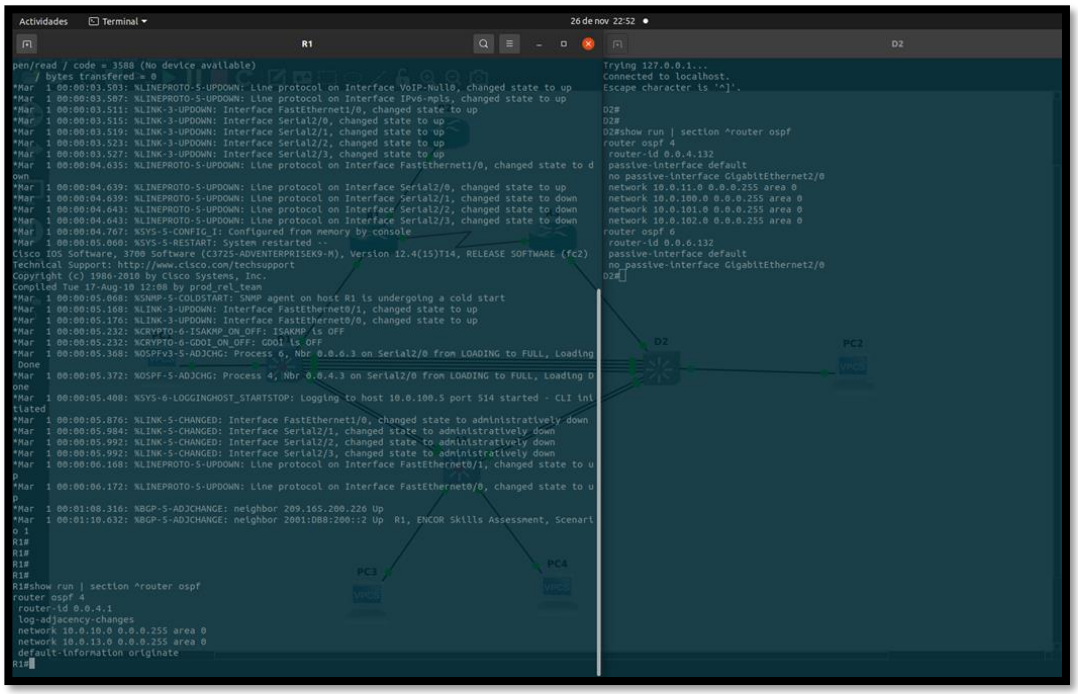


Figura 11 verificación OSFv3

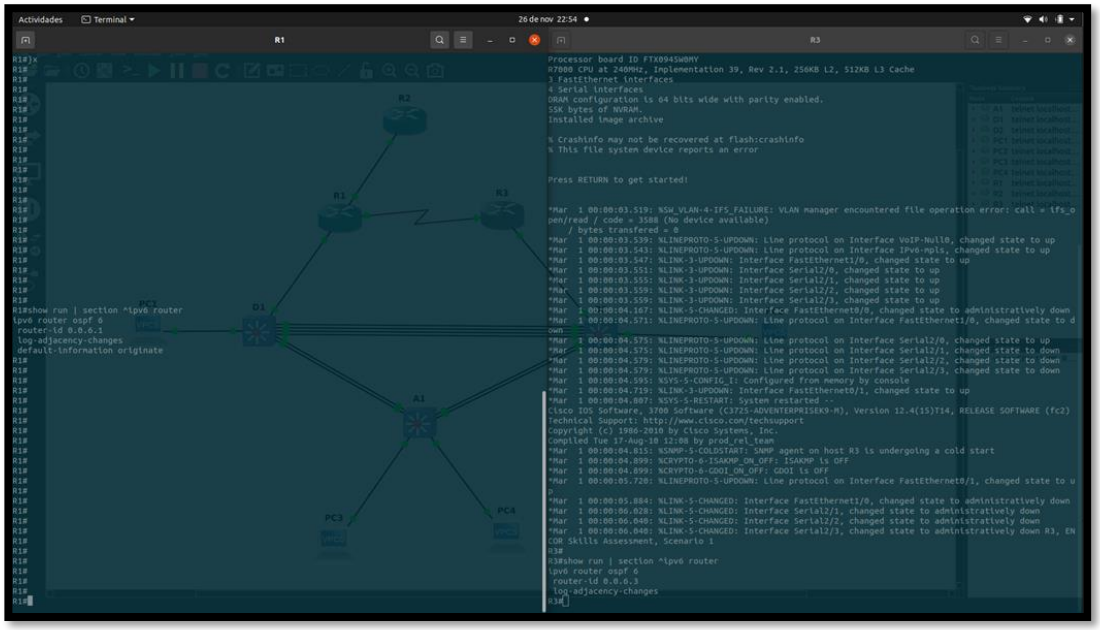


Figura 12 verificación Red ISP

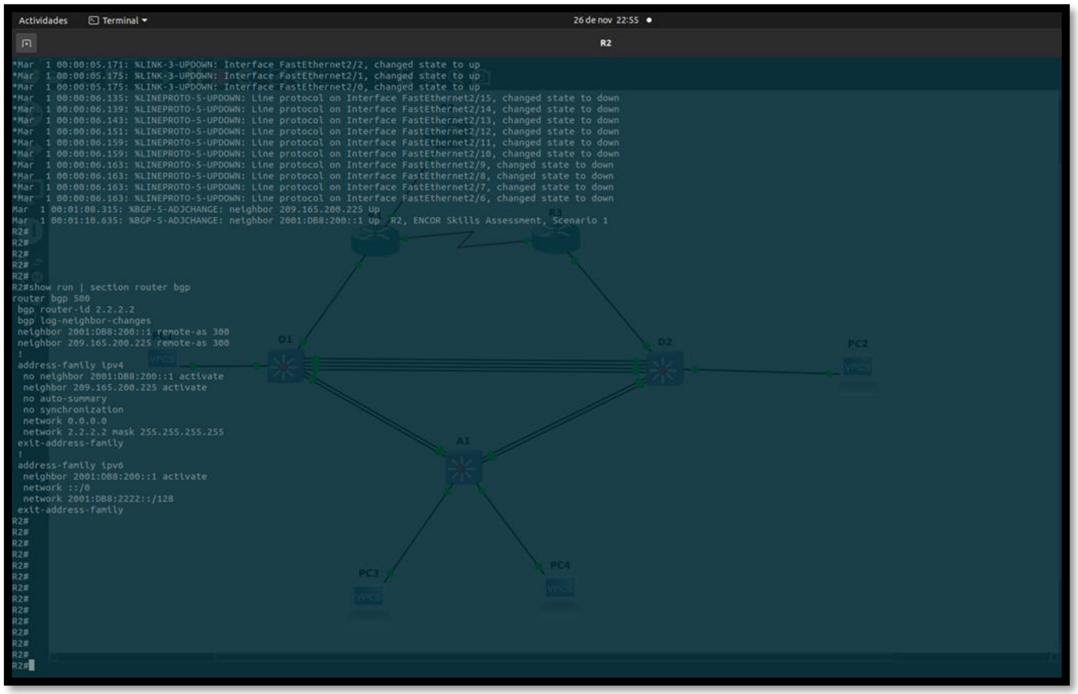
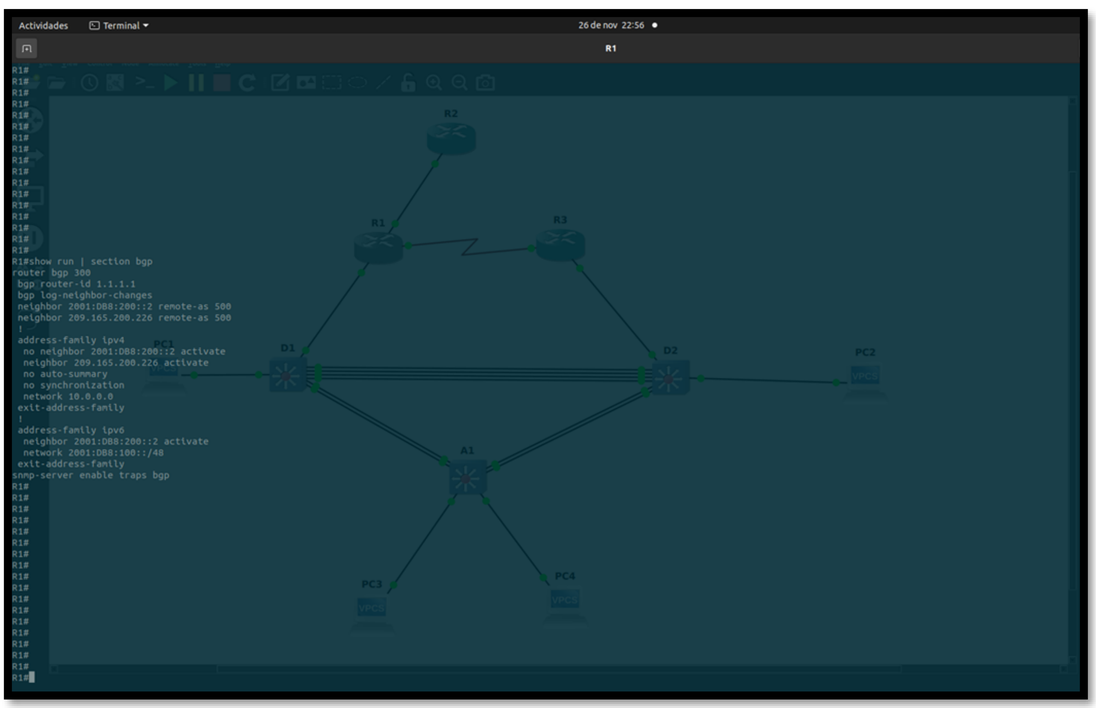


Figura 13 verificación MP-BGP



Parte 4: Configurar la redundancia del primer salto (first hop redundancy)

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

4. Las tareas de configuración son las siguientes:

Tabla 4. Tarea de configuración parte 4

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	Cree dos IP SLAs. • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	Cree IP SLAs. • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.

4.4	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

Switch D1

4.1. Inicialmente se utiliza la IP SLA para monitoreo continuo del tráfico de la red y se configura para que cada 5 segundos pruebe la interfaz en R3, tanto para la IPV4 como para la IPV6.

```
Enable
Config t
ip sla 4                                  //configuración Sla
icmp-echo 10.0.10.1                       //interfaz a verificar
frequency 5                               //Configuración de frecuencia
exit
ip sla 6
icmp-echo 2001:db8:100:1010::1
frequency 5
exit
```

Programación de la SLA para implementación inmediata sin tiempo de finalización

```
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life-forever start-time now
```

Los objetos retrasados notifican a D1 el estado de la IP SLA cambiando de bajo a alto después de 10 segundos o de alto a bajo en 15 segundos.

```
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
```

4.2 configuración de IP Slas para comprobar accebilidad con la interfaz en R3

Switch D2

```
Enable
Config t
ip sla 4                                    //configuración Sla
icmp-echo 10.0.11.1                         //interfaz a probar
frequency                                   //frecuencia
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
```

4.3 Configuración D1 como router primario para las VLAN 100 y 102 cambiando su prioridad a 150

```
interface vlan 100                          //configuración interfaz
standby version 2                           //habilitación HSRPv2
standby 104 ip 10.0.100.254                 //asignación IP
standby 104 priority 150                    //prioridad del grupo
standby 104 preempt                         //habilitación de preferencia
standby 104 track 4 decrement 60            //decremento y rastreo
```

```
standby 106 ipv6 autoconfig          //Asignación IPV6 para el respectivo grupo
standby 106 priority 150             //prioridad del grupo
standby 106 preempt                  //Habilitación de preferencias

standby 106 track 6 decrement 60     //rastreo y decremento
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
end
```

4.4. La configuración que se realiza en el switch 2 es prácticamente la misma del switch anterior

Switch D2

```
Enable
Config t
ip sla 4
icmp-echo 10.0.11.1
frequency
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 preempt
```

standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.0.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
end

