DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HAYR ALEXIS MARTINEZ PEÑA

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HAYR ALEXIS MARTINEZ PEÑA

DIPLOMADO DE OPCIÓN DE GRADO PARA OPTAR 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
DUITAMA
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Duitama, 29 de noviembre 2021

AGRADECIMIENTOS

De ante mano quiero agradecer a Dios y mi familia por brindarme el apoyo incondicional para cumplir con mis sueños y metas, por otro lado, quiero agradecer el apoyo durante todo este proceso al Ingeniero Héctor Julian Parra y al Director Gerardo Granados Acuña por brindarme las herramientas y retroalimentar las inquietudes que tuve durante la culminación del diplomado de profundización en CCNP, el cual me permite estar un paso más cerca de ser profesional. De igual manera agradecido con cada uno de los docentes y compañeros que a lo largo de estos años han influido en mi para que el día de hoy este cumpliendo uno de mis más grandes sueños.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CCNP: Curso de certificación en networking profesional el cual consiste en diseñar e implementar redes, se centra en aportar y garantizar conocimientos y habilidades prácticas y concretas a la hora de ofrecer soluciones complejas y soporte a redes empresariales mayores, garantizando que éstas puedan perdurar en el tiempo y ser de gran utilidad a empresas y proyectos.

Packet Tarcer: Es un software de simulación el cual permite recrear un entorno administrar equipos cisco, los cuales permiten crear distintas simulaciones del funcionamiento o instalación de redes de telecomunicaciones e informática.

Topología de Red: Conjunto de nodos o mapa lógico o físico que conforman una red con el fin de enviar y recibir datos de los equipos conectados a la red, en esta abarcan distintos tipos de topologías las cuales son empleadas para casos específicos al momento de diseñar una red.

Enrutamiento: Es una función la cual permite a los router o switches capa 2 o 3, buscar un camino redirigiendo paquetes de datos por una interfaz especifica la cual permite establecer comunicación en topologías muy grandes o con cantidad de redes y equipos, así poder facilitar el intercambio de información entre ellos.

IPv4: Protocolo de internet versión 4, el cual permite la interconexión de datos en redes basadas en internet, permite el envío y recepción de datos entre equipos de red.

VLAN: Red de área local virtual, la cual consiste en crear generar redes virtuales independientes alojadas dentro de un mismo router permitiendo ampliar la red LAN de una forma en la cual no es necesario disponer de más equipos de red. Hoy en día es mucho más común tener este tipo de infraestructura en empresas y demás entes.

Interfaces de Red: Permite utilizar el servicio de enrutamiento y comunicación o acceso remoto con distintos equipos de red, permitiendo el intercambio de paquetes entre ellos.

RESUMEN

En el presente documento se evidencia las pruebas de habilidades prácticas para el diplomado de profundización CCNP, el cual consiste en implementar por medio de un escenario propuesto los conocimientos teóricos y prácticos en el área de networking de CISCO. Por medio de un software de simulación (Packet tracer), se implementa la solución para el escenario mencionado con anterioridad, evidenciando por medio de comandos y evidencias ilustrativas. Aplicando protocolos de enrutamiento para establecer una conmutación de los equipos de red y servicios configurados en las distintas redes, este tipo de escenarios son muy comunes en las ramas de la electrónica y las telecomunicaciones.

Por otro lado, el documento permite al lector evidenciar cada una de las etapas tratadas en el mismo, verificando así el trabajo que se realizó en temas de enrutamiento, protocolos de IPv4 y IPv6, seguridad y demás servicios configurados en el escenario, permitiendo evidenciar la aplicación de cada uno de los conceptos mencionados durante el desarrollo del diplomado de profundización CCNP.

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

ABSTRACT

This document shows the practical skills tests for the CCNP deepening diploma, which consists of implementing through a proposed scenario the theoretical and practical knowledge in the CISCO networking area. By means of a simulation software (Packet tracer), the solution for the scenario is implemented, showing through commands and illustrative evidence. Applying routing protocols to establish a switching of the network equipment and services configured in the different networks, these types of scenarios are very common in the branches of electronics and telecommunications.

On the other hand, the document allows the reader to highlight each of the stages covered in it, thus verifying the work that was carried out on issues of routing, IPv4 and IPv6 protocols, security and other services configured in the scenario, allowing to demonstrate the application of each of the concepts mentioned during the development of the CCNP in-depth diploma.

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

INTRODUCCIÓN

En el presente documento corresponde a evidenciar las habilidades adquiridas durante el transcurso del diplomado de profundización CCNP, lo cual se puede apreciar en el desarrollo y solución del escenario planteado. Por otro lado, es importante el uso y estudio de los temas vistos durante todo el diplomado el cual ayudo a mejorar las capacidades y conocimientos que permitirán al profesional diseñar y solucionar requerimientos en networking respecto a tecnologías Cisco.

Se presenta un único escenario el cual está dividido en 6 partes en lo que compete a la solución de este, se utiliza como software de simulación (Packet tracer) en el cual se implementó la topología solicitada que contaba con los siguientes equipos: 3 router 4221, 2 switches 3650 y 1 switch 2960. Los cuales nos permitieron concretar las siguientes partes que consistente: Parte 1 consiste en cablear cada uno de los equipos como muestra la topología, configurar los parámetros básicos en cada uno de los dispositivos como lo fue direccionamiento IPv6 – IPv4, subir interfaces, creación de VLANs, crear pool DHCP para este servicio y por último guardar cada una de las configuraciones. Parte 2 se prioriza la configuración en los switches, se crean canales EtherChannel por medio de LACP, las interfaces se configuran en modo troncal, se cambió la VLAN nativa, se activa protocolo RSPT, se les da accesibilidad a los puertos, se realizan pruebas en la red LAN. Parte 3 se realiza enrutamiento por medio de protocolo OSPF, se deja una ruta por defecto de respaldo, se hace uso de redes IPS, se hace uso del protocolo BGP para la relación de vecino.

Llegando a la parte 4 donde se configura la redundancia de la red en general, se crean IPs SLAs las cuales permiten verificar disponibilidad de la interfaz, por otro lado, se configuro HSRP version 2 el cual permite administrar direcciones virtuales (Interfaces VLAN creadas en la parte 1). Parte 5 se realiza la parte de seguridad en la cual se configura protección en modo privilegiado, encriptación, se crea usuario y se le asignan permisos nivel 15 (acceso total), se habilita protocolo AAA. Por último, en la parte 6, se configura hora y fecha, se configura un servidor NTP para sincronizar los dispositivos, se configura syslog y SNMPv2c, y con eso se dio solución al escenario planteado.

ESCENARIO 1

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

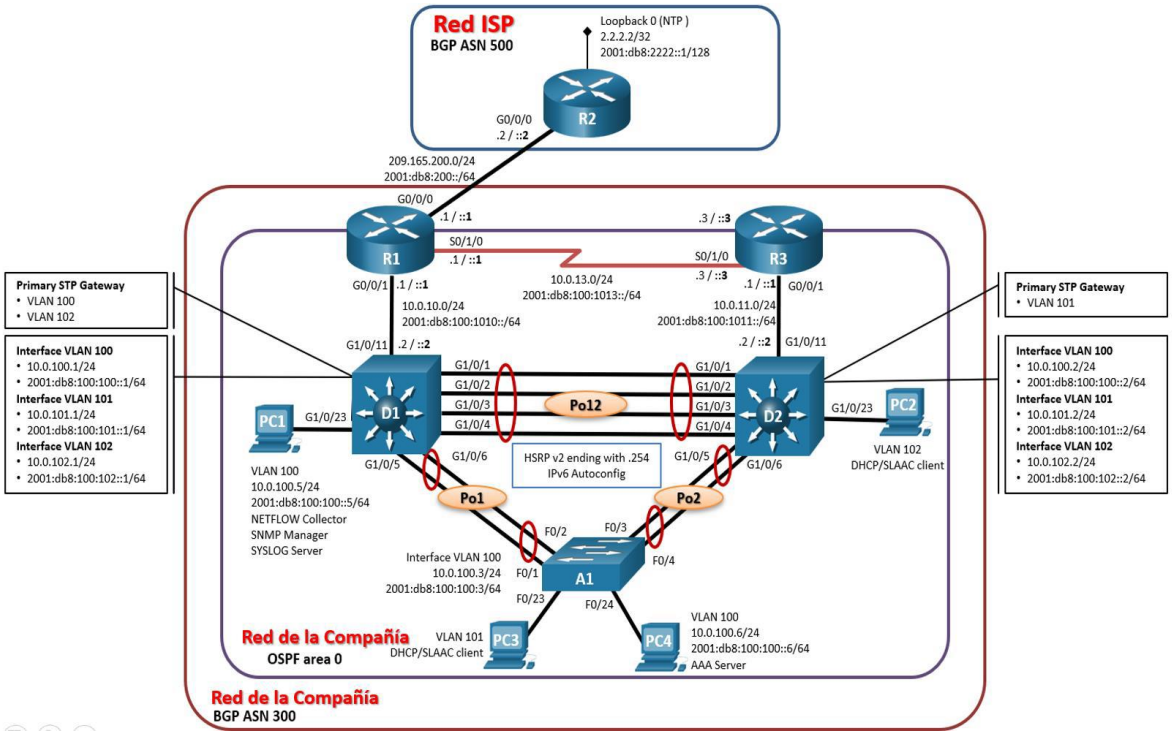

Figura 1. Escenario propuesto

Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
R1	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
R1	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
R2	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
R3	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
D1	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
D1	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
D1	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
D2	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
D2	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
D2	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

Tabla 1. Tabla de direccionamiento

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

Paso 1: Cablear la red como se muestra en la topología.
Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

