DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

IOHAM MORILLO HERNANDEZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

IOHAM MORILLO HERNANDEZ

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

DIRECTOR
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

VALLEDUPAR, 29 de noviembre de 2021

AGRADECIMIENTOS

A mí, por haberme permitido el tiempo y el esfuerzo necesario para llevar a feliz término la culminación de las actividades académicas propuestas y necesarias, dejando de lado otras actividades de carácter lúdico que algún momento pudieron parecer más atractivas.

CONTENIDO

AGRADECIMIENTOS....4
CONTENIDO....5
LISTA DE TABLAS....7
LISTA DE FIGURAS....8
GLOSARIO....9
RESUMEN....10
ABSTRACT....10
INTRODUCCION....11
ESCENARIO PROPUESTO....12
TOPOLOGIA PROPUESTA....12
TABLA DE DIRECCIONAMIENTO PROPUESTA....13
PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS Y EL DIRECCIONAMIENTO DE LAS INTERFACES. ...15
1.1 CONFIGURACIONES INICIALES....15
1.2 EVIDENCIAS DE LA CONFIGURACIÓN INICIAL DE LOS DISPOSITIVOS. 21
PARTE 2: CONFIGURAR LA CAPA 2 DE LA RED Y EL SOPORTE DE HOST ...25
2.1 CONFIGURACIÓN DE INTERFACES TRONCALES....25
2.2 CAMBIO DE VLAN NATIVA EN LOS ENLACES TRONCALES 26
2.3 CONFIGURACIÓN DEL PROTOCOLO RAPID SPANNING-TREE (RSTP) EN TODOS LOS SWITCH. 27
2.4 CONFIGURACIÓN DE LOS PUENTES RAÍZ RSTP (ROOT BRIDGES) EN D1 Y D2....27
2.5 CREACIÓN DE CTHERCHANNEL LACP EN TODOS LOS SWITCH....28
2.6 CONFIGURACIÓN EN TODOS LOS SWITCH DE LOS PUERTOS DE ACCESO DEL HOST (HOST ACCESS PORT) QUE SE CONECTAN A PC1, PC2, PC3 Y PC4. 30
PARTE 3: CONFIGURAR LOS PROTOCOLOS DE ENRUTAMIENTO 33
3.1 CONFIGURACIÓN DE OSPFV2....33
3.2 CONFIGURACIÓN DE OSPPFV3 34
3.3 CONFIGURACIÓN DE MP-BGP EN R2....39
3.4 CONFIGURACIÓN DE MP-BGP EN R1....40
PARTE 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO....43
4.1 CREAR IP SLAS EN D1 43

4.2 CREAR IP SLAS EN D2 43
4.3 CONFIGURAR HSRPV2 EN D1 45
4.4 CONFIGURAR HSRPV2 EN D2 46
PARTE 5: SEGURIDAD 49
5.1 PROTECCIÓN DEL EXEC PRIVILEGIADO 49
5.2 CREACIÓN DE USUARIO LOCAL 49
5.3 HABILITACIÓN DE AAA 49
5.4 CONFIGURACIÓN DEL SERVIDOR RADIUS 49
5.5 CONFIGURACION DE LISTA DE MÉTODOS DE AUTENTICACIÓN AAA 50
5.6 VERIFICACIÓN DEL SERVICIO AAA 50
PARTE 6: CONFIGURACIÓN DE LAS FUNCIONES DE ADMINISTRACIÓN DE RED. 52
6.1 CONFIGURACIÓN DEL RELOJ LOCAL A LA HORA UTC ACTUAL EN TODOS LOS DISPOSITIVOS. 52
6.2 CONFIGURACIÓN DE R2 COMO UN NTP MAESTRO EN EL NIVEL DE ESTRATO 3. 53
6.3 CONFIGURACIÓN DE NTP EN R1, R3, D1, D2, Y A1 53
6.4 CONFIGURACIÓN DE SYSLOG EN TODOS LOS DISPOSITIVOS EXCEPTO EN R2. 54
6.5 CONFIGURACIÓN DE SNMPV2C EN TODOS LOS DISPOSITIVOS EXCEPTO R2. 54
PARTE 7: VERIFICACIÓN DE CONECTIVIDAD ENTRE LOS DIFERENTES HOSTS DE LA RED. 56
CONCLUSIONES 58
BIBLIOGRAFIA 59

LISTA DE TABLAS

Tabla 1. Direccionamiento IPv4 e IPv6 13
Tabla 2 Lista de equipos utilizados 14

LISTA DE FIGURAS

Figura 1 Topología de red propuesta. 12
Figura 2 Montaje en GNS3 15
Figura 3 Lista de interfaces configuradas en R1. 21
Figura 4 Lista de interfaces configuradas en R2. 22
Figura 5 Lista de interfaces configuradas en R3. 22
Figura 6 Lista de interfaces Configuradas en D1. 23
Figura 7 Lista de interfaces configuradas en D2. 23
Figura 8 Lista de interfaces configuradas en A1. 24
Figura 9 Direccionamiento de PC1 y PC4. 24
Figura 10 Verificación de troncales en D1. 25
Figura 11 Verificación de troncales en D2. 26
Figura 12 Verificación de troncales en A1. 26
Figura 13 Verificación de protocolo RSTP en D1, D2 y A1. 27
Figura 14 Verificación de EtherChannel en D1. 30
Figura 15 Verificación de ping de PC1 a vlan100 en D1 y D2, y ping a PC4. 31
Figura 16 Verificación de ping de PC2 a vlan102 en D1 y D2. 32
Figura 17 Verificación de ping de PC3 a vlan101 en D1 y D2. 32
Figura 18 Verificación de ping de PC4 a vlan100 en D1 y D2, y ping a PC1. 32
Figura 19 Verificación de ospf 4 y ospf 6 en R1. 36
Figura 20 Verificación de ospf 6 en R3. 36
Figura 21 Verificación de OSPF en R3 37
Figura 22 Verificación de OSPF en D1. 37
Figura 23 Verificación de Ospf en D1 38
Figura 24 Verificación de Ospf en D2. 38
Figura 25 Verificación de BPG ipv4 en R2 40
Figura 26 Verificación de relaciones de vecindad en R1. 41
Figura 28 Verificación de ping desde D1 hasta Loopback. 41
Figura 29 Verificación de ping desde D2 hasta Loopback. 42
Figura 30 Verificación IP SLA en D1. 44
Figura 31 Verificación IP SLA en D2. 44
Figura 32 Verificación HSRPv2 en D1. 48
Figura 33 Verificación de HSRPv2 en D2 48
Figura 34 Verificación de aaa y radius en R1. 50
Figura 35 Verificación de aaa y radius en R3. 50
Figura 36 Verificación de aaa y radius en D1. 51
Figura 37 Verificación de aaa y radius en D2. 51
Figura 38 Verificación de timezone en cada dispositivo. 52
Figura 39 Verificación de ntp server en cada dispositivo. 53
Figura 40 Verificación de conectividad desde PC1. 56
Figura 41 Verificación de conectividad desde PC2. 56
Figura 42 Verificación de conectividad desde PC3. 57
Figura 43 Verificación de conectividad desde PC4. 57

GLOSARIO

AAA**:** Es un mecanismo de seguridad que garantiza la autenticación de los usuarios registrados en la red para impedir el acceso de usuarios no autorizados, de esta manera la integridad de la red se mantiene segura de manipulación no deseada.

BGP: Border Gateway Protocol es un protocolo que permite el intercambio de información de enrutamiento entre sistemas autónomos, seleccionando la ruta que tenga la menor cantidad posible de saltos entre sistemas. Es un protocolo altamente seguro y confiable.

EtherChannel: Es una agrupación lógica de enlaces ethernet físicos, para que se comporten como un solo canal sumando las capacidades de cada uno, resultando en un enlace troncal de mayor capacidad.

LACP: Es un protocolo que permite agrupar dos o más enlaces; este protocolo necesita que un extremo se configure en modo activo mientras que el otro extremo debe estar en modo pasivo.

Loopback: También es llamada “localhost”, es una dirección de bucle local muy útil verificar operatividad e red y para hacer diagnósticos; es una dirección ip reservada para tareas locales.

OSPF: Open Shortest Path First, o el camino más corto primero, es un protocolo que selecciona la mejor ruta que puede tomar un paquete al ser enviado a través de la red basándose en el menor costo y el mayor ancho de banda.

RESUMEN

Este diplomado de CCNP licenciado por Cisco condensa el desafío de darle solución a una prueba de habilidades prácticas, prueba que consiste en la configuración y puesta en servicio de un escenario propuesto, con unos requerimientos específicos y listados, que deben ser configurado desde cero, desde la configuración básica de cada uno de los equipos involucrados hasta las configuraciones finales de seguridad, con el apoyo de los conocimientos adquiridos durante los cursos previamente aprobados.

La configuración esperada al final de la prueba no dista de las soluciones que se deben implementar en entornos prácticos reales, donde se deben manejar conceptos claros y lógicos sobre las diferentes técnicas de enrutamiento, tales como OSPF y BGP, y el conocimiento de la operación de los diferentes protocolos necesariamente involucrados en la correcta configuración de los router y de los switches de capa 3.

Al ser desarrollado en un entorno totalmente simulado, los resultados se entregan en forma de capturas de pantalla que muestran los estados de los equipos virtual izados durante la simulación de la operación de la red propuesta.

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

ABSTRACT

This Cisco-licensed CCNP diploma condenses the challenge of solving a practical skills test, a test that consists of the configuration and commissioning of a proposed scenario, with specific requirements and lists, which must be programmed from scratch, from the basic configuration of each of the teams involved, up to the final security configurations, with the support of the knowledge acquired during the previously approved courses.

The expected configuration at the end of the test is not far from the solutions that must be implemented in real practical environments, where clear and logical concepts must be handled on the different routing techniques, such as OSPF and BGP, and the knowledge of the operation of the different ones necessarily involved in the correct configuration of the routers and Layer 3 switches.

Being developed in a fully simulated environment, the results are delivered in the form of screen captures that show the states of the virtual equipment hoisted during the simulation of the operation of the proposed network.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

Este diplomado de profundización de Cisco CCNP (Cisco Enterprise Network Core Technologies), ofrecido como requisito previo para recibir el título de Ingeniero de Telecomunicaciones, está orientado al desarrollo de las habilidades prácticas necesarias para diseñar y poner en marcha sistemas de redes de comunicaciones cableadas e inalámbricas, siguiendo el manual de buenas prácticas implementado por Cisco para cumplir con estándares de seguridad y calidad exigidos a nivel empresarial.

Para este caso en particular, se dará solución a un reto o desafío de conocimientos y habilidades que implica la configuración de la red WAN de una determinada empresa, con unos requerimientos específicos y particulares, siguiendo un orden lógico durante la ejecución de cada una de las tareas necesarias para dar solución al problema.

En la primera parte se hacen las configuraciones básicas de los equipos involucrados para poder iniciar su operación, en la siguiente etapa se configura la capa 2 de la red para que los host puedan recibir direccionamiento, seguidamente se implementan los protocolos de enrutamiento OSPF para poder después configurar un mecanismo de redundancia que ofrezca robustez a la red, seguidamente se hacen las configuraciones de seguridad configurando un servidor Radius e implementando un protocolo de autenticación aaa, antes de definir los mecanismos de administración de la red; al final se muestran capturas de pantalla con evidencias de conectividad entre los diferentes hosts y demás dispositivos.

ESCENARIO PROPUESTO

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. Se verificará que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere.

Topología Propuesta.
La figura 1 muestra la topología de red propuesta para el escenario 1.

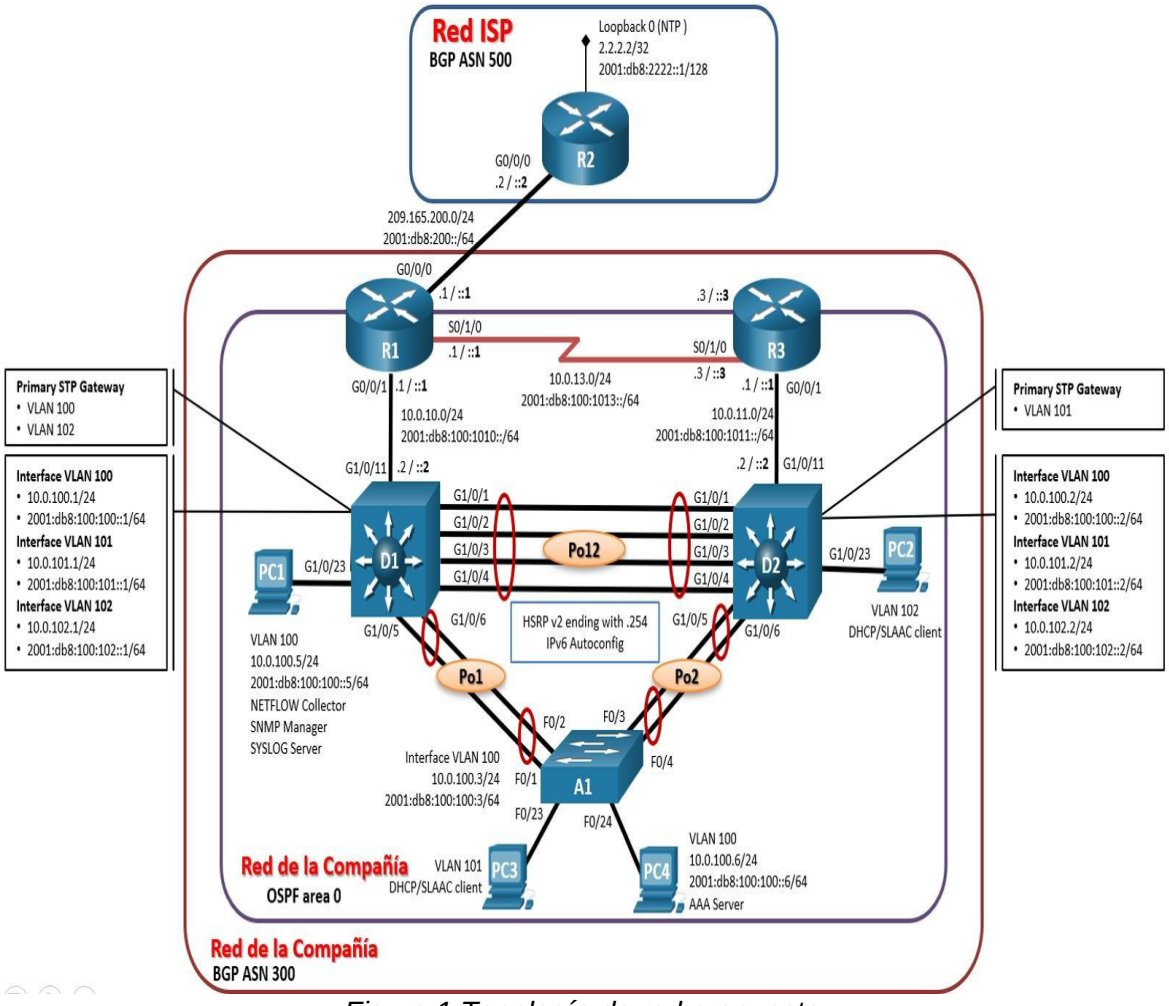

Figura 1 Topología de red propuesta.

Tabla de direccionamiento propuesta.
La tabla 1 muestra el direccionamiento propuesto para desarrollar el escenario 1.

Tabla 1. Direccionamiento IPv4 e IPv6

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	E0/0	209.165.200.1/24	2001:db8:200::1/64	fe80::1:1
	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E0/0	209.165.200.2/24	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E2/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E2/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	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

Lista de equipos utilizados para implementar la simulación por medio del software GNS3 version 2.2.4 y la máquina virtual VMWare Workstation version 15.5

Tabla 2 Lista de equipos utilizados para la simulación GNS3

Nombre	**Descripción**	**Version - Imagen**
Router R1	Router IOU L3	(i86bi_linux-adventerprisek9-ms.155-2.T.bin
Router R2	Router IOU L3	(i86bi_linux-adventerprisek9-ms.155-2.T.bin
Router R3	Router IOU L3	(i86bi_linux-adventerprisek9-ms.155-2.T.bin
Switch D1	Switch IOU L2	i86bi-linux-l2-adventerprisek9-15.2d.bin
Switch D2	Switch IOU L2	i86bi-linux-l2-adventerprisek9-15.2d.bin
Switch A1	Switch IOU L2	i86bi-linux-l2-adventerprisek9-15.2d.bin
Host PC1	PC VPC de GNS3	Virtual PC
Host PC2	PC VPC de GNS3	Virtual PC
Host PC3	PC VPC de GNS3	Virtual PC
Host PC4	PC VPC de GNS3	Virtual PC

El escenario se desarrollará y simulará totalmente con el software GNS3 con el apoyo de las imágenes Cisco IOU L2 (i86bi-linux-l2-adventerprisek9-15.2d.bin) que corresponde a un switch multicapa, y Cisco IOU L3 (i86bi_linux-adventerprisek9-ms.155-2.T.bin) que corresponde a un router.

