

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

VICTOR ALFONSO FRESNEDA HIGUERA

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

VICTOR ALFONSO FRESNEDA HIGUERA

Diplomado de opción de grado presentado para optar el título de INGENIERO
ELECTRONICO.

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 29 de noviembre de 2021

CONTENIDO

CONTENIDO.....	4
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO.....	8
RESUMEN	9
ABSTRACT	10
INTRODUCCION	11
DESARROLLO.....	12
Escenario propuesto.....	12
Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces	13
Parte 2: Configurar la capa 2 de la red y el soporte de Host	23
Parte 3: Configurar los protocolos de enrutamiento.....	33
Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy).....	41
Parte 5: Seguridad.....	48
Parte 6: Configure las funciones de Administración de Red.....	51
CONCLUSIONES	57
BIBLIOGRAFÍA	58

LISTA DE TABLAS

FIGURA 1. ESCENARIO PROPUESTO.....	12
TABLA 1. ENRUTAMIENTO ESCENARIO PROPUESTO.....	13
TABLA 2. TAREAS DE CONFIGURACIÓN PARTE 2.	23
TABLA 3. TAREAS DE CONFIGURACIÓN PARTE 3.	33
TABLA 4. TAREAS DE CONFIGURACIÓN PARTE 4.	41
TABLA 5. TAREAS DE CONFIGURACIÓN PARTE 5.	48
TABLA 6. TAREAS DE CONFIGURACIÓN PARTE 6.	51

LISTA DE FIGURAS

FIGURA 2. SIMULACIÓN DE ESCENARIO PROPUESTO.....	14
FIGURA 3. CONFIGURACIÓN DIRECCIONAMIENTO PC1.....	22
FIGURA 4. CONFIGURACIÓN DIRECCIONAMIENTO PC4.....	22
FIGURA 5. VERIFICACIÓN TAREA 2.1, 2.2, Y 2.5 EN SWITCH D1.	27
FIGURA 6. VERIFICACIÓN TAREA 2.3 Y 2.4 EN SWITCH D1.	28
FIGURA 7. VERIFICACIÓN TAREA 2.6 EN SWITCH D1.....	28
FIGURA 8. VERIFICACIÓN TAREA 2.5 EN SWITCH D2.....	29
FIGURA 9. VERIFICACIÓN TAREA 2.3 Y 2.4 EN SWITCH D2.	29
FIGURA 10. VERIFICACIÓN TAREA 2.6 EN SWITCH D2.....	30
FIGURA 11. VERIFICACIÓN TAREA 2.6 EN SWITCH A1.....	30
FIGURA 12. VERIFICACIÓN TAREA 2.8 CONECTIVIDAD DE LA LAN LOCAL PC1.....	31
FIGURA 13. VERIFICACIÓN TAREA 2.8 CONECTIVIDAD DE LA LAN LOCAL PC2.....	31
FIGURA 14. VERIFICACIÓN TAREA 2.8 CONECTIVIDAD DE LA LAN LOCAL PC3.....	32
FIGURA 15. VERIFICACIÓN TAREA 2.8 CONECTIVIDAD DE LA LAN LOCAL PC4.....	32
FIGURA 16. VERIFICACIÓN TAREA 3.1 EN R1 Y R3.	38
FIGURA 17. VERIFICACIÓN TAREA 3.1 EN D1 Y D2.	39
FIGURA 18. VERIFICACIÓN TAREA 3.2.....	39
FIGURA 19. VERIFICACIÓN TAREA 3.3.....	40
FIGURA 20. VERIFICACIÓN TAREA 3.4.....	40
FIGURA 21. VERIFICACIÓN TAREA 4.1 Y 4.3 EN SWITCH D1.	46
FIGURA 22. VERIFICACIÓN TAREA 4.3 EN SWITCH D1.....	47
FIGURA 23. VERIFICACIÓN TAREA 4.2 Y 4.3 EN SWITCH D2.	47
FIGURA 24. VERIFICACIÓN TAREA 5.1 Y 5.2.....	49
FIGURA 25. VERIFICACIÓN TAREA 5.3, 5.4 , 5.5 Y 5.6.....	50
FIGURA 26. VERIFICACIÓN TAREA 6.1 Y 6.2.....	55

FIGURA 27. VERIFICACIÓN TAREA 6.3..... 55

FIGURA 28. VERIFICACIÓN TAREA 6.4..... 56

FIGURA 29. VERIFICACIÓN TAREA 6.5..... 56

GLOSARIO

IPV6: se trata de la sexta versión del protocolo de enrutamiento que hace posible conectar los dispositivos en Internet, permitiendo que se identifiquen con una dirección unívoca.

VLAN: conocidas como redes de área local virtuales, se trata de una tecnología de redes que permite crear dentro de la misma red física, redes lógicas independientes.

ROUTER: se trata de un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función principal es guiar y dirigir los datos de la red mediante paquetes que contienen varios tipos de datos.

PROTOCOLO DE ENRUTAMIENTO: son un conjunto de reglas utilizadas por un router cuando se comunica con otros dispositivos para compartir información. Esta información es utilizada para mantener las tablas de enrutamiento.

SWITCH: es un dispositivo de interconexión utilizado para conectar equipos en red, formando redes en área local, y sus especificaciones técnicas siguen el estándar IEEE 802.3.

IP: es un código numérico utilizado para identificar equipos o dispositivos en una red. Estos dispositivos pueden ser: un PC, Tablet, router, un servidor web, un modem, etc.

RESUMEN

El presente informe consiste en desarrollar la prueba de habilidades del diplomado de profundización CCNP de cisco, para la carrera de ingeniería electrónica.

Esta prueba de habilidades está dividida en seis tareas, en la primera tarea se construye la red en el simulador GNS3 y se configuran los parámetros básicos de los dispositivos y el direccionamiento de las interfaces, en la segunda tarea se configura la capa 2 de la red y se genera el soporte de host, en su tercera parte se configuran los protocolos de enrutamiento IPv4 e IPv6 en todos los dispositivos, después de realizar estas configuraciones se procede a configurar la redundancia, que consiste en establecer el HSRP versión 2, para la quinta parte se realiza la configuración correspondiente de varios mecanismos de seguridad en todos los dispositivos de la red, y la configuración final se establecen las funciones de administrador de red, de esta manera se da cumplimiento a la configuración general de la topología, realizando una explicación detallada de cada uno de los comandos utilizados en las diferentes tareas.

ABSTRACT

This report consists of developing the skills test for the Cisco CCNP deepening diploma for the degree in electronic engineering.

This skills test is divided into six tasks, in the first task the network is built in the GNS3 simulator and the basic parameters of the devices and the addressing of the interfaces are configured, in the second task the layer 2 of the network is configured and the host support is generated, in its third part the IPv4 and IPv6 routing protocols are configured in all the devices, after making these configurations the redundancy is configured, which consists of establishing HSRP version 2, for the fifth In part, the corresponding configuration of various security mechanisms is carried out in all network devices, in the final configuration the network administrator functions are established, in this way the general configuration of the topology is fulfilled, making a detailed explanation of each of the commands used in the different tasks.

INTRODUCCION

Como bien sabemos, el avance de la tecnología en cuanto a redes de datos, equipos de cómputo y diferentes recursos que aportan al desarrollo de proyectos de calidad, y en este sentido, durante el presente proyecto se desarrollan pruebas de habilidades completando las configuraciones necesarias para obtener la accesibilidad requerida logrando la efectividad y ejecución en el escenario adecuado.

Para iniciar la construcción y cumplimiento del proyecto se realizan ajustes básicos de cada dispositivo con las respectivas interfaces y sus direccionamientos, se efectuará la configuración de la capa 2 de la red y el soporte de Host, los protocolos de enrutamiento, la seguridad y las características de administración de red.

En el presente proyecto se efectúa el acercamiento de la elaboración de simulaciones que se pueden enfrentar en un contexto real y que aportan a la formación de los futuros ingenieros en la configuración de equipos físicos y redes empresariales.

Tabla 1. Enrutamiento escenario propuesto.

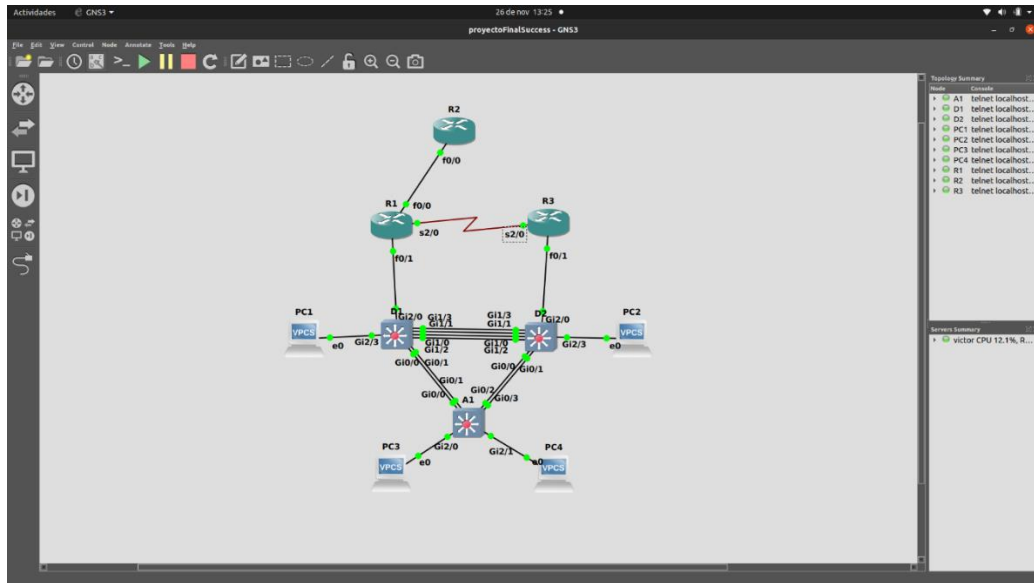
Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	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

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 2. Simulación de escenario propuesto.



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Router R1

```

Router>en /se ingresa a modo privilegiado
Router#conf term /se ingresa a modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1 /se nombra router R1
R1(config)#ipv6 unicast-routing /Tipo de dirección ipv6
unidifusión
R1(config)#no ip domain lookup /evitar retrasos al entrar un comando mal
escrito
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 # /mensaje
del día
R1(config)#line con 0 /se ingresa a modo configuración línea
R1(config-line)#exec-timeout 0 0 /se retira el límite de tiempo
R1(config-line)#logging synchronous /depurar mensajes no solicitados consola
R1(config-line)#exit /salir del modo configurar
línea
R1(config)#interface f0/0 /configurar interfaces
R1(config-if)# ip address 209.165.200.225 255.255.255.224 /asigna ip address
    
```

```
R1(config-if)# ipv6 address fe80::1:1 link-local /asigna ipv6 address
R1(config-if)# ipv6 address 2001:db8:200::1/64
R1(config-if)# no shutdown / Reinicia una interfaz desactivada
```

Se replica el código para cada dispositivo según corresponda:

Router R2

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface f0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

Router R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface f0/1
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
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
```

Switch D1

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
exit
vlan 100
  name Management
exit
vlan 101
  name UserGroupA
exit
vlan 102
  name UserGroupB
exit
vlan 999
  name NATIVE
exit
interface Gi2/0
  no switchport
  ip address 10.0.10.2 255.255.255.0
  ipv6 address fe80::d1:1 link-local
  ipv6 address 2001:db8:100:1010::2/64
  no shutdown
  exit
interface vlan 100
  ip address 10.0.100.1 255.255.255.0
  ipv6 address fe80::d1:2 link-local
  ipv6 address 2001:db8:100:100::1/64
  no shutdown
  exit
interface vlan 101
  ip address 10.0.101.1 255.255.255.0
  ipv6 address fe80::d1:3 link-local
  ipv6 address 2001:db8:100:101::1/64
```

```
no shutdown
exit
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range Gi2/0-3, Gi1/0-3, f0/0-15
shutdown
exit
```

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
```

```

interface Gi2/0
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range Gi2/0-3, Gi1/0-3, f0/0-15
shutdown
exit

```

Switch D2

```

hostname D2
ip routing
ipv6 unicast-routing

```

```
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
  exec-timeout 0 0
  logging synchronous
  exit
vlan 100
  name Management
  exit
vlan 101
  name UserGroupA
  exit
vlan 102
  name UserGroupB
  exit
vlan 999
  name NATIVE
  exit
interface Gi2/0
  no switchport
  ip address 10.0.11.2 255.255.255.0
  ipv6 address fe80::d1:1 link-local
  ipv6 address 2001:db8:100:1011::2/64
  no shutdown
  exit
interface vlan 100
  ip address 10.0.100.2 255.255.255.0
  ipv6 address fe80::d2:2 link-local
  ipv6 address 2001:db8:100:100::2/64
  no shutdown
  exit
interface vlan 101
  ip address 10.0.101.2 255.255.255.0
  ipv6 address fe80::d2:3 link-local
  ipv6 address 2001:db8:100:101::2/64
  no shutdown
  exit
interface vlan 102
  ip address 10.0.102.2 255.255.255.0
  ipv6 address fe80::d2:4 link-local
  ipv6 address 2001:db8:100:102::2/64
  no shutdown
  exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
```

```
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
interface range Gi2/0-3, Gi1/0-3, f0/0-15
shutdown
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range Gi0/0-3
shutdown
exit
```

- b. Copie el archivo running-config al archivo startup-config en todos los dispositivos.
Se realiza la copia utilizando el código en cada dispositivo:

Se utiliza el comando copy running-config startup-config para mantener una copia de seguridad de la configuración actual en ausencia de alimentación.

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

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

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

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

```
D2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- c. 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.

Para este paso se debe ingresar a cada PC, en desktop, ip configuración, se asigna los valores de la tabla de enrutamiento como se muestra en la imagen:

Figura 3. Configuración direccionamiento PC1.

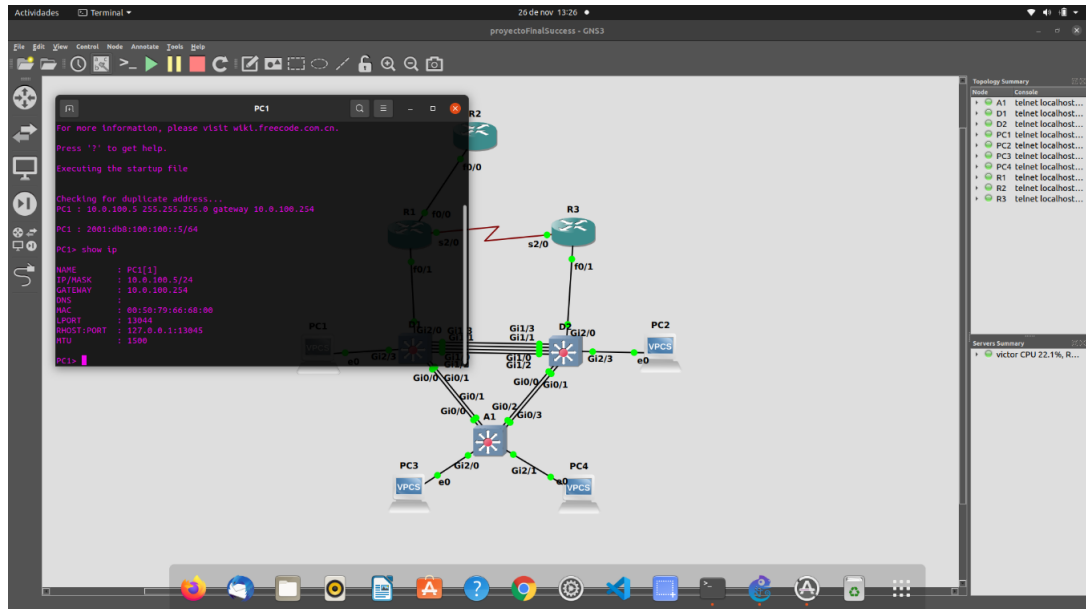
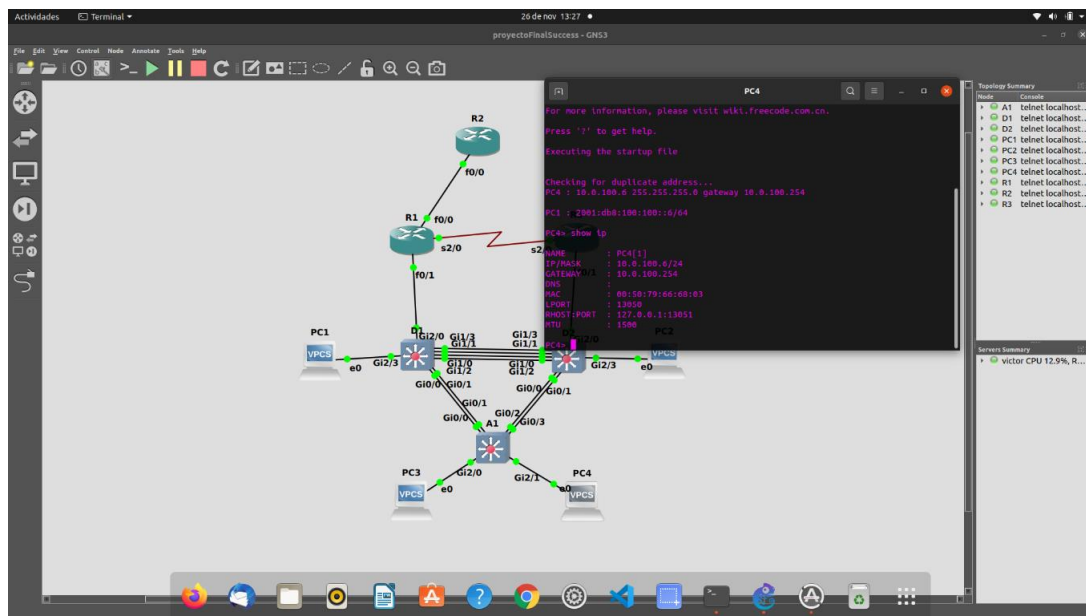


Figura 4. Configuración direccionamiento PC4.



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 debe poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

Tabla 2. Tareas 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: <ul style="list-style-type: none">• D1 and D2• D1 and A1• D2 and A1
2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: <ul style="list-style-type: none">• D1 a D2 – Port channel 12• D1 a A1 – Port channel 1• D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	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: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: <ul style="list-style-type: none"> • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5
-----	---	---

Solución

Configuración general de switch D1

Switch D1

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

```
interface range Gi1/0-3
switchport trunk encapsulation dot1q
switchport mode trunk
```

Se cambia la VLAN nativa en los enlaces troncales en el rango Gi1/0-3

```
switchport trunk native vlan 999
```

Se crea EtherChannels LACP en el rango Gi1/0-3

```
channel-group 12 mode active
no shutdown
exit
```

Se cambia la VLAN nativa en los enlaces troncales en el rango Gi0/0-1

```
interface range Gi0/0-1
switchport mode trunk
switchport trunk native vlan 999
```

Se crea EtherChannels LACP en el rango g1/0/5-6

```
channel-group 1 mode active
```

```
no shutdown
exit
```

Sé habilita el protocolo Rapid Spanning-Tree (RSTP)

```
spanning-tree mode rapid-pvst
spanning-tree vlan 100,102 root primary
spanning-tree vlan 101 root secondary
```

Se crea puerto de acceso para que solo se comuniquen con dispositivos que se encuentren en la misma VLAN en la interfaz Gi2/3

```
interface Gi2/3
switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end
```

Configuración general de switch D2

Switch D2

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

```
interface range Gi1/0-3
switchport mode trunk
```

Se cambia la VLAN nativa en los enlaces troncales en el rango Gi1/0-3

```
switchport trunk native vlan 999
```

Se crea EtherChannels LACP en el rango Gi1/0-3

```
channel-group 12 mode active
no shutdown
exit
```

Se cambia la VLAN nativa en los enlaces troncales en el rango Gi0/0-1

```
interface range Gi0/0-1
switchport mode trunk
switchport trunk native vlan 999
```

Se crea EtherChannels LACP en el rango Gi0/0-1

```
channel-group 2 mode active
no shutdown
exit
```

Sé habilita el modo Rapid Spanning-Tree (RSTP)

```
spanning-tree mode rapid-pvst
spanning-tree vlan 101 root primary
spanning-tree vlan 100,102 root secondary
```

Se crea puerto de acceso para que solo se comuniquen con dispositivos que se encuentren en la misma VLAN en la interfaz Gi2/3

```
interface Gi2/3
switchport mode access
switchport access vlan 102
spanning-tree portfast
no shutdown
exit
end
```

Configuración general de switch A1

Switch A1

Sé habilita el modo Rapid Spanning-Tree (RSTP)

```
spanning-tree mode rapid-pvst
```

Se cambia la VLAN nativa en los enlaces troncales en el rango Gi0/0-1

```
interface range Gi0/0-1
switchport mode trunk
switchport trunk native vlan 999
```

Se crea EtherChannels LACP en el rango Gi0/0-1

```
channel-group 1 mode active
no shutdown
exit
```

Se cambia la VLAN nativa en los enlaces troncales en el rango Gi0/2-3

```
interface range Gi0/2-3
```

```
switchport mode trunk
switchport trunk native vlan 999
```

Se crea EtherChannels LACP en el rango Gi0/2-3

```
channel-group 2 mode active
no shutdown
exit
```

Se crea puerto de acceso para que solo se comuniquen con dispositivos que se encuentren en la misma VLAN en la interface Gi0/2

```
interface Gi2/0
switchport mode access
switchport access vlan 101
spanning-tree portfast
no shutdown
exit
```

Se crea puerto de acceso para que solo se comuniquen con dispositivos que se encuentren en la misma VLAN en la interface Gi2/1

```
interface Gi2/1 switchport mode access
switchport access vlan 100
spanning-tree portfast
no shutdown
exit
end
```

Figura 5. Verificación tarea 2.1, 2.2, y 2.5 en Switch D1.

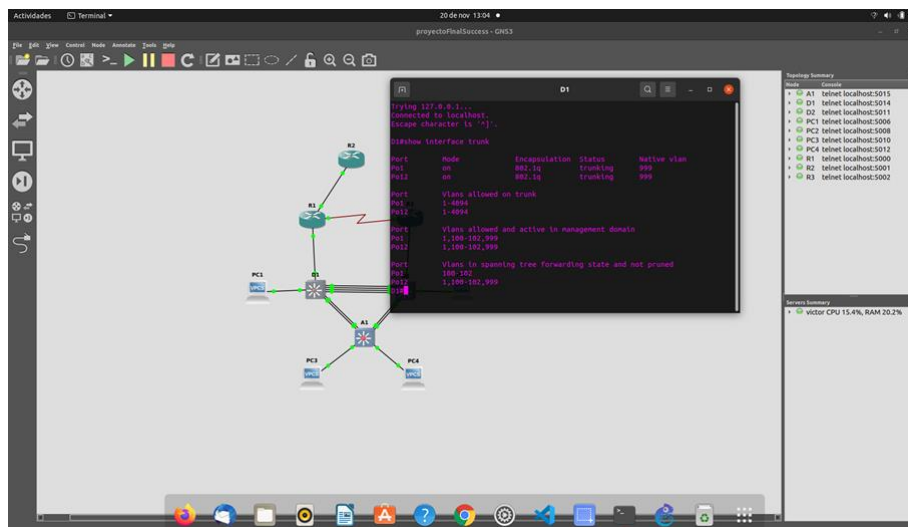


Figura 8. Verificación tarea 2.5 en Switch D2.

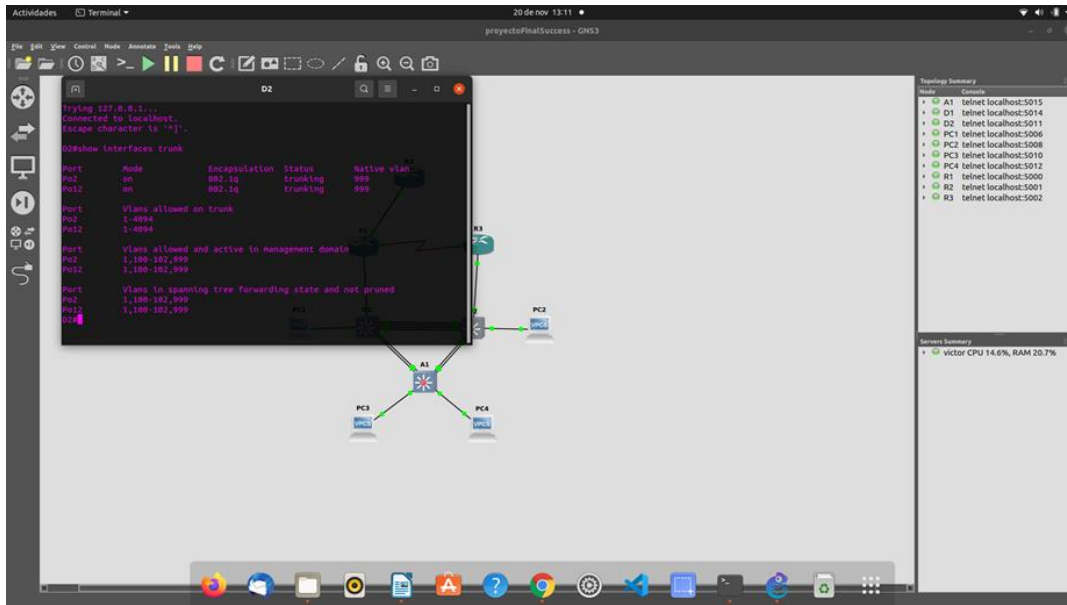


Figura 9. Verificación tarea 2.3 y 2.4 en Switch D2.

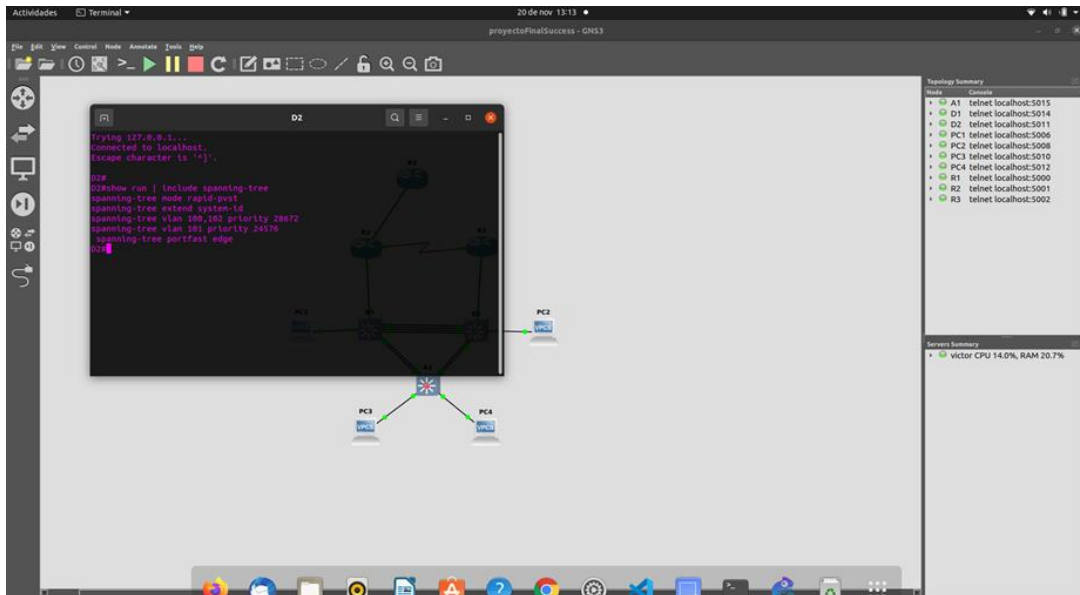


Figura 10. Verificación tarea 2.6 en Switch D2.

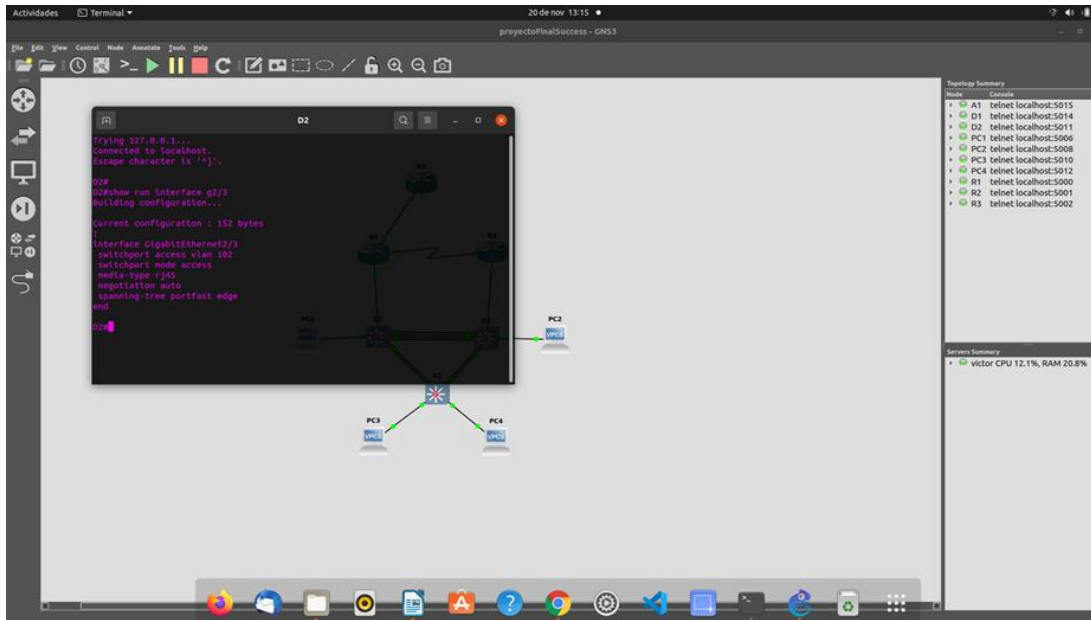


Figura 11. Verificación tarea 2.6 en Switch A1.

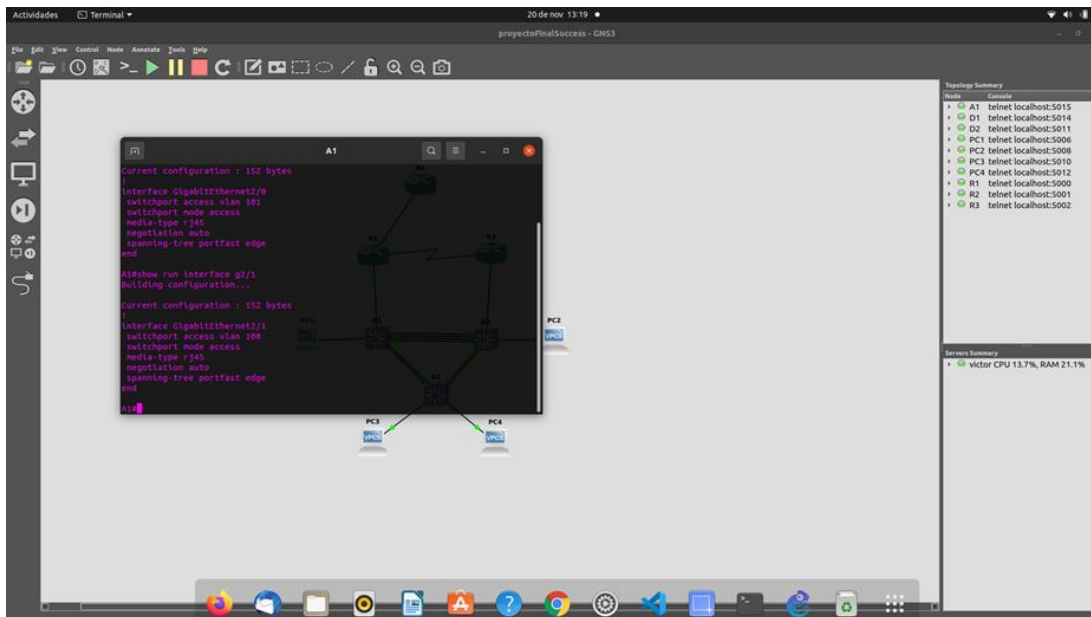


Figura 12. Verificación tarea 2.8 conectividad de la LAN local PC1

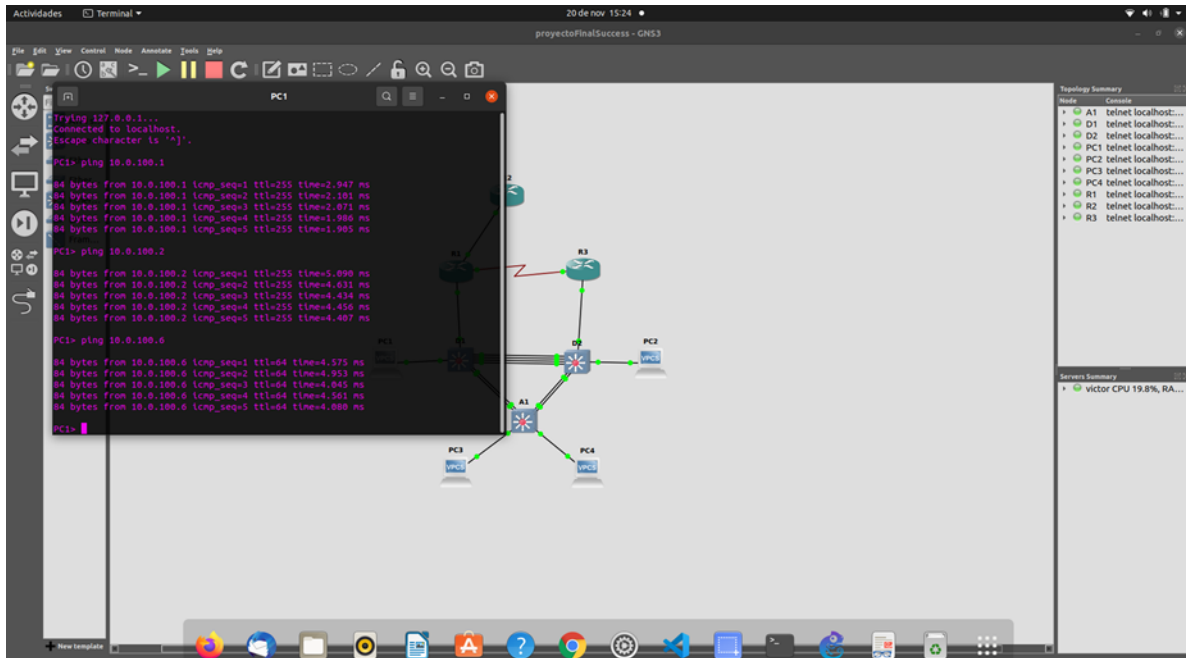


Figura 13. Verificación tarea 2.8 conectividad de la LAN local PC2

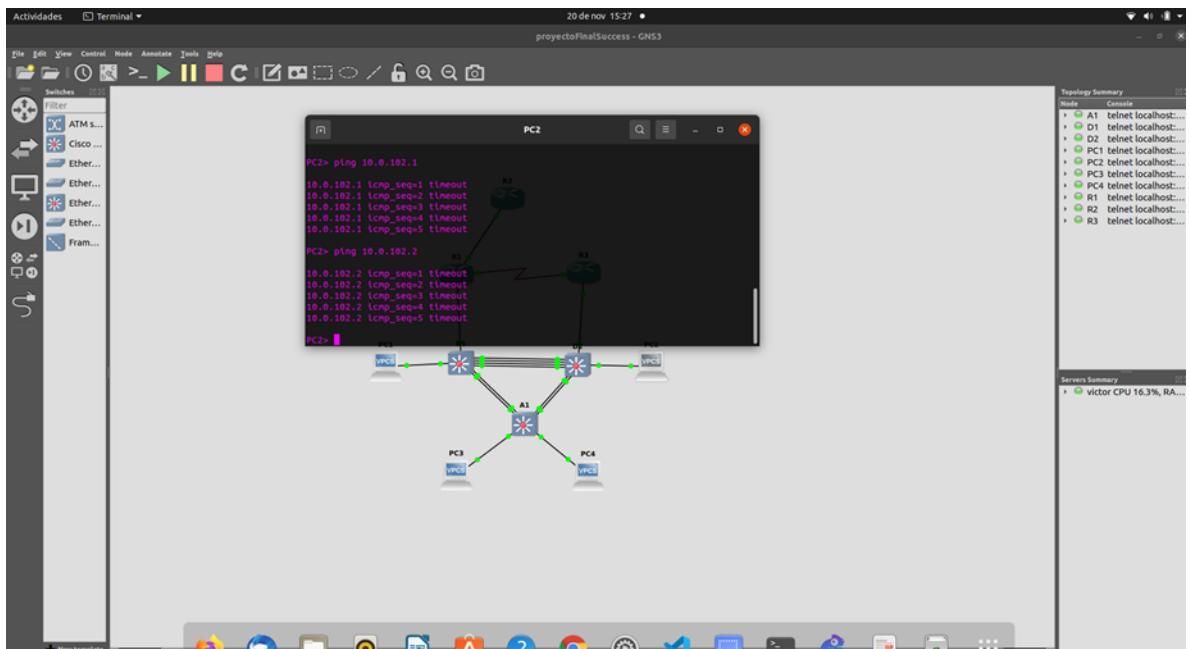


Figura 14. Verificación tarea 2.8 conectividad de la LAN local PC3

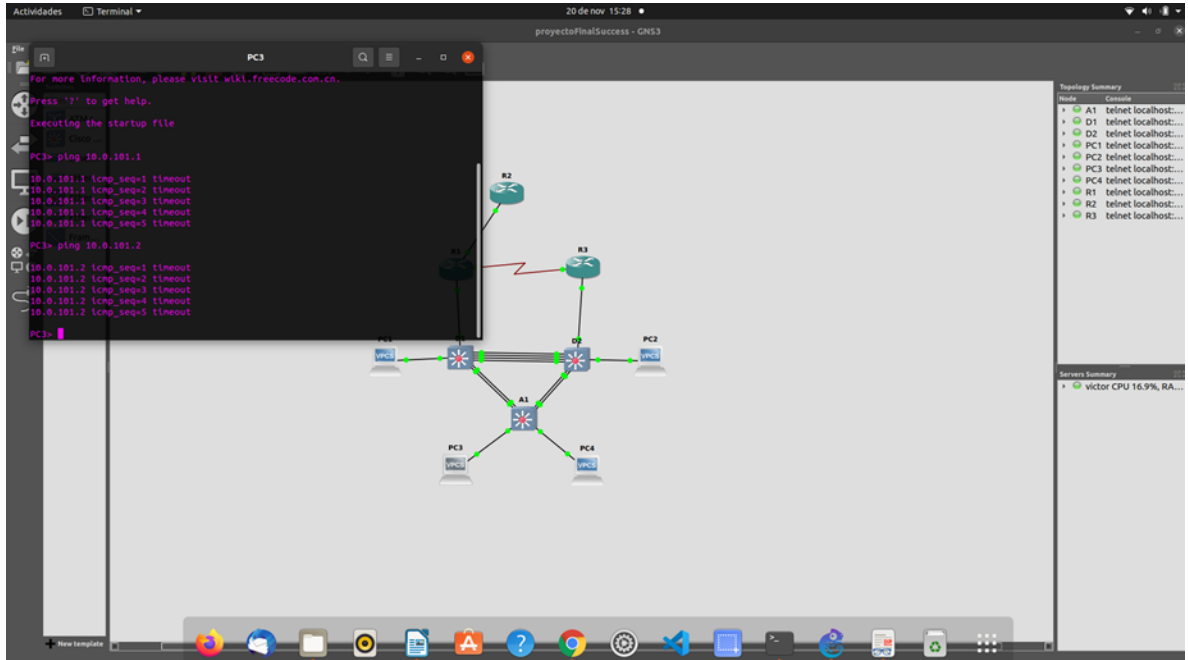
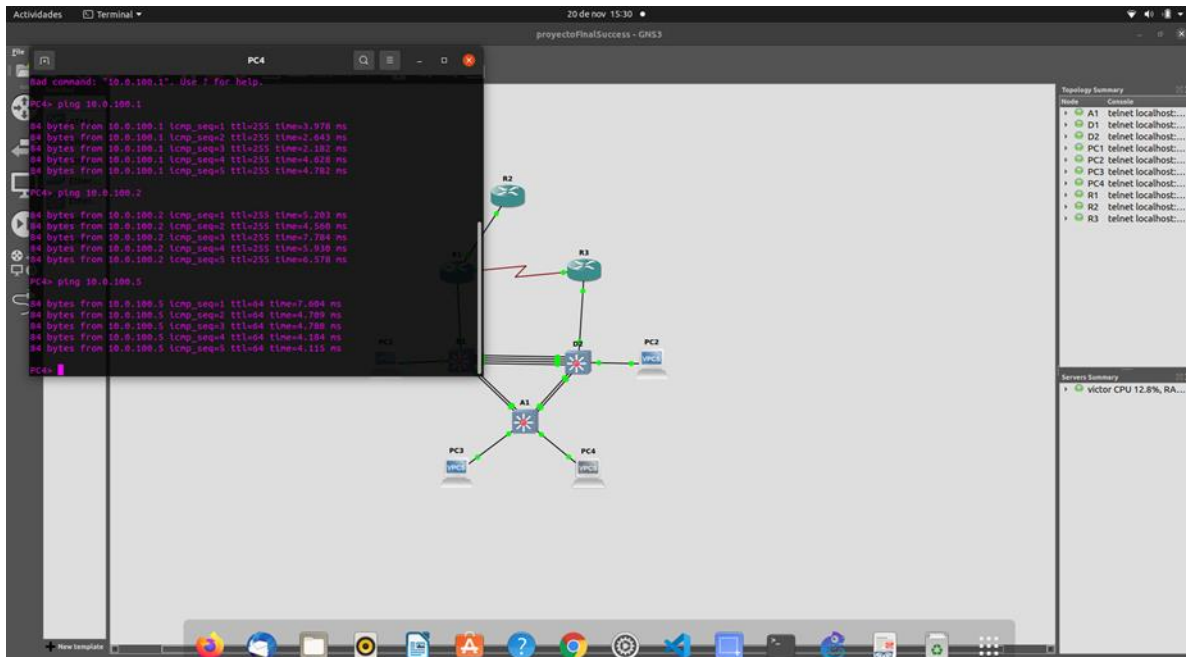


Figura 15. Verificación tarea 2.8 conectividad de la LAN local PC4



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:

Tabla 3. Tareas de configuración parte 3.

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.	Use OSPF Process ID 4 y asigne los siguientes router- IDs: <ul style="list-style-type: none">• R1: 0.0.4.1• R3: 0.0.4.3• D1: 0.0.4.131• D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• D1: todas las interfaces excepto G1/0/11• D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (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: <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En IPv4 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). <p>En IPv6 address family, anuncie:</p> <ul style="list-style-type: none"> • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas resumen estáticas a la interfaz Null 0:</p> <ul style="list-style-type: none"> • 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. <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En IPv4 address family:</p> <ul style="list-style-type: none"> • 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.

Solución

Configuración general de router R1

Router R1

Se configura single-area OSPFv2 en area 0

```
router ospf 4
router-id 0.0.4.1
```

```
network 10.0.10.0 0.0.0.255 area 0
network 10.0.13.0 0.0.0.255 area 0
default-information originate
exit
```

Se configura classic single-area OSPFv3 en area 0

```
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface f0/1
ipv6 ospf 6 area 0
exit
interface s2/0
ipv6 ospf 6 area 0
exit
```

Se configura MP-BGP en la red ISP

```
ip route 10.0.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.0.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family
```

Configuración general de router R2

Router R2

Se configura MP-BGP en la red ISP

```
ip route 0.0.0.0 0.0.0.0 loopback 0
ipv6 route ::/0 loopback 0
```

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

Configuración general de router R3

Router R3

Se configura single-area OSPFv2 en area 0

```
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
```

Se configura classic single-area OSPFv3 en area 0

```
ipv6 router ospf 6
  router-id 0.0.6.3
  exit
interface f0/1
  ipv6 ospf 6 area 0
  exit
interface s2/0
  ipv6 ospf 6 area 0
  exit
end
```

Configuración general de switch D1

Switch D1

Se configura single-area OSPFv2 en area 0

```
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 Gi2/0
exit
```

Se deshabilita las publicaciones OSPFv3 excepto en Gi2/0

```
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface Gi2/0
exit
interface Gi2/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end
```

Configuración general de switch D2

Switch D2

Se configura single-area OSPFv2 en area 0

```
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 Gi2/0
exit

```

Se deshabilita las publicaciones OSPFv3 excepto en Gi2/0

```

ipv6 router ospf 6
router-id 0.0.6.132
passive-interface default
no passive-interface Gi2/0
exit
interface Gi2/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
end

```

Figura 16. Verificación tarea 3.1 en R1 y R3.

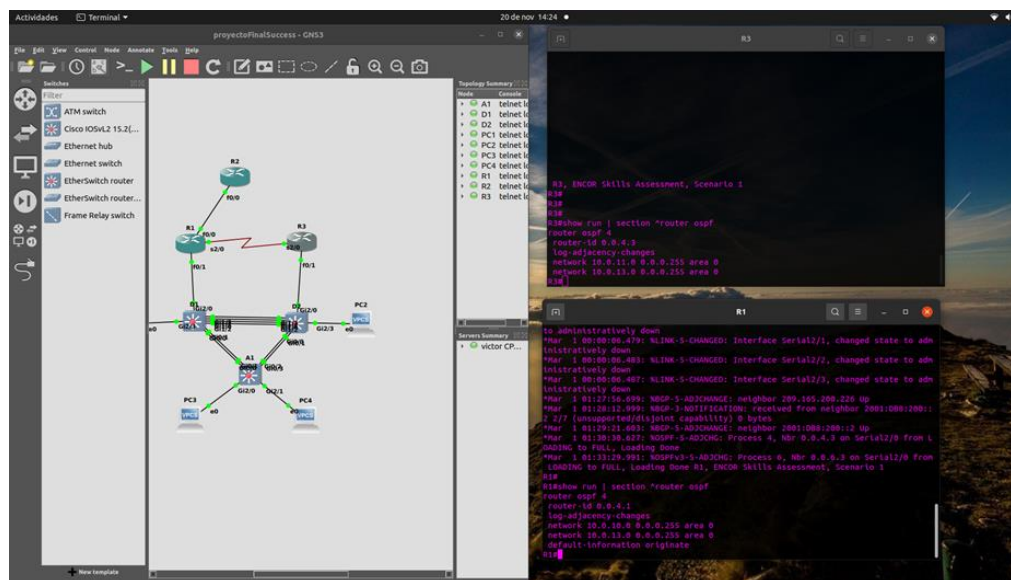


Figura 17. Verificación tarea 3.1 en D1 y D2.

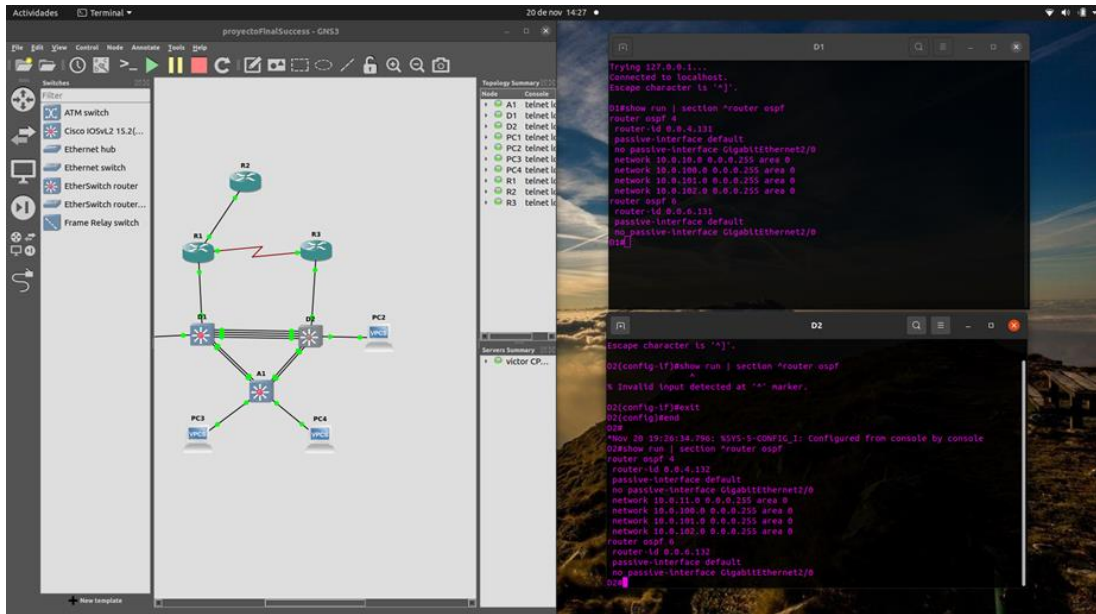


Figura 18. Verificación tarea 3.2

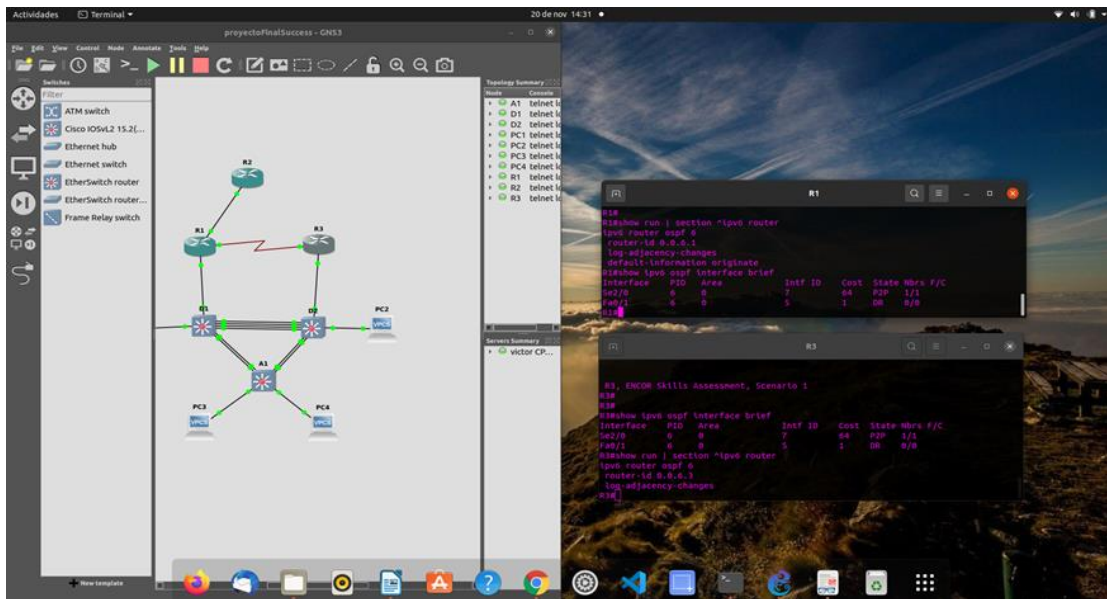


Figura 19. Verificación tarea 3.3

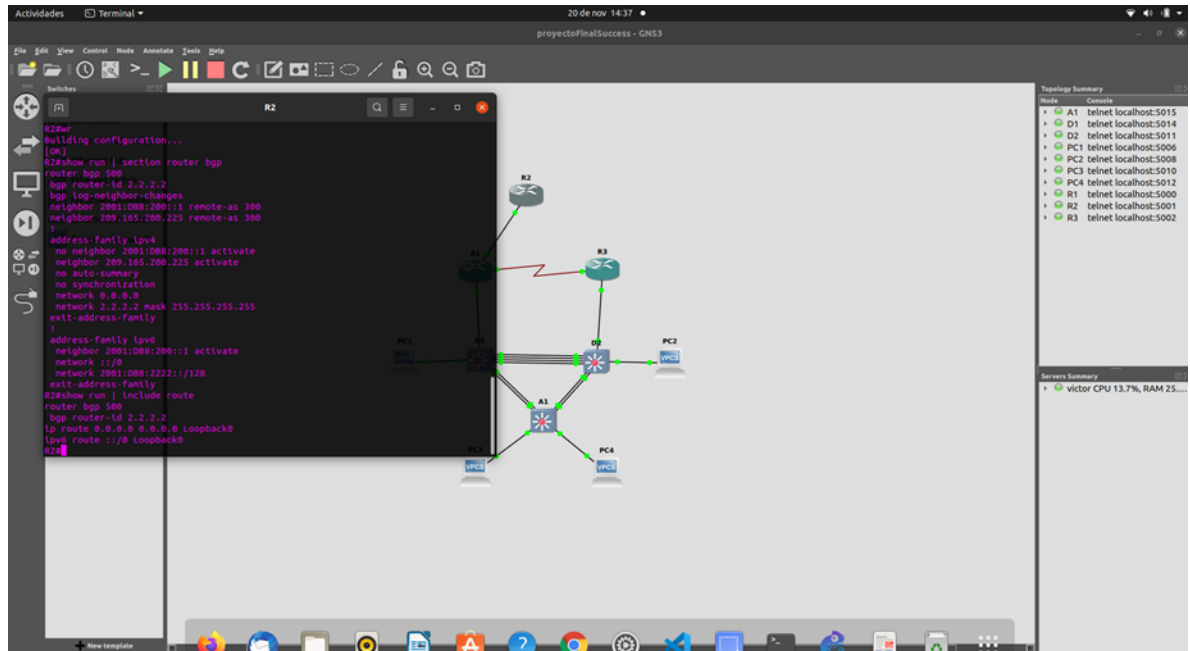
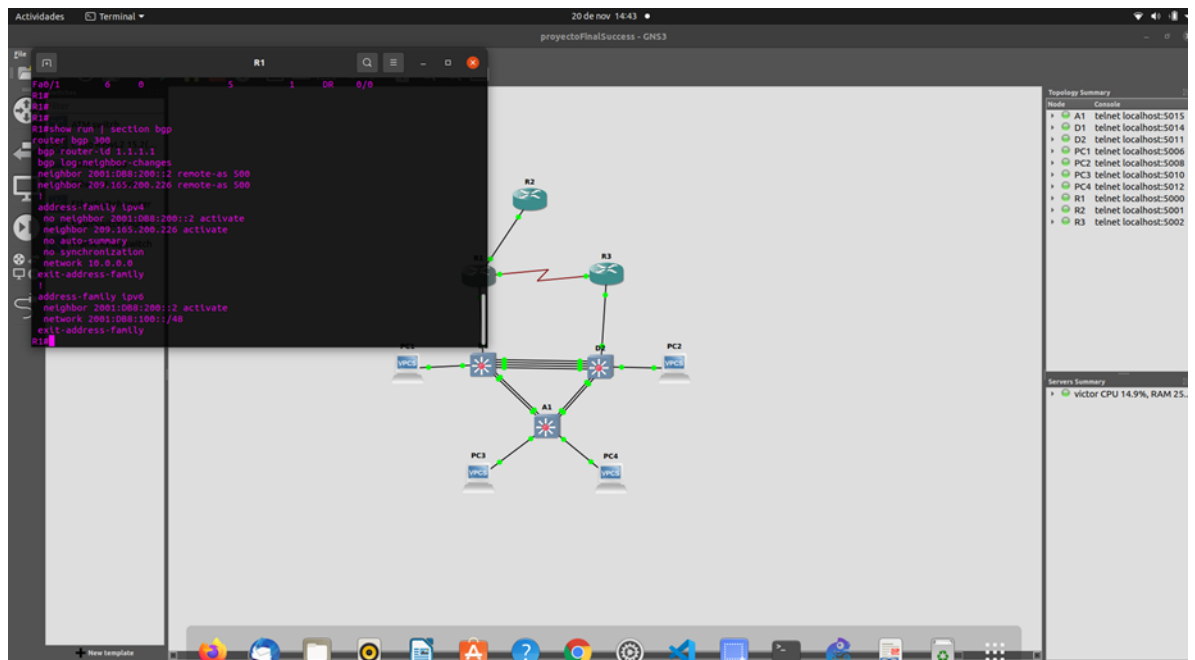


Figura 20. Verificación tarea 3.4



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 Compañía”. Las tareas de configuración son las siguientes:

Tabla 4. Tareas 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.	<p>Cree dos IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>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.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>
4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.	<p>Cree IP SLAs.</p> <ul style="list-style-type: none"> • Use la SLA número 4 para IPv4. • Use la SLA número 6 para IPv6. <p>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.</p> <ul style="list-style-type: none"> • Use el número de rastreo 4 para la IP SLA 4. • Use el número de rastreo 6 para la SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.</p>

4.3	En D1 configure HSRPv2.	<p>D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • 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.	<p>D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configure HSRP version 2.</p> <p>Configure IPv4 HSRP grupo 104 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. <p>Configure IPv4 HSRP grupo 114 para la VLAN 101:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv4 HSRP grupo 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. <p>Configure IPv6 HSRP grupo 106 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. <p>Configure IPv6 HSRP grupo 116 para la VLAN 101:</p> <ul style="list-style-type: none"> • 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. <p>Configure IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.
-----	--------------------------	--

Solución

Configuración general de switch D1

Switch D1

Se crea la IP SLAs número 4 y 6

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

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

```
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
```

Se configura D1 como router primario para las VLANs 100 y 102, y se cambia su prioridad a 150.

```
interface vlan 100
standby version 2
standby 104 ip 10.0.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.0.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
```

```
interface vlan 102
 standby version 2
 standby 124 ip 10.0.102.254
 standby 124 priority 150
 standby 124 preempt
 standby 124 track 4 decrement 60
 standby 126 ipv6 autoconfig
 standby 126 priority 150
 standby 126 preempt
 standby 126 track 6 decrement 60
 exit
 end
```

Configuración general de switch D2

Switch D2

Se crea la IP SLAs número 4 y 6

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

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

```
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
```

Se configura D2 como router primario para la VLAN 101, y se cambia su prioridad a 150.

```
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

```

Figura 21. Verificación tarea 4.1 y 4.3 en switch D1.

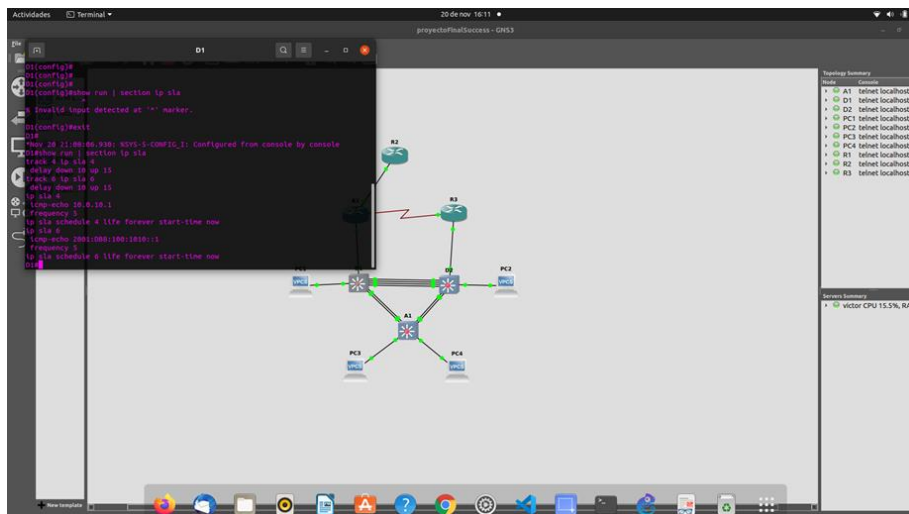


Figura 22. Verificación tarea 4.3 en switch D1.

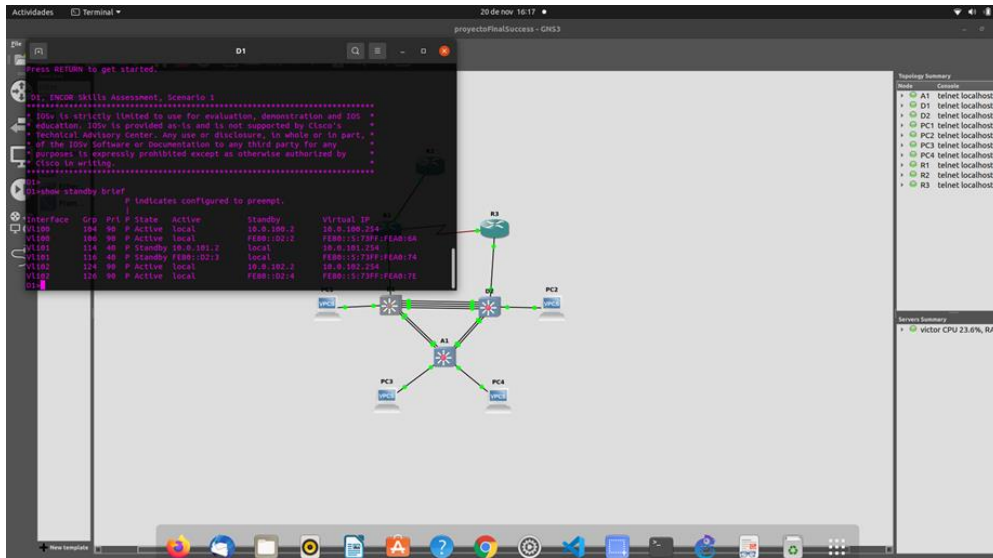
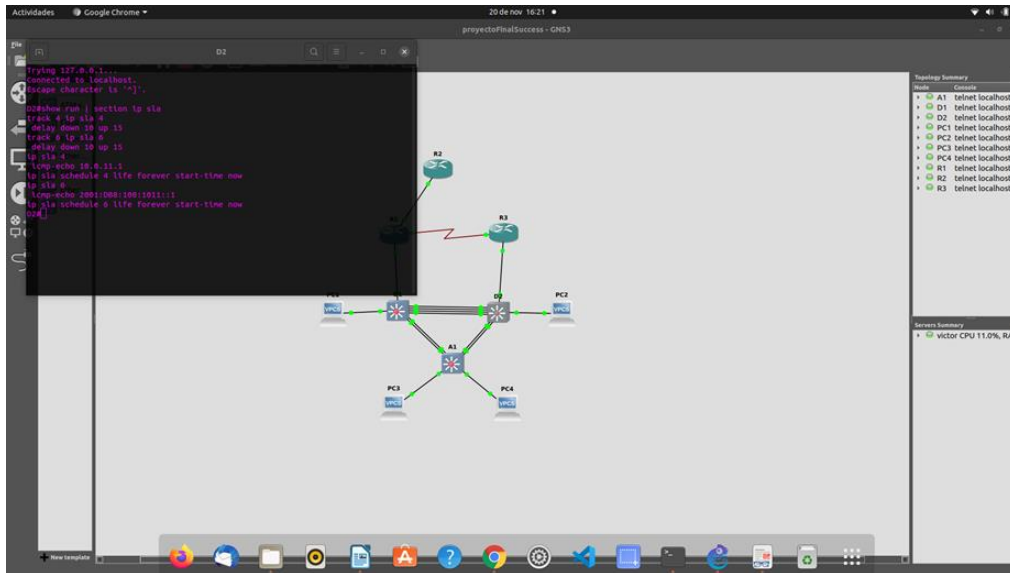


Figura 23. Verificación tarea 4.2 y 4.3 en switch D2.



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:

Tabla 5. Tareas de configuración parte 5.

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación SCRYPT.	Contraseña: cisco12345cisco
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.	<p>Detalles de la cuenta encriptada SCRYPT:</p> <ul style="list-style-type: none"> • 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.	<p>Especificaciones del servidor RADIUS.:</p> <ul style="list-style-type: none"> • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: \$trongPass
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	<p>Especificaciones de autenticación AAA:</p> <ul style="list-style-type: none"> • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS <p>De lo contrario, utilice la base de datos local.</p>
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 .

Solución

Configuración general para A1,D1,D2,R1,R2 y R3

Se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT y se asigna la contraseña cisco12345cisco

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

Se crea un usuario local y se protege usando el algoritmo de encriptación SCRYPT Con nivel de privilegio 15

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

los siguientes comandos se ingresan en todos los dispositivos excepto en R2

```
aaa new-model
```

Se habilita el AAA

```
radius server RADIUS
```

Se configura las especificaciones del servidor RADIUS

```
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
```

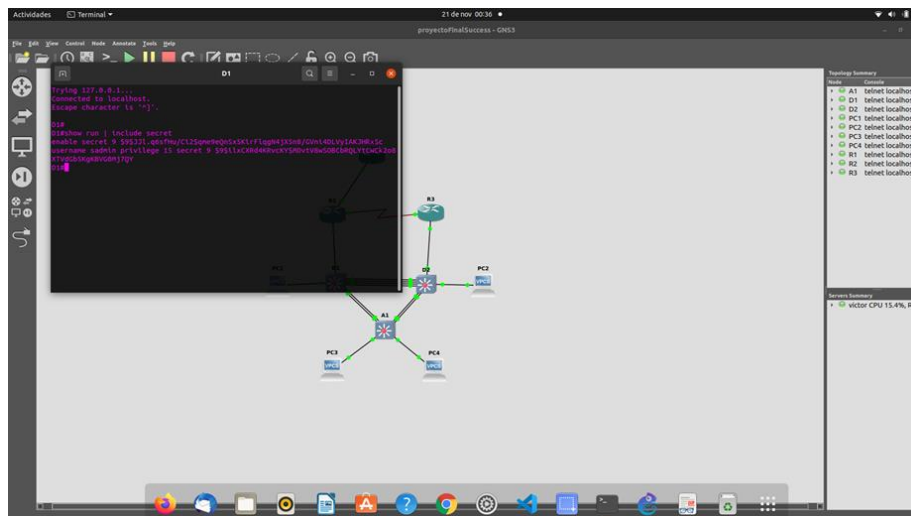
```
key $strongPass
```

```
exit
```

```
aaa authentication login default group radius local
```

```
end
```

Figura 24. Verificación tarea 5.1 y 5.2



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:

Tabla 6. Tareas de configuración parte 6.

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Establezca el <i>community string</i> en ENCORSA. En R3, D1, y D2, habilite el envío de <i>traps config</i> y <i>ospf</i> . <ul style="list-style-type: none"> • En R1, habilite el envío de <i>traps bgp, config, y ospf</i>. • En A1, habilite el envío de <i>traps config</i>.

Solución

Configuración general para R2

Router R2

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

```
ntp master 3  
end
```

Configuración general para R1

Router R1

Se configura NTP según especificaciones de la tabla

```
ntp server 2.2.2.2  
logging trap warning  
logging host 10.0.100.5  
logging on  
ip access-list standard SNMP-NMS  
permit host 10.0.100.5  
exit
```

Se configura SNMPv2c según especificaciones de la tabla

```
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
```

Configuración general para R3

Router 3

Se configura NTP según especificaciones de la tabla

```
ntp server 10.0.10.1  
logging trap warning  
logging host 10.0.100.5
```

```
logging on
ip access-list standard SNMP-NMS
  permit host 10.0.100.5
exit
```

Se configura SNMPv2c según especificaciones de la tabla

```
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
```

Configuración general para D1

Router D1

Se configura NTP según especificaciones de la tabla

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

Se configura SNMPv2c según especificaciones de la tabla

```
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
```

Configuración general para D2

Router D2

Se configura NTP según especificaciones de la tabla

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

Se configura SNMPv2c según especificaciones de la tabla

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

Router A1

Se configura NTP según especificaciones de la tabla

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

Se configura SNMPv2c según especificaciones de la tabla

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

Figura 26. Verificación tarea 6.1 y 6.2

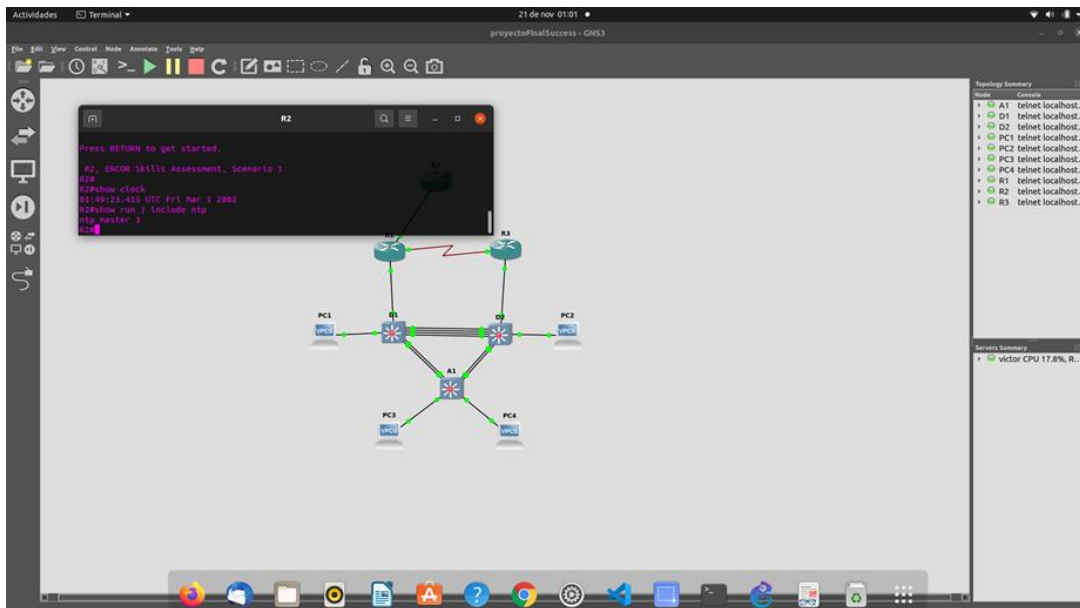


Figura 27. Verificación tarea 6.3

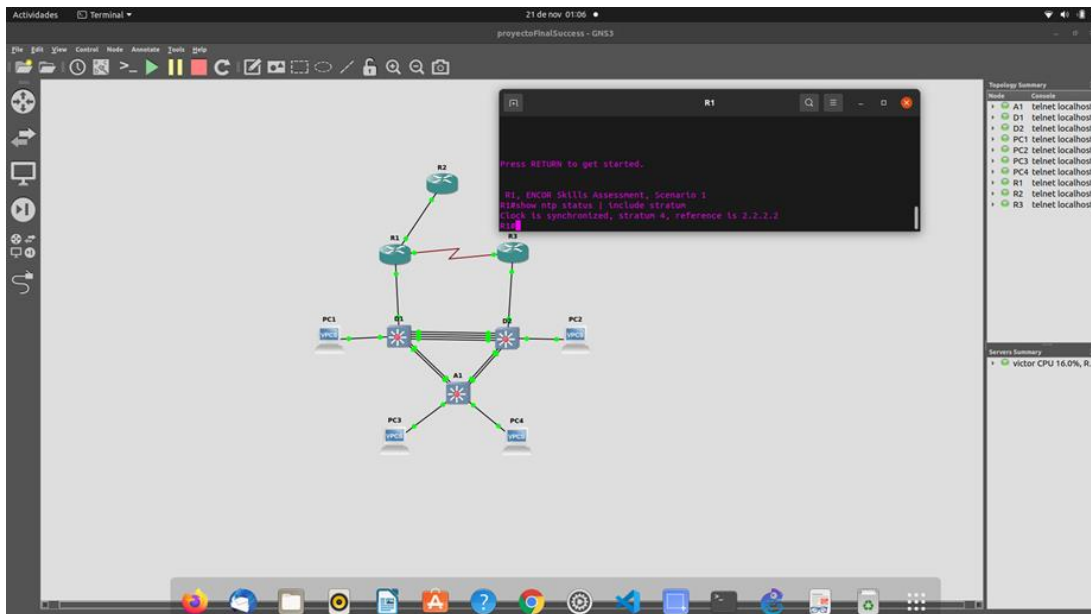


Figura 28. Verificación tarea 6.4

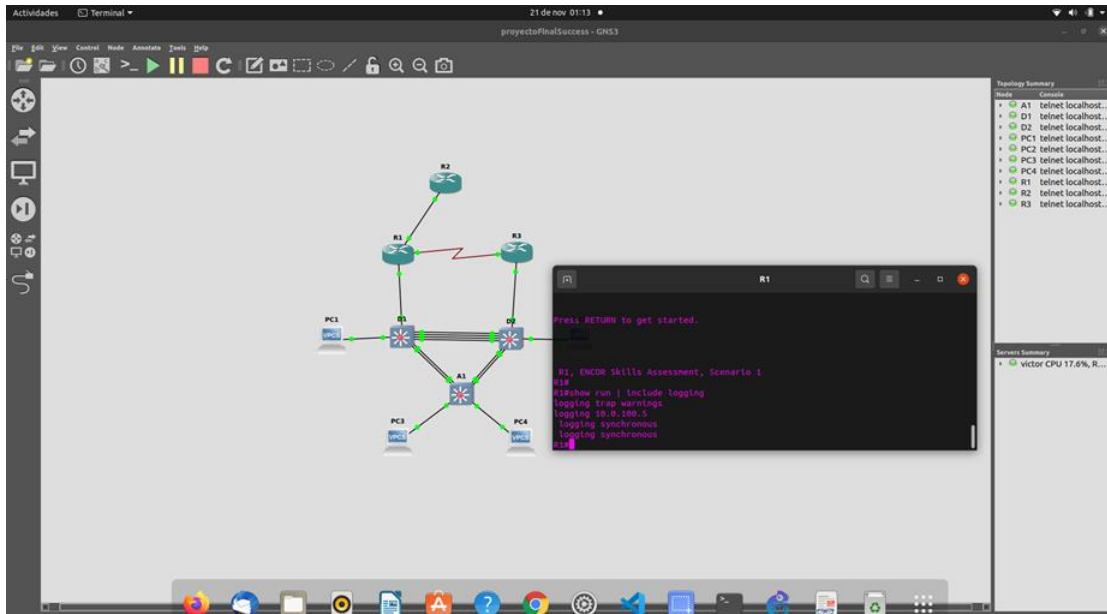
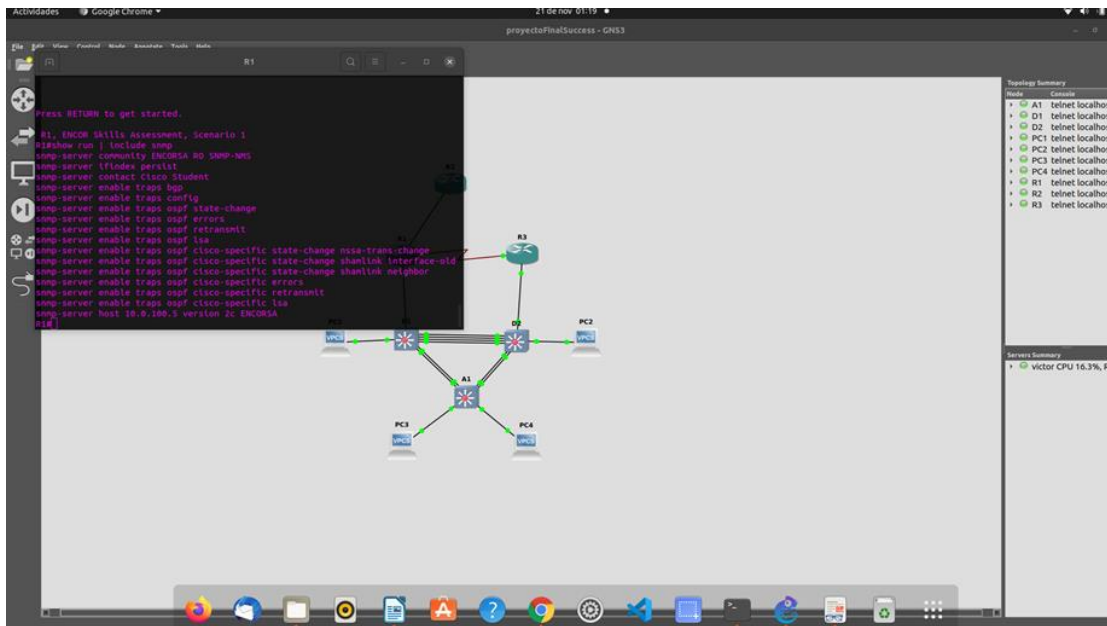


Figura 29. Verificación tarea 6.5



CONCLUSIONES

Con la implementación de redes mediante el simulador grafico GNS3 se facilita la comunicación, conectando de manera global con diferentes dispositivos en las topologías simuladas, haciéndolo más práctico y ágil para las compañías.

La culminación del proyecto y simulación de las actividades ejecutadas aportan a la organización laboral, profesional y personal, ofreciendo las herramientas para desarrollar las diferentes actividades en los procesos que se requieran en el campo de ejecución real.

Mediante el uso del simulador grafico GNS3 se puede identificar posibles fallas por medio de pruebas controladas, evitando que estas se ejecuten en la implementación física.

En este software podemos encontrar una herramienta completa y diversa la cual ofrece un abanico de implementación y ejecución en diferentes dispositivos.

BIBLIOGRAFÍA

- Cisco. (s.f.). *Qué es un router*. Obtenido de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html
- HotsGator. (s.f.). *Dirección IP: para qué sirve y cómo funciona*. Obtenido de <https://www.hostgator.mx/blog/que-es-una-direccion-ip/>
- Oracle. (s.f.). *Protocolos de enrutamiento*. Obtenido de https://docs.oracle.com/cd/E56339_01/html/E53805/ipref-13.html
- Telemáticas, R. (s.f.). *El switch: cómo funciona y sus principales características*. Obtenido de <https://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/>
- Zonas, R. (s.f.). *VLANs: Qué son, tipos y para qué sirven*. Obtenido de <https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>