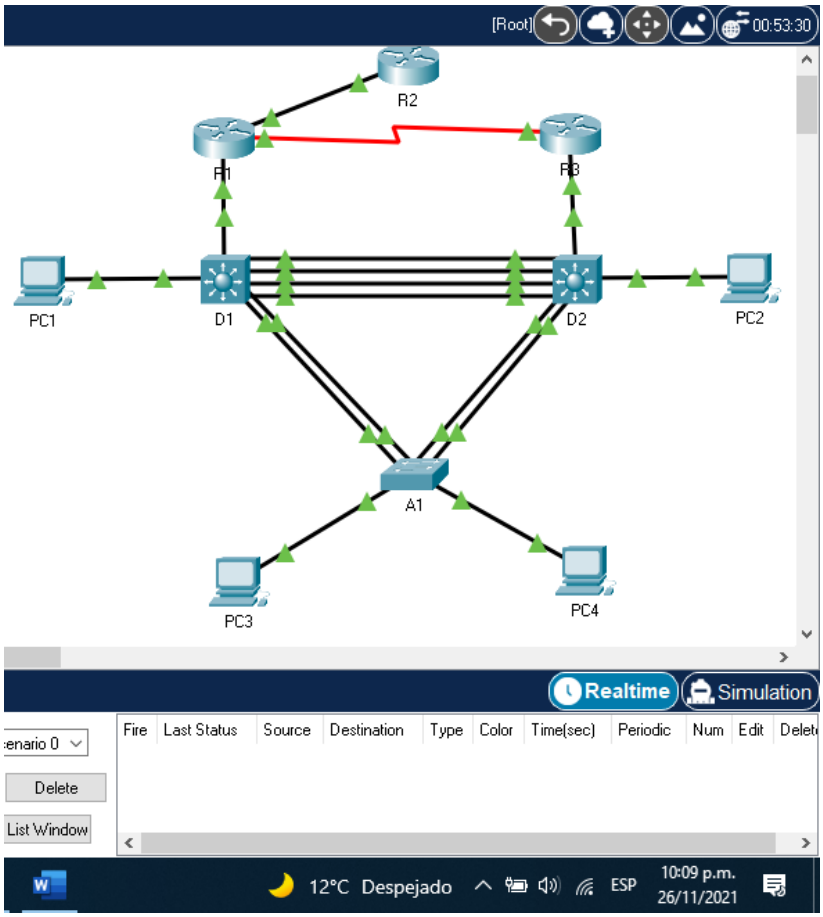

Figura 2. Topología de red - Packet tracer

En este paso se realiza conexión de los equipos físicos por medio de cable ethernet y cable serial correspondientemente, estas conexiones se hacen a las interfases correspondientes según el escenario planteado.

Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Se realiza la siguiente configuración en el R1, a continuación, se indican los comandos utilizados.

```
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit

R1(config)#interface g0/0/0
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)#interface g0/0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:2 link-local
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64
R1(config-if)#no shutdown

R1(config)#interface s0/1/0
R1(config-if)#ip address 10.0.13.1 255.255.255.0
R1(config-if)#ipv6 address fe80::1:3 link-local
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64
R1(config-if)#no shutdown
```

Como se puede apreciar en la configuración anterior, lo que se hizo en R1 fue ingresar a modo privilegiado y después a modo configuración para establecer un nombre al dispositivo, se activa modo global de rounting IPV6, desactivar la IP dominio de la red virtual (lookup), se configura IPV4 y IPV6 en las interfaces g0/0/0, g0/0/1 y serial0/1/0, estas dejándolas encendidas.

Se realiza la siguiente configuración en el R2, a continuación, se indican los comandos utilizados.

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

R2(config)#interface g0/0/0
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)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
```

Como se puede apreciar en la configuración anterior, lo que se hizo en R1 fue ingresar a modo privilegiado y después a modo configuración para establecer un nombre al dispositivo, se activa modo global de rounting IPV6, desactivar la IP dominio de la red virtual (lookup), se configura IPV4 y IPV6 en las interfaces g0/0/0, g0/0/1 y Loopback 0 es interfaz virtual probar capacidad de envió de datos utilizando BGP, estas dejándolas encendidas.

Se realiza la siguiente configuración en el R3, a continuación, se indican los comandos utilizados.

```
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
```

```
R3(config-line)#logging synchronous
R3(config-line)#exit

R3(config)#interface g0/0/1
R3(config-if)#ip address 10.0.11.1 255.255.255.0
R3(config-if)#ipv6 address fe80::3:2 link-local
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64
R3(config-if)#no shutdown

R3(config)#interface s0/1/0
R3(config-if)#ip address 10.0.13.3 255.255.255.0
R3(config-if)#ipv6 address fe80::3:3 link-local
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64
R3(config-if)#no shutdown
```

Como se puede apreciar en la configuración anterior, lo que se hizo en R1 fue ingresar a modo privilegiado y después a modo configuración para establecer un nombre al dispositivo, se activa modo global de rounting IPV6, desactivar la IP dominio de la red virtual (lookup), se configura IPV4 y IPV6 en las interfaces g0/0/0, g0/0/1 y serial0/1/0, estas dejándolas encendidas.

Se realiza la siguiente configuración en el D1, a continuación, se indican los comandos utilizados.

```
Switch(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, 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
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 g1/0/11
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
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
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
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
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool VLAN-101
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
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
```

Como se puede apreciar en la configuración anterior, lo que se hizo en D1 fue ingresar a modo privilegiado y después a modo configuración para establecer un nombre al dispositivo, se activa modo global de rounting IPV6, desactivar la IP

dominio de la red virtual (lookup), se configura IPV4 y IPV6 en la interface g1/0/11, por otro lado se crean Vlans y se cambia el número de la Vlan nativa, se asignan IPV4 y IPV6 a las interfaces de las Vlan creadas, se crea un dhcp individual para la Vlan 101 y 102, se realiza una exclusión de IPs para el dhcp.

Se realiza la siguiente configuración en el D2, a continuación, se indican los comandos utilizados.

```
Switch(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, 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 g1/0/11
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
```

Como se puede apreciar en la configuración anterior, lo que se hizo en D2 fue ingresar a modo privilegiado y después a modo configuración para establecer un nombre al dispositivo, se activa modo global de rounting IPV6, desactivar la IP dominio de la red virtual (lookup), se configura IPV4 y IPV6 en la interface g1/0/11, por otro lado se crean Vlans y se cambia el número de la Vlan nativa, se asignan IPV4 y IPV6 a las interfaces de las Vlan creadas, se crea un dhcp individual para la Vlan 101 y 102, se realiza una exclusión de IPs para el dhcp.

Se realiza la siguiente configuración en el A1, a continuación, se indican los comandos utilizados.

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

```
A1(config-vlan)#name Management
A1(config-vlan)#exit
A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit
A1(config)#vlan 102
A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999
A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
```

Se utiliza el siguiente comando para habilitar la configuración en IPV6 del switch, después de hacer esto hacemos un reload y seguimos con la configuración.

```
A1(config)#sdm prefer dual-ipv4-and-ipv6 default
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
```

Como se puede apreciar en la configuración anterior, lo que se hizo en A1 fue ingresar a modo privilegiado y después a modo configuración para establecer un nombre al dispositivo, se activa modo global de rounting IPV6, desactivar la IP dominio de la red virtual (lookup), por otro lado se crean Vlans y se cambia el número de la Vlan nativa, se asignan IPV4 y IPV6 a las interfaces de las Vlan creadas.

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

Se realiza el proceso de guardado en cada uno de los dispositivos, utilizando el siguiente comando, esto se debe hacer en modo privilegiado.

Copy running-config startup-config

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

En este paso se realiza direccionamiento estático en los PC1 y PC4, como se muestra en las siguientes figuras.

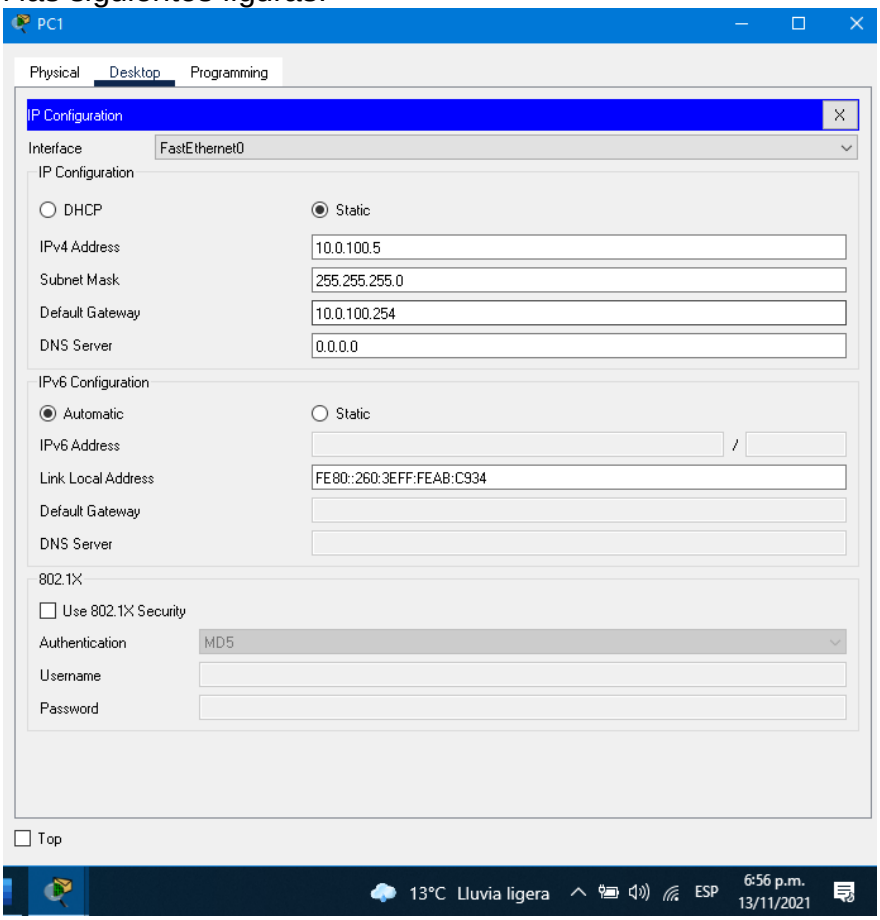

Figura 3. Asignación IP estática PC1

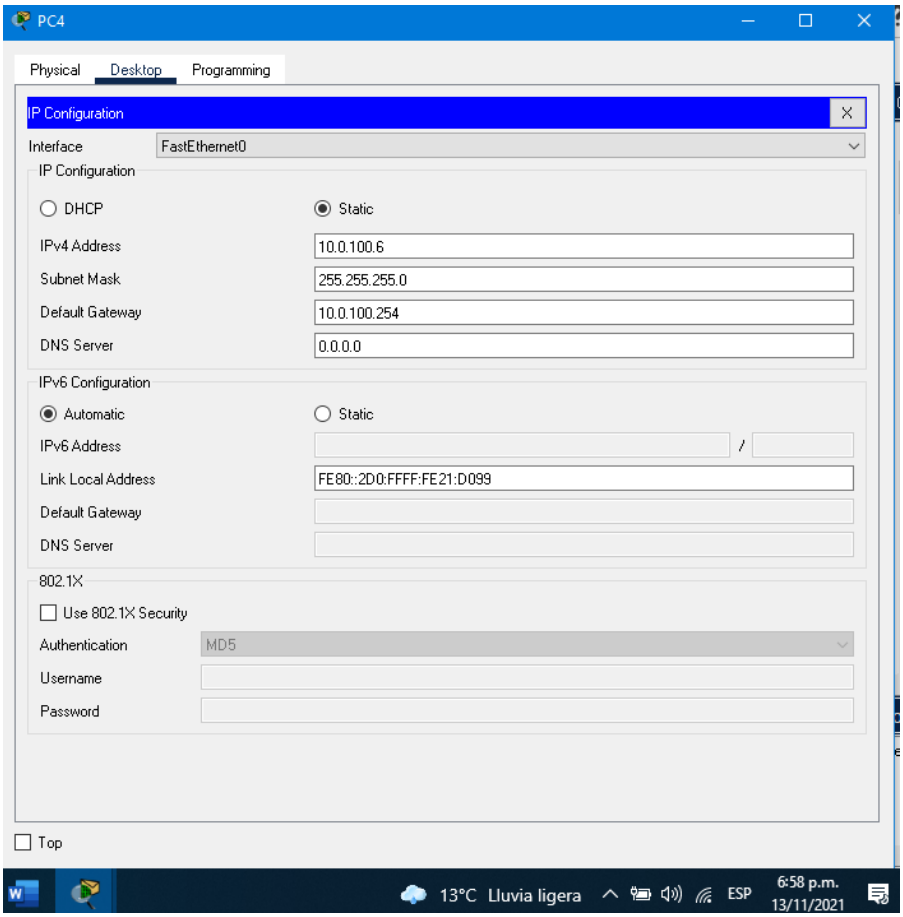

Figura 4. Asignación IP estática PC4

Parte 2: Configurar la capa 2 de la red y el soporte de Host.
En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

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

2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.
2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

Tabla 2. Lista de tareas parte 2

Tarea 2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

Para configurar el modo troncal en las interfaces, esto se hace en cada interfaz de las que se necesita este modo, para ello se tienen que ingresar los siguientes comandos, esto se debe hacer en cada uno de los switches, la forma más rápida de hacerlo es establecer rangos en vez de hacerlo uno por uno.