4.5. Verificación de conectividad punto 4

Figura 14 verificación IP SLAs R1

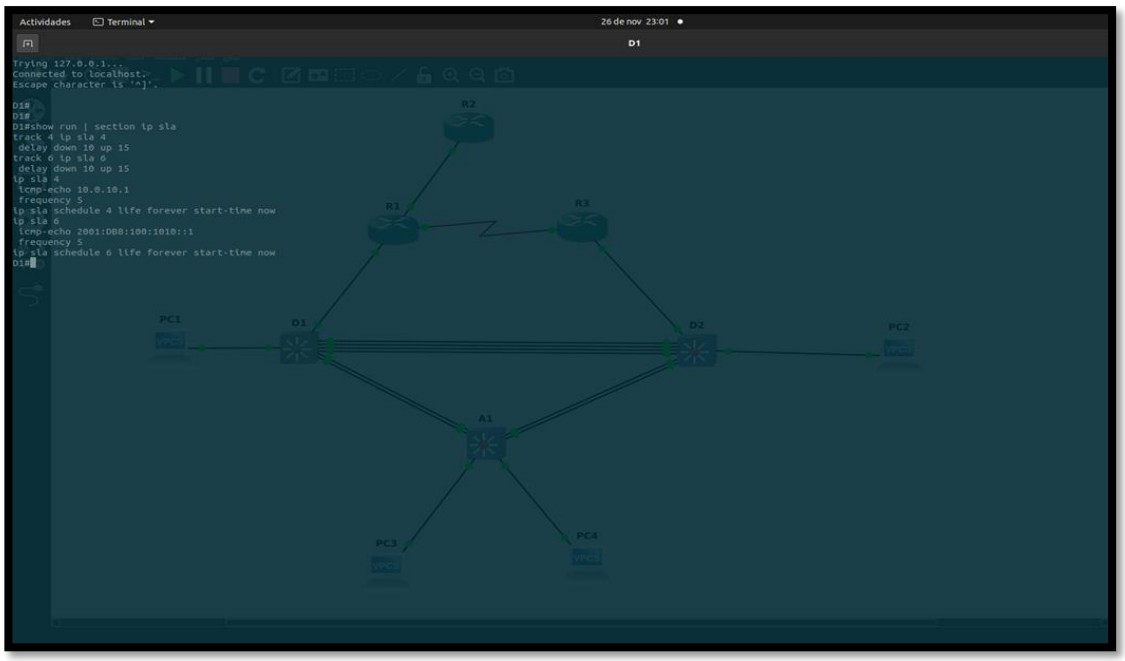


Figura 15 verificación IP SLAs R3

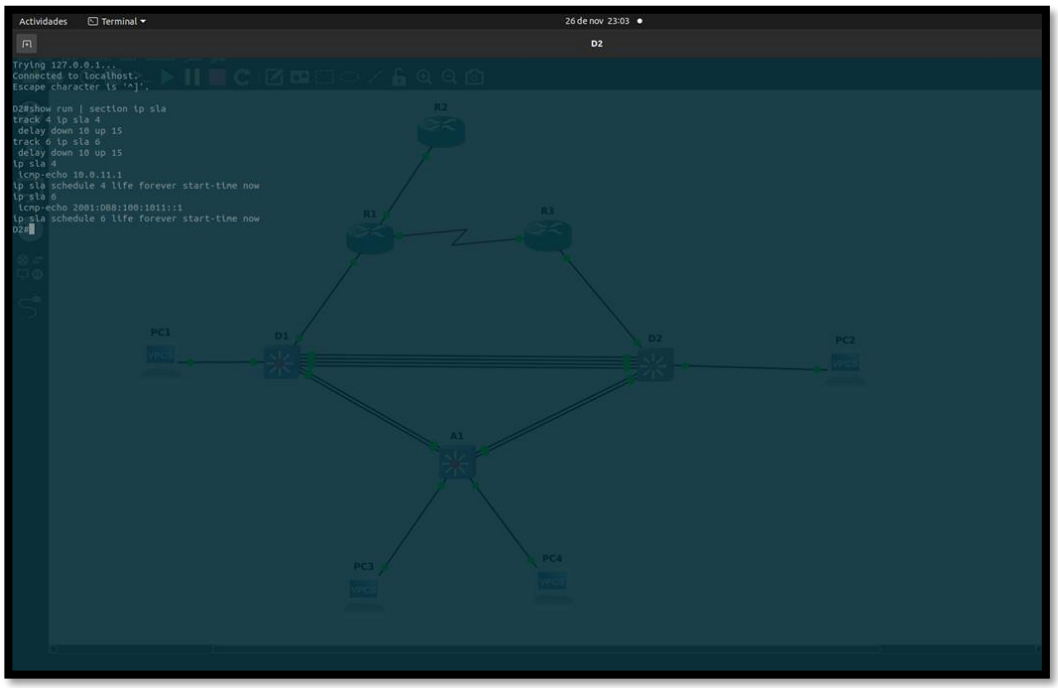
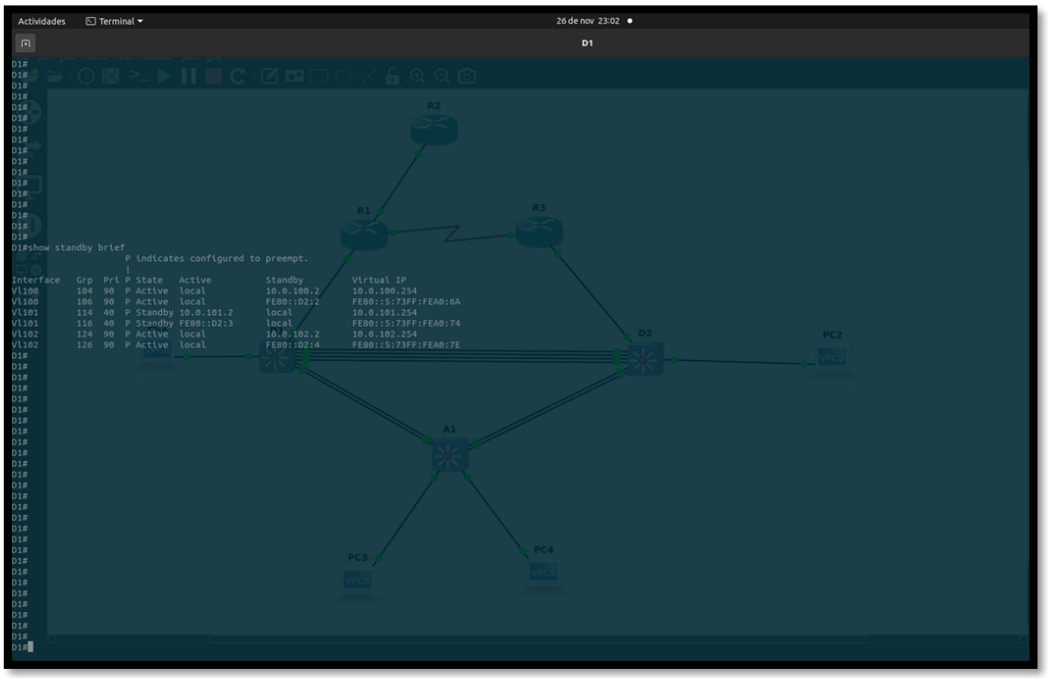


Figura 16 verificación HSRPv2



Parte 5: seguridad

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

5. Las tareas de configuración son las siguientes:

Tabla 5. Tarea de configuración parte 5

Tarea#	Tarea	Especificaciones
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son
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

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**.

