DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MARTIN LEONARDO BONILLA DUITAMA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN ELECTRÓNICA
BOGOTA D.C.
2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MARTIN LEONARDO BONILLA DUITAMA

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

DIRECTOR:
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN ELECTRÓNICA
BOGOTA D.C.
2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTA DC, noviembre del 2021

AGRADECIMIENTOS

A Dios en primer lugar por hacer posible la realización de estos estudios, por haberme dado la firmeza de principio a fin para alcanzar el título de Ingeniero en Electrónica, a mi familia, de manera especial mis padres, Leonardo Bonilla Pachón y Leonor Duitama Escobar, quienes a pesar de ser yo, una persona mayor, soñaron con migo este sueño y me apoyaron para que fuera real, a mi hermana Yineth Bonilla Duitama quien me animó siempre para que no abandonara este proyecto, y así fuera un orgullo más para nuestros padres, así mismo, a tutores y personal administrativo de la Universidad Nacional Abierta y a Distancia, quienes hicieron posible esta transferencia de conocimiento desde el desarrollo de los Pensum académicos, hasta el sostenimiento y soporte de la plataforma de estudios.

A mis compañeros de estudio, quienes con su participación aportaron en el logro de cada paso o etapa de este proceso académico.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BGP: BGP es un protocolo de puerta de enlace (EGP) exterior que se utiliza para intercambiar información de encaminamiento entre enrutadores de diferentes sistemas autónomos (Asoc). BGP información de enrutamiento incluye la ruta completa a cada destino. BGP utiliza la información de enrutamiento para mantener una base de datos con información sobre el alcance de la red, que intercambia con otros sistemas BGP.

CONVERGENCIA: Es el objetivo principal de todos los protocolos de enrutamiento. Cuando un conjunto de enrutadores converge significa que todos sus elementos se han puesto de acuerdo y reflejan la situación real del entorno de red donde se encuentran. La velocidad con la que los protocolos convergen después de un cambio es una buena medida de la eficacia del protocolo de enrutamiento

DHCP: El Servidor DHCP, de sus siglas en ingles Dynamic Host configuration Protocol, es un servidor de Red el cual permite una asignación automática de direcciones IP, getaways predeterminadas, así como otros parámetros de red que necesiten los clientes. El sistema DHCP envía automáticamente todos los parámetros para que los clientes se comuniquen sin problema dentro de la red.

OSPF: OSPF (Open Shortest Path First) es un protocolo de enrutamiento abierto del tipo Estado de Enlace (Link State). OSPF fue desarrollado por el IETF con el objetivo de reemplazar al protocolo RIP (Routing Information Protocol); En la actualidad OSPF es uno de los protocolos de enrutamiento más utilizado en la industria, el protocolo OSPF incluye un elemento diferente en su configuración: el concepto de Área, Un área representa un grupo de routers que intercambian tablas de enrutamiento.

PROTOCOLO DE ENRUTAMIENTO: Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento, dicha información se usa para construir y mantener las tablas de enrutamiento.

RADIUS: El protocolo del Remote Authentication Dial-In User Service (RADIUS) fue desarrollado por Livingston Enterprises, Inc., como una autenticación del Access Server y protocolo de contabilidad.

RESUMEN

Para el desarrollo del presente trabajo se plantea un escenario denominado habilidades prácticas CCNP ENCOR v8, donde se utilizan imágenes de dispositivos CISCO, el cual comprende actividades de configuración ajustes básicos de dispositivos y direccionamiento de interfaz, implementación de protocolos de enrutamiento, redundancia de enlaces, seguridad de la red y funciones de administración, por medio de las cuales se evalúan los conocimientos adquiridos durante el desarrollo del curso; es por ello, que se simula la topología de red mediante el uso de la herramienta software GNS3, realizando cada una de las tareas propuestas paso a paso, se describe y documentan los resultados obtenidos por medio de los comandos Show.

La topología comprende un dominio de enrutamiento con el protocolo OSPF en el área 0, un dominio de routing de border a través del protocolo BGP, los dispositivos intermedios de red utilizados son routers Cisco , Switches Cisco de capa 3 y Switch Cisco para la conmutación de capa 2, interconectados a través de conexiones seriales, ethernet, enlaces redundantes mediante la agregación de enlaces Ether channels, se implementa el protocolo spanning tree para evitar los bucles de capa dos en las redes, se crean las diferentes loopback, teniendo en cuenta el direccionamiento ipv4 e ipv6", entre otras configuraciones.

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

ABSTRACT

For the development of this work, a scenario called CCNP ENCOR v8 practical skills is proposed, which includes configuration activities, basic device settings and interface addressing, implementation of routing protocols, link redundancy, network security and administration functions. , by means of which the knowledge acquired during the development of the course is evaluated; For this reason, the network topology is simulated by using the GNS3 software tool, performing each of the proposed tasks step by step, the results obtained are described and documented through the Show commands.

The topology comprises an OSPF routing domain in area 0, a border routing domain through the BGP protocol, the intermediate network devices used are Cisco routers, Cisco Layer 3 Switches and Cisco Layer 2 Switches, interconnected through of serial connections, ethernet, redundant links through the aggregation of Ether channels links, the spanning tree protocol is implemented to avoid layer two loops, the different loopbacks are created, taking into account the IPv4 and IPv6 addressing ", among other configurations.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

En el presente trabajo se demuestra el desarrollo de las prácticas evaluativas del Diplomado de Profundización CCNP de la Universidad Nacional Abierta y a Distancia, donde se plantea un escenario de Networking, implementación de Protocolos de comunicación y enrutamiento de redes mediante el uso de herramienta GNS3. Para la práctica se documenta la red, se siguen los procedimientos solicitados, se describe y aplica los conocimientos adquiridos en la parte teórica del curso, la práctica se completa en dos momentos como se describe a continuación:

En el primer momento, se realizan las configuraciones iniciales y se implementa los protocolos de enrutamiento de redes como OSPF en routers, se crea interfaces Loopback, se crean Pool DHCP para realizar la asignación de direccionamiento ip automático a los hosts solicitados, se crean interfaces virtuales (VLAN) de acuerdo a lo solicitado se asigna el direccionamiento IP a cada interfaz y host.

En el segundo momento, se realiza la configuración de los enlaces redundantes mediante la creación de port-channel, de igual forma se configura la seguridad en los dispositivos, estableciendo contraseñas seguras mediante el algoritmo de cifrado Scrypt, se configura un servidor Radius para la autenticación de los usuarios creados, por otra parte, se configuran las funciones de administración de los dispositivos a través del protocolo SNMPv2, se sincroniza la hora de todos los dispositivos de la red, mediante la habilitación del servidor NTP, estas son algunas de las configuraciones a modo general, en el desarrollo del trabajo se evidencian las demás configuraciones específicas.

DESARROLLO

1) ESCENARIO 1

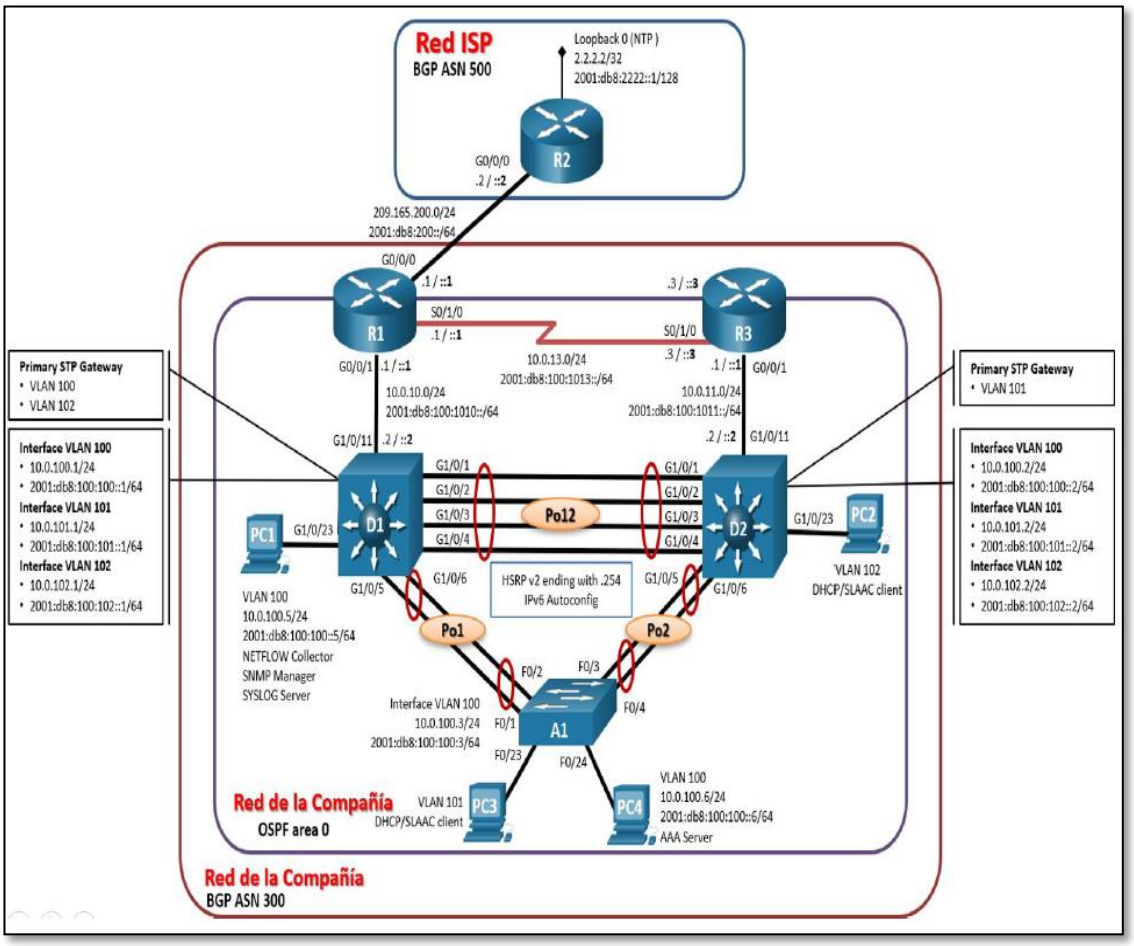


Figura 1. Escenario 1

Tabla 1. de Direccionamiento Ip

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	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
R3	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3

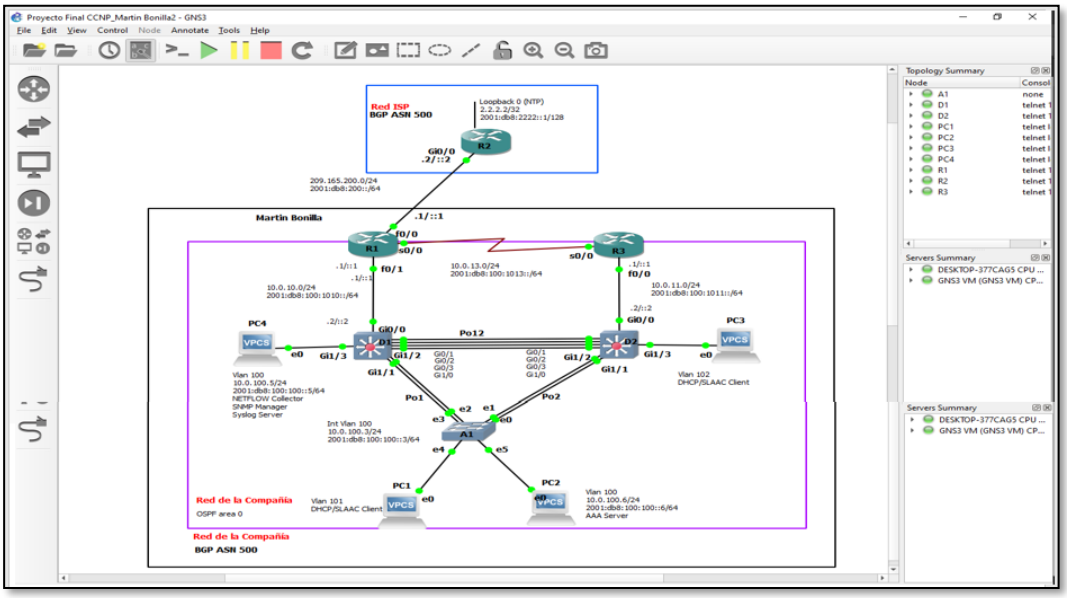
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
D1	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
D1	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
D1	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
D2	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

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. Escenario Simulado (GNS3)



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:

Configuración Inicial de un Dispositivo:

Router#configure terminal	▪ Ingreso al modo de configuración Global
Router(config)#hostname R1	▪ Modificar el nombre del Router A R1
ipv6 unicast-routing	▪ Habilita el direccionamiento Ipv6 en el router
R1(config)#no ip domain-lookup	▪ Desactivar la traducción de nombres o dominios
banner motd #	▪ Configurar un mensaje del día al arrancar el router
R1(config)#line console 0	▪ Ingreso a la línea de consola 0
R1(config-line)#logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
R1(config-line)#exec-timeout 0 0	▪ Desactivo el Timeout del Router
R1(config-line)#line vty 0 15	▪ Ingreso a las líneas VTY de la 0 a 15
R1(config-line) #logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de líneas VTY nos interrumpan la escritura de un comando
R1# wr o R1# copy running-config starup-config	▪ guardando configuración

Configuración Router R1

hostname R1	▪ Cambia nombre al router
ipv6 unicast-routing	▪ Habilita el direccionamiento Ipv6 en el router
no ip domain lookup	▪ Desactivar la traducción de nombres o dominios
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	▪ Mensaje del día, se muestra al iniciar e dispositivo
line con 0	▪ Ingreso a la línea de consola 0
exec-timeout 0 0	▪ Desactivo el Timeout del Router

logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
exit	▪ Regresa al modo configuración global
interface g0/0	▪ Se ingresa a la interfaz ethernet1/0 para su configuración
ip address 209.165.200.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::1:1 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:200::1/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresa al modo configuración global

con los comandos anteriores se ingresa a la interfaz Gigabit Ethernet 0/0, y se asigna el direccionamiento Ipv4 e Ipv6, se habilita o enciende, finalmente se sale de ella, de la misma forma se hace con cada interfaz en cada router a continuación:

interface g1/0	▪ Se ingresa a la interfaz g1/0 para su configuración
ip address 10.0.10.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::1:2 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:1010::1/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresa al modo configuración global
interface s2/0	▪ Se ingresa a la interfaz s2/0 para su configuración
ip address 10.0.13.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz

ipv6 address fe80::1:3 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:1013::1/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresa al modo configuración global

Configuración inicial Router R2

hostname R2	▪ Cambia nombre al router
ipv6 unicast-routing	▪ Habilita el direccionamiento Ipv6 en el router
no ip domain lookup	▪ Desactivar la traducción de nombres o dominios
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	▪ Mensaje del día, se muestra al iniciar e dispositivo
line con 0	▪ Ingreso a la línea de consola 0
exec-timeout 0 0	▪ Desactivo el Timeout del Router
logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
exit	▪ Regresa al modo configuración global
interface g0/0	▪ Se ingresa a la interfaz g0/0 para su configuración
ip address 209.165.200.2 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::2:1 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:200::2/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresa al modo configuración global
interface Loopback 0	▪ Se ingresa a la interfaz Lop0 para su configuración

ip address 2.2.2.2 255.255.255.255	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::2:3 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:2222::1/128	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz

Configuració Inicial Router R3

hostname R3	▪ Cambia nombre al router
ipv6 unicast-routing	▪ Habilita el direccionamiento Ipv6 en el router
no ip domain lookup	▪ Desactivar la traducción de nombres o dominios
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	▪ Mensaje del día, se muestra al iniciar el dispositivo
line con 0	▪ Ingreso a la línea de consola 0
exec-timeout 0 0	▪ Desactivo el Timeout del Router
logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
exit	▪ Regresa al modo configuración global
interface g1/0	▪ Se ingresa a la interfaz g1/0 para su configuración
ip address 10.0.11.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::3:2 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:1011::1/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresa al modo configuración global
interface s2/0	▪ Se ingresa a la interfaz s2/0 para su configuración
ip address 10.0.13.3 255.255.255.0	▪ Se asigna una ipv4 a la interfaz

ipv6 address fe80::3:3 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:1010::3/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresa al modo configuración global

Configuración Inicial Switch D1

conf t	▪ Ingresa a modo configuración global
hostname D1	▪ Cambia nombre al router
ipv6 unicast-routing	▪ Habilita el direccionamiento Ipv6 en el router
no ip domain lookup	▪ Desactivar la traducción de nombres o dominios
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	▪ Mensaje del día, se muestra al iniciar e dispositivo
line con 0	▪ Ingreso a la línea de consola 0
exec-timeout 0 0	▪ Desactivo el Timeout del Router
logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
	▪
vlan 100	▪ Con este comando se crea una interfaz Virtual con numero 100
name Management	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz
vlan 101	▪ Con este comando se crea una interfaz Virtual con numero 100
name UserGroupA	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz

vlan 102	▪ Con este comando se crea una interfaz Virtual con numero 100
name UserGroupB	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz
interface e1/0	▪ Se ingresa a la interfaz ethernet1/0 para su configuración
no switchport	▪ Permite el paso de tramas etiquetadas y sin etiquetar
ip address 10.0.10.2 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d1:1 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:1010::2/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Salir del submodo de configuración de interfaz
interface vlan 100	▪ Se ingresa a la interfaz vlan 100
ip address 10.0.100.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d1:2 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:100::1/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Salir del submodo de configuración de interfaz
interface vlan 101	▪ Se ingresa a la interfaz vlan 101
ip address 10.0.101.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d1:3 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:101::1/64	▪ Se asigna una ipv6 global a interfaz

no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Salir del submodo de configuración de interfaz
interface vlan 102	▪ Se ingresa a la interfaz vlan 102
ip address 10.0.102.1 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d1:4 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:102::1/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Salir del submodo de configuración de interfaz
	▪
ip dhcp excluded-address 10.0.101.1 10.0.101.109	▪ Excluye el rango de ip desde la 1 hasta la 109
ip dhcp excluded-address 10.0.101.141 10.0.101.254	▪ Excluye el rango de ip desde la 141 hasta la 254
ip dhcp excluded-address 10.0.102.1 10.0.102.109	▪ Excluye el rango de ip desde la 1 hasta la 109
ip dhcp excluded-address 10.0.102.141 10.0.102.254	▪ Excluye el rango de ip desde la 141 hasta la 254
ip dhcp pool VLAN-101	▪ Pool de las direcciones IP para asignar
network 10.0.101.0 255.255.255.0	▪ Red utilizada para el DHCP en vlan 101
default-router 10.0.101.254	▪ Puerta de enlace para los host con DHCP
exit	▪ Salir del Pool
ip dhcp pool VLAN-102	▪ Pool de las direcciones IP para asignar
network 10.0.102.0 255.255.255.0	▪ Red utilizada para el DHCP en vlan 102
default-router 10.0.102.254	▪ Puerta de enlace para los host con DHCP
exit	▪ Salir del Pool

Con los comandos anteriores, se crea y configuran un servidor DHCP, para los equipos que tienen acceso a la red de la Vlan 101 y 102, los cuales mediante el proceso DORA, recibirán una dirección ip de forma automática, con el comando "*ip dhcp excluded-address*" se excluyen direcciones ip individuales o por rango, en este caso en la Red de la vlan 101 se excluyeron las direcciones comprendidas entre la 10.0.101.1 y la 10.0.101.109 también las ip entre 10.0.101.1 y 10.0.101.109, de igual forma se hiso en la red de la vlan 102, por ende ninguna de estas ip se entrega por DHCP, deberán se configuradas en los host de forma manual.

int rang e2/0-3, e3/0-3	▪ Se crea un rango de interfaces
shutdown	▪ Se apagan todas las interfaces del rango
exit	▪ Salir del rango y regresar a modo configuración global.
	▪

Configuración Inicial Switch D2

conf t	▪ Ingresa a modo configuración global
hostname D2	▪ Cambia nombre al Switch
ipv6 unicast-routing	▪ Habilita el direccionamiento Ipv6 en el router
no ip domain lookup	▪ Desactivar la traducción de nombres o dominios
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	▪ Mensaje del día, se muestra al iniciar e dispositivo
line con 0	▪ Ingreso a la línea de consola 0
exec-timeout 0 0	▪ Desactivo el Timeout del Router
logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
exit	▪ Salir del submodo de configuración.
vlan 100	▪ Con este comando se crea una interfaz Virtual con numero 100
name Management	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz

vlan 101	▪ Con este comando se crea una interfaz Virtual con numero 101
name UserGroupA	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz
vlan 102	▪ Con este comando se crea una interfaz Virtual con numero 102
name UserGroupB	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz
vlan 999	▪ Con este comando se crea una interfaz Virtual con numero 100
name NATIVE	▪ Se asigna un nombre a la Vlan creada
exit	▪ Sirve para salir del submodo de configuración de interfaz
	▪
interface e1/0	▪ Ingresa al modo de configuración de interfaz
no switchport	▪ Permite el paso de tramas etiquetadas y sin etiquetar
ip address 10.0.11.2 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d1:1 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:1011::2/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Salir del submodo de configuración de interfaz
interface vlan 100	▪ Ingresa al modo de configuración de interfaz vlan
ip address 10.0.100.2 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d2:2 link-local	▪ Se asigna una ipv6 local a la interfaz

ipv6 address 2001:db8:100:100::2/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresar al modo de configuración global.
interface vlan 101	▪ Ingresa al modo de configuración de interfaz vlan
ip address 10.0.101.2 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d2:3 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:101::2/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresar al modo de configuración global.
interface vlan 102	▪ Ingresa al modo de configuración de interfaz vlan
ip address 10.0.102.2 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::d2:4 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:102::2/64	▪ Se asigna una ipv6 global a interfaz
no shutdown	▪ Se habilita o enciende la interfaz
exit	▪ Regresar al modo de configuración global.
ip dhcp excluded-address 10.0.101.1 10.0.101.109	▪ Excluye el rango de ip desde la 1 hasta la 109
ip dhcp excluded-address 10.0.101.241 10.0.101.254	▪ Excluye el rango de ip desde la 141 hasta la 254
ip dhcp excluded-address 10.0.102.1 10.0.102.209	▪ Excluye el rango de ip desde la 1 hasta la 109
ip dhcp excluded-address 10.0.102.241 10.0.102.254	▪ Excluye el rango de ip desde la 141 hasta la 254
ip dhcp pool VLAN-101	▪ Pool de las direcciones IP para asignar

network 10.0.101.0 255.255.255.0	▪ Red utilizada para el DHCP en vlan 101
default-router 10.0.101.254	▪ Puerta de enlace para los host con DHCP en la vlan1
exit	▪ Salir del Pool
ip dhcp pool VLAN-102	▪ Pool de las direcciones IP para asignar
network 10.0.102.0 255.255.255.0	▪ Red utilizada para el DHCP en vlan 102
default-router 10.0.102.254	▪ Puerta de enlace para los host con DHCP en la vlan1
exit	▪ Salir del Pool
int rang e2/0-3, e3/0-3	▪ Se ingresa a rango de interfaces
shutdown	▪ Se apagan las interfaces del rango
exit	▪ Salir del rango

Configuración Inicial Switch A1

	▪ Cambia nombre al Switch
hostname A1	
no ip domain lookup	▪ Desactivar la traducción de nombres o dominios
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	▪ Mensaje del día, se muestra al iniciar el dispositivo
line con 0	▪ Ingreso a la línea de consola 0
exec-timeout 0 0	▪ Desactivo el Timeout del Router
logging synchronous	▪ Activa la sincronización de registro así evitar que los mensajes de consola interrumpan la escritura de un comando
exit	▪ Regresa al modo configuración global
vlan 100	▪ Se crea la vlan 100
name Management	▪ Se asigna un nombre a la vlan
exit	▪ Salir modo configuración vlan

vlan 101	▪ Se crea la vlan 101
name UserGroupA	▪ Se asigna un nombre a la vlan
exit	▪ Salir modo configuración vlan
vlan 102	▪ Se crea la vlan 102
name UserGroupB	▪ Se asigna un nombre a la vlan
exit	▪ Salir modo configuración vlan
vlan 999	▪ Se crea la vlan 999
name NATIVE	▪ Se asigna un nombre a la vlan
exit	▪ Salir modo configuración vlan
	▪
interface vlan 100	▪ Se ingresa a la interfaz vlan 100
ip address 10.0.100.3 255.255.255.0	▪ Se asigna una ipv4 a la interfaz
ipv6 address fe80::a1:1 link-local	▪ Se asigna una ipv6 local a la interfaz
ipv6 address 2001:db8:100:100::3/64	▪ Se asigna una ipv6 global a la interfaz
no shutdown	▪ Se enciende la interfaz
exit	▪ Salir del modo de configuración de interfaz
interface range e1/2-3, e2/0-3, e3/0-3	▪ Se ingresa a un rango de interfaces del switch
shutdown	▪ Se apagan las interfaces del rango
exit	▪ Salir del submodo de configuración de rango de interfaces

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

D2#copy running-config startup-config	▪ Copia la configuración en ejecución a la configuración de inicio.
Destination filename [startup-config]?	▪ Confirma la copia
Building configuration...	▪ Se guarda la configuración

Con los anteriores comandos, se guarda la configuración en ejecución o que está corriendo, en la configuración de inicio, por tanto, al reiniciar el dispositivo, la cargará

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

En esta parte de la Evaluación de habilidades, completará la configuración de red de Capa 2 y establecerá el soporte básico del host. Al final de esta parte, todos los conmutadores deberían poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Sus tareas de configuración son las siguientes:

Tabla 2. Tareas de configuración Parte 2

Tarea #	Tarea	Especificación
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: 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

En la capa 2 del modelo de referencia OSI, se ubican los Switches de acceso, los cuales permiten conectar los hosts a la red, mediante sus múltiples puertos.

Comandos Configuración Switch D1

interface range e0/0-3
- Ingreso a rango de interfaces

switchport trunk encapsulation dot1q
- Se habilita enlace troncal

switchport trunk native vlan 999
- Configura como nativa la vlan999

channel-group 12 mode active	▪ Crea grupo de canales
no shutdown	▪ Enciende el grupo de canales
exit	▪ Salida

En las anteriores líneas de comandos, en orden respectivo, se realizan las siguientes acciones: se crea un rango de interfaces, es decir que al crearse el rango estas interfaces reciben la misma configuración con ingresar una sola vez el comando, se habilita los enlaces troncales para el router mediante la encapsulación y etiquetado de los paquetes bajo el protocolo dot1q, se establece como interfaz virtual nativa la Vlan 999, para que pase a través de ella todas las tramas no etiquetadas, se crea un grupo de caneles bajo número 12, es decir se agregaron varios enlaces para que el Switch los vea como un solo enlace lógico, y se mejora el ancho de banda, por último se habilita el enlaces para que esté en modo on, y se sale del modo de configuración de interfaz, estos comandos se repiten en los otros dos Switches.

interface range e1/3, e1/2	▪ Ingreso a rango de interfaces
switchport trunk encapsulation dot1q	▪ Se habilita enlace troncal
switchport trunk native vlan 999	▪ Configura como nativa la vlan999
channel-group 1 mode active	▪ Crea grupo de canales
no shutdown	▪ Enciende el grupo de canales
exit	▪ Salida
spanning-tree mode rapid-pvst	▪ Habilita el protocolo de árbol de expansión en el modo rápido
spanning-tree vlan 100,102 root primary	▪ Se establecen las vlan 100 y 102 con prioridad primaria
spanning-tree vlan 101 root secondary	▪ Se establece la vlan 101 con prioridad segundaria

En las líneas de comando anteriores, se habilita el Switch para que implemente el modo rápido del protocolo de árbol de expansión RSTP, así mismo, se establece la raíz primaria y secundaria del protocolo Spanning-tree, lo que se traduce en que las Vlans 100 y 102 tendrán una prioridad más baja, lo que convierte al Switch donde están estas Vlan en candidato para Root Bridge o pueste raíz, lo que significa que este no apagará administrativamente ninguna de sus interfaces, este procedimiento se repite en los otros Switches.

interface e1/1	▪ Ingreso a interfaz e1/1
switchport mode access	▪ Declara puerto como acceso
switchport access vlan 100	▪ Declara acceso a vlan 101
spanning-tree portfast	▪ Activa el modo de spanning tree puerto rápido
no shutdown	▪ Enciende interfaz
exit	▪ Salida de modo configuración de interfaz
end	▪ Finaliza y regresa al modo de usuario privilegiado.

Comandos Configuración Switch D2

interface range e0/0-3	▪ Ingreso a rango de 4 interfaces
switchport trunk encapsulation dot1q	▪ Se habilita enlace troncal
switchport trunk native vlan 999	▪ Configura como nativa la vlan999
channel-group 12 mode active	▪ Crea un grupo de canales
no shutdown	▪ Enciende el grupo de canales
exit	▪ Salida
interface range e1/2-3	▪ Ingreso a rango de 2 interfaces
switchport trunk encapsulation dot1q	▪ Se habilita enlace troncal
switchport trunk native vlan 999	▪ Configura como nativa la vlan999
channel-group 2 mode active	▪ Crea un grupo de canales
no shutdown	▪ Enciende el grupo de canales
exit	▪ Salida
spanning-tree mode rapid-pvst	▪ Habilita el protocolo de árbol de expansión en el modo rápido
spanning-tree vlan 101 root primary	▪ Se establece la vlan 101 con prioridad primaria
spanning-tree vlan 100,102 root secondary	▪ Se establecen las vlan 100 y 102 con prioridad segundaria
interface e1/1	▪ Ingreso a interfaz e1/1
switchport mode access	▪ Declara puerto como acceso
switchport access vlan 102	▪ Declara acceso a vlan 102
spanning-tree portfast	▪ Activa el modo de spanning tree puerto rápido
no shutdown	▪ Enciende interfaz

exit	▪ Salida de modo configuración de interfaz
end	▪ Finaliza y regresa al modo de usuario privilegiado.

Comandos Configuración Switch A1

conf t	▪ Ingreso a modo configuración global
spanning-tree mode rapid-pvst	▪ Habilita el protocolo de árbol de expansión en el modo rápido
interface range e0/2-3	▪ Ingreso a interfaz e1/1
switchport trunk encapsulation dot1q	▪ Declara puerto como acceso
switchport trunk native vlan 999	▪ Declara acceso a vlan 101
channel-group 1 mode active	▪ Activa el modo de spanning tree puerto rápido
no shutdown	▪ Enciende interfaz
exit	▪ Salida de modo configuración de interfaz
interface range e0/0-1	▪ Ingreso a rango de 2 interfaces
switchport trunk encapsulation dot1q	▪ Se habilita enlace troncal
switchport trunk native vlan 999	▪ Configura como nativa la vlan999
channel-group 2 mode active	▪ Crea un grupo de canales
no shutdown	▪ Enciende el grupo de canales
exit	▪ Salida
interface e1/0	▪ Ingreso a interfaz e1/0
switchport mode Access	▪ Declara puerto como acceso
switchport access vlan 101	▪ Declara acceso a vlan 101
spanning-tree portfast	▪ Activa el modo de spanning tree puerto rápido
no shutdown	▪ Enciende interfaz
exit	▪ Salida de modo configuración de interfaz
interface e1/1	▪ Ingreso a interfaz e1/1
switchport mode access	▪ Declara puerto como acceso
switchport access vlan 100	▪ Declara acceso a vlan 100
spanning-tree portfast	▪ Activa el modo de spanning tree puerto rápido

no shutdown	▪ Enciende interfaz
exit	▪ Salida de modo configuración de interfaz

Mediante los comandos anteriores, se habilitaron las interfaces para admitir tramas que provengan de las respectivas vlan, por tanto el computador conectado a dicha interfaz podrá recibir tráfico de esa vlan, asì mismo se habilitó e protocolo Spanning tree en las interfaces.

A continuación, se realizan las verificaciones de las configuraciones ingresadas en los dispositivos, a través de los comandos show.

Figura 03 D2# show interfaces trunk en D1

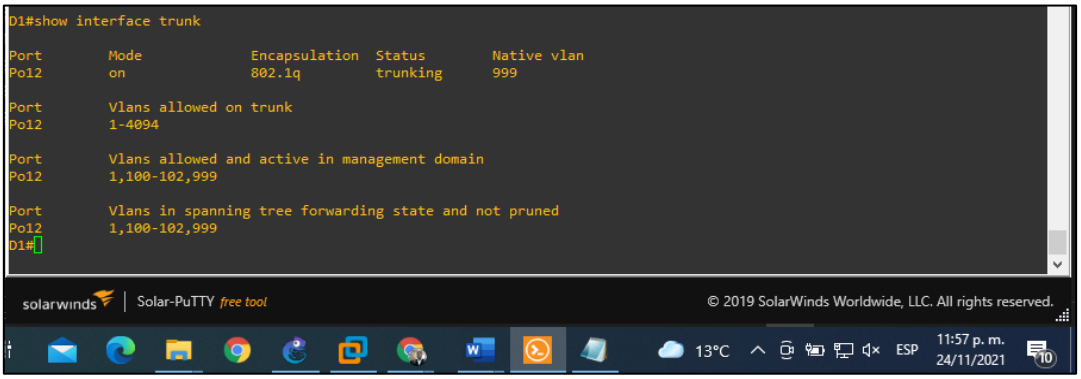
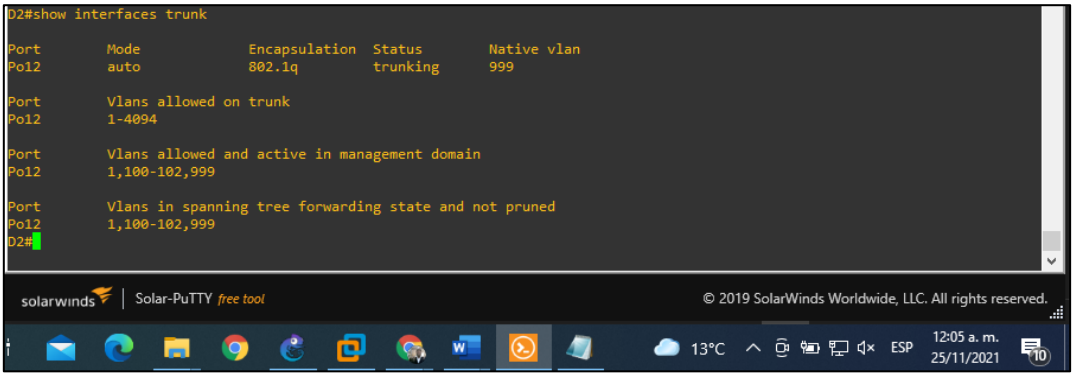


Figura 04 D2# show interfaces trunk en D2



De acuerdo a la información devuelta por el comando de verificación se evidencia que se cumplieron las tareas configurar enlaces troncales 802.1Q, cambiar la VLAN nativa en los enlaces troncales y crear LACP EtherChannels. Tareas 2.1, 2.2 y 2.5.

Figura 05 D1# show run | include spanning-tree en D1

Figura 06 D2# show run | include spanning-tree en D2

De acuerdo a la información devuelta por el comando de verificación se evidencia que se cumplieron las tareas configurar el Protocolo de árbol de expansión rápido, y configurar los puentes raíz RSTP, tareas 2.3 y 2.4.

Figura 07 D1# show run interface e1/1 en D1

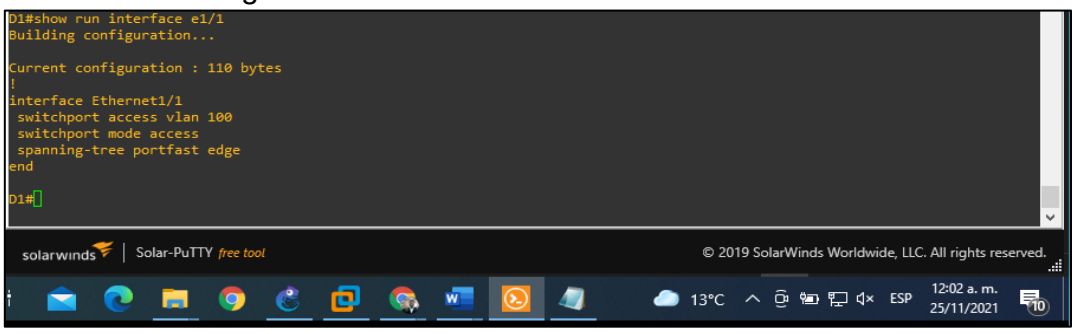


Figura 08 D1# show run interface e1/1 en D2

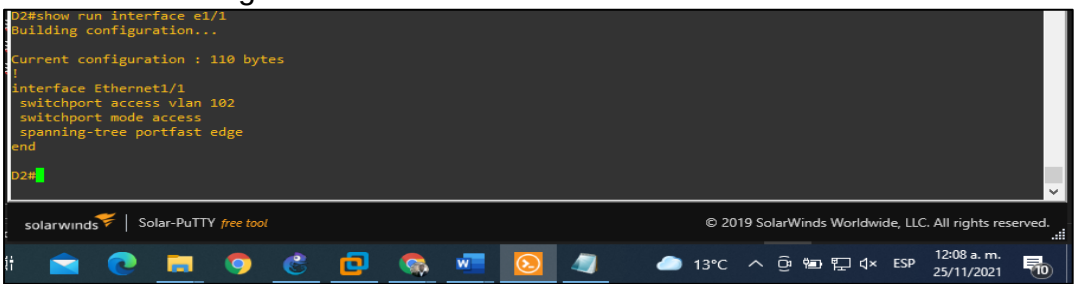
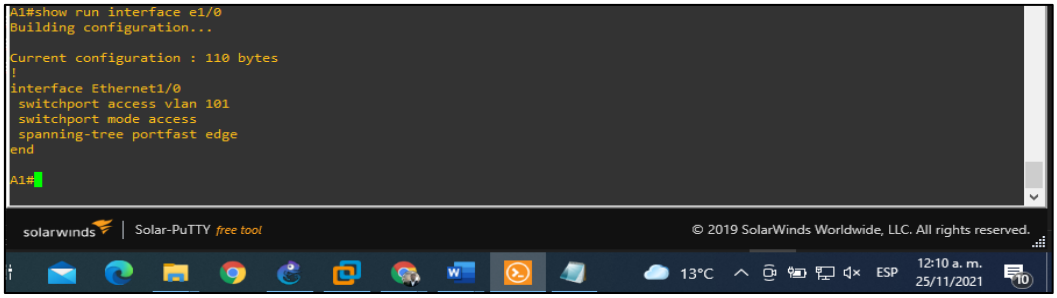


Figura 09 A1# show run interface e1/0 en A1



De acuerdo a la información devuelta por el comando de verificación se evidencia que se cumplieron las tareas configurar los puertos de acceso del host que se conecten a PC1, PC2, PC3 y PC4, tareas 2.6.

Parte 3: Configurar los protocolos de enrutamiento

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

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.

Las tareas de configuración son las siguientes:

Tabla 3. Tareas de Configuración Parte 3

Tarea#	Tarea	Especificación
3.1	En la “Red de la Compañia” (es decir, R1, R3, D1, y D2), configure singlearea OSPFv2 en area 0.	Use OSPF Process ID **4** y asigne los siguientes routerIDs: 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 Compañia” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID **6** y asigne los siguientes routerIDs: 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
3.3		Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

	En R2 en la “Red ISP”, configure MPBGP.	Una ruta estática predeterminada IPv4. Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: La red Loopback 0 IPv4 (/32). La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: La red Loopback 0 IPv4 (/128). La ruta por defecto (::/0).
3.4	En R1 en la “Red ISP”, configure MPBGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN **300** y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

El enrutamiento dinámico es fundamental en las redes grandes como la que se simula en el presente trabajo, toda vez que un protocolo de enrutamiento dinámico, enseña al router a aprender y guardar en su tabla de enrutamiento

las mejores rutas para llegar a sus destinos, en este caso se utiliza el protocolo OSPF, el cual basa su métrica en el costo de la interfaz, a menor costo mejor ruta, su algoritmo se basa en abrir la ruta más corta primero.

Comandos de Configuración parte 3

Comandos Configuración R1

router ospf 4	▪ Habilita el protocolo OSPF
router-id 0.0.4.1	▪ Asigna un identificador de reouter
network 10.0.10.0 0.0.0.255 area 0	▪ Anuncia la rede conectadas directamente
network 10.0.13.0 0.0.0.255 area 0	▪ Anuncia la rede conectadas directamente
default-information originate	▪ Establece origen de información de rutas
exit	▪ Salir del modo de configuración

En las líneas de comando anteriores se da cumplimiento a la tarea 3.1, donde se configura el dominio de routin de OSPF en el número de proceso 4, y se asignan los ID para cada uno de los routers, y se anuncian las redes conectadas a al área 0, de igual forma se establece que R1 sea el origen de la información de la ruta predeterminada y que propague la ruta estática predeterminada en las actualizaciones OSPF.

ipv6 router ospf 6	▪ Habilita el protocolo OSPF
router-id 0.0.6.1	▪ Asigna un identificador de reouter
default-information originate	▪ Establece origen de información de rutas
exit	▪ Salir del modo de configuración
interface g1/0	▪ Ingreso a modo de configuración de la interfaz g0/1
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF
exit	▪ Salir del modo de configuración

interface s2/0	▪ Ingreso a modo de configuración de la interfaz s2/0.
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF
exit	▪ Salir del modo de configuración
ip route 10.0.0.0 255.0.0.0 null0 ipv6 route 2001:db8:100::/48 null0	▪ Estos comandos hacen referencia a rutas estáticas de redes públicas que apuntan a interfaces nulas
router bgp 300	▪ Habilita el routing de border
bgp router-id 1.1.1.1	▪ Habilita un Id de router
neighbor 209.165.200.226 remote-as 500	▪ Estable conexión con sistema autónomo 500
neighbor 2001:db8:200::2 remote-as 500	▪ Estable conexión con sistema autónomo 500
address-family ipv4 unicast	▪ Familia de direcciones ipv4
neighbor 209.165.200.2 activate	▪ Activa la conexión remota con el router vecino en ipv4
neighbor 2001:db8:200::2 activa	▪ Activa la conexión remota con el router vecino en ipv6
network 10.0.0.0 mask 255.0.0.0	▪ Se estable red y mascara de red ipv4
exit-address-family	▪ Salir de la familia de direcciones ipv4
address-family ipv6 unicast	▪ Familia de direcciones ipv6
no neighbor 209.165.200.2	▪ Activa la conexión remota con el router vecino en ipv4
neighbor 2001:db8:200::2 activate	▪ Activa la conexión remota con el router vecino en ipv6
network 2001:db8:100::/48	▪ Se estable red y mascara de red ipv6
exit-address-family	▪ Salir de la familia de direcciones ipv4

Comandos Configuración R2

ip route 0.0.0.0 0.0.0.0 loopback 0	▪ Ruta estática hacia loopback 0
ipv6 route ::/0 loopback 0	▪ Configura ruta predeterminada a loopback 0

router bgp 500	▪ Configura la intefaz loopback para el routing BGP
bgp router-id 2.2.2.2	▪ Establece router id
neighbor 209.165.200.1 remote-as 300	▪ Estable conexión con sistema autónomo 500
neighbor 2001:db8:200::1 remote-as 300	▪ Estable conexión con sistema autónomo 500
address-family ipv4	▪ Ingreso a familia de direcciones ipv4
neighbor 209.165.200.1 activate	▪ Activa la conexión remota con el router vecino en ipv4
no neighbor 2001:db8:200::1 activate	▪ desactiva la conexión remota con el router vecino en ipv6
network 2.2.2.2 mask 255.255.255.255	▪ Se estable red y mascara de red ipv4
network 0.0.0.0	▪ Se estable ip por defecto para ipv4
exit-address-family	▪ Salir de la familia de direcciones ipv4
address-family ipv6	▪ Ingreso a familia de direcciones ipv6
no neighbor 209.165.200.1 activate	▪ Desactiva la conexión remota con el router vecino en ipv4
neighbor 2001:db8:200::1 activate	▪ Activa la conexión remota con el router vecino en ipv4
network 2001:db8:2222::/128	▪ Se estable red y mascara de red ipv6
network ::/0	▪ Se estable ip por defecto para ipv6
exit-address-family	▪ Salir de la familia de direcciones ipv6

Comandos Configuración R3

router ospf 4	▪ Habilita el protocolo OSPF
router-id 0.0.4.3	▪ Asigna un identificador de reouter
network 10.0.11.0 0.0.0.255 area 0	▪ Anuncia la red conectada directamente
ipv6 router ospf 6	▪ Habilita el protocolo OSPF

router-id 0.0.6.3	▪ Asigna un identificador de reouter
exit	▪ Salir del modo de configuración
interface g1/0	▪ Ingreso a modo de configuración de la interfaz g0/1
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en la interfaz.
exit	▪ Salir del modo de configuración
interface s2/0	▪ Ingreso a modo de configuración de la interfaz s2/0.
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF
exit	▪ Salir del modo de configuración
end	▪ Regresar al modo usuario

Comandos Configuración Switch D1

router ospf 4	▪ Habilita el protocolo OSPF
router-id 0.0.4.131	▪ Asigna un identificador de reouter
network 10.0.100.0 0.0.0.255 area 0	▪ Anuncia la red conectada directamente
network 10.0.101.0 0.0.0.255 area 0	▪ Anuncia la rede conectadas directamente
network 10.0.102.0 0.0.0.255 area 0	▪ Anuncia la rede conectadas directamente
network 10.0.10.0 0.0.0.255 area 0	▪ Anuncia la rede conectadas directamente
passive-interface default	▪ No envía paquetes ni hellos
no passive-interface e1/0	▪ La interfaz no envía paquetes ni hellos
exit	▪ Regreso a modo global
ipv6 router ospf 6	▪ Habilita el protocolo OSPF en router
router-id 0.0.6.131	▪ Asigna un identificador de reouter
passive-interface default	▪ No envía paquetes ni hellos
no passive-interface e1/0	▪ La interfaz no envía paquetes ni hellos

exit	▪ Regreso a modo global
interface e1/0	▪ Ingreso a modo configuración de interfaz
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
interface vlan 100	▪ Ingreso a vlan 100
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
interface vlan 101	▪ Ingreso a vlan 101
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
interface vlan 102	▪ Ingreso a vlan 102
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
end	▪ Salida a modo usuario

Comandos Configuración Switch D2

router ospf 4	▪ Habilita el protocolo OSPF
router-id 0.0.4.131	▪ Asigna un identificador de reouter
network 10.0.100.0 0.0.0.255 area 0	▪ Anuncia la red conectada directamente
network 10.0.101.0 0.0.0.255 area 0	▪ Anuncia la red conectada directamente
network 10.0.102.0 0.0.0.255 area 0	▪ Anuncia la red conectada directamente
network 10.0.10.0 0.0.0.255 area 0	▪ Anuncia la red conectada directamente
passive-interface default s	▪ No envía paquetes ni hello
no passive-interface e1/0	▪ La interfaz no envía paquetes ni hellos
exit	▪ Salida a modo configuración global

ipv6 router ospf 6	▪ Habilita el protocolo OSPF en el Switch
router-id 0.0.6.131	▪ Asigna un identificador de proceso
passive-interface default	▪ No envía paquetes ni hello
no passive-interface e1/0	▪ La interfaz no envía paquetes ni hellos
exit	▪ Salir del modo de configuración
interface e1/0	▪ Ingreso a interfaz e1/0
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
interface vlan 100	▪ Ingreso a vlan 100
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
interface vlan 101	▪ Ingreso a vlan 101
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
interface vlan 102	▪ Ingreso a vlan 102
ipv6 ospf 6 area 0	▪ Habilita el protocolo OSPF en el área 0.
exit	▪ Regreso a modo global
end	▪ Regresa a modo usuario

Con los anteriores grupos de comandos se configuró un dominio de routing OSPF en el área 0, ahora todas las interfaces que hacen parte de este dominio, podrán intercambiar información de estado de enlace, es decir cada router enviará de forma periódica una actualización, de su tabla de enrutamiento a los router vecinos, cuando se presente un cambio en una ruta, todos los router actualizaran su tabla de enrutamiento y recalcularan la forma los caminos para alcanzar nuevamente las redes lejanas, se configuran algunas interfaces en el modo pasivo, para que no envíen actualizaciones y así evitar que el ancho de banda de la red se vea afectado; el protocolo BGP, actúa como router fronterizo, es decir, interconecta dos redes diferentes, en este caso los sistemas autónomos 500 y 300 que representan a la red del ISP y la red la compañía respectivamente.

A continuación, se realizan las verificaciones de las configuraciones ingresadas en los dispositivos, a través de los comandos show.

Figura 10 R1 # show run | sección ^ router ospf en R1

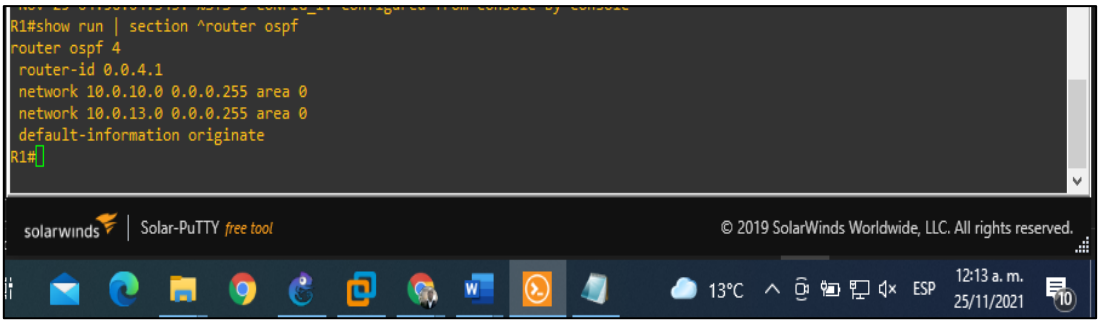


Figura 11 R3 # show run | sección ^ router ospf en R3

Figura 12 D2s # show run | sección ^ router ospf en D1

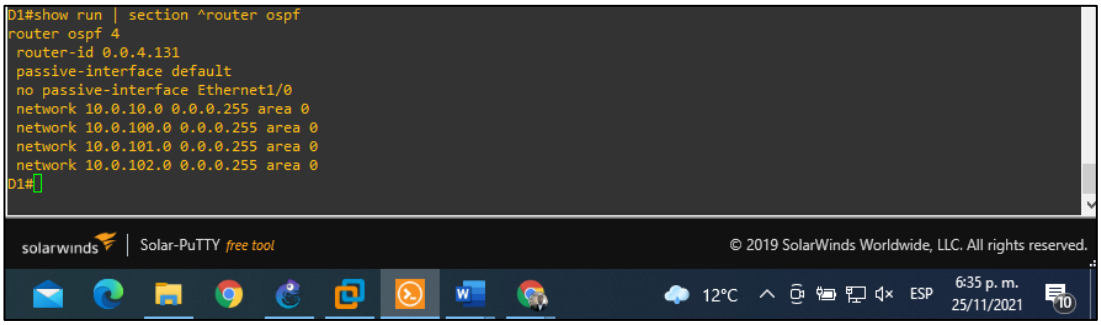


Figura 13 D2 # show run | sección ^ router ospf en D2

De acuerdo a la información devuelta por el comando de verificación se evidencia que se cumple la tarea configurar OSPFv2 de área única en el área 0. Tarea 3.1.

Figura 14 R1# show run | section ^ipv6 router en R1

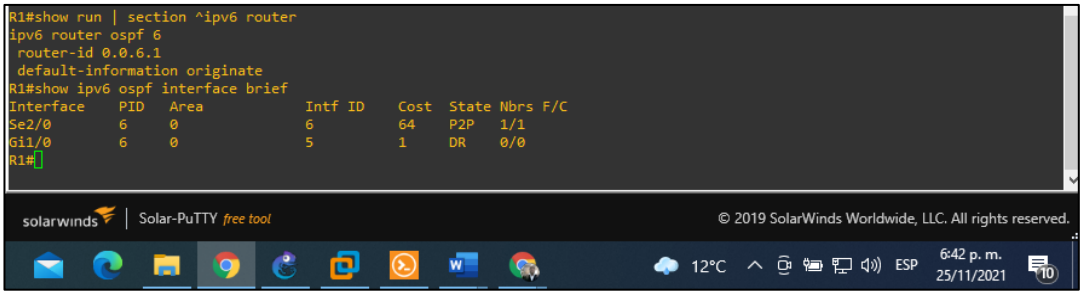


Figura 15 R3# show run | section ^ipv6 router en R3

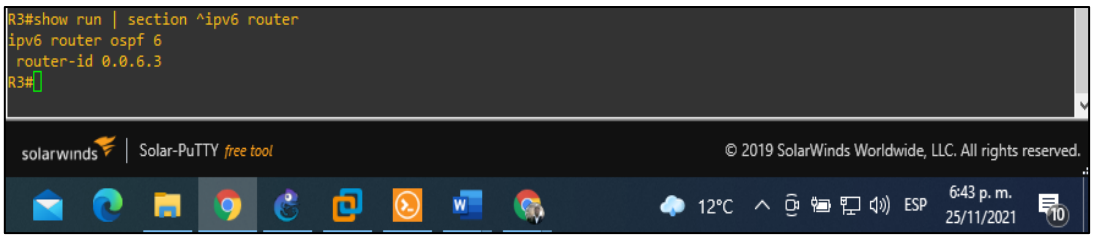


Figura 16 R3# show ipv6 ospf interface brief en R3

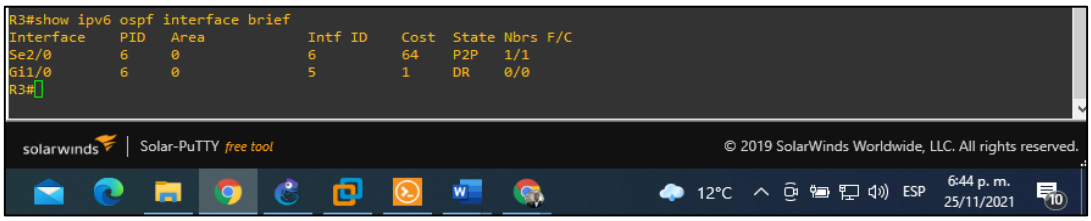


Figura 17 D1# show run | section ^ipv6 router en D1

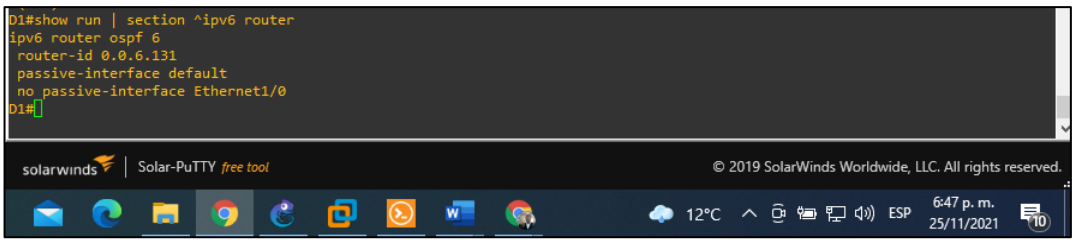


Figura 18 D1# show ipv6 ospf interface brief en D1

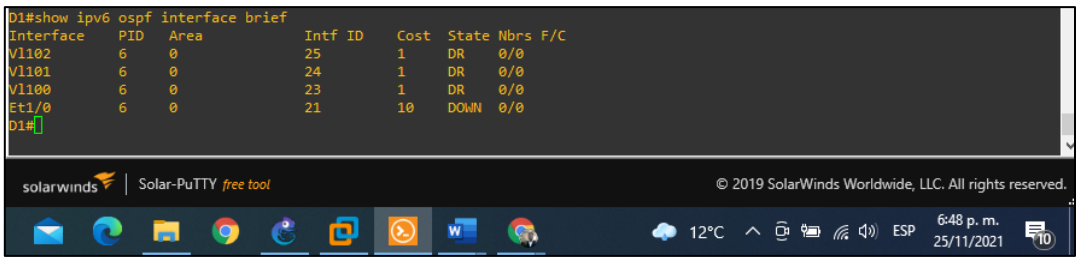


Figura 19 D2# show run | section ^ipv6 router en D12

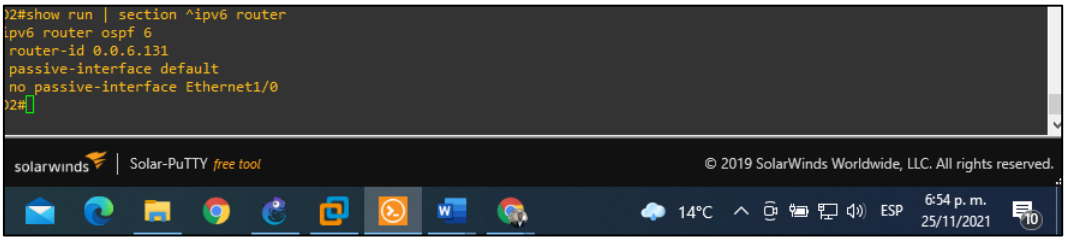
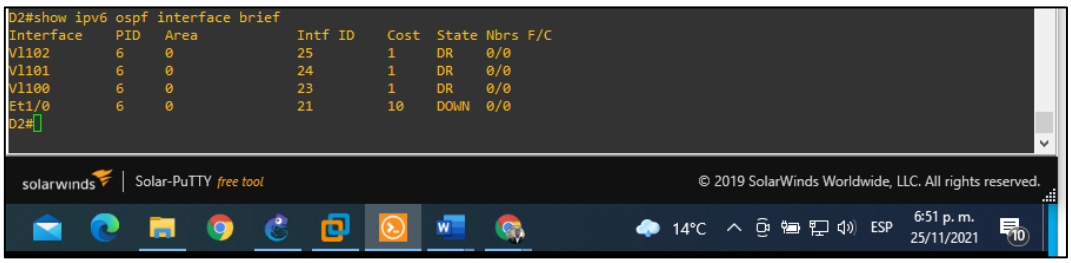


Figura 20 D2# show ipv6 ospf interface brief



De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumple la tarea configurar configure el OSPFv3 clásico de área única en el área 0.. Tarea 3.2.

Figura 21 R2# show run | section router bgp en R2

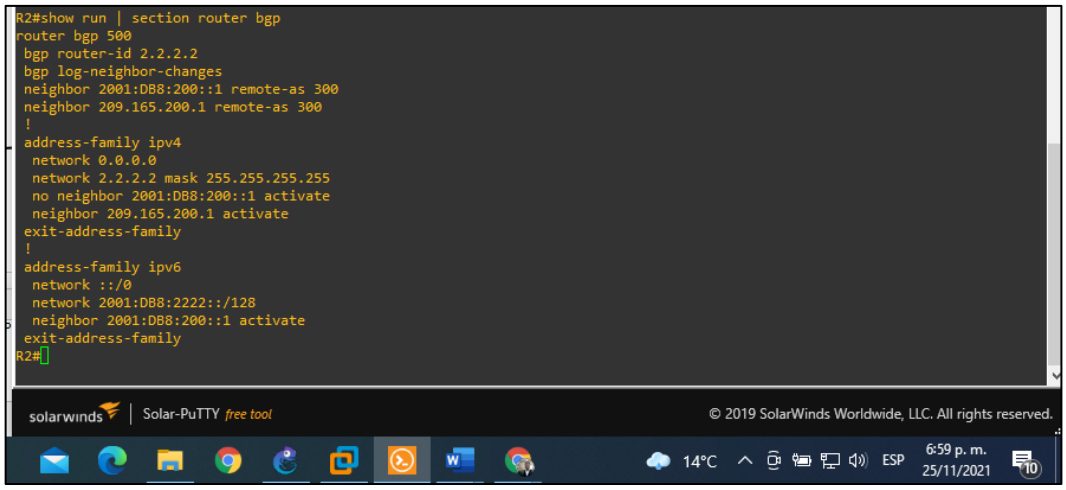
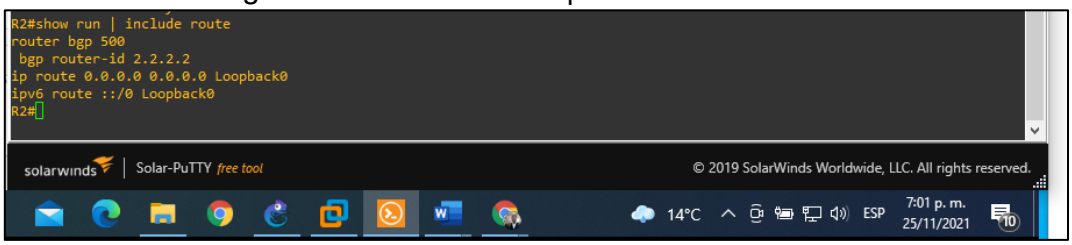


Figura 22 R2# show run | include routeen R2



De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumple la tarea, en R2 en la “Red ISP”, configure MP-BGP.Tarea 3.3

Figura 23 R1# show run | section bgp en R1

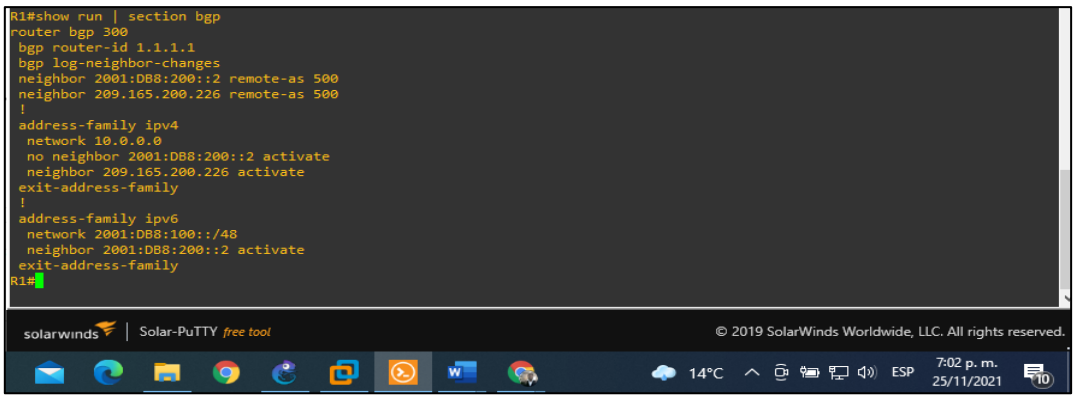


Figura 24 R1# show ip route | include O|B en R1

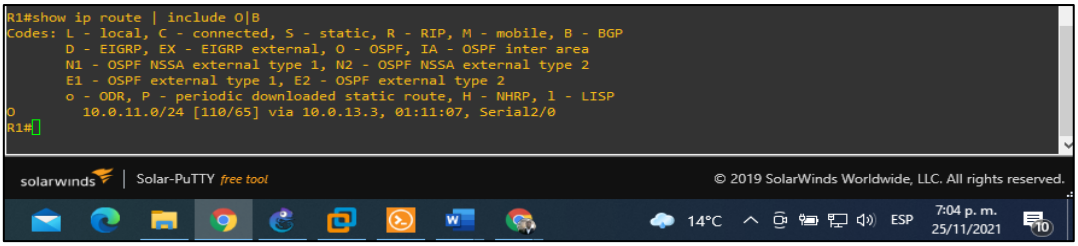


Figura 25 R1# show ipv6 route en R1

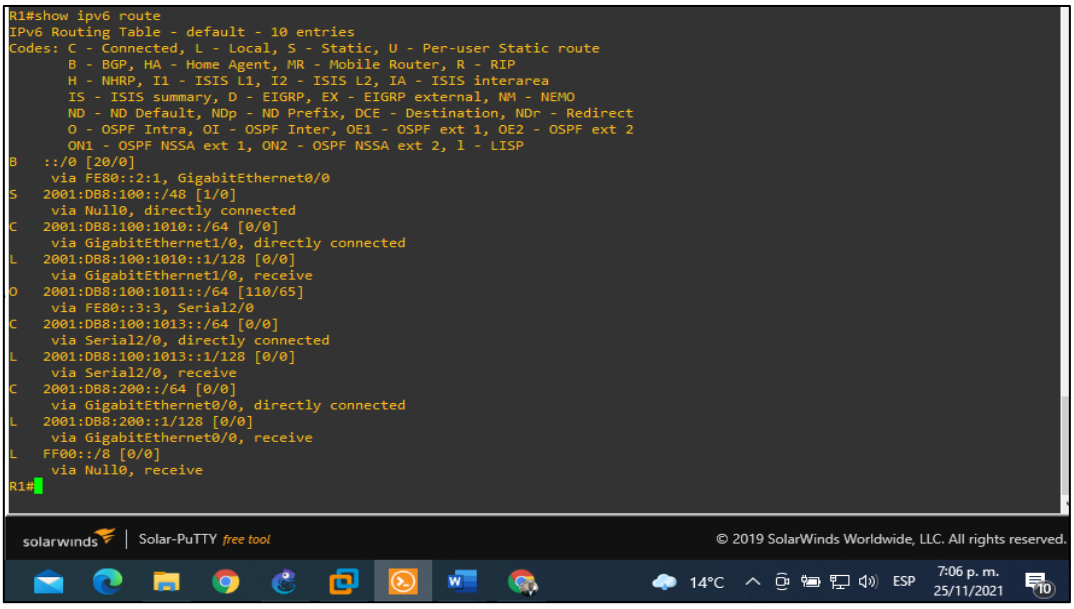
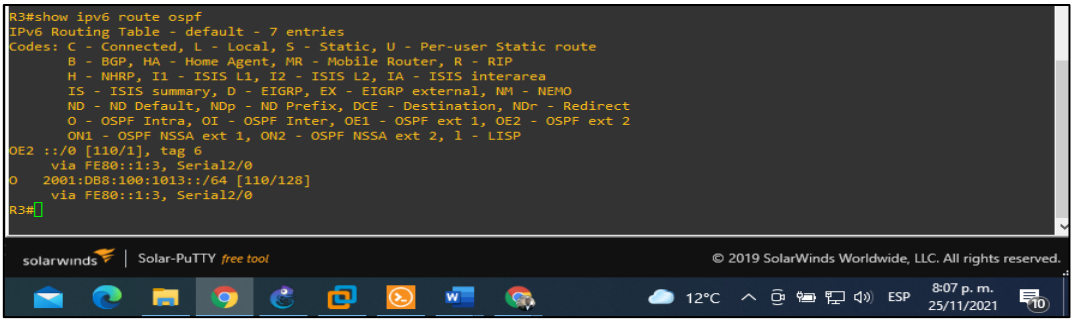


Figura 26 R3# show ip route ospf | begin Gateway en R3

Figura 27 R3# show ipv6 route ospfen R3



De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumple la tarea, en R1 en la “Red ISP”, configure MP-BGP. Tarea 3.4

Parte 4: Configurar la redundancia del primer salto (FHRP/SLA)

En esta parte, configurará HSRP versión 2 para proporcionar redundancia de primer salto para hosts en la "red de la empresa".

Tabla 4. Tareas de Configuración Parte 4

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.	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. 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.
	En D2, configure HSRPv2.	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**. E stablezca 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.

En esta parte se realiza la configuración de redundancia a nivel de Gateway, lo que se traduce, en que el grupo de router utilizaran una ip y una mac virtual, que será común para ellos, más, sin embargo, solo deberá haber un router en el modo active quien será el que utilice la ip virtual.

Comandos de Configuración Switch D1

ip sla 4	▪ Se habilita el modo monitoreo en ipv4
icmp-echo 10.0.10.1	▪ Monitoreo mediante ping a ip 10.0.10.1

frequency 5	▪ Establece como frecuencia cada 5 milisegundos
exit	▪ Salida
ip sla 6	▪ Se habilita el modo monitoreo en ipv6
icmp-echo 2001:db8:100:1010::1	▪ Monitoreo mediante ping a ipv6
frequency 5	▪ Establece como frecuencia cada 5 milisegundos
exit	▪ Salida
ip sla schedule 4 life forever start-time now	▪ Establece tiempo de inicio y duración
ip sla schedule 6 life-forever start-time now	▪ Establece tiempo de inicio y duración
track 4 ip sla 4	▪ Establece el objeto llamado ip sla 4
delay down 10 up 15	▪ Se establece tiempos de retardo entre 10 y 15 ms
exit	▪ Salir
track 6 ip sla 6	▪ Establece el objeto llamado ip sla 6
delay down 10 up 15	▪ Se establece tiempos de retardo entre 10 y 15 ms
exit	▪ Salida
interface vlan 100	▪ Ingreso a la interfaz vlan 100
standby version 2	▪ Habilita la versión 2 de HSRP
standby 104 ip 10.0.100.254	▪ Configura una ip en Standby para D1 en vlan 100
standby 104 priority 150	▪ Asigna una prioridad de 150 a D1
standby 104 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 104 track 4 decrement 60	▪ Realizar un decremento de 60
standby 106 ipv6 autoconfig	▪ Realiza autoconfiguración de IPV6 en el grupo 106
standby 106 priority 150	▪ Configura el router para sustituir el router activo.

standby 106 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 106 track 6 decrement 60	▪ Realizar un decremento de 60
exit	▪ Salida
interface vlan 101	▪ Ingreso a la interfaz vlan 101
standby version 2	▪ Habilita la versión 2 de HSRP
standby 114 ip 10.0.101.254	▪ Configura una ip en Standby para D1 en vlan 101
standby 114 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 114 track 4 decrement 60	▪ Realizar un decremento de 60
standby 116 ipv6 autoconfig	▪ Realiza autoconfiguración de IPV6 en el grupo 116
standby 116 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 116 track 6 decrement 60	▪ Realizar un decremento de 60
exit	▪ Salida
interface vlan 102	▪ Ingreso a la interfaz vlan 102
standby version 2	▪ Habilita la versión 2 de HSRP
standby 124 ip 10.0.102.254	▪ Configura una ip en Standby para D1 en vlan 102
standby 124 priority 150	▪ Asigna una prioridad de 150 a D1
standby 124 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 124 track 4 decrement 60	▪ Realizar un decremento de 60
standby 126 ipv6 autoconfig	▪ Realiza autoconfiguración de IPV6 en el grupo 116
standby 126 priority 150	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 126 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 126 track 6 decrement 60	▪ Realizar un decremento de 60
exit	▪ Salida
end	▪ Modo usuario

Comandos de Configuración Switch D2

ip sla 4	▪ Se habilita el modo monitoreo en ipv4

icmp-echo 10.0.10.1	▪ Monitoreo mediante ping a ip 10.0.10.1
frequency 5	▪ Establece como frecuencia cada 5 milisegundos
exit	▪ Salida
ip sla 6	▪ Se habilita el modo monitoreo en ipv6
icmp-echo 2001:db8:100:1010::1	▪ Monitoreo mediante ping a ipv6
frequency 5	▪ Establece como frecuencia cada 5 milisegundos
exit	▪ Salida
ip sla schedule 4 life forever start-time now	▪ Establece tiempo de inicio y duración
ip sla schedule 6 life-forever start-time now	▪ Establece tiempo de inicio y duración
track 4 ip sla 4	▪ Establece el objeto llamado ip sla 4
delay down 10 up 15	▪ Se establece tiempos de retardo entre 10 y 15 ms
exit	▪ Salir
track 6 ip sla 6	▪ Establece el objeto llamado ip sla 6
delay down 10 up 15	▪ Se establece tiempos de retardo entre 10 y 15 ms
exit	▪ Salida
interface vlan 100	▪ Ingreso a la interfaz vlan 100
standby version 2	▪ Habilita la versión 2 de HSRP
standby 104 ip 10.0.100.254	▪ Configura una ip en Standby para D1 en vlan 100
standby 104 priority 150	▪ Asigna una prioridad de 150 a D1
standby 104 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 104 track 4 decrement 60	▪ Realizar un decremento de 60
standby 106 ipv6 autoconfig	▪ Realiza autoconfiguración de IPV6 en el grupo 106

standby 106 priority 150	▪ Configura el router para sustituir el router activo.
standby 106 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 106 track 6 decrement 60	▪ Realizar un decremento de 60
exit	▪ Salida
interface vlan 101	▪ Ingreso a la interfaz vlan 101
standby version 2	▪ Habilita la versión 2 de HSRP
standby 114 ip 10.0.101.254	▪ Configura una ip en Standby para D1 en vlan 101
standby 114 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 114 track 4 decrement 60	▪ Realizar un decremento de 60
standby 116 ipv6 autoconfig	▪ Realiza autoconfiguración de IPV6 en el grupo 116
standby 116 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 116 track 6 decrement 60	▪ Realizar un decremento de 60
exit	▪ Salida
interface vlan 102	▪ Ingreso a la interfaz vlan 102
standby version 2	▪ Habilita la versión 2 de HSRP
standby 124 ip 10.0.102.254	▪ Configura una ip en Standby para D1 en vlan 102
standby 124 priority 150	▪ Asigna una prioridad de 150 a D1
standby 124 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 124 track 4 decrement 60	▪ Realizar un decremento de 60
standby 126 ipv6 autoconfig	▪ Realiza autoconfiguración de IPV6 en el grupo 116
standby 126 priority 150	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 126 preempt	▪ Habilita el Protocolo de router en reserva activo HSRP
standby 126 track 6 decrement 60	▪ Realizar un decremento de 60
exit	▪ Salida
end	▪ Modo usuario

Por medio de las líneas de comandos anteriores se establecieron como ips virtuales las direcciones 10.0.100.254, 10.0.101.254, 10.0.102.254, y una prioridad de 150, por lo tanto, la interfaz, router con mayor prioridad será el router «active» y se encargará de enrutar los paquetes a través de la IP virtual, en este caso D1

A continuación, se realizan las verificaciones de las configuraciones ingresadas en los dispositivos, a través de los comandos show.

Figura 28 D1# show run | section ip sla en D1

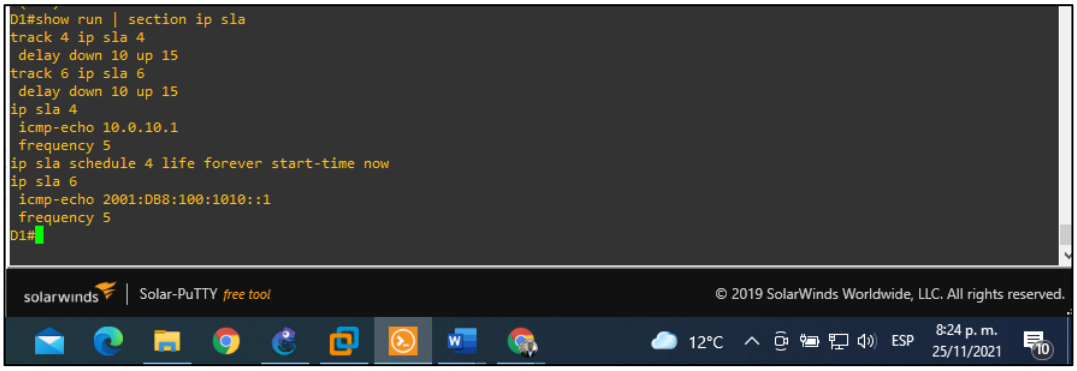


Figura 29 D1# show standby brief en D1

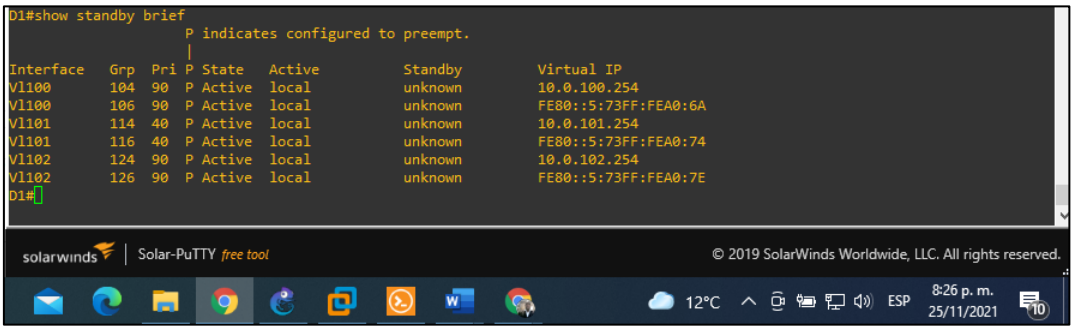
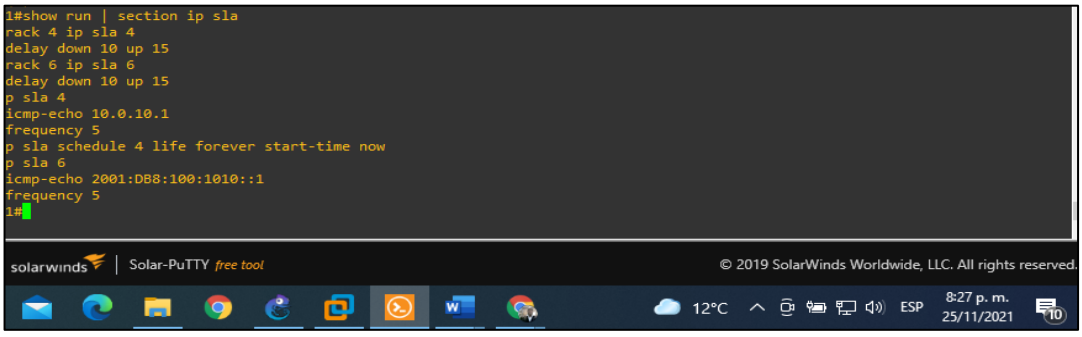


Figura 30 D2# show run | section ip sla en D2



De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumple la tarea configurar en D1, HSRPv2. Tarea 4.3.

Parte 5: Seguridad

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

Sus tareas de configuración son las siguientes**:**

Tabla 5. Tareas de Configuración Parte 5

Tarea#	Tarea	Especificación
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de 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**.

Comandos configuración Seguridad en cada dispositivo

enable algorithm-type SCRYPT secret cisco12345cisco	▪ Se protege el EXEC privilegiado mediante el algoritmo de cifrado SCRYPT.
username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco	▪ Con el anterior comando, en todos los dispositivos, cree un localizador y asegúrelo con el algoritmo de cifrado SCRYPT.
aaa new-model	▪ En todos los dispositivos menos en R2 se habilita la autenticación AAA
radius server RADIUS	▪ Crea servidor Radius
address ipv4 10.0.100.6 auth-port 1812 acct-port 1813	▪ Crea servidor Radius
key $trongPass	▪ Configura contaseña
exit	▪ Salir
aaa authentication login default group radius local	▪ Autenticación AAA
end	▪ Finalizar

Con el grupo de comandos anteriores, se configuran las especificaciones del servidor RADIUS.

A continuación, se realizan las verificaciones de las configuraciones ingresadas en los dispositivos, a través de los comandos show.

Figura 31 R1# show run | include secret en R1

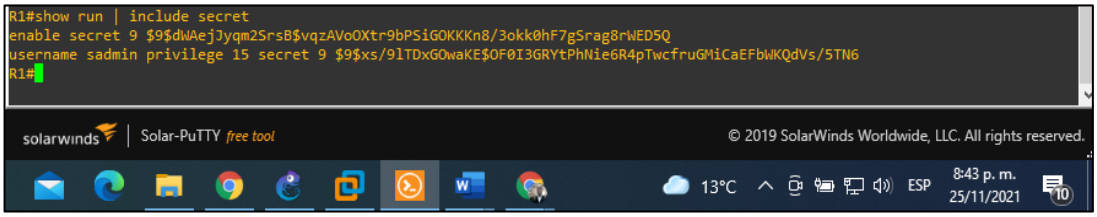
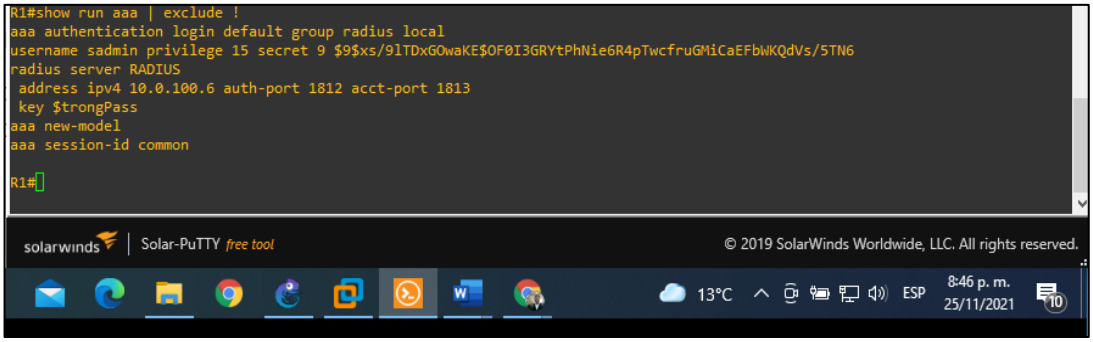


Figura 32 R1# show run aaa | exclude en R1



De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumplieron las tareas, En todos los dispositivos, proteja el EXEC privilegiado mediante el algoritmo de cifrado SCRYPT, configure las especificaciones del servidor RADIUS Tareas 5.1 al 5.6

Parte 6: Configure las funciones de Administración de Red

En esta parte, debe configurar varias funciones de administración de red. Las tareas de configuración son las siguientes:

Tabla 6. Tareas de Configuración Parte 6

Tarea #	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.

6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: R1 debe sincronizar con R2. R3, D1 y A1 para sincronizar la hora con R1.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel
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.

En esta parte se realizará la configuración de un protocolo ara la administración de la red, el cual es fundamental para el intercambio de información entre dispositivos y facilitar la administración remota.

Comandos de Configuración R2:

-

ntp master 3

- Configura a R2 como NTP maestro.

End

- Finalizar

Comandos de Configuración R1

ntp server 2.2.2.2

- Establece el servidor ntp

logging trap warning

- Controla los mensajes enviados al servidor Syslog

logging host 10.0.100.5

- Se configura la dirección ip de syslog

logging on

- Se loguea

ip access-list standard SNMP-NMS

- Se ingresa snmp-nms a ACL estándar

permit host 10.0.100.5	▪ Se permite en la regla de la ACL el host 10.0.100.5
exit	▪ Salir del modo de configuración
snmp-server contact Cisco Student	▪ Habilita el contacto del sistema
snmp-server community ENCORSA ro SNMP-NMS	▪ Define identificación de comunidad en este caso ENCORSA
snmp-server host 10.0.100.5 version 2c ENCORSA,	▪ Se envían notificaciones a 10.
snmp-server ifindex persist	▪ Valor de índice de interfaz persist
snmp-server enable traps bgp	▪ Habilita bgp para recopilar información
snmp-server enable traps config	▪ Habilita configuración de snmp
snmp-server enable traps ospf	▪ Habilita ospf para recopilar información
end	▪ Finalizar

Comandos de Configuración de R3

ntp server 10.0.10.1	▪ Establece el servidor ntp
logging trap warning	▪ Controla los mensajes enviados al servidor Syslog
logging host 10.0.100.5	▪ Se configura la dirección ip de syslog
logging on	▪ Se loguea
ip access-list standard SNMP-NMS	▪ Se ingresa snmp-nms a ACL estándar
permit host 10.0.100.5	▪ Se permite en la regla de la ACL el host 10.0.100.5
exit	▪ Salir del modo de configuración
snmp-server contact Cisco Student	▪ Habilita el contacto del sistema
snmp-server community ENCORSA ro SNMP-NMS	▪ Define identificación de comunidad en este caso ENCORSA
snmp-server host 10.0.100.5 version 2c ENCORSA	▪ Se envían notificaciones a 10.
snmp-server ifindex persist	▪ Valor de índice de interfaz persist

snmp-server enable traps config	▪ Habilita bgp para recopilar información
snmp-server enable traps ospf	▪ Habilita configuración de traps para config
end	▪ Habilita ospf para recopilar información

Comandos de Configuración Switch D1

ntp server 10.0.10.1	▪ Establece el servidor ntp
logging trap warning	▪ Controla los mensajes enviados al servidor Syslog
logging host 10.0.100.5	▪ Se configura la dirección ip de syslog
logging on	▪ Se loguea
ip access-list standard SNMP-NMS	▪ Se ingresa snmp-nms a ACL estándar
permit host 10.0.100.5	▪ Se permite en la regla de la ACL el host 10.0.100.5
exit	▪ Salir del modo de configuración
snmp-server contact Cisco Student	▪ Habilita el contacto del sistema
snmp-server community ENCORSA ro SNMP-NMS	▪ Define identificación de comunidad en este caso ENCORSA
snmp-server host 10.0.100.5 version 2c ENCORSA	▪ Se envían notificaciones a 10.0.100.5
snmp-server ifindex persist	▪ Valor de índice de interfaz persist
snmp-server enable traps config	▪ Habilita configuración de traps para config
snmp-server enable traps ospf	▪ Habilita ospf para recopilar información
end	▪ Finalizar

Comandos de Configuración Switch D2

ntp server 10.0.10.1	▪ Establece el servidor ntp
logging trap warning	▪ Controla los mensajes enviados al servidor Syslog
logging host 10.0.100.5	▪ Se configura la dirección ip de syslog

logging on	▪ Se loguea
ip access-list standard SNMP-NMS	▪ Se ingresa snmp-nms a ACL estándar
permit host 10.0.100.5	▪ Se permite en la regla de la ACL el host 10.0.100.5
exit	▪ Salir del modo de configuración
snmp-server contact Cisco Student	▪ Habilita el contacto del sistema
snmp-server community ENCORSA ro SNMP-NMS	▪ Define identificación de comunidad en este caso ENCORSA
snmp-server host 10.0.100.5 version 2c ENCORSA	▪ Se envían notificaciones a 10.0.100.5
snmp-server enable traps config	▪ Habilita configuración de traps para config
snmp-server enable traps ospf	▪ Habilita ospf para recopilar información
end	▪ Finalizar

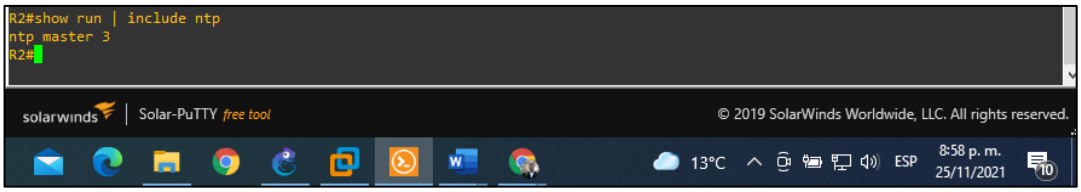
Comandos de Configuración Switch D2

ntp server 10.0.10.1	▪ Establece el servidor ntp
logging trap warning	▪ Controla los mensajes enviados al servidor Syslog
logging host 10.0.100.5	▪ Se configura la dirección ip de syslog
logging on	▪ Se loguea
ip access-list standard SNMP-NMS	▪ Se ingresa snmp-nms a ACL estándar
permit host 10.0.100.5	▪ Se permite en la regla de la ACL el host 10.0.100.5
exit	▪ Salir del modo de configuración
snmp-server contact Cisco Student	▪ Habilita el contacto del sistema
snmp-server community ENCORSA ro SNMP-NMS	▪ Define identificación de comunidad en este caso ENCORSA
snmp-server host 10.0.100.5 version 2c ENCORSA	▪ Se envían notificaciones a 10.0.100.5
snmp-server ifindex persist	▪ Valor de índice de interfaz persist

snmp-server enable traps config	▪ Habilita configuración de traps para config
snmp-server enable traps ospf	▪ Habilita ospf para recopilar información
end	▪ Finalizar

A continuación, se realizan las verificaciones de las configuraciones ingresadas en los dispositivos, a través de los comandos show.

Figura 33 R1# show run | include ntp en R1



De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumplió la tarea Configure R2 como maestro NTP. 6.2

Figura 34 R1# show run | include loggingen R1

De acuerdo con la información devuelta por el comando de verificación se evidencia que se cumplió la tarea Configure SNMPv2c en todos los dispositivos excepto R2. 6.5

Figura 35 D1# show ip access-list SNMP-NMS D1

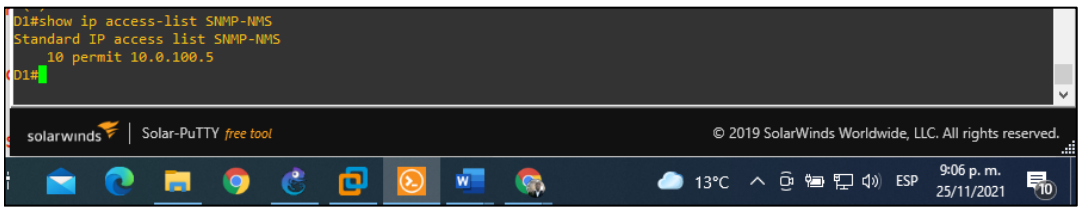


Figura 36 R1# show run | include snmpen R1

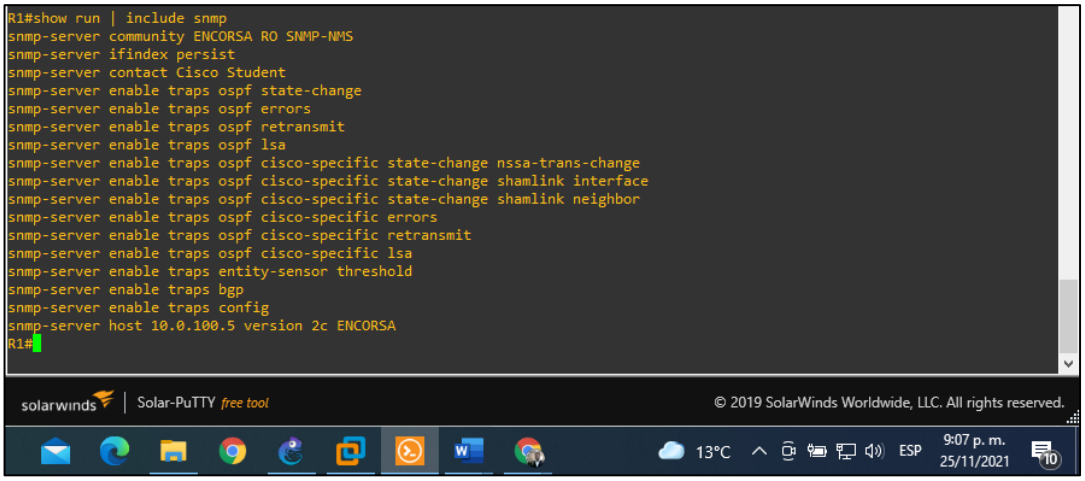


Figura 37 R3# show run | include snmp en R3

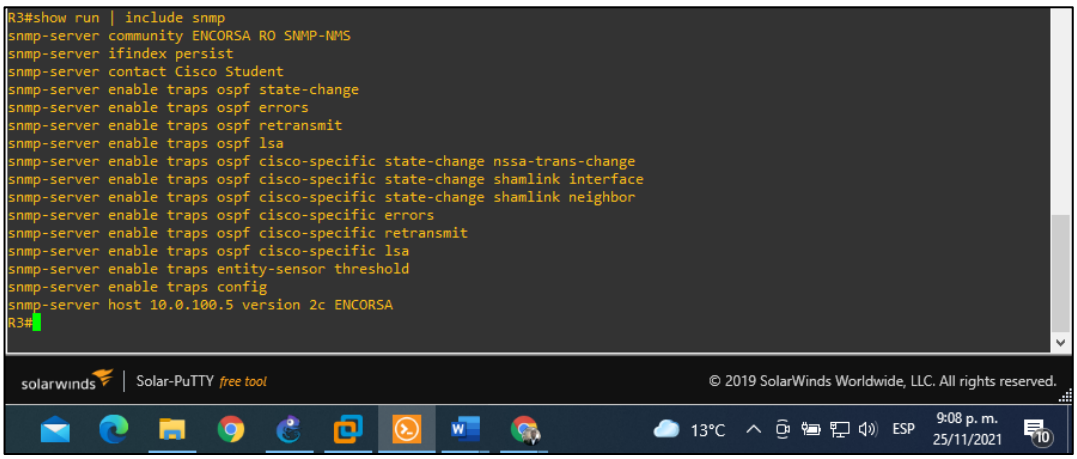


Figura 38 D1# show run | include snmp en D1

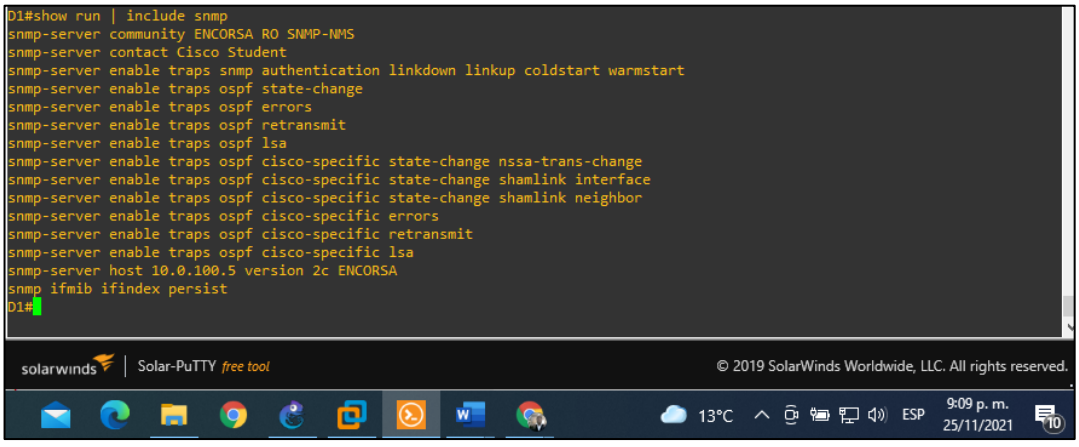


Figura 39 D2# show run | include snmp en D2

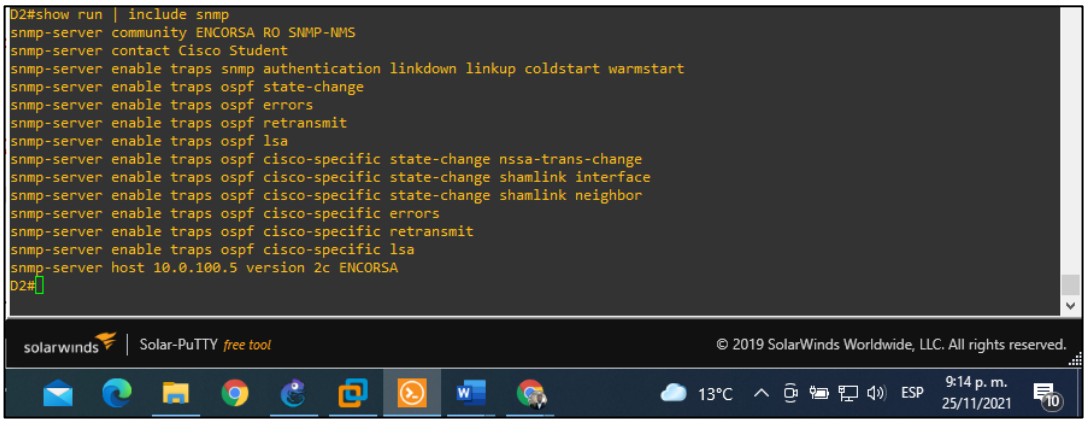
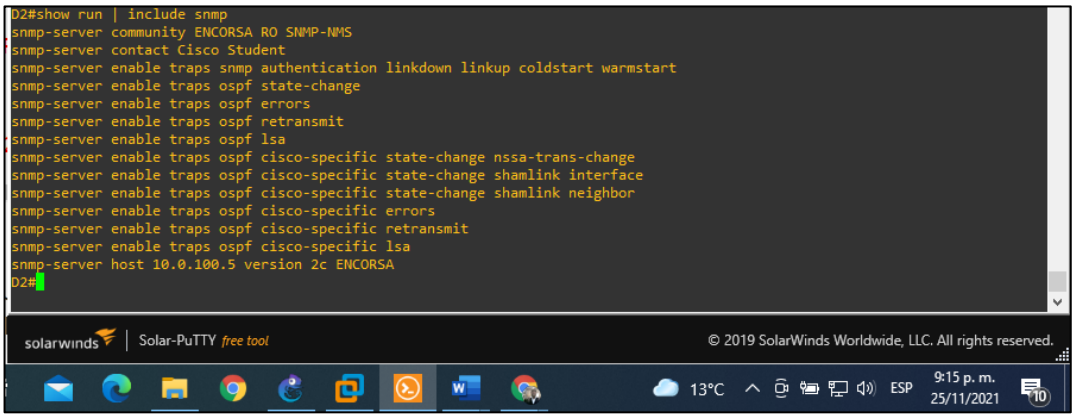


Figura 40 A1# show run | include snmp en A1



De acuerdo con la información devuelta por los comandos de verificación, se evidencia que se cumplieron las tareas Configure Syslog en todos los dispositivos excepto R2. 6.3 y 6.4.

CONCLUSIONES

Los profesionales en redes de TI de las organizaciones desarrollan un papel fundamental, para el mantenimiento de la infraestructura tecnológica de su organización, quizá es un trabajo silencioso pero esencial; El desarrollo de esta práctica de habilidades nos permitió comprender los desafíos que a diario se deben enfrentar n el ámbito laboral, aunque la simulación se llevó a cabo en software de simulación, se utilizaron comandos de configuración e imágenes reales, que permitieron afianzar los conocimientos objetos de este estudio, los cuales no difieren en gran manera de los necesarios para configurar y mantener dispositivos de red reales en operación.

El servidor NTP configurado en la red, es el encargado de mantener sincronizados los equipos de la red a la hora local, y así evitar errores de funcionamiento en los dispositivos.

Cuando se conectan dos Switches de capa 2 de forma redundante, se generan bucles, en esta práctica se implementó el protocolo Spanning-tree, el cual apaga administrativamente una de las interfaces, para evitar el bucle de capa, y fue posible implementar la técnica de agregación de enlaces, para mejorar los anchos de banda de los enlaces participantes.

Es necesario realizar una práctica constante para alcanzar el dominio de este campo, ya que, debido a los constantes cambios en la seguridad informática, cada vez se implementan nuevas configuraciones de seguridad en los dispositivos que se encuentran en producción.

BIBLIOGRAFIA

Escuela de redes. (2019 febrero 18). First Steps with GNS3 - Network School Tutorial. https://www.youtube.com/watch?v=O2WXl1kxwnk

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Pag 97 – 108. https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Pag 193 – 225. https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Techclub.tajamar.es. (18 de 07 de 2016). Configuración de Etherchannel. https://techclub.tajamar.es/configuracion-de-etherchannel/