```
D1(config)#inter range gigabitEthernet 1/0/1-4
D1(config-if)#switchport mode trunk
```

Tarea 2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales. Para cambiar la Vlan nativa en el enlace troncal se usa los siguientes comandos. Este mismo proceso se repite en cada una de las interfaces troncales. Hay que ingresar a el rango de interfaces que se van a intervenir y primero borrar la Vlan nativa, después de esto se ingresa el comando con el numero de la Vlan nativa que se va asignar.

D2(config)#inter range giga 1/0/1-4

D2(config-if)#no switchport trunk native vlan

D2(config-if)#switchport trunk native vlan 999

Después verificamos con el comando sh interfaces gi1/0/1 switchport

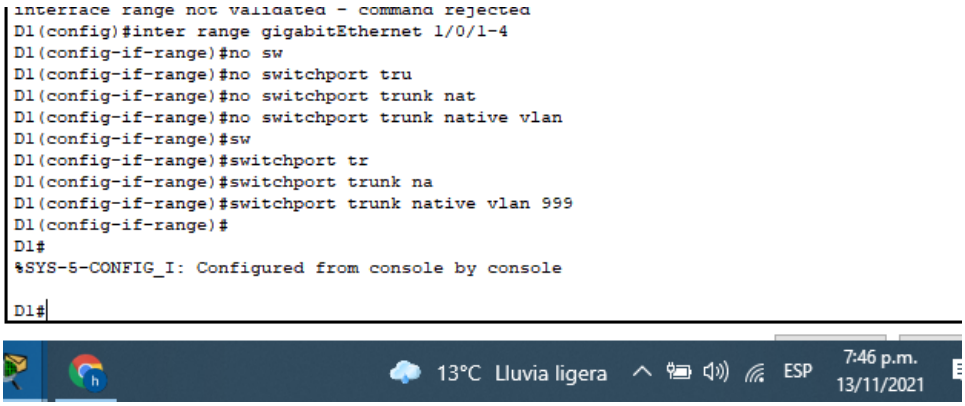

Figura 5. Cambio de Vlan nativa D1

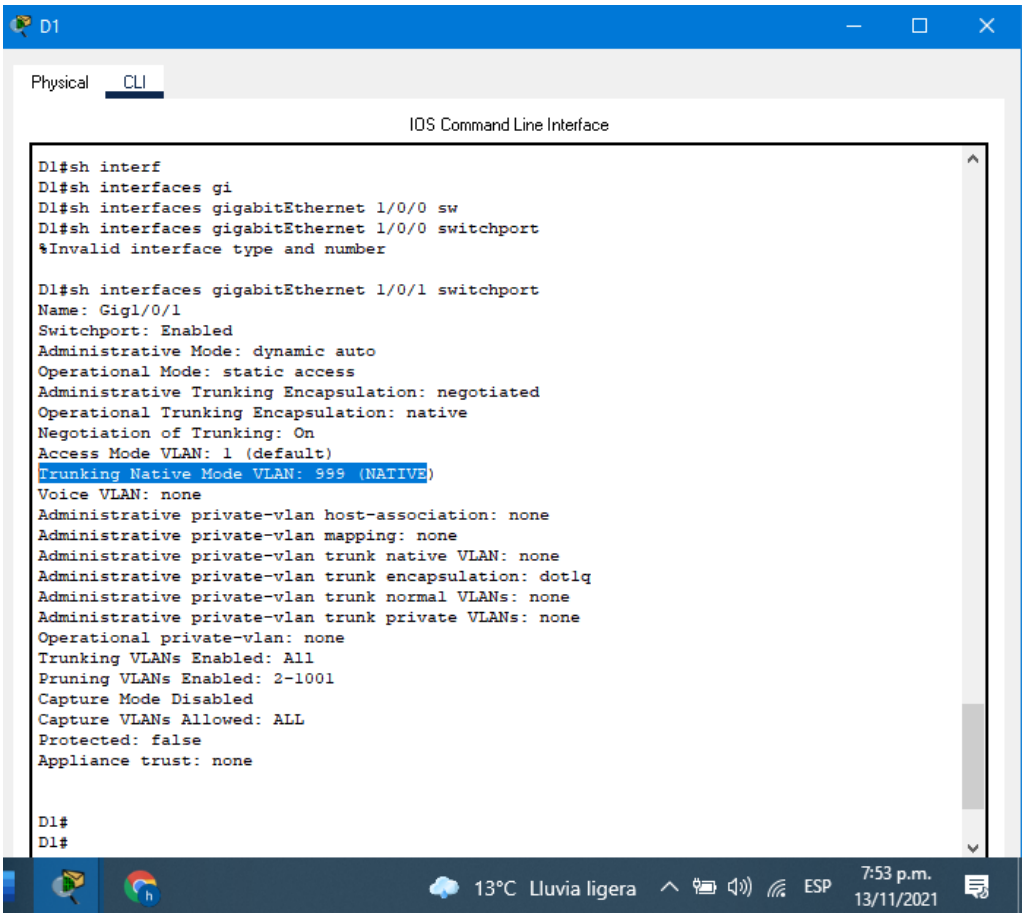

Figura 6. Verificación Native Vlan

Tarea 2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP).

El protocolo de RSPT se activa con el siguiente comando, esto se debe realizar en todos los switches. Esta configuración se debe hacer en el modo configuración así podemos activar el protocolo.

D1(config)#spanning-tree mode rapid-pvst

Tarea 2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

En D1 tenemos como prioridad la vlan 100 y la 102.

D1(config)#spanning-tree vlan 100,102 root primary

Para D2 tenemos como prioridad la vlan 101

D2(config)#spanning-tree vlan 101 root primary

Tenemos con principal el D1 y como respaldo el D2.

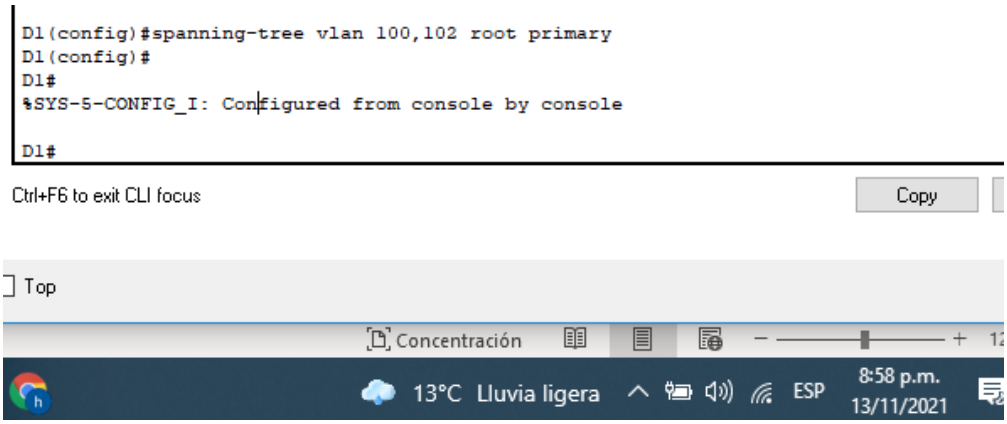

Figura 7. Configuración root bridge

Tarea 2.5 En todos los switches, cree EtherChannel LACP como se muestra en el diagrama de topología.

Para configurar el EtherChannel y los puestos se configura de la siguiente manera.

Primero se debe crear un grupo con las interfaces y después se debe agregar el puerto en cada una de las interfases. Se debe configurar un lado como active y el otro como active para que puedan negociar los dispositivos.

D1(config)#interface range gi0/0-3
D1(config-if-range)#channel-group 12 mode active
D2(config-if-range)#channel-group 12 mode active