La seguridad de cada uno de los dispositivos es considerado lo más importante que debe tener una topología como esta que se esta trabajando, debido a que hay personas mal intencionadas que intentan extraer información delicada para sobornos u otras codas, (modalidades que se ven de hoy en día), es por ellos que las contraseñas ayudan a evitar que personal no autorizado pueda acceder a esta información y solo tenga acceso a lo esencial.

Para la configurar las contraseñas de los dispositivos utilizados se procede a:

Configuración general para todos los dispositivos

5.1. Se protege el EXEC privilegiado usando: encripción SCRYPT y se le asigna la contraseña cisco12345cisco

Router 1, Router 2, Router 3, Switch D1, Switch D2, Switch A1

```
Enable
config t
anable algorithm-type
SCRYPT secret cisco12345cisco
```

5.2. Se crea un usuario local y se protege usando el algoritmo de encripción SCRYPT con nivel de privilegio 15

Router 1, Router 2, Router 3, Switch D1, Switch D2, Switch A1

```
Enable
Config t
username sadmin privilege 15 algorithm-type
SCRYPT secret cisco12345cisco
```

5.3. En todos los dispositivos excluyendo R2 se habilita AAA para cumplir con los protocolos de autenticación autorización y contabilización

Router 1, Router 3, Switch D1, Switch D2, Switch A1

enable
config t
aaa new-model

5.4. En todos los dispositivos excluyendo R2 se configuran las especificaciones del servidor Radius para autenticación y autorización para aplicaciones de acceso a la red

Router 1, Router 3, Switch D1, Switch D2, Switch A1

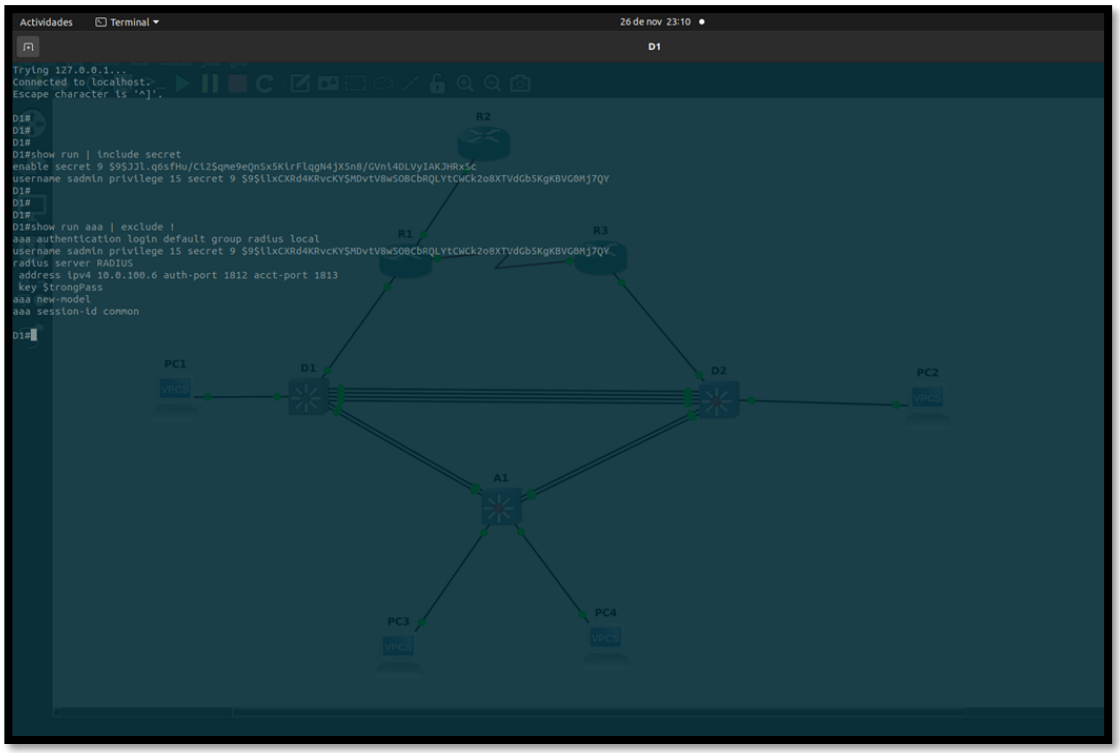
enable
config t
radius server RADIUS

5.5. Configuración de las especificaciones del servidor RADIUS

enable
config t
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
key $trongPass
exit

5.6. Verificación de conectividad punto 5

Figura 17 verificación de seguridad



Parte 6: Configurar las funciones de administración de red

En esta parte, debe configurar varias funciones de administración de red. Las 6. tareas de configuración son las siguientes:

Tabla 6. Tarea de configuración parte 6

Tarea#	Tarea	Especificaciones
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. En R3, D1, y D2, habilite el envío de *traps config* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

6.1 Se configura el reloj a la hora actual UTC

Router R1, R2, R3, D1, D2, A1

Enable
Config t
Clock timezone utc - 5

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

Router R2

```
Config t
ntp master 3
end
```

6.3 Se configura NTP según especificaciones de la tabla para sincronizar los relojes, se configuran las SNMPv2c para mejorar rendimiento

Router R1

```
Config t
ntp server 2.2.2.2
```

Router R3

```
Config t
ntp server 10.0.10.1
```

Switch D1

```
Config t
ntp server 10.0.10.1
```

Switch D2

```
Config t
ntp server 10.0.10.1
```

Switch

```
Config t
ntp server 10.0.10.1
```

6.4 Se configuran los Syslog en todos los dispositivos

Router R1 y R2

```
Enable
Config t
logging trap warning          //configuración Syslog peligroso
logging host 10.0.100.5       //configuración del envío
logging on                    //habilitación del Syslog
```

Switch D1, D2 y A1

```
Enable
Config t
logging trap warning
logging host 10.0.100.5
logging on
```

6.5 Configuración SNMPv2 en todos los dispositivos

Router R1

```
Enable
Config t
ip access-list standard SNMP-NMS                    //lista de acceso estandar
permit host 10.0.100.5                              //configuración SNMP al PC1
exit
snmp-server contact Cisco Student
snmp-server community ENCORSA ro SNMP-NMS           //configuración solo lectura
snmp-server host 10.0.100.5 version 2c ENCORSA      //configuración de envío
snmp-server ifindex persist                         //habilitación persistencia de index
snmp-server enable traps bgp                        //habilitación de envíos BPG
snmp-server enable traps config                     //habilitación de envío config
snmp-server enable traps ospf                       //habilitación de envío OSPF
end
```

Router 3

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

Switch D1

```
Enable
Config t
ip access-list standard SNMP-NMS
permit host 10.0.100.5
exit
```

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

Switch D2

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

Switch A1

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

6.6 Verificación de conectividad punto 6

Figura 18. Verificación UTC actual y NTP R2

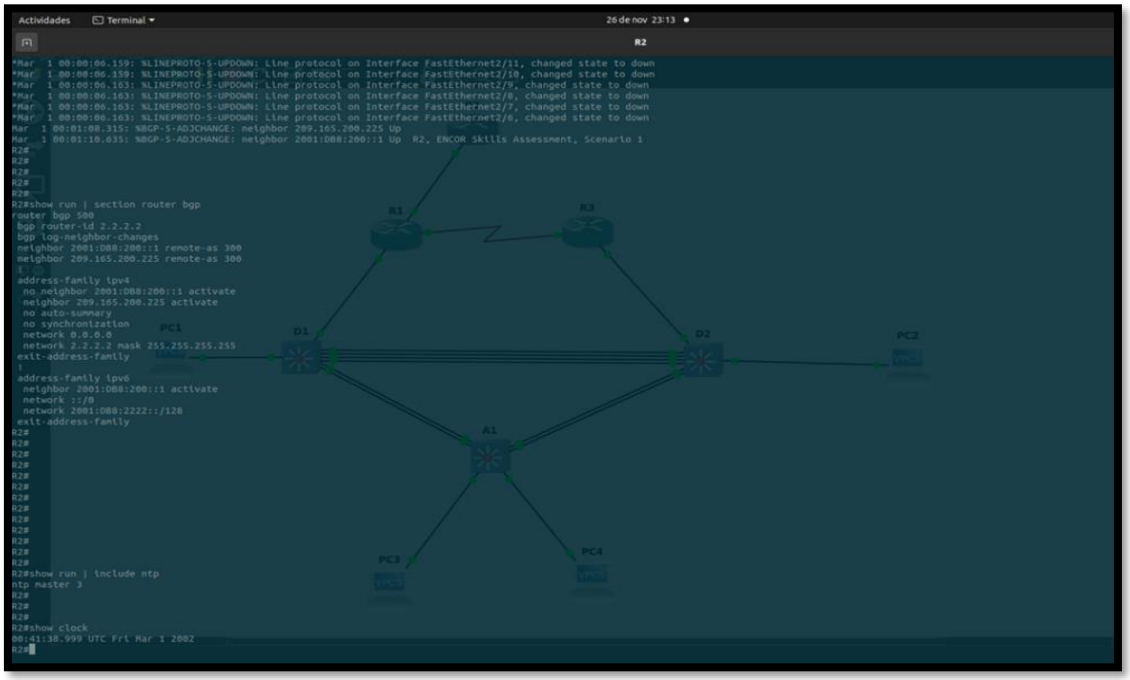


Figura 19 UTC actual y NTP R1,R3,D1,D2,A1

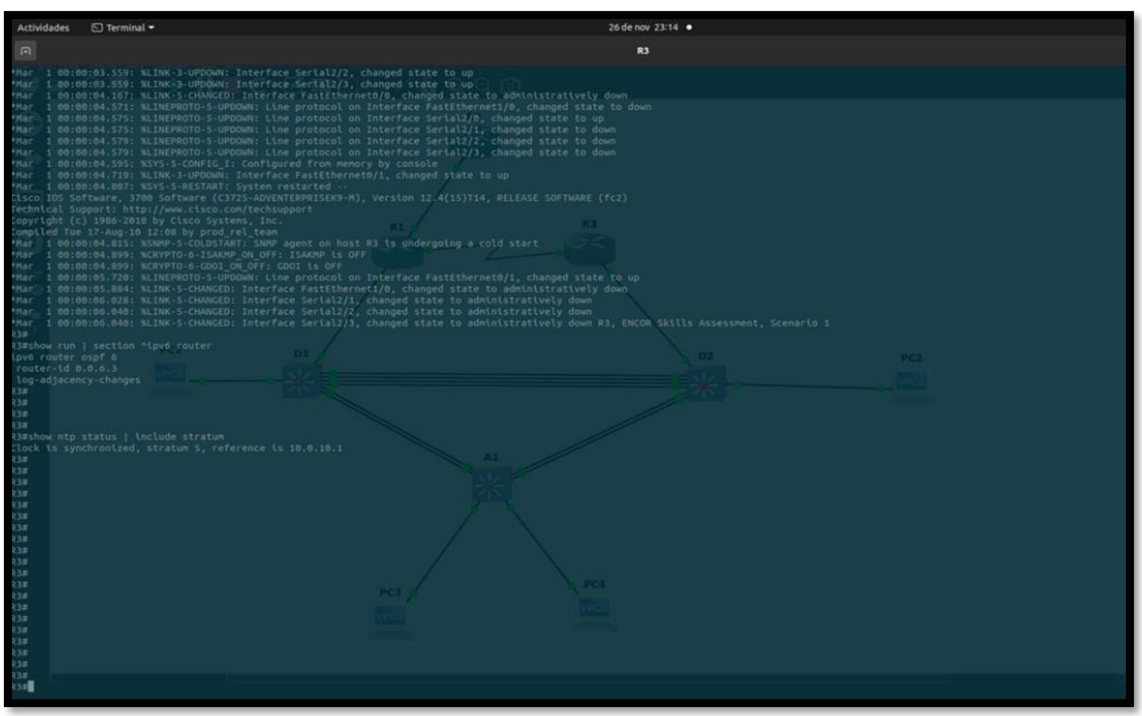


Figura 20 Verificación Syslog

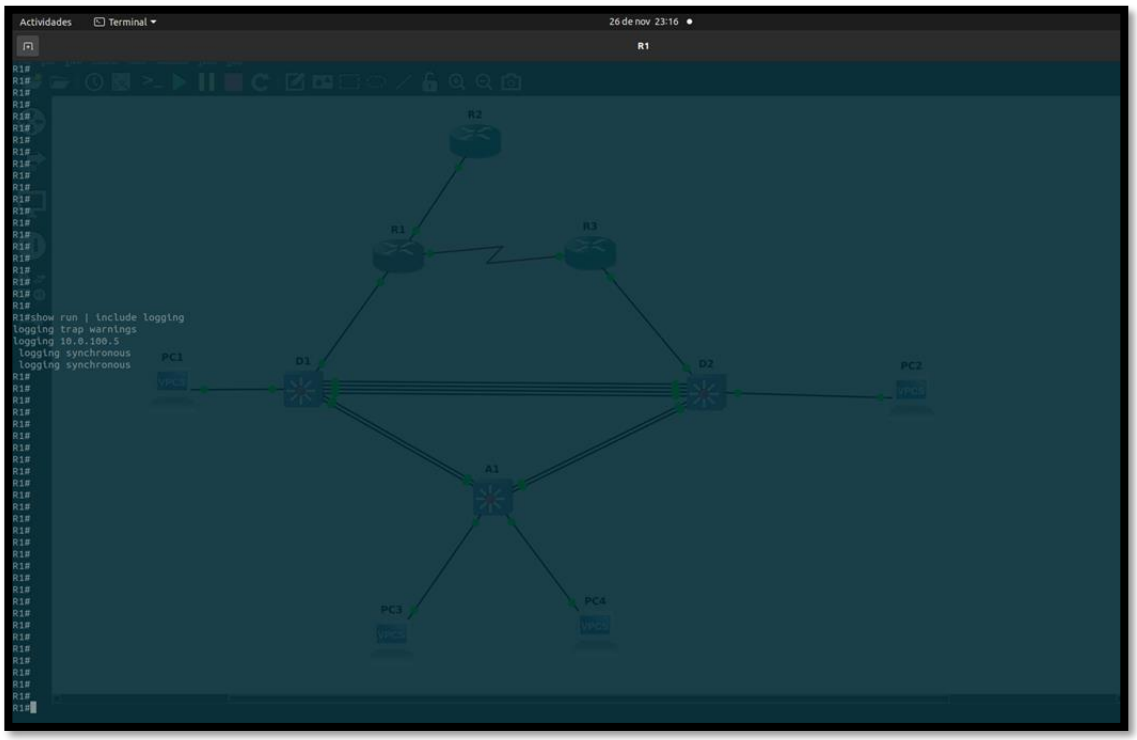
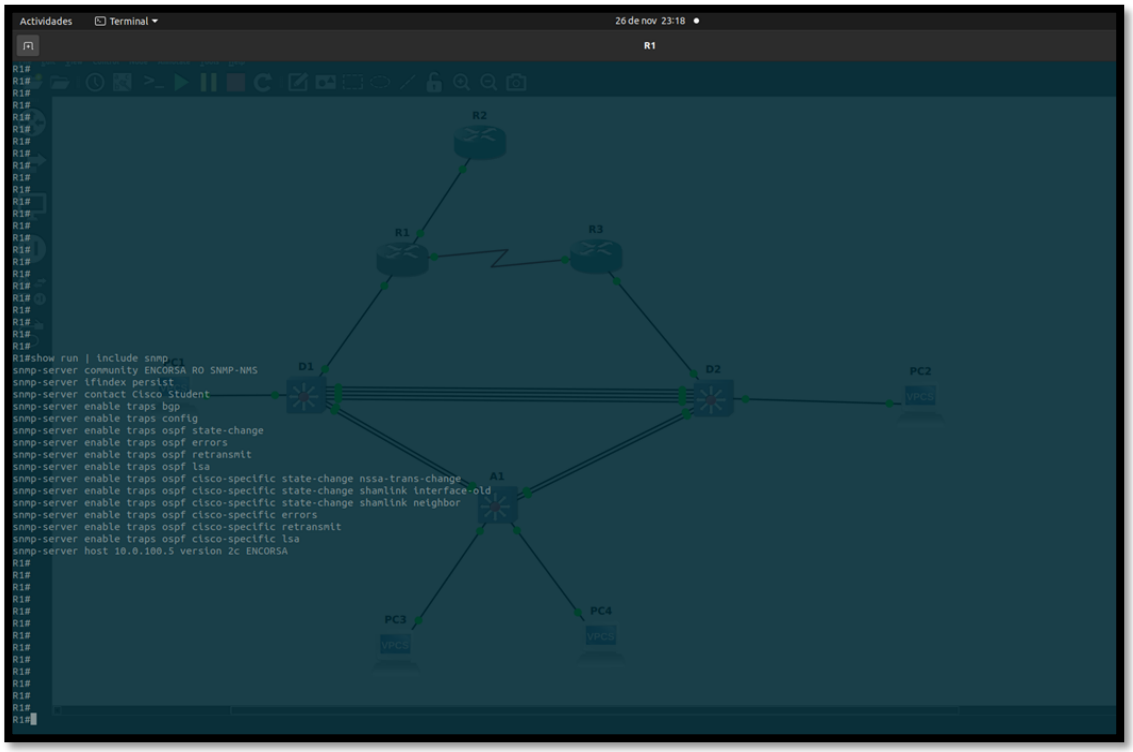


Figura 21 verificación SNMPv2



CONCLUSIONES

Por medio del simulador grafico de red GNS3 se desarrolla una topología de red, se configuran todos los dispositivos y direccionamiento de las interfases tanto de los Router como los Switch, se configuran la capa de red y el soporte de los PC ingresados a la topología con el fin de administrar la red de la compañía y la correcta ejecución del proyecto.

La configuración de protocolos en los Router y los estados de enlace para IPV4 con el protocolo OSPFv2 (Open Shortest Path First), se definen los direccionamientos de la red IPV6 (OSPFv3) en las interfaces de interconexión, declarando los protocolos de la puerta de enlace marginal (BGP), para lograr la estructura de los protocolos de enrutamiento establecidos en ola topología propuesta.

Se establecen mecanismos de seguridad en los dispositivos de la topología, para protegerlos de personal no autorizado y evitar que puedan conectar físicamente un cable al dispositivo y obtenga acceso a este.

Al culminar la simulación de la actividad propuesta, se identifica que se puede optar en el ámbito laboral, profesional y personal, ofreciendo las herramientas para desarrollar diferentes actividades en los procesos que se requieran en el campo de ejecución real.

BIBLIOGRAFÍA

Cisco. Cómo funciona un router. *Cisco.* [En línea] https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html.

Gerometta, Oscar. Ruta estática condicionada por IP SLA. *Mis Libros de Networking.* [En línea] http://librosnetworking.blogspot.com/2014/11/ruta-estatica-condicionada-por-ip-sla.html.

Help, Fireware. Configurar un Servidor DHCP IPv4. [En línea] https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/networksetup/configure_dhcp_server_c.html.

Networks, JUNIPER. Descripción general de BGP. [En línea] https://www.juniper.net/documentation/mx/es/software/junos/bgp/topics/topic-map/bgp-overview.html.

Pulgarin, Camilo. Evolución de OSPF. [En línea] https://www.reuter.com.ar/CCNA/CCNA2/mod8_ccna2/.

.

Torres, Carlos Eduardo. Redes Telemáticas. *El switch: cómo funciona y sus principales características.* [En línea] https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/.