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

En la primera parte se construye la red y se configuran los parámetros básicos de los dispositivos, así como el direccionamiento de cada una de las interfaces presentes.

La figura 2 muestra la topología de red construida en la plataforma de GNS3.

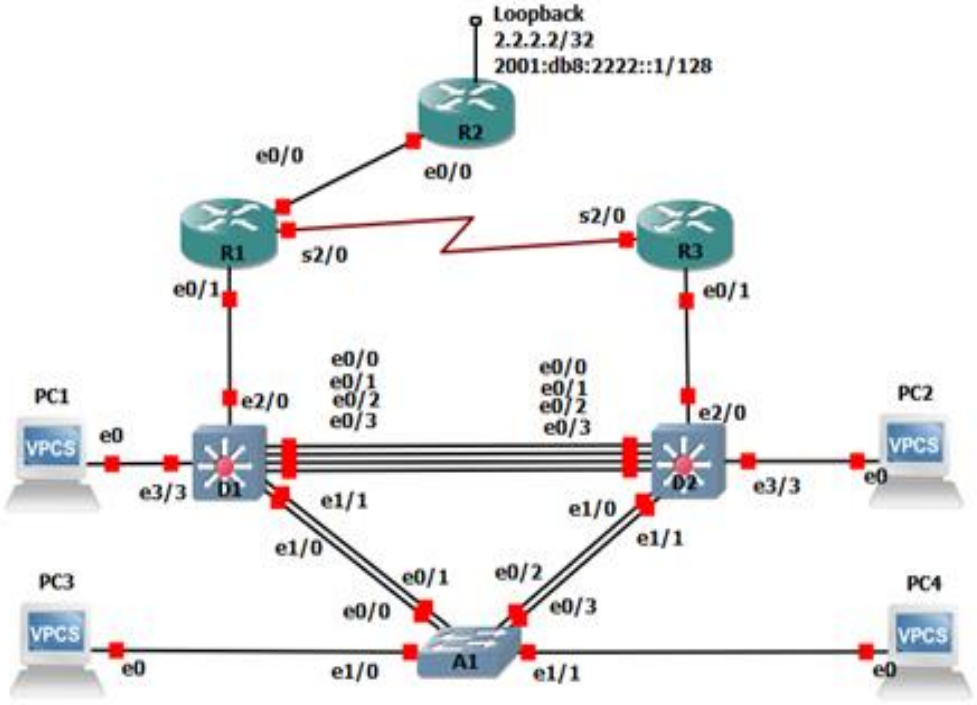

Figura 2 Montaje en GNS3

1.1 Configuraciones Iniciales.

A continuación, se listan los comandos necesarios para la configuración inicial de cada dispositivo. Y al frente se podrá leer una breve descripción de la función de cada línea de comandos. La descripción o comentarios de los comandos no se hará repetitiva para comandos repetidos; los comandos son iguales y se comportan igual en todos los dispositivos.

Configuración inicial para el router R1.

IOU1#config ter *#se ingresa al modo de configuración global*
IOU1(config)#hostname R1 *#Se define R1 como para el nombre del router*
R1(config)#ipv6 unicast-routing *#Se activa el direccionamiento IPv6*
R1(config)#no ip domain lookup *# desactiva la traducción de nombres a dirección del dispositivo*

```
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #   #Se define
      mensaje de bienvenida a la interfaz de configuración
R1(config)#line con 0          #Ingreso al modo de conf. de línea de consola
R1(config-line)# exec-timeout 0 0     #Se deshabilita la desconexión de CLI por inactividad
R1(config-line)# logging synchronous          #Para evitar que mensajes en pantalla
      afecten el ingreso de comandos nuevos
R1(config-line)# exit
R1(config)#interface e0/0      #Ingreso a la conf. De la interface E0/0
R1(config-if)# ip address 209.165.200.1 255.255.255.0      #Se asigna dir. IPv4 a la
      interface E0/0
R1(config-if)# ipv6 address fe80::1:1 link-local        #Se asigna dir. Link-local IPv6 a la
      interface E0/0
R1(config-if)# ipv6 address 2001:db8:200::1/64      #Se asigna dir. IPv6 a la interface
      E0/0
R1(config-if)# no shutdown    #Se activa la interface E0/0
R1(config-if)# exit
R1(config)#interface e0/1      #Ingreso a la conf. De la interface E0/1 para asignar dir.
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      #Ingreso a la conf. De la interface E0/1 para asignar dir.
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(config)#do write    #Se graba la información ingresada en el archivo running-config
R1(config)#copy running-config startup-config
```

Configuración inicial para el router R2:

```
IOU2#config term
IOU2(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)#exit
R2(config)#interface e0/0      #Ingreso a la conf. De la interface E0/0 para asignar dir.
R2(config-if)#ip address 209.165.200.2 255.255.255.0
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      #Ingreso a la conf. De la interface Loopback para
      asignar direccionamiento IPv4 e IPv6.
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(config)#do write
R2(config)#do copy running-config startup-config
```

Configuración inicial para el router R3:

```
IOU3#conf term
IOU3(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       #Ingreso a la conf. De la interface E0/1 para asignar dir.
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       #Ingreso a la conf. De la interface S2/0 para asignar dir.
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#write
R3#copy running-config startup-config
```

Configuración inicial para el switch de capa 3 D1:

```
IOU4#config term
IOU4(config)#hostname D1
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   #Se crea la vlan 100
D1(config-vlan)#name Management  #Se asigna nombre a la vlan 100
D1(config-vlan)#exit
D1(config)#vlan 101   #Se crea la vlan 101
D1(config-vlan)#name UserGroupA  #Se asigna nombre a la vlan 101
D1(config-vlan)#exit
```

```
D1(config)#vlan 102   #Se crea la vlan
D1(config-vlan)#name UserGroupB  #Se asigna nombre a la vlan 102
D1(config-vlan)#exit
D1(config)#vlan 999   #Se crea la vlan 999
D1(config-vlan)#name NATIVE                #Se asigna nombre a la vlan 999
D1(config-vlan)#exit
D1(config)#interface e2/0      #Ingreso a la conf. De la interface E2/0 para asignar dir.
D1(config-if)#no switchport
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 100#Ingreso a la conf. De la vlan 100 para asignar dir.
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 101#Ingreso a la conf. De la vlan 101 para asignar dir.
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#interface vlan 102#Ingreso a la conf. De la vlan 102 para asignar dir.
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
      #El rango de direcciones de vlan 101 descrito se excluye del direccionamiento
      dhcp.
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
      #El rango de direcciones de vlan 101 descrito se excluye del direccionamiento
      dhcp.
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
      #El rango de direcciones de vlan 101 descrito se excluye del direccionamiento
      dhcp.
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
      #El rango de direcciones de vlan 102 descrito se excluye del direccionamiento
      dhcp.
D1(config)#ip dhcp pool VLAN-101           #se crea pool dhcp para vlan 101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102           #se crea pool dhcp para vlan 101
```

```
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, e2/1-3, e3/0-3
D1(config-if-range)#shutdown          #Se desactiva el rango de interfaces descrito.
D1(config-if-range)#exit
D1(config)#do write
D1(config)# do copy running-config startup-config
```

Configuración inicial para el switch de capa 3 D2:

```
IOU5#config term
IOU5(config)#hostname D2
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 e2/0
D2(config-if)#no switchport
D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
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, e2/1-3, e3/0-3
D2(config-if-range)#shutdown
D2(config-if-range)#exit
D2#write
D2#copy running-config startup-config
```

Configuración inicial para el switch de capa 2 A1:

```
IOU6#conf term
IOU6(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 e1/2-3
A1(config-if-range)#shutdown
A1(config-if-range)#exit
A1(config)#do write
A1(config)#do copy running-config startup-config
```

Configuración inicial para el host PC1:

```
PC1> ip 10.0.100.5/24 10.0.100.254 #se asigna dir. IPv4 estática
PC1> ip 2001:db8:100:100::5/64 EUI-64      #se asigna dir. IPv6 estática
```

Configuración inicial para el host PC4:

```
PC4> ip 10.0.100.6/24 10.0.100.254 #se asigna dir. IPv4 estática
PC4> ip 2001:db8:100:100::6/64 EUI-64      #se asigna dir. IPv6 estática
```

1.2 Evidencias de la configuración inicial de los dispositivos.

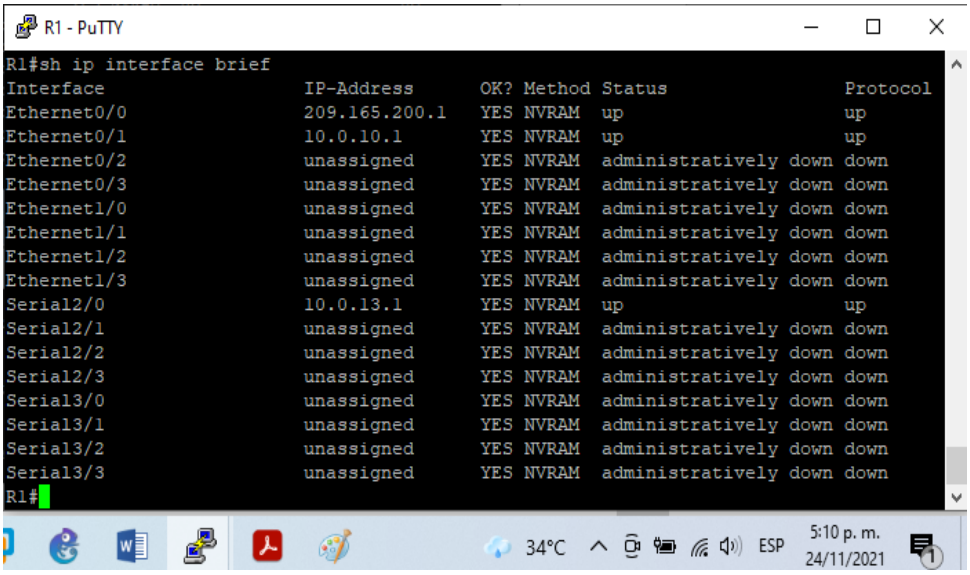

Figura 3 Lista de interfaces configuradas en R1.

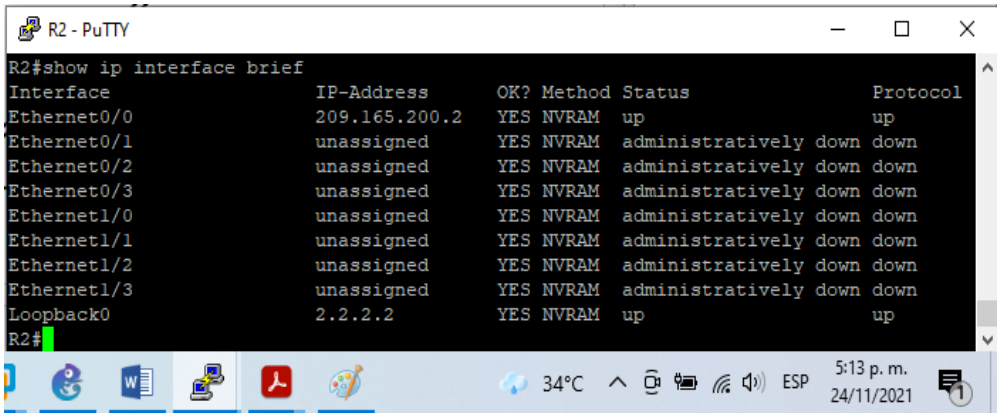

Figura 4 Lista de interfaces configuradas en R2.

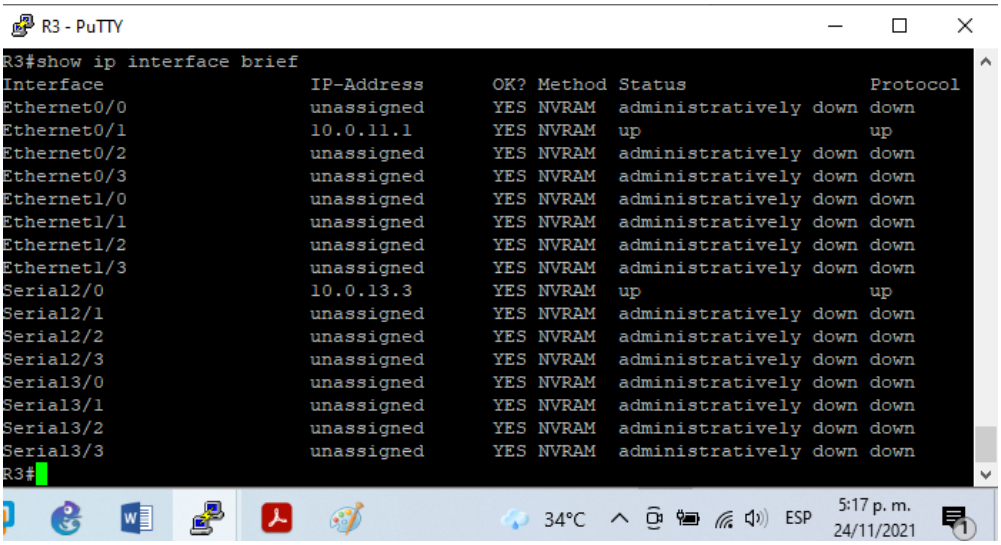

Figura 5 Lista de interfaces configuradas en R3.

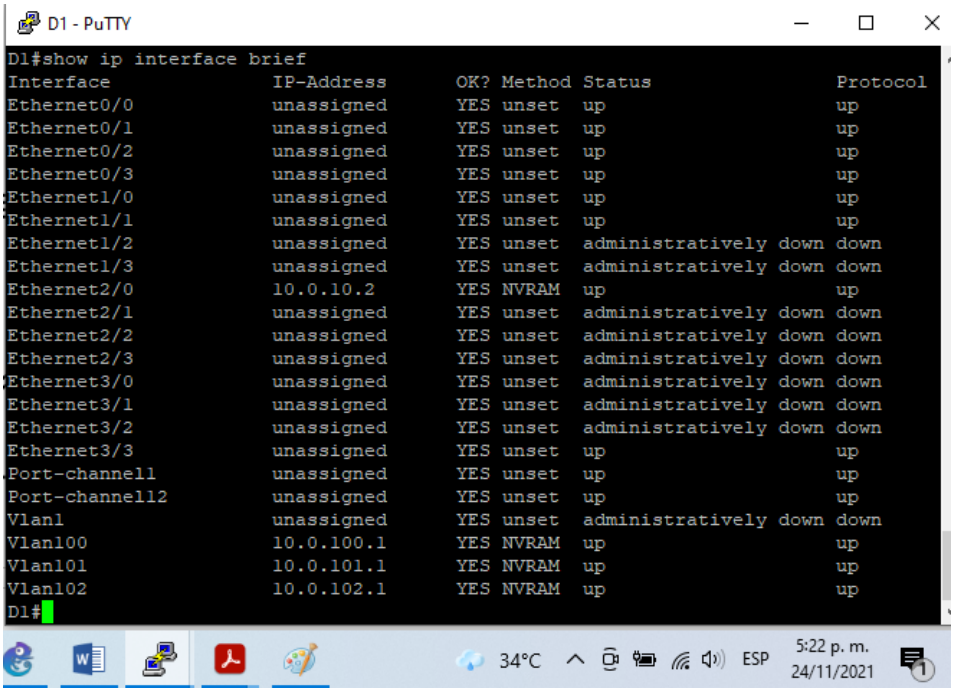

Figura 6 Lista de interfaces Configuradas en D1.

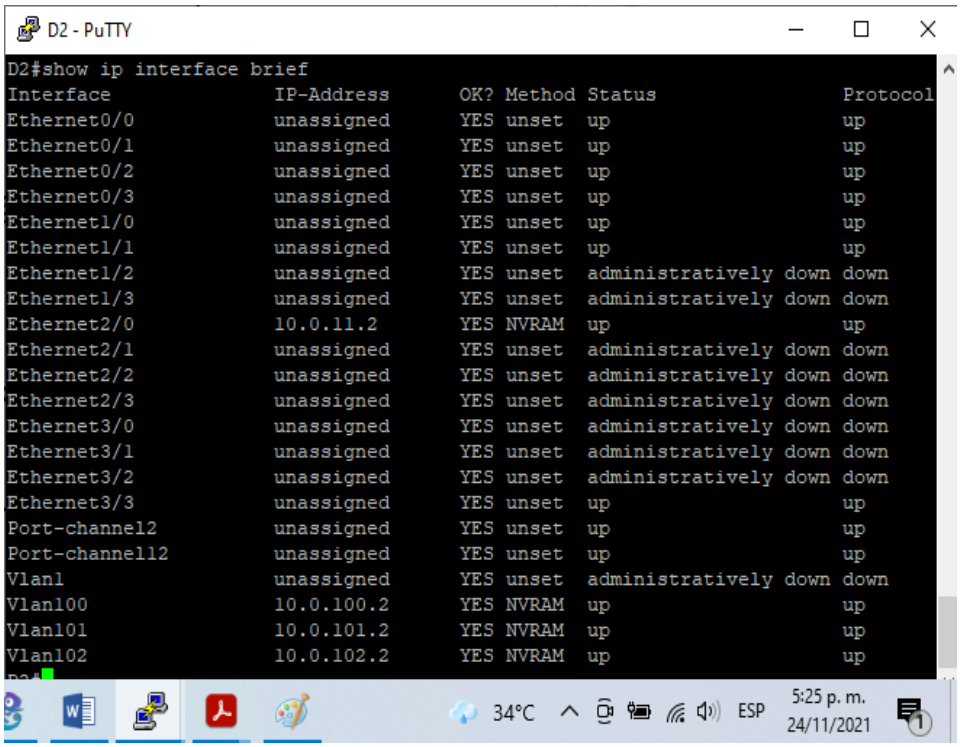

Figura 7 Lista de interfaces configuradas en D2.

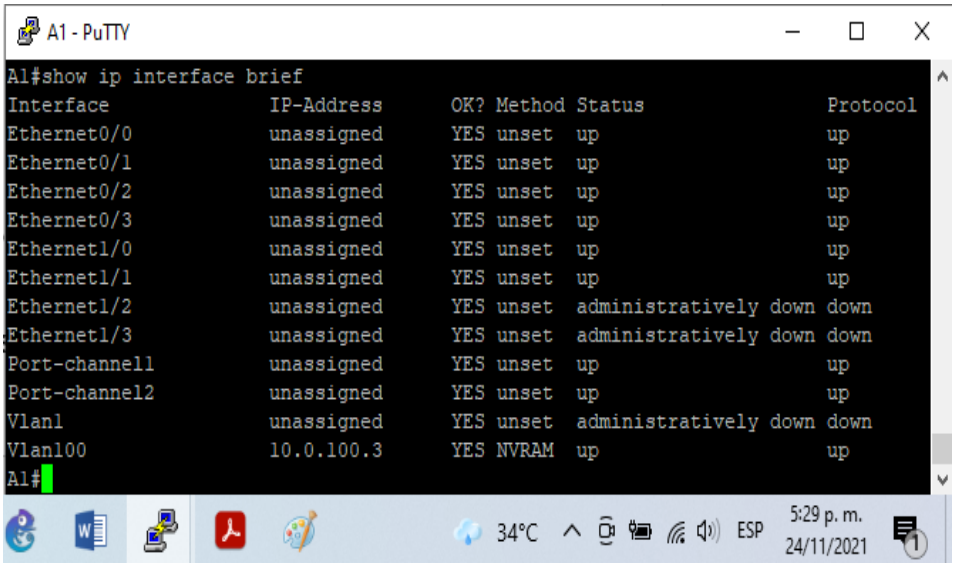

Figura 8 Lista de interfaces configuradas en A1.

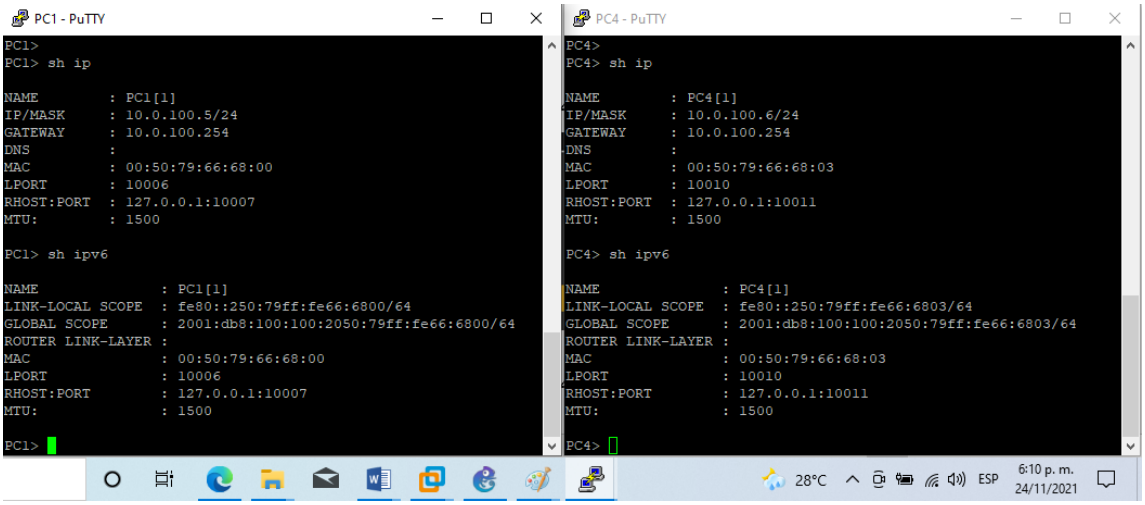

Figura 9 Direccionamiento de PC1 y PC4.

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

En la segunda parte se hace la configuración de la capa 2 de la red y el soporte de host para que todos los switches puedan comunicarse y a su vez los PC2 y PC3 reciban direccionamiento DHCP y SLAAC.

2.1 Configuración de interfaces troncales
Se configuran interfaces troncales para habilitar los enlaces de interconexión entre los switches D1-D2, D1-A1 y D2-A1.

Comandos para configurar interfaces troncales en D1:
D1(config)#int range e0/0-3, e1/0-1 *#Se define el rango de interfaces para la troncal#*
D1(config-if-range)#switchport trunk encapsulation dot1q *#Se define troncal IEEE 802.1Q#*
D1(config-if-range)#switchport mode trunk *#Se pasan las interfaces al modo trunk#.*
D1(config-if-range)#exit

Comandos para configurar interfaces troncales en D2:
D2(config)#int range e0/0-3, e1/0-1
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#exit

Comandos para configurar interfaces troncales en A1:
A1(config)#int range e0/0-3
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#exit

En cada dispositivo se puede verificar la creación de switchport en modo troncal con la instrucción: *show interface switchport | section trunk*

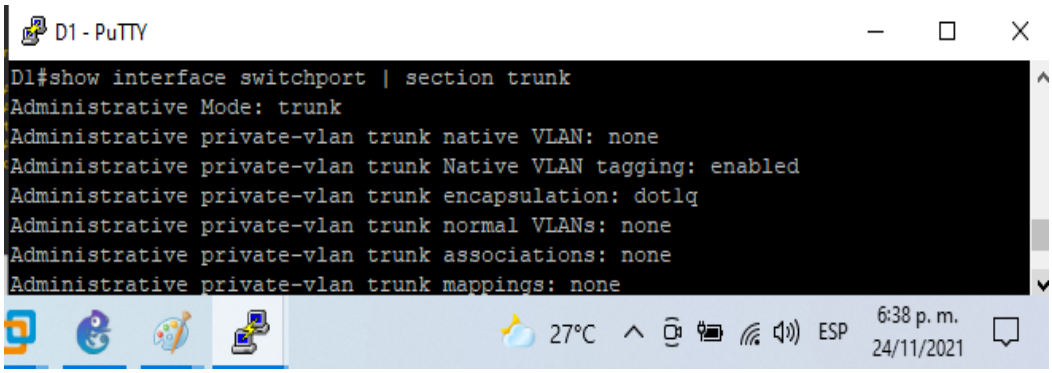

Figura 10 Verificación de troncales en D1.

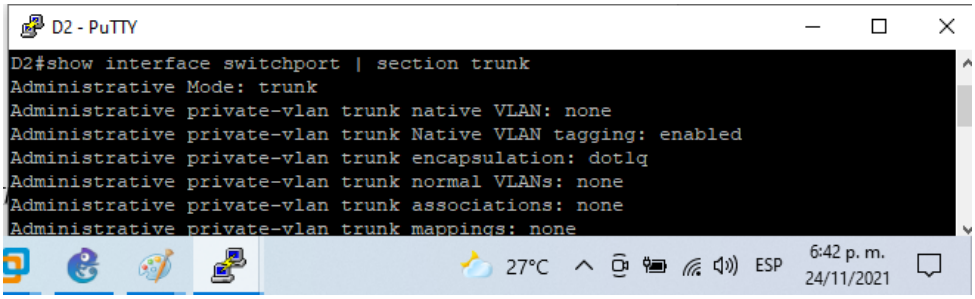

Figura 11 Verificación de troncales en D2.

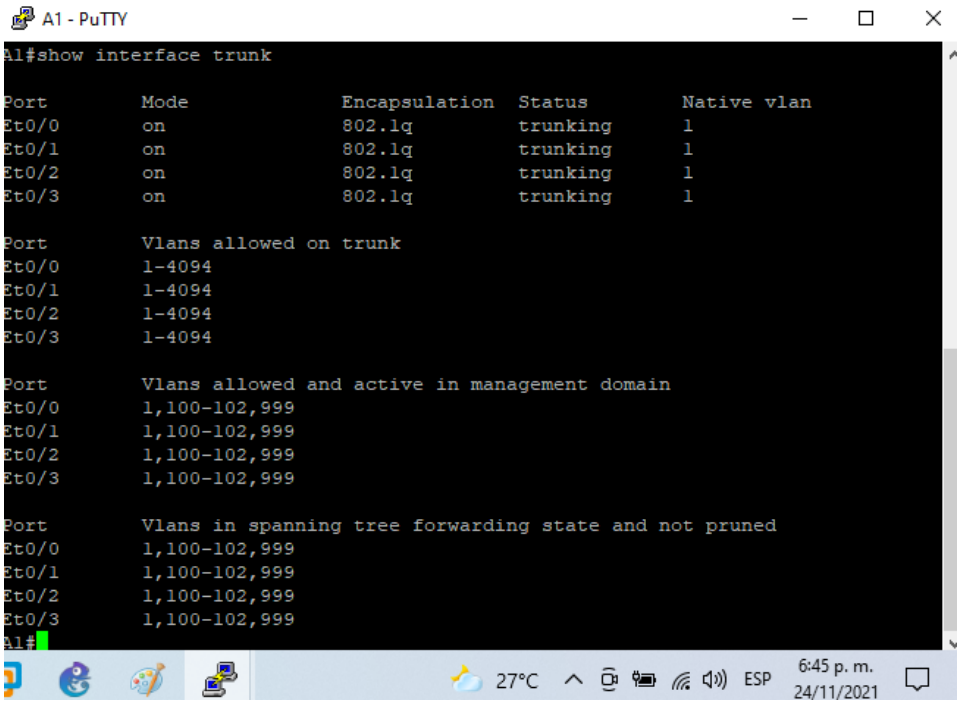

Figura 12 Verificación de troncales en A1.

2.2 Cambio de VLAN nativa en los enlaces troncales
Se usa la VLAN 999 como la VLAN nativa.

Comandos para cambiar la vlan nativa en D1:
D1(config)#int range e0/0-3, e1/0-1
D1(config-if-range)#switchport trunk native vlan 999 *#Se hace el cambio de la vlan 999 a la vlan native#*
D1(config-if-range)#exit
Código para cambiar la vlan nativa en D2:
D2(config)#int range e0/0-3, e1/0-1
D2(config-if-range)#switchport trunk native vlan 999

Comandos para cambiar la vlan nativa en A1:
A1(config)#int range e0/0-3

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

2.3 Configuración del protocolo Rapid Spanning-Tree (RSTP) en todos los switch.

Comandos para configurar RSTP en D1:
D1(config)#spanning-tree mode rapid-pvst

Comandos para configurar RSTP en D2:
D1(config)#spanning-tree mode rapid-pvst

Comandos para configurar RSTP en A1:
A1(config)#spanning-tree mode rapid-pvst

2.4 Configuración de los puentes raíz RSTP (root bridges) en D1 y D2
Configuración de D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch. D1 y D2 proporcionarán respaldo si falla el puente raíz (root bridge).

Comandos para configurar puentes raíz RSTP en D1:
D1(config)#spanning-tree vlan 100 root primary *#Se define vlan 100 como primaria dentro de RSTP#*
D1(config)#spanning-tree vlan 102 root primary *#Se define vlan 102 como primaria dentro de RSTP#*
D1(config)#spanning-tree vlan 101 root secondary *#Se define vlan 101 como secundaria dentro de RSTP#*

Comandos para configurar puentes raíz RSTP en D2:
D2(config)#spanning-tree vlan 101 root primary
D1(config)#spanning-tree vlan 100 root secondary
D2(config)#spanning-tree vlan 102 root secondary

Con el comando *show run | include spanning-tree* en cada dispositivo se puede verificar la configuración del protocolo RSTP y la asignación de prioridades a las vlan.

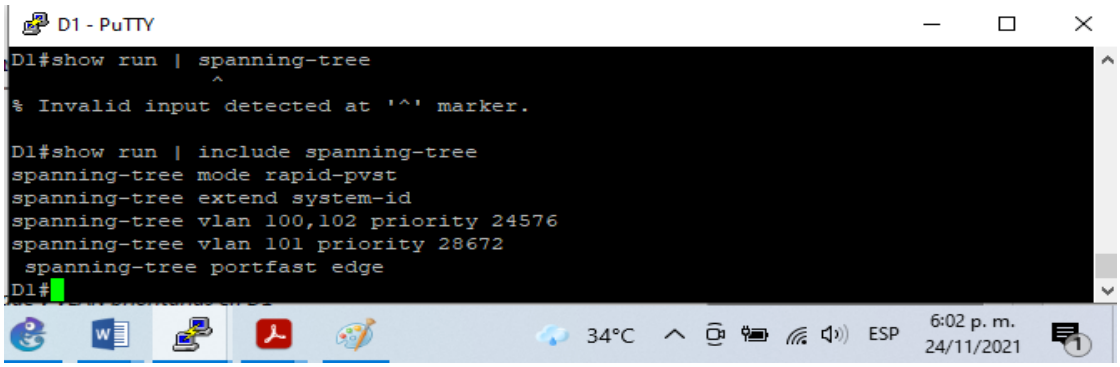

Figura 13 Verificación de protocolo RSTP en D1, D2 y A1.

2.5 Creación de EtherChannel LACP en todos los switch
Se usarán los siguientes números de canales:
D1 a D2 Port channel 12
D1 a A1 Port channel 1
D2 a A1 Port channel 2
En todos los switches se habilita el protocolo Rapid Spanning-Tree (RSTP) y se crean EtherChannels LACP entre D1-D2, D1-A1 y D2-A1.

Comandos para crear EtherChannel LACP y Port-Channel 12 de D1 a D2 en D1:

```
D1(config)#int range e0/0-3              #Se ingresa al rango de interfaces seleccionadas#
D1(config-if-range)#channel-protocol lacp    #Se activa el protocolo EtherChannel LACP#
D1(config-if-range)#channel-group 12 mode active  #Se define el canal 12 en modo
      activo#
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#int port-channel 12          #Se ingresa a la configuración del canal 12#
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#exit
D1(config)#
```

Comandos para crear EtherChannel LACP y Port-Channel 12 de D1 a D2 en D2:

```
D2(config)#int range e0/0-3
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 12 mode passive                #Se define el canal 12
      en modo pasivo#
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#int port-channel 12
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#exit
D2(config)#
```

Comandos para crear EtherChannel LACP y Port-Channel 1 de D1 a A1 en D1:

```
D1(config)#int range e1/0-1
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-group 1 mode active    #Se define el canal 1 en modo activo#
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#int port-channel 1
D1(config-if)#switchport trunk encapsulation dot1q
D1(config-if)#switchport mode trunk
D1(config-if)#switchport mode trunk
D1(config-if)#exit
D1(config)#
```

Comandos para crear EtherChannel LACP y Port-Channel 1 de D1 a A1 en A1:

```
A1(config)#int range e0/0-1
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 1 mode passive #Se define el canal 1 en modo pasivo#
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#int port-channel 1
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
A1(config-if)#exit
A1(config)#
```

Comandos para crear EtherChannel LACP y Port-Channel 2 de D2 a A1 en D2:

```
D2(config)#int range e1/0-1
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 2 mode active    #Se define el canal 2 en modo activo#
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#int port-channel 2
D2(config-if)#switchport trunk encapsulation dot1q
D2(config-if)#switchport mode trunk
D2(config-if)#exit
D2(config)#
```

Comandos para crear EtherChannel LACP y Port-Channel 2 de D2 a A1 en A1:

```
A1(config)#int range e0/2-3
A1(config-if-range)#channel-protocol lacp
A1(config-if-range)#channel-group 2 mode passive #Se define el canal 2 en modo pasivo#
A1(config-if-range)#exit
A1(config)#int port-channel 2
A1(config-if)#switchport trunk encapsulation dot1q
A1(config-if)#switchport mode trunk
A1(config-if)#exit
A1(config)#
```

Con el comando *show etherchannel summary* en cada dispositivo se puede verificar la creación y configuración de los canales 1 y 12 en D1, 2 y 12 en D2, y 1 y 2 en A1.

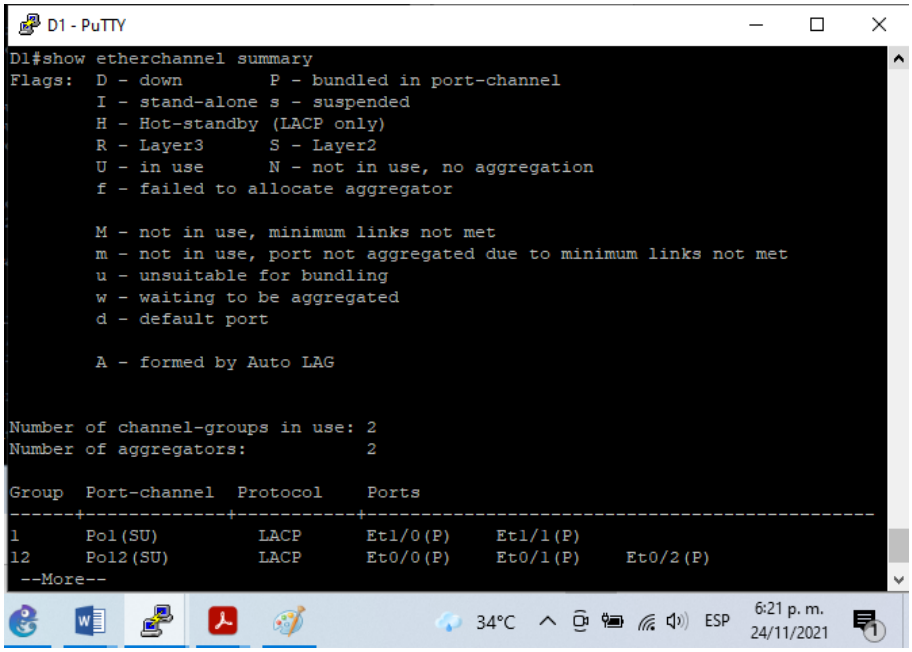

Figura 14 Verificación de EtherChannel en D1.

2.6 Configuración en todos los switch de los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.
Los puertos de host pasarán inmediatamente al estado de reenvío (forwarding).

Configuración de puertos de acceso para los hosts.
Se configuran en D1, D2 y A1 los puertos de acceso para los hosts PC1, PC2, PC3 y PC4
Comandos para configurar puertos de acceso en D1
D1(config)#int e3/3
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100 *#Se permite el acceso de PC1 a la vlan 100#*
D1(config-if)#spanning-tree portfast *#Se activa el forwarding#*
D1(config-if)#no shutdown

Comandos para configurar puertos de acceso en D2
D2(config)#int e3/3
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102 *#Se permite el acceso de PC2 a la vlan 102#*
D2(config-if)#spanning-tree portfast *#Se activa el forwarding#*
D2(config-if)#no shutdown

Comandos para configurar puertos de acceso en A1
A1(config)#int e1/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101 *#Se permite el acceso de PC3 a la vlan 101#*
A1(config-if)#spanning-tree portfast *#Se activa el forwarding#*

A1(config-if)#no shutdown
A1(config)#int e1/1
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100 *#Se permite el acceso de PC4 a la vlan 100#*
A2(config-if)#spanning-tree portfast *#Se activa el forwarding#*
A1(config-if)#no shutdown

PC2>ip dhcp *#PC2 recibirá direccionamiento dhcp y slaac#*
PC2>save

PC3>ip dhcp *#PC2 recibirá direccionamiento dhcp y slaac#*
PC3>save

Verificación de conectividad entre los hosts y la vlan100, 102 y 102 en D1 y D2 por medio de comandos ping:

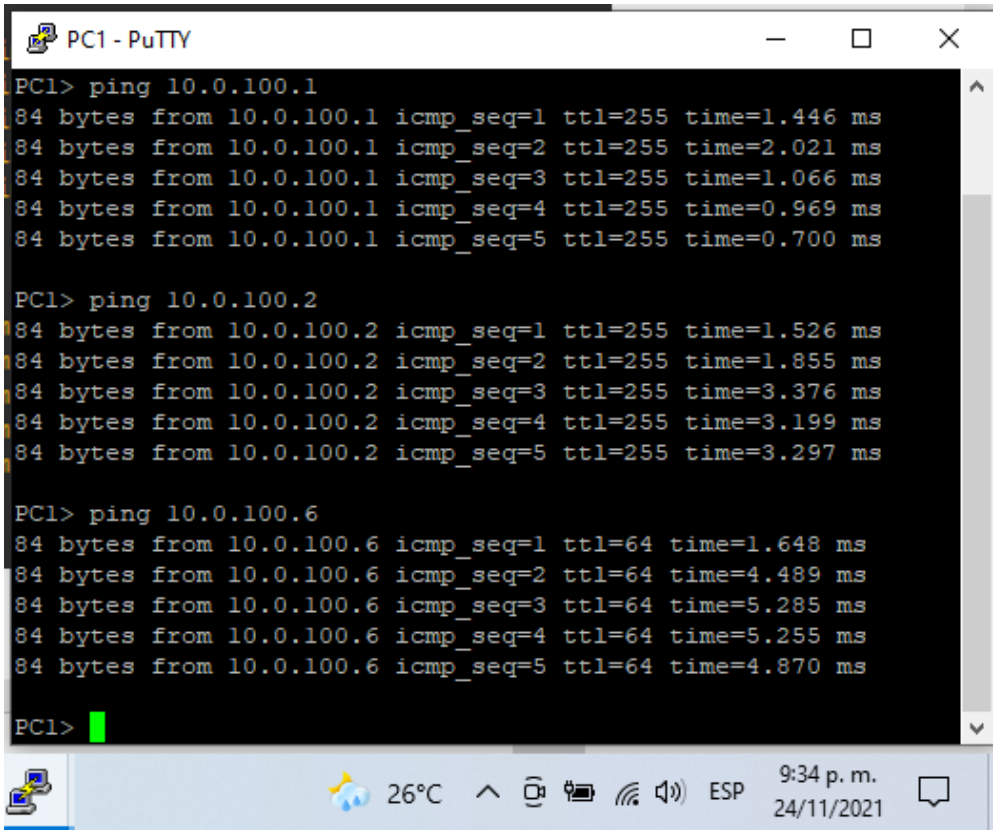

Figura 15 Verificación de ping de PC1 a vlan100 en D1 y D2, y ping a PC4.

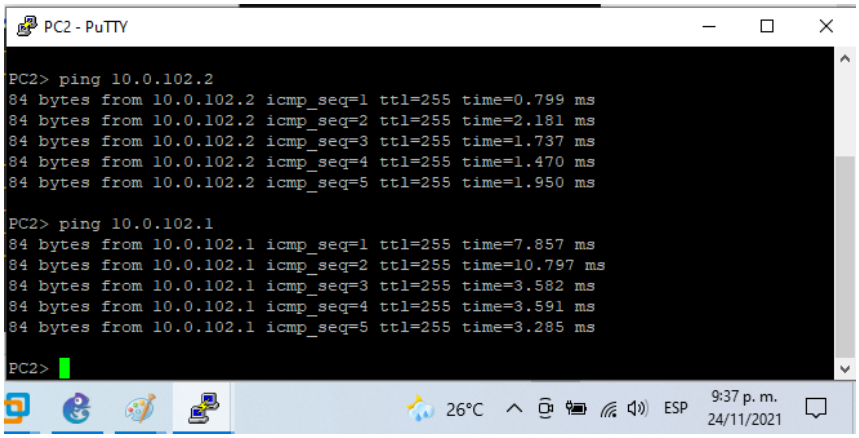

Figura 16 Verificación de ping de PC2 a vlan102 en D1 y D2.

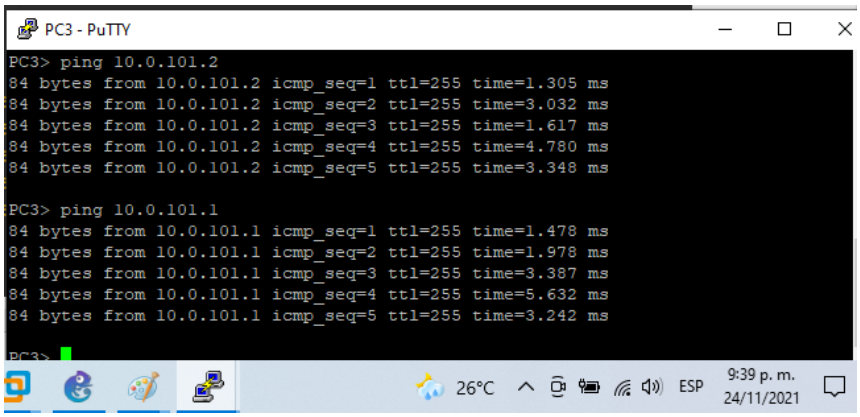

Figura 17 Verificación de ping de PC3 a vlan101 en D1 y D2.

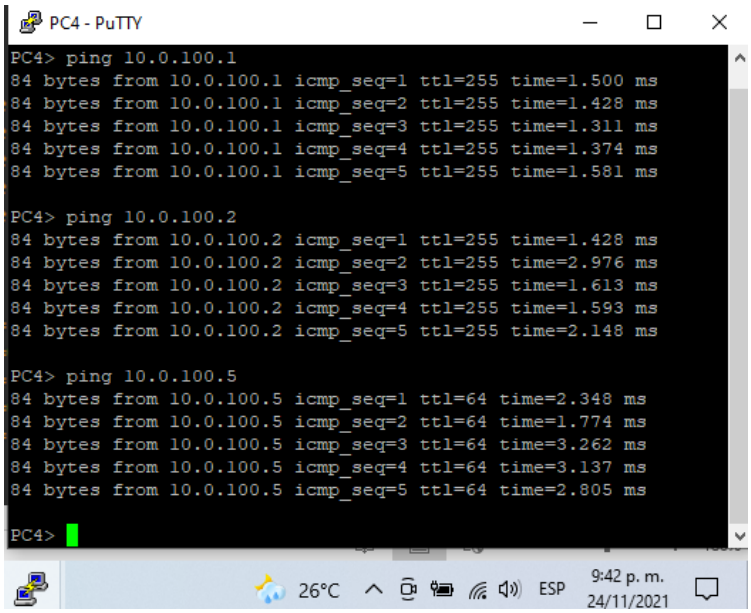

Figura 18 Verificación de ping de PC4 a vlan100 en D1 y D2, y ping a PC1.

Parte 3: Configurar los protocolos de enrutamiento

En esta parte se configuran los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red será completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 serán ser exitosos.
Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

3.1 Configuración de OSPFv2

En la "Red de la Compañía" (es decir, R1, R3, D1, y D2), se configura single- área OSPFv2 en área 0 con las siguientes especificaciones:
Se usa OSPF Process ID 4 y se asignan 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, se anuncian todas las redes directamente conectadas/ VLANs en Área 0.

- En R1, no se publica la red R1 – R2.
- En R1, se propaga una ruta por defecto provista por BGP.

Se deshabilitan las publicaciones OSPFv2 en:

- D1: En todas las interfaces excepto e2/0
- D2: En todas las interfaces excepto e2/0

Comandos para la configuración OSPFv2 en R1:

```
R1(config)#router ospf 4        #Se crea el proceso ospf 4 para R1#
R1(config-router)#router-id 0.0.4.1    #Se identifica R1 dentro de ospf 4#
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0        #se anuncia red R1-D1 en
        Area 0#
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0        #se anuncia red R1-R3 en
        Area 0
R1(config-router)#defaul-information originate        #Se propaga ruta por defecto BGP#
```

Comandos para la configuración OSPFv2 en R3:

```
R3(config)#router ospf 4        #Se crea el proceso ospf 4 para R3#
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0        #se anuncia red R3-D2 en
        Area 0#
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0        #se anuncia red R1-R1 en
        Area 0#
```

Comandos para la configuración OSPFv2 en D1:

```
D1(config)#router ospf 4        #Se crea el proceso ospf 4 para D1#
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
```

D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface e2/0

Comandos para la configuración OSPFv2 en D2:
D2(config)#router ospf 4 *#Se crea el proceso ospf 4 para D2#*
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.11.0 0.0.0.255 area0
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
D2(config-router)#passive-interface default *#Se deshabilitan publicaciones ospf para todas las interfaces#*
D2(config-router)#no passive-interface e2/0 *#Se habilitan publicaciones ospf para la interfaces E2/0#*

3.2 Configuración de OSPFv3
En la “Red de la Compañía” (R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0 con las siguientes especificaciones:
Se usa OSPF Process ID 6 y se asignan los siguientes router- IDs:

- R1: 0.0.6.1
- 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, se anuncian todas las redes directamente conectadas / VLANs en Area 0.
En R1, no se publica la red R1 – R2.
En R1, se propaga una ruta por defecto provista por BGP.
Se deshabilitan las publicaciones OSPFv3 en:

- D1: todas las interfaces excepto e2/0
- D2: todas las interfaces excepto e2/0

Comandos para la configuración OSPFv3 en R1:
R1(config)#ipv6 router ospf 6 *#Se crea el proceso ospf 6 para R1#*
R1(config-rtr)#router-id 0.0.6.1 *#Se identifica R1 dentro de ospf 6#*
R1(config-rtr)#default-information originate *#Se propaga ruta por defecto BGP#*
R1(config.rtr)#exit
R1(config)#interface e0/1
R1(config.if) ipv6 ospf 6 area 0 #Se a*nuncia en ospf 6 la red conectada en E0/1#*
R1(config-if)# exit
R1(config)#interface s2/0
R1(config.if) ipv6 ospf 6 area 0 #Se a*nuncia en ospf 6 la red conectada en S2/0#*

Comandos para la configuración OSPFv3 en R3:

```
R3(config)#ipv6 router ospf 6
R3(config-rtr)#router-id 0.0.6.2
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
```

Comandos para la configuración OSPFv3 en D1:

```
D1(config)#ipv6 router ospf 6
D1(config-rtr)#router-id 0.0.6.131
D1(config-rtr)#passive-interface default
D1(config-rtr)#no passive-interface e2/0
D1(config-rtr)#exit
D1(config)#int e2/0
D1(config-if)#ipv6 ospf 6 area 0
```

Comandos para la configuración OSPFv3 en D2:

```
D2(config)#ipv6 router ospf 6 #Se crea el proceso ospf 6 para D2#
D2(config-rtr)#router-id 0.0.6.132      #Se identifica D2 dentro de ospf 6#
D2(config-rtr)#passive-interface default      #Se deshabilitan publicaciones ospf para
      todas las interfaces#
D2(config-rtr)#no passive-interface e2/0      #Se habilitan publicaciones ospf para la
      interfaces E2/0#
D1(config-rtr)#exit
D2(config)#int e2/0
D2(config-if)#ipv6 ospf 6 area 0      #Se anuncia en ospf 6 la red conectada en E2/0#
D2(config-if)#exit
D2(config)#int vlan 100
D2(config-if)#ipv6 ospf 6 area 0      #Se anuncia en ospf 6 la red conectada en la vlan
      100#
D2(config-if)#exit
D2(config)#int vlan 101
D2(config-if)#ipv6 ospf 6 area 0      #Se anuncia en ospf 6 la red conectada en la vlan
      101#
D2(config-if)#exit
D2(config)#int vlan 102
D2(config-if)#ipv6 ospf 6 area 0      #Se anuncia en ospf 6 la red conectada en la vlan
      102#
D2(config-if)#exit
D1(config)#
```

Con el comando *show run | section ospf* se puede evidenciar la configuración de OSPF en cada dispositivo.

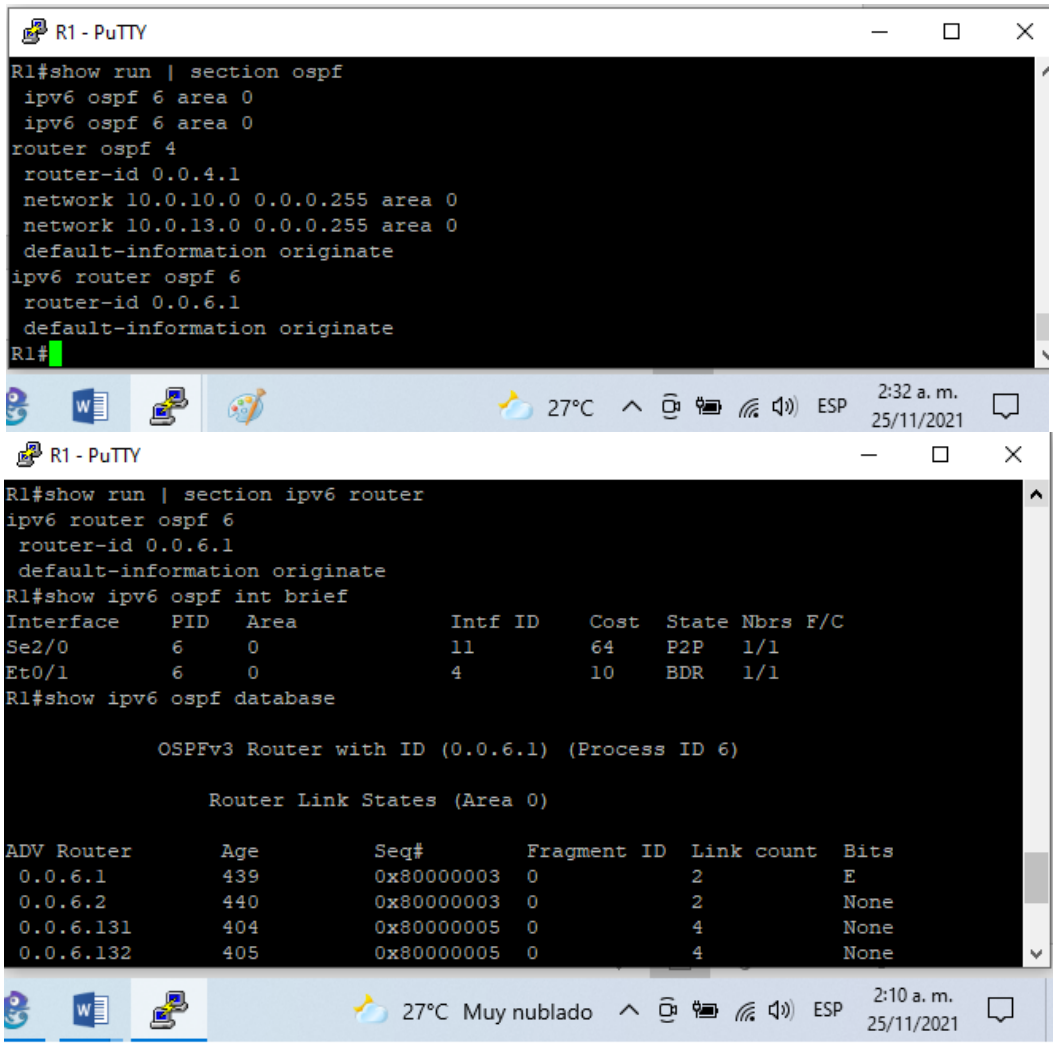

Figura 19 Verificación de ospf 4 y ospf 6 en R1.

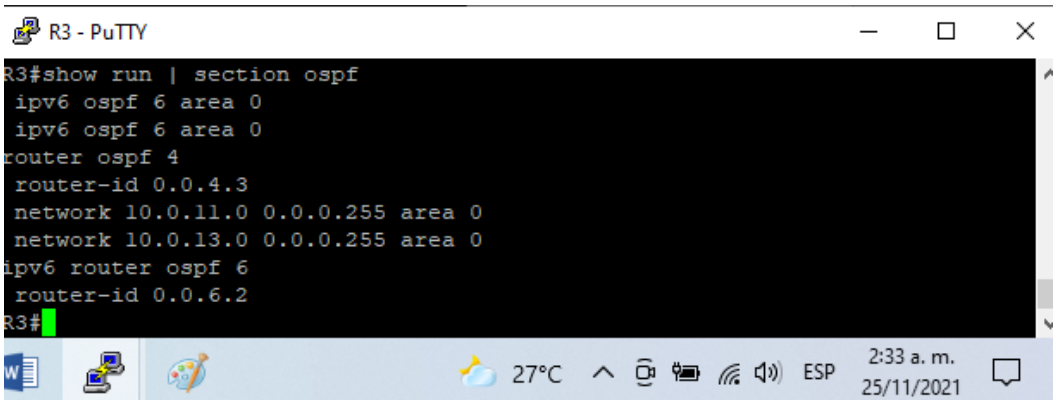

Figura 20 Verificación de ospf 6 en R3.

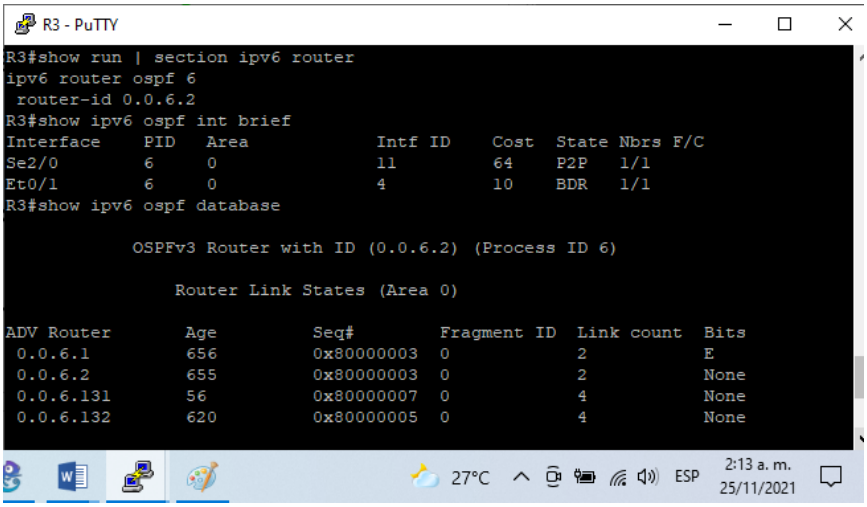

Figura 21 Verificación de OSPF en R3

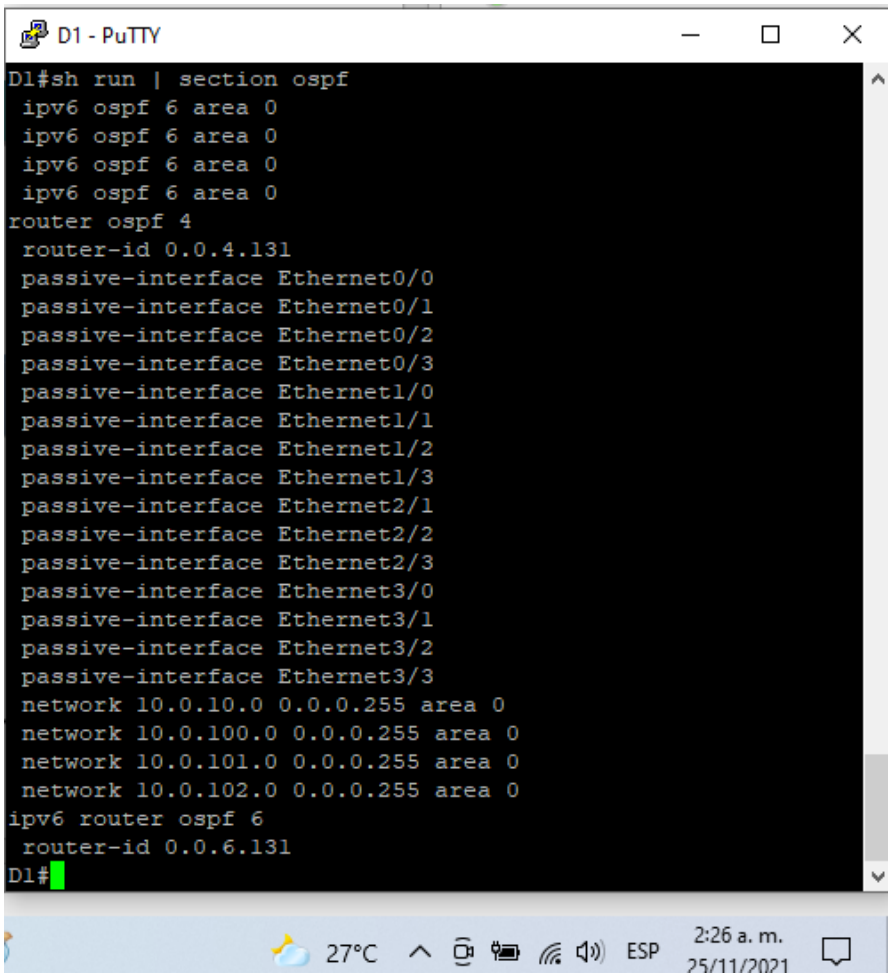

Figura 22 Verificación de OSPF en D1.

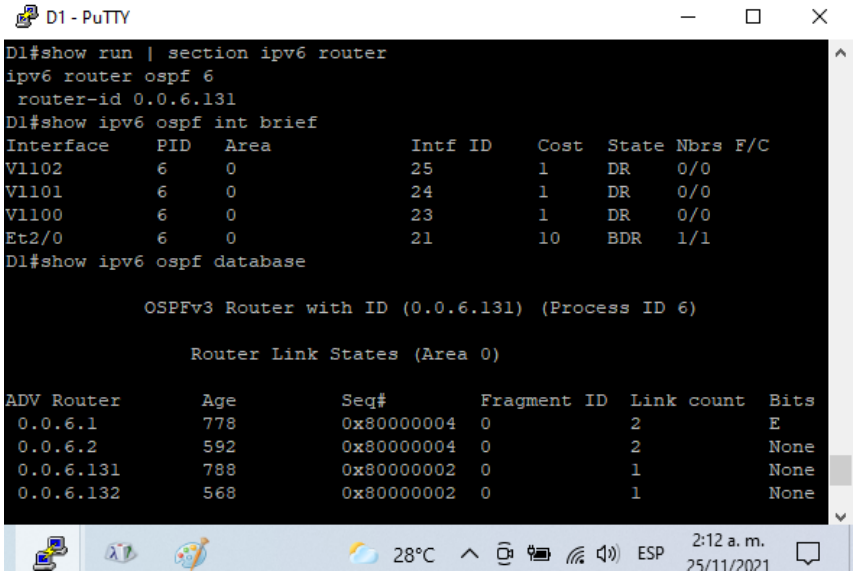

Figura 23 Verificación de Ospf en D1

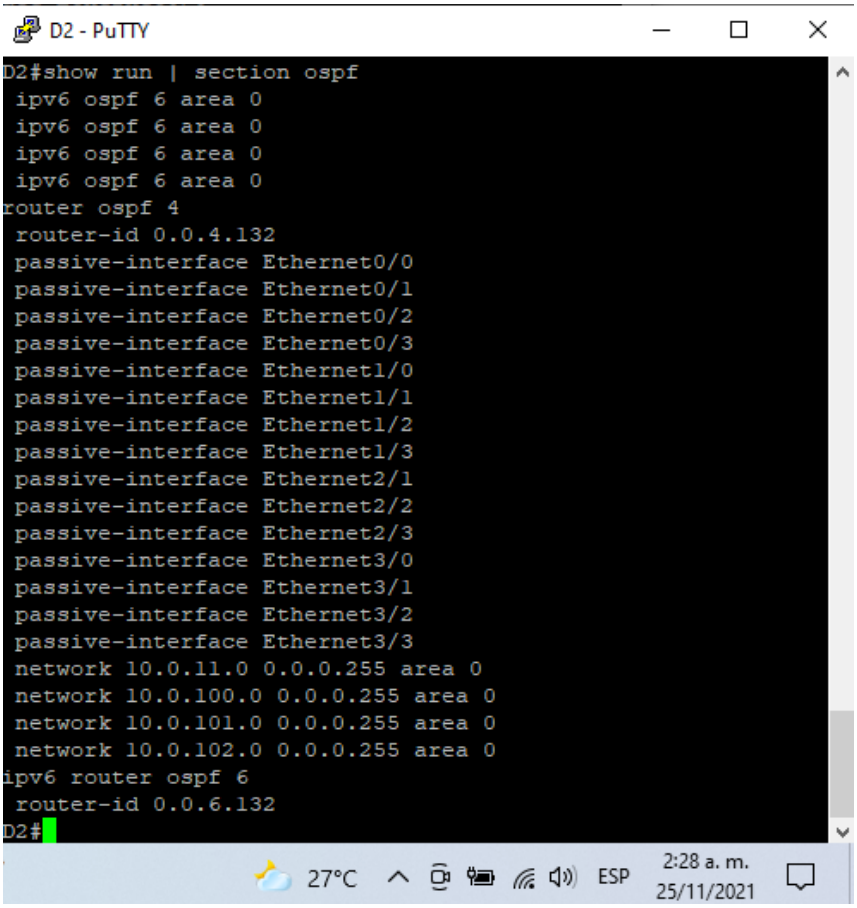

Figura 24 Verificación de Ospf en D2.

3.3 Configuración de MP-BGP en R2

En R2 en la “Red ISP”, se configura MP- BGP según las siguientes especificaciones:

Se configuran dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada IPv4.
- Una ruta estática predeterminada IPv6.

Se configura R2 en BGP ASN 500 usando el router-id 2.2.2.2.

Se configura y habilita una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

En IPv4 address family, se anuncia:

- La red Loopback 0 IPv4 (/32).
- La ruta por defecto (0.0.0.0/0).

En IPv6 address family, se anuncia:

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

Comandos para configurar BGP en R2:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 Loopback 0
R2(config)#ipv6 route ::/0 Loopback 0
        #Configuración de 2 rutas estáticas predeterminadas a través de Loopback#
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
        #Configuración de BGP en ANS 300#
R2(config-router)#neighbor 209.165.200.1 remote-as 300
R2(config-router)#neighbor 2001:db8:200::1 remote-as 300
        #Configurar y habilitar relación vecino con R1 en ASN 300#
R2(config-router)#address-family ipv4
R2(config-router-af)#neighbor 209.165.200.1 activate
R2(config-router-af)#no neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255
R2(config-router-af)#network 0.0.0.0
        #En IPv4 address-family anuncia red Loopback/ruta por defecto y vecinos#
R2(config-router)#address-family ipv6
R2(config-router-af)#no neighbor 209.165.200.1 activate
R2(config-router-af)#neighbor 2001:db8:200::1 activate
R2(config-router-af)#network 2001:db8:2222::1/128
R2(config-router-af)#network ::/0
        # En IPv4 address-family anuncia red Loopback/ruta por defecto y vecinos#
```

Con los comandos *show bgp ipv4 unicast* y *show bgp ipv6 unicast* se puede verificar el proceso BGP en cada router.

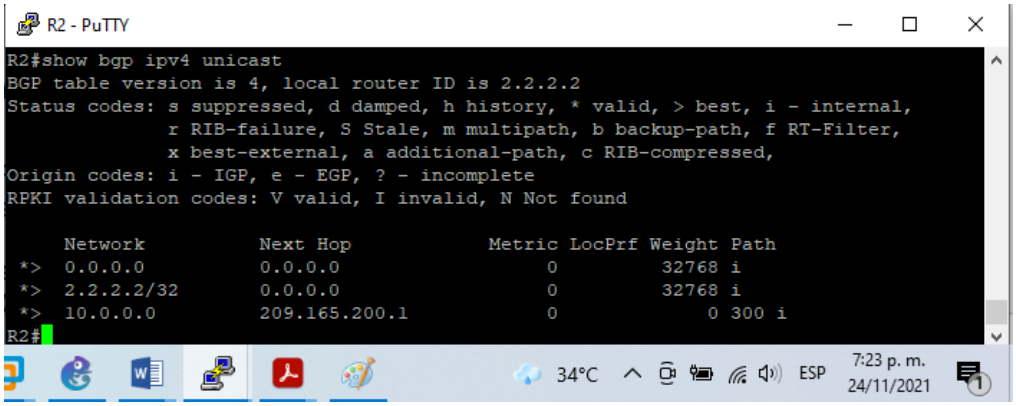

Figura 25 Verificación de BPG ipv4 en R2

3.4 Configuración de MP-BGP en R1

En R1 en la “Red ISP” se configura MP- BGP según las siguientes especificaciones:

Se configuran 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.

Se configura R1 en BGP ASN 300 usando el router-id 1.1.1.1.

Se configura una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

En IPv4 address family:

- Se deshabilita la relación de vecino IPv6.
- Se habilita la relación de vecino IPv4.
- Se anuncia la red 10.0.0.0/8.

En IPv6 address family:

- Se deshabilita la relación de vecino IPv4.
- Se habilita la relación de vecino IPv6.
- Se anuncia la red 2001:db8:100::/48.

Comandos para configurar BGP en R1:

R1(config)# ip route 10.0.0.0 255.0.0.0 null0
R1(config)# ipv6 route 2001:db8:100::/48 null0
 # Configuración de 2 rutas resumen estáticas a la interface Null 0#
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
 # Configuración de BGP en ANS 500#
R1(config-router)# neighbor 209.165.200.2 remote-as 500
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500
 # Configurar y habilitar relación vecino con R2 en ASN 500#
R1(config-router)#address-family ipv4 unicast
R1(config-router-af)# neighbor 209.165.200.2 activate
R1(config-router-af)# no neighbor 2001:db8:200::2 activate
R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)#exit
 # En IPv4 address-family se deshabilita vecindad ipv6, se habilita vecindad ipv4 anuncia red resumen ipv4#

```
R1(config-router)#address-family ipv6 unicast
R1(config-router-af)# no neighbor 209.165.200.2 activate
R1(config-router-af)# neighbor 2001:db8:200::2 activate
R1(config-router-af)# network 2001:db8:100::/48
R1(config-router-af)#exit
R1(config-router)#exit
```

 # En IPv4 address-family se deshabilita vecindad ipv4, se habilita vecindad ipv6 anuncia red resumen ipv6#

Con el comando *show run | include neighbor* se pueden verificar las relaciones de vecindad creadas.

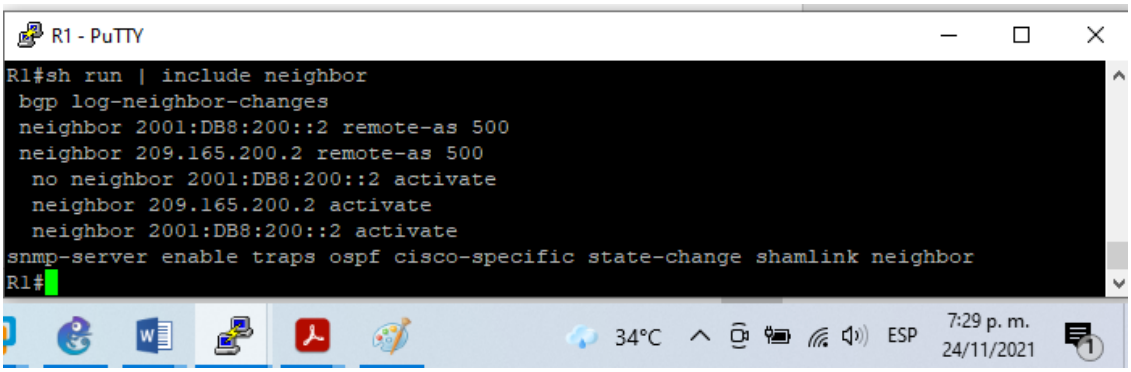

Figura 26 Verificación de relaciones de vecindad en R1.

Al finalizar esta etapa se puede verificar que los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 son exitosos.

Desde D1 y desde D2 se envían ping a la dirección 2.2.2.2 y a la dirección 2001:db8:2222::1

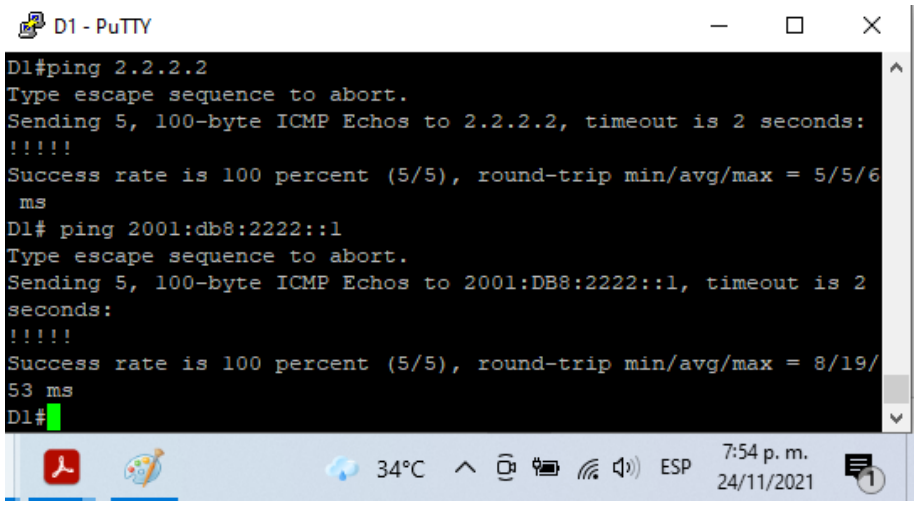

Figura 27 Verificación de ping desde D1 hasta Loopback.

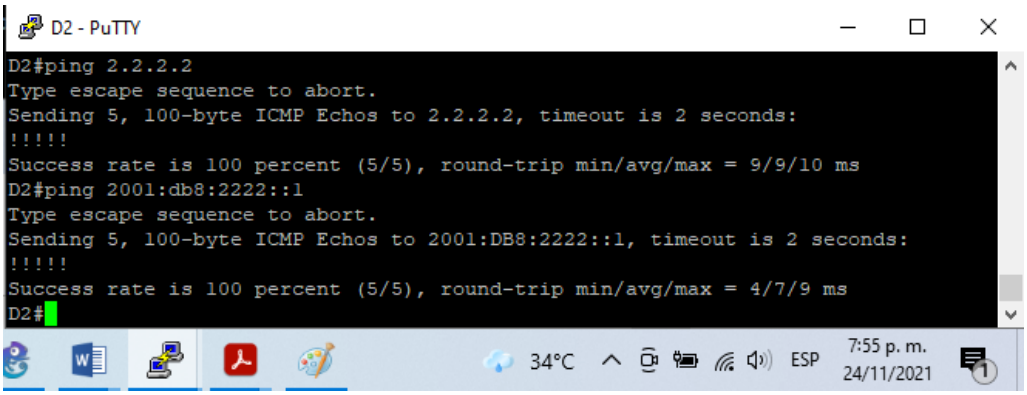

Figura 28 Verificación de ping desde D2 hasta Loopback.

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

En esta parte, debe configurar HSRP versión 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañía”.
Las tareas de configuración son las siguientes:

4.1 Crear IP SLAs en D1

Creación en D1 de dos IP SLAs que prueben la accesibilidad de la interfaz e0/1 de R1 según las siguientes especificaciones:

- Se crearán dos IP SLAs: SLA número 4 para IPv4 y SLA 6 para IPv6
- Las IP SLAs probarán disponibilidad de la interface e0/1 de R1 cada 5 seg.
- La SLA se programará para implementación inmediata sin tiempo de finalización.
- Se creará una IP SLA objeto para la IP SLA 4 con el número de rastreo 4 y otra para la IP SLA 6 con el número de rastreo 6.
- Los objetos rastreados se notificarán 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

Comandos para crear IP SLAs en D1

```
D1(config)#ip sla 4          #Creación de IP SLA 4#
D1(config-ip-sla)#icmp-echo 10.0.10.1 source-ip 10.0.10.2
D1(config-ip-sla-echo)#frequency 5        #Para probar la disponibilidad de la interface
    E0/1 de R1 cada 5 seg#
D1(config-ip-sla-echo)#ip sla schedule 4 life forever start-time now
    #Implementación inmediata de la SLA#
D1(config)#track 4 ip sla 4 #Objeto de rastreo numero 4#
D1(config-track)#delay up 10 down 15
D1(config-track)#exit
D1(config)#ip sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-ip 2001:db8:100:1010::2
    #Se crea la redundancia del primer salto#
D1(config-ip-sla-echo)#frequency 5
D1(config-ip-sla-echo)#ip sla schedule 6 life forever start-time now
D1(config)#track 6 ip sla 6
D1(config-track)#delay up 10 down 15
D1(config-track)#exit
D1(config)#
```

4.2 Crear IP SLAs en D2

Creación en D2 de dos IP SLAs que prueben la accesibilidad de la interfaz e0/1 de R3 según las siguientes especificaciones:

- Se crearán dos IP SLAs: SLA número 4 para IPv4 y SLA 6 para IPv6
- Las IP SLAs probarán disponibilidad de la interface e0/1 de R3 cada 5 seg.
- La SLA se programará para implementación inmediata sin tiempo de finalización.
- Se creará una IP SLA objeto para la IP SLA 4 con el número de rastreo 4 y otra para la IP SLA 6 con el número de rastreo 6.
- Los objetos rastreados se notificarán 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

Comandos para crear IP SLAs en D2

```
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)#ip sla schedule 4 life forever start-time now
D2(config)#track 4 ip sla 4
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
D2(config)#ip sla 6
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-ip 2001:db8:100:1011::2
D2(config-ip-sla-echo)#frequency 5
D2(config-ip-sla-echo)#ip sla schedule 6 life forever start-time now
D2(config)#track 6 ip sla 6
D2(config-track)#delay up 10 down 15
D2(config-track)#exit
```

Con el comando *show run | section ip sla* se puede verificar la configuración de la IP SLA

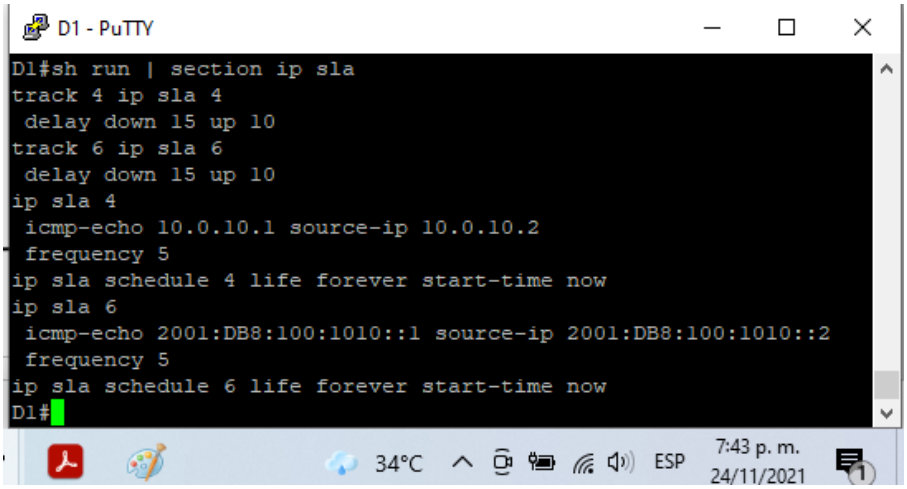

Figura 29 Verificación IP SLA en D1.

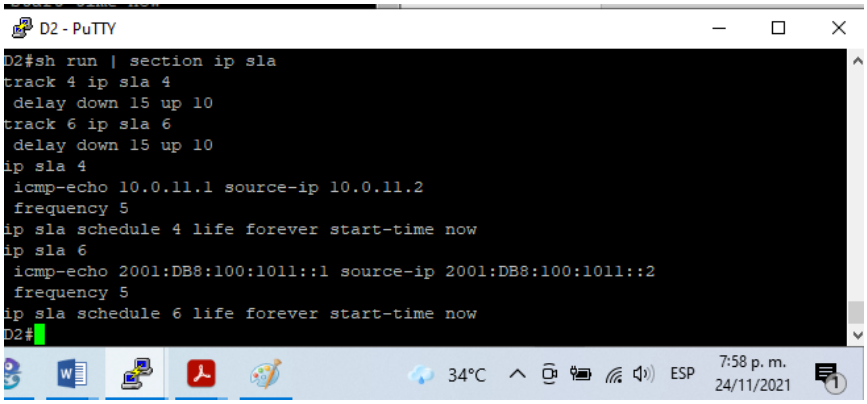

Figura 30 Verificación IP SLA en D2.

4.3 Configurar HSRPv2 en D1

Configuración de HSRPv2 en D1 según las siguientes especificaciones:

- D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.
- Configuración de IPv4 HSRP grupo 104 para la VLAN 100 con los parámetros:
  - Dirección IP virtual 10.0.100.254.
  - Prioridad del grupo en 150.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 4 y disminuir en 60.
- Configuración de IPv4 HSRP grupo 114 para la VLAN 101 con los parámetros:
  - Dirección IP virtual 10.0.101.254.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 4 y disminuir en 60.
- Configuración de IPv4 HSRP grupo 124 para la VLAN 102 con los parámetros:
  - Dirección IP virtual 10.0.102.254.
  - Prioridad del grupo en 150.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 4 y decrementar en 60.
- Configuración de IPv6 HSRP grupo 106 para la VLAN 100 con los parámetros:
  - Dirección IP virtual ipv6 autoconfig
  - Prioridad del grupo en 150.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 6 y decrementar en 60.
- Configuración de IPv6 HSRP grupo 116 para la VLAN 101 con los parámetros:
  - Dirección IP virtual ipv6 autoconfig
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 6 y decrementar en 60.
- Configuración de IPv6 HSRP grupo 126 para la VLAN 102 con los parámetros:
  - Dirección IP virtual ipv6 autoconfig
  - Prioridad del grupo en 150.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 6 y decrementar en 60.

Comandos para configurar HSRPv2 en D1

```
D1(config)#int vlan 100          #Para acceder a la configuración de vlan 100#
D1(config-if)#standby 104 version 2  #Creacion de HSRPv2#
D1(config-if)#standby 104 ip 10.0.100.254    #Se crea dirección virtual para vlan 100#
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt
D1(config-if)#standby 104 track 4 decrement 60
D1(config-if)#exit

D1(config)#int vlan 101
D1(config-if)#standby 114 version 2
D1(config-if)#standby 114 ip 10.0.101.254    #Se crea dirección virtual para vlan 101#
D1(config-if)#standby 114 preempt
D1(config-if)#standby 114 track 4 decrement 60
```

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

D1(config)#int vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254    #Se crea dirección virtual para vlan 102#
D1(config-if)#no standby 124 priority 150
D1(config-if)#standby 124 preempt
D1(config-if)#standby 124 track 4 decrement 60
D1(config-if)#exit

D1(config)#int vlan 100
D1(config-if)#standby version 2
D1(config-if)#standby 106 ipv6 autoconfig
D1(config-if)#standby 106 priority 150
D1(config-if)#standby 106 preempt
D1(config-if)#standby 106 track 4 decrement 60
D1(config-if)#exit

D1(config)#int vlan 101
D1(config-if)#standby version 2
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt
D1(config-if)#standby 116 track 4 decrement 60
D1(config-if)#exit

D1(config)#int vlan 102
D1(config-if)#standby version 2
D1(config-if)#standby 126 ipv6 autoconfig
D1(config-if)#standby 126 priority 150
D1(config-if)#standby 126 preempt
D1(config-if)#standby 126 track 4 decrement 60
```

4.4 Configurar HSRPv2 en D2

Configuración de HSRPv2 en D2 según las siguientes especificaciones:

- D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.
- Configuración de IPv4 HSRP grupo 104 para la VLAN 100 con los parámetros:
  - Dirección IP virtual 10.0.100.254.
  - Prioridad del grupo en 150.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 4 y disminuir en 60.
- Configuración de IPv4 HSRP grupo 114 para la VLAN 101 con los parámetros:
  - Dirección IP virtual 10.0.101.254.
  - Preferencia (preemption) habilitada.
  - Rastrear el objeto 4 y disminuir en 60.
- Configuración de IPv4 HSRP grupo 124 para la VLAN 102 con los parámetros:
  - Dirección IP virtual 10.0.102.254.

    - Prioridad del grupo en 150.
    - Preferencia (preemption) habilitada.
    - Rastrear el objeto 4 y decrementar en 60.
- Configuración de IPv6 HSRP grupo 106 para la VLAN 100 con los parámetros:
    - Dirección IP virtual ipv6 autoconfig
    - Prioridad del grupo en 150.
    - Preferencia (preemption) habilitada.
    - Rastrear el objeto 6 y decrementar en 60.
- Configuración de IPv6 HSRP grupo 116 para la VLAN 101 con los parámetros:
    - Dirección IP virtual ipv6 autoconfig
    - Preferencia (preemption) habilitada.
    - Rastrear el objeto 6 y decrementar en 60.
- Configuración de IPv6 HSRP grupo 126 para la VLAN 102 con los parámetros:
    - Dirección IP virtual ipv6 autoconfig
    - Prioridad del grupo en 150.
    - Preferencia (preemption) habilitada.
    - Rastrear el objeto 6 y decrementar en 60.

```
D2(config)#inter vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt
D2(config-if)#standby 104 track 4 decrement 60
D2(config-if)#exit

D2(config)#inter vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.100.254
D2(config-if)#standby 126 priority 150
D2(config-if)#standby 114 preempt
D2(config-if)#standby 114 track 4 decrement 60
D2(config-if)#exit

D2(config)#inter vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.100.254
D2(config-if)#standby 124 priority 150
D2(config-if)#standby 124 preempt
D2(config-if)#standby 124 track 4 decrement 60
D2(config-if)#exit

D2(config)#inter vlan 100
D2(config-if)#standby version 2
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt
D2(config-if)#standby 106 track 4 decrement 60
D2(config-if)#exit
```

```
D2(config)#inter vlan 101
D2(config-if)#standby version 2
D2(config-if)#standby 116 ipv6 autoconfig
D2(config-if)#standby 116 priority 150
D2(config-if)#standby 116 preempt
D2(config-if)#standby 116 track 4
D2(config-if)#standby 116 track 4
D2(config-if)#exit

D2(config)#inter vlan 102
D2(config-if)#standby version 2
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
D2(config-if)#standby 126 track 4 decrement 60
D2(config-if)#exit
D2(config)#
```

Con el comando *show standby brief* se pueden verificar las configuraciones de HSRPv2

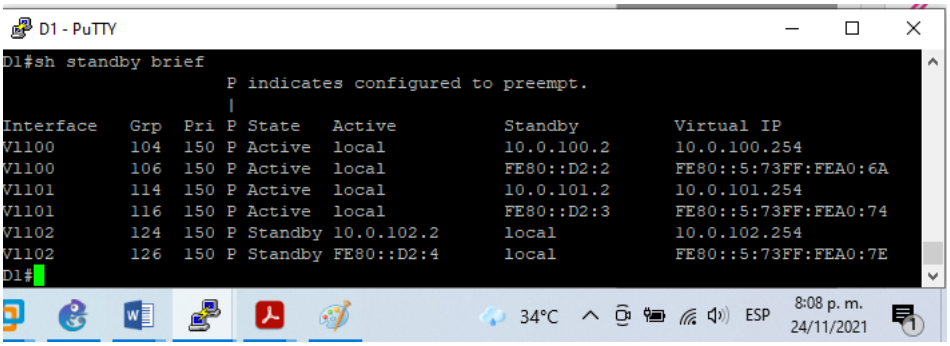

Figura 31 Verificación HSRPv2 en D1.

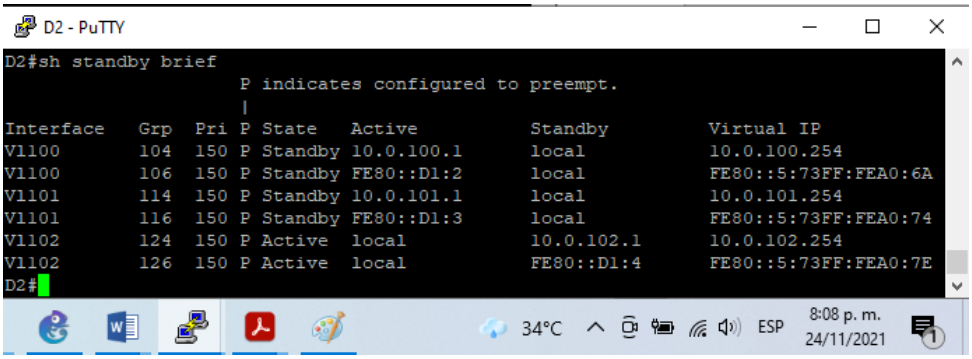

Figura 32 Verificación de HSRPv2 en D2

Parte 5: Seguridad

En esta parte se configuran varios mecanismos de seguridad en los dispositivos de la topología siguiendo los siguientes pasos:

5.1 Protección del EXEC Privilegiado
En todos los dispositivos se protege el EXEC privilegiado con algoritmo de encriptación SCRYP. La contraseña será cisco12345cisco

```
R1(config)#enable algorithm-type scrypt secret cisco12345cisco
R2(config)#enable algorithm-type scrypt secret cisco12345cisco
R3(config)#enable algorithm-type scrypt secret cisco12345cisco
D1(config)#enable algorithm-type scrypt secret cisco12345cisco
D2(config)#enable algorithm-type scrypt secret cisco12345cisco
A1(config)#enable algorithm-type scrypt secret cisco12345cisco
```

5.2 Creación de usuario local
En todos los dispositivos se crea un usuario local protegido con algoritmo de encriptación SCRYP. Nombre de usuario local: sadmin. Nivel de privilegio 15. Contraseña cisco12345cisco

```
R1(config)#username sadmin privilege 15 pass cisco12345cisco
R3(config)#username sadmin privilege 15 pass cisco12345cisco
R3(config)#username sadmin privilege 15 pass cisco12345cisco
D1(config)#username sadmin privilege 15 pass cisco12345cisco
D2(config)#username sadmin privilege 15 pass cisco12345cisco
A1(config)#username sadmin privilege 15 pass cisco12345cisco
```

5.3 Habilitación de AAA
En todos los dispositivos, excepto en R2, se habilita AAA.

```
R1(config)#aaa new-model
R3(config)#aaa new-model
D1(config)#aaa new-model
D2(config)#aaa new-model
A1(config)#aaa new-model
```

5.4 Configuración del servidor RADIUS
En todos los dispositivos, excepto en R2, se configuran las especificaciones del servidor RADIUS: Dirección IP 10.0.100.6. Puertos UDP 1812 y 1813. Contraseña $trongPass

```
R1(config)#radius-server host 10.0.100.6 acct-port 1812 key $trongPass
R1(config)#radius-server host 10.0.100.6 acct-port 1813 key $trongPass
R3(config)#radius-server host 10.0.100.6 acct-port 1812 key $trongPass
R3(config)#radius-server host 10.0.100.6 acct-port 1813 key $trongPass
```

```
D1(config)#radius-server host 10.0.100.6 acct-port 1812 key $trongPass
D1(config)#radius-server host 10.0.100.6 acct-port 1813 key $trongPass
D2(config)#radius-server host 10.0.100.6 acct-port 1812 key $trongPass
D2(config)#radius-server host 10.0.100.6 acct-port 1813 key $trongPass
A1(config)#radius-server host 10.0.100.6 acct-port 1812 key $trongPass
A1(config)#radius-server host 10.0.100.6 acct-port 1813 key $trongPass
```

5.5 Configuración de la lista de métodos de autenticación AAA
En todos los dispositivos, excepto en R2, se configura la lista de métodos de autenticación AAA: Se usa la lista de métodos por defecto. Se valida contra el grupo de servidores RADIUS, de lo contrario se usa la base de datos local.

```
R1(config)#aaa authentication login default group radius local
R3(config)#aaa authentication login default group radius local
D1(config)#aaa authentication login default group radius local
D2(config)#aaa authentication login default group radius local
A1(config)#aaa authentication login default group radius local
```

5.6 Verificación del servicio AAA
Se verifica el servicio AAA en todos los dispositivos, excepto en R2, cerrando e iniciando sesión en todos los dispositivos, excepto en R2, con el usuario: raduser y la contraseña: upass123.

Con el comando *show run aaa | exclude ¡* se pueden verificar las configuraciones de aaa y de radius en los dispositivos.

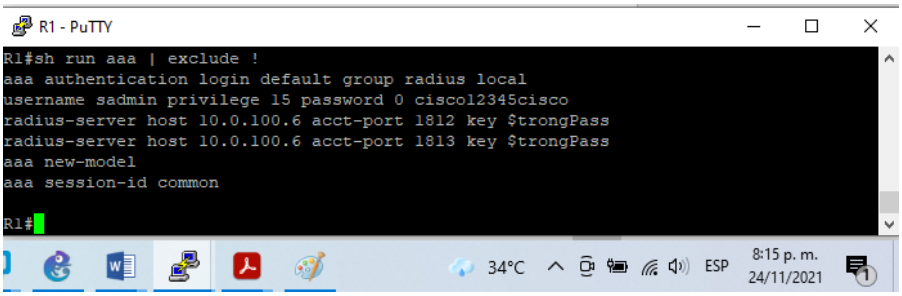

Figura 33 Verificación de aaa y radius en R1.

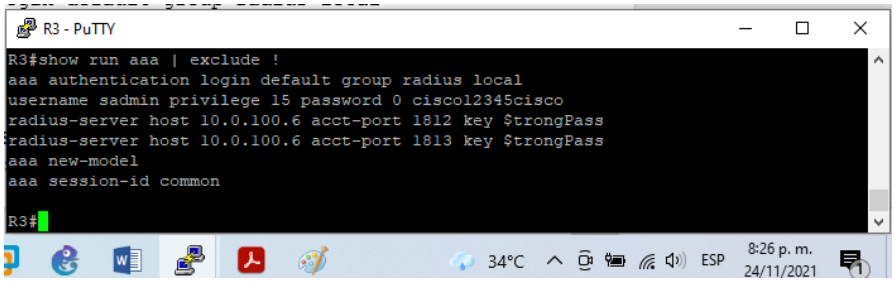

Figura 34 Verificación de aaa y radius en R3.

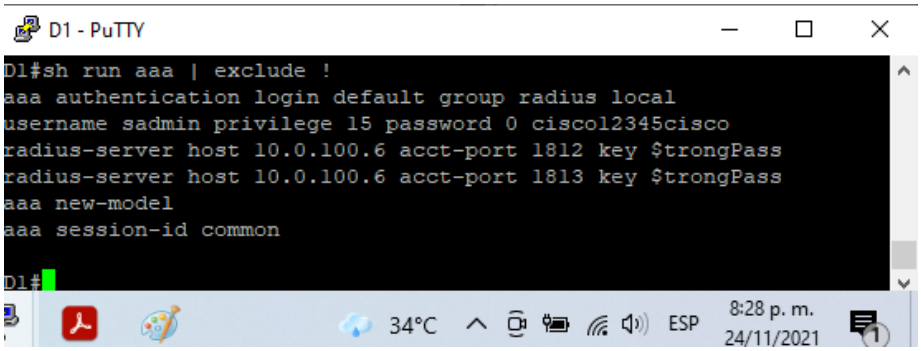

Figura 35 Verificación de aaa y radius en D1.

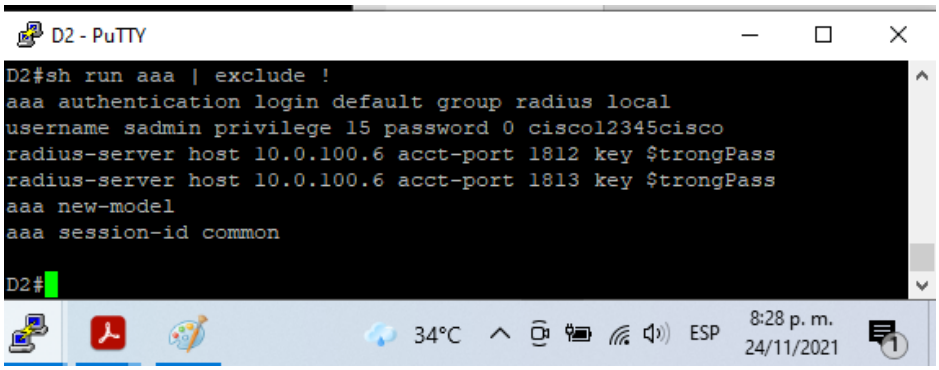

Figura 36 Verificación de aaa y radius en D2.

Parte 6: Configuración de las funciones de Administración de Red.

En esta parte se configuran varias funciones de administración de red.

6.1 Configuración del reloj local a la hora UTC actual en todos los dispositivos.

```
R1(config)#clock timezone UTC -5
R2(config)#clock timezone UTC -5
R3(config)#clock timezone UTC -5
D1(config)#clock timezone UTC -5
D2(config)#clock timezone UTC -5
A1(config)#clock timezone UTC -5
```

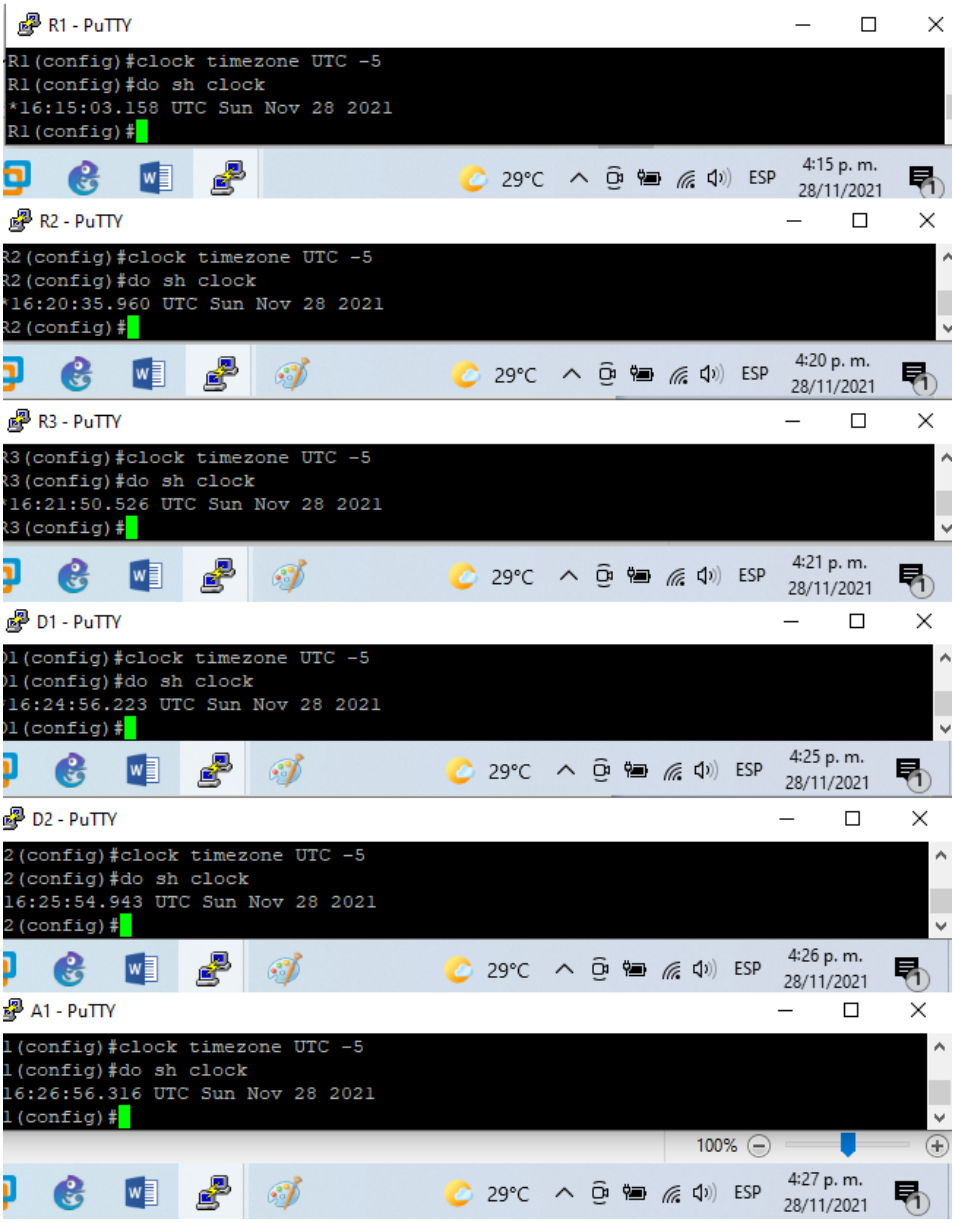

Figura 37 Verificación de timezone en cada dispositivo.

6.2 Configuración de R2 como un NTP maestro en el nivel de estrato 3.
R2(config)#ntp master 3

6.3 Configuración de NTP en R1, R3, D1, D2, y A1, de la siguiente manera:
R1 sincronizará con R2.
R1(config)#ntp server 209.165.200.2

R3, D1 y A1 sincronizarán la hora con R1.
R3(config)#ntp server 10.0.13.1
D1(config)#ntp server 10.0.10.1
A1(config)#ntp server 10.0.13.1

D2 sincronizará la hora con R3.
D2(config)#ntp server 10.0.11.1

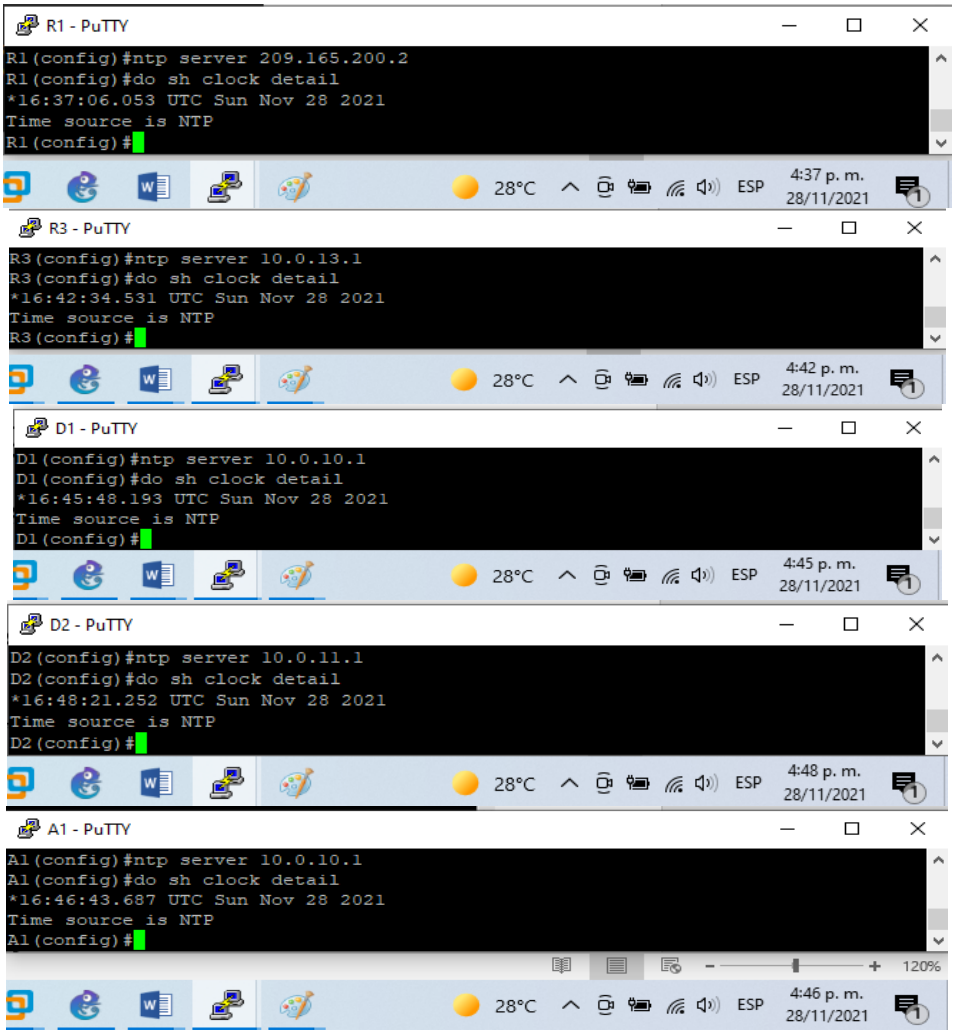

Figura 38 Verificación de ntp server en cada dispositivo.

6.4 Configuración de Syslog en todos los dispositivos excepto en R2.
Syslogs se enviarán a la PC1 en 10.0.100.5 en el nivel WARNING.

R1(config)#logging on*#Se activa el envió de syslog#*
R1(config)#logging 10.0.100.5 *#se configura syslog para que se enviado a PC1#*
R1(config)#logging trap warning #Se configura los mensajes syslog en el nivel warning#

R3(config)#logging on
R3(config)#logging 10.0.100.5
R3(config)#logging trap warning

D1(config)#logging on
D1(config)#logging 10.0.100.5
D1(config)#logging trap warning

D2(config)#logging on
D2(config)#logging 10.0.100.5
D2(config)#logging trap warning

A1(config)#logging on
A1(config)#logging 10.0.100.5
A1(config)#logging trap warning

6.5 Configuración de SNMPv2c en todos los dispositivos excepto R2.
Especificaciones de SNMPv2:

- Únicamente se usará SNMP en modo lectura (Read-Only).
- Limite el acceso SNMP a la dirección IP de la PC1.
- Configuración del 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.

Comandos para configurar SNMP en R1

R1(config)#snmp-server community ENCORSA ro *#Se habilita SNMP en modo lectura cambiando el string community por ENCORSA#*
R1(config)#snmp-server contact IMORILLOH *#Se cambia el valor de contacto de SNMP por el nombre del autor#*
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA *#Se habilita en SNMP el PC1#*
R1(config)#snmp-server enable traps bgp *#Se habilita envio de traps bgp#*
R1(config)#snmp-server enable traps config *#Se habilita envio de traps config#*
R1(config)#snmp-server enable traps ospf *#Se habilita envio de traps ospf#*
R1(config)#ip access-list standard ENCORSA *#Se crea lista de acceso estándar#*
R1(config-std-nacl)#permit 10.0.100.5 *#se permite el la lista de acceso a PC1#*

R1(config-std-nacl)#exit
Comandos para configurar SNMP en R3
R3(config)#snmp-server community ENCORSA ro
R3(config)#snmp-server contact IMORILLOH
R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)#snmp-server enable traps config
R3(config)#snmp-server enable traps ospf
R3(config)#ip access-list standard ENCORSA
R3(config-std-nacl)#permit 10.0.100.5
R3(config-std-nacl)#exit

Comandos para configurar SNMP en D1
D1(config)#snmp-server community ENCORSA ro
D1(config)#snmp-server contact IMORILLOH
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)#snmp-server enable traps config
D1(config)#snmp-server enable traps ospf
D1(config)#ip access-list standard ENCORSA
D1(config-std-nacl)#permit 10.0.100.5
D1(config-std-nacl)#exit

Comandos para configurar SNMP en D2
D2(config)#snmp-server community ENCORSA ro
D2(config)#snmp-server contact IMORILLOH
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)#snmp-server enable traps config
D2(config)#snmp-server enable traps ospf
D2(config)#ip access-list standard ENCORSA
D2(config-std-nacl)#permit 10.0.100.5
D2(config-std-nacl)#exit

Comandos para configurar SNMP en A1
A1(config)#snmp-server community ENCORSA ro
A1(config)#snmp-server contact IMORILLOH
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
A1(config)#snmp-server enable traps config
A1(config)#snmp-server enable traps ospf
A1(config)#ip access-list standard ENCORSA
A1(config-std-nacl)#permit 10.0.100.5
A1(config-std-nacl)#exit

Parte 7: verificación de conectividad entre los diferentes hosts de la Red.

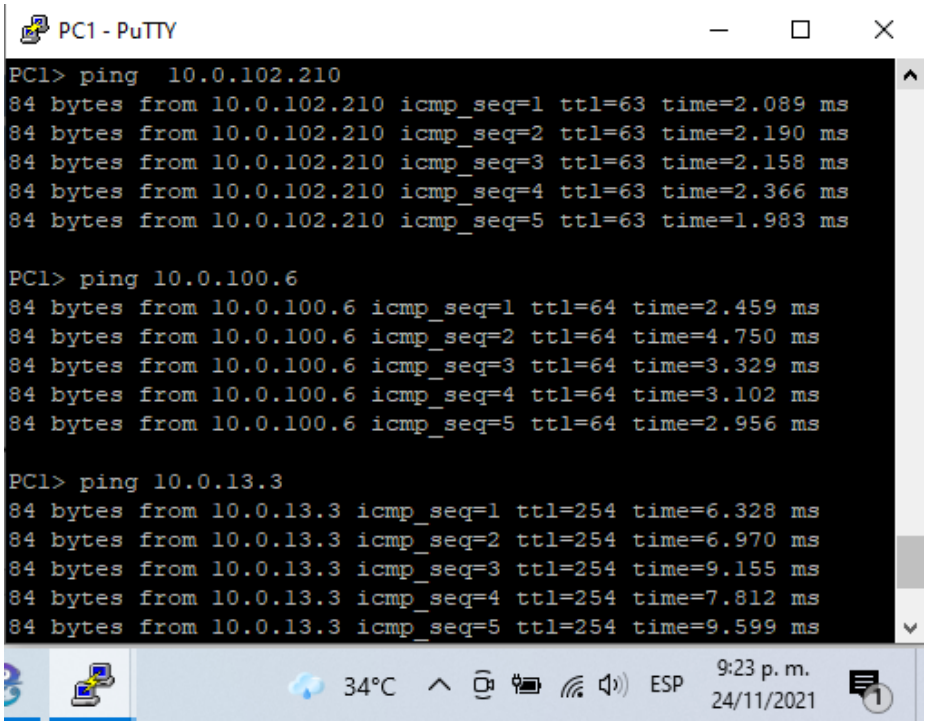

Figura 39 Verificación de conectividad desde PC1.

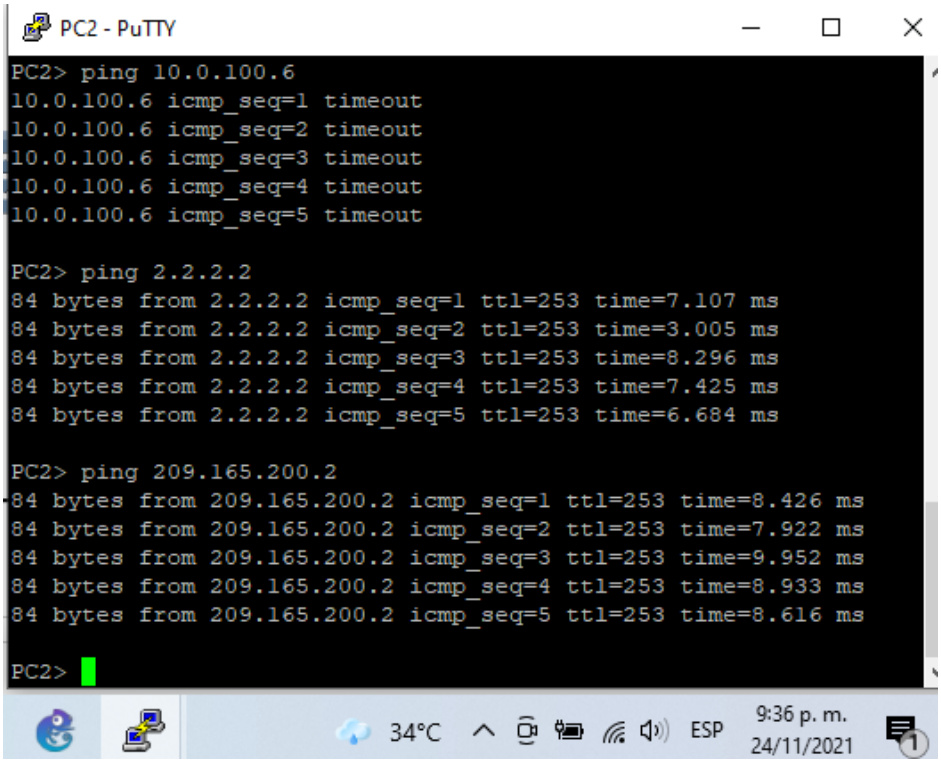

Figura 40 Verificación de conectividad desde PC2.

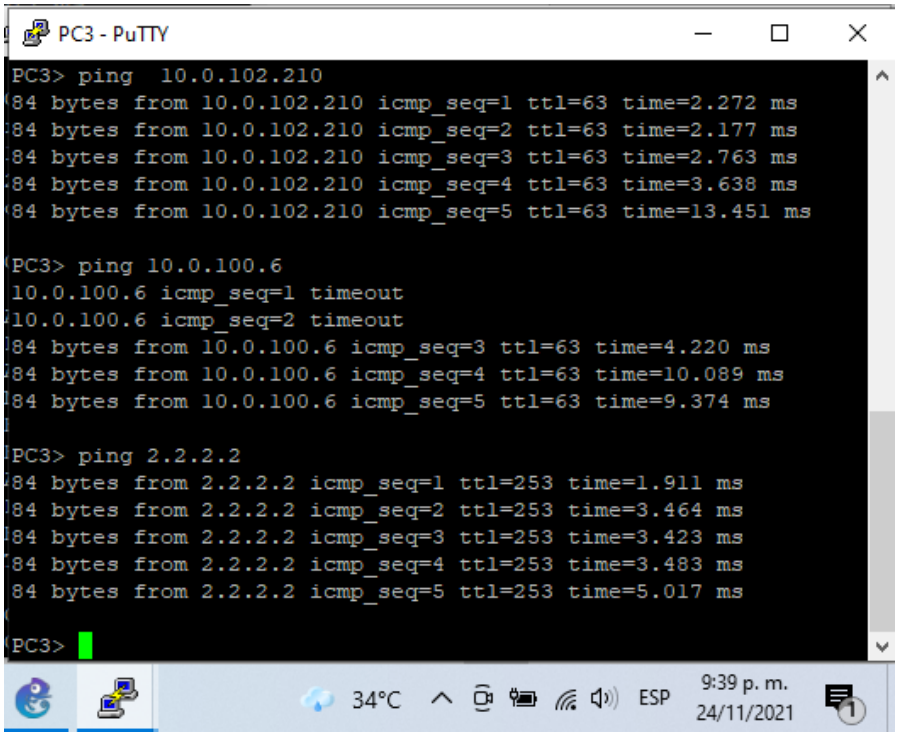

Figura 41 Verificación de conectividad desde PC3.

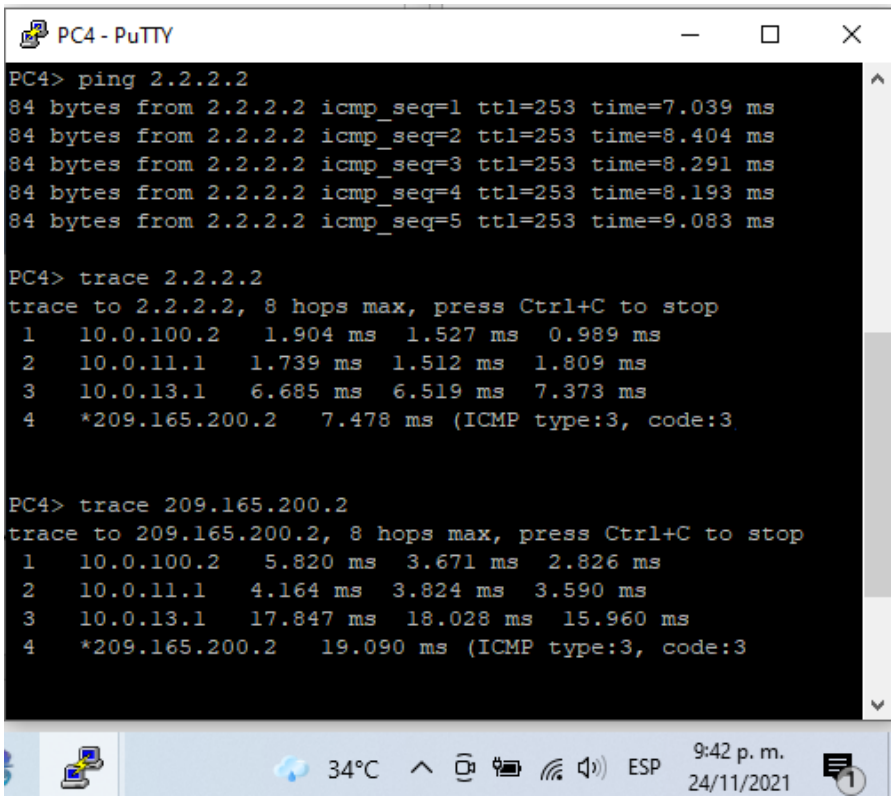

Figura 42 Verificación de conectividad desde PC4.

CONCLUSIONES

Los escenarios virtuales se han convertido en herramientas esenciales y de gran valor para poder realizar todo tipo de ensayos y pruebas en cualquier topología de red que se pueda imaginar para ser diseñada, para poder posteriormente llegar a un entorno práctico real con una visión muy cercana a la realidad de cómo debería funcionar y comportarse la red diseñada.

El escenario de simulación basado en GNS3 y su máquina virtual permitieron implementar la red propuesta en el reto de habilidades del diplomado de profundización CCNP de Cisco, se inició desde la configuración básica de cada uno de los dispositivos involucrados, pasando por procesos de enrutamiento más elaborados, la implementación de reglas de seguridad necesarias para blindar la red de accesos no deseados y terminando con la verificación de conectividad entre los diferentes hosts.

El escenario de simulación Packet Tracer en principio se muestra más intuitivo y más amigable para implementar simulaciones de topologías de redes, pero no ofrece soporte para virtualizar algunos comandos menos genéricos y más especializados.

Al finalizar el desarrollo del reto de la prueba de habilidades prácticas del diplomado, se pudo comprobar la necesidad de haber revisado cada uno de los temas teóricos propuestos durante los diferentes cursos anteriores, contenidos todos enfocados en brindar y apropiar fortalezas indispensables para imaginar y diseñar redes realmente escalables, para luego poder ponerlas en marcha y posteriormente poder solucionar las posibles fallas que pudieran presentarse en las redes de comunicaciones.

BIBLIOGRAFIA

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

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

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

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

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Guide CCNP ROUTE 300-101.
https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx
IOS [OVA]. https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg

Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning
Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and
Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGR

Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

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