Al hacer esto el crea lo puestos para las interfaces, para comprobar lo hacemos con el siguiente comando. Esto lo hacemos dependiendo el grupo en las interfases de los switches involucrados.

D2#sh etherchannel summary

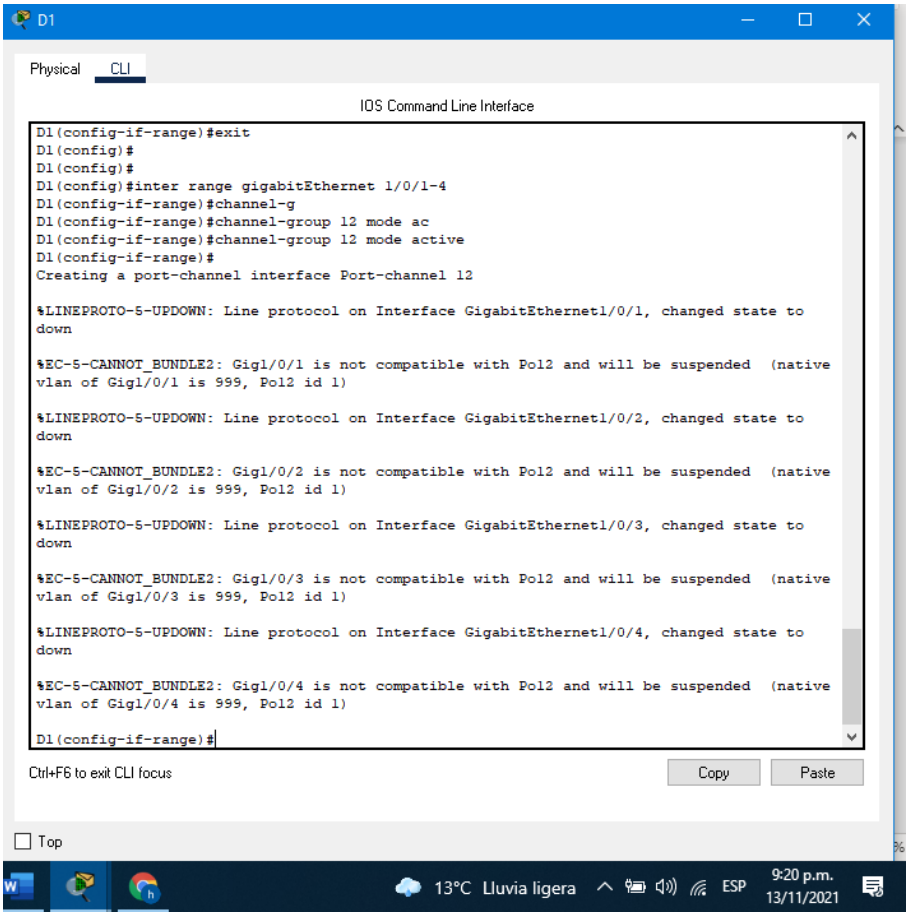

Figura 8. Configuración EtherChannel LACP

Tarea 2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

Para asignar puertos a las Vlans se utiliza los siguientes comandos. Para habilitar el modo forwarding es necesario utilizar el comando spanning-tree portfast, este mismo proceso se debe realizar en los otros switches, cabe recalcar que el acceso a la Vlan debe ser correspondiente al puerto PC que se quiere habilitar.

D1(config)#interface gi1/0/23

D1(config-if)# spanning-tree portfast
D1(config-if)#switchport access vlan 100
D1(config-if)#no shutdown

Y para comprobar se hace un show Vlan y show Spanning-tree.

Tarea 2.7 Verifique los servicios DHCP IPv4.
Se realiza prueba para verificar el servicio DHCP en los PC2 y PC3, esto lo podemos validar ingresando al PC en la parte de escritorio y seleccionando configuración IP después seleccionar DCHP.

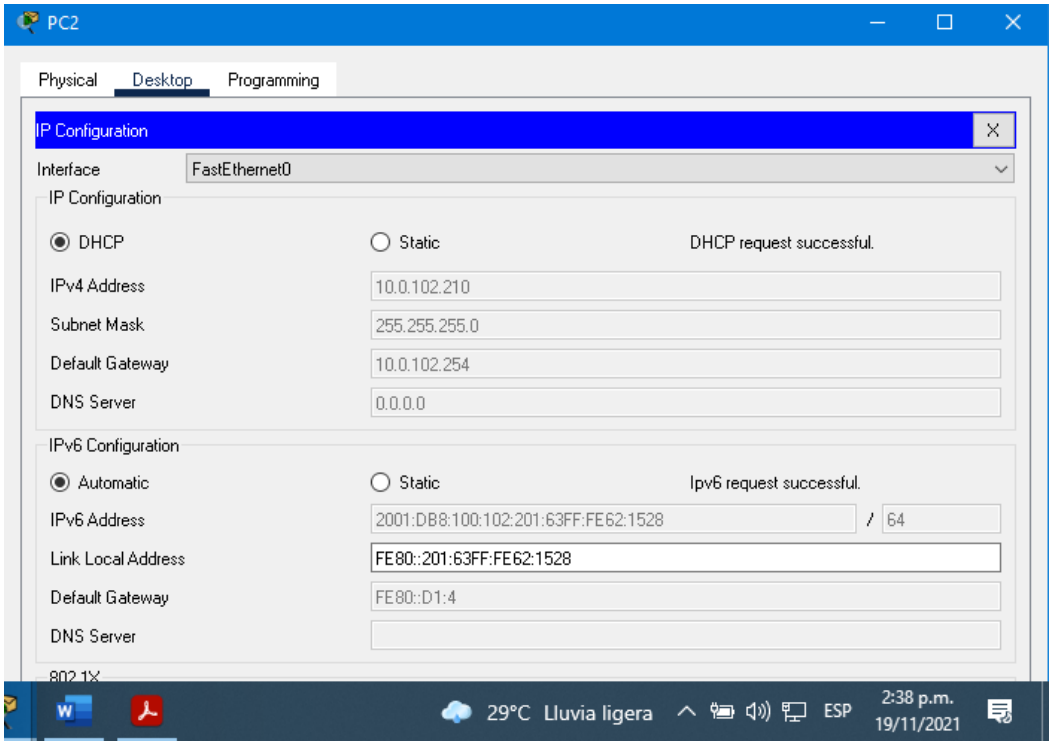

Figura 9. IP Dinámica PC2

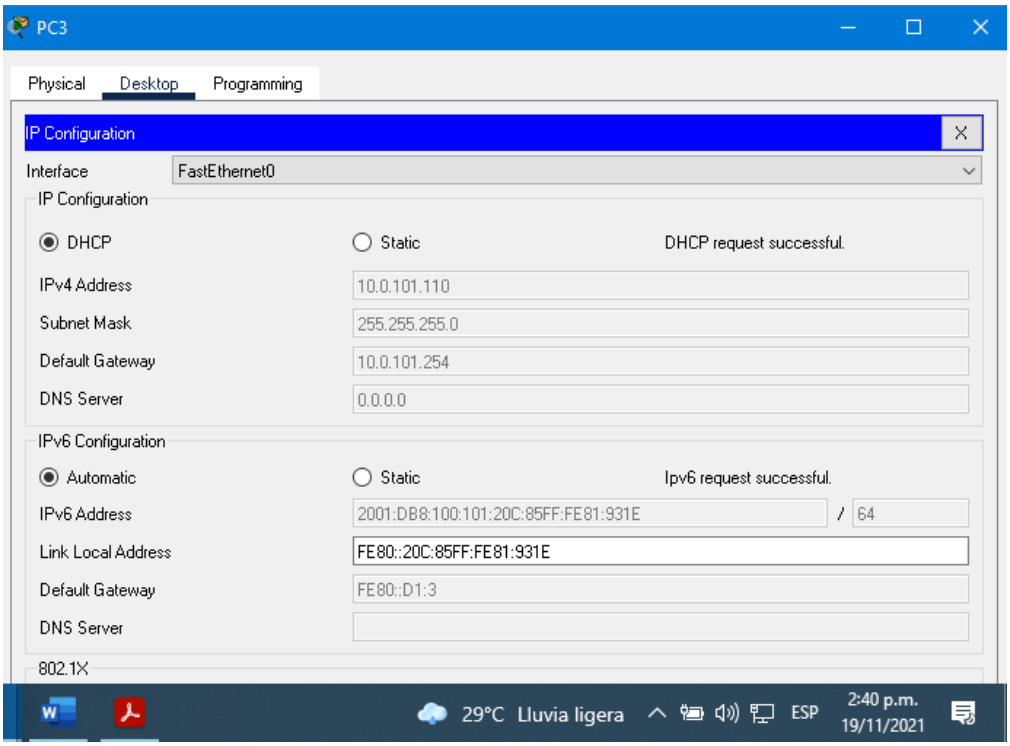

Figura 10. IP Dinámica PC3

Tarea 2.8 Verifique la conectividad de la LAN local.
Se realiza pruebas de conexión dentro de la red LAN, esto se hace para verificar conexión entre PCs y Switches.

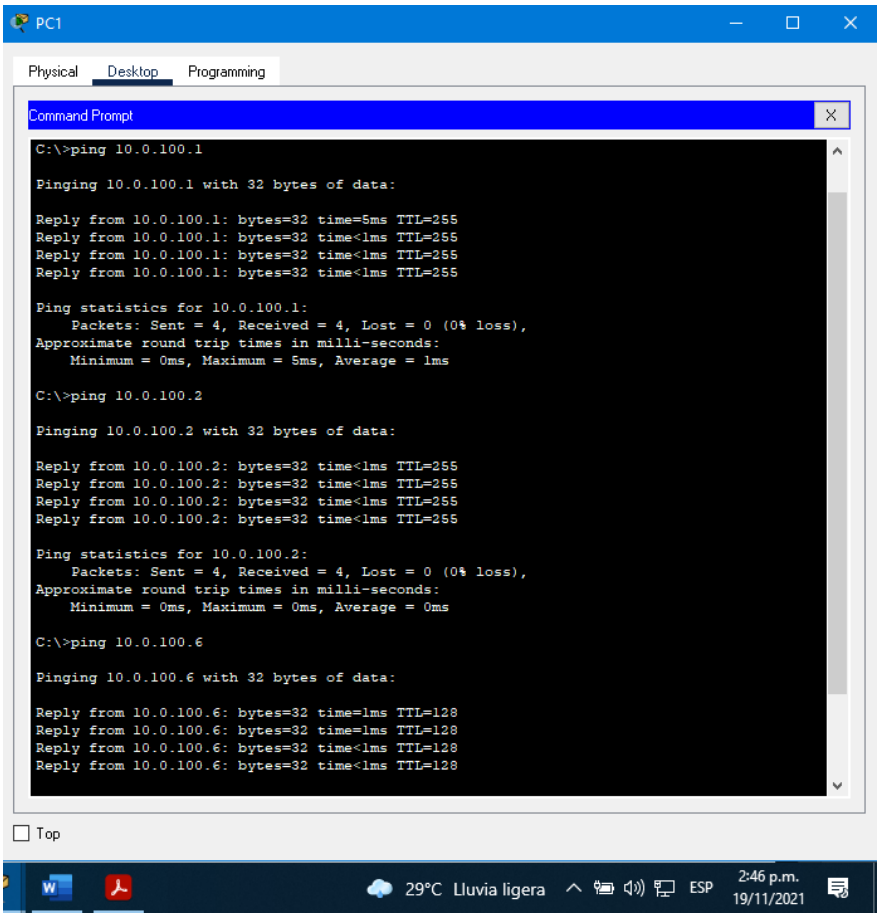

Figura 11. Pruebas de conexión desde PC1

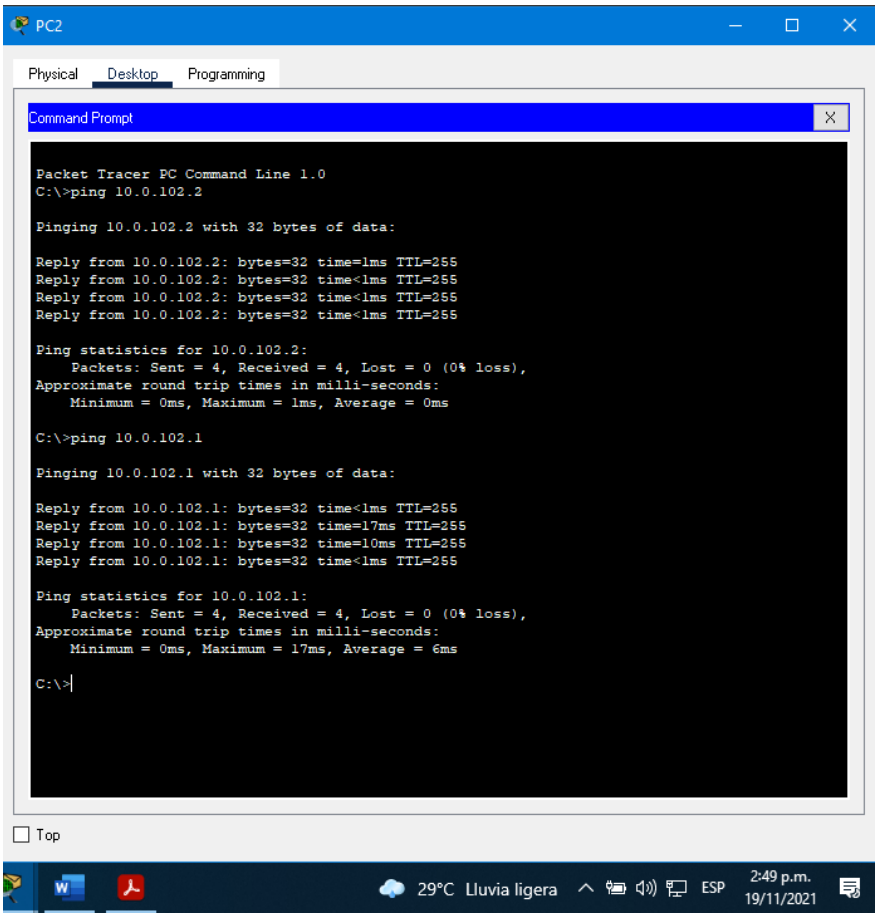

Figura 12. Pruebas de conexión desde PC2

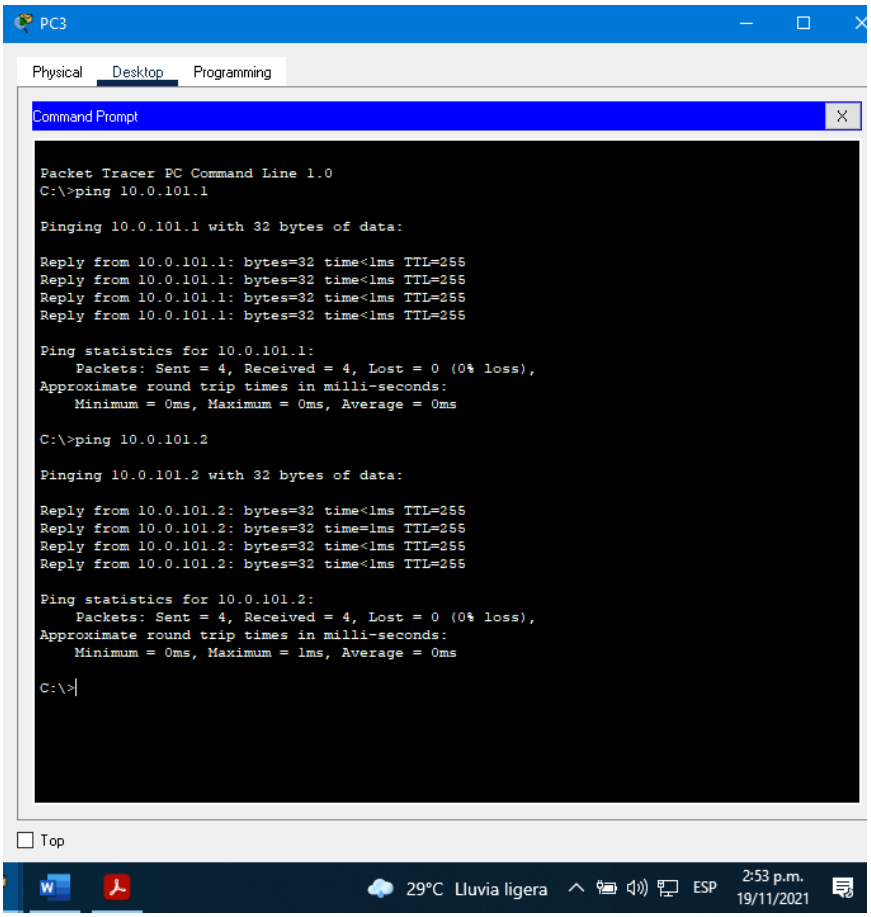

Figura 13 Pruebas de conexión desde PC3

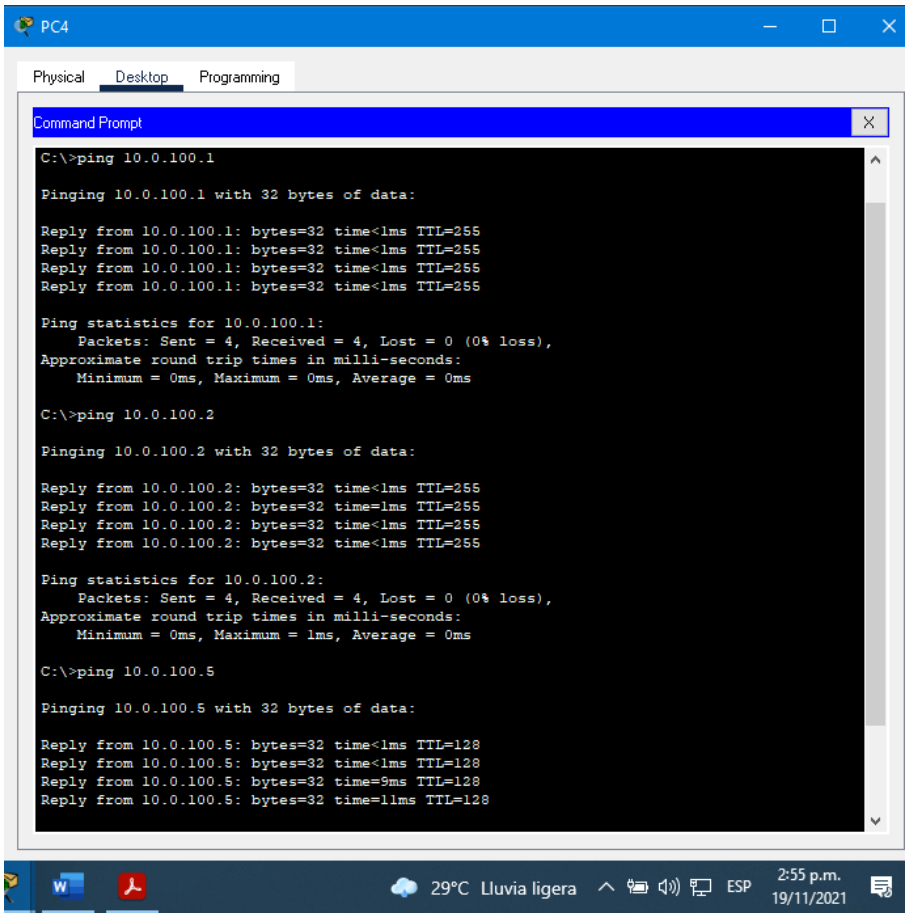

Figura 14. Pruebas de conexión desde PC4

Se puede evidenciar que al realizar las pruebas de conectividad tenemos una eficiencia del 100%. Teniendo así conexión en toda la red LAN.

Parte 3: Configurar los protocolos de enrutamiento.

