DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DÍDIER JAVIER RAMÍREZ HENAO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DÍDIER JAVIER RAMÍREZ HENAO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Manizales, 19 de noviembre de 2021

AGRADECIMIENTOS

Este trabajo lo dedico a mi esposa y a mi hija. Lo dedico a mi esposa porque me ha impulsado a alcanzar un sueño que creía frustrado y lo dedico a mi hija porque ha sido mi gran motor para superarme.

Debo agradecer en primera instancia a Dios, a aquella fuente primordial y única que no comprendemos pero que nos permite existir y que lo sostiene todo, desde el microcosmos hasta el macrocosmos de forma perfecta.

Agradezco infinitamente a mis padres, porque sentaron las bases del ser que ahora soy y me enseñaron a luchar con constancia y sacrificio por mis ideales; porque aún en momentos de dificultad siempre permanecieron unidos, conservando como un tesoro nuestra hermosa familia y porque aún en la carencia todo lo dieron por mis hermanas y por mí y no se reservaron nada.

Tengo que agradecer a mis hermanas y amigos que siempre creyeron en mí, los cuales siempre me alentaron para continuar cuando el camino se hacía áspero y cuando la meta no se alcanzaba a vislumbrar.

También agradezco a mis maestros, a todos los que he tenido durante toda mi vida; especialmente a aquellos que con dedicación han trabajo de forma honesta por educar seres que aporten de forma positiva a nuestro planeta y a la humanidad; a aquellos que se convirtieron en antorcha viva y que con su ejemplo se volvieron guías que limpiaron y trazaron el camino para avanzar por la senda del conocimiento que destierra la ignorancia y permite ver con claridad.

Finalmente agradezco a mi esposa y a mi hija, ya que han sido las mayores sacrificadas por todo el tiempo que no les pude dedicar debido al trabajo y el estudio. Su amor desinteresado y sincero me llena de alegría, le da color a mi vida y me impulsa cada día a seguir adelante. Este triunfo también es de ustedes.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

AAA: La sigla AAA puede traducirse en español como Autenticación, Autorización y Auditoría (originalmente, Authentication, Authorization y Accounting). Cuando se habla de AAA (triple A), no se está basando en un solo protocolo o en algunos en especial, sino en una familia de protocolos que proveen los servicios anteriormente mencionados.

ENLACE TRONCAL: Es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

ETHERCHANNEL: Es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad. Los puertos usados deben tener las mismas características y configuración.

HSRP: El Hot Standby Router Protocol (o HSRP por sus siglas en inglés) es un protocolo propiedad de CISCO que permite el despliegue de enrutadores redundantes tolerantes de fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

IP SLA: Es una herramienta incluida dentro de las versiones modernas de IOS de los equipos Cisco (solo en algunos modelos), que permite monitorizar los niveles de servicio para aplicaciones y determinados indicadores de rendimiento de la red. Esta herramienta recopila información de rendimiento en tiempo real, siendo capaz de medir el rendimiento de las conexiones tanto desde la perspectiva de los dispositivos de red como desde la de los equipos de trabajo.

NTP: El Network Time Protocol (NTP) es ampliamente utilizado para sincronizar un ordenador a los Servidores de tiempo de Internet o a otras fuentes, tales como una radio o receptores satelitales o servicios del módem del teléfono. La exactitud es típicamente menos de un milisegundo en las LAN y hasta algunos milisegundos en las WAN. Las configuraciones NTP típicas utilizan servidores redundantes múltiples y diversos trayectos de red para alcanzar una elevada precisión y confiabilidad.

VLAN: Es una red LAN independiente, Una VLAN es una subred IP separada de manera lógica. Las VLAN permiten que redes de IP y subredes múltiples existan en la misma red conmutada.

RESUMEN

El presente documento tiene gran relevancia, puesto que en este quedan plasmados los diversos conocimientos que fueron adquiridos en el transcurso de los cursos que componen la ingeniería de telecomunicaciones, especialmente aquellos cursos relacionados con el enrutamiento y la conmutación, como lo son los cursos CCNA de CISCO.

Parece increíble que, en un lapso relativamente corto, se haya desarrollado de forma tan vertiginosa las redes y todo el cúmulo de conocimiento que hay a su alrededor, desde configuraciones de los dispositivos de forma básica hasta configuraciones mucho más avanzadas que hace que nos encontremos con diversos niveles de profesionales en el campo de las redes.

Para el desarrollo de este trabajo se requiere de una sólida comprensión de los protocolos comunes de la industria junto con la arquitectura y configuración de los dispositivos y lo que hace valioso este diplomado, es que, mediante la obtención del título y el certificado correspondiente, se genera credibilidad en el campo laboral y académico, lo que nos abre puertas para podernos desempeñar en el cada vez más basto mundo de las redes.

El mundo avanza y con él avanzamos todos a un mundo cada vez más digital, por lo que se hace imprescindible contar con personas capacitadas para atender las diversas demandas de diseño, configuración y montaje de redes, que brinden todas las características de administración y seguridad requeridas para poder dar solución a las necesidades empresariales y personales y para ello estamos los futuros profesionales preparándonos para poder atender dichas demandas.

Comprender los temas inmersos en el desarrollo de cada tarea es fundamental para cualquier estudiante que quiera ser un profesional en redes, ya que la conmutación y el enrutamiento van mucho más allá de las configuraciones básicas y en un mundo donde impera cada vez más la electrónica, se requiere de personas íntegras que mantengan la seguridad de la red.

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

ABSTRACT

This document is highly relevant, since it reflects the various knowledge that was acquired in the course of the courses that make up telecommunications engineering, especially those courses related to routing and switching, such as the CCNA courses of CISCO.

It seems incredible that, in a relatively short period of time, networks and all the accumulation of knowledge around them have developed so rapidly, from basic device configurations to much more advanced configurations that makes us find ourselves with various levels of professionals in the field of networking.

For the development of this work, a solid understanding of the common protocols of the industry is required together with the architecture and configuration of the devices and what makes this diploma valuable is that, by obtaining the title and the corresponding certificate, generates credibility in the labor and academic field, which opens doors for us to be able to perform in the increasingly vast world of networks.

The world advances and with it we all advance to an increasingly digital world, which is why it is essential to have trained people to meet the various demands of network design, configuration and assembly, which provide all the required administration and security characteristics. to be able to solve the business and personal needs and for this we are the future professionals preparing ourselves to be able to meet these demands.

Understanding the topics involved in the development of each task is essential for any student who wants to be a professional in networks, since switching and routing go far beyond the basic configurations and in a world where electronics is increasingly prevalent, people of integrity are required to maintain network security

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

INTRODUCCIÓN

En el presente documento se tiene un escenario y una tabla de direccionamiento para desarrollar diversas actividades concernientes al módulo CCNP de CISCO. En primer lugar, se realiza la construcción y el cableado de la red de acuerdo con la topología dada y es implementada en GNS3; luego, se configuran los parámetros básicos de cada dispositivo teniendo presente la tabla de direccionamiento.

En la segunda parte se configura la capa 2 de la red y el soporte de host; para ello, en todos los conmutadores se configura interfaces troncales, se habilita el protocolo RSTP, se crean EtherChannels y se configuran los puertos de acceso del host. Los enrutadores D1 y D2 se configuran como root para las VLAN indicadas. Finalmente se verifican los servicios DHCP IPv4 y se verifica la conectividad de la LAN local. Para la tercera parte se configuran los protocolos de enrutamiento para IPv4 e IPv6 como son OSPFv2 y OSPFv3 y se configura MP – BGP. En la cuarta parte se configura la redundancia del primer salto HSRP versión 2 para proveer la redundancia de primer salto para los hosts en la red de la compañía.

La quinta parte consiste en configurar diversos mecanismos de seguridad en los dispositivos, tales como la protección del EXEC privilegiado usando el algoritmo de encriptación SCRIPT, la habilitación de AAA, la configuración de las especificaciones del servidor RADIUS y configurando la lista de métodos de autenticación AAA. Para finalizar en la sexta parte del trabajo se configuran las funciones de administración de red configurando NTP, syslog y SNMPv2.

ESCENARIO PROPUESTO

Figura 1. Escenario propuesto (Topología de red).

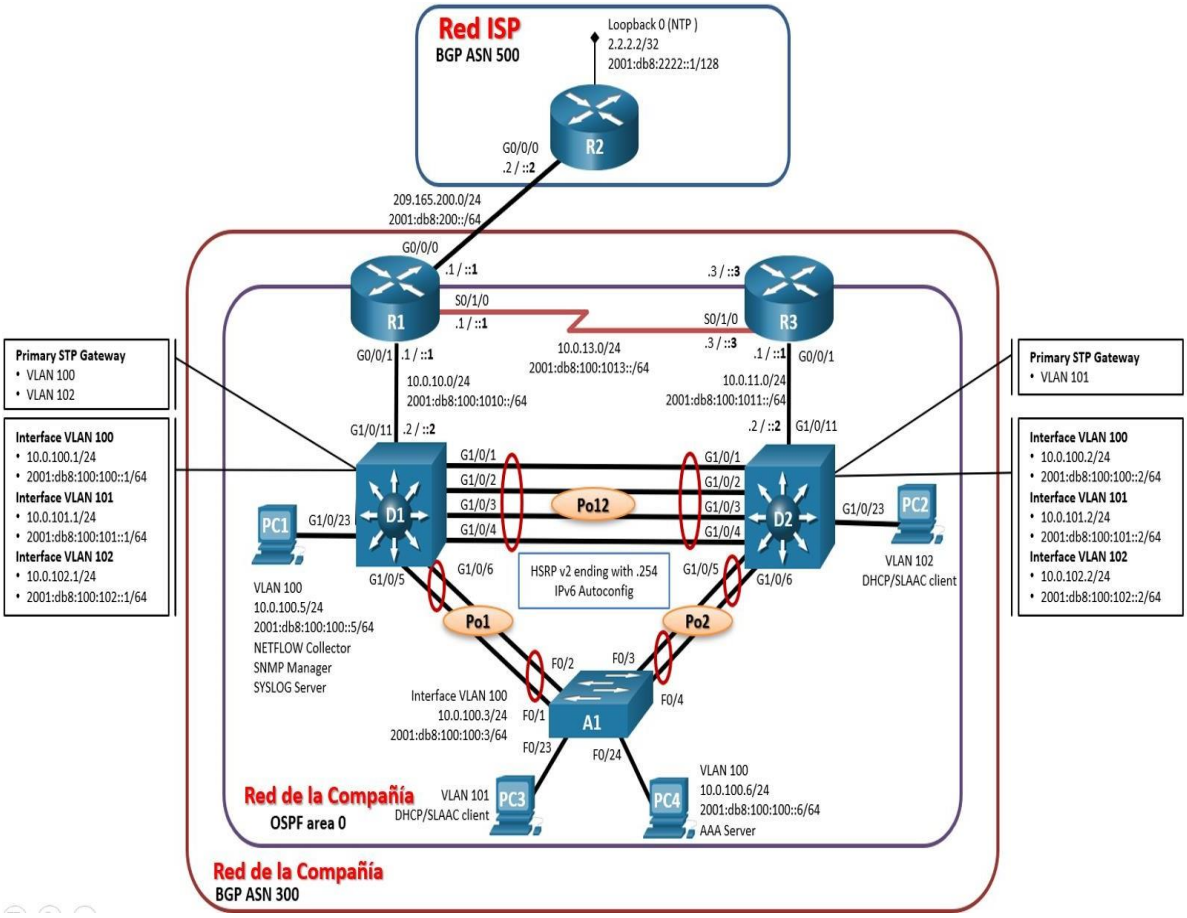


Tabla 1. Tabla de direccionamiento.

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
	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
	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

DESARROLLO

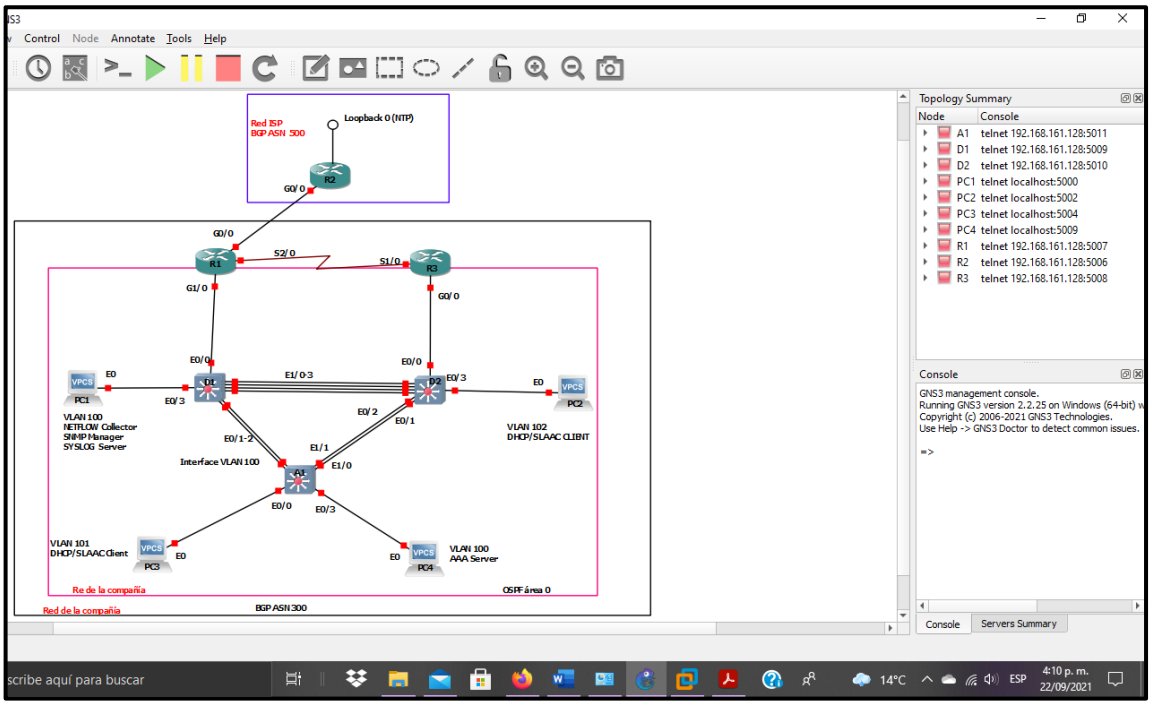
Debido a que los switches empleados no tienen interfaces gigabit - ethernet ni fast - ethernet, se trabajó para dichos switches con interfaces ethernet. A continuación, se muestra la asignación de interfaces en cada uno de los dispositivos:

Tabla 2. Tabla de direccionamiento con la nueva asignación de interfaces.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E0/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E0/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

y la figura 2 es la topología con el cambio de interfaces:

Figura 2. Topología con las nuevas interfaces asignadas.



Objetivos

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces.
Part 2: Configurar la capa 2 de la red y el soporte de Host
Part 3: Configurar los protocolos de enrutamiento
Part 4: Configurar la redundancia del primer salto.
Part 5: Configurar la seguridad.
Part 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 la Compañía**" 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 variar de 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 tengan configuraciones de inicio.

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. 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.

Para el cableado de la red, ver figura 2.

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:

Tabla 3. Configuración básica de R1.

R1#	Se ingresa al modo privilegiado
R1(config)#hostname R1	En el modo de configuración global se asigna el nombre al router R1
R1(config)#ipv6 unicast-routing	Se habilita router como router IPv6
R1(config)#no ip domain lookup	Se habilita la traducción de nombre a dirección basado en DNS del host.
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	Se crea un mensaje de aviso
R1(config)#line con 0	Se ingresa al modo de configuración de línea de la consola 0.
R1(config-line)#exec-timeout 0 0	En el puerto de la consola 0 nunca se agotará el tiempo de espera.
R1(config-line)#logging synchronous	Evita que los mensajes inesperados que aparecen en pantalla, desplacen los comandos que estamos escribiendo en el momento.
R1(config)#interface g0/0	Se procede a configurar la interface g0/0 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	Se asigna la dirección ipv6.

2001:db8:200::1/64 R1(config-if)#no shutdown R1(config)#interface g1/0 R1(config-if)#ip address 10.0.10.1 255.255.255.0 R1(config-if)#ipv6 address fe80::1:2 link-local R1(config-if)#ipv6 address 2001:db8:100:1010::1/64 R1(config-if)#no shutdown R1(config)#interface s2/0 R1(config-if)#ip address 10.0.13.1 255.255.255.0 R1(config-if)#ipv6 address fe80::1:3 link-local R1(config-if)#ipv6 address 2001:db8:100:1013::1/64 R1(config-if)#no shutdown	 Se habilita la interface g0/0. Se procede a configurar la interface g1/0 de R1. Se asigna la dirección ipv4 y la máscara de subred. Se asigna la dirección link local. Se asigna la dirección ipv6. Se habilita la interface g1/0. Se procede a configurar la interface s2/0 de R1. Se asigna la dirección ipv4 y la máscara de subred. Se asigna la dirección link local. Se asigna la dirección ipv6. Se habilita la interfaz s2/0.

Figura 3. Configuración básica de R1.

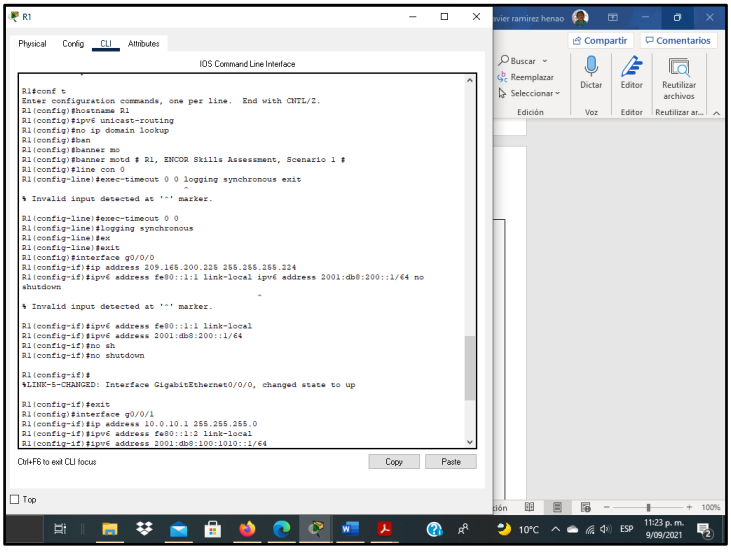


Tabla 4. Configuración básica de R2

Router>enable	Se ingresa al modo privilegiado
Router(config)#hostname R2	En el modo de configuración global se asigna el nombre al router R2
R2(config)#ipv6 unicast-routing	Se habilita router como router IPv6
R2(config)#no ip domain lookup	Se habilita la traducción de nombre a dirección basado en DNS del host.
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	Se crea un mensaje de aviso.
R2(config)#line con 0	Se ingresa al modo de configuración de línea de la consola 0.
R2(config-line)#exec-timeout 0 0	En el puerto de la consola 0 nunca se agotará el tiempo de espera.
R2(config-line)#logging synchronous	Evita que los mensajes inesperados que aparecen en pantalla desplacen los comandos que estamos escribiendo en el momento.
R2(config-line)#exit	
R2(config)#interface g0/0	Se procede a configurar la interface g0/0 de R2.
R2(config-if)#ip address 209.165.200.226 255.255.255.224	Se asigna la dirección ipv4 y la máscara de subred.
R2(config-if)#ipv6 address fe80::2:1 link-local	Se asigna la dirección link local a la interface.
R2(config-if)#ipv6 address 2001:db8:200::2/64	Se asigna la dirección ipv6.
R2(config-if)#no shutdown	Se habilita la interface g0/0.
R2(config)#interface Loopback 0	Se procede a configurar la interface Loopback 0 de R2.
R2(config-if)#ip address 2.2.2.2 255.255.255.255	Se asigna la dirección ipv4 y la máscara de subred.
R2(config-if)#ipv6 address fe80::2:3 link-local	Se asigna la dirección link local.
R2(config-if)#ipv6 address 2001:db8:2222::1/128	Se asigna la dirección ipv6.
R2(config-if)#no shutdown	Se habilita la interface Loopback 0

Figura 4. Configuración básica de R2.

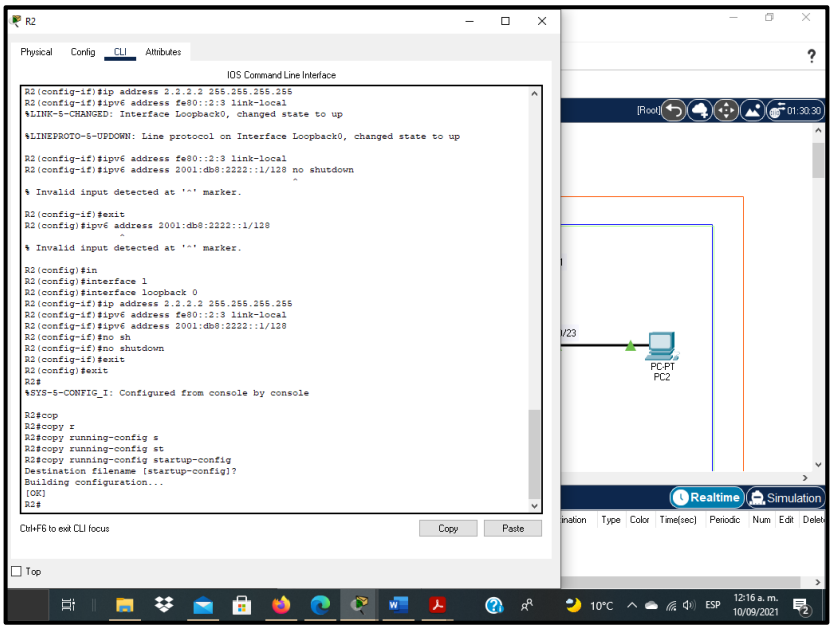


Tabla 5. Configuración básica de R3.

Router(config)#hostname R3	En el modo de configuración global se asigna el nombre al router R3.
R3(config)#ipv6 unicast-routing	Se habilita router como router IPv6
R3(config)#no ip domain lookup	Se habilita la traducción de nombre a dirección basado en DNS del host.
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	Se crea un mensaje de aviso.
R3(config)#line con 0	Se ingresa al modo de configuración de línea de la consola 0.
R3(config-line)#exec-timeout 0 0	En el puerto de la consola 0 nunca se agotará el tiempo de espera.
R3(config-line)#logging synchronous	Evita que los mensajes inesperados que aparecen en pantalla desplacen los comandos que estamos escribiendo en el momento.
R3(config-line)#exit	
R3(config)#interface g0/0	Se procede a configurar la interface g0/0 de R3.
R3(config-if)#ip address 10.0.11.1	Se asigna la dirección ipv4 y la

255.255.255.0	máscara de subred.
R3(config-if)#ipv6 address fe80::3:2 link-local	Se asigna la dirección link local a la interface.
R3(config-if)#ipv6 address 2001:db8:100:1011::1/64	Se asigna la dirección ipv6.
R3(config-if)#no shutdown	Se habilita la interface g0/0.
R3(config)#interface s1/0	Se procede a configurar la interface s1/0 de R3.
R3(config-if)#ip address 10.0.13.3 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
R3(config-if)#ipv6 address fe80::3:3 link-local	Se asigna la dirección link local.
R3(config-if)#ipv6 address 2001:db8:100:1010::2/64	Se asigna la dirección ipv6.
R3(config-if)#no shutdown	Se habilita la interface s1/0.

Figura 5. Configuración básica de R3.

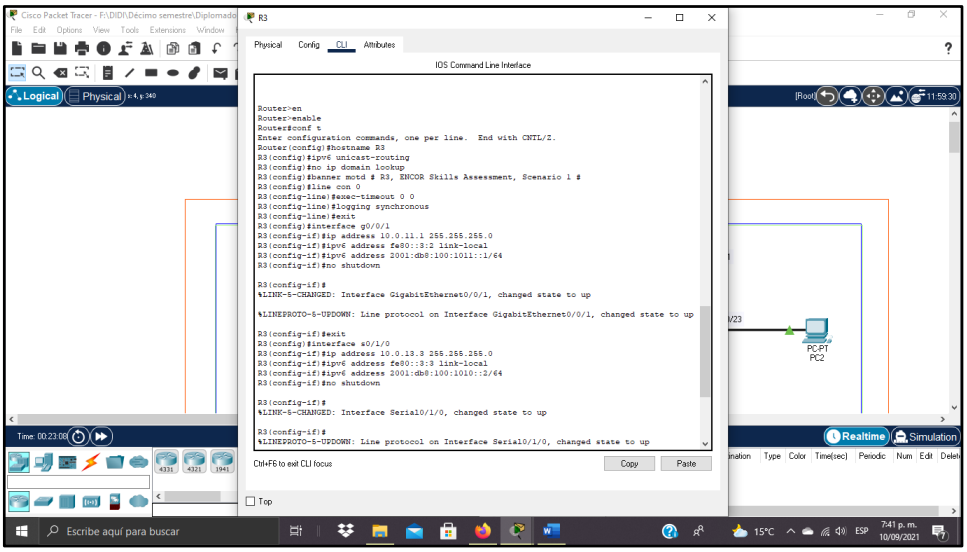


Tabla 6. Configuración básica del switch D1.

hostname D1	En el modo de configuración global se asigna el nombre al Switch D1.
ip routing	Se habilita el routing ipv4.
ipv6 unicast-routing	Se habilita routing IPv6
no ip domain lookup	Se habilita la traducción de nombre a dirección basado en DNS del host.
banner motd # D1, ENCOR Skills	Se crea un mensaje de aviso
Assessment, Scenario 1 #	Se ingresa al modo de
line con 0	configuración de línea de la consola 0.
exec-timeout 0 0	En el puerto de la consola 0 nunca se agotará el tiempo de espera.
logging synchronous	Evita que los mensajes inesperados
exit	que aparecen en pantalla desplacen los comandos que estamos escribiendo en el momento.
vlan 100	Se configura la vlan 100 en D1.
name Management	Se le asigna nombre.
exit	
vlan 101	Se configura la vlan 101 en D1.
name UserGroupA	Se le asigna nombre.
exit	
vlan 102	Se configura la vlan 102 en D1.
name UserGroupB	Se le asigna nombre.
exit	
vlan 999	Se configura la vlan 999
name NATIVE	Se le asigna nombre como la vlan
exit	nativa.
interface E0/0	Se procede a configurar la interface E0/0 de D1.
no switchport	Se aporta a la interface capacidad de capa3.
ip address 10.0.10.2 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d1:1 link-local	Se asigna la dirección link local a la interface.
ipv6 address 2001:db8:100:1010::2/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface E0/0.
exit	Se sale de la interfaz E0/0.
interface vlan 100	Se procede a configurar la interface vlan 100 de D1.

ip address 10.0.100.1 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d1:2 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:100::1/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 100.
exit	
interface vlan 101	Se procede a configurar la interface vlan 101 de D1.
ip address 10.0.101.1 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d1:3 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:101::1/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 101.
exit	
interface vlan 102	Se procede a configurar la interface vlan 102 de D1.
ip address 10.0.102.1 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d1:4 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:102::1/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 102.
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.109	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp excluded-address 10.0.101.141 10.0.101.254	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp excluded-address 10.0.102.1 10.0.102.109	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp excluded-address 10.0.102.141 10.0.102.254	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp pool VLAN-101	Se configura un servidor dhcp en la VLAN 101
network 10.0.101.0 255.255.255.0	Se asigna la dirección de red con la máscara de subred.
default-router 10.0.101.254	Se asigna la puerta de enlace predeterminada.
exit	
ip dhcp pool VLAN-102	Se hace un proceso similar al anterior, pero con la vlan 102.
network 10.0.102.0 255.255.255.0	
default-router 10.0.102.254	
exit	
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4 shutdown	No fue necesario deshabilitar interfaces en este switch, debido a que todas fueron utilizadas.
exit	

Figura 6. Configuración básica del switch D1.

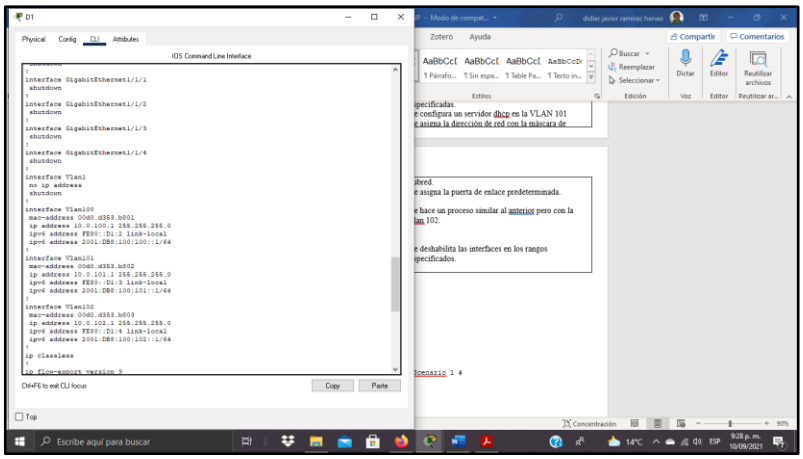


Tabla 7. Configuración básica del switch D2.

hostname D2	En el modo de configuración global se asigna el nombre al Switch D2.
ip routing	Se habilita el routing ipv4
ipv6 unicast-routing	Se habilita routing IPv6
no ip domain lookup	Se habilita la traducción de nombre a dirección basado en DNS del host.
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	Se crea un mensaje de aviso.
line con 0	Se ingresa al modo de configuración de línea de la consola 0.
exec-timeout 0 0	En el puerto de la consola 0 nunca se agotará el tiempo de espera.
logging synchronous	Evita que los mensajes inesperados que aparecen enpantalla, desplacen los comandos que estamos escribiendo en el momento.
exit	
vlan 100	Se configura la vlan 100 en D2.
name Management	Se le asigna nombre.
exit	
vlan 101	Se configura la vlan 101 en D2.
name UserGroupA	Se le asigna nombre.
exit	
vlan 102	Se configura la vlan 102.
name UserGroupB	Se le asigna nombre.
exit	

vlan 999	Se configura la vlan 999 en D2.
name NATIVE	Se le asigna nombre como vlan nativa.
exit	
interface E0/0	Se procede a configurar la interface E0/0 de D2.
no switchport	Se aporta a la interface capacidad de capa3.
ip address 10.0.11.2 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d1:1 link-local	Se asigna la dirección link local a la interface.
ipv6 address 2001:db8:100:1011::2/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface E0/0.
exit	Se sale de la interfaz E0/0.
interface vlan 100	Se procede a configurar la interface vlan 100 de D2.
ip address 10.0.100.2 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d2:2 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:100::2/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 100.
exit	
interface vlan 101	Se procede a configurar la interface vlan 101 de D2.
ip address 10.0.101.2 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d2:3 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:101::2/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 101.
exit	
interface vlan 102	Se procede a configurar la interface vlan 102 de D2.
ip address 10.0.102.2 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::d2:4 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:102::2/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 102.
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.209	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp excluded-address 10.0.101.241 10.0.101.254	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp excluded-address 10.0.102.1 10.0.102.209	Se excluye el rango de direcciones ipv4 especificadas.

ip dhcp excluded-address 10.0.102.241 10.0.102.254	Se excluye el rango de direcciones ipv4 especificadas.
ip dhcp pool VLAN-101	Se configura un servidor dhcp en la VLAN 101
network 10.0.101.0 255.255.255.0	Se asigna la dirección de red con la máscara de subred.
default-router 10.0.101.254	
exit	
ip dhcp pool VLAN-102	Se configura un servidor dhcp en la VLAN 102
network 10.0.102.0 255.255.255.0	Se asigna la dirección de red con la máscara de subred.
default-router 10.0.102.254	Se asigna la puerta de enlace predeterminada.
exit	
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4 shutdown	No fue necesario deshabilitar interfaces en D2 porque todas fueron ocupadas.
exit	

Figura 7. Configuración básica del switch D2.

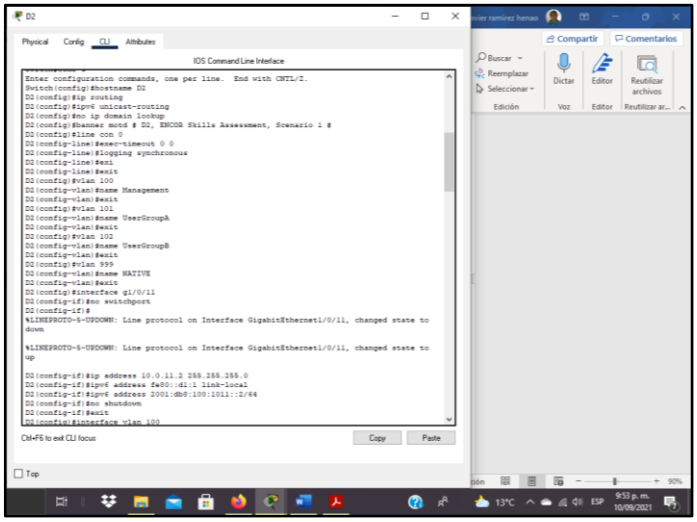
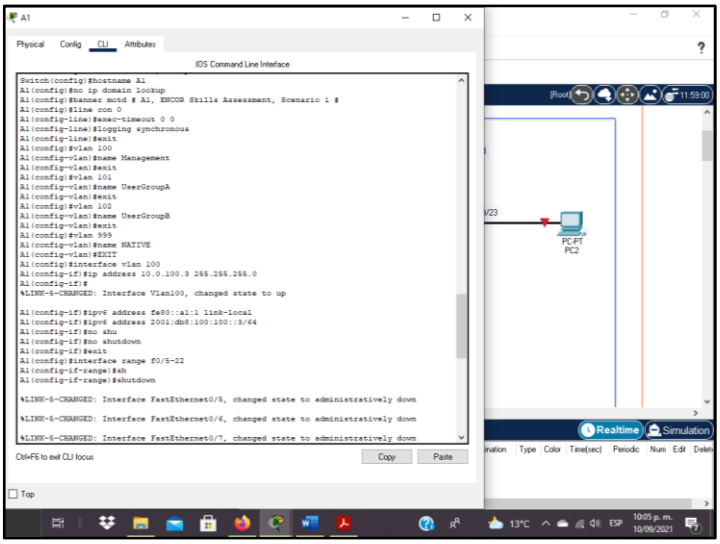


Tabla 8. Configuración básica de A1.

hostname A1	En el modo de configuración global se asigna el nombre al Switch A1.
no ip domain lookup	Se habilita la traducción de nombre a dirección basado en DNS del host.
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	Se crea un mensaje de aviso
line con 0	Se ingresa al modo de configuración de línea de la consola 0.
exec-timeout 0 0	En el puerto de la consola 0 nunca se agotará el tiempo de espera.
logging synchronous	Evita que los mensajes inesperados que aparecen en pantalla, desplacen los comandos que estamos escribiendo en el momento.
exit	
vlan 100	Se configura la vlan 100 en A1.
name Management	Se le asigna nombre.
exit	
vlan 101	Se configura la vlan 101en A1.
name UserGroupA	Se le asigna nombre.
exit	
vlan 102	Se configura la vlan 102 en A1.
name UserGroupB	Se le asigna nombre.
exit	
vlan 999	Se configura la vlan 999 en A1.
name NATIVE	Se le asigna nombre como vlan nativa.
exit	
interface vlan 100	Se procede a configurar la interface vlan 100 de A1.
ip address 10.0.100.3 255.255.255.0	Se asigna la dirección ipv4 y la máscara de subred.
ipv6 address fe80::a1:1 link-local	Se asigna la dirección link local.
ipv6 address 2001:db8:100:100::3/64	Se asigna la dirección ipv6.
no shutdown	Se habilita la interface vlan 100.
exit	
interface range E1/2-3 shutdown	Se deshabilita las interfaces en los rangos especificados.
exit	

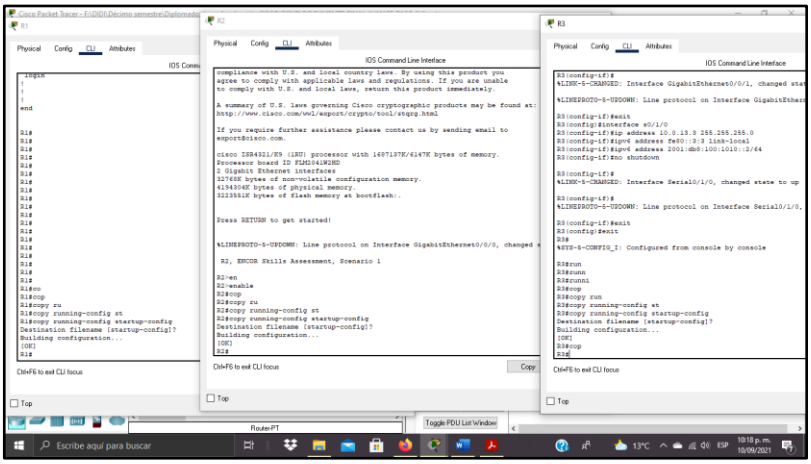
Figura 8. Configuración básica switch A1.



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

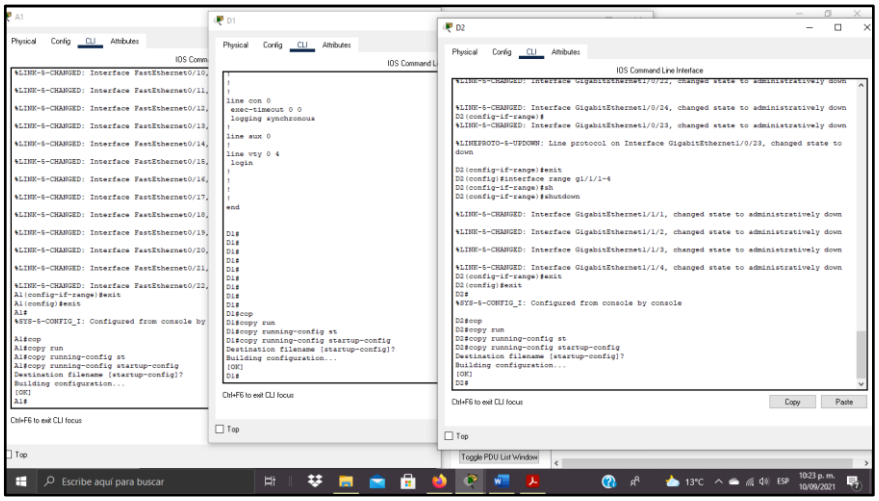
Se emplea el comando: copy running-config startup-config en R1, R2 y R3.

Figura 9. Copia al archivo starup-config en R1, R2 y R3.



Se emplea el comando: copy running-config startup-config en A1, D1 y D2.

Figura 10. Copia al archivo starup-config en A1, D1 y D2.



b. 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.

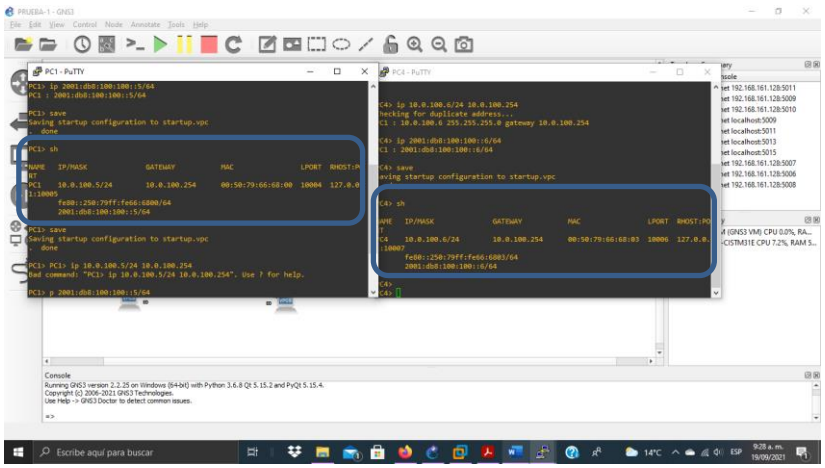
Configuración de PC1

PC1> ip 10.0.100.5/24 10.0.100.254 Checking for duplicate address... PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254	Se configura la dirección ipv4 y el Gateway predeterminado.
PC1> ip 2001:db8:100:100::5/64 PC1 : 2001:db8:100:100::5/64	Se configura la dirección ipv6.

Configuración de PC4

PC4> ip 10.0.100.6/24 10.0.100.254 Checking for duplicate address... PC1 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254	Se configura la dirección ipv4 y el Gateway predeterminado.
PC4> ip 2001:db8:100:100::6/64	Se configura la dirección ipv6.

Figura 11. Verificación del direccionamiento de PC1 y PC4.



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

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

Tabla 9. Lista de tareas de la 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

Desarrollo Tarea 2.1, 2.2, 2.3.

Switch D1:

D1(config)#interface range ethernet 1/0-3, ethernet 0/1-2	Se selecciona el rango de interfaces ethernet 1/0-3, ethernet 0/1-2.
D1(config-if-range)#switchport trunk encapsulation dot1q	Se configuran como interfaces troncales.
D1(config-if-range)#switchport mode trunk	
D1(config-if-range)#switchport trunk allowed vlan 100,101,102,999	Se permiten solo las vlan 100,101,102 y 999 para estas interfaces troncales.
D1(config-if-range)#switchport trunk native vlan 999	Se asigna la vlan 999 como nativa.
D1(config-if-range)#no shutdown	Se activan las interfaces.
D1(config)# spanning-tree mode rapid-pvst	Se activa el protocolo RSPT.

Switch D2:

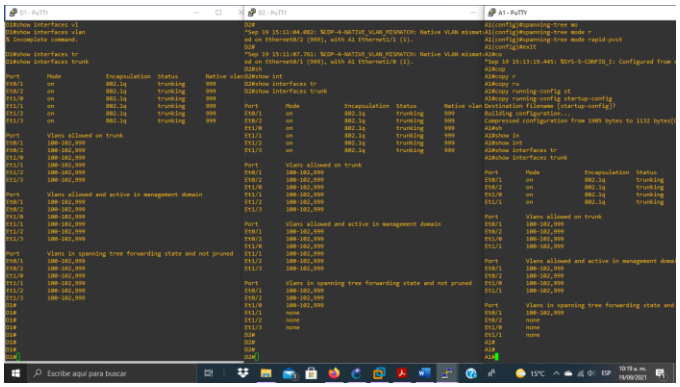
D2(config)#interface range ethernet 1/0-3, ethernet 0/1-2	Se selecciona el rango de interfaces ethernet 1/0-3, ethernet 0/1-2.
D2(config-if-range)#switchport trunk encapsulation dot1q	Se configuran como interfaces troncales.
D2(config-if-range)#switchport mode trunk	
D2(config-if-range)#switchport trunk allowed vlan 100,101,102,999	Se permiten solo las vlan 100,101,102 y 999 para estas interfaces troncales.
D2(config-if-range)#switchport trunk native vlan 999	Se asigna la vlan 999 como nativa.
D2(config-if-range)#no shutdown	Se activan las interfaces.
D2(config)#spanning-tree mode rapid-pvst	Se activa el protocolo RSPT.

Switch A1:

A1(config)#interface range fastEthernet 0/1-4	Se selecciona el rango de interfaces Fa 0/1-4.
A1(config-if-range)#switchport trunk native vlan 999	Se asigna la vlan 999 como nativa.
A1(config-if-range)#switchport mode trunk	Se configuran como interfaces troncales.
A1(config-if-range)#switchport trunk allowed vlan 100,101,102,999	Se permiten solo las vlan 100,101,102 y 999 para estas interfaces troncales.
A1(config-if-range)#no shutdown	Se activan las interfaces.

A1(config-if-range)#exit	
A1(config)#spanning-tree mode rapid-pvst	Se activa el protocolo RSPT.

Figura 12. Verificación de la creación de las interfaces troncales, la vlan nativa y la activación del protocolo RSPT en D1, D2 y A1.



Desarrollo de la tarea 2.4

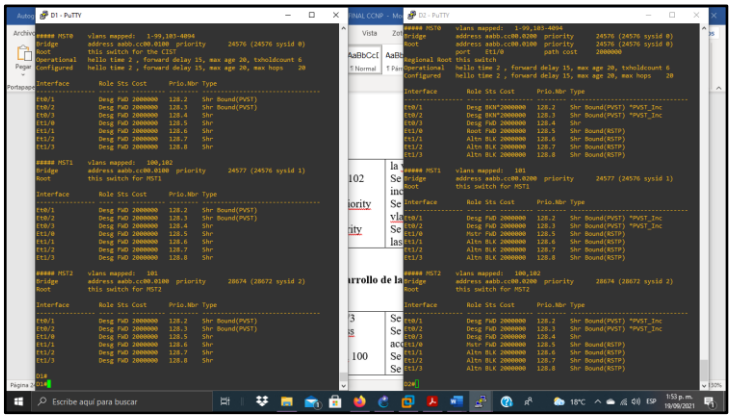
Configuración de D1 como raíz (root) para las VLAN apropiadas.

D1(config)#spanning-tree mode mst	Se configura D1 para usar mst.
D1(config)#spanning-tree extend system-id	Se acomoda la información de VLAN adicional, tomando prestados 12 bits de la Prioridad de puente original.
D1(config)#spanning-tree mst configuration	Se ingresa al modo de configuración mst.
D1(config-mst)#name CCNPv8	Se asigna un nombre de región mst.
D1(config-mst)#revision 1	Se configura un número de revisión de configuración de MST.
D1(config-mst)#instance 1 vlan 100-102	Se configura la instancia 1 donde se incluyen las vlan 100 y 102.
D1(config-mst)#instance 2 vlan 101	Se configura la instancia 2 donde se incluye la vlan 101.
D1(config)#spanning-tree mst 0-1 priority 24576	Se estable mst0 y mst1 como raíz (para las vlan 100 y 102).
D1(config)#spanning-tree mst 2 priority 28672	Se establece mst2 como secundario (para la vlan 101).

Configuración de D2 como raíz (root) para las VLAN apropiadas.

D2(config)#spanning-tree mode mst	Se configura D2 para usar mst.
D2(config)#spanning-tree extend system-id	Se acomoda la información de VLAN adicional, tomando prestados 12 bits de la Prioridad de puente original.
D2(config)#spanning-tree mst configuration	Se ingresa al modo de configuración mst.
D2(config-mst)#name CCNPv8	Se asigna un nombre de región mst
D2(config-mst)#revision 1	Se configura un número de revisión de configuración de MST.
D2(config-mst)#instance 1 vlan 101	Se configura la instancia 1 donde se incluye la vlan 101.
D2(config-mst)#instance 2 vlan 100-102	Se configura la instancia 2 donde se incluyen las vlan 100 y 102.
D2(config)#spanning-tree mst 0-1 priority 24576	Se estable mst0 y mst1 como raíz (para la vlan 101).
D2(config)#spanning-tree mst 2 priority 28672	Se establece mst2 como secundario (para las vlan 100 y 102).

Figura 13. Configuración del root bridge para las vlan indicadas en D1 y D2



Desarrollo de la tarea 2.5

Activando el canal 12 en D1 y configurando LACP:

D1(config)#interface ethernet 1/0	Se accede a configurar la interface E1/0.
D1(config-if)#switchport mode trunk	Se coloca en modo trunk.
D1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D1(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.
D1(config)#interface ethernet 1/1	Se accede a configurar la interface

	E1/1.
D1(config-if)#switchport mode trunk	Se coloca en modo trunk.
D1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D1(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.
D1(config)#interface ethernet 1/2	Se accede a configurar la interface E1/2.
D1(config-if)#switchport mode trunk	Se coloca en modo trunk.
D1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D1(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.
D1(config)#interface ethernet 1/3	Se accede a configurar la interface E1/3.
D1(config-if)#switchport mode trunk	Se coloca en modo trunk.
D1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D1(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.

Activando el canal 12 en D2 y configurando LACP:

D2(config)#interface ethernet 1/0	Se accede a configurar la interface E1/0.
D2(config-if)#switchport mode trunk	Se coloca en modo trunk.
D2(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D2(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.
D2(config)#interface ethernet 1/1	Se accede a configurar la interface E1/1.
D2(config-if)#switchport mode trunk	Se coloca en modo trunk.
D2(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D2(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.
D2(config)#interface ethernet 1/2	Se accede a configurar la interface E1/2.
D2(config-if)#switchport mode trunk	Se coloca en modo trunk.
D2(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D2(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.
D2(config)#interface ethernet 1/3	Se accede a configurar la interface E1/3.
D2(config-if)#switchport mode trunk	Se coloca en modo trunk.
D2(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D2(config-if)#channel-group 12 mode active	Se activa el protocolo LACP de forma incondicional.

Activando el canal 1 en D1 y configurando LACP:

D1(config)#interface ethernet 0/1	Se accede a configurar la interface E0/1.
D1(config-if)#switchport mode trunk	Se coloca en modo trunk.
D1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D1(config-if)#channel-group 1 mode active	Se activa el protocolo LACP de forma incondicional.
D1(config)#interface ethernet 0/2	Se accede a configurar la interface E0/2.
D1(config-if)#switchport mode trunk	Se coloca en modo trunk.
D1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D1(config-if)#channel-group 1 mode active	Se activa el protocolo LACP de forma incondicional.

Activando el canal 1 en A1 y configurando LACP:

A1(config)#interface ethernet 0/1	Se accede a configurar la interface E0/1.
A1(config-if)#switchport mode trunk	Se coloca en modo trunk.
A1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
A1(config-if)#channel-group 1 mode active	Se activa el protocolo LACP de forma incondicional.
A1(config)#interface ethernet 0/2	Se accede a configurar la interface E0/2.
A1(config-if)#switchport mode trunk	Se coloca en modo trunk.
A1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
A1(config-if)#channel-group 1 mode active	Se activa el protocolo LACP de forma incondicional.

Activando el canal 2 en D2 y configurando LACP:

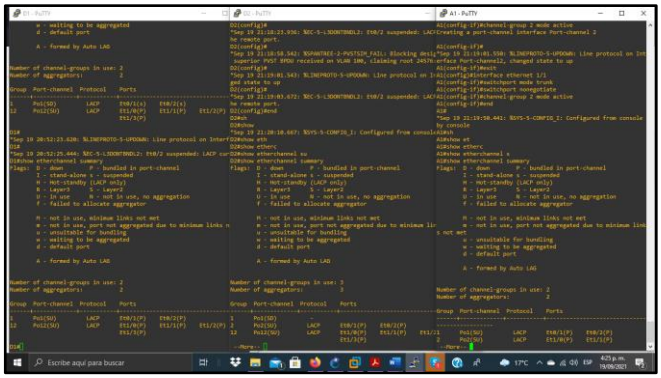
D2(config)#interface ethernet 0/1	Se accede a configurar la interface E0/1.
D2(config-if)#switchport mode trunk	Se coloca en modo trunk.
D2(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
D2(config-if)#channel-group 2 mode active	Se activa el protocolo LACP de forma incondicional.
D2(config)#interface ethernet 0/2	Se accede a configurar la interface E0/2.
D2(config-if)#switchport mode trunk	Se coloca en modo trunk.
D2(config-if)#switchport nonegotiate	Se evita generar tramas DPT.

D2(config-if)#channel-group 2 mode active	Se activa el protocolo LACP de forma incondicional.

Activando el canal 2 en A1 y configurando LACP:

A1(config)#interface ethernet 1/0	Se accede a configurar la interface E1/0.
A1(config-if)#switchport mode trunk	Se coloca en modo trunk.
A1(config-if)#switchport nonegotiate	Se evita generar tramas DPT
A1(config-if)#channel-group 2 mode active	Se activa el protocolo LACP de forma incondicional
A1(config)#interface ethernet 1/1	Se accede a configurar la interface E1/1.
A1(config-if)#switchport mode trunk	Se coloca en modo trunk.
A1(config-if)#switchport nonegotiate	Se evita generar tramas DPT.
A1(config-if)#channel-group 2 mode active	Se activa el protocolo LACP de forma incondicional.

Figura 14. Evidencia de la creación de los etherchannel LACP en D1, D2 y A1.



Desarrollo de la tarea 2.6

Configuración puerto de acceso D1:

D1(config-vlan)#interface ethernet 0/3	Se accede a configurar la interface E0/3.
D1(config-if)#switchport mode access	Se indica que se va a configurar el modo de acceso.
D1(config-if)#switchport access vlan 100	Se asigna la vlan 100.

D1(config-if)#no shutdown	Se activa la interface.

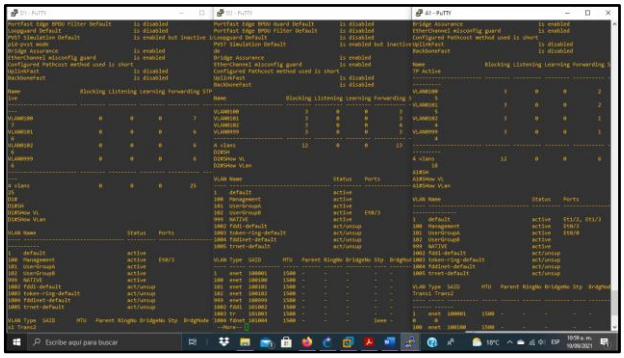
Configuración puerto de acceso A1:

A1(config)#interface Ethernet 0/0	Se accede a configurar la interface E0/0.
A1(config-if)#switchport mode Access	Se indica que se va a configurar el modo de acceso.
A1(config-if)#switchport access vlan 101	Se asigna la vlan 101.
A1(config-if)#no shutdown	Se activa la interface.
A1(config)#interface Ethernet 0/3	Se accede a configurar la interface E0/3.
A1(config-if)#switchport mode access	Se indica que se va a configurar el modo de acceso.
A1(config-if)#switchport access vlan 100	Se asigna la vlan 100.
A1(config-if)#no shutdown	Se activa la interface

Configuración puerto de acceso D2:

D2(config)#interface Ethernet 0/3	Se accede a configurar la interface E0/3.
D2(config-if)#switchport mode access	Se indica que se va a configurar el modo de acceso.
D2(config-if)#switchport access vlan 102	Se asigna la vlan 102.
D2(config-if)#no shutdown	Se activa la interface.

Figura 15. Verificación de la configuración de los puertos de acceso con la VLAN y los puertos quedan en estado de reenvío.

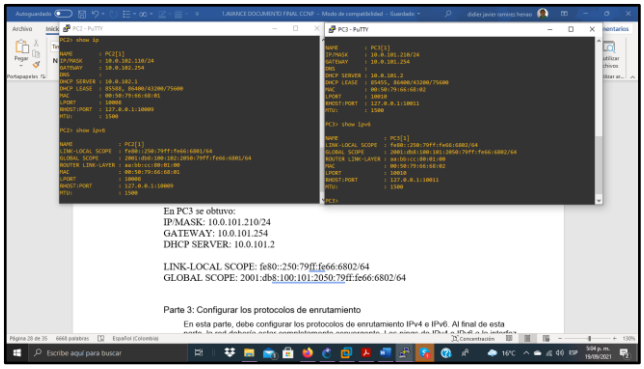


Desarrollo de la tarea 2.7

Se emplea el comando “ip dhcp” en PC2 y PC3 para obtener las direcciones ip válidas.
En PC2 se obtuvo:
IP/MASK: 10.0.102.110/24
GATEWAY: 10.0.102.254
DHCP SERVER: 10.0.102.1
LINK-LOCAL SCOPE: fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE: 2001:db8:100:102:2050:79ff:fe66:6801/64

En PC3 se obtuvo:
IP/MASK: 10.0.101.210/24
GATEWAY: 10.0.101.254
DHCP SERVER: 10.0.101.2
LINK-LOCAL SCOPE: fe80::250:79ff:fe66:6802/64
GLOBAL SCOPE: 2001:db8:100:101:2050:79ff:fe66:6802/64

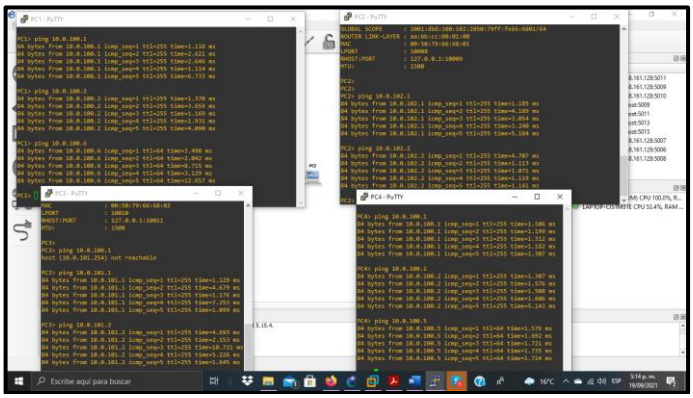
Figura 16. Verificación de los servicios DHCP en PC2 y PC3.



Desarrollo de la tarea 2.8

Todos los ping fueron exitosos:

Figura 17. Evidencia de los ping realizados.



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 10. Lista de tareas de configuración de protocolos de enrutamiento.

Tarea #	Tarea	Especificación
3.1	En la “Red de la Compañia” (es decir,R1, R3, D1, y D2), configure single- area OSPFv2 en area 0.	Use OSPF Process ID **4** y asigne los siguientes router-IDs: R1: 0.0.4.1 R3: 0.0.4.3 D1: 0.0.4.131 D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redesdirectamente 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 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 redesdirectamente conectadas / VLANs en Area 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

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.

Desarrollo de la tarea 3.1

Configuración de R1:

R1(config)#router ospf 4	Se ingresa a configurar OSPF indicando el id del proceso (4).
R1(config-router)#router-id 0.0.4.1	Se asigna el router id a R1.
R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 R1(config-router)#network 10.0.13.0 0.0.0.255 area 0	Se anuncian las redes directamente conectadas a R1 a excepción de la red 209.165.200.224 que está entre R1 – R2, para definir las interfaces que van a participar en OSPF, delimitando el área.
R1(config-router)#default-information originate	Se ordena a R1 para que de origen a la información de la ruta predeterminada y para que la ruta estática predeterminada se propague al actualizarse OSPF.

Configuración de R3:

R3(config)#router ospf 4	Se ingresa a configurar OSPF indicando el id del proceso (4).
R3(config-router)#router-id 0.0.4.3	Se asigna el router id a R3.
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0 R3(config-router)#network 10.0.13.0 0.0.0.255 area 0	Se anuncian las redes directamente conectadas a R3, para definir las interfaces que van a participar en OSPF, delimitando el área.

Configuración de D1:

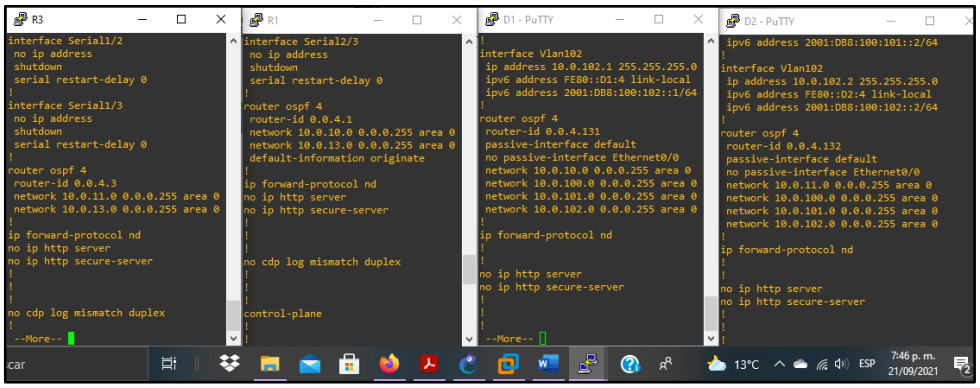
D1(config)#router ospf 4	Se ingresa a configurar OSPF indicando el id del proceso (4).
D1(config-router)#router-id 0.0.4.131	Se asigna el router id a D1.
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0 D1(config-router)#network 10.0.100.0 0.0.0.255 area 0 D1(config-router)#network 10.0.101.0 0.0.0.255 area 0 D1(config-router)#network 10.0.102.0 0.0.0.255 area 0	Se anuncian las redes directamente conectadas a D1, para definir las interfaces que van a participar en OSPF, delimitando el área.
D1(config-router)#passive-interface default	Todas las interfaces de D1 se colocan en estado pasivo para OSPF y así no

	se tienen publicaciones OSPFv2.
D1(config-router)# no passive-interface ethernet 0/0	La única interface que se habilita para OSPFv2 es la ethernet 0/0.

Configuración de D2:

D2(config)#router ospf 4	Se ingresa a configurar OSPF indicando el id del proceso (4).
D2(config-router)#router-id 0.0.4.131	Se asigna el router id a D2.
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0 D2(config-router)#network 10.0.100.0 0.0.0.255 area 0 D2(config-router)#network 10.0.101.0 0.0.0.255 area 0 D2(config-router)#network 10.0.102.0 0.0.0.255 area 0	Se anuncian las redes directamente conectadas a D2, para definir las interfaces que van a participar en OSPF, delimitando el área.
D2(config-router)#passive-interface default	Todas las interfaces de D2 se colocan en estado pasivo para OSPF y así no se tienen publicaciones OSPFv2.
D2(config-router)# no passive-interface ethernet 0/0	La única interface que se habilita para OSPFv2 es la ethernet 0/0.

Figura 18. Comando show running-config para verificar la configuración de OSPFv2 área 0 en la red de la compañía en R1, R3, D1 y D2.



Desarrollo de la tarea 3.2

Configuración de R1:

R1(config)#ipv6 router ospf 6	Se ingresa a configurar OSPFv3 indicando el id del proceso (6).
R1(config-rtr)# router-id 0.0.6.1	Se asigna el router id a R1.
R1(config-rtr)# default-information originate	Se ordena a R1 para que de origen a la información de la ruta predeterminada y para que la ruta estática predeterminada se propague al actualizarse OSPF.
R1(config-rtr)# exit	
R1(config)#interface gigabitEthernet 1/0	Se accede a la interface gi1/0.
R1(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface en el área 0.
R1(config-if)# exit	
R1(config)#interface serial 2/0	Se accede a la interface se2/0.
R1(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
R1(config-if)# exit	La interface entre R1 y R2 (G0/0) no se habilitó.

Configuración de R3:

R3(config)#ipv6 router ospf 6	Se ingresa a configurar OSPFv3 indicando el id del proceso (6).
R3(config-rtr)# router-id 0.0.6.3	Se asigna el router id a R3.
R3(config-rtr)# exit	
R3(config)#interface gigabitEthernet 0/0	Se accede a la interface gi0/0.
R3(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface en el área 0.
R3(config-if)# exit	
R3(config)#interface serial 1/0	Se accede a la interface se1/0.
R3(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
R3(config-if)# exit	

Configuración de D1:

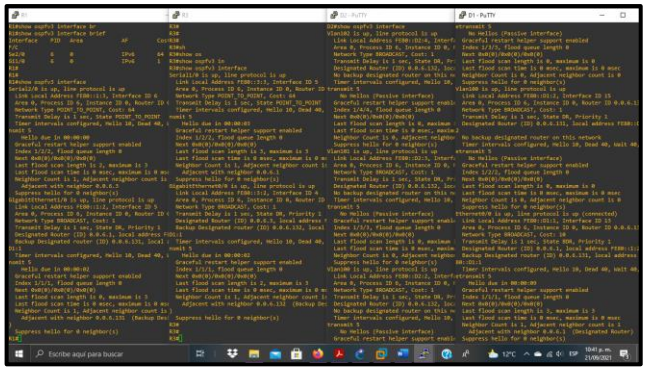
D1(config)#ipv6 router ospf 6	Se ingresa a configurar OSPFv3 indicando el id del proceso (6).
D1(config-rtr)# router-id 0.0.6.131	Se asigna el router id a D1.
D1(config-rtr)# passive-interface default	Todas las interfaces de D1 se colocan en estado pasivo para OSPF y así no se tienen publicaciones OSPFv3.
D1(config-rtr)# no passive-interface	La única interface que se habilita para

ethernet 0/0	anunciar OSPFv3 es la ethernet 0/0.
D1(config-rtr)#exit	
D1(config)#interface ethernet 0/0	Se accede a la interface Et0/0.
D1(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface en
D1(config-if)# exit	el área 0.
D1(config)#interface vlan 100	Se accede a la interface vlan 100.
D1(config-if)# ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
D1(config-if)# exit	
D1(config)#interface vlan 101	Se accede a la interface vlan 101.
D1(config-if)# ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
D1(config-if)# exit	
D1(config)#interface vlan 102	Se accede a la interface vlan 102.
D1(config-if)# ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
D1(config-if)# exit	

Configuración de D2:

D2(config)#ipv6 router ospf 6	Se ingresa a configurar OSPFv3 indicando el id del proceso (6).
D2(config-rtr)# router-id 0.0.6.132	Se asigna el router id a D2.
D2(config-rtr)# passive-interface default	Todas las interfaces de D1 se colocan en estado pasivo para OSPF y así no se tienen publicaciones OSPFv3.
D2(config-rtr)# no passive-interface ethernet 0/0	La única interface que se habilita para anunciar OSPFv3 es la ethernet 0/0.
D2(config-rtr)#exit	
D2(config)#interface ethernet 0/0	Se accede a la interface Et0/0.
D2(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface en
D2(config-if)# exit	el área 0.
D2(config)#interface vlan 100	Se accede a la interface vlan 100.
D2(config-if)# ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
D2(config-if)# exit	
D2(config)#interface vlan 101	Se accede a la interface vlan 101.
D2(config-if)# ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
D2(config-if)# exit	
D2(config)#interface vlan 102	Se accede a la interface vlan 102.
D2(config-if)# ipv6 ospf 6 area 0	Se habilita OSPFv6 para la interface.
D2(config-if)# exit	

Figura 19. Comando "show ospfv3 interface", para verificar la correcta implementación de OSPFv3 área 0 en la red de la compañía.



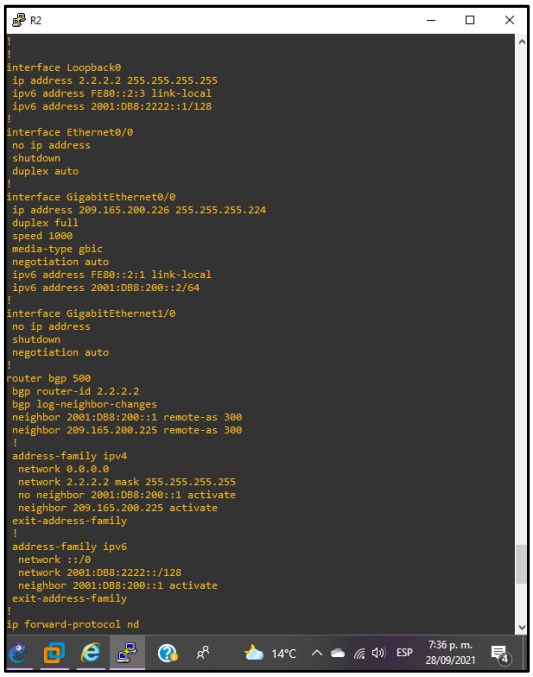
Desarrollo de la tarea 3.3

Configuración de MP-BGP en la red ISP de R2.

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0	Se configura la ruta estática ipv4 predeterminada a través de la interface loopback 0.
R2(config)#ipv6 route ::/0 loopback 0	Se configura la ruta estática ipv6 predeterminada a través de la interface loopback 0.
R2(config)#router bgp 500	Se define el proceso BGP en R2 y el número de ASN al que pertenece.
R2(config-router)# bgp router-id 2.2.2.2	Se asigna el id del protocolo BGP.
R2(config-router)# neighbor 209.165.200.225 remote-as 300	Se configura la relación de vecino IPv4 e IPv6 con R1 en ASN 300.
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300	
R2(config-router)# address-family ipv4	Se accede a la familia de direcciones ipv4.
R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255	Se anuncia la red loopback 0 ipv4 (/32).
R2(config-router-af)# network 0.0.0.0	Se anuncia la ruta por defecto.
R2(config-router-af)# exit-address-family	Se sale de la configuración de la familia de direcciones ipv4.
R2(config-router)# address-family ipv6	Se accede a la familia de direcciones ipv6.
R2(config-router-af)# network 2001:db8:2222::/128	En IPv6 address family se anuncia la red Loopback 0 IPv4 (/128).
R2(config-router-af)# network ::/0	En IPv6 address family se anuncia la ruta por defecto (::/0).

R2(config-router-af)# exit-address-family R2(config-router)#	Se sale de la configuración de la familia de direcciones ipv6.

Figura 20. Show running config para verificar la configuración de MP-BGP en R2.



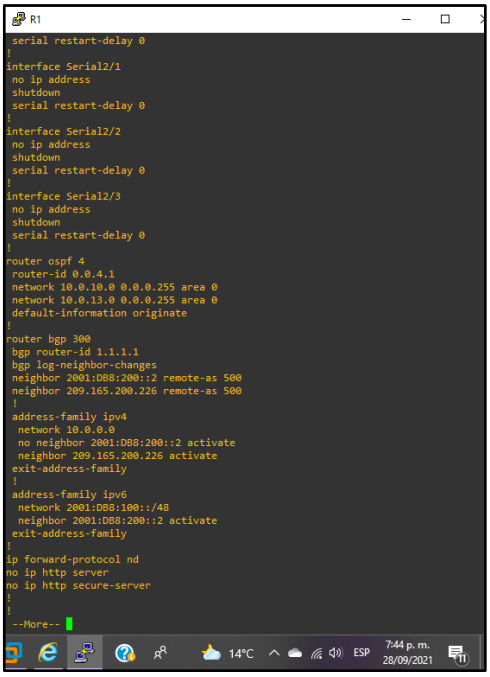
Desarrollo de la tarea 3.4

Configuración de MP-BGP en la red ISP de R1.

R1(config)#ip route 10.0.0.0 255.0.0.0 null0	Se configura la ruta resumen ipv4 a la interface Null0.
R1(config)#ipv6 route 2001:db8:100::/48 null0	Se configura la ruta resumen ipv6 a la interface Null0.
R1(config)#router bgp 300	Se define el proceso BGP en R1 y el número de ASN al que pertenece.
R1(config-router)#bgp router-id 1.1.1.1	Se asigna el id del protocolo BGP.
R1(config-router)#neighbor 209.165.200.226 remote-as 500 R1(config-router)#neighbor 2001:db8:200::2 remote-as 500	Se configure la relación de vecino IPv4 e IPv6 con R2 en ASN 500.
R1(config-router)#address-family ipv4 unicast	Se accede a la familia de direcciones ipv4 unicast.
R1(config-router-af)#neighbor 209.165.200.226 activate	Se activa la relación de vecino ipv4 con 209.165.200.226.
R1(config-router-af)#no neighbor	Se desactiva la relación de vecino ipv6.

2001:db8:200::2 activate	con 2001:db8:200::2.
R1(config-router-af)#network 10.0.0.0 mask 255.0.0.0	Se anuncia la red 10.0.0.0/8.
R1(config-router-af)#exit-address-family	Se sale de la configuración de la familia de direcciones ipv4.
R1(config-router)#address-family ipv6 unicast	Se accede a la familia de direcciones ipv6 unicast.
R1(config-router-af)#no neighbor 209.165.200.226 activate	Se desactiva la relación de vecino ipv4 con 209.165.200.226.
R1(config-router-af)#neighbor 2001:db8:200::2 activate	Se activa la relación de vecino ipv6 con 2001:db8:200::2.
R1(config-router-af)#network 2001:db8:100::/48	Se anuncia la red 2001:db8:100::/48.
R1(config-router-af)#exit-address-family	Se sale de la configuración de la familia de direcciones ipv6.

Figura 21. Show running config para verificar la configuración de MP-BGP en R1.



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

En esta parte, debe configurar HSRP version 2 para proveer redundancia de primer salto para los hosts en la “Red de la Compañia”.

Las tareas de configuración son las siguientes:

Tabla 11. Lista de tareas parte 4 (Configurar la redundancia del primer salto).

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.
4.3	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**. Establezca la prioridad del grupo en 150. Habilite la preferencia (preemption). Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: Asigne la dirección IP virtual usando **ipv6 autoconfig**. Habilite la preferencia (preemption). Rastree el objeto 6 para disminuir en 60.

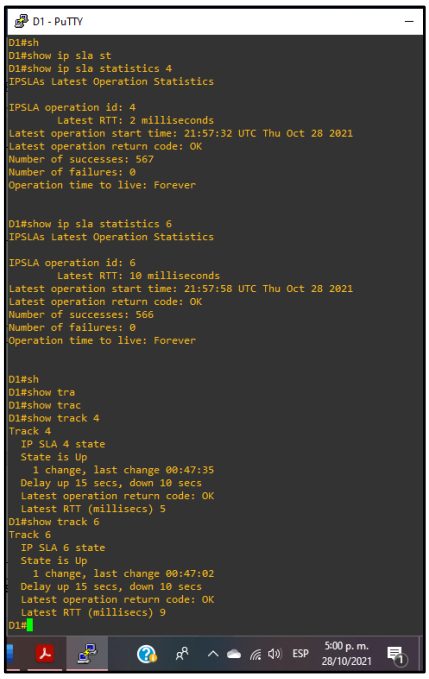
Desarrollo de la tarea 4.1

En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.
Para nuestro caso, la interfaz es la R1 G1/0.

D1(config)#ip sla 4	Se define el número de sesión 4 del SLA
D1(config-ip-sla)#icmp-echo 10.0.10.1	Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv4 G1/0 de R1.
D1(config-ip-sla-echo)#frequency 5 D1(config-ip-sla-echo)#exit	Se prueba la disponibilidad de la interfaz G1/0 de R1 cada 5 segundos.
D1(config)#ip sla 6	Se define el número de sesión 6 del SLA.
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1	Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv6 G1/0 de R1.
D1(config-ip-sla-echo)#frequency 5 D1(config-ip-sla-echo)#exit	Se prueba la disponibilidad de la interfaz G1/0 de R1 cada 5 segundos
D1(config)#ip sla schedule 4 life forever start-time now	Se programa la SLA 4 para una implementación inmediata sin tiempo de finalización.
D1(config)#ip sla schedule 6 life forever start-time now	Se programa la SLA 6 para una implementación inmediata sin tiempo de finalización.
D1(config)#track 4 ip sla 4	Se crea el número de rastreo 4 y se asocia al IP SLA 4.
D1(config-track)#delay down 10 up 15	Cada 10 segundos se debe notificar el

D1(config-track)#exit	cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando para de up a down.
D1(config)#track 6 ip sla 6	Se crea el número de rastreo 6 y se asocia al IP SLA 6.
D1(config-track)#delay down 10 up 15	Cada 10 segundos se debe notificar el
D1(config-track)#exit	cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando pasa de up a down.

Figura 22. Validación del estado de las IP SLA y de los track en D1.



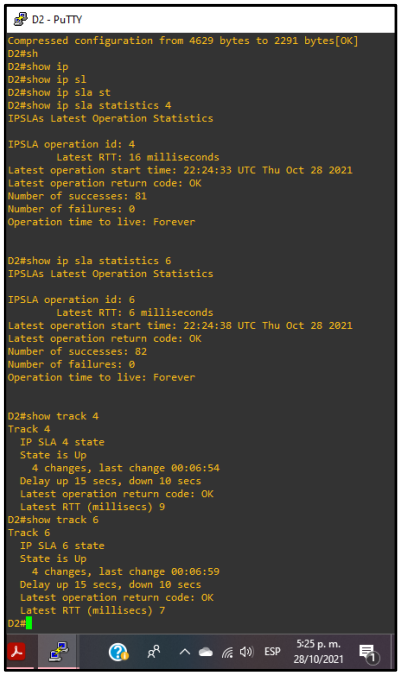
Desarrollo de la tarea 4.2

En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1. Para nuestro caso, la interfaz es la R3 G0/0.

D2(config)#ip sla 4	Se define el número de sesión 4 del SLA.
D2(config-ip-sla)#icmp-echo 10.0.11.1	Se inicia la configuración IP SLA ICMP Echo con destino a la interfaz ipv4 G0/0 de R3.
D2(config-ip-sla-echo)#frequency 5	Se prueba la disponibilidad de la
D2(config-ip-sla-echo)#exit	interfaz G0/0 de R3 cada 5 segundos.
D2(config)#ip sla 6	Se define el número de sesión 6 del SLA.
D2(config-ip-sla)# icmp-echo	Se inicia la configuración IP SLA ICMP

2001:db8:100:1011::1	Echo con destino a la interfaz ipv6 G0/0 de R3.
D2(config-ip-sla-echo)# frequency 5 D2(config-ip-sla-echo)#exit	Se prueba la disponibilidad de la interfaz G1/0 de R1 cada 5 segundos.
D2(config)#ip sla schedule 4 life forever start-time now	Se programa la SLA 4 para una implementación inmediata sin tiempo de finalización.
D2(config)#ip sla schedule 6 life forever start-time now	Se programa la SLA 6 para una implementación inmediata sin tiempo de finalización.
D2(config)#track 4 ip sla 4	Se crea el número de rastreo 4 y se asocia al IP SLA 4.
D2(config-track)# delay down 10 up 15 D2(config-track)# exit	Cada 10 segundos se debe notificar el cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando pasa de up a down.
D2(config)#track 6 ip sla 6	Se crea el número de rastreo 6 y se asocia al IP SLA 6
D2(config-track)# delay down 10 up 15 D2(config-track)# exit	Cada 10 segundos se debe notificar el cambio de estado de la IP SLA cuando pasa de down a up y cada 15 segundos cuando para de up a down

Figura 23. Validación del estado de las IP SLA y de los track en D2.



Desarrollo de la tarea 4.3

Configurando HSRPv2 en D1.

D1(config)#interface vlan 100	Se accede a la interfaz VLAN 100.
D1(config-if)# standby version 2	Se configura el HSRP para usar la versión 2.
D1(config-if)# standby 104 ip 10.0.100.254	Se inicia la configuración IPv4 HSRP grupo 104 para la VLAN 100, asignando la ip virtual 10.0.100.254.
D1(config-if)# standby 104 priority 150	Se establece la prioridad del grupo 104 en 150.
D1(config-if)# standby 104 preempt	Se habilita la preferencia al grupo 104
D1(config-if)#standby 104 track 4 decrement 60	Se rastrea el objeto 4 y se decrementa en 60.
D1(config-if)#standby 106 ipv6 autoconfig	Se inicia la configuración IPv6 HSRP grupo 106 para la VLAN 100. Se asigna la dirección IP virtual usando ipv6 autoconfig .
D1(config-if)# standby 106 priority 150	Se establece la prioridad del grupo en 150.
D1(config-if)# standby 106 preempt	Se habilita la preferencia al grupo 106
D1(config-if)#standby 106 track 6 decrement 60	Se rastrea el objeto 6 y se decrementa en 60.
D1(config-if)# exit	
D1(config)#interface vlan 101	Se accede a la interfaz VLAN 101.
D1(config-if)# standby version 2	Se configura el HSRP para usar la versión 2.
D1(config-if)#standby 114 ip 10.0.101.254	Se inicia la configuración IPv4 HSRP grupo 114 para la VLAN 101, asignando la ip virtual 10.0.101.254.
D1(config-if)# standby 114 preempt	Se habilita la preferencia al grupo 114.
D1(config-if)#standby 114 track 4 decrement 60	Se rastrea el objeto 4 y se decrementa en 60.
D1(config-if)#standby 116 ipv6 autoconfig	Se inicia la configuración IPv6 HSRP grupo 116 para la VLAN 101. Se asigna la dirección IP virtual usando ipv6 autoconfig.
D1(config-if)# standby 116 preempt	Se habilita la preferencia al grupo 116.
D1(config-if)#standby 116 track 6 decrement 60	Se rastrea el objeto 6 y se decrementa en 60.
D1(config-if)# exit	
D1(config)#interface vlan 102	Se accede a la interfaz VLAN 102.
D1(config-if)# standby version 2	Se configura el HSRP para usar la versión 2.

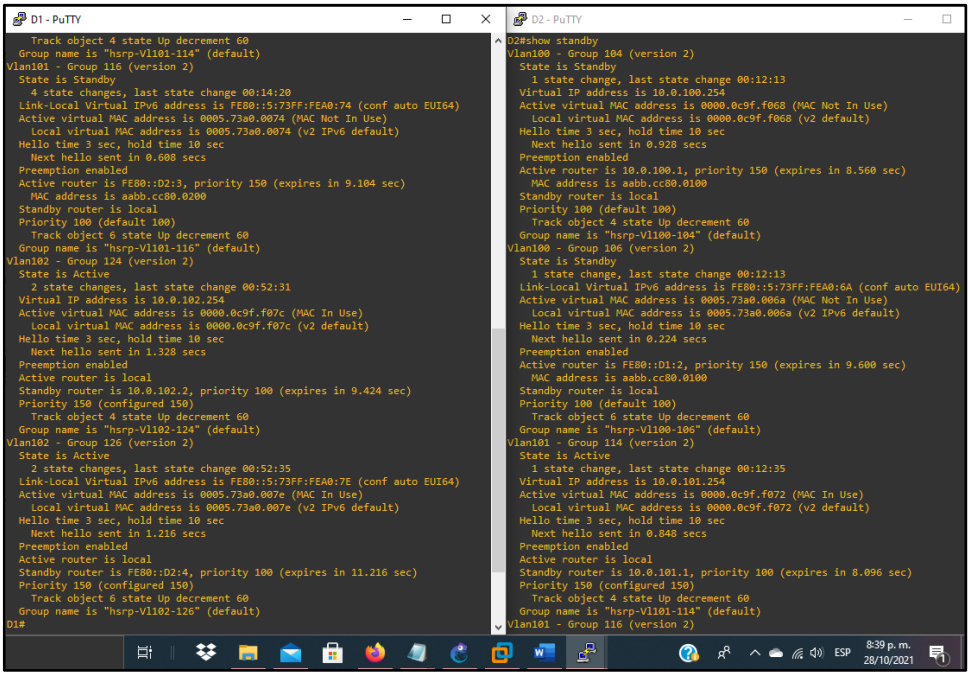
D1(config-if)# standby 124 ip 10.0.102.254	Se inicia la configuración IPv4 HSRP grupo 124 para la VLAN 102, asignando la ip virtual 10.0.102.254.
D1(config-if)# standby 124 priority 150	Se establece la prioridad del grupo 124 en 150.
D1(config-if)# standby 124 preempt	Se habilita la preferencia al grupo 124.
D1(config-if)# standby 124 track 4 decrement 60	Se rastrea el objeto 4 y se decrementa en 60.
D1(config-if)# standby 126 ipv6 autoconfig	Se inicia la configuración IPv6 HSRP grupo 126 para la VLAN 102. Se asigna la dirección IP virtual usando ipv6 autoconfig.
D1(config-if)# standby 126 priority 150	Se establece la prioridad del grupo en 150.
D1(config-if)# standby 126 preempt	Se habilita la preferencia al grupo 126.
D1(config-if)#standby 126 track 6 decrement 60	Se rastrea el objeto 6 y se decrementa en 60.
D1(config-if)# exit	

Configurando HSRPv2 en D2.

D2(config)#interface vlan 100	Se accede a la interfaz VLAN 100.
D2(config-if)# standby version 2	Se configura el HSRP para usar la versión 2.
D2(config-if)#standby 104 ip 10.0.100.254	Se inicia la configuración IPv4 HSRP grupo 104 para la VLAN 100, asignando la ip virtual 10.0.100.254.
D2(config-if)# standby 104 preempt	Se habilita la preferencia al grupo 104.
D2(config-if)#standby 104 track 4 decrement 60	Se rastrea el objeto 4 y se decrementa en 60.
D2(config-if)#standby 106 ipv6 autoconfig	Se inicia la configuración IPv6 HSRP grupo 106 para la VLAN 100. Se asigna la dirección IP virtual usando ipv6 autoconfig.
D2(config-if)# standby 106 preempt	Se habilita la preferencia al grupo 106.
D2(config-if)#standby 106 track 6 decrement 60	Se rastrea el objeto 6 y se decrementa en 60.
D2(config-if)# exit	
D2(config)#interface vlan 101	Se accede a la interfaz VLAN 101.
D2(config-if)# standby version 2	Se configura el HSRP para usar la versión 2.
D2(config-if)#standby 114 ip 10.0.101.254	Se inicia la configuración IPv4 HSRP grupo 114 para la VLAN 101, asignando la ip virtual 10.0.101.254.
D2(config-if)# standby 114 priority 150	Se establece la prioridad del grupo en

	150.
D2(config-if)# standby 114 preempt	Se habilita la preferencia al grupo 114.
D2(config-if)#standby 114 track 4 decrement 60	Se rastrea el objeto 4 y se decrementa en 60.
D2(config-if)#standby 116 ipv6 autoconfig	Se inicia la configuración IPv6 HSRP grupo 116 para la VLAN 101. Se asigna la dirección IP virtual usando ipv6 autoconfig.
D2(config-if)# standby 116 priority 150	Se establece la prioridad del grupo en 150.
D2(config-if)# standby 116 preempt	Se habilita la preferencia al grupo 116.
D2(config-if)#standby 116 track 6 decrement 60	Se rastrea el objeto 6 y se decrementa en 60.
D2(config-if)# exit	
D2(config)#interface vlan 102	Se accede a la interfaz VLAN 102.
D2(config-if)# standby version 2	Se configura el HSRP para usar la versión 2.
D2(config-if)#standby 124 ip 10.0.102.254	Se inicia la configuración IPv4 HSRP grupo 124 para la VLAN 102, asignando la ip virtual 10.0.102.254.
D2(config-if)# standby 124 preempt	Se habilita la preferencia al grupo 124.
D2(config-if)#standby 124 track 4 decrement 60	Se rastrea el objeto 4 y se decrementa en 60.
D2(config-if)#standby 126 ipv6 autoconfig	Se inicia la configuración IPv6 HSRP grupo 126 para la VLAN 102. Se asigna la dirección IP virtual usando ipv6 autoconfig.
D2(config-if)# standby 126 preempt	Se habilita la preferencia al grupo 126.
D2(config-if)#standby 126 track 6 decrement 60	Se rastrea el objeto 6 y se decrementa en 60.
D2(config-if)# exit	

Figura 24. Verificación de la implementación de HSRPv2 en D1 y D2 con el comando "show standby".



Parte 5: Seguridad

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

Las tareas de configuración son las siguientes:

Tabla 12. Lista de tareas parte 5. (Seguridad).

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**.

Desarrollo de la tarea 5.1

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

Para R1: R1(config)#enable algorithm-type scrypt secret cisco12345cisco

Para R2: R2(config)#enable algorithm-type scrypt secret cisco12345cisco

Para R3: R3(config)#enable algorithm-type scrypt secret cisco12345cisco

Para D1: D1(config)#enable algorithm-type scrypt secret cisco12345cisco

Para D2: D2(config)#enable algorithm-type scrypt secret cisco12345cisco

Para A1 A1(config)#enable algorithm-type scrypt secret cisco12345cisco

Desarrollo de la tarea 5.2

En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.

Para R1: R1(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

Para R2: R2(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

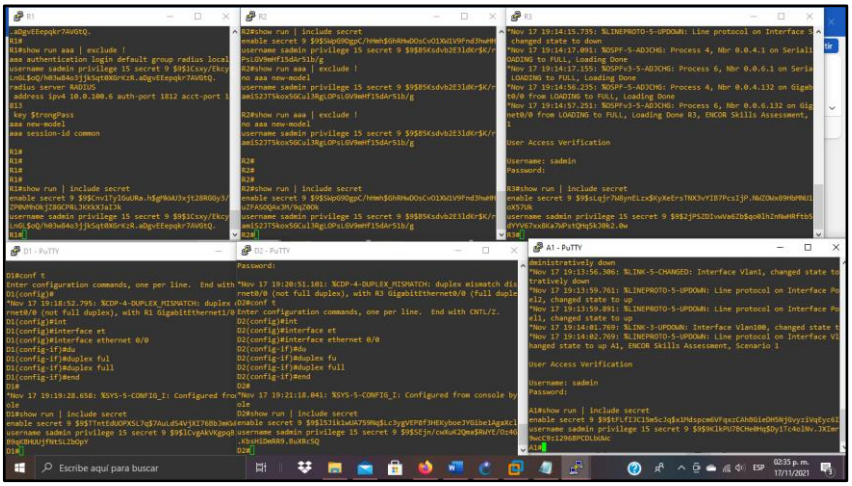
Para R3: R3(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

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

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

Para A1 A1(config)# username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco

Figura 25. Verificación de los puntos 5.1 y 5.2 con el comando "show run | include secret".



En la figura 25, se evidencia que se han configurado todos los dispositivos, protegiendo el EXEC privilegiado y usando el algoritmo de encripción SCRYPT. También todos los dispositivos, tienen creado un usuario local y está protegido usando el algoritmo de encripción SCRYPT.

Desarrollo de la tarea 5.3

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

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

Desarrollo de la tarea 5.4

En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

R1(config)#radius server RADIUS	Se inicia la configuración del servidor RADIUS en R1.
R1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813	Se especifica la dirección IP y los puertos UDP para R1.
R1(config-radius-server)# key $trongPass	Se asigna la contraseña al servidor RADIUS para R1.
R1(config-radius-server)# exit	
R3(config)#radius server RADIUS	Se inicia la configuración del servidor RADIUS en R3.
R3(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813	Se especifica la dirección IP y los puertos UDP para R3.
R3(config-radius-server)# key $trongPass	Se asigna la contraseña al servidor RADIUS para R3.
R3(config-radius-server)# exit	
D1(config)#radius server RADIUS	Se inicia la configuración del servidor RADIUS en D1.

D1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813	Se especifica la dirección IP y los puertos UDP para D1.
D1(config-radius-server)# key $trongPass	Se asigna la contraseña al servidor RADIUS para D1.
D1(config-radius-server)# exit	
D2(config)#radius server RADIUS	Se inicia la configuración del servidor RADIUS en D2.
D2(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813	Se especifica la dirección IP y los puertos UDP para D2.
D2(config-radius-server)# key $trongPass	Se asigna la contraseña al servidor RADIUS para D2.
D2(config-radius-server)# exit	
A1(config)#radius server RADIUS	Se inicia la configuración del servidor RADIUS en A1.
A1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812 acct-port 1813	Se especifica la dirección IP y los puertos UDP para A1.
A1(config-radius-server)# key $trongPass	Se asigna la contraseña al servidor RADIUS para A1.
A1(config-radius-server)# exit	

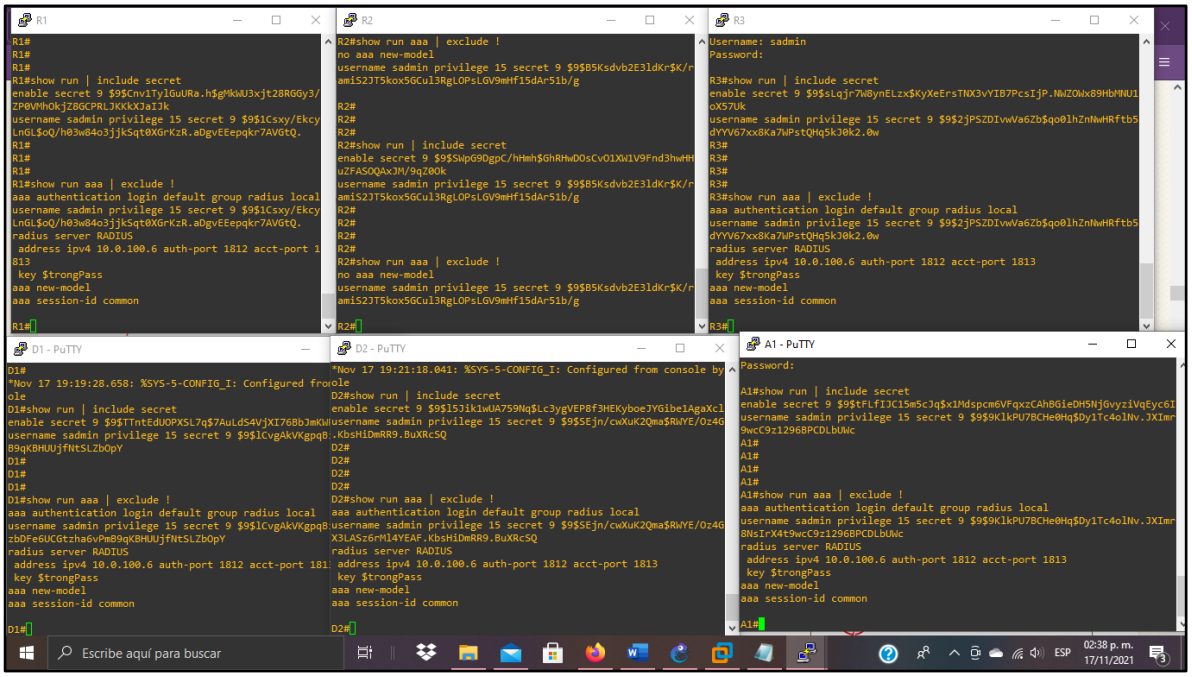
Desarrollo de la tarea 5.5

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

R1(config)#aaa authentication login default group radius local	Se configura la lista de métodos de autenticación AAA en R1. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método).
R3(config)#aaa authentication login default group radius local	Se configura la lista de métodos de autenticación AAA en R3. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método).
D1(config)#aaa authentication login default group radius	Se configura la lista de métodos de autenticación AAA en D1. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se

local	utiliza la base de datos local del router (el segundo método).
D2(config)#aaa authentication login default group radius local	Se configura la lista de métodos de autenticación AAA en D2. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método).
A1(config)#aaa authentication login default group radius local	Se configura la lista de métodos de autenticación AAA en A1. Se usa la lista de métodos por defecto (default). La autenticación de todos los usuarios se hace usando el servidor Radius (el primer método). Si no responde el servidor de RADIUS, después se utiliza la base de datos local del router (el segundo método).

Figura 26. Comando "show run aaa | exclude !" para verificar las tareas 5.3, 5.4 y 5.5.

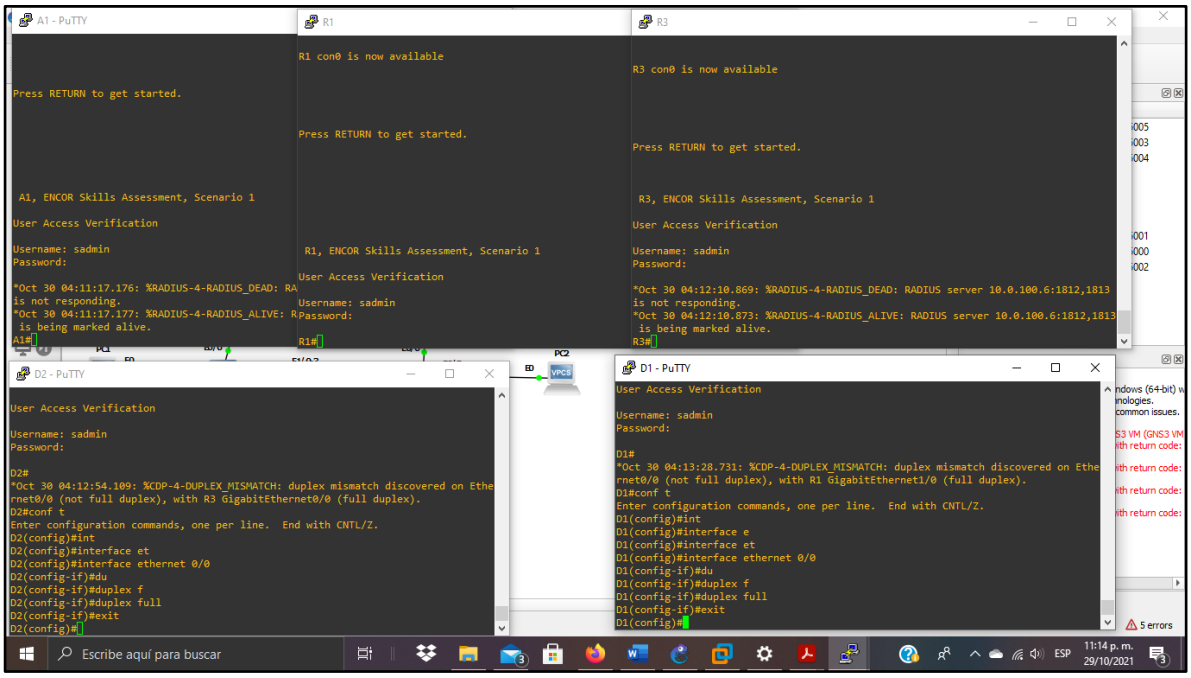


En la figura 26 se observa que, en todos los dispositivos, excepto R2, se habilitó AAA, se configuraron las especificaciones del servidor RADIUS y se configuró la lista de métodos de autenticación AAA.

Desarrollo de la tarea 5.6

Verifique el servicio AAA en todos los dispositivos (except R2).

Figura 27. Verificación del servicio AAA en los dispositivos (excepto R2).



Como se observa en la figura 25, se ha cerrado e iniciado sesión en R1, R3, D1, D2 y A1. En R1, D1 y D2 respondió el servidor RADIUS; en R3 y A1 respondió el servidor local.

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 13. Lista de tareas parte 6. Configure las funciones de administración de red.

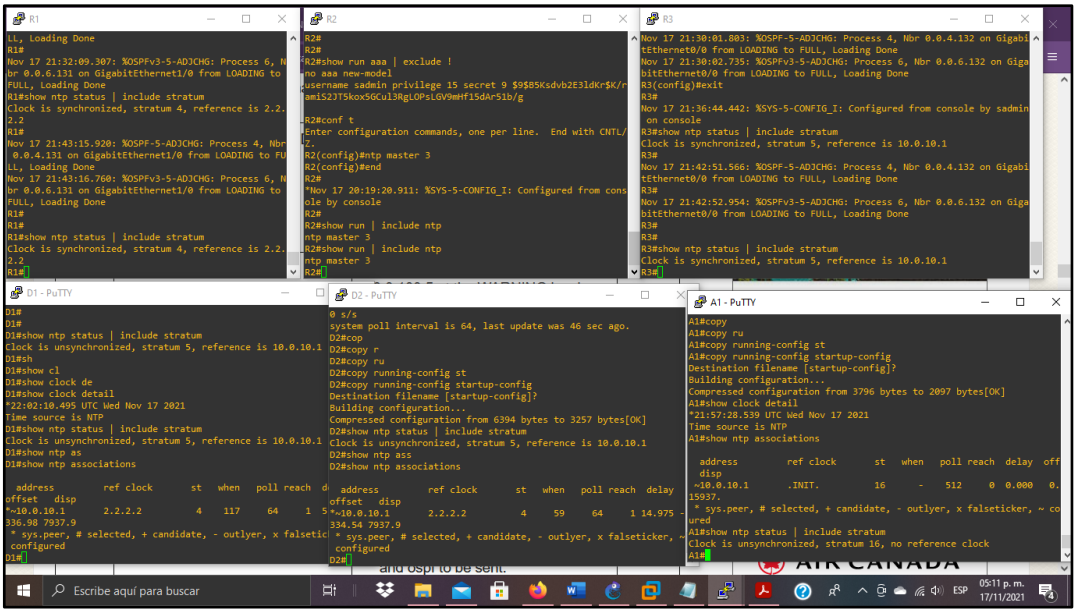
Tarea #	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure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

Desarrollo de la tarea 6.1, 6.2 y 6.3

R1(config)#ntp server 2.2.2.2	Se configura el reloj local de R1 a la hora UTC actual. Para ello se configura NTP para que R1 se sincronice por medio de la interfaz loopback 0 de R2.
R3(config)#ntp server 10.0.10.1	Se configura el reloj local de R3 a la hora UTC actual. Para ello se configura NTP para que R3 se sincronice por medio de la interfaz G1/0 de R1.
D1(config)#ntp server	Se configura el reloj local de D3 a la hora UTC actual.

10.0.10.1	Para ello se configura NTP para que R3 se sincronice por medio de la interfaz G1/0 de R1.
A1(config)#ntp server	Se configura el reloj local de A1 a la hora UTC actual.
10.0.10.1	Para ello se configura NTP para que R3 se sincronice por medio de la interfaz G1/0 de R1.
D2(config)#ntp server	Se configura el reloj local de D2 a la hora UTC actual.
10.0.10.1	Para ello se configura NTP para que D2 se sincronice por medio de la interfaz G0/0 de R3.
R2(config)#ntp master 3	Se configura R2 como NTP maestro en el nivel de estrato 3.

Figura 28. Verificación de la configuración de NTP en los equipos.



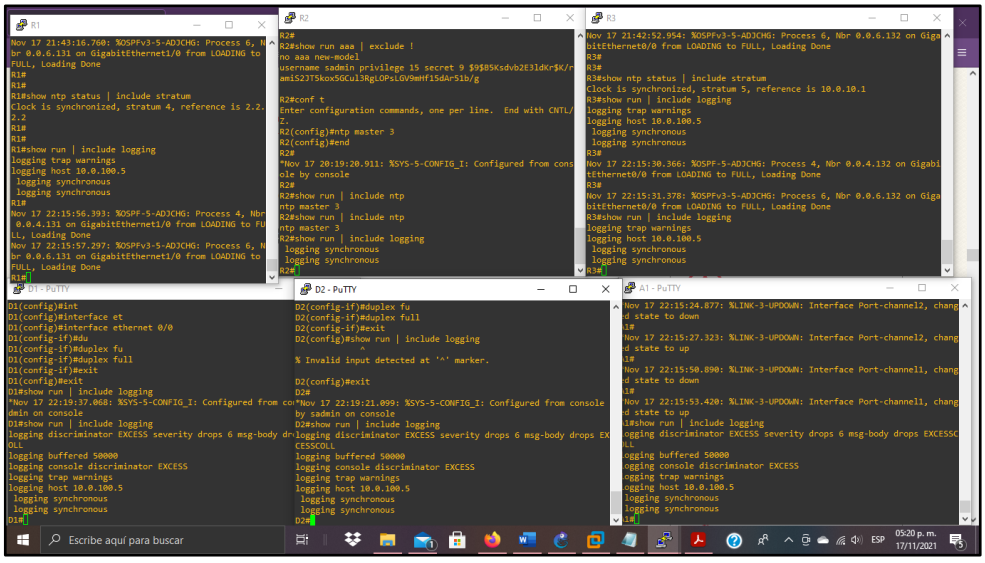
Desarrollo de la tarea 6.4

Configure Syslog en todos los dispositivos excepto R2

R1(config)# logging host 10.0.100.5	Se configura el host PC1 para que sea el host de registro de destino para R1.
R1(config)#logging trap warning	Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.
R1(config)#logging on	Se habilita el registro para que los mensajes puedan ser enviados.
R3(config)# logging host 10.0.100.5	Se configura el host PC1 para que sea el host de registro de destino para R3.
R3(config)#logging trap warning	Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de

	advertencia.
R3(config)# logging on	Se habilita el registro para que los mensajes puedan ser enviados.
D1(config)# logging host 10.0.100.5	Se configura el host PC1 para que sea el host de registro de destino para D1.
D1(config)#logging trap warning	Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.
D1(config)# logging on	Se habilita el registro para que los mensajes puedan ser enviados.
D2(config)#logging host 10.0.100.5	Se configura el host PC1 para que sea el host de registro de destino para D2.
D2(config)#logging trap warning	Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.
D2(config)# logging on	Se habilita el registro para que los mensajes puedan ser enviados.
A1(config)#logging host 10.0.100.5	Se configura el host PC1 para que sea el host de registro de destino para A1.
A1(config)#logging trap warning	Se establece el nivel de prioridad del “trap” en el nivel 4 (warning) para brindar condiciones de advertencia.
A1(config)#logging on	Se habilita el registro para que los mensajes puedan ser enviados

Figura 29. Se verifica que syslog quedó configurado.



En la figura 29, se evidencia que syslog quedó configurado en todos los equipos, excepto en R2.

Desarrollo de la tarea 6.5

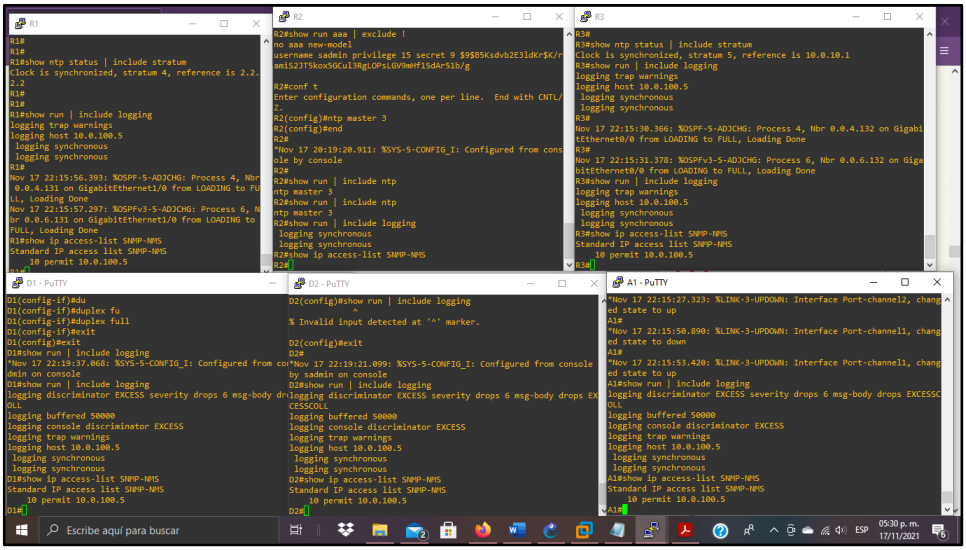
Configurando SNMPv2c en todos los dispositivos excepto R2

R1(config)# snmp-server community ENCORSA ro SNMP-NMS	Se establece el “community string” en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.
R1(config)#ip access-list standard SNMP-NMS R1(config-std-nacl)# permit host 10.0.100.5 R1(config-std-nacl)# exit	Se limita el acceso SNMP a la dirección IP de PC1.
R1(config)#snmp-server contact Didier Ramirez	Se configura el valor de contacto SNMP con mi nombre.
R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA	Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.
R1(config)#snmp-server enable traps bgp R1(config)# snmp-server enable traps config R1(config)#snmp-server enable traps ospf R1(config)#end	En R1, se habilita el envío de traps: bgp, config, y ospf.
R3(config)# snmp-server community ENCORSA ro SNMP-NMS	Se establece el “community string” en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.
R3(config)#ip access-list standard SNMP-NMS R3(config-std-nacl)# permit host 10.0.100.5 R3(config)# exit	Se limita el acceso SNMP a la dirección IP de PC1.
R3(config)# snmp-server contact Didier Ramirez	Se configura el valor de contacto SNMP con mi nombre.
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA	Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.
R3(config)# snmp-server enable traps config R3(config)# snmp-server enable traps ospf R3(config)#end	En R3, se habilita el envío de traps: config, y ospf..
D1(config)# snmp-server community ENCORSA ro SNMP-NMS	Se establece el “community string” en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.
D1(config)#ip access-list standard	Se limita el acceso SNMP a la dirección IP

SNMP-NMS D1(config-std-nacl)# permit host 10.0.100.5 D1(config-std-nacl)# exit	de PC1
D1(config)# snmp-server contact Didier Ramirez	Se configura el valor de contacto SNMP con mi nombre.
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA	Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.
D1(config)# snmp-server enable traps config D1(config)# snmp-server enable traps ospf D1(config)#end	En D1, se habilita el envío de traps: config, y ospf.
D2(config)#snmp-server community ENCORSA ro SNMP-NMS	Se establece el “community string” en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.
D2(config)#ip access-list standard SNMP-NMS D2(config-std-nacl)# permit host 10.0.100.5 D2(config-std-nacl)#exit	Se limita el acceso SNMP a la dirección IP de PC1.
D2(config)# snmp-server contact Didier Ramirez	Se configura el valor de contacto SNMP con mi nombre.
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA	Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.
D2(config)# snmp-server enable traps config D2(config)# snmp-server enable traps ospf end	En D2, se habilita el envío de traps: config, y ospf.
A1(config)#snmp-server community ENCORSA ro SNMP-NMS	Se establece el “community string” en ENCORSA y se especifica el uso de SNMPv2 como solo lectura.
A1(config)#ip access-list standard SNMP-NMS A1(config-std-nacl)# permit host 10.0.100.5 A1(config-std-nacl)#exit	Se limita el acceso SNMP a la dirección IP de PC1.
A1(config)# snmp-server contact Didier Ramirez	Se configura el valor de contacto SNMP con mi nombre.
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se especifica a PC1 como el destinatario de las operaciones de trap de SNMP.
A1(config)# snmp-server enable	En R3, se habilita el envío de traps: config.

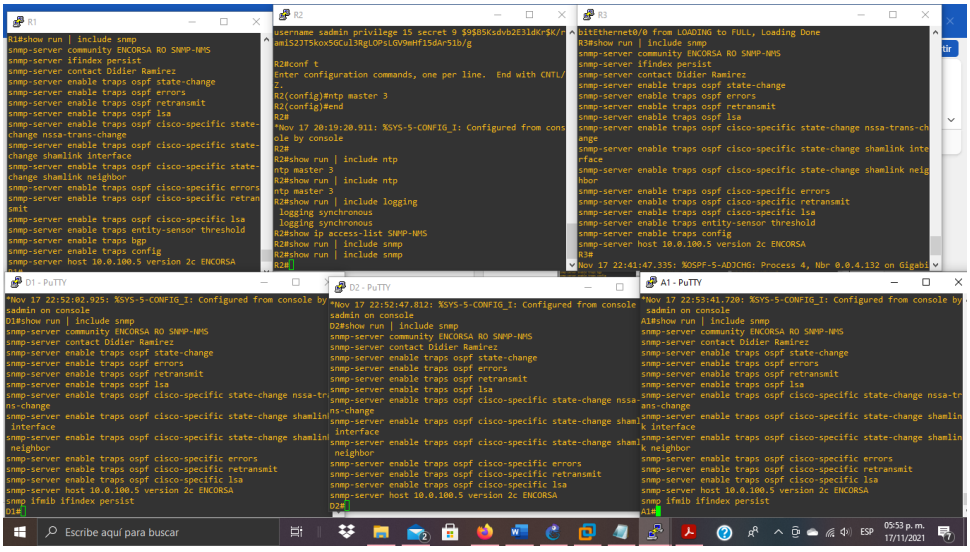
traps config
A1(config)#end

Figura 30. Se limita el acceso SNMP a la dirección IP de la PC1.



En la figura 30 se observa que se configuró SNMP en todos los equipos, excepto en R2, limitando el acceso a la dirección IP de la PC1.

Figura 31. Verificación de la configuración de SNMPv2c en todos los dispositivos excepto R2.



CONCLUSIONES

La topología de la red muestra la forma en que están organizados los componentes de la red. Dicha topología puede representar tanto los componentes físicos enlazados por medio de cables o de forma inalámbrica, como la topología lógica, la cual muestra la forma en que se encuentran unidos los datos y viajan dentro de la red.

Como su nombre lo indica, la tabla de direccionamiento permite visualizar las direcciones asignadas a los dispositivos en sus respectivas interfaces.

Los enlaces troncales son enlaces que se realizan punto a punto entre dos dispositivos que están dentro de una red para lograr transportar más de una VLAN, Por medio de los enlaces troncales de VLAN, se logra extender las VLAN a través de la red.

El protocolo RSTP (Rapid Spanning Tree Protocol) es un protocolo que funciona en el nivel de enlace de datos y su función es gestionar los enlaces que son redundantes.

Por medio del protocolo LACP es posible tener agrupados de manera lógica diversos enlaces físicos Ethernet con lo que se obtiene un enlace único; lo anterior permite añadir las velocidades de cada enlace y así se cuenta con un enlace agrupado de alta velocidad.

Los protocolos de enrutamiento administran las actividades que tienen que ver con el enrutamiento de las redes y permiten que los enrutadores compartan datos de las redes conocidas con otros enrutadores.

Con el fin de alterar lo menos posible una red cuando falla el Gateway predeterminado, es esencial proteger a la red, de manera que le sea posible recobrarse de forma dinámica; de ahí, la importancia de implementar la redundancia del primer salto.

Es fundamental la implementación de la seguridad a los equipos de la red, tanto de forma física como por medio de software, ya que las vulnerabilidades de la red son aprovechadas por ciberdelincuentes con diversos propósitos.

Es supremamente valiosa la labor del administrador de la red, ya que, es el encargado de realizar las respectivas configuraciones de la red, de encontrar y solucionar los fallos que se presenten, de buscar obtener mejores desempeños y de mantener la red segura.

REFERENCIAS BIBLIOGRÁFICAS

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

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

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

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). **OSPF v3**. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Overlay Tunnels. 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). Wireless Signals and Modulation. 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). Wireless Infrastructure. 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). Understanding Wireless Roaming and Location Services. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Authenticating Wireless Clients. 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). Troubleshooting Wireless Connectivity. 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). Fabric Technologies. 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 Assurance. 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

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

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

Granados, G. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]**.** Recuperado de http://hdl.handle.net/10596/24167

Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP [OVI]**.** Recuperado de https://repository.unad.edu.co/handle/10596/24419

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