DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RODRIGO LINCER CEBALLOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
FLORENCIA-CAQUETA
2022

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

RODRIGO LINCER CEBALLOS

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

DIRECTOR:

Ing. JOHN HAROLD PÉREZ CALDERÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
FLORENCIA-CAQUETA
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

FLORENCIA, 25 de noviembre del 2022

AGRADECIMIENTOS

Este trabajo de prueba de habilidades prácticas fue realizado individualmente por el estudiante de último semestre de la ingeniería en telecomunicaciones, se agradece el apoyo desinteresado a lucrarse de muchas personas que directa o indirectamente ayudaron a superar los numerosos obstáculos en el camino, por ello se tiene que dar gracias.

En primera instancia sin duda alguna agradezco a mi Dios quien me aprestado la vida para seguir en la lucha de mis sueños y lograr mis triunfos, es el quien me provee de toda la salud para seguir adelante con mis propósitos y mis sueños.

En segundo lugar, a mis padres, mis infinitas gracias por el apoyo moral y económico y todo el sacrificio que han hecho por mí, por guiarme siempre por el buen y mejor camino de la vida, eligiendo así el correcto; heredándome con dignidad la mejor educación, gratitud inmensa a mis amigos por la amistad y empuje que en ciertos momentos me brindaron y al resto de familia que siempre están allí apoyándome moralmente

A la Universidad Nacional Abierta y a Distancia y su cuerpo de docentes, por todos los conocimientos adquiridos a lo largo de esta hermosa carrera.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ASN: Autonomous System Number, se le denomina al grupo de red que es gestionado por algún operador de red por ruteo externo.

BGP: Border Gateway Protocol, utilizado para conectar distintos sistemas autónomos principalmente con el canal de internet.

DHCP: Dynamic Host Configuration Protocol, funciona en el modelo cliente/servidor y proporciona automáticamente direcciones IP y otra información relacionada como la máscara y el Gateway.

HSRP: (Host Standby Routing Protocol), asigna a un grupo de redundancia un router activo, otro standby y los demás en estado listen, donde el activo tendrá la IP virtual.

ISP: (Internet Service Provider), término que identifica las compañías que proveen acceso a internet.

LACP: (Link Agregation Control Protocol), característico de la capa 2 une puertos físicos de la red en un único puerto lógico de gran ancho de banda, y crea redundancias.

MP-BGP: (Multiprotocol -BGP), permite que BGP lleve información de IPv6 y otros protocolos de red múltiple.

OSPFv2: (Open Shortest Path First), protocolo de enrutamiento dinámico que detecta cambios en la topología, fallas de enlace y converge en una nueva estructura rápidamente, específicamente para IPv4.

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

Root bridge: Punto de referencia dentro de la red que puede soportar más conmutación, todos los switches deben estar conectados hacia él con el mejor coste.

RSTP: Rapid (Spanning Tree Protocol), aplicable a la capa 2 reduce considerablemente la convergencia de la topología cuando ocurre algún cambio.

VLAN: Virtual LAN, método utilizado para crear varias redes lógicas dentro de una solo red física.

RESUMEN

El presente trabajo se desarrolla como opción de grado para la ingeniería en telecomunicaciones y electrónica , aplicando todas las habilidades prácticas y adquiridas bajo un escenario de CCNP planteado, este escenario se desarrolla en el simulador de GNS3 utilizando y empleando imágenes IOS de los dispositivos de CISCO, el escenario se observa como una propuesta simple, sin embargo los requisitos exigidos por la guía son muy diversos para poder lograr simular tal cual la red a nivel profesional, aplicando todas las habilidades adquiridas y conocimientos por el estudiante en las redes de datos configurando así como primera instancia los protocolos para la conmutación en la capa 2 del modelo OSI y paralelamente se configura los protocolos de la capa 3 para establecer el enrutamiento entre la propia LAN (red empresa) y otro sistema autónomo (ISP) obteniendo como resultado redes convergentes que se comunican entre sí con políticas de seguridad establecidas simulando escenarios a los cuales se va a enfrentar el futuro egresado.

Palabras clave: CCNP, CISCO, CONMUTACIÓN, ENRUTAMIENTO, REDES.

ABSTRACT

The present work is developed as a degree option for telecommunications and electronics engineering, applying all the practical and acquired skills under a proposed CCNP scenario, this scenario is developed in the GNS3 simulator using and using IOS images of CISCO devices, the scenario is seen as a simple proposal, however the requirements demanded by the guide are very diverse to be able to simulate the network as it is at a professional level: applying all the skills acquired and knowledge by the student in data networks configuring as well as In the first instance, the protocols for switching in layer 2 of the OSI model and in parallel, the layer 3 protocols are configured to establish routing between the LAN itself (company network) and another autonomous system (ISP), obtaining as a result convergent networks that are communicate with each other with established security policies simulating scenarios to which What will the future graduate

Keywords: CCNP, CISCO, SWITCHING, ROUTING, NETWORKS

INTRODUCCION

Las redes en este mundo moderno cada año toma fuerza, desarrollándose tanto en la vida cotidiana como en los negocios, lo que permite el intercambio de todo tipo de información facilitando la interacción y comunicación entre personas y empresas; por esto es importante que los futuros ingenieros en comunicaciones entiendan y aprendan a crear diferentes protocolos que brinden conectividad.

El siguiente trabajo es un producto de la labor de ingeniería en comunicaciones y de esta manera se define la situación, incluyendo 3 routers, 3 switches y 4 pcs, simulando las redes a las cuales se desenvolverá en un futuro.

Inicialmente se configura el direccionamiento IP en todos los dispositivos tanto IPv4 e IPv6, luego utilizando 2 switches multicapa como si fueran los CORE de la red encargados de la conmutación cada uno enfatizado en VLAN diferente y con enlaces redundantes, adicional 1 switch de capa 2 utilizado como el acceso a los clientes, en general en la capa 2 se debe trabajar el RSTP Rapid Spinning Tree Protocol y enlaces LACP, a nivel de capa 3 se soluciona la convergencia de la red totalmente, donde se configura el OSPFv2 para IPV4 y OSPF para IPv6 de la LAN; el enrutamiento BGP para IPv4 y MP-BGP para IPv6 para conectar el sistema autónomo de las dos redes planteadas, esta primera parte asegura la interconexión de los equipos de la LAN de la empresa con los servicios del ISP.

Se espera que en la segunda fase se pueda volver a cambiar la conexión, corrigiendo así la reducción del primer salto con el protocolo HSRP utilizando la dirección VIP 254; y la implementación de todos los protocolos de seguridad AAA y políticas de acceso y contraseñas para cada terminal, lo que aumenta la seguridad de los dispositivos administrados; Y finalmente, debe configurar la sincronización de tiempo NTP entre todos los dispositivos y el sistema de administración utilizando el protocolo SNMPv2 para tener un monitoreo de red en tiempo real.

ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

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

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

Figura 1. Montaje del escenario propuesto.

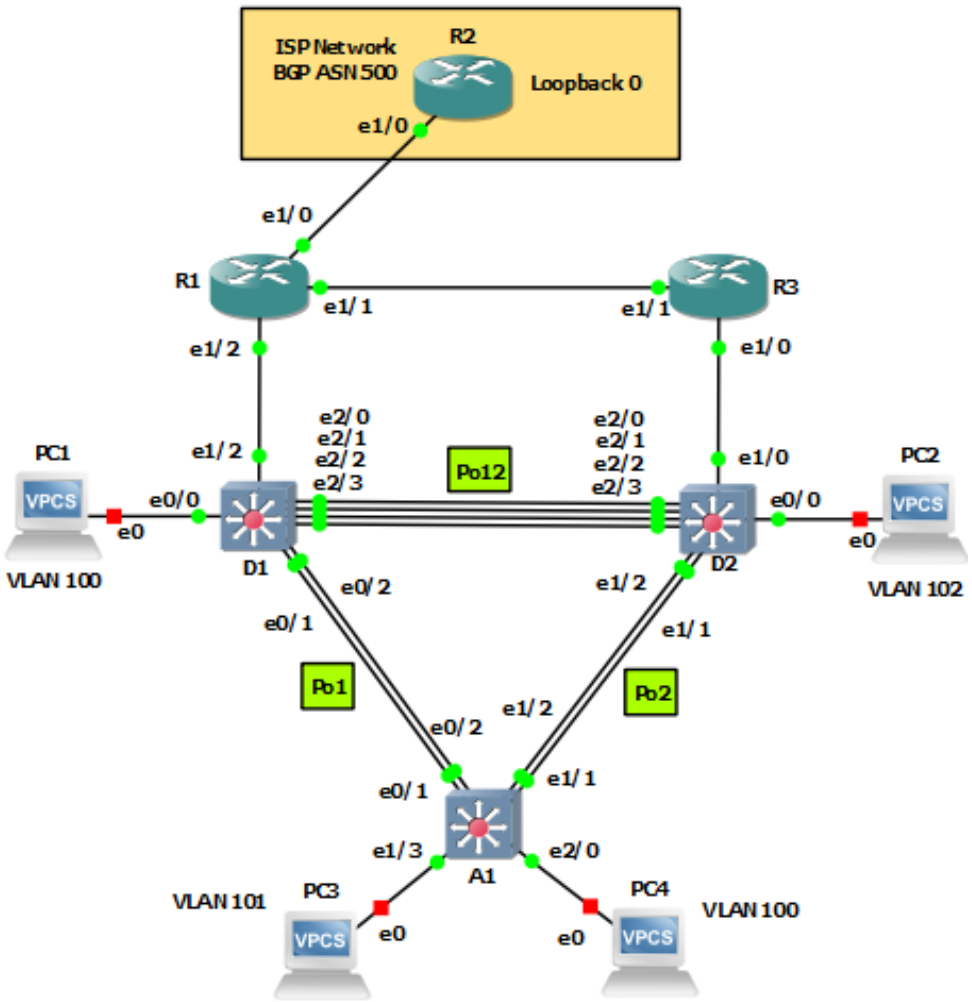


Tabla de direccionamiento:

Tabla 1. Tabla de direccionamiento Escenario 1

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/1	10.77.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/2	10. 77.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10. 77.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10. 77.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10. 77.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10. 77.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.77.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.77.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.77.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.77.100.2/24	2001:db8:100:100::2/64	fe80::d2:2

Device	Interface	IPv4 Address	IPv6 Address	IPv6 Link-Local
	VLAN 101	10.77.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.77.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.77.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.77.100.5/24	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

Fuente: Propia

1.1 Parte 1: Construcción de la red y configuración básica de dispositivos y el direccionamiento de la interfaz

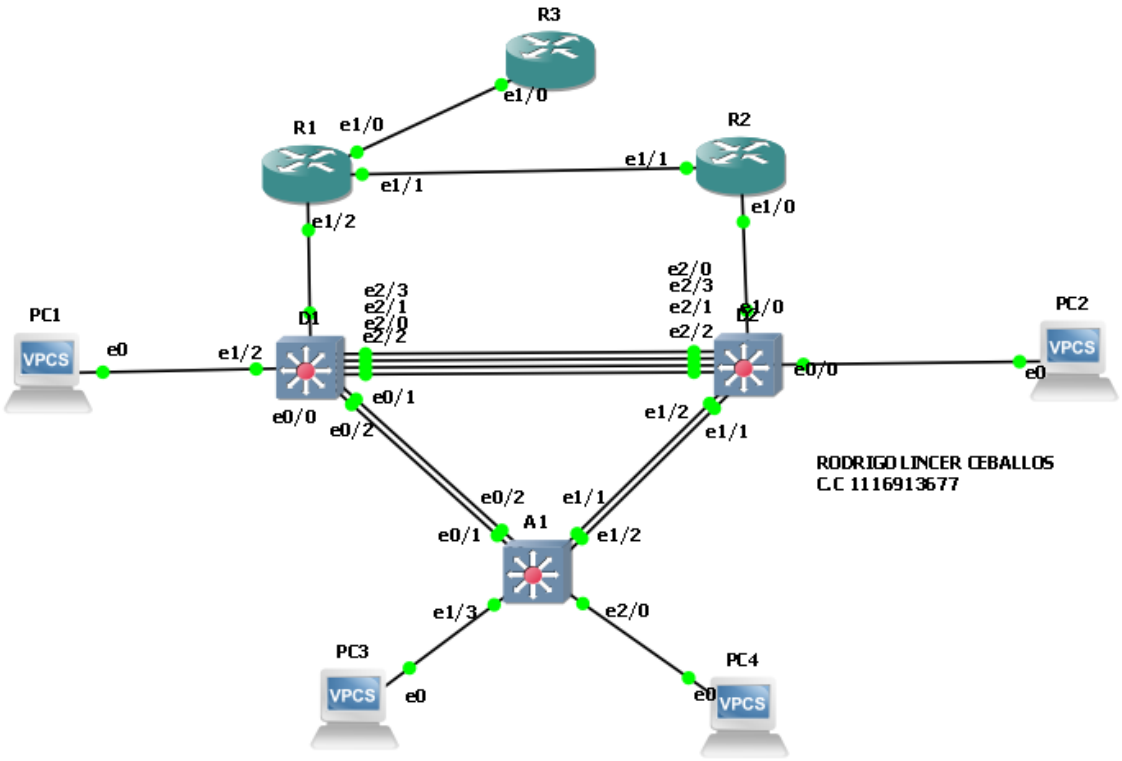
En la Parte 1, configurará la topología de la red y configurará los ajustes básicos y el direccionamiento de la interfaz.

1.1.1 Paso 1: Cableado de la topología

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

Se procede a realizar las respectivas conexiones entre los routers, los switches, los PC y sus interfaces en el simulador GNS3, como se ilustra en la figura 1.

Figura 1. Conexión de la topología del Escenario 1 en GNS3



Fuente: Propia

1.1.2 Paso 2: Configuración de los ajustes básicos para cada dispositivo

- **a.** Ingrese al modo de configuración global y aplique la configuración básica. Las configuraciones de inicio para cada dispositivo se proporcionan a continuación.
- **b.** Guarde la configuración en ejecución en ***startup-config*** en todos los dispositivos.

En primer lugar, se aplicarán las configuraciones básicas de cada dispositivo tales como: nombre del host, las interfaces Ethernet y Loopback asociada a cada router y switch, la configuración de las direcciones IPv4 e IPv6, y posteriormente se procede a guardar la configuración de los dispositivos:

Router 1:

R1#configure terminal //se ingresa a configuración global
R1(config)#hostname R1 // se nombre el router
R1(config)#ipv6 unicast-routing // habilita el routing en IPV6
R1(config)#no ip domain lookup //desactiva la traducción de nombres a dirección

```
R1(config)# banner motd # R1, ENCOR Skills Assessment#
R1(config)# line con 0  // configuración de la línea de consola
R1(config-line)# exec-timeout 0 0
R1(config-line)# logging synchronous
R1(config-line)#exit
R1(config)# interface e1/0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# ipv6 address 2001:db8:200::1/64
R1(config-if)# no shutdown
R1(config-if)#exit
R1(config)# interface e1/2
R1(config-if)# ip address 10.77.10.1 255.255.255.0
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 e1/1
R1(config-if)# ip address 10.77.13.1 255.255.255.0
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)# exit
R1# copy running-config startup-config // guarda la configuracion actual
```

Router 2:

```
R2#configure terminal
R2(config)#hostname R2
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)# banner motd # R2, ENCOR Skills Assessment#
R2(config)# line con 0
R2(config-line)# exec-timeout 0 0
R2(config-line)# logging synchronous
R2(config-line)#exit
R2(config)# interface e1/0
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 // se configura la interfaz virtual
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)# exit
R2# copy running-config startup-config
```

Router 3:

```
R3#configure terminal
R3(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)# banner motd # R3, ENCOR Skills Assessment#
R3(config)# line con 0
R3(config-line)# exec-timeout 0 0
R3(config-line)# logging synchronous
R3(config-line)#exit
R3(config)# interface e1/0
R3(config-if)# ip address 10.77.11.1 255.255.255.0
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 e1/1
R3(config-if)# ip address 10.77.13.3 255.255.255.0
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(config)# exit
R3# copy running-config startup-config
```

Switch D1:

```
D1#configure terminal
D1(config)#hostname D1
D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)# banner motd # D1, ENCOR Skills Assessment#
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
D1(config-vlan)# name Management
D1(config-vlan)# exit
D1(config)# vlan 101
D1(config-vlan)# name UserGroupA
D1(config-vlan)#exit
D1(config)# vlan 102
D1(config-vlan)# name UserGroupB
D1(config-vlan)# exit
D1(config)# vlan 999
D1(config-vlan)# name NATIVE
D1(config-vlan)#exit
D1(config)# interface e1/2
D1(config-if)# no switchport  // Brinda la capacidad capa 3 al puerto
D1(config-if)# ip address 10.77.10.2 255.255.255.0
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  // se configura las IP de la VLAN
D1(config-if)# ip address 10.77.100.1 255.255.255.0
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
D1(config-if)# ip address 10.77.101.1 255.255.255.0
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
D1(config-if)# ip address 10.77.102.1 255.255.255.0
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 10.77.101.1 10.77.101.109
D1(config)# ip dhcp excluded-address 10.77.101.141 10.77.101.254
D1(config)# ip dhcp excluded-address 10.77.102.1 10.77.102.109
D1(config)# ip dhcp excluded-address 10.77.102.141 10.77.102.254
D1(config)# ip dhcp pool VLAN-101 // Crea el pool para la VLAN
D1(dhcp-config)# network 10.77.101.0 255.255.255.0
D1(dhcp-config)# default-router 10.77.101.254
```

```
D1(dhcp-config)# exit
D1(config)# ip dhcp pool VLAN-102
D1(dhcp-config)# network 10.77.102.0 255.255.255.0
D1(dhcp-config)# default-router 10.77.102.254
D1(dhcp-config)# exit
D1(config)# interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3
D1(config-if-range)# shutdown
D1(config-if-range)# exit
D1(config)# exit
D1# copy running-config startup-config
```

Switch 2:

```
D2#configure terminal
D2(config)#hostname D2
D2(config)#ip routing
D2(config)#ipv6 unicast-routing
D2(config)#no ip domain lookup
D2(config)# banner motd # D2, ENCOR Skills Assessment#
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 e1/0
D2(config-if)# no switchport
D2(config-if)# ip address 10.77.11.2 255.255.255.0
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 10.77.100.2 255.255.255.0
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 10.77.101.2 255.255.255.0
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 10.77.102.2 255.255.255.0
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 10.77.101.1 10.77.101.209
D2(config)# ip dhcp excluded-address 10.77.101.241 10.77.101.254
D2(config)# ip dhcp excluded-address 10.77.102.1 10.77.102.209
D2(config)# ip dhcp excluded-address 10.77.102.241 10.77.102.254
D2(config)# ip dhcp pool VLAN-101
D2(dhcp-config)# network 10.77.101.0 255.255.255.0
D2(dhcp-config)# default-router 77.0.101.254
D2(dhcp-config)# exit
D2(config)# ip dhcp pool VLAN-102
D2(dhcp-config)# network 10.77.102.0 255.255.255.0
D2(dhcp-config)# default-router 10.77.102.254
D2(dhcp-config)# exit
D2(config)# interface range e0/0-3,e1/1-3,e2/0-3,e3/0-3
D2(config-if-range)# shutdown
D2(config-if-range)# exit
D2(config)# exit
D2# copy running-config startup-config
```

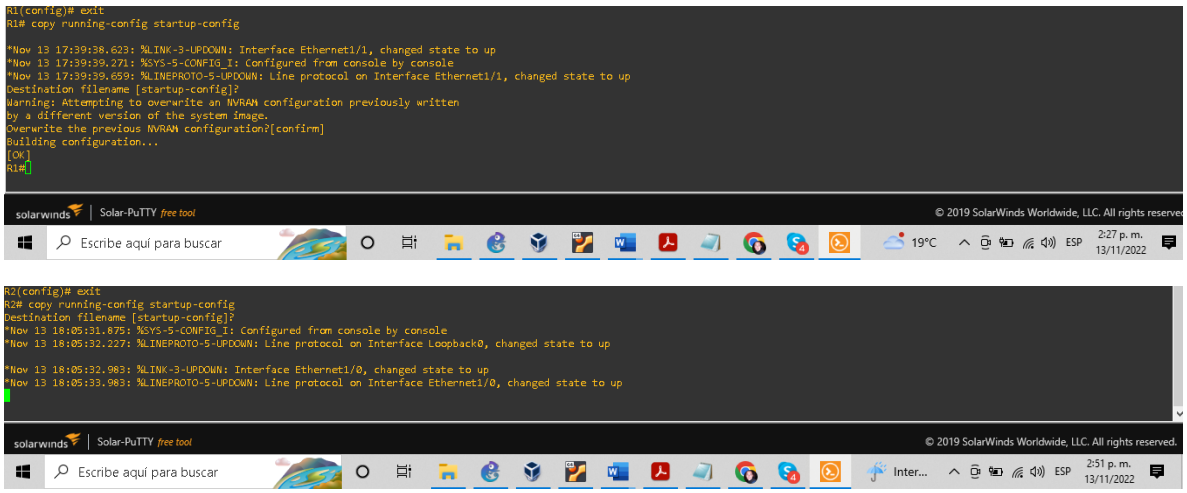
Switch A1:

```
A1#configure terminal
A1(config)#hostname A1
A1(config)#no ip domain lookup
A1(config)# banner motd # A1, ENCOR Skills Assessment#
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 10.77.100.3 255.255.255.0
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 e2/1,e2/2,e2/3,e3/0,e3/0-3,e0/3,e1/0
A1(config-if-range)# shutdown
A1(config-if-range)# exit
A1(config)# exit
A1# copy running-config startup-config
```

El siguiente paso es guardar la configuración en cada dispositivo mediante el comando ***copy running-config startup-config*** como se observa en la figura 2:

Figura 2. Configuración guardada en los dispositivos

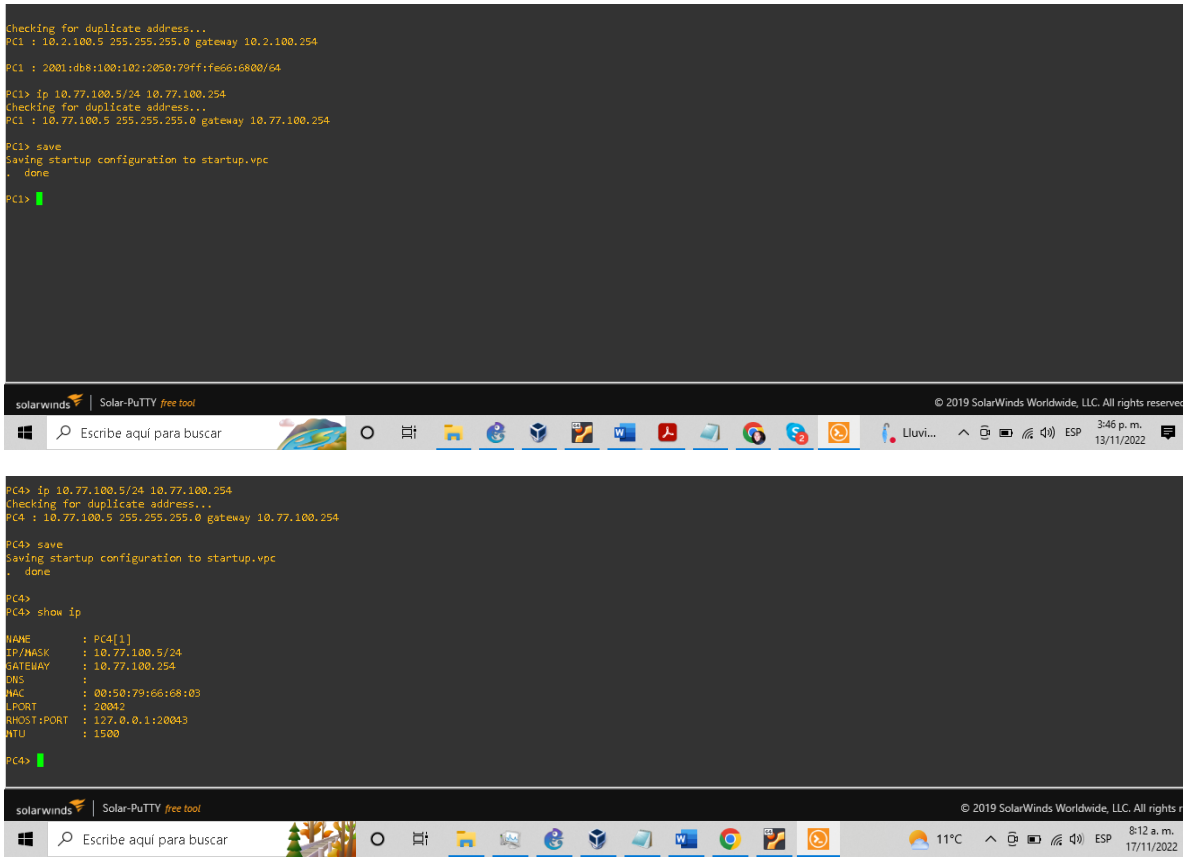


Fuente: Propia

c. Configure el direccionamiento de host de PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.77.100.254, que será la dirección IP virtual de HSRP utilizada en la Parte 4.

Se procede a configurar las direcciones IPv4 e IPv6 en PC1 y PC4, así como el gateway predeterminado, para ello se emplea la tabla 1 de direccionamiento dada anteriormente como se muestra en la figura 3:

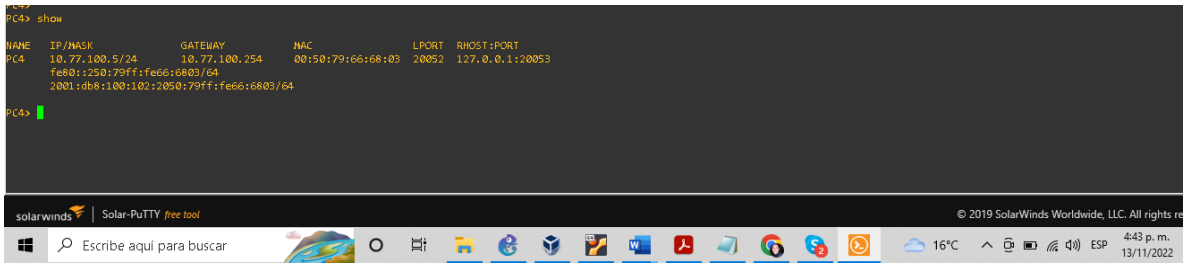
Figura 3. Configuración IP del PC1 y PC4



Fuente: Propia

Ahora se realiza la verificación de la configuración de los PCs:

Figura 4. Verificación de la IP de PC1 y PC4



Fuente: Propia

1.2 Parte 2: Configurar la red de capa 2 y la compatibilidad con el host

En esta parte de la evaluación de habilidades, completará la configuración de la red de capa 2 y configurará el soporte de host básico. Al final de esta parte, todos los interruptores deberían poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC:

Task#	Task	Specification	Points
2.1	On all switches, configure IEEE 802.1Q trunk interfaces on interconnecting switch links	Enable 802.1Q trunk links between: • D1 and D2 • D1 and A1 • D2 and A1	6
2.2	On all switches, change the native VLAN on trunk links.	Use VLAN 999 as the native VLAN.	6
2.3	On all switches, enable the Rapid Spanning-Tree Protocol.	Use Rapid Spanning Tree.	3
2.4	On D1 and D2, configure the appropriate RSTP root bridges based on the information in the topology diagram. D1 and D2 must provide backup in case of root bridge failure.	Configure D1 and D2 as root for the appropriate VLANs with mutually supporting priorities in case of switch failure.	2

Task#	Task	Specification	Points
2.5	On all switches, create LACP EtherChannels as shown in the topology diagram.	Use the following channel numbers: • D1 to D2 – Port channel 12 • D1 to A1 – Port channel 1 • D2 to A1 – Port channel 2	3
2.6	On all switches, configure host access ports connecting to PC1, PC2, PC3, and PC4.	Configure access ports with appropriate VLAN settings as shown in the topology diagram. Host ports should transition immediately to forwarding state.	4
2.7	Verify IPv4 DHCP services.	PC2 and PC3 are DHCP clients and should be receiving valid IPv4 addresses.	1
2.8	Verify local LAN connectivity.	PC1 should successfully ping: • D1: 10.77.100.1 • D2: 10.77.100.2 • PC4: 10.77.100.6 PC2 should successfully ping: • D1: 10.77.102.1 • D2: 10.77.102.2 PC3 should successfully ping: • D1: 10.77.101.1 • D2: 10.77.101.2 PC4 should successfully ping: • D1: 10.77.100.1 • D2: 10.77.100.2 • PC1: 10.77.100.5	1

Tabla 2. Tareas de configuración

En las tareas 2.1 y 2.2 se realizan las configuraciones de las interfaces troncales IEEE 802.1Q en todos los switches, teniendo en cuenta que se debe cambiar la

VLAN nativa en estos enlaces troncales. En las tareas 2.3 y 2.4 se habilitará el protocolo Rapid Spanning-Tree (RSTP) en todos los switches, además, en los switches D1 y D2 se debe configurar los puentes raíz RSTP apropiados según la información del diagrama de topología, teniendo en cuenta que estos deben proporcionar respaldo en caso de falla del puente raíz. En las tareas 2.5 y 2.6 se deben crear LACP EtherChannel en todos los switches, como se muestra en el diagrama de topología, teniendo en cuenta que se deben especificar los números de canal de la siguiente manera: D1 a D2 debe usar el Port channel 12, D1 a A1 debe usar el Port channel 1, D2 a A1debe usar el Port channel 2. Por otro lado, en todos los switches se deben configurar los puertos de acceso de host que se conectan a PC1, PC2, PC3 y PC4 con la configuración de VLAN adecuada, como se muestra en el diagrama de topología, donde se debe evidenciar que los puertos de host deben pasar inmediatamente al estado de reenvío.

Finalmente, para las tareas 2.7 y 2.8 se debe verificar los servicios DHCP IPv4, teniendo en cuenta que PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas, realizando la verificación de la conectividad de la LAN haciendo ping entre los PC y los switches. A continuación, se anexan las líneas de configuración de los dispositivos para dar cumplimiento con estas tareas:

Paso 1: Configurar las interfaces troncales

Switch D1:

```
D1#configure terminal
D1(config)#interface range e2/0-3  // configura un grupo de interfaces
D1(config-if-range)#switchport trunk encapsulation dot1q // establece la encapsulación en el estándar IEEE 802.1Q
D1(config-if-range)#switchport mode trunk //configura la interfaz truncal
D1(config-if-range)#switchport trunk native vlan 999
D1(config-if-range)#channel-group 12 mode active
D1(config-if-range)#no shutdown
D1(config-if-range)#exit
D1(config)#interface range e0/1-2
D1(config-if-range)#switchport trunk encapsulation dot1q
D1(config-if-range)#switchport mode trunk
D1(config-if-range)#switchport trunk native vlan 999
D1((config-if-range)#channel-group 1 mode active
D1(config-if-range)#no shutdown
D1(config)#exit
D1(config)#spanning-tree mode rapid-pvst
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface e0/0
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100
```

D1(config-if)#spanning-tree portfast
D1(config-if)#no shutdown
D1(config-if)#exit
D1(config)#exit
D1#copy running-config startup-config

Switch D2:

D2#configure terminal
D2(config)#interface range e2/0-3
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999 // Configura la VLAN como nativa
D2(config-if-range)#channel-group 12 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#interface range e1/1-2
D2(config-if-range)#switchport trunk encapsulation dot1q
D2(config-if-range)#switchport mode trunk
D2(config-if-range)#switchport trunk native vlan 999
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#no shutdown
D2(config-if-range)#exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#interface e0/0
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102
D2(config-if)#spanning-tree portfast
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#exit
D2#copy running-config startup-config

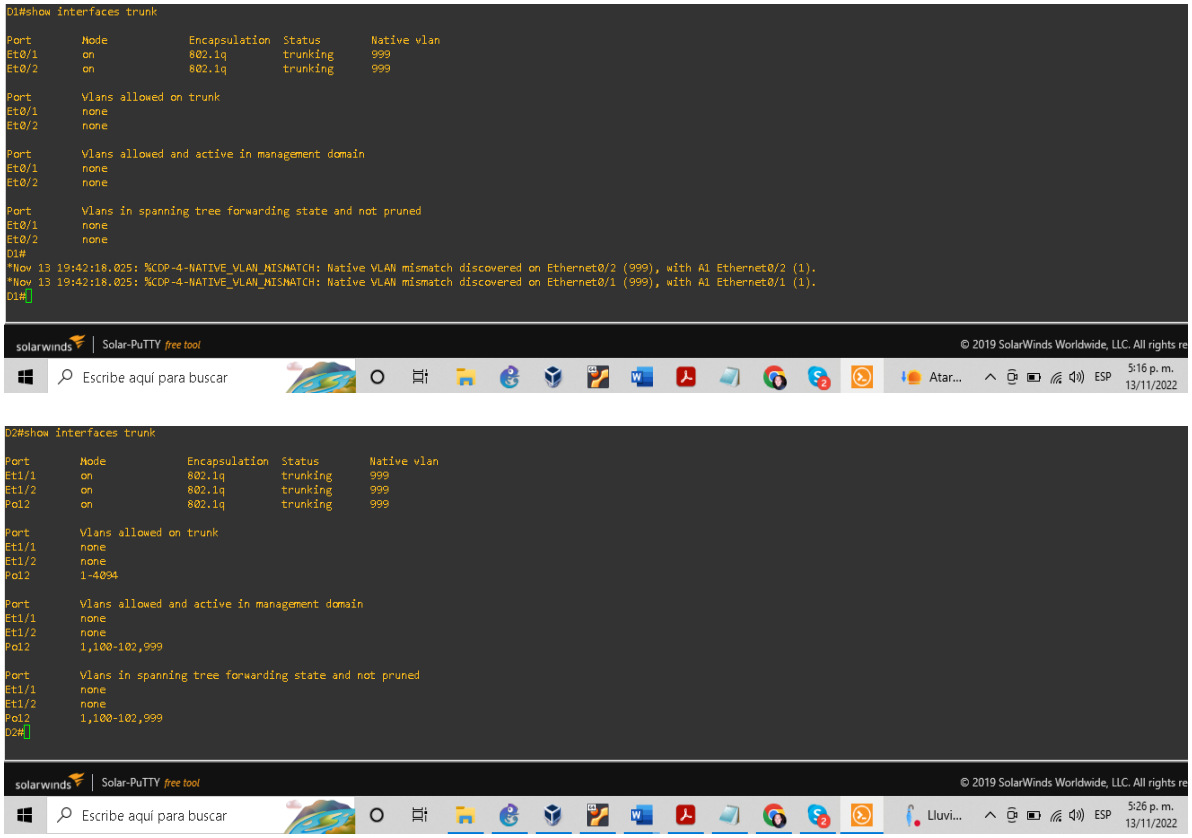
Switch A1:

A1#configure terminal
A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range e0/1-2
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 1 mode active

```
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface range e1/1-2
A1(config-if-range)#switchport trunk encapsulation dot1q
A1(config-if-range)#switchport mode trunk
A1(config-if-range)#switchport trunk native vlan 999
A1(config-if-range)#channel-group 2 mode active
A1(config-if-range)#no shutdown
A1(config-if-range)#exit
A1(config)#interface e1/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#interface e2/0
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100
A1(config-if)#spanning-tree portfast
A1(config-if)#no shutdown
A1(config-if)#exit
A1(config)#exit
A1#copy running-config startup-config
```

Una vez realizada las configuraciones en los dispositivos, el siguiente paso es verificar la configuración de la interfaz troncal y la VLAN nativa en D1 y D2 como se ilustra en la figura 5:

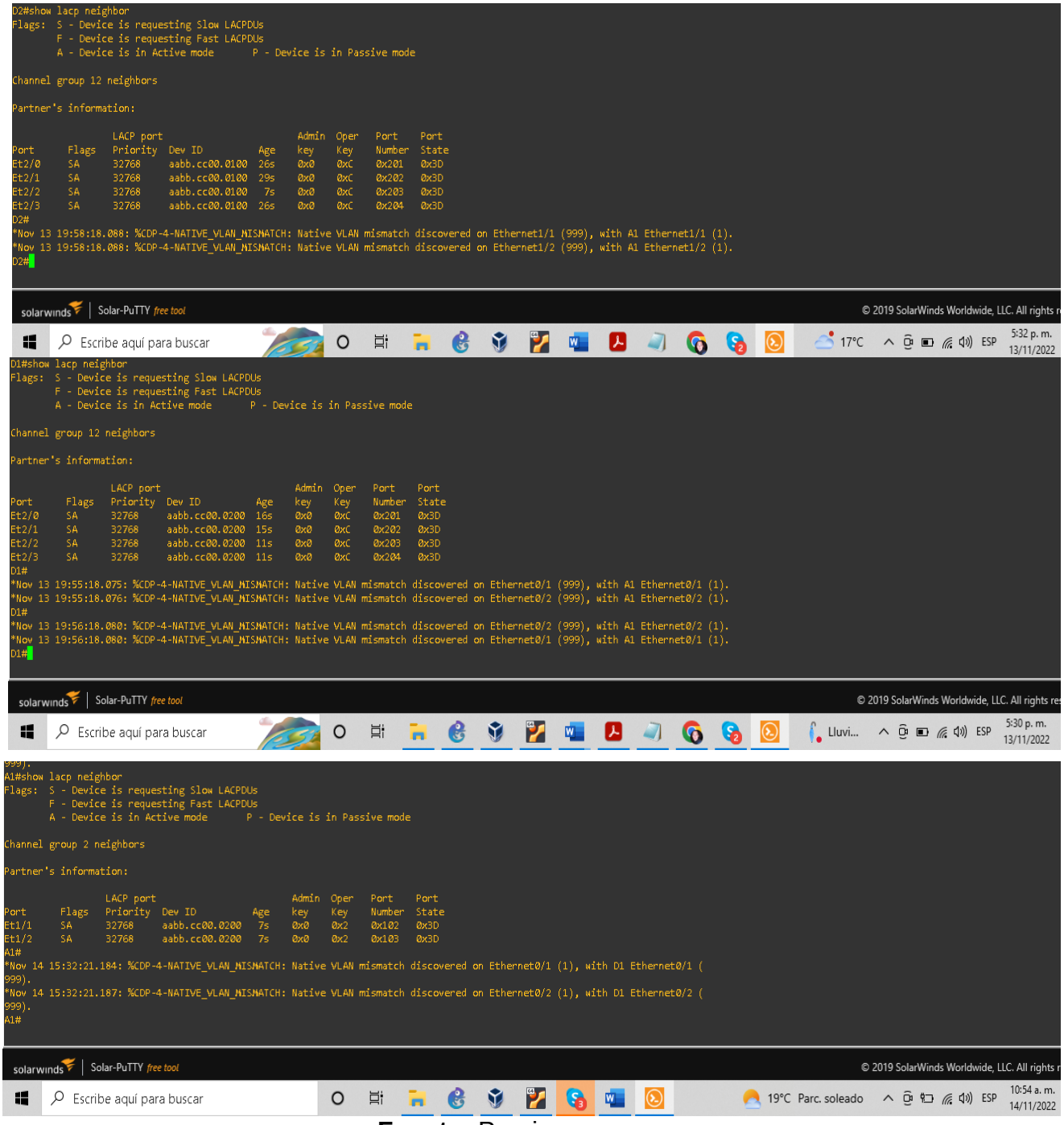
Figura 5. Verificación de las interfaces troncales y la VLAN nativa en D1 y D2



Fuente: Propia

Un aspecto que es necesario a tener en cuenta es que el enlace troncal que se configuro en los puertos del switch permite el paso del tráfico de la VLAN que hemos configurado. Hay que comprender que, sin un enlace troncal, el hecho de querer presentar dos o más VLAN a dos o más switches, necesitaría un enlace de cada VLAN en cada switch a la misma VLAN en todos los demás switches que participan en dicha VLAN. Por otro lado, en la figura 5 se puede ver a simple vista que el puerto está formando un canal de forma eficaz, además de que los canales LACP en los switches están en el modo activo y fueron configurados según la tabla 1 de direccionamiento como se observa en la figura 6.

Figura 6. Verificación de la creación de los LACP EtherChannel



Fuente: Propia

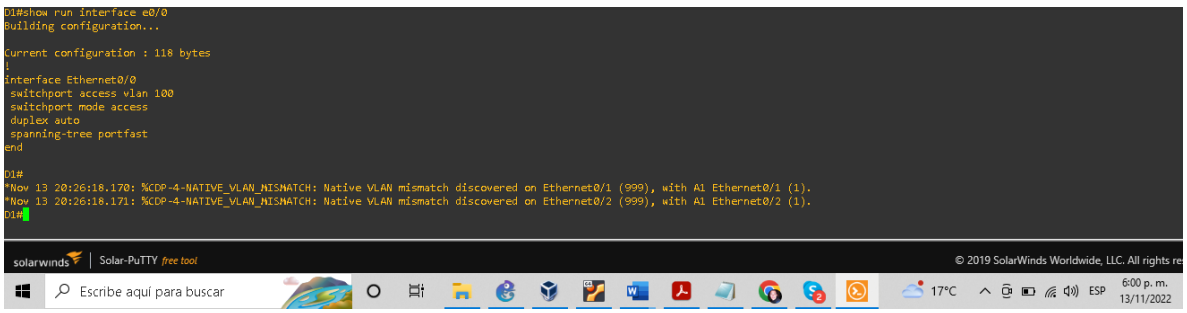
Ahora se verifica la configuración del protocolo Rapid Spanning-Tree (RSTP) en todos los switches, al igual que la configuración del puente raíz RSTP en los switches D1 y D2 como se observa en la figura 7.

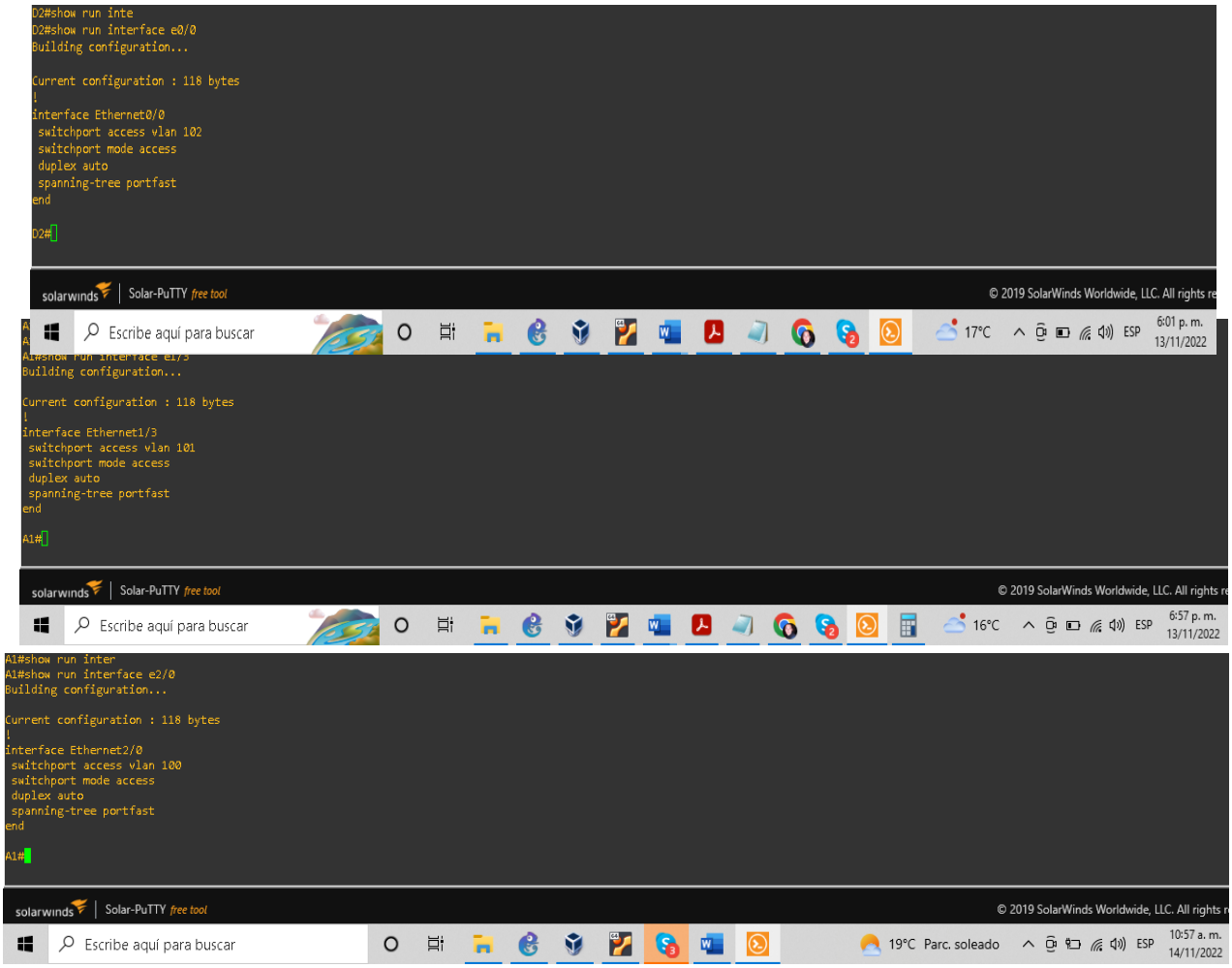
Figura 7. Verificación del RSTP en D1 y D2

Fuente: Propia

En la figura 8 se observa la configuración adecuada de la VLAN en los tres switches teniendo en cuenta el diagrama de topología.

Figura 8. Configuración adecuada de la VLAN en los 3 switches

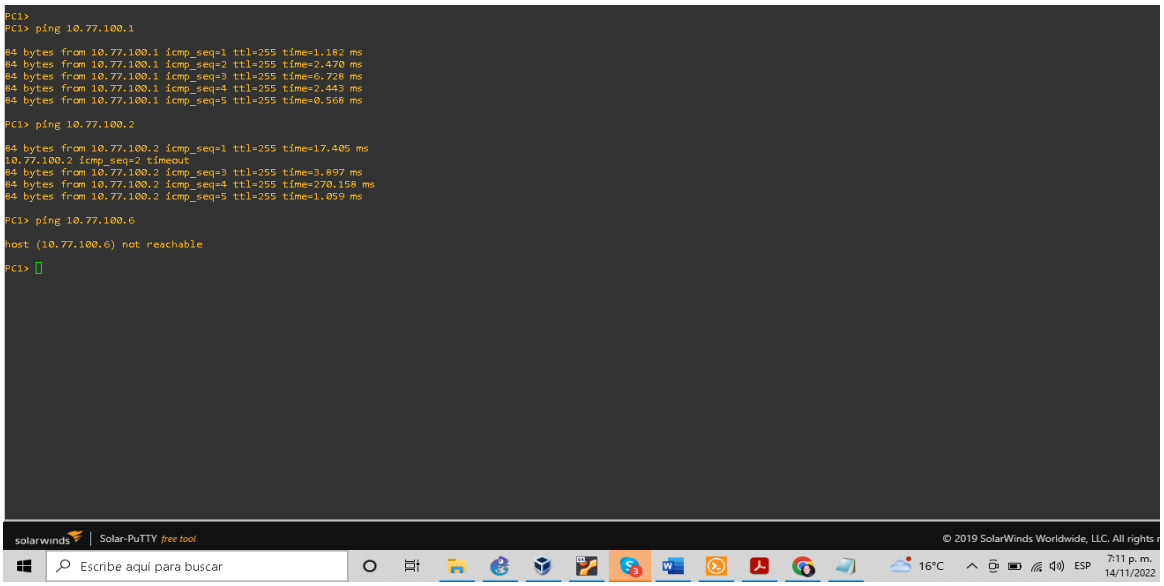




Fuente: Propia

Finalmente, se verifica la conectividad de la LAN haciendo ping entre los PCs y los switches D1 y D2. Para comprobar la conectividad entre los PCs, se ejecute un ***ping*** desde cada PC a los demás. Ejecutamos ping desde el PC1 hacia D1, D2 y PC4 como se observa en la figura 9:

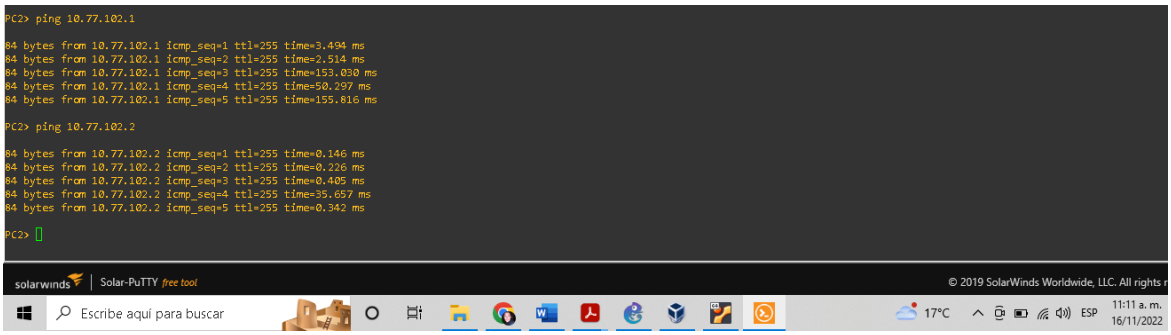
Figura 9. Ping desde PC1 hacia D1, D2 y PC4



Fuente: Propia

Se ejecuta ping desde el PC2 hacia D1 y D2 como se muestra en la figura 10:

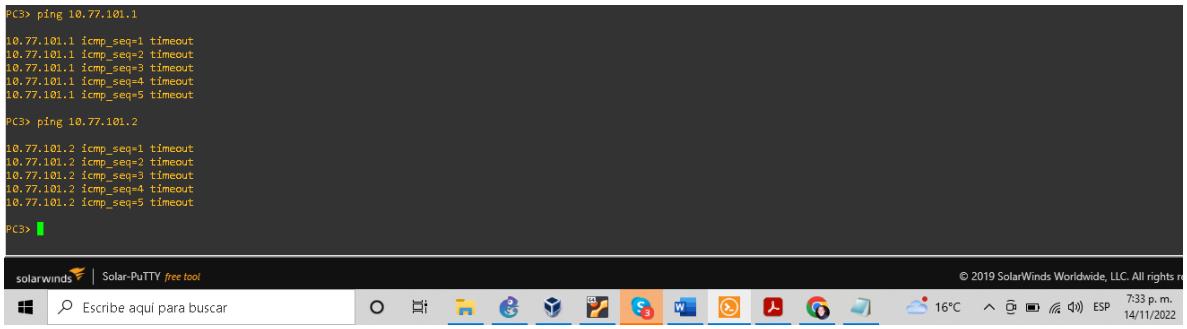
Figura 10. Ping desde PC2 hacia D1 y D2



Fuente: Propia

Se ejecuta ping desde el PC3 hacia D1 y D2 como se muestra en la figura 11:

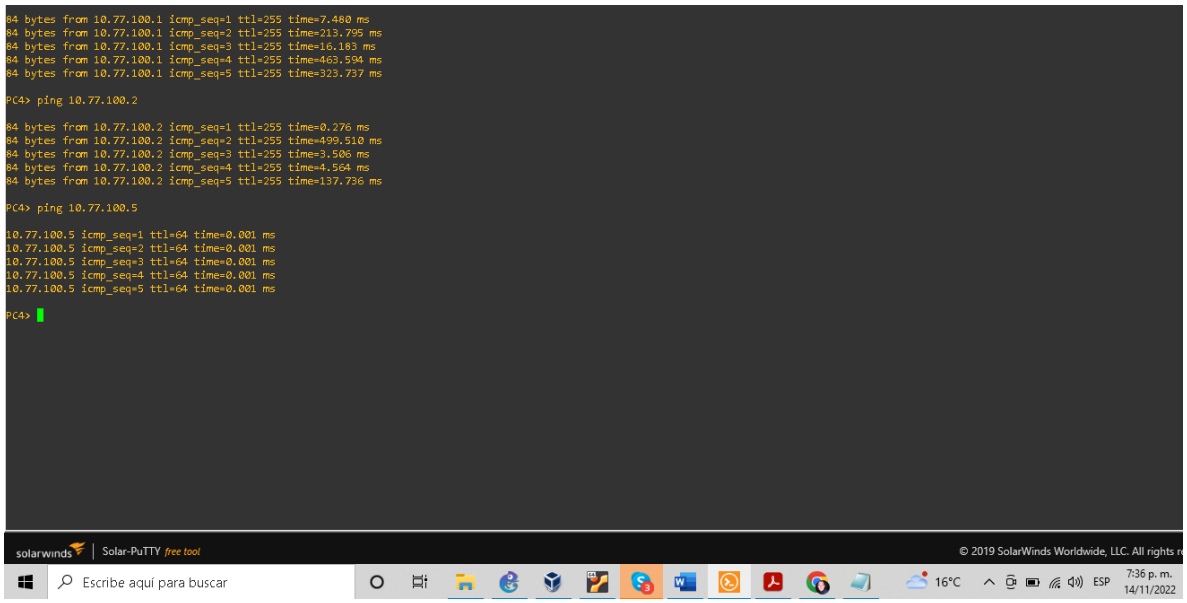
Figura 11. Ping desde PC3 hacia D1 y D2



Fuente: Propia

Finalmente se realiza ping desde el PC4 hacia D1, D2 y PC1 como se muestra en la figura 12:

Figura 12. Ping desde PC4 hacia D1, D2 y PC1



Fuente: Propia

En las figuras 9, 10, 11 y 12 se observa que en este caso el ping ha sido satisfactorio, los cinco paquetes de prueba han llegado correctamente, esto se debe a que los 3 switches se encuentran configurados dentro de la misma VLAN, en este

caso la vlan 999, que les permite cambiar información entre ellos mediante los enlaces troncales que fueron configurados inicialmente.

Parte 3: configurar los protocolos de enrutamiento

Paso 1: Configuración OSPFv2

Router R1:

```
configure terminal
router ospf 4
router-id 0.0.4.1
network 10.77.10.0 0.0.0.255 area 0
network 10.77.13.0 0.0.0.255 area 0
default-information originate
exit
ipv6 router ospf 6
router-id 0.0.6.1
default-information originate
exit
interface e1/2
ipv6 ospf 6 area 0
exit
interface e1/1
ipv6 ospf 6 area 0
exit
```

Router R3:

```
configure terminal
router ospf 4
router-id 0.0.4.3
network 10.77.11.0 0.0.0.255 area 0
network 10.77.13.0 0.0.0.255 area 0
exit
ipv6 router ospf 6
router-id 0.0.6.3
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface e1/1
ipv6 ospf 6 area 0
```

```
exit
exit
```

Swicht D1:

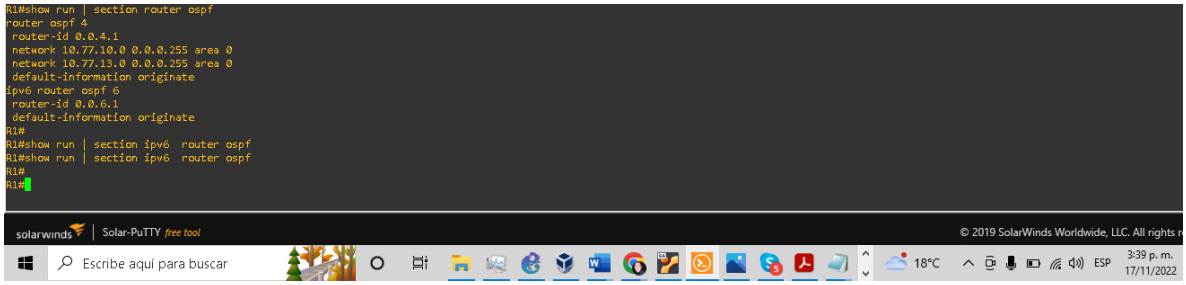
```
configure terminal
router ospf 4
router-id 0.0.4.131
network 10.77.100.0 0.0.0.255 area 0
network 10.77.101.0 0.0.0.255 area 0
network 10.77.102.0 0.0.0.255 area 0
network 10.77.10.0 0.0.0.255 area 0
passive-interface default
no passive-interface e1/2
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface e1/2
exit
interface e1/2
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
exit
```

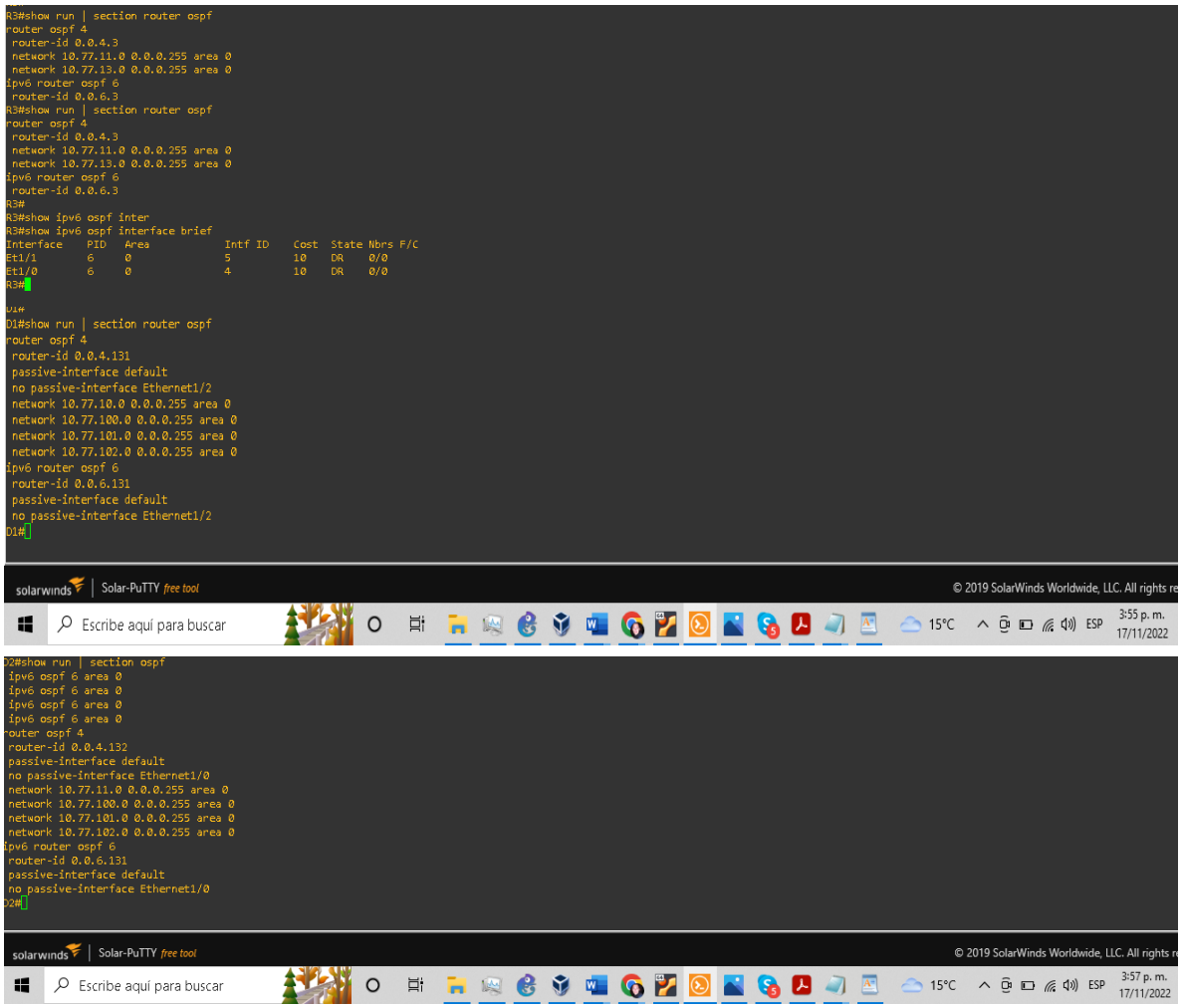
Swicht D2:

```
configure terminal
router ospf 4
router-id 0.0.4.132
network 10.77.100.0 0.0.0.255 area 0
network 10.77.101.0 0.0.0.255 area 0
network 10.77.102.0 0.0.0.255 area 0
network 10.77.11.0 0.0.0.255 area 0
passive-interface default
```

no passive-interface e1/0
exit
ipv6 router ospf 6
router-id 0.0.6.131
passive-interface default
no passive-interface e1/0
exit
interface e1/0
ipv6 ospf 6 area 0
exit
interface vlan 100
ipv6 ospf 6 area 0
exit
interface vlan 101
ipv6 ospf 6 area 0
exit
interface vlan 102
ipv6 ospf 6 area 0
exit
exit

***Figura 13**. Verificación de la tabla de ruta IPv6, OSPFv2-OSPFv3*





Fuente: Propia

Paso 3: Configuración MP-BGP en la red ISP R2.

Router R2:

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

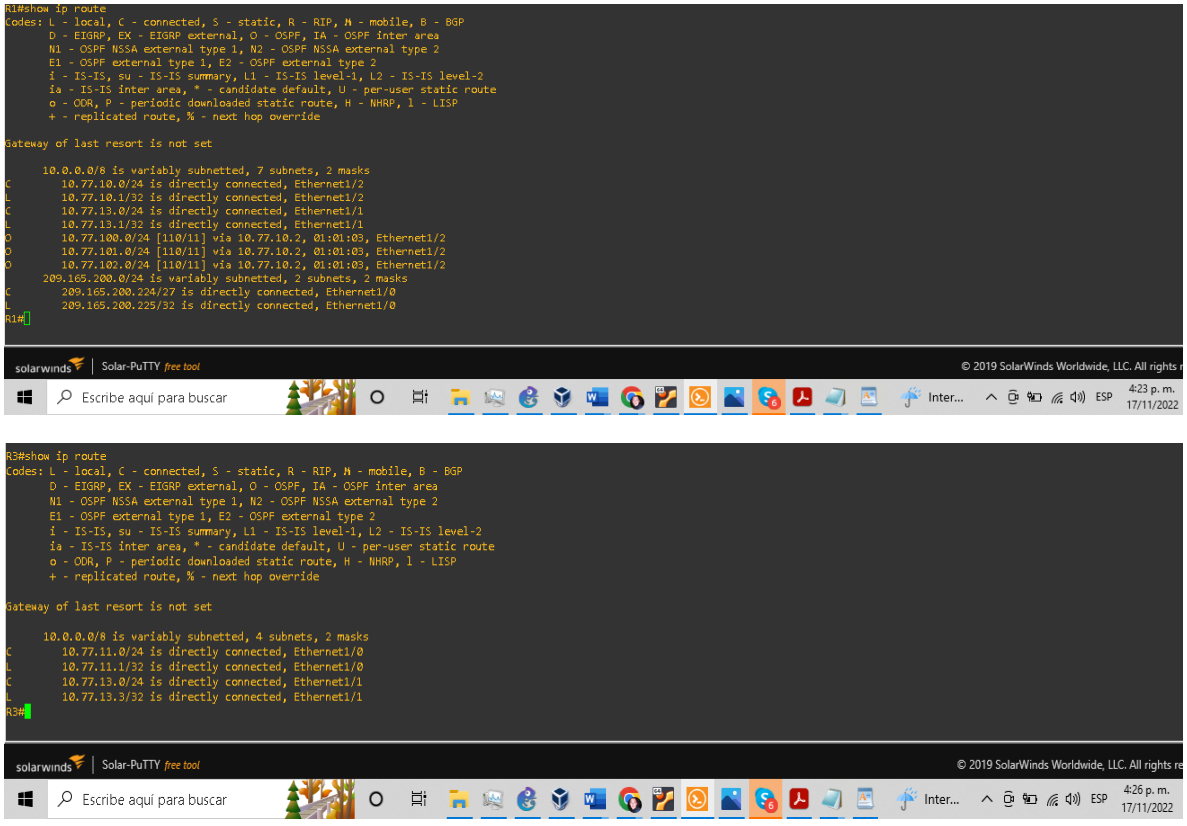
Paso 4: Configuración MP-BGP en la red ISP R1

Router R1:

```
configure terminal
ip route 10.77.0.0 255.0.0.0 null0
ipv6 route 2001:db8:100::/48 null0
router bgp 300
bgp router-id 1.1.1.1
neighbor 209.165.200.226 remote-as 500
neighbor 2001:db8:200::2 remote-as 500
address-family ipv4 unicast
neighbor 209.165.200.226 activate
no neighbor 2001:db8:200::2 activate
network 10.77.0.0 mask 255.0.0.0
exit-address-family
address-family ipv6 unicast
```

no neighbor 209.165.200.226 activate
neighbor 2001:db8:200::2 activate
network 2001:db8:100::/48
exit-address-family
exit

***Figura 14**. Verificación de la tabla de ruta IPv4:*



Fuente:Propia

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

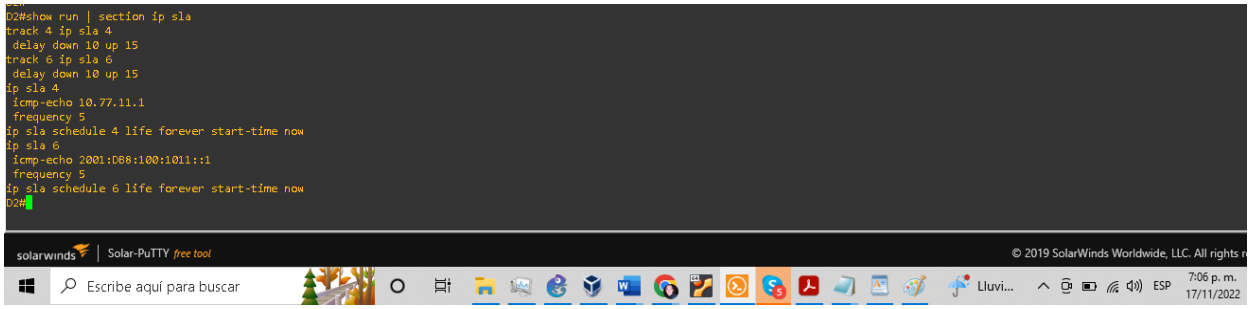
Paso 2: En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 E1/0.

Switch D2:

```
configure terminal
ip sla 4
icmp-echo 10.77.11.1
frequency 5
exit
ip sla 6
icmp-echo 2001:db8:100:1011::1
frequency 5
exit
ip sla schedule 4 life forever start-time now
ip sla schedule 6 life forever start-time now
track 4 ip sla 4
delay down 10 up 15
exit
track 6 ip sla 6
delay down 10 up 15
exit
interface vlan 100
standby version 2
standby 104 ip 10.77.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.77.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.77.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
```

standby 126 preempt
standby 126 track 6 decrement 60
exit

***Figura 15**. Verificación de las SLAs.*



Fuente: Propia

Paso 3: En D1 configure HSRPv2.

Switch D1:

interface vlan 100
standby version 2
standby 104 ip 10.77.100.254
standby 104 priority 150
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 priority 150
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.77.101.254
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.77.102.254

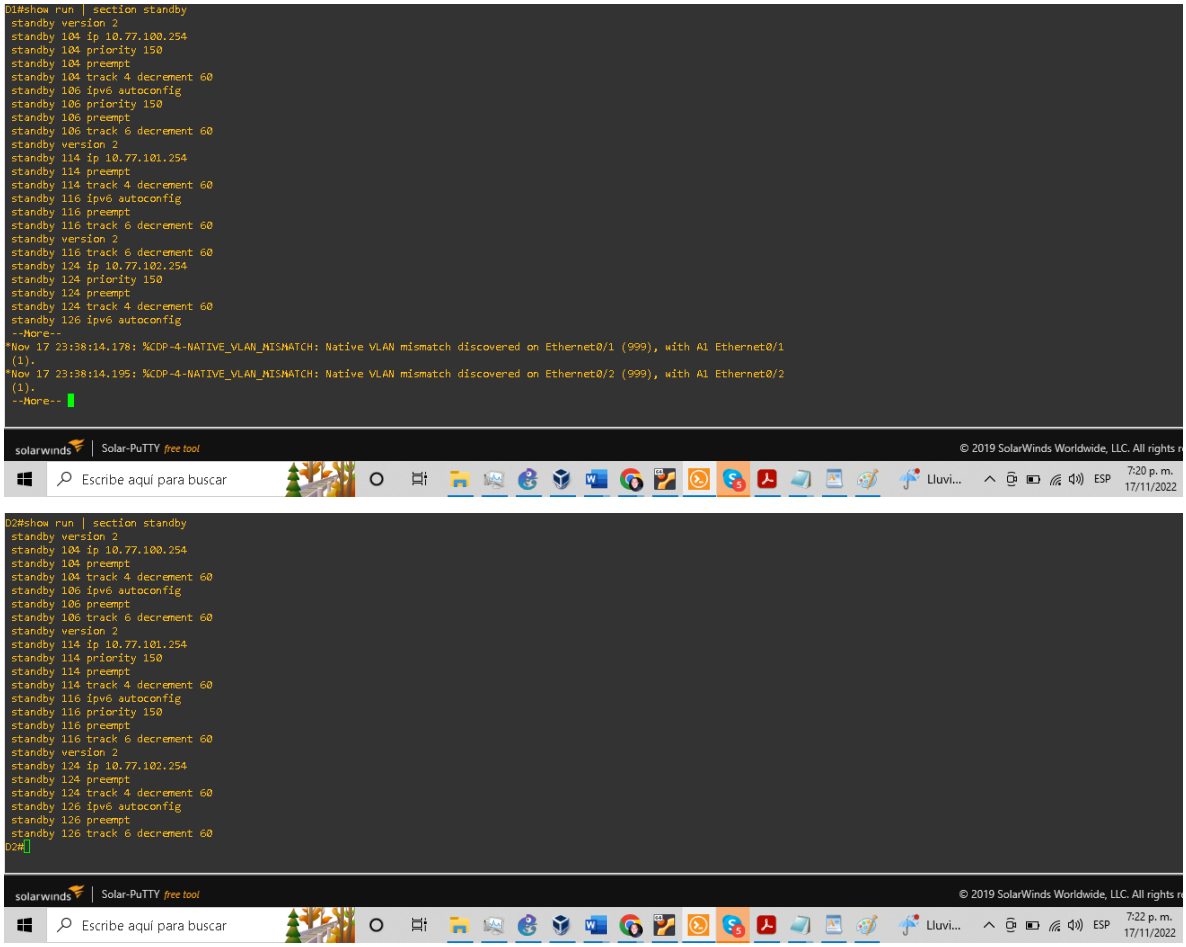
```
standby 124 priority 150
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 priority 150
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Paso 4: En D2 configure HSRPv2.

Switch D2:

```
interface vlan 100
standby version 2
standby 104 ip 10.77.100.254
standby 104 preempt
standby 104 track 4 decrement 60
standby 106 ipv6 autoconfig
standby 106 preempt
standby 106 track 6 decrement 60
exit
interface vlan 101
standby version 2
standby 114 ip 10.77.101.254
standby 114 priority 150
standby 114 preempt
standby 114 track 4 decrement 60
standby 116 ipv6 autoconfig
standby 116 priority 150
standby 116 preempt
standby 116 track 6 decrement 60
exit
interface vlan 102
standby version 2
standby 124 ip 10.77.102.254
standby 124 preempt
standby 124 track 4 decrement 60
standby 126 ipv6 autoconfig
standby 126 preempt
standby 126 track 6 decrement 60
exit
```

Figura 15. *Verificación del Standby*



Fuente: Propia

CONCLUSIONES

Es interesante notar cómo la combinación de técnicas y protocolos como:

Redundancia de enlaces, Spanning tree y LACP para aprovechar al máximo la conectividad de capa 2; donde el primero permite la tolerancia a fallas y protege contra la inactividad, el segundo asegura que solo existe una ruta lógica y evita bucles en estas redundancias, finalmente LACP agrupa la redundancia física en un solo enlace lógico de alta velocidad; una combinación poderosa, pero debe hacerse con cuidado y para evitar crear errores pre calculados en la red.

Los protocolos de enrutamiento utilizados en este escenario OSPF y BGP son los protocolos más comunes que se pueden encontrar en un entorno real, muchas organizaciones utilizan OSPF para el enrutamiento como un protocolo interno porque permite que se conozca toda la red a través de la tabla de enrutamiento de cada enrutador evitando bucles. también actualizar automáticamente las tablas con cualquier cambio en la topología; BGP para conectar sistemas autónomos porque normalmente no todas las organizaciones usan el mismo protocolo de enrutamiento interno que los ISP.

De acuerdo con lo que se dijo anteriormente sobre la importancia de la redundancia de capa 3, también se utilizan para evitar que los dispositivos locales queden fuera de la red debido a una falla en el puerto, utilizando SLA para monitorear continuamente las interfaces de puerta de enlace y HSRP para tener un enrutador trabajando con el interfaz virtual y la otra en espera.

Debido a la gran cantidad de amenazas que existen en la red, es importante utilizar protocolos para mejorar la seguridad e integridad de los dispositivos conectados localmente. En este caso se utiliza el apellido AAA, donde se verifica que el usuario loqueado es quien dice ser. es decir, proporciona privilegios preestablecidos por el administrador y también registra todos los eventos en modo de registro para que se puedan identificar las acciones realizadas.

BIBLIOGRAFIA

ARIGANELLO, E., SEVILLA, E. Redes CISCO. CCNP a fondo. Guía de estudio para profesionales. Editorial RA-MA S.A Editorial y Publicaciones. Madrid. Pág. 201-225

DUGGNA, M. Cisco CCIE Routing and Switching v5.0 Configuration Practice Labs. Pearson Education. Third Edition

TEARE, D., VACHON B., GRAZIANI, R. (2015). CISCO Press (Ed). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101

EDGEWORTH, R., FOSS, A., RIOS, R. (2015). CISCO Press (Ed). IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols.

HUCABY, D., MCQUERRY, S. (2003). CISCO Press (Ed). Cisco Field Manual: Catalyst Switch Configuration. A complete, concise reference for implementing the most features of the Cisco family of switches.

JACK, T. (2004). CCNP: Building Cisco MultiLayer Switched Networks Study Guide

FROOM, R., SIVASUBRAMANIAN, B., FRAHIM, E. (2010). CISCO Press (Ed) Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide Foundation Learning for SWITCH 642-813