DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBAS DE HABILIDADES PRÁCTICAS CCNP

CESAR ENRIQUE NOVA ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA-ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2021

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBAS DE HABILIDADES PRÁCTICAS CCNP

CESAR ENRIQUE NOVA ORTIZ

Diplomado de opción de grado presentado para optar el
título de INGENIERO ELECTRÓNICO

DIRECTOR:
MSc: GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA-ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 25 de noviembre del 2021

AGRADECIMIENTOS

Se brinda un agradecimiento general a las directivas del profesorado de la facultad de la escuela de ciencias básicas, tecnología e ingeniería-ECBTI de la UNIVERSIDAD ABIERTA Y A DISTANCIA-UNAD JOSE ACEVEDO YGOMEZ, por todos los servicios prestados y por la enseñanza que me brindaron, al MSc GERARDO GRANADOS ACUÑA por su orientación y apoyo en el desarrollo del presente trabajo.

A los compañeros y amigos que de una u otra forma colaboraron con este proceso, a mi familia por su apoyo incondicional, sus consejos y sabiduría.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

OSPF: protocolo de direccionamiento de tipo enlace, que su funcionalidad en particular va dirigida para las redes IP con base en algoritmos y su función principal es la de hacer un testeo de las rutas en el menor tiempo posible cuando la topología de red cambia.

CISCO: empresa con sede en San José, California (cisco systems) dedicada a la fabricación, mantenimiento y venta de equipos de telecomunicaciones.

CCNP: Cisco certifield Networking Professional, en pocas palabras certificado de networking y telecomunicaciones ofrece un servicio mayor en el ámbito de las telecomunicaciones a diferencia del CCNA que es un básico.

PROTOCOLO: conjunto de reglas y normas que rigen el funcionamiento de comunicación entre 2 o más equipos.

ROUTER: es un equipo denominado por su nombre enrutador que permite la comunicación entre computadoras que funciona dentro de una misma red.

SWITCH: dispositivo que permite la conexión de las computadoras y demás dispositivos que hacen parte de una red.

RESUMEN

En el desarrollo de este trabajo se evidencia las habilidades prácticas en cisco CCNP, donde se colocan a pruebas todo lo aprendido a lo largo de los diferentes cursos realizados en la plataforma cisco CCNA.

Este archivo contiene etapas, en donde inicialmente se desarrolla la topología de y la configuración de cada uno de los dispositivos que hacen parte de esta, en la etapa 2 se configura la red y el soporte de host, etapa 3 Configuración de los protocolos de enrutamiento, etapa 4 Configuración de la redundancia del primer salto, seguridad de dispositivos y la última etapa características de administración de red.

Palabras claves: CISCO, CCNP, CCNA, Topología, Red.

ABSTRACT

In the development of this work, the practical skills in Cisco CCNP are evidenced, where everything learned throughout the different courses taken on the Cisco CCNA platform is put to the test.

This file contains stages, where initially the topology of and the configuration of each of the devices that are part of it is developed, in stage 2 the network and host support are configured, stage 3 Configuration of the routing protocols , Stage 4 Configuring First Hop Redundancy, Device Security, and Last Stage Network Management Features.

Keywords: CISCO, CCNP, CCNA, Topology, Network

INTRODUCCIÓN

Este documento contiene las pruebas de habilidades donde se puede observar la solución de una red, el cual permite fortalecer los conocimientos en redes y telecomunicaciones para ser un profesional en tecnologías de la información, el desarrollo de estas habilidades se ha venido trabajando desde años anteriores con los cursos de CCNA que han sido de mucho apoyo para dar continuación al diplomado en CCNP, en el escenario propuesto para esta etapa se desarrolla la administración de dispositivos de red incluyendo la arquitectura dual-stack.

Este archivo contiene etapas, en donde inicialmente se desarrolla la topología de y la configuración de cada uno de los dispositivos que hacen parte de esta, en la etapa 2 se configura la red y el soporte de host, etapa 3 Configuración de los protocolos de enrutamiento, etapa 4 Configuración de la redundancia del primer salto, seguridad de dispositivos y la última etapa características de administración de red.

El desarrollo de trabajo se realizó en el software packet tracer debido a la facilidad de esta y por otro lado se encuentra bastante información para poder desarrollar las actividades en el software.

DESARROLLO

Escenario 1

Figura 1. Escenario 1

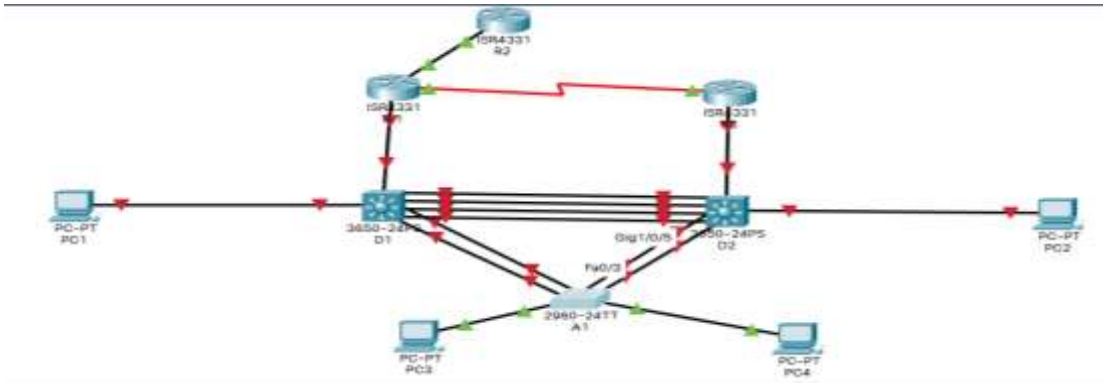


Tabla 1. Tabla de direccionamiento

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
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	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
	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
	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
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Objetivos

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

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

Parte 3: Configurar los protocolos de enrutamiento

Parte 4: Configurar la redundancia del primer salto

Parte 5: Configurar la seguridad

Parte 6: Configurar las características de administración de red

Escenario

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

Nota: Los routers usados son Cisco 4221 con CISCO IOS XE version 16.9.4 (imagen universalk9). Los switches usados son Cisco Ctalyst 3650 con Cisco IOS XE version 16.9.4 (imagen universalk9) y Cisco Catalyst 2960 con Cisco IOS version 15.2(2) (imagen lanbasek9). Se pueden usar otras versiones de switches, routers y Cisco IOS. Dependiendo del modelo y la versión de Cisco IOS, los comandos disponibles y el resultado producido pueden variarde lo que se muestra en las prácticas de laboratorio.

Nota: Si trabaja directamente con equipos remotos, asegúrese que los switches hayan sido borrados y no tenganconfiguraciones de inicio.

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soportaIPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global sdm prefer dual-ipv4-and-ipv6 default. Cambiar la plantilla requerirá el reinicio del switch.

Recursos necesarios

- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
- 4 PCs (utilice el programa de emulación de terminal)
- Los cables de consola para configurar los dispositivos Cisco IOS van a

través de los puertos de consola

- Los cables Ethernet y seriales van como se muestra en la topología

Parte 1: Construir la red y configurar los 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.

Paso 2: Configurar los parámetros básicos para cada dispositivo.

- 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:

R1

R1>enable // ingreso de modo privilegiado
R1#configure terminal// ingreso modo configuración
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1 //se asigna nombre al router..
R1(config)#ipv6 unicast-routing// se habilita la traducción del nombre basado en DNS.
R1(config)#no ip domain lookup
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario # 1// se crea un mensaje aviso.
R1(config)#line con 0 // ingreo al modo de configuración consola 0, en el puerto de consola 0 nunca se agota el tiempo de espera.
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#interface g0/0/0 // se configure la interface g0/0/0 de R1.
R1(config-if)#ip address 209.165.200.225 255.255.255.224// se asigna la dirección ipv4 y la máscara de subred.
R1(config-if)#ipv6 address fe80::1:1 link-local // se asigna la dirección link local a la interface.
R1(config-if)#ipv6 address 2001:db8:200::1/64 // se asigna la dirección ipv6
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface g0/0/1 // se habilita la interface g0/0/1
R1(config-if)#ip address 10.0.10.1 255.255.255.0 // se asigna la dirección ipv4 y la mascara de subred.

R1(config-if)#ipv6 address fe80::1:2 link-local // se asigna la dirección link local.
R1(config-if)#ipv6 address 2001:db8:100:1010::1/64 // se asigna la dirección ipv6
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/1/0 // se configure la interface.
R1(config-if)#ip address 10.0.13.1 255.255.255.0 // se asigna la dirección ipv4 y la mascara de subred.
R1(config-if)#ipv6 address fe80::1:3 link-local // se asigna la dirección link local.
R1(config-if)#ipv6 address 2001:db8:100:1013::1/64 // se asigna la dirección ipv6.
R1(config-if)#no shutdown
R1(config-if)#exit

R2

R2>enable // ingreso al modo privilegiado.
R2#configure terminal // ingreso al modo configuración global.
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2 // asigno nombre al router.
R2(config)#ipv6 unicast-routing // habilito router como router ipv6
R2(config)#no ip domain lookup // habilito la traducción de nombre basado en DNS del host.
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 # //
R2(config)#line con 0 // ingreso al modo de configuración de línea consola 0.
R2(config-line)#exec-timeout 0 0 // el Puerto de la consola 0 nunca se agotara el tiempo de espera.
R2(config-line)#logging synchronous // evita que aparezcan mensajes inesperados en la pnatalla y que desplacen los comandos que estamos digitando.
R2(config-line)#exit
R2(config)#interface g0/0/0 // se configure la interface g0/0/0
R2(config-if)#ip address 209.165.200.226 255.255.255.224 // asigno la dirección ipv4 y la mascara de subred.
R2(config-if)#ipv6 address fe80::2:1 link-local // asigno la dirección link local a la interface.
R2(config-if)#ipv6 address 2001:db8:200::2/64 // asigno la dirección ipv6.
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Loopback 0 // configuro la interface loopback.
R2(config-if)#ip address 2.2.2.2 255.255.255.255 // asigno la dirección ipv4 y la máscara de subred.
R2(config-if)#ipv6 address fe80::2:3 link-local //asigno la dirección link local.
R2(config-if)#ipv6 address 2001:db8:2222::1/128 // asigno la direcció ipv6.
R2(config-if)#no shutdown
R2(config-if)#exit

R3

R3#enable // ingreso al modo privilegiado
R3#configure terminal // ingreso al modo de configuración global.
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#hostname R3 // asigno nombre al router
R3(config)#ipv6 unicast-routing // habilito como router ipv6
R3(config)#ip domain lookup // habilito la traducción de nombre a dirección basado en DNS del host.
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 # //creo un mensaje de aviso.
R3(config)#line con 0 // ingreso al modo de configuración de línea de la consola 0.
R3(config-line)#exec-timeout 0 0 // en el Puerto de la consola 0 nuca se agotara el tiempo de espera.
R3(config-line)#logging synchronous // evita que los mensajes inesperados que aparecen en la pantalla desplacen los commandos que estamos digitando.
R3(config-line)#exit
R3(config)#interface g0/0/1 // configure la interface.
R3(config-if)#ip address 10.0.11.1 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
R3(config-if)#ipv6 address fe80::3:2 link-local // asigni la dirección link local a la interface.
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64 // asigno la dirección ipv6.
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/1/0 //configuro interface
R3(config-if)#ip address 10.0.13.3 255.255.255.0 // asigni la dirección ipv4 y la mascara de subred.
R3(config-if)#ipv6 address fe80::3:3 link-local // asigno la dirección link local a la interface.
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64 // asigno la dirección ipv6
R3(config-if)#no shutdown
R3(config-if)#exit

D1

D1>enable // ingreso al modo privilegiado
D1#configure terminal // ingreso al modo de configuración global.
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#hostname D1 //asigno nombre al Switch
D1(config)#ip routing // habilito el routing ipv4
D1(config)#ipv6 unicast-routing // habilito el routing ipv6

D1(config)#no ip domain lookup // habilito la traducción del nombre a dirección basado en DNS del host
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 # // creo un mensaje de aviso.
D1(config)#line con 0 // ingreso al modo de configuración consola 0.
D1(config-line)#exec-timeout 0 0 // en el tiempo de la consola 0 nunca se agotara el tiempo de espera.
D1(config-line)#logging synchronous // evita que los mensajes inesperados que aparecen en pantalla desplacen a los comandos que estamos digitando.
D1(config-line)#exit
D1(config)#vlan 100 // se configure la vlan 100 en D1, se le asigna nombre.
D1(config-vlan)#name Management
D1(config-vlan)#exit
D1(config)#vlan 101 // se configure la vlan 101 en D1, se le asigna nombre.
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit
D1(config)#vlan 102 // se configure la vlan 102 en D1, se le asigna nombre.
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit
D1(config)#vlan 99
D1(config-vlan)#name NATIVE
VLAN #999 and #99 have an identical name: NATIVE
D1(config-vlan)#vlan 999 // se configure la vlan 999
D1(config-vlan)#name NATIVE // asigno nombre como la vlan native.
D1(config-vlan)#exit
D1(config)#interface g1/0/11 // configuro la interface
D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#no switchport // asigno a la interface capacidad de capa 3.
D1(config-if)#ip address 10.0.10.2 255.255.255.0 // asigno la dirección ipv4 y la máscara de subred.
D1(config-if)#ipv6 address fe80::d1:1 link-local // asigno la direccion de link local a la interface.
D1(config-if)#ipv6 address 2001:db8:100:100:1010::2/64 // asigno la dirección ipv6
%GigabitEthernet1/0/11: Error: 2001:DB8:100:100::/64 is overlapping with 2001:DB8:100:100::/64 on Vlan100
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown // habilito la interface.
D1(config-if)#exit
D1(config)#interface vlan 100 // configure la interface vlan 100 de D1.
D1(config-if)#ip address 10.0.100.1 255.255.255.0 // asigno dirección ipv4 y la mascara de subred.
D1(config-if)#ipv6 address fe80::d1:2 link-local // asigno dirección link local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64 // asigno dirección ipv6
D1(config-if)#no shutdown // habilito la interface vlan 100.
D1(config-if)#exit

D1(config)#interface vlan 101 // configure la interface vlan 101 de D1.
D1(config-if)#ip address 10.0.101.1 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
D1(config-if)#ipv6 address fe80::d1:3 link-local // asigno la dirección link local.
D1(config-if)#ipv6 address 2001:db8:100:101::1/64 // asigno la dirección ipv6
D1(config-if)#no shutdown // habilito la vlan 101.
D1(config-if)#exit
D1(config)#interface vlan 102 // configure la interface vlan 102 de D1.
D1(config-if)#ip address 10.0.102.1 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
D1(config-if)#ipv6 address fe80::d1:4 link-local // asigno la dirección link local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64 // asigno la dirección ipv6
D1(config-if)#no shutdown // habilito la interface vlan 102.
D1(config-if)#exit
D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109 // excluyo el rango de direcciones ipv4 especificadas
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254 // excluyo el rango de direcciones ipv4 especificadas
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109 // excluyo el rango de direcciones ipv4 especificadas
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254 // excluyo el rango de direcciones ipv4 especificadas
D1(config)#ip dhcp pool VLAN-101 // configure un servidor dhcp en la vlan 101
D1(dhcp-config)#network 10.0.101.0 255.255.255.0 // asigno la dirección de red con la máscara de subred.
D1(dhcp-config)#default-router 10.0.101.254 // asigno la puerta de enlace predeterminada.
D1(dhcp-config)#exit
D1(config)#ip dhcp pool VLAN-102 // // configure un servidor dhcp en la vlan 101
D1(dhcp-config)#network 10.0.102.0 255.255.255.0 // asigno la dirección de red con la máscara de subred.
D1(dhcp-config)#default-router 10.0.102.254 // asigno la puerta de enlace predeterminada.
D1(dhcp-config)#exit
D1(config)#interface range g1/0/1-24 // no deshabilite interfaces debido a que todas fueron utilizadas.
D1(config-if-range)#shutdown

D2

D2>enable // ingreso al modo privilegiado
D2#configure terminal //ingreso al modo de configuración global.

Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#hostname D2 // asigno nombre al switch
D2(config)#ip routing // habilito el routing ipv4
D2(config)#ipv6 unicast-routing // habilito el routing ipv6
D2(config)#no ip domain lookup // habilito la traducción de nombre a dirección basado en DNS del host.
D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 # // creo un mensaje de aviso.
D2(config)#line con 0 // ingreso al modo de configuración de línea de la consola 0.
D2(config-line)#exec-timeout 0 0 // puerto de consola 0 nunca se agotará el tiempo de espera.
D2(config-line)#logging synchronous // eita esos mensajes en pantalla que puedan desplazar los comandos al momento de digitarlos.
D2(config-line)#exit
D2(config)#vlan 100 // configuro la interface vlan 100 de D1.
D2(config-vlan)#name Management // asigno nombre
D2(config-vlan)#exit
D2(config)#vlan 101 // configuro la interface vlan 101 de D1
D2(config-vlan)#name UserGroupA // asigno nombre
D2(config-vlan)#exit
D2(config)#vlan 102 // configuro la interface vlan 102 de D1
D2(config-vlan)#name UserGroupB // asigno nombre
D2(config-vlan)#exit
D2(config)#vlan 999 // configure la vlan 999 en D2.
D2(config-vlan)#name NATIVE // asigno nombre como vlan native.
D2(config-vlan)#exit
D2(config)#interface g1/0/11 // configuro interface
D2(config-if)#no switchport // asigno a la interface capacidad de capa 3
D2(config-if)#ip address 10.0.11.2 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
D2(config-if)#ipv6 address fe80::d1:1 link-local // asigno la dirección link local a la interface.
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64 // asigno la dirección ipv6
D2(config-if)#no shutdown // habilito la interface
D2(config-if)#exit
D2(config)#interface vlan 100 // configure la interface vlan 100 de D2.
D2(config-if)#ip address 10.0.100.2 255.255.255.0 // asigno la la dirección ipv4 y la mascara de subred.
D2(config-if)#ipv6 address fe80::d2:2 link-local // asigno la dirección link local.
D2(config-if)#ipv6 address 2001:db8:100:100::2/64 // asigno la dirección ipv6
D2(config-if)#no shutdown // habilito la interface vlan 100
D2(config-if)#exit
D2(config)#interface vlan 101 // configure la interface vlan 101
D2(config-if)#ip address 10.0.102.2 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.

% 10.0.102.0 overlaps with Vlan102
D2(config-if)#ip address 10.0.101.2 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
D2(config-if)#ipv6 address fe80::d2:3 link-local // asigno la dirección link local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64 // asigno la dirección ipv6
D2(config-if)#no shutdown // habilito la interface vlan 101
D2(config-if)#exit
D2(config)#interface vlan 102 // configure la interface vlan 102 D2.
D2(config-if)#ip address 10.0.102.2 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
D2(config-if)#ipv6 address fe80::d2:4 link-local // asigno la dirección link local.
D2(config-if)#ipv6 address 2001:db8:100:102::2/64 // asigno la dirección ipv6
D2(config-if)#no shutdown // habilito la interface vlan 102
D2(config-if)#exit
D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209 // excluyo el rango de direcciones ipv4 especificadas
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254 // excluyo el rango de direcciones ipv4 especificadas
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209 // excluyo el rango de direcciones ipv4 especificadas
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254 // excluyo el rango de direcciones ipv4 especificadas
D2(config)#ip dhcp pool VLAN-101 // configure un servidor dhcp en la vlan 101.
D2(dhcp-config)#network 10.0.101.0 255.255.255.0 // asigno dirección de red con la máscara de subred.
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#ip dhcp pool VLAN-102 // configuro un servidor de red en la vlan 102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0 // asigno la dirección de red con la máscara de subred.
D2(dhcp-config)#default-router 10.0.102.254 // asigno puerta de enlace predeterminada.
D2(dhcp-config)#exit
D2(config)#interface range g1/0/1-23 // no deshabilite interfaces en D2 por que se utilizaron todas.
D2(config-if-range)#shutdown

A1

Switch>enable // ingreso al modo privilegiado
Switch#configure terminal // ingreso al modo de configuración global.
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname A1 // asigno nombre al switch
A1(config)#no ip domain lookup // habilito la traducción de nombre a dirección basado en DNS del host.
A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 # // creo un mensaje de aviso.
A1(config)#line con 0 // ingreso al modo de configuración consola de línea de consola 0
A1(config-line)#exec-timeout 0 0 // el Puerto de consola 0 nunca se agota el tiempo de espera.
A1(config-line)#logging synchronous // evita los mensajes inesperarados que puedan afectar la digitación de los comandos.
A1(config-line)#exit
A1(config)#vlan 100 // configuro la vlan 100 en A1.
A1(config-vlan)#name Management // asigno nombre.
A1(config-vlan)#exit
A1(config)#vlan 101 // configuro la vlan 101
A1(config-vlan)#name UserGroupA // asigno nombre
A1(config-vlan)#exit
A1(config)#vlan 102 // configure la vlan 102
A1(config-vlan)#name UserGroupB // asigno nombre
A1(config-vlan)#exit
A1(config)#vlan 999 // configure la vlan 999 en A1
A1(config-vlan)#name NATIVE // asigno nombre como vlan native.
A1(config-vlan)#exit
A1(config)#interface vlan 100 // configure interface vlan 100 de A1.
A1(config-if)#
A1(config-if)#ip address 10.0.100.3 255.255.255.0 // asigno la dirección ipv4 y la mascara de subred.
A1(config-if)#ipv6 address fe80::a1:1 link-local // asigno la dirección link local
A1(config-if)#ipv6 address 2001:db8:100:100::3/64 // asigno la direccion ipv6
A1(config-if)#no shutdown // habilito la interface vlan 100
A1(config-if)#exit
A1(config)#interface range f0/5-22 // habilito las interfaces en los rangos especificados.
A1(config-if-range)#shutdown
A1(config-if-range)#exit

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

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.

Las tareas de configuración son las siguientes:

Tabla 2. Configurar la capa 2 de la red y el soporte de Host

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.

Tarea	Tarea	Especificación

#		
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

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

Se habilitaron enlaces trunk 802.1Q de los switches entre D1 y D2, D1 y A1 y por ultimo D2 y A1.

D1

D1(config-if-range)#exit
D1(config)#interface range g1/0/1-4 // selecciono el rango de interfaces.
D1(config-if-range)# switchport mode trunk // configure como interfaces troncales.

D2

D2(config-if-range)# exit
D2(config)#interface range g1/0/1-4 // selecciono el rango de interfaces
D2(config-if-range)# switchport mode trunk // configuro como interfaces troncales.

A1

A1(config)#spanning-tree mode rapid-pvst
A1(config)#interface range f0/1-2 // selecciono rango de interfaces
A1(config-if-range)# switchport mode trunk

2.2 En todos los switches cambie la VLAN nativaen los enlaces troncales.
Se utilizo la vlan 999 como la vlan nativa.

D1

D1(config-if-range)# switchport trunk native vlan 999 // asigno la vlan 999 como nativa.
D1(config-if-range)# channel-group 12 mode active
D1(config-if-range)# no shutdown
D1(config-if-range)# no shutdown // active las interfaces.
D1(config-if-range)#exit

D2

D2(config-if-range)# switchport trunk native vlan 999 // asigno la vlan 999 como nativa.
D2(config-if-range)# channel-group 12 mode active // active el protocolo LACP de forma incondicional.
D2(config-if-range)# no shutdown

D2(config-if-range)# no shutdown // activo las interfaces
D2(config-if-range)#exit

A1

A1(config-if-range)# switchport trunk native vlan 999 // asigno la vlan 999 como native.
A1(config-if-range)# channel-group 1 mode active // active el protocol LACP de forma incondicional.
A1(config-if-range)# no shutdown
A1(config-if-range)# no shutdown // activo las interfaces.
A1(config-if-range)#exit

2.3 En todos los switches habilite el protocoloRapid Spanning-Tree (RSTP)
Se utilizo Rapid Spanning-Tree (RSTP) donde se configuro en modo acceso

D1

D1(config)#spanning-tree mode rapid-pvst // active el protocolo RSPT.
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary
D1(config)#interface g1/0/23
D1(config-if)#switchport mode access // indico que voy a configurar en modo acceso.
D1(config-if)# switchport access vlan 100
D1(config-if)# spanning-tree portfast
D1(config-if)#exit
D1(config)#end

D2

D2(config)#interface range g1/0/5-6 //configure interface
D2(config-if-range)# switchport mode trunk // coloco en modo troncal.
D2(config-if-range)# no shutdown // activo las interfaces.
D2(config-if-range)#exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#interface g1/0/23
D2(config-if)# switchport mode access // indico que voy a configurar el modo acceso

D2(config-if)# switchport access vlan 102 // asigno la vlan 102
D2(config-if)# spanning-tree portfast
D2(config-if)#exit
D2(config)#end

A1

A1(config)#interface range f0/3-4 // configure la interface.
A1(config-if-range)# switchport mode trunk // coloco en modo troncal.

A1(config-if-range)# switchport trunk native vlan 999
A1(config-if-range)# channel-group 2 mode active // active el protocolo LACP de forma incondicional.
A1(config-if-range)# no shutdown
A1(config-if-range)# no shutdown
A1(config-if-range)#exit
A1(config)#interface f0/23 // configuro la interface
A1(config-if)# switchport mode access // indico que voy a configurar el modo acceso.
A1(config-if)# switchport access vlan 101 // asigno la vlan 101
A1(config-if)# spanning-tree portfast //
A1(config-if)# no shutdown // active la interface
A1(config-if)#exit
A1(config)#interface f0/24
A1(config-if)# switchport mode access // indico que voy a configurar el modo acceso.
A1(config-if)# switchport access vlan 100 // asigno la vlan 100
A1(config-if)# spanning-tree portfast
A1(config-if)#exit
A1(config)#end

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 casode falla del puente raíz (root bridge). Se configuro D1 y D2 como la raíz (root) con las vlan apropiadas.

D1
D1(config)#spanning-tree vlan 100,102 root primary
D1(config)#spanning-tree vlan 101 root secondary

D1(config)#interface g1/0/23
D1(config-if)#switchport mode access // indico que voy a configurar en modo acceso.
D1(config-if)# switchport access vlan 100

D2

D2(config-if-range)#exit
D2(config)#spanning-tree mode rapid-pvst
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 100,102 root secondary
D2(config)#interface g1/0/23
D2(config-if)# switchport mode access // indico que voy a configurar el modo acceso
D2(config-if)# switchport access vlan 102 // asigno la vlan 102

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.
Usar los siguiente números:
D1 a D2 – Port channel 12
D1 a A1 – Port channel 1
D2 a A1 – Port channel 2
active el protocolo LACP de forma incondicional.

D1

D1(config-if-range)# channel-group 12 mode active

D2

D2(config-if-range)# channel-group 12 mode active

A1

A1(config-if-range)# channel-group 2 mode active

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.
Se configuraron los puertos de acceso con cada vlan asignada a los switches.

D1

D1(config-if)# switchport access vlan 100

D2

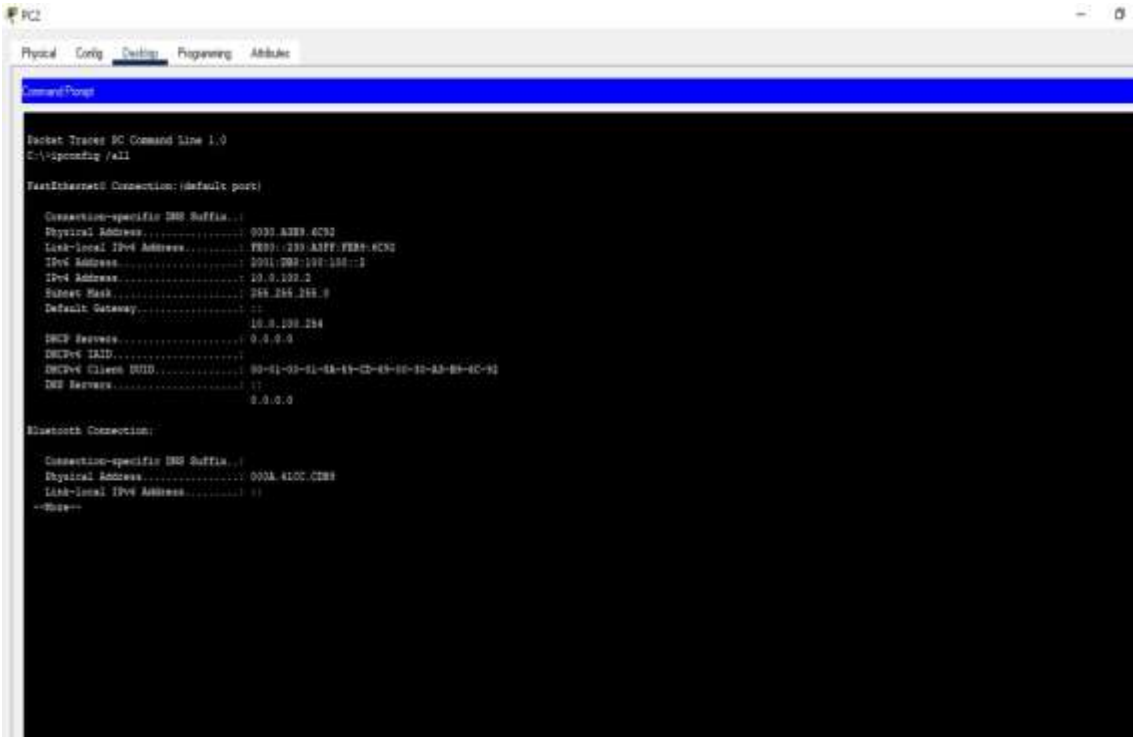
D2(config-if)# switchport access vlan 102

A1

A1(config-if)# switchport access vlan 101

2.7 Verifique los servicios DHCP IPv4.

Figura 2. Verificación de servicios DHCP IPv4



2.8 Verifique la conectividad de la LAN local

Figura 3. Ping PC1 a D1, D2 y PC4

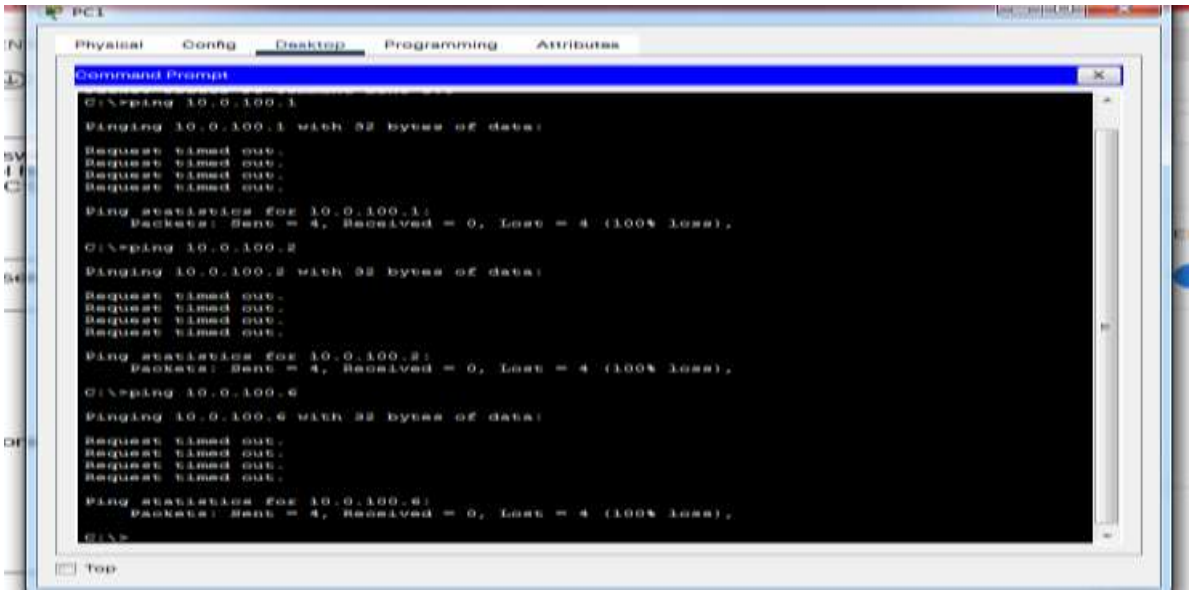
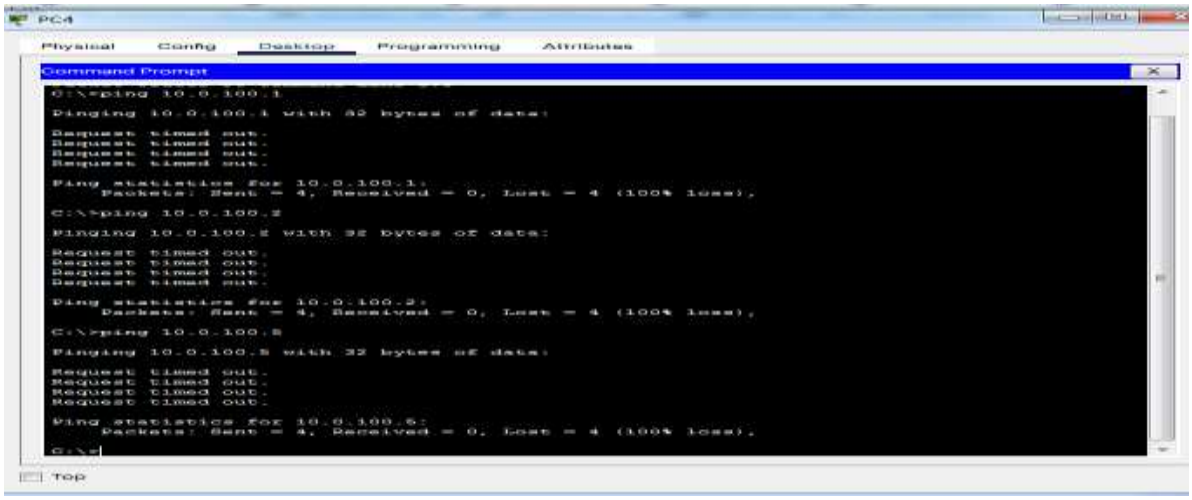


Figura 4 ping de PC4 a D1, D2 y PC1



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.

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

Las tareas de configuración son las siguientes:

Tabla 3. Configurar los protocolos de enrutamiento

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

Tarea	Tarea	Especificación
3.3	En R2 en la “Red ISP”, configure MP-BGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).

3.4	En R1 en la “Red ISP”, configure MP-BGP.	Configure dos rutas resumen estáticas a la interfaz Null 0: • Una ruta resumen IPv4 para 10.0.0.0/8. • Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1. Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500. En IPv4 address family: • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.0.0.0/8. En IPv6 address family: • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48.

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

R1

R1(config)#
R1(config)#router ospf 4 // asigno la ospf indicando el proceso
R1(config-router)#router-id 0.0.4.1 // asigno al router id a R1.
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 // asigno area 0 a la interface
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0 // asigno area 0 a la interface
R1(config-router)#default-information originate // declaro informacion predeterminada.

R3

R3(config)#router ospf 4 // ingreso al ospf indicando el id del proceso 4
R3(config-router)# router-id 0.0.4.3 // asigno el router id a R3.
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0 // asigno area 0 a la interface
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0 // asigno area 0 a la interface.
R3(config-router)#exit

D1

D1(config)#router ospf 4 // ingreso al ospf indicando el id del proceso.
D1(config-router)#router-id 0.0.4.131 // asigno el router id a D1.
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0 // asigno area 0 a la interface
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0 // asigno area 0 a la interface
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0 // asigno area 0 a la interface
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0 // asigno area 0 a la interface.
D1(config-router)#passive-interface default // coloco las interfaces de D1 en estado pasivo para ospf
D1(config-router)#no passive-interface g1/0/11// solo habilito esta interface.
D1(config-router)#exit

D2

D2(config)#router ospf 4 // ingreso configure ospf indicando el id del proceso 4
D2(config-router)#router-id 0.0.4.132 // asigno el router id a D2
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0 // asigno area 0 a la interface
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0 // asigno area 0 a la interface
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0 // asigno area 0 a la interface
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0 // asigno area 0 a la interface
D2(config-router)#passive-interface default // coloco las interfces D2 en estado pasivo para ospf
D2(config-router)# no passive-interface g1/0/11 // habilito interface para anunciar ospf
D2(config-router)#exit

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

Use OSPF Process ID **6** y asigne los siguientes router-IDs:

- R1: 0.0.6.1
- R3: 0.0.6.3
- D1: 0.0.6.131
- D2: 0.0.6.132

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en área 0.

- En R1, no publique la red R1 – R2.
- On R1, propague una ruta por defecto. Note que laruta 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

R1

R1(config)#ipv6 router ospf 6 // asigno la ospf indicando el proceso.
R1(config-rtr)#router-id 0.0.6.1// asigno al router id a R1.
R1(config-rtr)#default-information originate // declare información predeterminada.
R1(config-rtr)#exit
R1(config)#interface g0/0/1 // accedo a la interface
R1(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface en el area 0.
R1(config-if)#exit
R1(config)#interface s0/1/0 // accedo a la interface
R1(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface en el area 0
R1(config-if)#exit

R3

R3(config)#router ospf 4 // ingreso al ospf indicando el id del proceso 4
R3(config-router)# router-id 0.0.4.3 // asigno el router id a R3.
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0 // asigno area 0 a la interface
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0 // asigno area 0 a la interface.
R3(config-router)#exit
R3(config)#ipv6 router ospf 6 // ingreso al ospfv3 indicando el id del proceso 6
R3(config-rtr)#router-id 0.0.6.3 // asigno el router id a R3.
R3(config-rtr)#exit
R3(config)#interface g0/0/1 // accedo a la interface
R3(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface
R3(config-if)#exit

D1

D1(config)#ipv6 router ospf 6 // igreso y configuro ospfv3 indicando el id del proceso 6
D1(config-rtr)#router-id 0.0.6.131 // asigno el router id a D1.
D1(config-rtr)#passive-interface default // coloco las intefaces en estado pasivo

D1(config-rtr)#no passive-interface g1/0/11 // habilito la interface para anunciar ospfv3.
^
% Invalid input detected at '^' marker.
D1(config-rtr)#exit
D1(config)#interface g1/0/11 // accedo a la interface
D1(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para interface en el area 0
D1(config-if)#exit
D1(config)#interface vlan 100 // accedo a la interface vlan 100
D1(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface
D1(config-if)#exit
D1(config)#interface vlan 101 // accedo a la interface vlan 101
D1(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6para la interface
D1(config-if)#exit
D1(config)#interface vlan 102 // accedo a la interface vlan 102
D1(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface.
D1(config-if)#exit
D1(config)#end

D2

D2(config)#ipv6 router ospf 6 // habilito ospfv6 para la interface
D2(config-rtr)#router-id 0.0.6.132 // asigno el router id a D2.
D2(config-rtr)#passive-interface default // coloco las interfcaces en estado pasivo ospf
D2(config-rtr)#no passive-interface g1/0/11//no lo soporta parkertracer // habilito interface para anunciar ospfv3.
D2(config-rtr)#exit
D2(config)#interface g1/0/11 // accedo a la interface
D2(config-if)# ipv6 ospf 6 area 0 //habilito ospfv6 para la interface
D2(config-if)#exit
D2(config)#interface vlan 100 // accedo a la interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface.
D2(config-if)#exit
D2(config)#interface vlan 101 // accedo a la interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface
D2(config-if)#exit
D2(config)#interface vlan 102 // accedo a la vlan 102
D2(config-if)#ipv6 ospf 6 area 0 // habilito ospfv6 para la interface
D2(config-if)#exit
D2(config)#end

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

Configure dos rutas estáticas predeterminadas através de la interfaz Loopback 0:

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

R2

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 // configure la ruta estativa ipv4
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0 // configure la ruta estatica ipv6

Configure R2 en BGP ASN 500 y use el router-id2.2.2.2.

Configure y habilite una relación de vecino IPv4 e IPv6con 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).
Router 2

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 // configure la ruta estativa ipv4
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 loopback 0 // configure la ruta estatica ipv6
R2(config)#router bgp 500 // define el proceso BGP en R2 y el numero ASN al que pertenece.
R2(config-router)#bgp router-id 2.2.2.2 // asigno el id del protocol BGP.
R2(config-router)#neighbor 209.165.200.225 remote-as 300 // configure la relación vecino ipv4 e ipv6 con R1
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 209.165.200.225 Up

R2(config-router)#neighbor 2001:db8:200::1 remote-as 300// no lo soporta parkertracer
R2(config-router)#address-family ipv4// no lo soporta packet tracer // accedo a las direcciones ipv4
R2(config-router)#neighbor 209.165.200.225 activate// no lo soporta packet tracer
R2(config-router)#no neighbor 2001:db8:200::1 activate// no lo soporta packet tracer
R2(config-router)#network 2.2.2.2 mask 255.255.255.255 // anucio la red loopback ipv4

R2(config-router)#network 0.0.0.0 // anuncio la ruta por defecto.
R2(config-router)#exit-address-family// no lo soporta packet tracer // salgo de la configuración ipv4
R2(config-router)#address-family ipv6// no lo soporta packet tracer // accedo a las direcciones ipv6
R2(config-router)#no neighbor 209.165.200.225 activate// no lo soporta packet tracer
R2(config-router)#neighbor 2001:db8:200::1 activate// no lo soporta packet tracer
R2(config-router)#network 2001:db8:2222::/128// no lo soporta packet tracer // anuncio la red loopback 0
R2(config-router)#network ::/0// no lo soporta packet tracer // anuncio la ruta por defecto.
R2(config-router)#exit-address-family // salgo de la configuración ipv6

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

Configure dos rutas resumen estáticas a la interfaz Null 0:

- Una ruta resumen IPv4 para 10.0.0.0/8.
- Una ruta resumen IPv6 para 2001:db8:100::/48. Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.

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

En IPv4 address family:

- Deshabilite la relación de vecino IPv6.
- Habilite la relación de vecino IPv4.
- Anuncie la red 10.0.0.0/8. En IPv6 address family:
- Deshabilite la relación de vecino IPv4.
- Habilite la relación de vecino IPv6.

Anuncie la red 2001:db8:100::/48.

Para este subpunto la moyoria de comandos no se pueden ejecutar en el software packet tracer y no fue posible evidenciar su funcionamiento.

R1

R1(config)#ip route 10.0.0.0 255.0.0.0 null0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route 2001:db8:100::/48 null0
^
% Invalid input detected at '^' marker.
R1(config)#router bgp 300
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor 209.165.200.226 remote-as 500
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500 //comando no soportado por packet tracer

R1(config-router)#address-family ipv4 unicast //comando no soportado por packet tracer
R1(config-router)#neighbor 209.165.200.226 activate //comando no soportado por packet tracer
R1(config-router)#no neighbor 2001:db8:200::2 activate//comando no soportado por packet tracer
R1(config-router)#network 10.0.0.0 mask 255.0.0.0
R1(config-router)#exit-address-family//comando no soportado por packet tracer
R1(config-router)#address-family ipv6 unicast//comando no soportado por packet tracer
R1(config-router)#no neighbor 209.165.200.226 activate//comando no soportado por packet tracer
R1(config-router)#neighbor 2001:db8:200::2 activate//comando no soportado por packet tracer
R1(config-router)#network 2001:db8:100::/48//comando no soportado por packet tracer
R1(config-router)#exit-address-family//comando no soportado por packet tracer
R1(config-router)#

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 host en la “Red dela compañía”.

Las tareas de configuración son las siguientes:

Tabla 4. Configurar la redundancia del primer salto

Tarea	Tarea	Especificación

4.1	En D1, cree IP SLAs que prueben la accesibilidad dela 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 R1G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sintiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 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 estadode 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 dela 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 R3G0/0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sintiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 6. • Use el número de rastreo **4** para la IP SLA4. • Use el número de rastreo **6** para la SLA 6. Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos.

Tarea	Tarea	Especificación

4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lotanto, 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.

4.1 En D1, cree IP SLAs que prueben la accesibilidad dela 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 R1G0/0/1 cada 5 segundos.

Programe la SLA para una implementación inmediata sintiempo de finalización.

Cree una IP SLA objeto para la IP SLA 4 y una para la IPSLA 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 estadode IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Para este caso gran parte de los comando no fue posible la ejecución per en un ambiente ideal inicialmente se ingresa al modo privilegiado y luego a la configuración global para llevar a cabo el desarrollo.

D1

D1>enable // ingreso al modo privilegiado
D1#configure terminal // ingreso al modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ip sla 4// no soportado por packet tracer // defino el número de sesión 4 de la SLA
D1(config-ip-sla)# icmp-echo 10.0.10.1// no soportado por packet tracer // inicio la configuración IP SLA ICMP ECHO con destino ipv4

D1(config-ip-sla-echo)# frequency 5// no soportado por packet tracer // pruebo la disponibilidad de la interface cada 5 segundos.
D1(config-ip-sla-echo)#exit
D1(config)#ip sla 6// no soportado por packet tracer // defino el número de sesión 6 del SLA
D1(config)# icmp-echo 2001:db8:100:1010::1// no soportado por packet tracer // inicio la configuración IP SLA ICMP ECHO con destino ipv6
D1(config)# frequency 5// no soportado por packet tracer // pruebo la disponibilidad de la interface cada 5 segundos.
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now// no soportado por parkertracer // programo el SLA 4 para iniciar inmediatamente sin tiempo de finalización
D1(config)#ip sla schedule 6 life-forever start-time now// no soportado por parkertracer// programo el SLA 6 para iniciar inmediatamente sin tiempo de finalización
D1(config)#track 4 ip sla 4// no soportado por packet tracer // creo el número de rastreo 4 y lo asocio al IP SLA 4.
D1(config-track)# delay down 10 up 15// no soportado por packet tracer //
D1(config-track)#exit
D1(config)#track 6 ip sla 6// no soportado por packet tracer
D1(config-track)# delay down 10 up 15// no soportado por packet tracer// notifica cada 10 segundos el cambio de estadp de la IP SLA.
D1(config-track)#exit
D1(config)#interface vlan 100 // accedo a la interface vlan 100
D1(config-if)# standby version 2 // configuro el HSRP para usar la version 2
D1(config-if)# standby 104 ip 10.0.100.254 // inicio la configuración ipv4 HSRP grupo 104 para la vlan 100, asignando la ip virtual
D1(config-if)# standby 104 priority 150 // establezco la prioridad del grupo 104 en 150
D1(config-if)# standby 104 preempt // habilito la preferencia del grupo 104.
D1(config-if)# standby 104 track 4 decrement 60// no soportado por packet tracer // rastreo el objeto 4 y se decrement en 60.
D1(config-if)# standby 106 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 106 para la vlan 100, asigno la dirección ip virtual.
D1(config-if)# standby 106 priority 150 // establezco la prioridad del grupo en 150.
D1(config-if)# standby 106 preempt // habilito la preferencia al grupo 106.
D1(config-if)# standby 106 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60
D1(config-if)# standby 106 track 6 decrement 60// no soportado por packet tracer
D1(config-if)#exit
D1(config)#interface vlan 101 // accedo a la interface vlan 101
D1(config-if)# standby version 2 // configure el HSRP para usar la versión 2.
D1(config-if)# standby 114 ip 10.0.101.254 // inicio la configuración ipv4 HSRP grupo 114 para la vlan 101, asignando la ip virtual.

D1(config-if)# standby 114 preempt // habilito la preferencia al grupo 114
D1(config-if)# standby 114 track 4 decrement 60// no soportado por packet tracer // rastreo el objeto 4 y se decrement en 60
D1(config-if)# standby 116 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 116 para la vlan 101, asignando la dirección ip virtual usando ipv6 autoconfig.
D1(config-if)# standby 116 preempt // habilito la preferencia al grupo 116
D1(config-if)# standby 116 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60.
D1(config-if)# standby 116 track 6 decrement 60// no soportado por packet tracer
D1(config-if)#exit
D1(config)#interface vlan 102 // accedo a la interface vlan 102
D1(config-if)# standby version 2// configure el HSRP para usar la versión 2.
D1(config-if)# standby 124 ip 10.0.102.254 // inicio la configuración ipv4 HSRP grupo 124 para la vlan 102, asignando la ip virtual.
D1(config-if)# standby 124 priority 150 // establezco la prioridad del grupo 124.
D1(config-if)# standby 124 preempt // hhabilito la preferencia al grupo 124.
D1(config-if)# standby 124 track 4 decrement 60// no soportado por packet tracer // rastreo el objeto 4 y se decrement en 60.
D1(config-if)# standby 126 ipv6 autoconfig // configure ipv6 HSRP grupo 126 para la vlan 102, asignando la dirección ip virtual usando ipv6 autoconfig.
D1(config-if)# standby 126 priority 150 // establezco la prioridd al grupo 150.
D1(config-if)# standby 126 preempt // habilito la preferencia al grupo 126
D1(config-if)# standby 126 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60.
D1(config-if)# standby 126 track 6 decrement 60// no soportado por packet tracer // se rastrea el objeto 6 y se decrement en 60.
D1(config-if)#exit

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

Programe la SLA para una implementación inmediata sintiempo de finalización.

Cree una IP SLA objeto para la IP SLA 4 and one for IPSLA 6.

- Use el número de rastreo 4 para la IP SLA4.
- Use el número de rastreo 6 para la SLA 6.

Los objetos rastreados deben notificar a D1 si el estadode IP SLA cambia de Down a Up después de 10 segundos.
Para este caso gran parte de los comando no fue posible la ejecución per en un ambiente ideal inicialmente se ingresa al modo privilegiado y luego a la configuración global para llevar a cabo el desarrollo.

D2

D2#enable // ingreso al modo privilegiado
D2#configure terminal // ingreso al modo de configuración global.
D2(config)#ip sla 4// no lo soporta packet tracer
D2(config-ip-sla)#icmp-echo 10.0.11.1// no lo soporta packet tracer // inicio la configuración IP SLA ICMP ECHO con destino a la iterface ipv6.
D2(config-ip-sla-echo)# frequency// no lo soporta packet tracer // pruebo la disponibilidad de la interface.
D2(config)#exit
D2(config)#ip sla 6// no lo soporta packet tracer // programo el SLA 6 para una implementación inmediata sin tiempo de finalización
D2(config)# icmp-echo 2001:db8:100:1011::1// no lo soporta packt tracer //
D2(config)# frequency// no lo soporta packet tracer
D2(config)#exit
D2(config)#ip sla schedule 4 life forever start-time now// no lo soporta packet tracer // programo el SLA 4 para una implementación inmediata sin tiempo de finalización
D2(config)#ip sla schedule 6 life forever start-time now// no lo soporta packet tracer // programo el SLA 6 para una implementación inmediata sin tiempo de finalización
D2(config)#track 4 ip sla 4// no lo soporta packet tracer // creo el número de rastreo 4 y se asocia al IP SLA 4.
D2(config)# delay down 10 up 15// no lo soporta packet tracer// se notifica cada 10 segundos el cambio de estado dela IP SLA 4
D2(config)#exit
D2(config)#track 6 ip sla 6// no lo soporta packet tracer // creo el número de rastreo 6 y se asocia al IP SLA 6.
D2(config)# delay down 10 up 15// no lo soporta packet tracer // // se notifica cada 10 segundos el cambio de estado dela IP SLA cuando pasa de down a up y cada 15 segundos cuando pasa de up a down.

D2(config)#exit
D2(config)#interface vlan 100 // accedo a la interface vlan 100
D2(config-if)# standby version 2 // configure el HSRP para usar la versión 2
D2(config-if)# standby 104 ip 10.0.100.254 // inicio la configuración ipv4 HSRP grupo 104 para la vlan 100
D2(config-if)# standby 104 preempt // habilito la preferencia del grupo 104.
D2(config-if)# standby 104 track 4 decrement 60// no lo soporta packet tracer // rastreo el objeto 4 y se decrementa en 60.
D2(config-if)# standby 106 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 106 para la vlan 100, asignado la dirección ip virtual usando ipv6 autoconfig.
D2(config-if)# standby 106 preempt // habilito la preferencia del grupo 106.
D2(config-if)# standby 106 track 6 decrement 60
D2(config-if)# standby 106 track 6 decrement 60// no lo soporta packet tracer // rastreo el objeto 6 y se decrement en 60
D2(config)#exit

D2(config-if)#interface vlan 101 // accedo a la interface vlan 101
D2(config-if)# standby version 2 // configure el HSRP para usar la versión 2
D2(config-if)# standby 114 ip 10.0.101.254 // inicio la configuración ipv4 HSRP gupo 114 para la vlan 101, asignado la ip virtual.
D2(config-if)# standby 114 priority 150 // establezco la prioridad del grupo en 150
D2(config-if)# standby 114 preempt // habilito la preferencia del grupo 114.
D2(config-if)# standby 114 track 4 decrement 60// no lo soporta packet tracer // rastreo el objeto 4 y se decrement en 60.
D2(config-if)# standby 116 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 116 para la vlan 101, asignando la dirección ip virtual ipv6 autoconfig.
D2(config-if)# standby 116 priority 150 // se establece la prioridad del grupo 150
D2(config-if)# standby 116 preempt // habilito la preferencia del grupo 116
D2(config-if)# standby 116 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60.
D2(config-if)# standby 116 track 6 decrement 60// no lo soporta packet tracer
D2(config)#exit
D2(config-if)#interface vlan 102 // accedo a la interface vlan 102
D2(config-if)# standby version 2 // configure el HSRP para usar la versión 2.
D2(config-if)# standby 124 ip 10.0.102.254 // inicio la configuración ipv4 HSRP grupo 124 para la vlan 102, asignando la ip virtual
D2(config-if)# standby 124 preempt // habilito la preferencia del grupo 124.
D2(config-if)# standby 124 track 4 decrement 60// no lo soporta packet tracer // rastreo el objeto 4 y se decrement en 60
D2(config-if)# standby 126 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 126 para la vlan 102, se asigna la dirección ip virtual ipv6 autoconfig.
D2(config-if)# standby 126 preempt // habilito la preferencia del grupo 126
D2(config-if)# standby 126 track 6 decrement 60// no lo soporta packet tracer // rastreo el objeto 6 y se decrement en 60.
D2(config-if)# exi

4.3 En D1 configure HSRPv2.

D1 es el router primario para las VLANs 100 y 102; por lotanto, 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.

D1

D1(config)#interface vlan 100 // accedo a la interface vlan 100
D1(config-if)# standby version 2 // configuro el HSRP para usar la version 2
D1(config-if)# standby 104 ip 10.0.100.254 // inicio la configuración ipv4 HSRP grupo 104 para la vlan 100, asignando la ip virtual
D1(config-if)# standby 104 priority 150 // establezco la prioridad del grupo 104 en 150
D1(config-if)# standby 104 preempt // habilito la preferencia del grupo 104.
D1(config-if)# standby 104 track 4 decrement 60// no soportado por packet tracer // rastreo el objeto 4 y se decrement en 60
Para este caso se utilizo este comando pero no funciono debido a las características del software packet tracer.

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.

grupo 116 para la vlan 101, asignando la dirección ip virtual usando ipv6 autoconfig.
D1(config-if)# standby 116 preempt // habilito la preferencia al grupo 116
D1(config-if)# standby 116 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60.
D1(config-if)# standby 116 track 6 decrement 60// no soportado por packet tracer
D1(config-if)#exit
D1(config)#interface vlan 102 // accedo a la interface vlan 102
D1(config-if)# standby version 2// configure el HSRP para usar la versión 2.

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.

D1(config)#interface vlan 102 // accedo a la interface vlan 102
D1(config-if)# standby version 2// configure el HSRP para usar la versión 2.
D1(config-if)# standby 124 ip 10.0.102.254 // inicio la configuración ipv4 HSRP grupo 124 para la vlan 102, asignando la ip virtual.
D1(config-if)# standby 124 priority 150 // establezco la prioridad del grupo 124.
D1(config-if)# standby 124 preempt // hhabilito la preferencia al grupo 124.
D1(config-if)# standby 124 track 4 decrement 60// no soportado por packet tracer // rastreo el objeto 4 y se decrement en 60

Se utilizo este comando pero no funciono por problemas en la carracteristiacas del software, este comnado es utulizado para el rastreo de objeto disminuyendo 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.

D1(config-if)# standby 106 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 106 para la vlan 100, asigno la dirección ip virtual.
D1(config-if)# standby 106 priority 150 // establezco la prioridad del grupo en 150.
D1(config-if)# standby 106 preempt // habilito la preferencia al grupo 106.
D1(config-if)# standby 106 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60
D1(config-if)# standby 106 track 6 decrement 60// no soportado por packet tracer

Se utilizo este comando pero no funciono por problemas en la carracteristiacas del software, este comnado es utulizado para el rastreo de objeto disminuyendo 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.

D1(config-if)# standby 116 ipv6 autoconfig // inicio la configuración ipv6 HSRP grupo 116 para la vlan 101, asignando la dirección ip virtual usando ipv6 autoconfig.
D1(config-if)# standby 116 preempt // habilito la preferencia al grupo 116
D1(config-if)# standby 116 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60.
D1(config-if)# standby 116 track 6 decrement 60// no soportado por packet tracer

D1(config-if)#exit

Se utilizo este comando pero no funciono por problemas en la carracteristiacas del software, este comnado es utulizado para el rastreo de objeto disminuyendo 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.

D1(config-if)# standby 126 ipv6 autoconfig // configure ipv6 HSRP grupo 126 para la vlan 102, asignando la dirección ip virtual usando ipv6 autoconfig.
D1(config-if)# standby 126 priority 150 // establezco la prioridd al grupo 150.
D1(config-if)# standby 126 preempt // habilito la preferencia al grupo 126
D1(config-if)# standby 126 track 6 decrement 60 // rastreo el objeto 6 y se decrement en 60.
D1(config-if)# standby 126 track 6 decrement 60// no soportado por packet tracer // se rastrea el objeto 6 y se decrement en 60.

Se utilizo este comando pero no funciono por problemas en la carracteristiacas del software, este comnado es utulizado para el rastreo de objeto disminuyendo en 60.

Tabla 5. Configuración de seguridad

Tarea	Tarea	Especificación

5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmode 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 es10.0.100.6. • Puertos UDP del servidor RADIUS son1812 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 servidoresRADIUS • De lo contrario, utilice la base de datoslocal.
5.6	Verifique el servicio AAA en todos losdispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y lacontraseña: upass123.

5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.
Se ejecuto el comando pero packet tracer no lo soporto por las características del software de simulación.

R1

R1#configure terminal // ingreso al modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco//no lo soporta packet tracer

R2

R2#configure terminal // ingreso al modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco//no lo soporta packet tracer

R3

R3#enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco//no lo soporta packet tracer

D1

D1#enable
D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

A1

A1#enable
A1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco//no lo soporta packet tracer

5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.
Se ejecuto el comando pero packet tracer no lo soporto por las características del software de simulación.

R1

R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco//no lo soporta packet tracer

R3

R3(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco//no lo soporta packet tracer

D1

D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

D2

D2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

5.3 En todos los dispositivos (excepto R2), habilite AAA.

R1

R1(config)#aaa new-model

R3

R3(config)#aaa new-model

D1

D1(config)#aaa new-model

D2
D2(config)#aaa new-model

A1

A1(config)#aaa new-model

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

R1

R1(config)#radius server RADIUS // inicio la configuración del servidor
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813//no lo soporta packet tracer // especifico la dirección ip y los puertos UDP para R1

R3

R3(config)#radius server RADIUS
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813//no lo soporta packet tracer

D1
D1(config)#radius server RADIUS//no lo soporta packet tracer
D1(config)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813//no lo soporta packet tracer

D2

D2(config)#radius server RADIUS//no lo soporta packet tracer
D2(config)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813//no lo soporta packet trace
A1

A1(config)#radius server RADIUS//no lo soporta packet tracer
A1(config)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813//no lo soporta packet tracer

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

R1

R1(config)#aaa authentication login default group radius local
R1(config)#end

R3

R3(config)#aaa authentication login default group radius local
R3(config)#end

D1

D1#aaa authentication login default group radius local//no lo soporta packet tracer
D1#end

D2

D2#aaa authentication login default group radius local//no lo soporta packet tracer
D2#end

A1

A1#aaa authentication login default group radius local//no lo soporta packet tracer
D2#end

5.6 Verifique el servicio AAA en todos losdispositivos (except R2)

En esta situación no fue posible verificar el servicio AAA en todos los dispositivos por que no se pudo realizar la configuración debido a la compatibilidad del software con los comandos.

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. Configure las funciones de administración de red

Tarea	Tarea	Especificación
6.1	En todos los dispositivos, configureel reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTPmaestro.	Configurar R2 como NTP maestro en el nivel deestrato 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 losdispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 enel nivel WARNING.
6.5	Configure SNMPv2c en todos losdispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura(Read-Only). • Limite el acceso SNMP a la dirección IP de laPC1. • Configure el valor de contacto SNMP con sunombre. • Establezca el community string en ENCORSA. • En R3, D1, y D2, habilite el envío de trapsconfig y ospf. • En R1, habilite el envío de traps bgp, config, y ospf. • En A1, habilite el envío de traps config.

6.1 En todos los dispositivos, configureel reloj local a la hora UTC actual.
Configure el reloj local a la hora UTC actual

R1

R1#enable
R1#configure terminal // inicio modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 2.2.2.2 // configure el reloj local de R1 ala hora UTC actual.

R2

R2#enable
R2#configure terminal // inicio modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 2.2.2.2 // configure el reloj local de R1 ala hora UTC actual

D1

D1#enable
D1#configure terminal // inicio modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ntp server 2.2.2.2 // configure el reloj local de R1 ala hora UTC actual

D2

D2#enable
D2#configure terminal // inicio modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ntp server 2.2.2.2 // configure el reloj local de R1 ala hora UTC actual

A1

A1#enable
A1#configure terminal // inicio modo de configuración global
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#ntp server 2.2.2.2 // configure el reloj local de R1 ala hora UTC actual

6.2Configure R2 como un NTPmaestro.

R2

R2(config-router)#ntp master 3
R2(config)#end
Router R1

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

R1

R1 con R2

R1#configt t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 209.165.200.2226

R3 con R1

R3#configt t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 10.0.13.1

D1 con R1

D1#configt t
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ntp server 10.0.10.1

A1 con R1

A1#configt t
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#ntp server 10.0.10.1

D2 con R3

D2#configt t
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#ntp server 10.0.11.1

6.4 Configure Syslog en todos losdispositivos excepto R2
Syslogs deben enviarse a la PC1 en 10.0.100.5 enel nivel WARNING.
En la totalidad de los dispositivos no fue posible configurar el Syslog debido a la compatibilidad de packet tracer en un ambiente ideal los comandos serian:

R1

R1(config)#logging host 10.0.100.5

R1(config)#logging trap warning//no lo soporta parkertracer // establezco el nivel de prioridad del “trap” en el nivel 4 warning para brindar condiciones de advertencia

Y de esta misma manera se aplica para los dispositivos R3, D1, D2 y A1.

6.5 Configure SNMPv2c en todos losdispositivos excepto R2

Especificaciones de SNMPv2:

- Unicamente se usará SNMP en modo lectura(Read-Only).
- Limite el acceso SNMP a la dirección IP de laPC1.
- Configure el valor de contacto SNMP con sunombre.
- Establezca el community string en ENCORSA.
- En R3, D1, y D2, habilite el envío de trapsconfig y ospf.
- En R1, habilite el envío de traps bgp, config, y ospf.

En A1, habilite el envío de traps config.
En la totalidad de los dispositivos no fue posible configurar el Syslog debido a la compatibilidad de packet tracer en un ambiente ideal los comandos serian:

R1

R1(config)#logging host 10.0.100.5 // configure el host PC1 para que sea el host de registro de destino para R1.
R1(config)#logging on // habilito el registro para que los mensajes se puedan enviar.

R1(config)#ip access-list standard SNMP-NMS // limito el acceso SNMP a la dirección ip PC1
R1(config-std-nacl)#permit host 10.0.100.5
R1(config-std-nacl)#exit
R1(config)#snmp-server contact Cisco Cesar Nova//no lo soporta packet tracer // configuro el valor de contacto SNMP con mi nombre
R1(config)#snmp-server community ENCORSA ro SNMP-NMS//no lo soporta packet tracer //especifico a PC1 como el destinario de las operaciones del trap de SNMP.
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA//no lo soporta packet tracer // especifico a PC1 como el destinario de las operaciones del trap de SNMP.

R1(config)#snmp-server ifindex persist//no lo soporta packet tracer

R1(config)#snmp-server enable traps bgp//no lo soporta packet tracer
R1(config)#snmp-server enable traps config//no lo soporta packet tracer
R1(config)#snmp-server enable traps ospf//no lo soporta packet tracer
R1(config)#end

La configuración no funciono snmp-server no funcionó en packet tracer no lo ejecuta.

CONCLUSIONES

Se realizó este trabajo con el software packet Tracer, llevando a cabo la simulación de la escena planteada para esta actividad con algunas dificultades a la hora de ejecutar los comandos.

Se hizo la simulación de la escena planteada, algunos comandos no fueron posibles ejecutarlos debido a las limitaciones que tiene el software packet Tracer.

El diplomado CCNP me deja una gran enseñanza en cuanto al as habilidades y destrezas implementadas en el desarrollo de este que ayudaran a fortalecer mi carrera profesional.

Con el desarrollo de la práctica entendí que a la hora de administrar y configurar equipos hay situciones que se tornan difíciles cuando el software no responde a los requerimientos.

BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **IP Routing Essentials**. 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

dgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **EIGRP**. 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). **Enterprise Network Architecture**. 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). **Secure Access Control**. 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). **Network Device Access Control and Infrastructure Security**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8