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	Use OSPF Process ID **4** y asigne los siguientes router-Ids: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en 36rea 0.	Use OSPF Process ID **6** y asigne los siguientes router-Ids: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.

		Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11

Tabla 3. Lista de tareas parte 3

Tarea 3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en área 0.

Primero se crea el ID del enrutamiento OSPF, después se le asigna el ID al dispositivo que se esta configurando esto se realiza con los siguientes comandos los cuales se utilizaran para todos los equipos involucrados.

R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1

Después se realiza la configuración de las redes directamente conectadas y las Vlans esto tiene que ir al area 0.

R1(config-router)#network 10.0.11.0 255.255.255.0 area 0
R1(config-router)#network 10.0.13.0 255.255.255.0 area 0
R1(config-router)#network 10.0.10.0 255.255.255.0 area 0
R1(config-router)#network 10.0.100.0 255.255.255.0 area 0
R1(config-router)#network 10.0.101.0 255.255.255.0 area 0
R1(config-router)#network 10.0.102.0 255.255.255.0 area 0

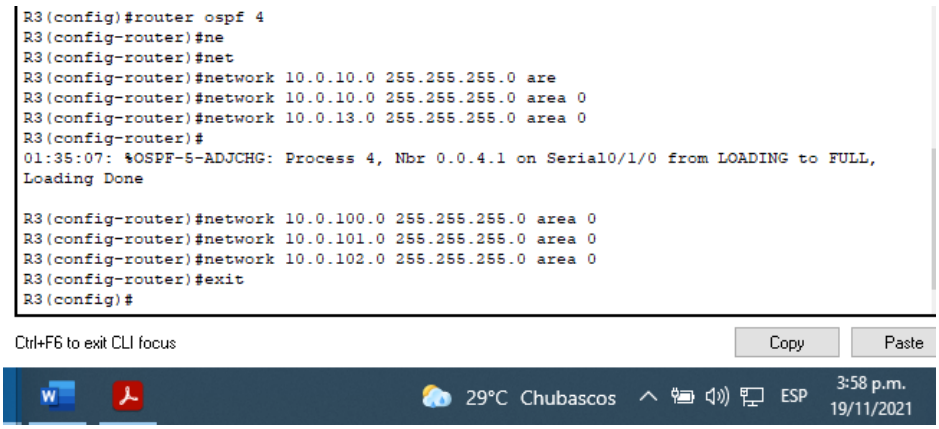

Figura 15. Publicación redes OSPF en R3

Se configura una ruta por defecto en el router R1, se realiza con el siguiente comando, se configura para que las interfaces de salida envíen paquetes a toda la red LAN para lograr la comunicación. Lo que le indicamos con este comando es que permita salida y entrada de cualquier tipo de IP.

R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.13.3

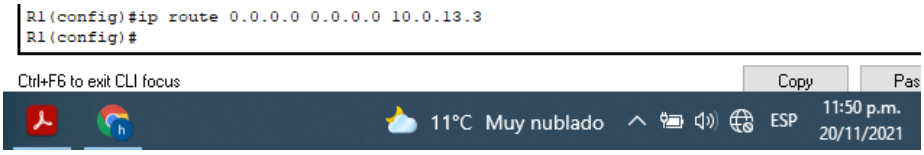

Figura 16. Ruta por defecto R1

Se deshabilitan las publicaciones OSPv2 en D1 y D2 menos la de las interfaces g1/0/11.

Figura 17. Deshabilitar OSPF en D1

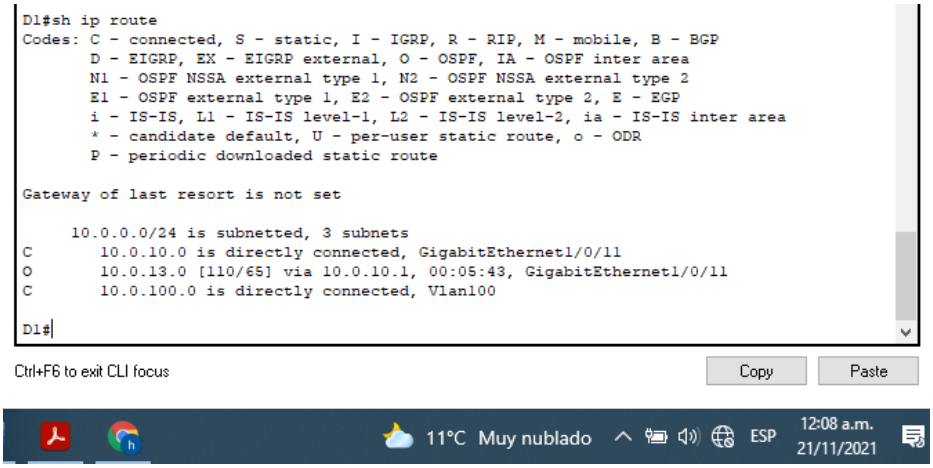

Figura 18. Verificar OSPF en G1/0/11

Tarea 3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.

Primero se crea el ID del enrutamiento OSPFv3, después se le asigna el ID al dispositivo que se está configurando esto se realiza con los siguientes comandos los cuales se utilizaran para todos los equipos involucrados.

```
R1(config)#ipv6 router ospf 6
R1(config-rtr)#router-id 0.0.4.1
```

Para el enrutamiento no es necesario agregar todas las redes, solo se agrega el siguiente comando en las interfaces de salida de cada dispositivo.

```
R1(config)#interfa serial 0/1/0
R1(config-if)#ipv6 ospf 6 area 0
R1(config-if)#interfa gi 0/0/1
R1(config-if)#ipv6 ospf 6 area 0
```

Tarea 3.3 En R2 en la “Red ISP”, configure MP-BGP.

Se configura una ruta estática en R2 por medio de la interfaz loopback0, tanto para el protocolo IPv4 y IPv6. Utilizando los siguientes comandos.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 Loopback0
R2(config)#ipv6 route ::/0 Loopback0
```

Se configura en R2 en BGP ASN 500 y use el router-id 2.2.2.2. Se utiliza los siguientes comandos.

```
R2(config)#router bgp 500
R2(config-router)#bgp router-id 2.2.2.2
```

Se configura en R1en ANS 300 la relación de vecino IPv4 e IPv6. Se utilizan los siguientes comandos.

```
R1(config)#router bgp 300
R1(config-router)#no bgp default ipv4-unicast ( comando utilizado para utilizar IPv6)
```

Por otro lado, se tienen que activar en R1 la relación de vecino, el simulador no soporta estos comandos, pero se incluyen en el documento.

R1(config-router)#address-family ipv4
R1(config-router)#address-family ipv6

Tarea 3.4 En R1 en la “Red ISP”, configure MP-BGP.

Se configura en R1 el ID 1.1.1.1, se deje ruta estática en la interfaz null0 por medio del protocolo IPv4, en IPv6 no esta funcionando por problemas del simulador, por lo cual se está trabajando con IPv4.

R1(config)#router bgp 300
R1(config-router)#network 10.0.0.0 mask 255.0.0.0
R1(config-router)#ip route 10.0.0.0 255.0.0.0 null0

En R2 se hace una relación vecino con R1 utilizando protocolo IPv4, esto se realiza con los siguientes comandos.

R2(config)#router bgp 500
R2(config-router)#neighbor 10.0.0.0 remote-as 300

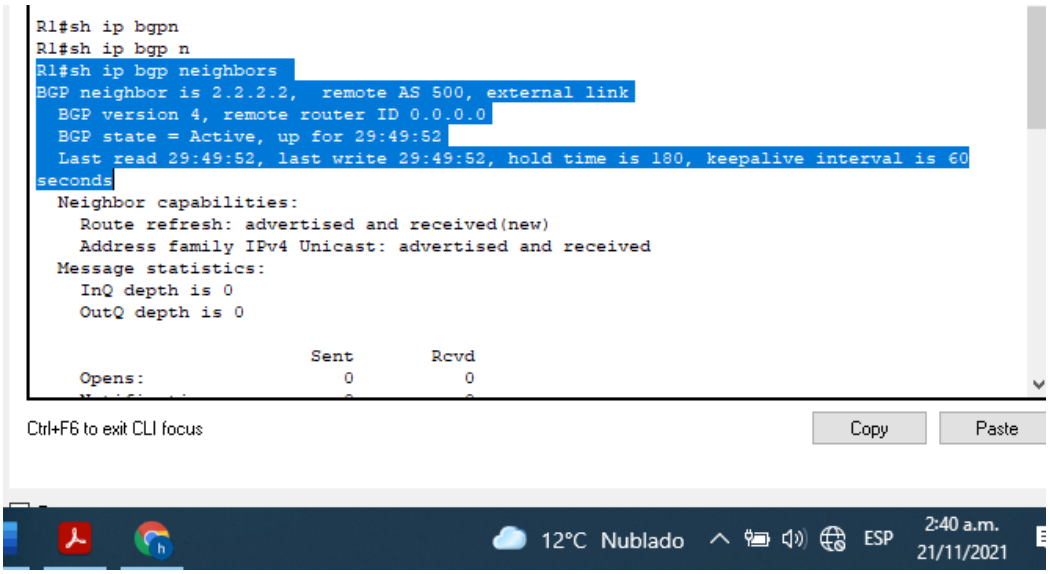

Figura 19. Verificación BGP

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”.

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

		Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • • Use el número de rastreo **4** para la IP SLA 4. • • Use el número de rastreo **6** para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.
4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60.

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

		Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo 106 para la VLAN 100: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

		Configure IPv6 HSRP grupo 126 para la VLAN 102: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

Tabla 4. Lista de tareas parte 4

Tarea 4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

Para la creación de IP SLAs se utiliza las siguientes líneas de comandos, también se realiza monitoreo en la interfaz G0/0/1 del R1, esto se indica en la segunda línea del comando, en la tercera línea indicamos que se haga un monitoreo en la interfaz de 5 segundos. En packet tracer no tiene compatibilidad con la configuración SLAs de igual forma se dejan los comandos en el documento.

```
D1(config)#ip sla 4
D1(config-ip-sla)#icmp-echo 10.0.10.1 source-interface Gi1/0/11
D1(config-ip-sla-echo)#timeout 5000
D1(config-ip-sla-echo)#exit
D1(config-ip-sla)#exit

D1(config)#ipv6 sla 6
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-ip 2001:db8:100:1010::2
D1(config-ip-sla-echo)#timeout 5000
D1(config-ip-sla-echo)#exit
D1(config-ip-sla)#exit
```

Con el siguiente comando se programa la SLA para una implementación inmediata sin tiempo de finalización.

```
D1(config-ip-sla)#ip sla schedule 1 life forever start-time now
```

Se configura un objeto de rastreo tanto para IPv4 como IPv6, se utilizan los siguientes comandos. Por otro lado también se configura la notificación a D1 para saber si el objeto que esta monitoreando IP SLA está arriba o abajo.

```
D1(config)#track 4 ip sla 4 state
D1(config-track)#delay up 10 down 15
```

D1(config)#track 6 ipv6 sla 6 state
D1(config-track)#delay up 10 down 15

Figura 20.Configuración IP SLAs D1

Tarea 4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

Para la creación de IP SLAs se utiliza las siguientes líneas de comandos, también se realiza monitoreo en la interfaz G0/0/1 del R3, esto se indica en la segunda línea del comando, en la tercera línea indicamos que se haga un monitoreo en la interfaz de 5 segundos. En packet tracer no tiene compatibilidad con la configuración SLAs de igual forma se dejan los comandos en el documento.

D2(config)#ip sla 4
D2(config-ip-sla)#icmp-echo 10.0.11.1 source-interface Gi1/0/11
D2(config-ip-sla-echo)#timeout 5000
D2(config-ip-sla-echo)#exit
D2(config-ip-sla)#exit

D2(config)#ipv6 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)#timeout 5000
D2(config-ip-sla-echo)#exit
D2(config-ip-sla)#exit

Con el siguiente comando se programa la SLA para una implementación inmediata sin tiempo de finalización.

D2(config-ip-sla)#ip sla schedule 1 life forever start-time now

Se configura un objeto de rastreo tanto para IPv4 como IPv6, se utilizan los siguientes comandos. Por otro lado también se configura la notificación a D2 para saber si el objeto que está monitoreando IP SLA está arriba o abajo.

```
D2(config)#track 4 ip sla 4 state
D2(config-track)#delay up 10 down 15

D2(config)#track 6 ipv6 sla 6 state
D2(config-track)#delay up 10 down 15
```

Tarea 4.3 En D1 configure HSRPv2.

Se configura HSRP V2 en el D1 para lo cual se utilizan los siguientes comandos, se configura la versión de HSRP V2 después se configura la IP virtual y grupo, después la prioridad y se habilita la preferencia, esto se hace con todas las interfaces que se solicitan.

```
D1(config)#interface vlan100
D1(config-if)#standby version 2
D1(config-if)#standby 104 ip 10.0.100.254
D1(config-if)#standby 104 priority 150
D1(config-if)#standby 104 preempt

D1(config)#interface vlan101
D1(config-if)#standby version 2
D1(config-if)#standby 114 ip 10.0.101.254
D1(config-if)#standby 114 preempt

D1(config)#interface vlan102
D1(config-if)#standby version 2
D1(config-if)#standby 124 ip 10.0.102.254
D1(config-if)#standby 124 priority 150
D1(config-if)#standby 124 preempt



D1(config)#interface vlan100
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)#interface vlan101
```

D1(config-if)#standby version 2
D1(config-if)#standby 116 ipv6 autoconfig
D1(config-if)#standby 116 preempt

D1(config)#interface vlan102
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

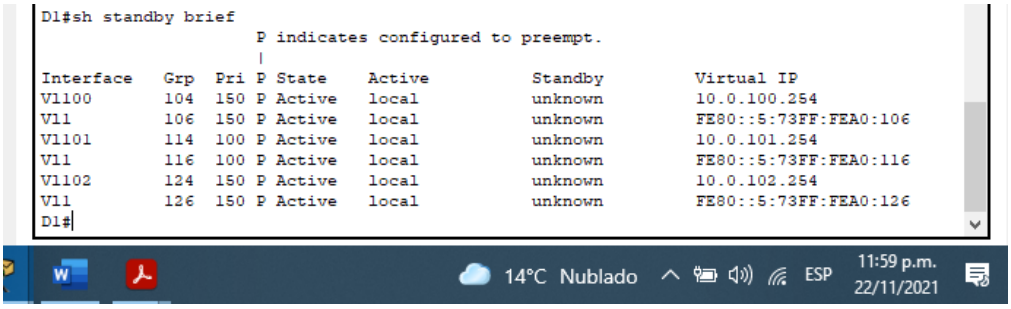

Figura 21. Verificación HSRP v2 D1

En D2, configure HSRPv2.

Se configura HSRP V2 en el D2 para lo cual se utilizan los siguientes comandos, se configura la versión de HSRP V2 después se configura la IP virtual y grupo, después la prioridad y se habilita la preferencia, esto se hace con todas las interfaces que se solicitan.

D2(config)#interface vlan100
D2(config-if)#standby version 2
D2(config-if)#standby 104 ip 10.0.100.254
D2(config-if)#standby 104 preempt

D2(config)#interface vlan101
D2(config-if)#standby version 2
D2(config-if)#standby 114 ip 10.0.101.254
D2(config-if)#standby 114 priority 150
D2(config-if)#standby 114 preempt

```
D2(config)#interface vlan102
D2(config-if)#standby version 2
D2(config-if)#standby 124 ip 10.0.102.254
D2(config-if)#standby 124 preempt

D2(config)#interface vlan100
D2(config-if)#standby version 2
D2(config-if)#standby 106 ipv6 autoconfig
D2(config-if)#standby 106 preempt

D2(config)#interface vlan101
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)#interface vlan102
D2(config-if)#standby version 2
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)#standby 126 preempt
```

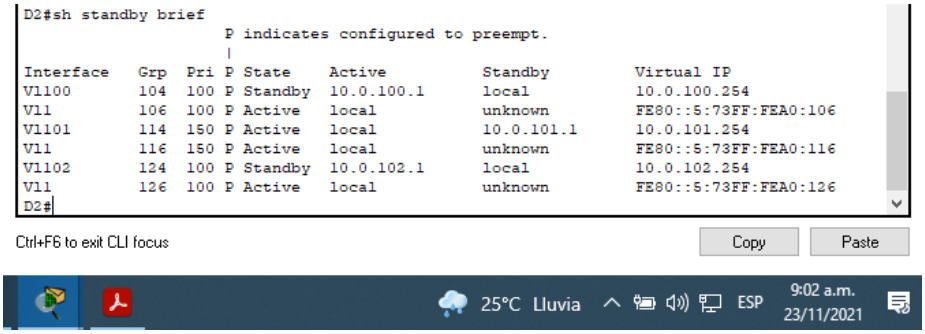

Figura 22. Verificación HSRP v2 D2

Parte 5: Seguridad.

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

Las tareas de configuración son las siguientes:

Tarea#	**Tarea**	**Especificación**
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio 15 • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.

5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **raduser** y la contraseña: **upass123**.

Tabla 5. Lista de tareas parte 5

Tarea 5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

Se utiliza el siguiente comando para proteger EXEC privilegiado usando el algoritmo de encripción SCRYPT, esto mismo se hace en todos los dispositivos.

D1(config)#enable secret cisco12345cisco
D2(config)#enable secret cisco12345cisco
R1(config)#enable secret cisco12345cisco
R2(config)#enable secret cisco12345cisco
R3(config)#enable secret cisco12345cisco

Tarea 5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.
Se crean usuarios y de le asigna privilegios nivel 15 que es el que tiene full access, se repite el mismo proceso en todos los equipos.

R1(config)#username sadmin privilege 15 password cisco12345cisco
R2(config)#username sadmin privilege 15 password cisco12345cisco

R3(config)#username sadmin privilege 15 password cisco12345cisco
D1(config)#username sadmin privilege 15 password cisco12345cisco
D2(config)#username sadmin privilege 15 password cisco12345cisco

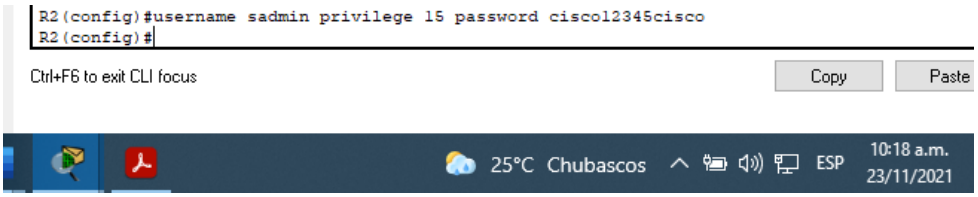

Figura 23. Creación user nivel 15

Tarea 5.3 En todos los dispositivos (excepto R2), habilite AAA.
Se habilita AAA (accounting and auditing) con los siguientes comandos, se habilita en todos los dispositivos menos R2.

```
D2(config)#aaa new-model
D2(config)#aaa authentication login default local
D2(config)#aaa authorization exec default local
```

Tarea 5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.
Se realiza configuración del servidor Radius en todos los dispositivos, por limitaciones del software en los switches no fue posible configurar, igual se adiciona el comando.

```
R1(config)#radius server RADIUS
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R1(config-radius-server)# key $trongPass
R1(config-radius-server)#aaa authentication login default group radius local

R3(config)#radius server RADIUS
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
R3(config-radius-server)# key $trongPass
R3(config-radius-server)#aaa authentication login default group radius local

D1(config)#radius server RADIUS
D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D1(config-radius-server)# key $trongPass
D1(config-radius-server)#aaa authentication login default group radius local

D2(config)#radius server RADIUS
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
D2(config-radius-server)# key $trongPass
D2(config-radius-server)#aaa authentication login default group radius local
```

Tarea 5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.

Esta autenticación AAA se debe configurar en todos los equipos menos R2.

R3(config-radius-server)#aaa authentication login default group radius local
R3(config)#aaa authentication login console local

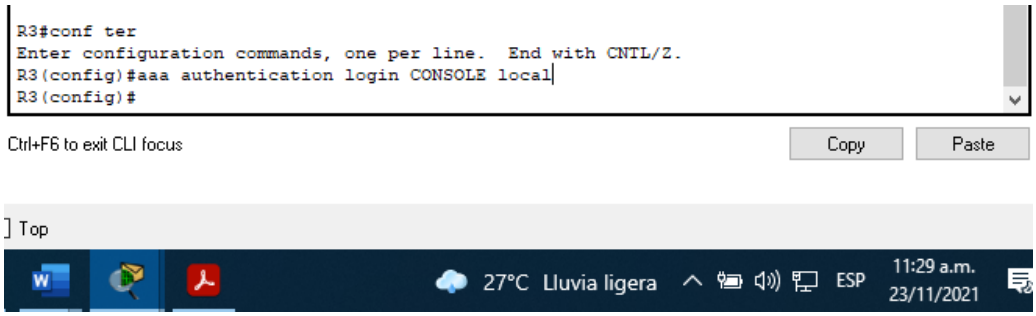

Figura 24. Lista de métodos de autenticación AAA.

Tarea 5.6 Verifique el servicio AAA en todos los dispositivos (excepto R2).

Debido a que el simulador no permitió ingresar todos los comandos del servicio AAA no podemos ingresar son las siguientes credenciales.

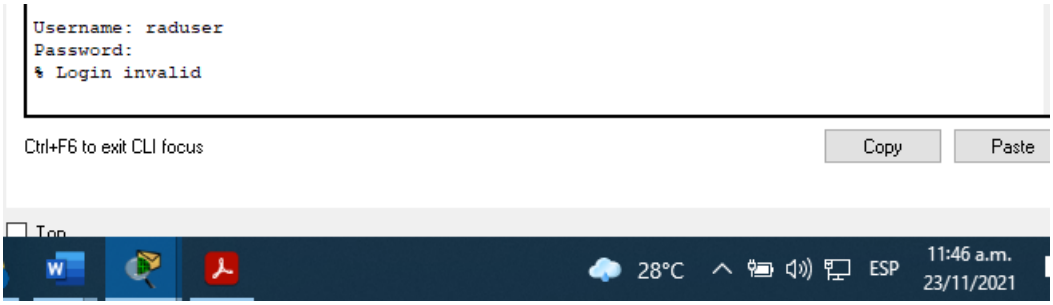

Figura 25. Verificación servicio AAA

Parte 6: Configure las funciones de Administración de Red.
En esta parte, debe configurar varias funciones de administración de red.

Las tareas de configuración son las siguientes:

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

Tabla 6. Lista de tareas parte 6

Tarea 6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.
Se configura la hora y fecha de los dispositivos con el siguiente comando.

R1#clock set 13:52:00 23 nov 2021
R1#sh clock

R2#clock set 13:52:00 23 nov 2021
R3#clock set 13:52:00 23 nov 2021
D1#clock set 13:52:00 23 nov 2021
D2#clock set 13:52:00 23 nov 2021

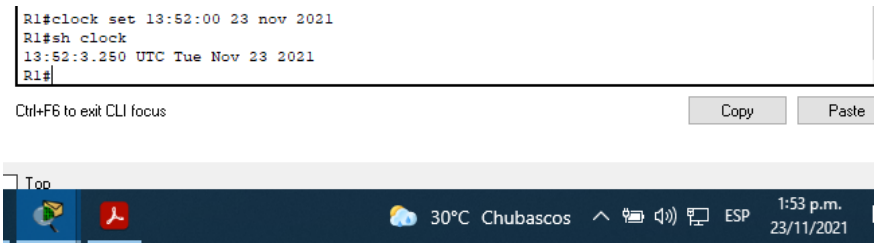

Figura 26. Configuración hora / fecha

Tarea 6.2 Configure R2 como un NTP maestro.
Se configura R2 como servidor NTP maestro con estrato 3.

R2(config)#ntp master 3

Tarea 6.3 Configure NTP en R1, R3, D1, D2, y A1.

R1 debe sincronizar con R2. La IP que se asigna en este comando es la que está configurada en la interfaz G0/0/0 de R2 que es el NTP máster.

R1(config)#ntp server 209.165.200.226

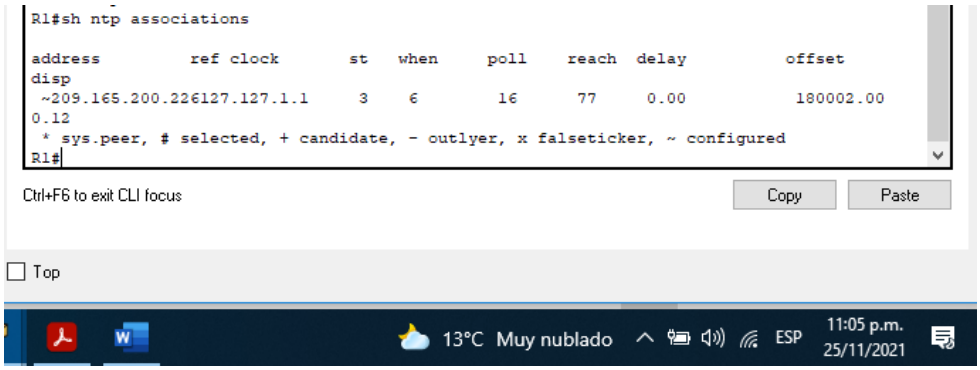

Figura 27. Verificación conexión server NTP

R3, D1 y A1 para sincronizar la hora con R1.

R3(config)#ntp server 10.0.13.1
D1(config)#ntp server 10.0.10.1
A1(config)#ntp sources fas 0/5-6
A1(config)#ntp server 10.0.10.1

Tarea 6.4 Configure Syslog en todos los dispositivos excepto R2.
Se configura el syslog en los distintos equipos, se tiene un inconveniente debido al alcance de packet tracer con el comando logging trap ya que no tiene la opción de warning, igual se deja especificado en los comandos del documento. Este mismo proceso se realiza en los demás dispositivos.

R1(config)#logging 10.0.100.5
R1(config)#logging trap warning

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

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

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

Tarea 6.5 Configure SNMPv2c en todos los dispositivos excepto R2. Únicamente se usará SNMP en modo lectura (Read-Only), se limita el acceso al PC1 y se configura valor de contacto, este mismo paso se realiza en todos los dispositivos menos R2, el simulador presenta inconvenientes con la toma de los comandos, de igual manera se dejan los comandos utilizados en el documento.

```
R1(config)#snmp-server community word ro
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)# snmp-server contact Alexis Martinez
```

Para habilitar traps config y ospf. en los dispositivos se utiliza el siguiente comando, este paso se hace en R3, D1, D2.

```
R3(config)# snmp-server enable traps ospf
R3(config)# snmp-server enable traps config
```

En R1 se habilitan traps bgp, config y ospf.

```
R1(config)# snmp-server enable traps ospf
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps bgp
```

En A1 se habilitan traps config.

```
A1(config)# snmp-server enable traps config
```

CONCLUSIONES

En la elaboración de este trabajo encontré dificultades con el software GNS3 ya que no se conectaba al servidor de la máquina virtual, algunas imágenes me generaban error, como ya se estaba volviendo reiterativo estas fallas se decidió realizar el trabajo con el software packet tracer el cual no genero problemas al momento de usarlo pero si tiene inconsistencias al momento de la compatibilidad de algunos comandos, pero eso no fue ningún impedimento para lograr el objetivo del mismo ya que se dejó estipulado en el documento los comandos utilizados en las partes que no se pudo configurar en el simulador.

Puedo concluir que el desarrollo de este documento logre implementar y poner en práctica conceptos y habilidades aprendidas durante el desarrollo del diplomado, logrando un grado de satisfacción al ver el resultado de este.

Durante el desarrollo del documento y del diplomado logre tomar aprecio y gusto al tema de CCNP el cual me gustaría continuar para así seguir reforzando y adquiriendo más conocimientos sobre este tema el cual ayuda por otro lado a seguir formándome como profesional.

Logre aprender mucho más sobre CCNP ya que es mucho más robusto a lo que tenía entendido en el inicio del diplomado, esto me permitió esforzarme y preparar de la mejor manera el escenario propuesto en este documento, por otro lado, el uso de la plataforma de netcad de cisco fue una herramienta muy útil durante todo el diplomado ya que permitía ver excelente contenido teórico y práctico.

BIBLIOGRAFÍA

Digital, L. I. (2019, 22 julio). Tipos de Topología de red: malla, estrella, árbol, bus y anillo. Locura Informática Digital. https://www.locurainformaticadigital.com/2018/07/17/topologia-de-red-malla-estrella-arbol-bus-anillo/.

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Advanced OSPF. 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). BGP. 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). IP Services. 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.

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

Interfaces de red. (2014, 23 octubre). Todo Sobre Redes. https://sobretodoredes.wordpress.com/redes-cableadas/elementos-de-una-red/interfaces-de-red/.

Prat, D. D. B. (2020, 10 julio). Enrutamiento | Fundamentos y Protocolos - El Taller del Bit. El Taller del BIT. https://eltallerdelbit.com/enrutamiento-fundamentos-y-protocolos/.

S. (2020, 17 junio). Diferencias entre CCNA y CCNP. Formatalent Business School. https://formatalent.com/diferencias-entre-ccna-y-ccnp/.

School, T. (2021, 30 agosto). Principales funciones de Cisco Packet Tracer. Tokio School. https://www.tokioschool.com/noticias/cisco-packet-tracer/.

School, T. (2021b, agosto 30). ¿Sabes qué es una red VLAN? ¡Te contamos los detalles! Tokio School. https://www.tokioschool.com/noticias/que-es-vlan/.

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC.