DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

TIVISAY RUBIANO QUINTERO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

TIVISAY RUBIANO QUINTERO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cali,28 de noviembre de 2021

AGRADECIMIENTOS

Agradezco a la universidad por haberme brindado todos los recursos para tener una formación profesional correcta, a los tutores que me acompañaron en cada dificultad a lo largo de este gran trayecto que dejan como resultado a un profesional con capacidades y fortalezas para poder desempeñarme en mi vida laboral, a mi familia y compañeros que me brindaron apoyo moral ya que no fue un proceso sencillo de llevar a cabo y culminarlo, sé que voy a cumplir un logro que me propuse cuando inicie esta etapa y fue llegar al final con la mejor actitud y entregando lo mejor como profesional, a todos los que hicieron parte de mi formación muchas gracias.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

RSTP:
protocolo que previene loops en una red de switches

SLAAC:
Stateless Address Autoconfiguration, es un mecanismo muy cómodo y potente y que no tiene un equivalente en IPv4

BGP:
Border Gateway Protocol, es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

HSRP:
Hot Standby Router Protocol, es un protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red.

SNMP:
Simple Network Management Protocol, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red

EIGRP:
Gateway Routing Protocol, es un protocolo de encaminamiento de vector distancia, propiedad de Cisco System

RESUMEN

A través del curso CISCO CCNP, se irán adquiriendo las habilidades, conocimientos que llevarán a estar preparado para realizar los exámenes de implementación y funcionamiento de las tecnologías principales de las redes empresariales de Cisco (350-401 ENCOR), de implementación de enrutamiento y servicios avanzados de Cisco Enterprise (300-410 ENARSI)).

Dados los fundamentos del curso se estará preparado para implementar tecnologías avanzadas para generar una arquitectura empresarial segura y escalable. En conjunto con las Telecomunicaciones y la Electrónica, se configurarán las redes empresariales para una alta disponibilidad y un rendimiento optimo, se configurará y administrará redes inalámbricas de acceso remoto que permitirán la conmutación de sitio a sitio seguras, se alcanzará una comprensión de la virtualización y la automatización de la red.

ABSTRACT

Through the CISCO CCNP course, you will acquire the skills, knowledge that will lead you to be prepared to take the implementation and operation exams of the core technologies of Cisco enterprise networks (350-401 ENCOR), routing implementation and advanced services of Cisco Enterprise (300-410 ENARSI)).

Given the fundamentals of the course you will be prepared to implement advanced technologies to generate a secure and scalable enterprise architecture. In conjunction with Telecommunications and Electronics, enterprise networks will be configured for high availability and optimal performance, remote access wireless networks will be configured and managed that will enable secure site-to-site switching, an understanding of network virtualization and automation will be achieved.

INTRODUCCIÓN

En el siguiente trabajo se desarrollará un escenario planteado con el fin de analizar e implementar los protocolos a nivel empresarial aprendidos con base a los conceptos desarrollados por CISCO durante el curso teniendo como resultado este informe final. Donde habrá una serie de objetivos que llevan como resultado a crear una red segura, automatizada.

El escenario está comprendido en la red de una compañía que esta interconectado por una serie de dispositivos (Routers, PC, switches capa 2 y capa 3). Se medirán las habilidades aprendidas mediante el uso de los comandos apropiados para desarrollar las conexiones tanto virtuales como físicas.

Se procederá a configurar unas interfaces troncales entre los switches, seguido de un puente raíz RSTP con respaldo. La comunicación entre los PC`s se hará por medio de VLAN`s. El enrutamiento se llevará a cabo usando los protocolos IPv4 e IPv6, se usará una interfaz Loopback y se protegerá el ingreso a los dispositivos de modo local y remoto.

DESARROLLO DEL ESCENARIO PROPUESTO

1. Escenario 1

Figura 1. Escenario 1

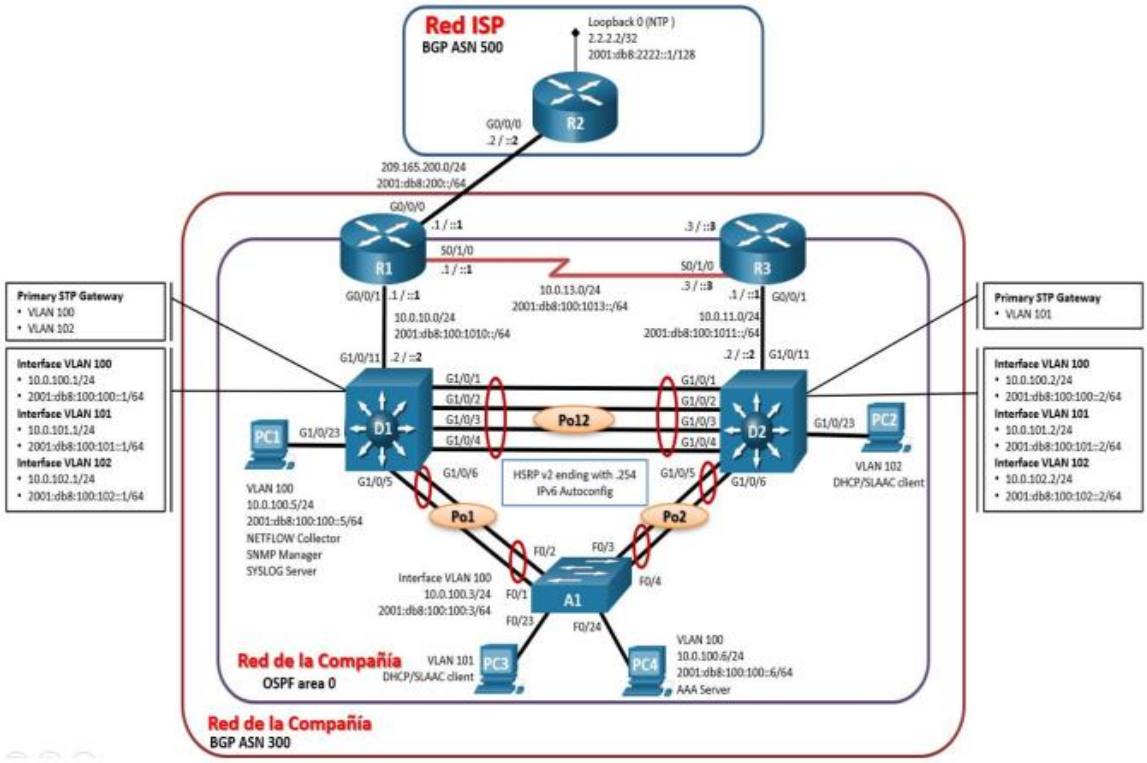


Tabla 1. Tabla de Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	interface e0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	interface e0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	interface s2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	interface e0/0	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	interface e0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	interface s2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	interface e0/1	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	interface e0/1	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

Escenario

En esta prueba de habilidades, debe completar la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default Gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

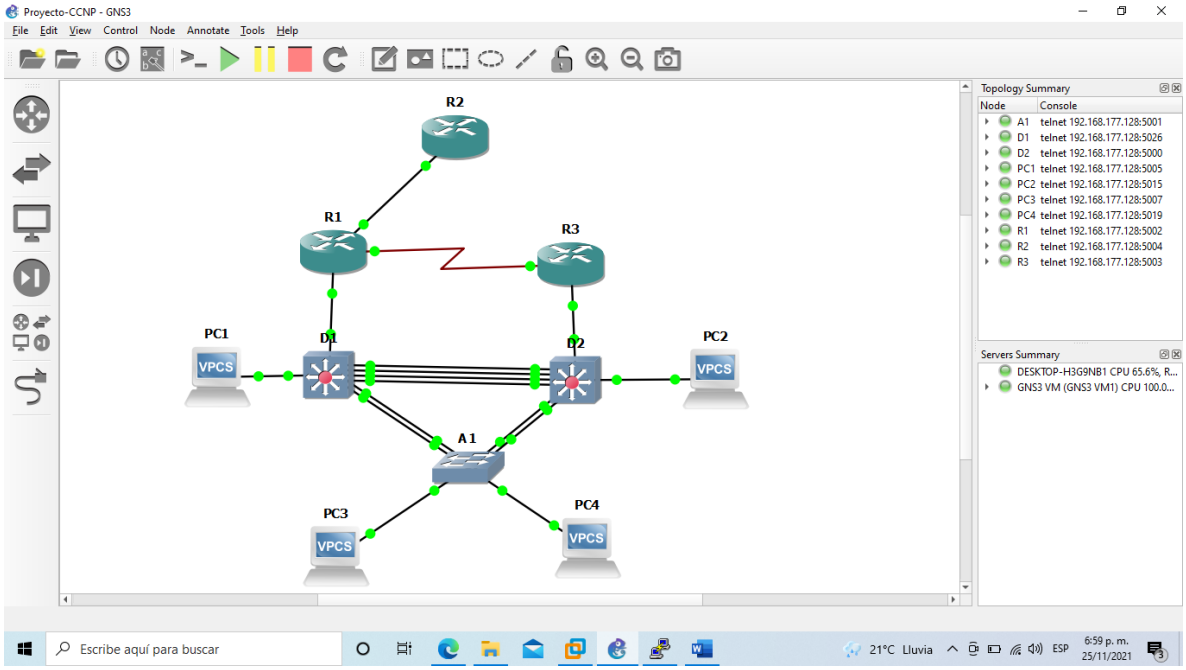
Recursos necesarios

- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
- 4 PC´s (utilice el programa de emulación de terminal)
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
- Los cables Ethernet y seriales van como se muestra en la topología

Parte 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces

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

Figura 2. Topología GNS3



Paso 2: Configurar los parámetros básicos para cada dispositivo

Se entra al modo de configuración global y se aplica los siguientes parámetros básicos en los dispositivos.
Se usa el comando running-config startup-config en todos los dispositivos para guardar la configuración.

Router R1

Router>
Router>enable // entro a modo privilegiado //
Router#config t // entro a modo configuration global //
Router(config)#hostname R1 // modifico el nombre //
R1(config)#ipv6 unicast-routing // habilitación direccionamiento IPv6 //

R1(config)#no ip domain lookup // desactiva la traducción de nombres a dirección del dispositivo //
R1(config)#banner motd // mensaje de aviso // # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0 // ingresar al modo de configuración de línea de la consola //
R1(config-line)#exec-timeout 0 0 // desconexión por inactividad //
R1(config-line)#logging synchronous // controla la impresión de mensajes de registro en el terminal de un usuario //
R1(config-line)#exit // salir //
R1(config)#interface e0/1 // entro al modo configuración de interfaz //
R1(config-if)#ip address 209.165.200.225 255.255.255.224 // IPv4 //
R1(config-if)#ipv6 address fe80::1:1 link-local // IPv6 //
R1(config-if)#ipv6 address 2001:db8:200::1/64
R1(config-if)#no shutdown // activar interfaz //
R1(config-if)#exit
R1(config)#interface e0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s2/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1#do copy run start // guardar configuración //

Router R2

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

```
R2(config)#interface e0/1
R2(config-if)# ip address 209.165.200.226 255.255.255.224
R2(config-if)#ipv6 address fe80::2:1 link-local
R2(config-if)# ipv6 address 2001:db8:200::2/64
R2(config-if)#no shutdown
R2(config-if)# exit
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)# ipv6 address 2001:db8:2222::1/128
R2(config-if)# no shutdown
R2(config-if)#exit
R2#do copy run start
```

Router 3

```
Router>
Router>enable
Router#config t
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface e0/1
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)# ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown
R3(config-if)# exit
R3(config)# interface s2/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
R3(config-if)#exit
R3#copy run start
```

Switch D1

```
Switch>
Switch>enable
Switch#config t
Switch#hostname D1
D1(config)#ip routing // configure tabla de enrutamiento //
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit
D1(config)#vlan 100 // entro al modo de configuración de interfaz virtual //
D1(config-vlan)#name Management // nombro //
D1(config-vlan)#exit
D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit
D1(config)#interface e0/1
D1(config-if)#no switchport // cambio interfaz al modo de acceso inactive //
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100 // entro a configuración de interfaz virtual //
D1(config-vlan)#ip address 10.0.100.1 255.255.255.0
D1(config-vlan)#ipv6 address fe80::d1:2 link-local
D1(config-vlan)#ipv6 address 2001:db8:100:100::1/64
D1(config-vlan)#no shutdown
D1(config-vlan)#exit
```

D1(config)#interface vlan 101
D1(config-vlan)#ip address 10.0.101.1 255.255.255.0
D1(config-vlan)#ipv6 address fe80::d1:3 link-local
D1(config-vlan)#ipv6 address 2001:db8:100:101::1/64
D1(config-vlan)#no shutdown
D1(config-vlan)#exit
D1(config)#interface vlan 102
D1(config-vlan)#ip address 10.0.102.1 255.255.255.0
D1(config-vlan)#ipv6 address fe80::d1:4 link-local
D1(config-vlan)#ipv6 address 2001:db8:100:102::1/64
D1(config-vlan)#no shutdown
D1(config-vlan)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109 // reservo direcciones que están asignadas estáticamente a hosts //
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101 // monto servidor DHCP //
D1(dhcp-config)#network 10.0.101.0 255.255.255.0 // dirección de red con clase directamente conectado //
D1(dhcp-config)#default-router 10.0.101.254 // Puerta de enlace predeterminada //
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102 // asignar un conjunto de direcciones el servidor DHCP //
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3 // especifico un rango de interfaces //
D1(config-if-range)#shutdown // desactivar //
D1(config-if-range)#exit
D1#copy run start

Switch D2

Switch>enable
Switch#config t
Switch#hostname D2
D2(config)#ip routing

```
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit
D2(config)#interface e0/1
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config-)#interface vlan 100
D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:100::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 101
D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#interface vlan 102
```

```
D2(config-if)#ip address 10.0.102.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool VLAN-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
D2(config)#shutdown
D2(config)#exit
D2#copy run start
```

Switch A1

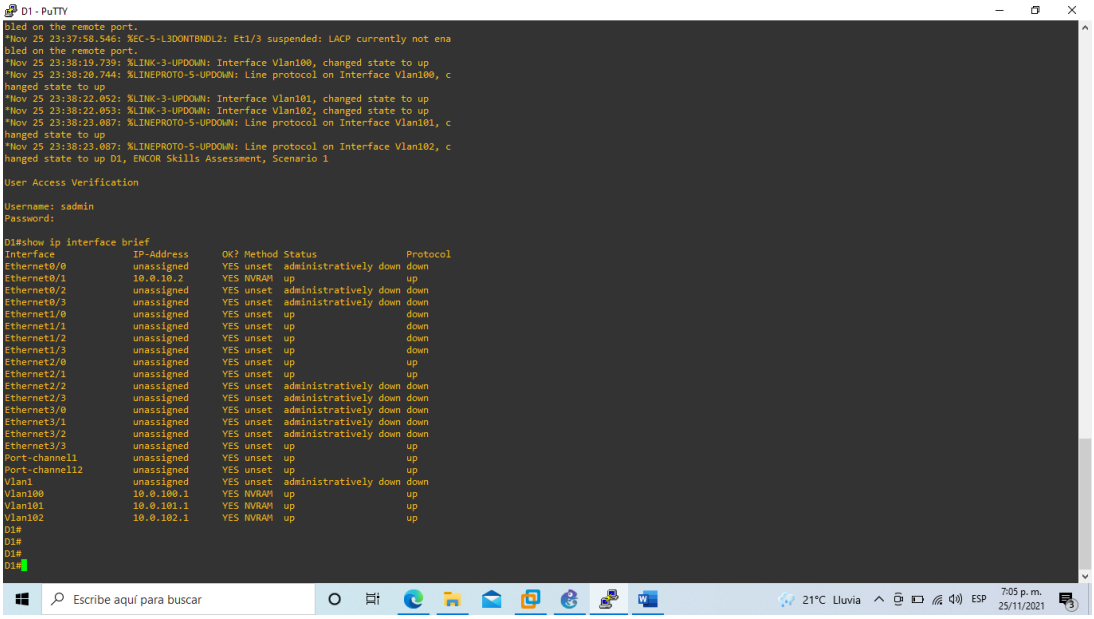
```
Switch>enable
Switch#config t
Switch(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
A1(config)#line con 0
A1(config-line)#exec-timeout 0 0
A1(config-line)#logging synchronous
A1(config-line)#exit
A1(config)#vlan 100
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
```

A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
A1(config)#interface vlan 100
A1(config-if)#ip address 10.0.100.3 255.255.255.0
A1(config-if)#ipv6 address fe80::a1:1 link-local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-3
A1(config-if)#shutdown
A1(config-if)#exit
A1#do copy run start

Show ip interface brief

Este comando genera un resumen de todas las interfaces incluyendo el estado y la dirección IP. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el switch D1

Figura 3. Show ip interface brief



Se configura las direcciones ipv4 e ipv6 para los PC1 Y PC4 de acuerdo con la tabla

PC1>ip 10.0.100.5 255.255.255.0 10.0.100.254 // asignar dirección IP //
PC1>ip 2001:db8:100:100::5/64 2001:db8:100:100::
PC1>save //guardar configuración //
PC1>sh // muestra la configuración IP //

PC4>ip 10.0.100.6 255.255.255.0 10.0.100.254
PC4>ip 2001:db8:100:100::6/64 2001:db8:100:100::1
PC4>save
PC4>sh

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

Se realizan las tareas de configuración siguientes:

Se configura los switches 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

Se configura la VLAN 999 como nativa en los switches

Se habilita el protocolo Rapid Spanning-Tree (RSTP) en los switches

Se configuran los puentes raíz RSTP (root bridges) según el diagrama de topología.

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

Se crea EtherChannels LACP según el diagrama de topología use los números de canales:

• D1 a D2 – Port channel 12

• D1 a A1 – Port channel 1

• D2 a A1 – Port channel 2

Se configura los puertos de acceso del host (host access port) en cada switch para PC1, PC2, PC3 Y PC4

Switch D1

D1(config)#interface range e1/0-3
D1(config-if)#switchport trunk encapsulation dot1q // establece el modo de encapsulación de la troncal //
D1(config-if)#switchport mode trunk // configura administrativamente el puerto como troncal //
D1(config-if)#switchport trunk native vlan 999 // establece el modo en la vlan de la troncal //

D1(config-if)#channel-group 12 mode active // configurar grupo de canal en modo activo //
D1(config-if)#exit
D1(config)#interface port-channel 12 // configuración de interfaz de canal del puerto //
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk allowed vlan 100,101,102 // permitir que las vlan crucen el enlace trooncal //
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#exit
D1(config)#interface range e2/0-1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#channel-group 1 mode active
D1(config-if)# exit
D1(config)#interface port-channel 1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport trunk allowed vlan 100,101,102
D1(config-if)#switchport trunk native vlan 999
D1(config-if)#exit
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100 root primary
D1(config)#spanning-tree vlan 102 root primary
D1(config)#interface e3/3
D1(config-if)#switchport mode access // convertirlo en puerto de acceso //
D1(config-if)#switchport access vlan 100 // asignarlo a una vlan //
D1(config-if)#exit

Switch D2

D2(config)#interface range e1/0-3
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#channel-group 12 mode active
D2(config-if)#exit

```
D2(config)#interface port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk allowed vlan 100,101,102
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#exit
D2(config)#interface range e2/0-1
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#channel-group 2 mode active
D2(config-if)#exit
D2(config)#interface port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#switchport trunk allowed vlan 100,101,102
D2(config-if)#switchport trunk native vlan 999
D2(config-if)#exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#interface e3/3
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#exit
```

Switch A1

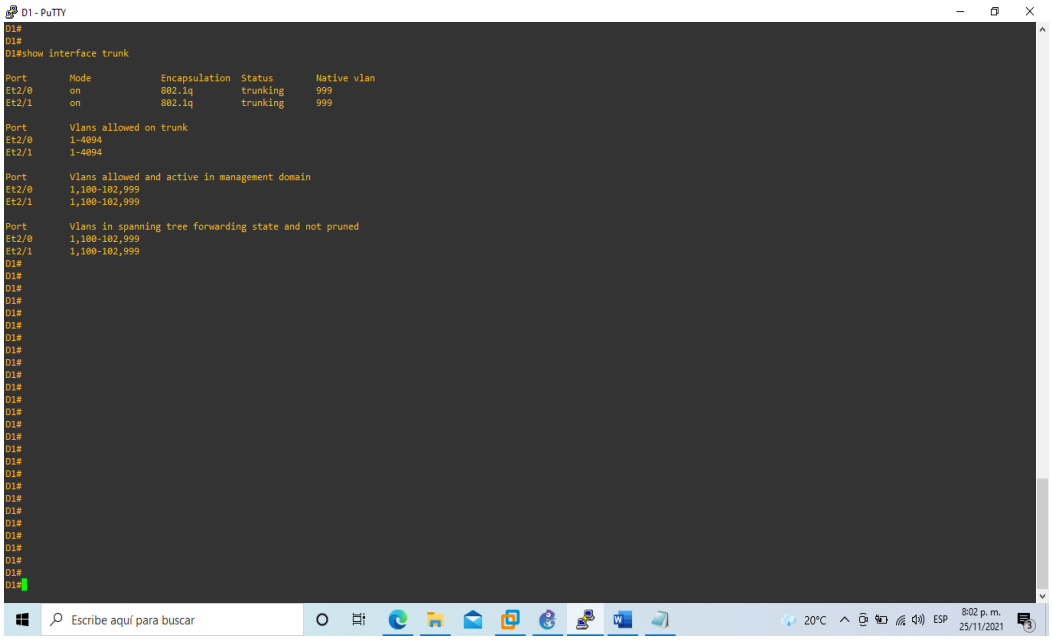
```
A1(config)#interface range e2/0-1
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#channel-group 1 mode active
A1(config-if)#exit
A1(config)#interface port-channel 1
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
A1(config-if)#switchport trunk allowed vlan 100,101,102
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#exit
A1(config)#interface range e2/2-3
```

```
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#channel-group 2 mode active
A1(config-if)#exit
A1(config)#interface port-channel 2
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
A1(config-if)#switchport trunk allowed vlan 100,101,102
A1(config-if)#switchport trunk native vlan 999
A1(config-if)#exit
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface e3/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#exit
A1(config)#interface e3/2
A1(config-if)# switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#exit
```

Show interface trunk

Permite verificar múltiples elementos de los enlaces troncales. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el switch D1

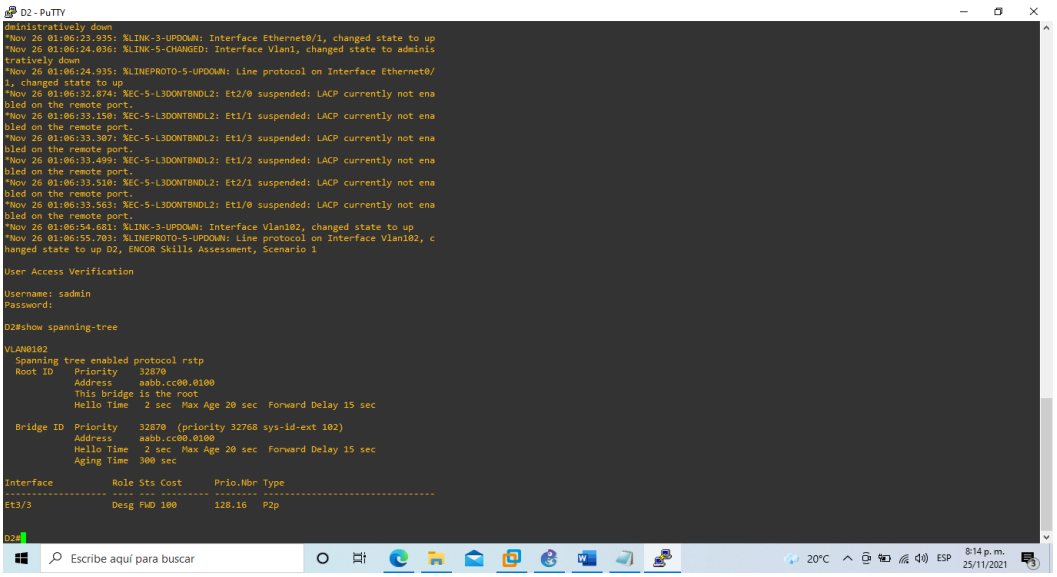
Figura 4. Show interface trunk



Show spanning-tree

Despliega la información del protocolo. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el switch D1

Figura 5. Show spanning-tree



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

Figura 6. DHCP PC 2

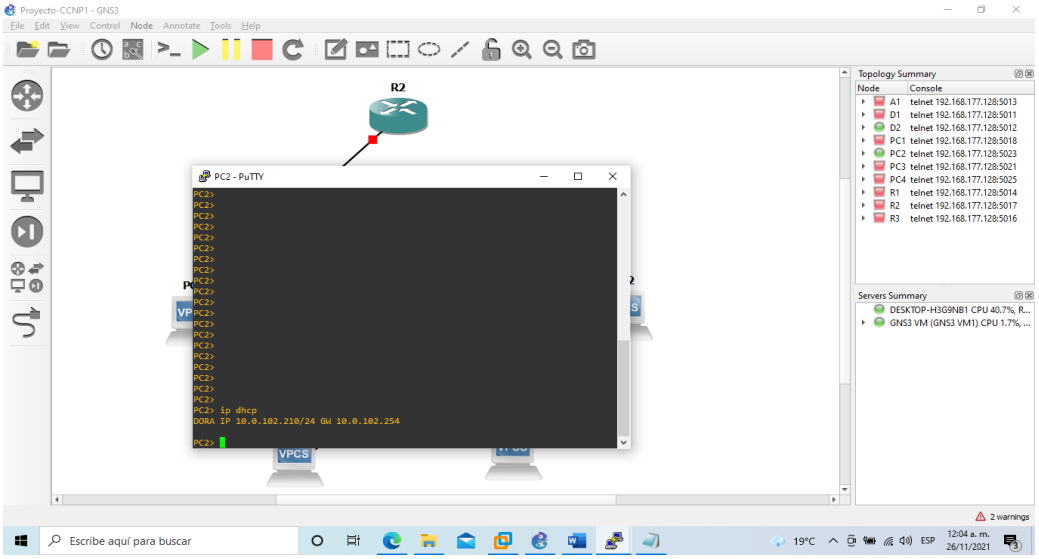
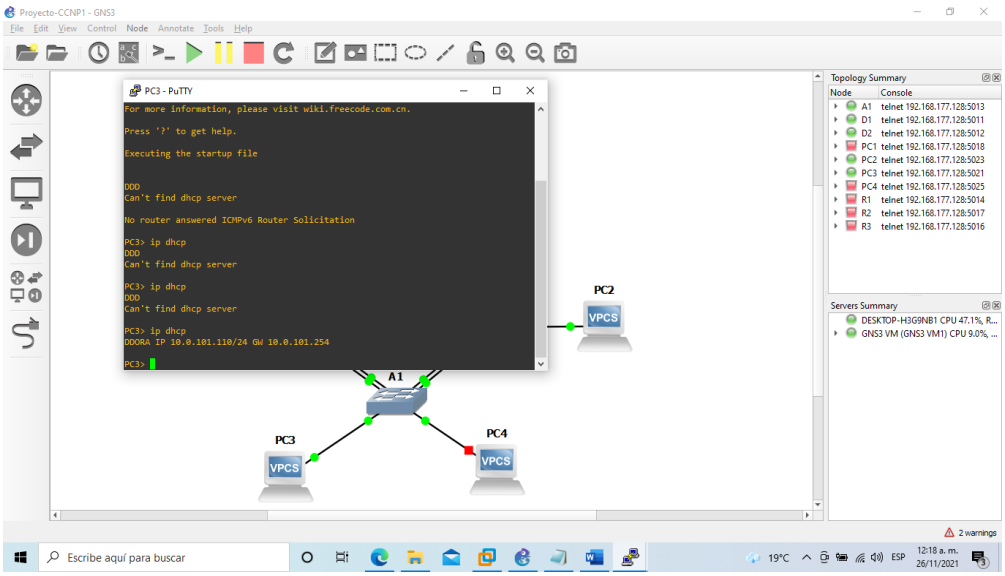


Figura 7. DHCP PC 3

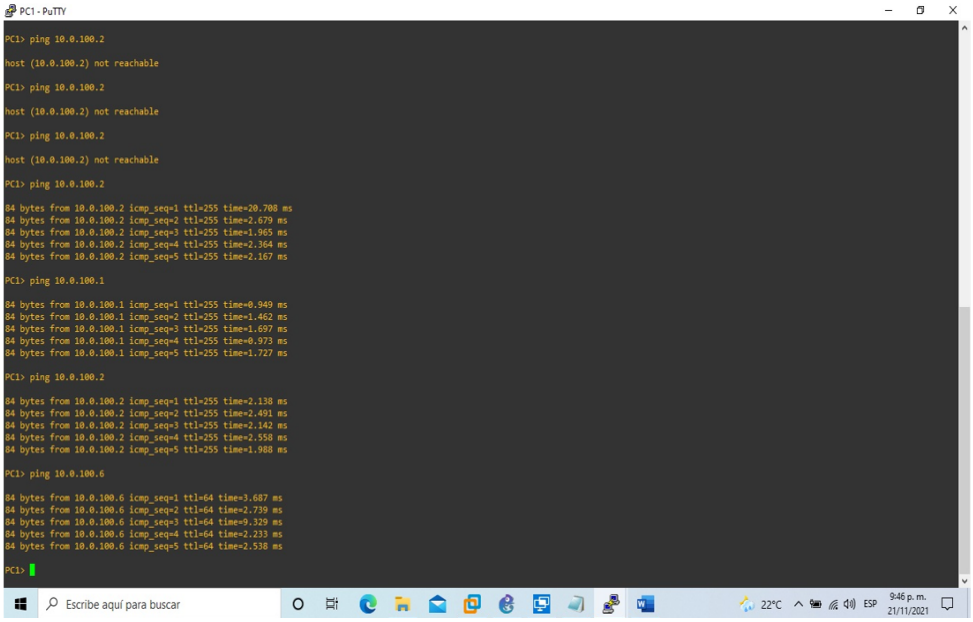


Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:
• D1: 10.0.100.1

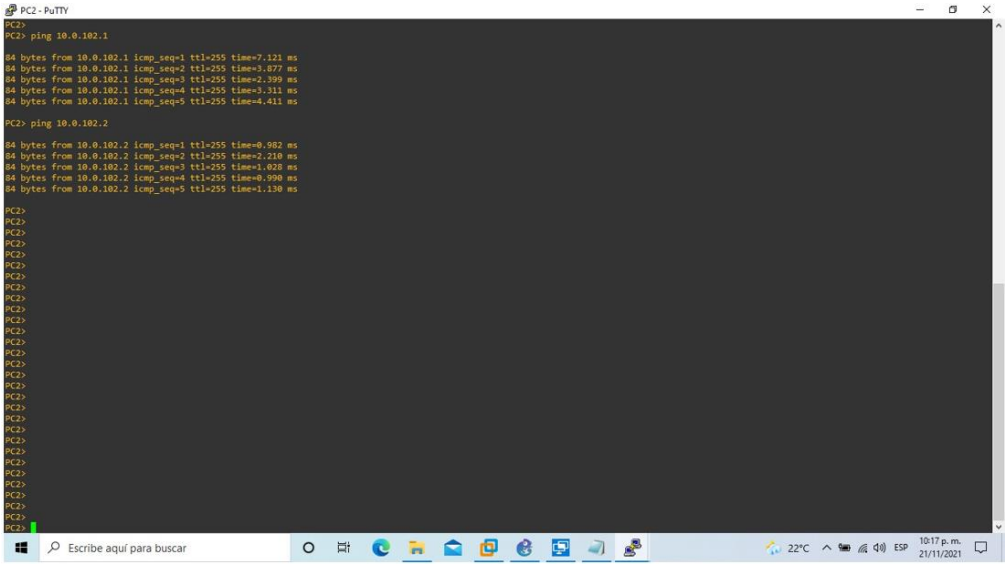
• D2: 10.0.100.2
• PC4: 10.0.100.6

Figura 8. PC 1



PC2 debería hacer ping con éxito a:
• D1: 10.0.102.1
• D2: 10.0.102.2

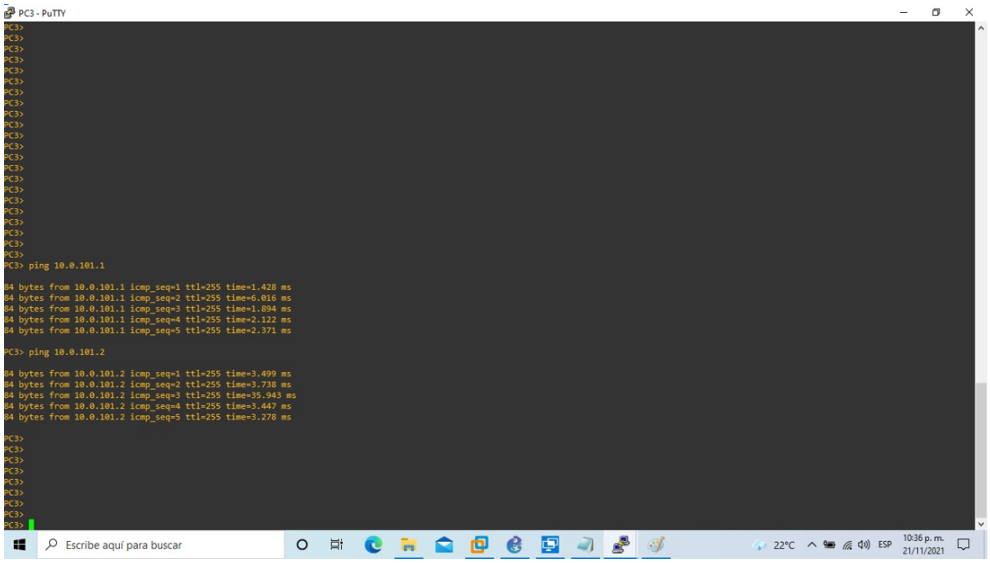
Figura 9. PC 2



PC3 debería hacer ping con éxito a:

• D1: 10.0.101.1
• D2: 10.0.101.2

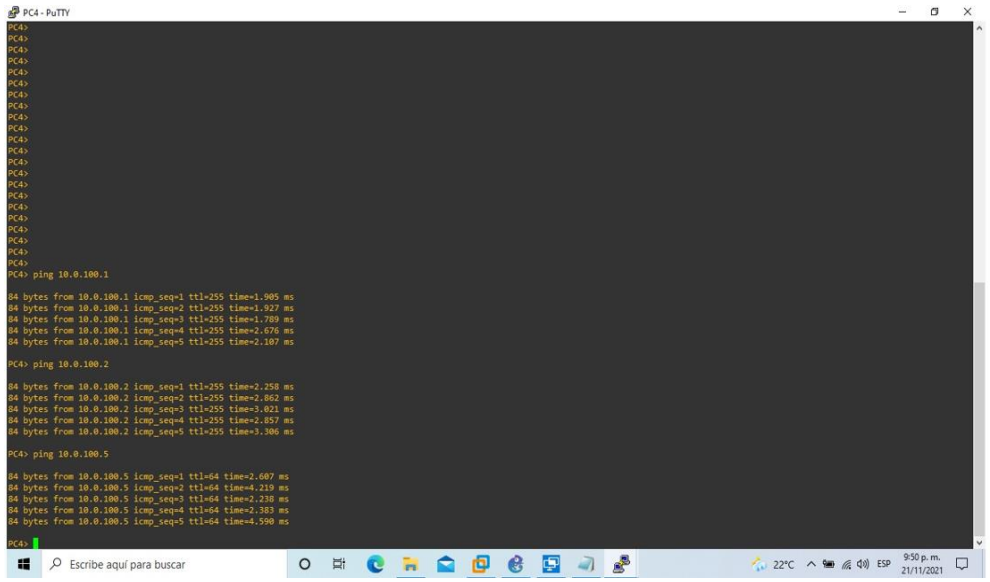
Figura 10. PC 3



PC4 debería hacer ping con éxito a:

• D1: 10.0.100.1
• D2: 10.0.100.2
• PC1: 10.0.100.5

Figura 11. PC 4



Parte 3: Configurar los protocolos de enrutamiento

Las tareas de configuración son las siguientes:

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

Use OSPF Process ID 4 y asigne los siguientes router-IDs:
• R1: 0.0.4.1
• R3: 0.0.4.3
• D1: 0.0.4.131
• D2: 0.0.4.132
En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en área 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 e0/1
• D2: todas las interfaces excepto e0/1

En la “Red de la compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.
Use OSPF Process ID 6 y asigne los siguientes router-IDs:
• R1: 0.0.6.1
• R3: 0.0.6.3
• D1: 0.0.6.131
• D2: 0.0.6.132
En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en área 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 e0/1
• D2: todas las interfaces excepto e0/1

Router R1

R1(config)#router ospf 4 // configurar enrutamiento por OSPF //
R1(config-route)#router-id 0.0.4.1 // configurar el proceso de enrutamiento por OSPF //
R1(config-route)#network 10.0.13.0 0.0.0.255 area 0 // habilitar para enviar y recibir paquetes OSPF //
R1(config-route)#network 10.0.10.0 0.0.0.255 area 0
R1(config-route)#exit
R1(config)#ipv6 router ospf 6 // configurar enrutamiento OSPF IPv6 //
R1(config-rtr)#router-id 0.0.6.1
R1(config-rtr)#exit
R1(config)#interface e0/1
R1(config-if)#ipv6 ospf 6 area 0 // asignar OSPF id y área id //
R1(config-if)#exit
R1(config)#interface S2/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config)#exit

Router R3

R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
R3(config-router)#exit
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.3
R3(config-rtr)#exit
R3(config)#interface e0/1
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit
R3(config)#interface S2/0
R3(config-if)#ipv6 ospf 6 area 0
R3(config-if)#exit

Switch D1

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.0.0 0.0.255.255 area 0
D1(config-router)#exit
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#exit
D1(config)#interface e0/1
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

Switch D2

```
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.132
D1(config-router)#network 10.0.0.0 0.0.255.255 area 0
D1(config-router)#exit
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.132
D1(config-rtr)#exit
D1(config)#interface e0/1
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

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 IPv6 con R1 en ASN 300.
En IPv4 address family, anuncie:
• La red Loopback 0 IPv4 (/32).
• La ruta por defecto (0.0.0.0/0).

En IPv6 address family, anuncie:
• La red Loopback 0 IPv4 (/128).
• La ruta por defecto (::/0).
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.

Router R2

R2(config)#ip route 0.0.0.0 0.0.0.0 Loopback 0 // asignar ruta estática //
R2(config)#ipv6 route ::/0 loopback 0 // asignar ruta estática IPv6 //
R2(config)#router bgp 500 // activo enrutamiento BGP //
R2(config-router)#bgp router-id 2.2.2.2 // configuro el ID del enrutador BGP //
R2(config-router)#bgp log-neighbor-changes // habilito el registro del vecino BGP //
R2(config-router)#network 209.165.200.224 mask 255.255.255.224 // asignar IP //
R2(config-router)#redistribute connected // redistribuyo todas las direcciones conectadas a la IP asignada //
R2(config-router)#neighbor 209.165.200.225 remote-as 300 // asigno un vecino al BGP //
R2(config-router)#no auto-summary // deshabilito el resumen automático //
R2(config-router-af)#address-family ipv4 // asigno dirección familiar para la sesión BGP usando IPv4 //
R2(config-router-af)#network 0.0.0.0 mask 0.0.0.0
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#exit
R2(config-router)#address-family ipv6 // asigno dirección familiar para la sesión BGP usando IPv6 //

R2(config-router-af)#network 2001:db8:2222::1/128
R2(config-router-af)#network ::/0
R2(config-router-af)#exit

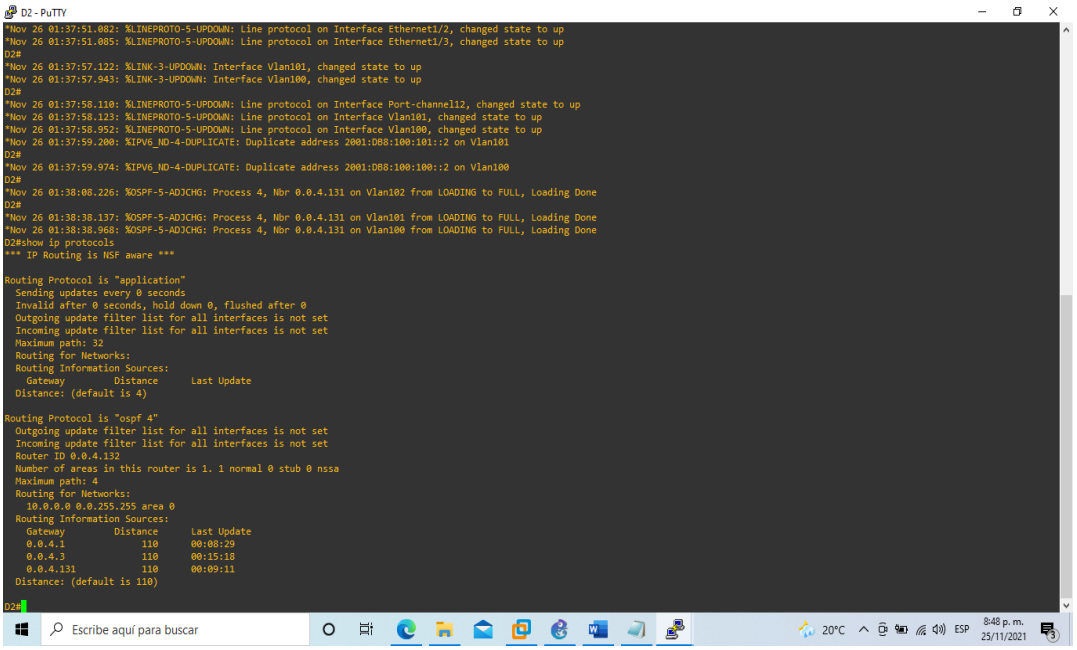
Router R1

R1(config)#ip route 10.0.0.0 255.0.0.0 null 0
R1(config)#ipv6 route 2001:db8:100::/48 null 0
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#bgp log-neighbor-changes
R1(config-router)#network 209.165.200.224 mask 255.255.255.224
R1(config-router)#network 10.0.10.0 mask 255.255.255.0
R1(config-router)#network 10.0.13.0 mask 255.255.255.0
R1(config-router)#redistribute connected
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500
R1(config-router)#address-family ipv4
R1(config-router-af)#neighbor 209.165.200.226 activate // activo la dirección vecino //
R1(config-router-af)#exit
R1(config-router)#address-family ipv6
R1(config-router-af)#network 2001:db8:100::/48
R1(config-router-af)#neighbor 2001:db8:200::2 activate
R1(config-router-af)#exit

Show ip protocols

Verifica información fundamental de configuración OSPF. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el switch D2

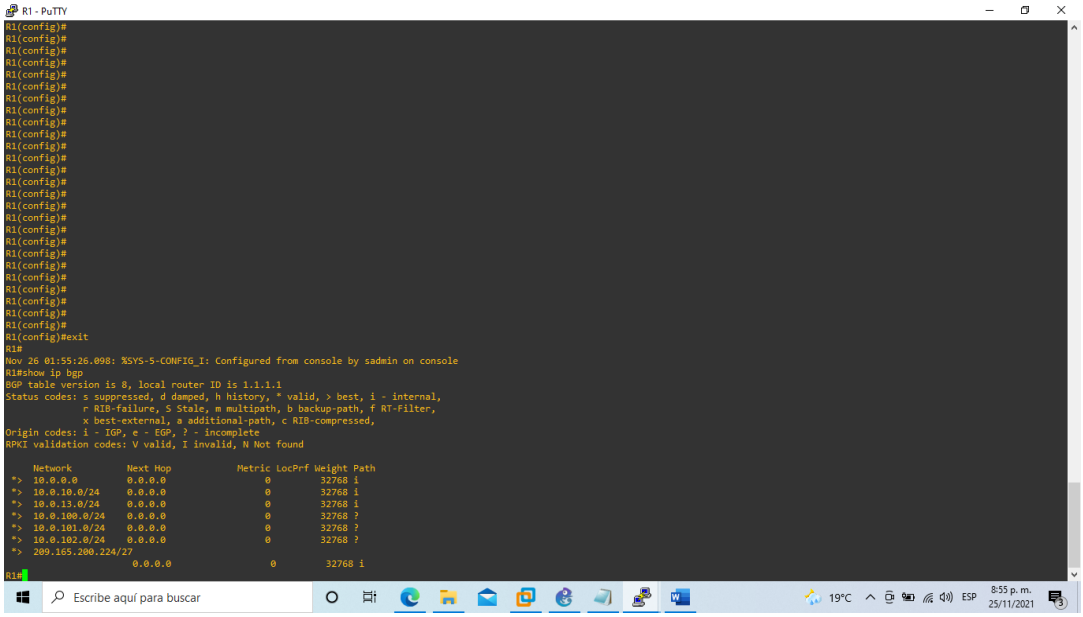
Figura 12. Show ip protocols



Show ip bgp

Muestra la tabla de routing BGP. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el switch R1

Figura 13. Show ip bgp



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

Las tareas de configuración son las siguientes:
En D(1,2), cree IP SLAs que prueben la accesibilidad de la interfaz R(1,3) e0/1.
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 R(1-3) 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.

Switch D1

D1(config)#interface e0/1
D1(config-if)#no switchport
D1(config-if)#exit
D1(config)#ip sla 4 // configuro IP SLA //
D1(config-ip-sla)#icmp-echo 10.0.11.1 source-ip 10.0.11.2 // defino una icmp-echo y lo asigno a la IP SLA //
D1(config-ip-sla-echo)#frequency 5 // agrego velocidad a la que se repita la IP SLA //
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 start-time now life forever // asigno un grupo y un rango de números para IP SLA //
D1(config)#track 4 ip sla 4 state // creo el track y lo asocio a la IP SLA //
D1(config-track)#delay up 15 down 10 // asigno un periodo de tiempo para retrasar los cambio de estado //
D1(config-track)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-ip
2001:db8:100:1011::2
D1(config-ip-sl-echo)#frequency 5
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 6 start-time now life forever

```
D1(config)#track 6 ip sla 6 state
D1(config-track)#delay up 15 down 10
D1(config-track)#exit
```

Switch D2

```
D2(config)#interface ethernet 0/1
D2(config-if)#no switchport
D2(config-if)#exit
D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1 source-ip 10.0.11.2
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 start-time now life forever
D2(config)#track 4 ip sla 4 state
D2(config-track)#delay up 15 down 10
D2(config-track)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-ip
2001:db8:100:1011::2
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 6 start-time now life forever
D2(config)#track 6 ip sla 6 state
D2(config-track)#delay up 15 down 10
D2(config-track)#exit
```

show ip sla configuration

Muestra la configuración IP SLA. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el switch D1

Figura 14. Show ip sla configuration

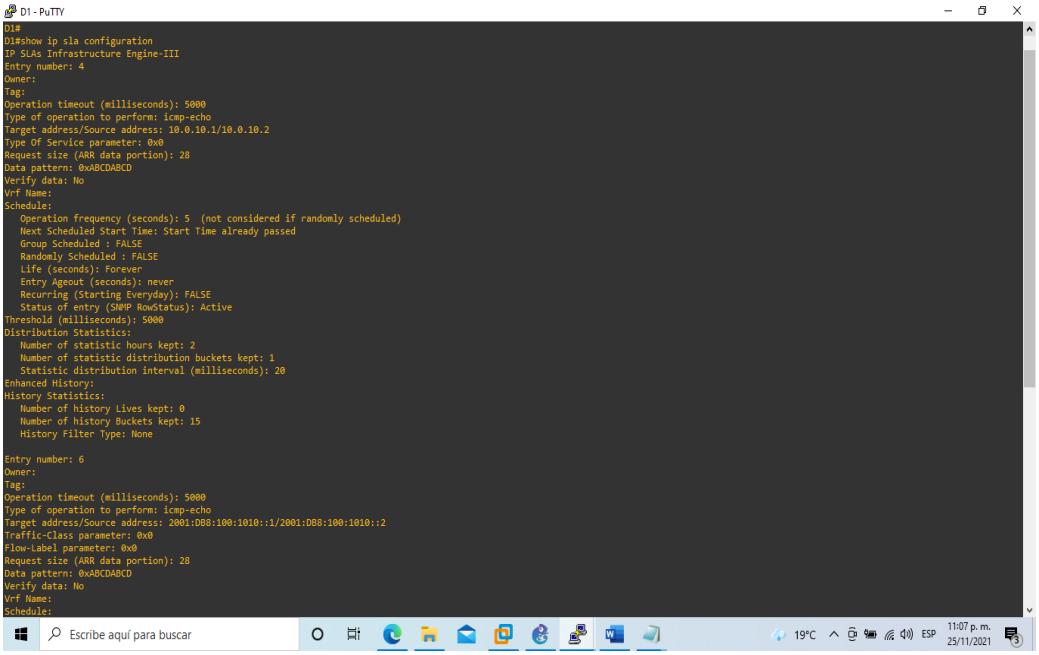
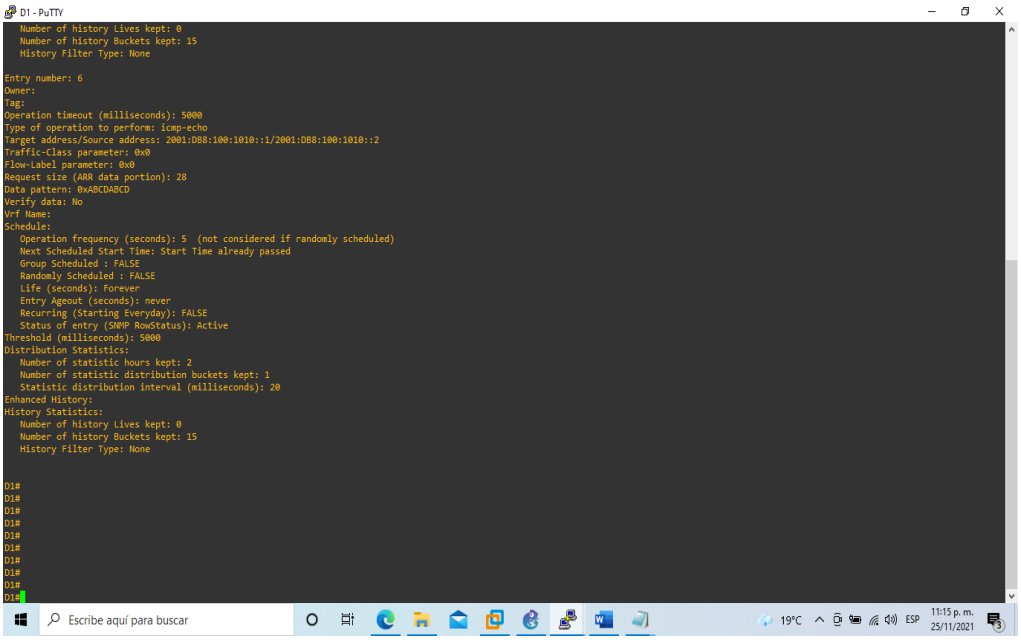


Figura 15. Show ip sla configuration 2



En R1 configure HSRPv2

R1 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.

Router R1

R1(config)#interface e0/1.100
R1(config-subif)#standby versión 2 // configuro HSRP versión 2 //

R1(config-if)#standby 104 ip 10.0.100.254 // asigno el número de rango del grupo a una IP a la interfaz //
R1(config-if)#standby 104 priority 150 // asigno la prioridad del enrutador que quedara en espera //
R1(config-if)#standby 104 preempt // activo la prioridad del enrutador para definir que enrutador queda activo //
R1(config-if)#standby 104 track 4 decrement 60 // configuro el seguimiento de objeto para cuando la prioridad disminuya //
R1(config-if)#exit
R1(config)#interface e0/1.101
R1(config-if)#standby version 2
R1(config-if)#standby 114 ip 10.0.101.254
R1(config-if)#standby 114 preempt
R1(config-if)#standby 114 track 4 decrement 60
R1(config-if)#exit
R1(config)#interface e0/1.102
R1(config-if)#standby version 2
R1(config-if)#standby 124 ip 10.0.102.254
R1(config-if)#standby 124 priority 150
R1(config-if)#standby 124 preempt
R1(config-if)#standby 124 track 4 decrement 60
R1(config-if)#exit
R1(config)# ipv6 unicast-routing // habilito IPv6 para HSRP //
R1(config)#interface e0/1.100
R1(config-if)#standby 106 ipv6 autoconfig // asigno el número de rango del grupo a una IPv6 de la interfaz //
R1(config-if)#standby 106 priority 150
R1(config-if)#standby 106 preempt
R1(config-if)#standby 106 track 6 decrement 60
R1(config-if)#ipv6 address 2001:db8:100:100::254/64 //asigno IPv6 a la interfaz //
R1(config-if)#exit
R1(config)#interface e0/1.101
R1(config-if)#standby 116 ipv6 autoconfig
R1(config-if)#standby 116 preempt
R1(config-if)#standby 116 track 6 decrement 60
R1(config-if)#ipv6 address 2001:db8:100:101::254/64
R1(config-if)#exit
R1(config)#interface e1/0.102
R1(config-if)#standby 126 ipv6 autoconfig

R1(config-if)#standby 126 priority 150
R1(config-if)#standby 126 preempt
R1(config-if)#standby 126 track 6 decrement 60
R1(config-if)#ipv6 address 2001:db8:100:102::254/64
R1(config-if)#exit
R1(config)#ip sla ethernet-monitor schedule 6 schedule-period 60 ip sla schedule 6 start-time now life forever

En R3, configure HSRPv2
R3 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.

Router R3

```
R3(config)#interface e0/1.100
R3(config-if)#standby version 2
R3(config-if)#standby 104 ip 10.0.100.254
R3(config-if)#standby 104 priority 150
R3(config-if)#standby 104 preempt
R3(config-if)#standby 104 track 4 decrement 60
R3(config-if)#exit
R3(config)#interface e0/1.101
R3(config-if)#standby version 2
R3(config-if)#standby 114 ip 10.0.101.254
R3(config-if)#standby 114 preempt
R3(config-if)#standby 114 track 4 decrement 60
R3(config-if)#exit
R3(config)#interface e0/1.102
R3(config-if)#standby version 2
R3(config-if)#standby 124 ip 10.0.102.254
R3(config-if)#standby 124 priority 150
R3(config-if)#standby 124 preempt
R3(config-if)#standby 124 track 4 decrement 60
R3(config-if)#exit
R3(config)# ipv6 unicast-routing
R3(config)#interface e0/1.100
R3(config-if)#standby 106 ipv6 autoconfig
R3(config-if)#standby 106 preempt
R3(config-if)#standby 106 track 6 decrement 60
R3(config-if)#ipv6 address 2001:db8:100:100::4/64
R3(config-if)#exit
R3(config)#interface e0/1.101
R3(config-if)#standby 116 ipv6 autoconfig
R3(config-if)#standby 116 priority 150
R3(config-if)#standby 116 preempt
R3(config-if)#standby 116 track 6 decrement 60
R3(config-if)#ipv6 address 2001:db8:100:101::4/64
R3(config-if)#exit
R3(config)#interface e0/1.102
R3(config-if)#standby 126 ipv6 autoconfig
R3(config-if)#standby 126 preempt
```

R3(config-if)#standby 126 track 6 decrement 60
R3(config-if)#ipv6 address 2001:db8:100:102::4/64
R3(config-if)#exit
R3(config)#ip sla ethernet-monitor schedule 6 schedule-period 60 ip sla schedule 6 start-time now life forever

Show standby

Muestra información del protocolo HSRP. Se debe estar en modo privilegiado (#) para ejecutar el comando. Como ejemplo se ejecuta en el router R1

Figura 16. Show standby

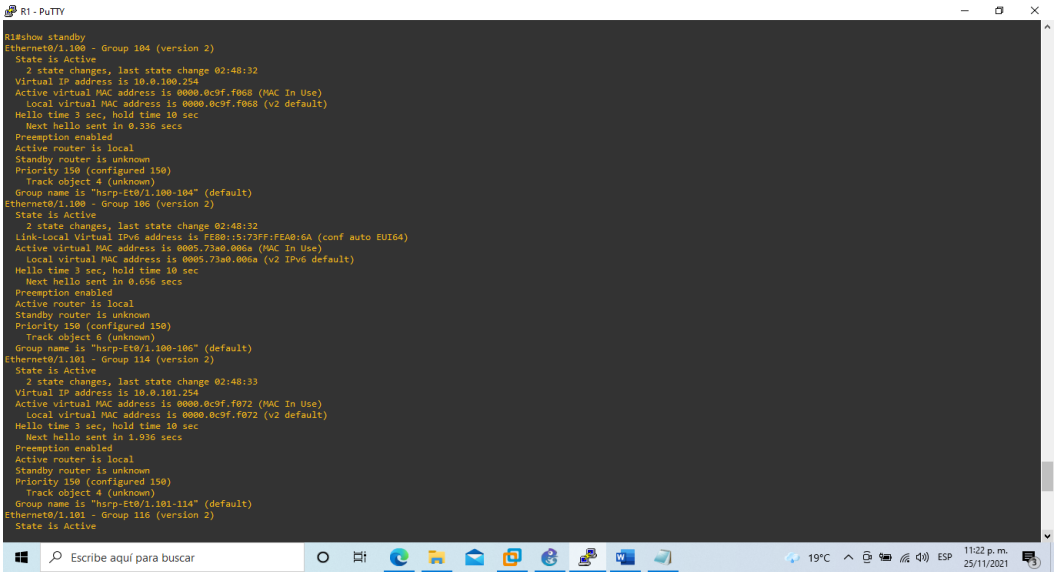
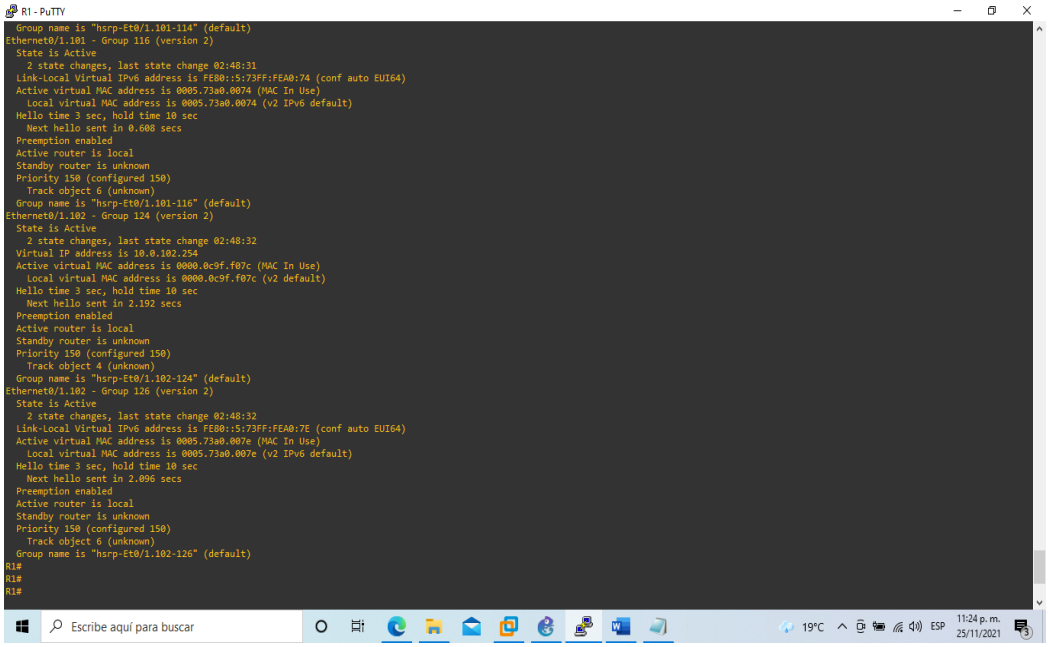


Figura 17. Show standby 2



Parte 5: Configurar la seguridad

Las tareas de configuración son las siguientes:
Nota: no se realizan estas configuraciones en el Router R2

Tabla 2. Mecanismos de seguridad

Tarea	Especificación
En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
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**
En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **sadmin** y la contraseña: **cisco12345cisco**.

Router R1

R1(config)#enable secret cisco12345cisco // protejo el acceso a modo privilegiado //
R1(config)#aaa new-model // configuro autenticación AAA //
R1(config)#aaa authentication login default local // autentico AAA el usuario local //
R1(config)#username sadmin privilege 15 password cisco12345cisco // asigno nombre usuario y clave //
R1(config)#service password-encryption // encripto la clave //
R1(config)#line console 0 // configuro la línea de consola //

R1(config-line)#login authentication default // asigno que la línea de consola pida autenticación //
R1(config-line)#exit
R1(config)#line vty 0 4 // configuro el acceso remoto //
R1(config-line)#password cisco12345cisco // asigno una clave //
R1(config-line)#login authentication default // atentico el usuario remoto //
R1(config-line)#service password-encryption // encripto la clave //
R1(config-line)#exit

Router R3

R3(config)#enable secret cisco12345cisco
R3(config)#aaa new-model
R3(config)#aaa authentication login default local
R3(config)#username sadmin privilege 15 password cisco12345cisco
R3(config)#service password-encryption
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco12345cisco
R3(config-line)#login authentication default
R3(config-line)#service password-encryption
R3(config-line)#exit

Switch D1

D1(config)#enable secret cisco12345cisco
D1(config)#aaa new-model
D1(config)#aaa authentication login default local
D1(config)#username sadmin privilege 15 password cisco12345cisco
D1(config)#service password-encryption
D1(config)#line console 0
D1(config-line)#login authentication default
D1(config-line)#exit
D1(config)#line vty 0 4
D1(config-line)#password cisco12345cisco
D1(config-line)#login authentication default
D1(config-line)#service password-encryption

D1(config-line)#exit

Switch D2

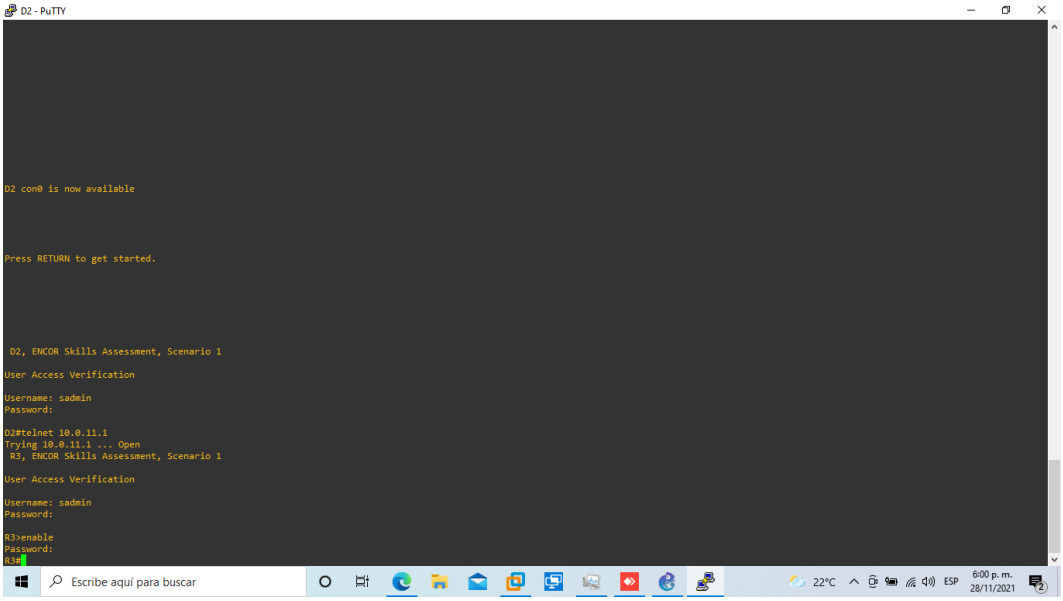
D2(config)#enable secret cisco12345cisco
D2(config)#aaa new-model
D2(config)#aaa authentication login default local
D2(config)#username sadmin privilege 15 password cisco12345cisco
D2(config)#service password-encryption
D2(config)#line console 0
D2(config-line)#login authentication default
D2(config-line)#exit
D2(config)#line vty 0 4
D2(config-line)#password cisco12345cisco
D2(config-line)#login authentication default
D2(config-line)#service password-encryption
D2(config-line)#exit

A1(config)#enable secret cisco12345cisco
A1(config)#aaa new-model
A1(config)#aaa authentication login default local
A1(config)#username sadmin privilege 15 password cisco12345cisco
A1(config)#service password-encryption
A1(config)#line console 0
A1(config-line)#login authentication default
A1(config-line)#exit
A1(config)#line vty 0 4
A1(config-line)#password cisco12345cisco
A1(config-line)#login authentication default
A1(config-line)#service password-encryption
A1(config-line)#exit

Telnet

Protocolo para establecer conexiones remotas

Figura 18. Protocolo Telnet



Parte 6: Configurar las características de administración de red

Las tareas de configuración son las siguientes:

Tabla 3. Funciones de administración de red

Tarea	Especificación
En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 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.
Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
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*.

Router R1

R1#clock set 21:30:00 24 nov 2021 // asigno hora y fecha //
R1#conf t
R1(config)#ntp server 209.165.200.226 // asigno dirección IP al ntp server //
R1(config)#ntp master 4 // asigno dirección IP como maestro //
R1(config)#logging host 10.0.100.5 // asigno dirección IP para recibir mensajes del sistema de registros //
R1(config)#logging trap warnings // asigno mensajes de registro de advertencia //
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA // asigno la versión para enviar capturas al host //
R1(config)#snmp-server community private ro // configurar la comunidad privada de solo lectura //
R1(config)#snmp-server contact TIVISAY QUINTERO RUBIANO // asigno un contacto al snmp //
R1(config)#snmp-server enable traps bgp // habilito el envío de mensajes de improviso del protocolo BGP //
R1(config)#snmp-server enable traps config
R1(config)#snmp-server enable traps ospf
R1(config)#exit

Router R2

R2#clock set 21:30:00 24 nov 2021
R2#conf t
R2(config)#ntp master 3
R2(config)#exit

Router R3

R3#clock set 21:30:51 24 nov 2021
R3#conf t
R3(config)#ntp server 10.0.10.1
R3(config)#ntp master 5
R3(config)#logging host 10.0.100.5
R3(config)#logging trap warnings
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server community private ro

R3(config)#snmp-server contact TIVISAY QUINTERO RUBIANO
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#exit

Switch D1

D1#clock set 21:30:51 24 nov 2021
D1#conf t
D1(config)#ntp server 10.0.10.1
D1(config)#logging host 10.0.100.5
D1(config)#logging trap warnings
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server community private ro
D1(config)#snmp-server contact TIVISAY QUINTERO RUBIANO
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
D1(config)#exit

Switch D2

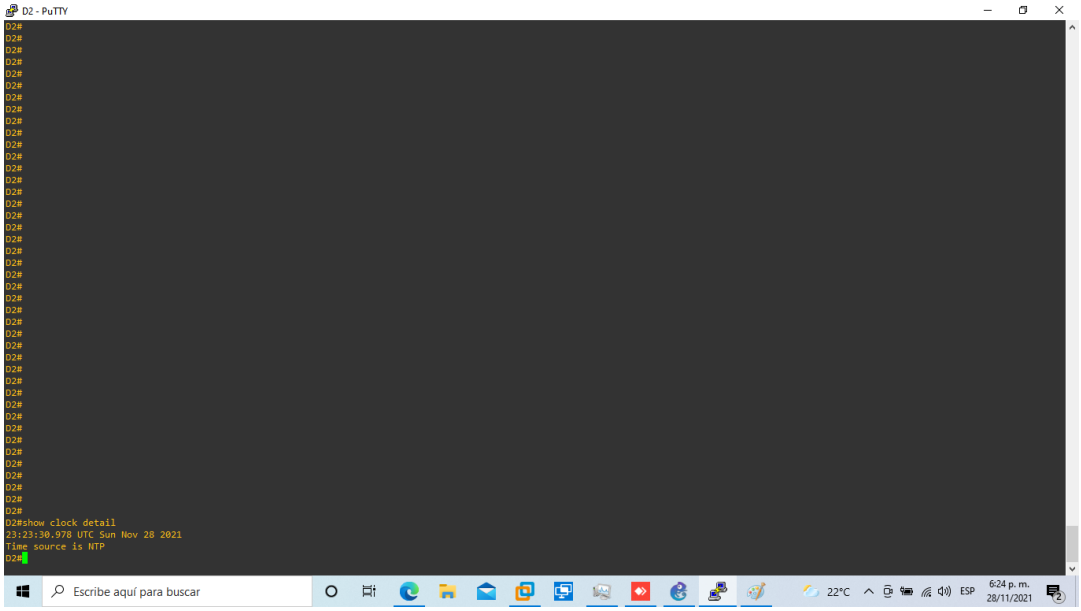
D2#clock set 21:30:51 24 nov 2021
D2#conf t
D2(config)#ntp server 10.0.11.1
D2(config)#logging host 10.0.100.5
D2(config)#logging trap warnings
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server community private ro
D2(config)#snmp-server contact TIVISAY QUINTERO RUBIANO
D2(config)#snmp-server enable traps config
D2(config)#snmp-server enable traps ospf
D2(config)#exiit

Switch A1

A1#clock set 21:30:51 24 nov 2021
A1#conf t
A1(config)#ntp server 10.0.10.1

A1(config)#logging host 10.0.100.5
A1(config)#logging trap warnings
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server community private ro
A1(config)#snmp-server contact TIVISAY QUINTERO RUBIANO
A1(config)#snmp-server enable traps config
A1(config)#exit

Figura 19. Show clock detail



CONCLUSIONES

Con el desarrollo de los anteriores pasos, aplicamos los protocolos adecuados para este trabajo final, estableciendo una conexión segura virtualizando la red y conexiones remotas, se obtienen conocimientos para administrar una red empresarial basada en su planificación, implementación y solución de problemas.

Se logra simular el escenario mediante la herramienta GNS3, ya que es un programa que permite realizar el montaje completo de diferentes dispositivos y protocolos, se implementó el escenario, su configuración, análisis y el funcionamiento de una red empresarial segura de alta gama.

Se adquirió habilidades para monitorear el flujo de datos, redundancia y rendimientos en las redes LAN y WAN

Los dispositivos de telecomunicación tienen una gran importancia en la funcionalidad de las redes garantizando su seguridad e interacción remotamente.

BIBLIOGRAFÍA

Cisco Networking Academy. Contenido en línea: http://www.netacad.com

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ

GNS3. Contenido en línea. https://www.gns3.com/

Syllabus de curso Diplomado de profundización CISCO CCNP (2018). Recuperado de http://campus08.unad.edu.co/ecbti35/mod/folder/view.php?id=2794

UNAD (2015). Switch CISCO -Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg