

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

JAVIER MAURICIO CARDENAS RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS-ECBTI
INGENIERIA ELECTRONICA
BOGOTA
2022

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

JAVIER MAURICIO CARDENAS RAMIREZ

Diplomado presentado como opción de grado para optar por el título de
INGENIERO ELECTRONICO

TUTOR
JOHN HAROLD PEREZ CALDERON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIAS E INGENIERIAS-ECBTI
INGENIERIA ELECTRONICA
BOGOTA
2022

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 13 de noviembre de 2022

AGRADECIMIENTOS

A mi padre, por su sacrificio y dedicación; a Gabriela mi querida hija, el centro de mi fuerza y voluntad en las largas noches de estudio.

CONTENIDO

1. INTRODUCCIÓN.....	13
2. MATERIALES Y MÉTODOS.....	14
2.1 Materiales.....	14
2.2 Metodología.....	14
3. DESARROLLO DEL PROYECTO.....	15
3.1 Construir la Red.....	15
3.1.1 Topología Propuesta.....	15
3.1.2 Crear la red en el simulador	16
3.1.3 Tabla de direccionamiento.....	16
3.2 Configurar los ajustes básicos para cada dispositivo y el direccionamiento del interfaz.....	18
3.2.1 Configuración para el Enrutador 1.....	18
3.2.2 Configuración para el Enrutador 2.....	19
3.2.3 Configuración para el Enrutador 3.....	19
3.2.4 Configuración para el Switch D1	20
3.2.5 Configuración para el Switch D2	22
3.2.6 Configuración para el Switch A1.....	23
3.2.7 Configuración de direccionamiento de host de PC 1	24
3.2.8 Configuración de direccionamiento de host de PC 4.....	25
3.3 Configurar la compatibilidad de red y host de capa 2	25
3.3.1 Configuración de compatibilidad de red y host de capa 2 en D1	27
3.3.2 Verificación de compatibilidad de red y host de capa 2 en D1.....	29
3.3.3 Configuración de compatibilidad de red y capa 2 en D2	31
3.3.4 Verificación de compatibilidad de red y host de capa 2 en D2.....	33
3.3.5 Configuración de compatibilidad de red y capa 2 en A1.....	35
3.3.6 Verificación de compatibilidad de red y host de capa 2 en A1.....	37
3.3.7 Comprobar los servicios DHCP IPv4.....	39
3.3.8 Compruebe la conectividad LAN local.....	40
3.4 Configurar los protocolos de enrutamiento IPv4 e IPv6.....	42
3.4.1 Configurar protocolos de enrutamiento IPv4 e IPv6 en R1.....	45
3.4.2 Configurar protocolos de enrutamiento IPv4 e IPv6 en R3.....	47

3.4.3	Configurar los protocolos de enrutamiento IPv4 e IPv6 en D1	48
3.4.4	Configurar los protocolos de enrutamiento IPv4 e IPv6 en D2	50
3.4.5	Configurar los protocolos de enrutamiento IPv4 e IPv6 en R2	51
3.4.6	Verificar los protocolos de enrutamiento IPv4 e IPv6.	52
3.5	Configurar la redundancia de primer salto.....	60
3.5.1	Configurar redundancia de primer salto en D1	62
3.5.2	Configurar redundancia de primer salto en D2	65
3.5.3	Verificar configuración de redundancia de primer salto.	67
4.	CONCLUSIONES	69
5.	BIBLIOGRAFÍA	71

LISTA DE TABLAS

	Pág.
Tabla 1. Direccionamiento de la topología simulada	16
Tabla 2. Tareas de configuración de red y host de capa 2– ENCOR	25
Tabla 3. Tareas de configuración de Enrutamiento IPv4 e IPv6 – ENCOR	42
Tabla 4. Tareas de configuración redundancia de primer salto - ENCOR	61

LISTA DE FIGURAS

Pág.

Figura 1. Escenario Propuesto.....	15
Figura 2. Topología simulada	16
Figura 3. Configuración de interfaces troncales en D1.....	30
Figura 4. Configuración de spanning-tree en D1.....	30
Figura 5. Configuración de interfaz e 0/0 en D1	31
Figura 6. Configuración de interfaces troncales en D2.....	34
Figura 7. Configuración de spanning-tree en D2.....	34
Figura 8. Configuración de interfaz e 0/0 en D2.....	35
Figura 9. Configuración de interfaces troncales en A1	38
Figura 10. Configuración de interfaz e1/3 y e2/0 en A1	38
Figura 11. PC2 - DHCP -IPv4	39
Figura 12. PC3 - DHCP -IPv4	39
Figura 13. Ping desde PC1 a D1,D2,PC4.....	40
Figura 14. Ping desde PC2 a D1,D2.....	40
Figura 15. Ping desde PC3 a D1,D2.....	41
Figura 16. Ping desde PC4 a D1,D2, PC1.....	41
Figura 17. Configuración OSPF en R1.....	52
Figura 18. Configuración redes IPv4 en R1	53
Figura 19. Configuración redes IPv6 en R1	53
Figura 20. BGP en R2	54
Figura 21. Configuración de redes IPv4 en R2.....	54
Figura 22. Configuración de redes IPv6 en R2	55
Figura 23. Configuración OSPF en R3.....	55
Figura 24. Configuración de redes IPv4 en R3	56
Figura 25. Configuración de redes IPv6 en R3	56
Figura 26. Configuración OSPF en D1.....	57
Figura 27. Configuración de redes IPv4 en D1	57
Figura 28. Configuración de redes IPv6 en D1	58
Figura 29. Configuración OSPF en D2.....	58
Figura 30. Configuración de redes IPv4 en D2	59
Figura 31. Configuración de redes IPv6 en D2	60
Figura 32. HSRP en D1	68
Figura 33. HSRP en D2	68

GLOSARIO

DHCP: es un protocolo que permite generar de forma automática un host de Protocolo de Internet (IP) con la dirección IP, incluyendo la puerta de enlace predeterminada y la máscara de subred.

HOST: se puede definir como una tecnología que permite interactuar con todos los equipos que se conectan a una red, utilizando como recurso un PC huésped. El PC interactúa con los clientes intercambiando información. Es decir, un host es un dispositivo con dirección IP interconectado a otros dispositivos, permitiendo el inicio y final del flujo de datos.

HSRP: este protocolo perteneciente a la compañía Cisco, se desarrolla para lograr la conmutación por falla de un dispositivo IPv4 de primer salto. El protocolo permite una alta disposición de la red, generando redundancia de primer salto en los dispositivos IPv4 en las redes IPv4. Es utilizado en los enrutadores para escoger dispositivos activos y de reserva.

INTERFAZ: se define como interfaz, a la conexión física que se establece entre dos dispositivos para permitir la intercomunicación.

IPv4: es una forma de direccionamiento estándar que logra la comunicación vía internet de todo tipo de dispositivos. IPv4 se conforma de una cadena de dígitos de 32 bits, que incluye cuatro números entre 0 y 255, separados por puntos.

IPv6: (protocolo de internet versión 6) es un protocolo actualizado que permite la identificación de los dispositivos conectados a Internet. Permite dar una identificación única a cada ordenado. El protocolo IPv6 incrementa la cantidad de direcciones IP posibles, y se escribe como una cadena hexadecimal de dígitos de 128 bits.

LOOPBACK: esta interfaz no contiene un puerto físico asignado, por consiguiente, no es posible conectarla a otro equipo. Loopback es una interfaz de software, cuyo estado activo está condicionado al funcionamiento del enrutador. Su utilidad radica en prueba y administración de un equipo Cisco IOS, asegurando la disponibilidad de al menos una interfaz.

OSPF: se considera un protocolo de enlace, que tiene la capacidad de hallar alteraciones en la red en el interior de un Sistema autónomo, lo que permite tener una red sin bucles. OSPF soluciona dificultades de escalabilidad, producidas por el congestionamiento de los enrutadores, produciendo inestabilidad en el sistema.

RED: se considera red a la interconexión de una cantidad de dispositivos o de redes, utilizando equipos alámbricos o inalámbricos; estos equipos usan señales eléctricas, ondas electromagnéticas, o líneas físicas, para interactuar en un flujo de información.

SLA IP: es una tecnología de Cisco utilizada para dar seguimiento al tráfico en la red, permitiendo medir su desempeño. Utilizando IP SLA, se logra una red perceptible a métricas críticas, dañinas para la productividad de la red.

SLAAC: es un procedimiento utilizado para que un equipo pueda tener la dirección IPv6 de unidifusión, no teniendo que utilizar un servidor de DHCP version 6. usa mensajes anunciando y solicitando enrutador ICMPv6, dando información de configuración usualmente proporcionada por DHCP.

VALN: es una red virtual de área local, se utilizan para construir una red lógica independiente, dentro de la red física. Su función es segmentar la red en subredes, lo que permite una administración del tráfico en dichas subredes usando dispositivos de capa 3.

RESUMEN

Este documento integra el desarrollo de la actividad denominada “prueba de habilidades practica” perteneciente al Diplomado de profundización CISCO CCNP. El trabajo esta dividido en dos partes; la primera parte llamada Escenario 1, tiene como objetivo estructurar redes conmutadas usando el protocolo STP y configurando VLANs, para comprender el fundamento de una red multiservicio, así como la implementación de soluciones de red, configurando protocolos de enrutamiento.

La segunda parte llamada Escenario 2, tiene como finalidad la implementación de una red empresarial, segura, automatizada y virtualizada, configurando protocolos de enrutamiento IPv4 - IPv6, y además estableciendo la redundancia de primer salto HSRP, para crear una red convergente.

La actividad se desarrolla utilizando como recurso el laboratorio simulado GNS3, previa configuración del sistema y máquina virtual. En él se implementa la topología propuesta en la actividad, que consta de tres enrutadores, tres conmutadores, y cuatro PC.

En el desarrollo del escenario 1, primero se construirá la red propuesta, y luego se configurarán los ajustes básicos de cada dispositivo, tales como: nombres, levantamiento interfaces, IPv4, IPv6, VLANs, etc. Seguido se configurará la compatibilidad de red y host de capa 2. En donde al terminar deberá existir comunicación efectiva entre los dispositivos.

En el desarrollo del escenario 2. Se iniciará configurando los protocolos de enrutamiento IPv4 - IPv6 para crear una red convergente, utilizando configuraciones OSPF v2 y OSPF v3, así como MP-BGP. Seguido se configurará la redundancia de primer salto, estableciendo HSRP v2 en los dispositivos. La actividad termina realizando pruebas de conectividad entre los dispositivos para verificar la correcta implementación de la red.

PALABRAS CLAVE: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

This document integrates the development of the activity called "practical skills test" belonging to the CISCO CCNP in-depth training course. The work is divided in two parts; the first part called Scenario 1, has as objective to structure switched networks using the STP protocol and configuring VLANs, to understand the basis of a multiservice network, as well as the implementation of network solutions, configuring routing protocols.

The second part called Scenario 2, aims at implementing a secure, automated, and virtualized enterprise network, configuring IPv4 - IPv6 routing protocols, and also establishing HSRP first hop redundancy, to create a converged network.

The activity is developed using the GNS3 simulated laboratory as a resource, after configuring the system and virtual machine. The topology proposed in the activity, consisting of three routers, three switches, and four PCs, is implemented.

In the development of scenario 1, first the proposed network will be built, and then the basic settings of each device will be configured, such as: names, interfaces, IPv4, IPv6, VLANs, etc. Then the network and layer 2 host compatibility will be configured. At the end there should be effective communication between the devices.

In the development of scenario 2, we will start by configuring the IPv4 - IPv6 routing protocols to create a converged network, using OSPF v2 and OSPF v3 configurations, as well as MP-BGP. Next, first hop redundancy will be configured, establishing HSRP v2 on the devices.

The activity ends by performing connectivity tests between devices to verify the correct implementation of the network.

KEYWORDS: CISCO, CCNP, Switching, Routing, Networking, Electronics

1. INTRODUCCIÓN

La evolución tecnológica ha permitido el desarrollo de la humanidad mejorando su calidad de vida no solo a nivel personal, sino también en el ámbito empresarial. En consecuencia, las redes informáticas representan las vías esenciales de la conectividad, siendo estas una herramienta de trabajo multidisciplinar. Las redes permiten una versatilidad operativa que abarca diferentes ángulos, como, por ejemplo, imprimir un documento desde un celular, o que ejecutivos puedan acceder a una base de datos corporativa almacenada en un servidor en cualquier parte del mundo. Para lograr esta conectividad y lograr el intercambio de datos entre dispositivos es necesaria la conexión física y el enlace lógico de los sistemas, el cual se establece usando protocolos específicos de red.

Este informe integra el desarrollo de la actividad llamada “prueba de habilidades práctica”, que hace parte del diplomado de profundización CISCO CCNP. Tomado como opción de grado para obtener el título de Ingeniero Electrónico. Aquí se plantea un escenario de red empresarial, para ser implementado con acceso seguro , a través de la virtualización y la automatización; teniendo en cuenta configurar los protocolos de enrutamiento para implementar adecuadamente los servicios IP. El laboratorio se desarrolla una vez se ha investigado y estudiado la documentación proporcionada por la universidad correspondiente a las unidades 1-10 del documento <CCNP and CCIE Enterprise Core ENCOR 350-401>, para luego implementar la topología propuesta usando el simulador grafico GNS3, y dar solución a las tareas de configuración indicadas en la actividad.

El informe se desarrolla en primera instancia con la implementación de la configuración básica de la red y la tabla de direcciones de las interfaces, seguido de la configuración de compatibilidad de red y host de capa 2, obteniendo como resultado la correcta conectividad LAN local. En segundo lugar, se hará la configuración de los protocolos de enrutamiento IPv4 - IPv6, implementando OSPFv2 y OSPFv3 en los dispositivos, con el objetivo de lograr una red convergente. La actividad finaliza configurando la redundancia de primer salto, utilizando HSRP versión 2, en los conmutadores.

2. MATERIALES Y MÉTODOS

2.1 Materiales.

- 3 Routers (Cisco 7200).
- 3 switches (Cisco IOU L2).
- 4 PC (VPCS del GNS3)

2.2 Metodología.

Los dispositivos usados en este laboratorio son: enrutadores “*Cisco 7200*”. Y conmutadores “*Cisco Catalyst L2 switches*”; no obstante, es posible utilizar otros enrutadores y conmutadores, con diferentes versiones de IOS.

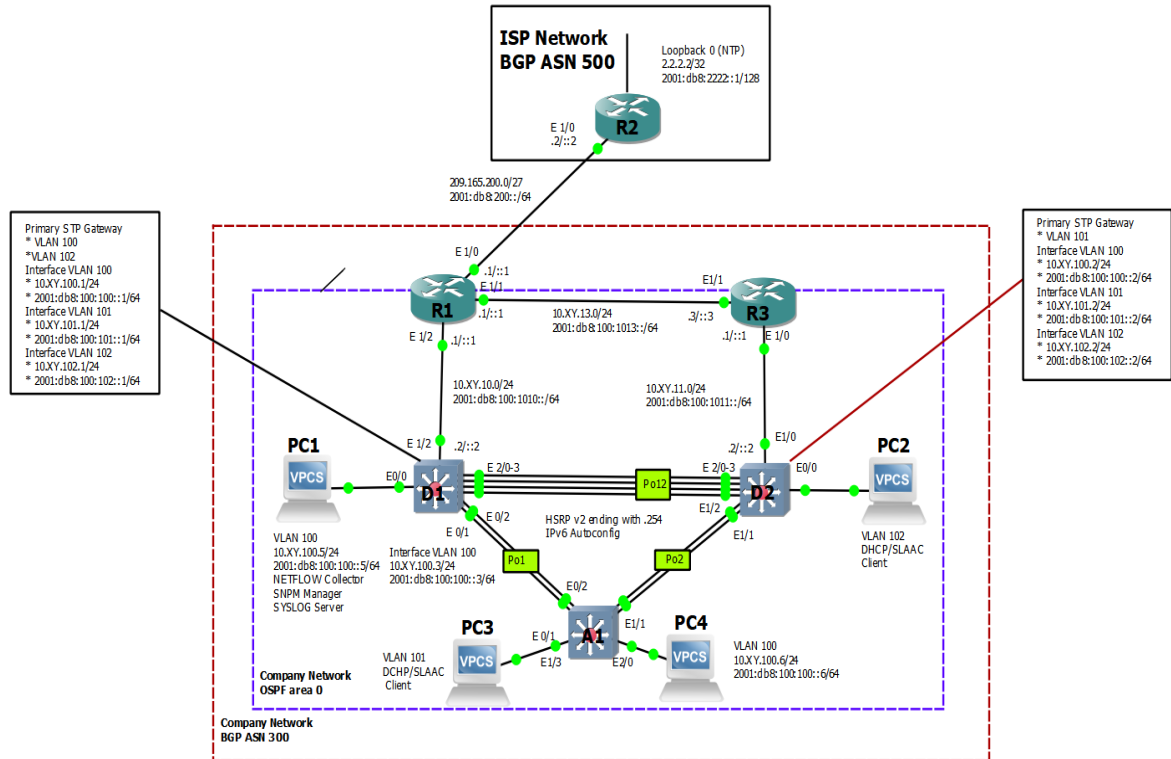
Se recomienda antes de iniciar cualquier configuración, borrar la configuración por defecto de los Switches.

3. DESARROLLO DEL PROYECTO

3.1 Construir la Red

3.1.1 Topología Propuesta

Figura 1. Escenario Propuesto

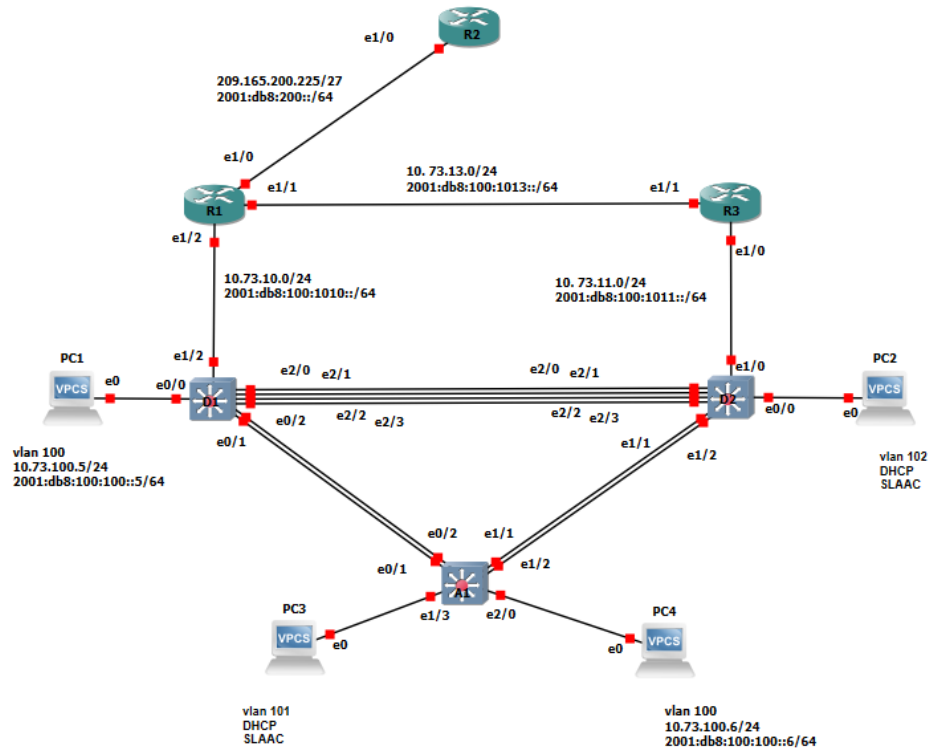


Fuente 1. Guía evaluación de habilidades de ENCOR – CCNP (Escenario 1)

En esta actividad, es necesario complementar las configuraciones de la red permitiendo acceso completo en todos los dispositivos.

3.1.2 Crear la red en el simulador

Figura 2. Topología simulada



Fuente 2. Autoría propia-simulador gns3

3.1.3 Tabla de direccionamiento

Tabla 1. Direccionamiento de la topología simulada

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R1	E1/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E1/2	10.73.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	E1/1	10.73.13.1/24	2001:db8:100:1013::1/64	fe80::1:3

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	Enlace IPv6 local
R2	E1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Bucle invertido 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E1/0	10.73.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	E1/1	10.73.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/2	10.73.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	vlan 100	10.73.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	vlan 101	10.73.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	vlan 102	10.73.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.73.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	vlan 100	10.73.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	vlan 101	10.73.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	vlan 102	10.73.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	vlan 100	10.73.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	Nada	10.73.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	Nada	DHCP	SLAAC	EUI-64
PC3	Nada	DHCP	SLAAC	EUI-64
PC4	Nada	10.73.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente 3. Guía evaluación de habilidades de ENCOR – CCNP (Escenario 1)

3.2 Configurar los ajustes básicos para cada dispositivo y el direccionamiento del interfaz

3.2.1 Configuración para el Enrutador 1

CODIGO USADO EN R1	
<pre>Configure terminal hostname R1 ipv6 unicast-routing no ip domain lookup banner motd # R1, ENCOR Skills Assessment# line con 0 exec-timeout 0 0 logging synchronous exit interface e1/0 ip address 209.165.200.225 255.255.255.224 ipv6 address fe80::1:1 link-local ipv6 address 2001:db8:200::1/64 no shutdown exit interface e1/2 ip address 10.73.10.1 255.255.255.0 ipv6 address fe80::1:2 link-local ipv6 address 2001:db8:100:1010::1/64 no shutdown exit interface e1/1 ip address 10.73.13.1 255.255.255.0 ipv6 address fe80::1:3 link-local ipv6 address 2001:db8:100:1013::1/64 no shutdown exit</pre>	<p>Modo de configuración Nombra el enrutador como R1 Habilito enrutamiento ipv6 Inactiva la traducción de nombres Crea un mensaje de bienvenida</p> <p>Entra en la línea 0 de la consola Inactiva la sección remota Elimina mensajes en la pantalla Salida Configuración interfaz ethernet 1/0 Dirección IPv4 y Mascara de Red</p> <p>Enlace IPv6 local Dirección IPv6 Sin apagado salida Configuración interfaz ethernet 1/2 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida Configuración interfaz ethernet 1/1 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p>

3.2.2 Configuración para el Enrutador 2

CODIGO USADO EN R2	
<pre>Configure terminal hostname R2 ipv6 unicast-routing no ip domain lookup banner motd # R2, ENCOR Skills Assessment# line con 0 exec-timeout 0 0 logging synchronous exit interface e1/0 ip address 209.165.200.226 255.255.255.224 ipv6 address fe80::2:1 link-local ipv6 address 2001:db8:200::2/64 no shutdown exit interface Loopback 0 ip address 2.2.2.2 255.255.255.255 ipv6 address fe80::2:3 link-local ipv6 address 2001:db8:2222::1/128 no shutdown exit</pre>	<p>Ingresa al modo de configuración Nombra el enrutador como R2 Habilito enrutamiento ipv6 Inactiva la traducción de nombres Crea un mensaje de bienvenida</p> <p>Entra en la línea 0 de la consola Inactiva la sección remota Elimina mensajes en la pantalla Salida</p> <p>Configuración interfaz ethernet 1/0 Dirección IPv4 y Mascara de Red</p> <p>Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración interfaz Loopback 0 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p>

3.2.3 Configuración para el Enrutador 3

CODIGO USADO EN R3	
<pre>Configure terminal hostname R3 ipv6 unicast-routing no ip domain lookup banner motd # R3, ENCOR Skills Assessment# line con 0 exec-timeout 0 0</pre>	<p>Ingresa al modo de configuración Nombra el enrutador como R3 Habilito enrutamiento ipv6 Inactiva la traducción de nombres Crea un mensaje de bienvenida</p> <p>Entra en la línea 0 de la consola Inactiva la sección remota</p>

<pre>logging synchronous exit interface e1/0 ip address 10.73.11.1 255.255.255.0 ipv6 address fe80::3:2 link-local ipv6 address 2001:db8:100:1011::1/64 no shutdown exit interface e1/1 ip address 10.73.13.3 255.255.255.0 ipv6 address fe80::3:3 link-local ipv6 address 2001:db8:100:1010::2/64 no shutdown exit</pre>	<p>Elimina mensajes en la pantalla Salida</p> <p>Configuración interfaz ethernet 1/0 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración interfaz ethernet 1/1 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p>
---	---

3.2.4 Configuración para el Switch D1

CODIGO USADO EN D1	
<pre>Configure terminal hostname D1 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D1, ENCOR Skills Assessment# line con 0 exec-timeout 0 0 logging synchronous exit vlan 100 name Management exit vlan 101 name UserGroupA exit vlan 102 name UserGroupB exit</pre>	<p>Ingresa al modo de configuración Nombra el Switch como D1 Habilito enrutamiento ipv4 Habilito enrutamiento ipv6 Inactiva la traducción de nombres DNS Crea un mensaje de bienvenida</p> <p>Entra en la línea 0 de la consola Inactiva la sección remota Elimina mensajes en la pantalla Salida</p> <p>Configuración de la vlan 100 Da el nombre a vlan de Administración Salida</p> <p>Configuración de la vlan 101 Da el nombre a vlan de usuarios A Salida</p> <p>Configuración de la vlan 102 Da el nombre a vlan de usuarios B salida</p>

<pre> vlan 999 name NATIVE exit interface e1/2 no switchport ip address 10.73.10.2 255.255.255.0 ipv6 address fe80::d1:1 link-local ipv6 address 2001:db8:100:1010::2/64 no shutdown exit interface vlan 100 ip address 10.73.100.1 255.255.255.0 ipv6 address fe80::d1:2 link-local ipv6 address 2001:db8:100:100::1/64 no shutdown exit interface vlan 101 ip address 10.73.101.1 255.255.255.0 ipv6 address fe80::d1:3 link-local ipv6 address 2001:db8:100:101::1/64 no shutdown exit interface vlan 102 ip address 10.73.102.1 255.255.255.0 ipv6 address fe80::d1:4 link-local ipv6 address 2001:db8:100:102::1/64 no shutdown exit ip dhcp excluded-address 10.73.101.1 10.73.101.109 ip dhcp excluded-address 10.73.101.141 10.73.101.254 ip dhcp excluded-address 10.73.102.1 10.73.102.109 ip dhcp excluded-address 10.73.102.141 10.73.102.254 ip dhcp pool VLAN-101 network 10.73.101.0 255.255.255.0 default-router 10.73.101.254 exit ip dhcp pool VLAN-102 network 10.73.102.0 255.255.255.0 default-router 10.73.102.254 exit </pre>	<p>Configuración de la vlan 999 Da el nombre de vlan Nativa salida</p> <p>Configuración interfaz ethernet 1/2 Sin puerto de conexión Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración de la vlan 100 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración de la vlan 101 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración de la vlan 102 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>dirección ip dhcp excluida</p> <p>dirección ip dhcp excluida</p> <p>dirección ip dhcp excluida</p> <p>dirección ip dhcp excluida</p>
--	--

<pre>interface range e0/0-3,e1/0-1,e1/3,e2/0-3,e3/0-3 shutdown exit</pre>	
---	--

3.2.5 Configuración para el Switch D2

CODIGO USADO EN D2	
<pre>Configure terminal hostname D2 ip routing ipv6 unicast-routing no ip domain lookup banner motd # D2, ENCOR Skills Assessment# line con 0 exec-timeout 0 0 logging synchronous exit vlan 100 name Management exit vlan 101 name UserGroupA exit vlan 102 name UserGroupB exit vlan 999 name NATIVE exit interface e1/0 no switchport ip address 10.73.11.2 255.255.255.0 ipv6 address fe80::d1:1 link-local ipv6 address 2001:db8:100:1011::2/64 no shutdown exit interface vlan 100 ip address 10.73.100.2 255.255.255.0 ipv6 address fe80::d2:2 link-local ipv6 address 2001:db8:100:100::2/64</pre>	<p>Ingresa al modo de configuración Nombramos el Switch como D2 Habilitamos enrutamiento ipv4 Habilitamos enrutamiento ipv6 Inactivamos la traducción de nombres DNS Creamos un mensaje de bienvenida</p> <p>Entra en la línea 0 de la consola Inactivamos la sección remota Eliminamos mensajes en la pantalla Salida</p> <p>Configuración de la vlan 100 Da el nombre a vlan de Administración Salida</p> <p>Configuración de la vlan 101 Da el nombre a vlan de usuarios A Salida</p> <p>Configuración de la vlan 102 Da el nombre a vlan de usuarios B salida</p> <p>Configuración de la vlan 999 Da el nombre de vlan Nativa salida</p> <p>Configuración interfaz ethernet 1/0 Sin puerto de conexión Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración de la vlan 100 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6</p>

<pre> no shutdown exit interface vlan 101 ip address 10.73.101.2 255.255.255.0 ipv6 address fe80::d2:3 link-local ipv6 address 2001:db8:100:101::2/64 no shutdown exit interface vlan 102 ip address 10.73.102.2 255.255.255.0 ipv6 address fe80::d2:4 link-local ipv6 address 2001:db8:100:102::2/64 no shutdown exit ip dhcp excluded-address 10.73.101.1 10.73.101.209 ip dhcp excluded-address 10.73.101.241 10.73.101.254 ip dhcp excluded-address 10.73.102.1 10.73.102.209 ip dhcp excluded-address 10.73.102.241 10.73.102.254 ip dhcp pool VLAN-101 network 10.73.101.0 255.255.255.0 default-router 73.0.101.254 exit ip dhcp pool VLAN-102 network 10.73.102.0 255.255.255.0 default-router 10.73.102.254 exit interface range e0/0-3,e1/1-3,e2/0- 3,e3/0-3 shutdown exit </pre>	<p>Sin apagado salida</p> <p>Configuración de la vlan 101 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>Configuración de la vlan 102 Dirección IPv4 y Mascara de Red Enlace IPv6 local Dirección IPv6 Sin apagado salida</p> <p>dirección ip dhcp excluida</p> <p>dirección ip dhcp excluida</p> <p>dirección ip dhcp excluida</p> <p>dirección ip dhcp excluida</p>
---	---

3.2.6 Configuración para el Switch A1

CODIGO USADO EN A1	
<pre> Configure terminal hostname A1 no ip domain lookup </pre>	<p>Ingresa al modo de configuración Nombra el Switch como D2 Inactiva la traducción de nombres DNS</p>

<pre> banner motd # A1, ENCOR Skills Assessment# line con 0 exec-timeout 0 0 logging synchronous exit vlan 100 name Management exit vlan 101 name UserGroupA exit vlan 102 name UserGroupB exit vlan 999 name NATIVE exit interface vlan 100 ip address 10.73.100.3 255.255.255.0 ipv6 address fe80::a1:1 link-local ipv6 address 2001:db8:100:100::3/64 no shutdown exit interface range e0/0,e0/3,e1/0,e2/1- 3,e3/0-3 shutdown exit </pre>	<p>Crea un mensaje de bienvenida</p> <p>Entra en la línea 0 de la consola</p> <p>Inactiva la sección remota</p> <p>Elimina mensajes en la pantalla</p> <p>Salida</p> <p>Configuración de la vlan 100</p> <p>Da el nombre a vlan de Administración</p> <p>Salida</p> <p>Configuración de la vlan 101</p> <p>Da el nombre a vlan de usuarios A</p> <p>Salida</p> <p>Configuración de la vlan 102</p> <p>Da el nombre a vlan de usuarios B</p> <p>salida</p> <p>Configuración de la vlan 999</p> <p>Da el nombre de vlan Nativa</p> <p>salida</p> <p>interfaz vlan 100</p> <p>Dirección IPv4 y Mascara de Red</p> <p>Enlace IPv6 local</p> <p>Dirección IPv6</p> <p>Sin apagado</p> <p>salida</p> <p>rango de interfaz</p> <p>apagado</p> <p>salida</p>
--	--

3.2.7 Configuración de direccionamiento de host de PC 1

CODIGO EN PC1	
Ip 10.73.100.5 255.255.255.0 10.73.100.254	asigna dirección ip y puerta de enlace

3.2.8 Configuración de direccionamiento de host de PC 4

CODIGO EN PC4	
Ip 10.73.100.6 255.255.255.0 10.73.100.254	asigna dirección ip y puerta de enlace

3.3 Configurar la compatibilidad de red y host de capa 2

Tabla 2. Tareas de configuración de red y host de capa 2– ENCOR SKILLS

Tarea #	Tarea	Especificación	Puntos
2.1	En todos los conmutadores, configure las interfaces troncales IEEE 802.1Q en los enlaces de conmutación interconectados	Habilite los enlaces troncales 802.1Q entre: <ul style="list-style-type: none"> • D1 y D2 • D1 y A1 • D2 y A1 	6
2.2	En todos los conmutadores, cambie la VLAN nativa en los enlaces troncales.	Utilice VLAN 999 como VLAN nativa.	6
2.3	En todos los conmutadores, habilite el protocolo De árbol de expansión rápida.	Utilice el árbol de expansión rápida.	3
2.4	En D1 y D2, configure los puertos raíz RSTP adecuados en función de la información del diagrama de topología. D1 y D2 deben proporcionar copia de seguridad en caso de fallo del puerto raíz.	Configure D1 y D2 como raíz para las VLAN adecuadas con prioridades de apoyo mutuo en caso de fallo del conmutador.	2

Tarea #	Tarea	Especificación	Puntos
2.5	En todos los switches, cree LACP EtherChannels como se muestra en el diagrama de topología.	Utilice los siguientes números de canal: <ul style="list-style-type: none"> • D1 a D2 – Canal de puerto 12 • D1 a A1 – Puerto canal 1 • D2 a A1 – Puerto canal 2 	3
2.6	En todos los conmutadores, configure los puertos de acceso al host 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 host deben pasar inmediatamente al estado de reenvío.	4
2.7	Compruebe los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.	1

Tarea #	Tarea	Especificación	Puntos
2.8	Compruebe la conectividad LAN local.	<p>PC1 debería hacer ping con éxito:</p> <ul style="list-style-type: none"> • D1: 10.XY.100.1 • D2: 10.XY.100.2 • PC4: 10.XY.100.6 <p>PC2 debería hacer ping correctamente:</p> <ul style="list-style-type: none"> • D1: 10.XY.102.1 • D2: 10.XY.102.2 <p>PC3 debería hacer ping correctamente:</p> <ul style="list-style-type: none"> • D1: 10.XY.101.1 • D2: 10.XY.101.2 <p>PC4 debería hacer ping correctamente:</p> <ul style="list-style-type: none"> • D1: 10.XY.100.1 • D2: 10.XY.100.2 • PC1: 10.XY.100.5 	1

Fuente 4. Guía evaluación de habilidades de ENCOR – CCNP (Escenario 1)

3.3.1 Configuración de compatibilidad de red y host de capa 2 en D1

CODIGO USADO EN D1	
<p>2.1 configurar las interfaces troncales IEEE 802.1Q</p> <p>Habilitar los enlaces troncales 802.1Q entre:</p> <ul style="list-style-type: none"> ○ D1 y D2 ○ D1 y A1 	
<p>Configure terminal interface range e2/0-3</p> <p>switchport trunk encapsulation dot1q switchport mode trunk</p>	<p>Ingresa al modo de configuración Configuración del rango de interfaz ethernet 2/0-3</p> <p>Encapsulación del enlace troncal Configura el puerto como enlace troncal</p>

<pre>exit interface range e0/1-2 switchport trunk encapsulation dot1q switchport mode trunk exit</pre>	<pre>salida Configuración del rango de interfaz ethernet e0/1-2 Encapsulación del enlace troncal Configura el puerto como enlace troncal salida</pre>
<p>2.2 cambiar la VLAN nativa en los enlaces troncales. Usar VLAN 999 como VLAN nativa.</p>	
<pre>Configure terminal interface range e2/0-3 switchport trunk native vlan 999 exit interface range e0/1-2 switchport trunk native vlan 999 exit</pre>	<pre>Ingresa al modo de configuración Configuración del rango de interfaz ethernet 2/0-3 Cambia la vlan nativa a 999 salida Configuración del rango de interfaz ethernet e0/1-2 Cambia la vlan nativa a 999 salida</pre>
<p>2.3 habilitar el protocolo De árbol de expansión rápida. usar el árbol de expansión rápida.</p>	
<pre>Configure terminal spanning-tree mode rapid-pvst</pre>	<pre>Ingresa al modo de configuración Habilito protocolo de árbol de expansión rápida</pre>
<p>2.4 Configurar en D1 los puertos raíz RSTP. D1 debe tener copia de seguridad si hay fallas en el puerto raíz.</p>	
<pre>spanning-tree vlan 100,102 root primary spanning-tree vlan 101 root secondary</pre>	<pre>Configura el Switch como puerto raíz primario para las vlan 100,102. Configura el Switch como puerto raíz secundario para las vlan 101.</pre>
<p>2.5 Cree LACP EtherChannels como se muestra en el diagrama de topología.</p> <p>Utilice los siguientes números de canal:</p> <ul style="list-style-type: none"> • D1 a D2 – Puerto canal 12 • D1 a A1 – Puerto canal 1 	

<pre>Configure terminal interface range e2/0-3 channel-group 12 mode active no shutdown exit interface range e0/1-2 channel-group 1 mode active no shutdown exit</pre>	<p>Ingresa al modo de configuración</p> <p>Configuración del rango de interfaz ethernet 2/0-3</p> <p>Crea el canal de puerto 12-LACP Sin apagado Salida</p> <p>Configuración del rango de interfaz ethernet e0/1-2</p> <p>Crea el canal de Puerto 1-LACP Sin apagado Salida</p>
<p>2.6 Configurar los puertos de acceso al host que se conectan a PC1, PC2, PC3 y PC4.</p>	
<pre>Configure terminal interface e0/0 switchport mode access switchport access vlan 100 spanning-tree portfast no shutdown exit end</pre>	<p>Ingresa al modo de configuración</p> <p>Configuración interfaz ethernet e0/0</p> <p>Configura el puerto en modo de acceso. Habilita el modo de acceso a la vlan 100 Habilita el puerto host a estado de reenvío Sin apagado salida fin</p>

3.3.2 Verificación de compatibilidad de red y host de capa 2 en D1.

Códigos utilizados.

- Show interfaces trunk
- Show run | include spanning-tree
- Show run interfaces e0/0

Figura 3. Configuración de interfaces troncales en D1

```
D1
*Oct 15 20:20:55.667: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/2 (not full duplex), with R1 Ethernet1/2 (full duplex).
D1#
*Oct 15 20:21:49.604: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethernet1/2 (not full duplex), with R1 Ethernet1/2 (full duplex).
D1#
D1#show interfaces trunk

Port      Mode           Encapsulation  Status        Native vlan
-----
Po1       on             802.1q         trunking     999
Po12      on             802.1q         trunking     999

Port      Vlans allowed on trunk
-----
Po1       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
-----
Po1       1,100-102,999
Po12      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
-----
Po1       1,100-102,999
Po12      1,100-102,999
D1#
```

Fuente 5. Autoría propia-simulador gns3

Figura 4. Configuración de spanning-tree en D1

```
D1
D1#
D1#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 24576
spanning-tree vlan 101 priority 28672
spanning-tree portfast edge
D1#
```

Fuente 6. Autoría propia-simulador gns3

Figura 5. configuración de interfaz e 0/0 en D1

```

D1#sh
*Oct 15 20:34:23.819: %CDP-4-DUPLEX_MISMATCH:
/2 (full duplex).
D1#
D1#show run interface e0/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet0/0
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end
D1#

```

Fuente 7. Autoría propia-simulador gns3

3.3.3 Configuración de compatibilidad de red y capa 2 en D2

CODIGO USADO EN D2	
<p>2.1 Configurar las interfaces troncales IEEE 802.1Q Habilitar los enlaces troncales 802.1Q entre:</p> <ul style="list-style-type: none"> ○ D1 y D2 ○ D2 y A1 	
<p>Configure terminal interface range e2/0-3</p> <p>switchport trunk encapsulation dot1q switchport mode trunk exit interface range e1/1-2</p> <p>switchport trunk encapsulation dot1q switchport mode trunk exit</p>	<p>Ingresa al modo de configuración Configuración del rango de interfaz ethernet 2/0-3 Encapsulación del enlace troncal Configura el puerto como enlace troncal salida Configuración del rango de interfaz ethernet e1/1-2 Encapsulación del enlace troncal Configura el puerto como enlace troncal salida</p>

2.2 Cambiar la VLAN nativa en los enlaces troncales. Usar VLAN 999 como VLAN nativa.	
Configure terminal interface range e2/0-3 switchport trunk native vlan 999 exit interface range e1/1-2 switchport trunk native vlan 999 exit	Ingresa al modo de configuración Configuración del rango de interfaz ethernet 2/0-3 Cambia la vlan nativa a 999 salida Configuración del rango de interfaz ethernet e1/1-2 Cambia la vlan nativa a 999 salida
2.3 Habilitar el protocolo De árbol de expansión rápida.	
Configure terminal spanning-tree mode rapid-pvst	Ingresa al modo de configuración Habilito protocolo de árbol de expansión rápida
2.4 Configurar en D2 los puertos raíz RSTP D2 debe tener copia de seguridad en caso de fallas en el puerto raíz.	
spanning-tree vlan 101 root primary spanning-tree vlan 100,102 root secondary	Configura el Switch como puerto raíz primario para las vlan 101. Configura el Switch como puerto raíz secundario para las vlan 100,102.
2.5 Cree LACP EtherChannels como se muestra en el diagrama de topología. Usar los siguientes números de canal: D1 a D2 – Canal de puerto 12, D2 a A1 – Puerto canal 2	
Configure terminal interface range e2/0-3 channel-group 12 mode active no shutdown exit interface range e1/1-2 channel-group 2 mode active no shutdown exit	Ingresa al modo de configuración Configuración del rango de interfaz ethernet 2/0-3 Crea el canal de puerto 12-LACP Sin apagado Salida Configuración del rango de interfaz ethernet e1/1-2 Crea el canal de Puerto 2 -LACP Sin apagado Salida

2.6 configurar los puertos de acceso al host que están conectados a las PC1, PC2, PC3 y PC4	
<pre>Configure terminal interface e0/0 switchport mode access switchport access vlan 102 spanning-tree portfast no shutdown exit end</pre>	<pre>Ingresa al modo de configuración Configuración interfaz ethernet e0/0 Configura el puerto en modo de acceso. Habilita el modo de acceso a la vlan 102 Habilita el puerto host a estado de reenvío Sin apagado salida fin</pre>

3.3.4 Verificación de compatibilidad de red y host de capa 2 en D2.

Códigos utilizados.

- Show interfaces trunk
- Show run | include spanning-tree
- Show run interfaces e0/0

Figura 6. Configuración de interfaces troncales en D2

```
D2#
D2#show interfaces trunk

Port      Mode          Encapsulation  Status        Native vlan
Po2       on            802.1q         trunking      999
Po12      on            802.1q         trunking      999

Port      Vlans allowed on trunk
Po2       1-4094
Po12      1-4094

Port      Vlans allowed and active in management domain
Po2       1,100-102,999
Po12      1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po2       1,100-102,999
Po12      1,100-102,999
D2#
```

Fuente 8. Autoría propia-simulador gns3

Figura 7. Configuración de spanning-tree en D2

```
D2#show run | include spanning-tree
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100,102 priority 20480
spanning-tree vlan 101 priority 28672
spanning-tree portfast edge
D2#
```

Fuente 9. Autoría propia-simulador gns3

Figura 8. configuración de interfaz e 0/0 en D2

```

D2#
D2#show run interface e0/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet0/0
  switchport access vlan 102
  switchport mode access
  spanning-tree portfast edge
end
    
```

Fuente 10. Autoría propia-simulador gns3

3.3.5 Configuración de compatibilidad de red y capa 2 en A1

CODIGO USADO EN A1	
<p>2.1 Configurar las interfaces troncales IEEE 802.1Q Habilitar los enlaces troncales 802.1Q entre:</p> <ul style="list-style-type: none"> ○ D1 y A1 ○ D2 y A1 	
<p>Configure terminal interface range e0/1-2</p> <p>switchport trunk encapsulation dot1q switchport mode trunk exit interface range e1/1-2</p> <p>switchport trunk encapsulation dot1q switchport mode trunk exit</p>	<p>Ingresa al modo de configuración Configuración del rango de interfaz ethernet e0/1-2 Encapsulación del enlace troncal Configura el puerto como enlace troncal salida Configuración del rango de interfaz ethernet e1/1-2 Encapsulación del enlace troncal Configura el puerto como enlace troncal salida</p>

2.2 Cambiar la VLAN nativa en los enlaces troncales. Usar VLAN 999 como VLAN nativa.	
<p>Configure terminal interface range e0/1-2</p> <p>switchport trunk native vlan 999 exit interface range e1/1-2</p> <p>switchport trunk native vlan 999 exit</p>	<p>Ingresa al modo de configuración Configuración del rango de interfaz ethernet 0/1-2</p> <p>Cambia la vlan nativa a 999 salida</p> <p>Configuración del rango de interfaz ethernet e1/1-2</p> <p>Cambia la vlan nativa a 999 salida</p>
2.3 habilitar el protocolo De árbol de expansión rápida. Usar el árbol de expansión rápida.	
<p>Configure terminal spanning-tree mode rapid-pvst</p>	<p>Ingresa al modo de configuración Habilito protocolo de árbol de expansión rápida</p>
2.5 Crear LACP EtherChannels como se muestra en el diagrama de topología. <p>Utilice los siguientes números de canal:</p> <ul style="list-style-type: none"> • D1 a A1 – Puerto canal 1 • D2 a A1 – Puerto canal 2 	
<p>Configure terminal interface range e0/1-2</p> <p>channel-group 1 mode active no shutdown exit interface range e1/1-2</p> <p>channel-group 2 mode active no shutdown exit</p>	<p>Ingresa al modo de configuración Configuración del rango de interfaz ethernet e0/1-2</p> <p>Crea el canal de puerto 1 -LACP Sin apagado Salida</p> <p>Configuración del rango de interfaz ethernet e1/1-2</p> <p>Crea el canal de Puerto 2 -LACP Sin apagado Salida</p>

2.6 Configurar los puertos de acceso al host que están conectados a las PC1, PC2, PC3, PC4.	
<pre>Configure terminal interface e1/3 switchport mode access switchport access vlan 101 spanning-tree portfast no shutdown exit interface e2/0 switchport mode access switchport access vlan 100 spanning-tree portfast no shutdown exit end</pre>	<pre>Ingresa al modo de configuración Configuración interfaz ethernet e1/3 Configura el puerto en modo de acceso. Habilita el modo de acceso a la vlan 101 Habilita el puerto host a estado de reenvío Sin apagado salida Configuración interfaz ethernet e2/0 Configura el puerto en modo de acceso. Habilita el modo de acceso a la vlan 100 Habilita el puerto host a estado de reenvío Sin apagado salida fin</pre>

3.3.6 Verificación de compatibilidad de red y host de capa 2 en A1.

Códigos utilizados.

- Show interfaces trunk
- Show run interfaces e1/3
- Show run interfaces e2/0

Figura 9. Configuración de interfaces troncales en A1

```
A1#show interface trunk

Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po2       on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po1       1-4094
Po2       1-4094

Port      Vlans allowed and active in management domain
Po1       1,100-102,999
Po2       1,100-102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,100-102,999
Po2       none
A1#
```

Fuente 11. Autoría propia-simulador gns3

Figura 10. configuración de interfaz e1/3 y e2/0 en A1

```
A1#show run int e1/3
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet1/3
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast edge
end

A1#show run int e2/0
Building configuration...

Current configuration : 110 bytes
!
interface Ethernet2/0
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast edge
end

A1#
```

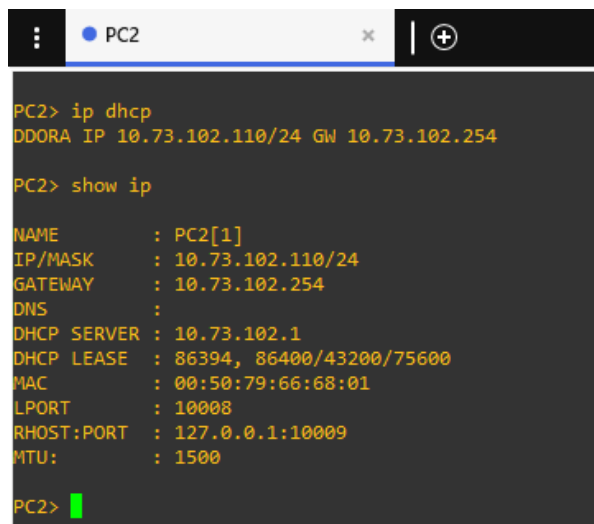
Fuente 12. Autoría propia-simulador gns3

3.3.7 Comprobar los servicios DHCP IPv4

DHCP en PC2
y PC3

Verificación

Figura 11. PC2 - DHCP -IPv4



```
PC2> ip dhcp
DDORA IP 10.73.102.110/24 GW 10.73.102.254

PC2> show ip

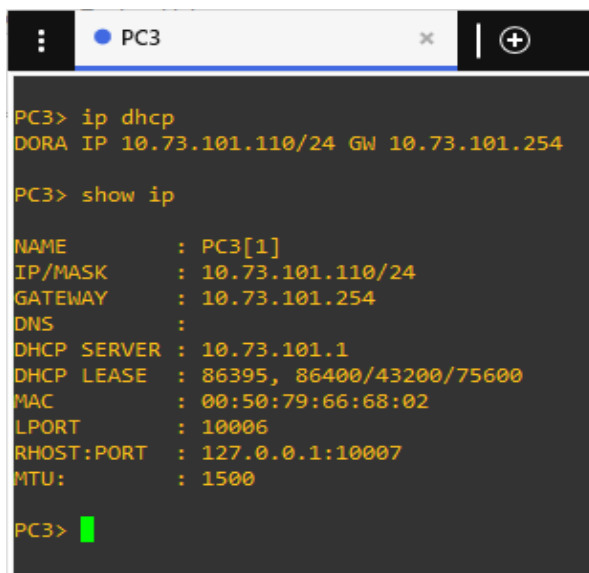
NAME          : PC2[1]
IP/MASK       : 10.73.102.110/24
GATEWAY       : 10.73.102.254
DNS           :
DHCP SERVER   : 10.73.102.1
DHCP LEASE    : 86394, 86400/43200/75600
MAC           : 00:50:79:66:68:01
LPORT        : 10008
RHOST:PORT    : 127.0.0.1:10009
MTU           : 1500

PC2>
```

Fuente 13. Autoría propia-simulador gns3

2.7

Figura 12. PC3 - DHCP -IPv4



```
PC3> ip dhcp
DORA IP 10.73.101.110/24 GW 10.73.101.254

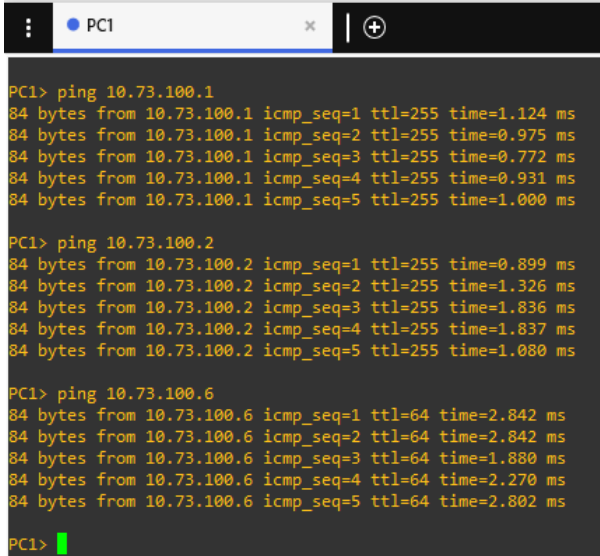
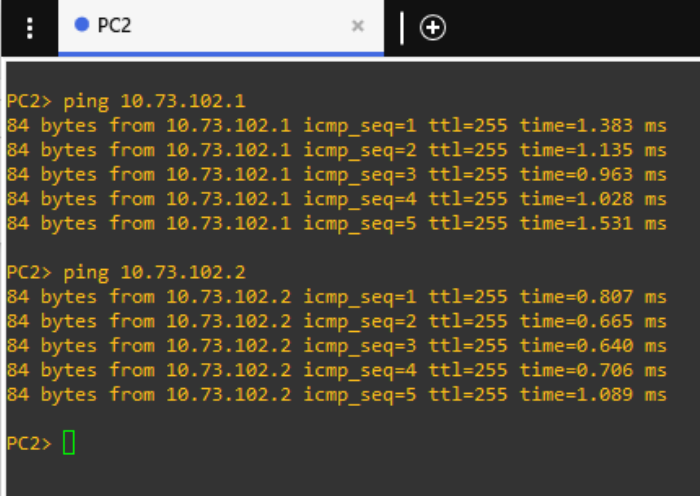
PC3> show ip

NAME          : PC3[1]
IP/MASK       : 10.73.101.110/24
GATEWAY       : 10.73.101.254
DNS           :
DHCP SERVER   : 10.73.101.1
DHCP LEASE    : 86395, 86400/43200/75600
MAC           : 00:50:79:66:68:02
LPORT        : 10006
RHOST:PORT    : 127.0.0.1:10007
MTU           : 1500

PC3>
```

Fuente 14. Autoría propia-simulador gns3

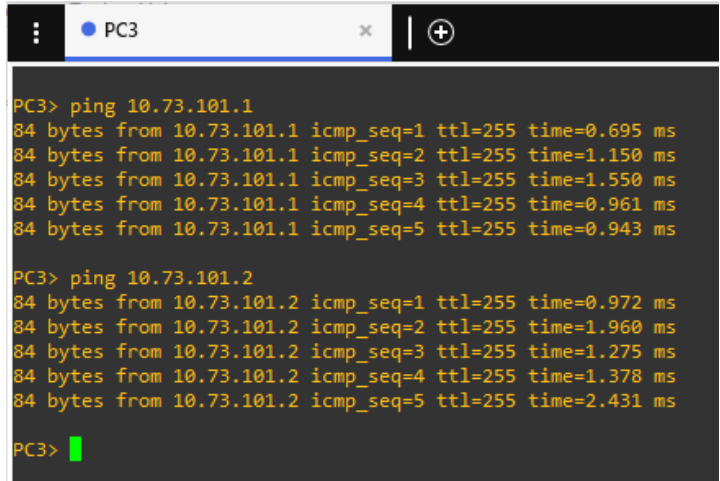
3.3.8 Compruebe la conectividad LAN local

2.8	<p>Ping desde PC1 a:</p> <ul style="list-style-type: none">• D1: 10.73.100.1• D2: 10.73.100.2• PC4: 10.73.100.6 <p>Ping desde PC2 a:</p> <ul style="list-style-type: none">• D1: 10.73.102.1• D2: 10.73.102.2	<p>Figura 13. Ping desde PC1 a D1,D2,PC4.</p>  <pre>PC1> ping 10.73.100.1 84 bytes from 10.73.100.1 icmp_seq=1 ttl=255 time=1.124 ms 84 bytes from 10.73.100.1 icmp_seq=2 ttl=255 time=0.975 ms 84 bytes from 10.73.100.1 icmp_seq=3 ttl=255 time=0.772 ms 84 bytes from 10.73.100.1 icmp_seq=4 ttl=255 time=0.931 ms 84 bytes from 10.73.100.1 icmp_seq=5 ttl=255 time=1.000 ms PC1> ping 10.73.100.2 84 bytes from 10.73.100.2 icmp_seq=1 ttl=255 time=0.899 ms 84 bytes from 10.73.100.2 icmp_seq=2 ttl=255 time=1.326 ms 84 bytes from 10.73.100.2 icmp_seq=3 ttl=255 time=1.836 ms 84 bytes from 10.73.100.2 icmp_seq=4 ttl=255 time=1.837 ms 84 bytes from 10.73.100.2 icmp_seq=5 ttl=255 time=1.080 ms PC1> ping 10.73.100.6 84 bytes from 10.73.100.6 icmp_seq=1 ttl=64 time=2.842 ms 84 bytes from 10.73.100.6 icmp_seq=2 ttl=64 time=2.842 ms 84 bytes from 10.73.100.6 icmp_seq=3 ttl=64 time=1.880 ms 84 bytes from 10.73.100.6 icmp_seq=4 ttl=64 time=2.270 ms 84 bytes from 10.73.100.6 icmp_seq=5 ttl=64 time=2.802 ms PC1> █</pre> <p>Fuente 15. Autoría propia-simulador gns3</p> <p>Figura 14. Ping desde PC2 a D1,D2.</p>  <pre>PC2> ping 10.73.102.1 84 bytes from 10.73.102.1 icmp_seq=1 ttl=255 time=1.383 ms 84 bytes from 10.73.102.1 icmp_seq=2 ttl=255 time=1.135 ms 84 bytes from 10.73.102.1 icmp_seq=3 ttl=255 time=0.963 ms 84 bytes from 10.73.102.1 icmp_seq=4 ttl=255 time=1.028 ms 84 bytes from 10.73.102.1 icmp_seq=5 ttl=255 time=1.531 ms PC2> ping 10.73.102.2 84 bytes from 10.73.102.2 icmp_seq=1 ttl=255 time=0.807 ms 84 bytes from 10.73.102.2 icmp_seq=2 ttl=255 time=0.665 ms 84 bytes from 10.73.102.2 icmp_seq=3 ttl=255 time=0.640 ms 84 bytes from 10.73.102.2 icmp_seq=4 ttl=255 time=0.706 ms 84 bytes from 10.73.102.2 icmp_seq=5 ttl=255 time=1.089 ms PC2> █</pre> <p>Fuente 16. Autoría propia-simulador gns3</p>
-----	---	--

Ping desde PC3 a:

- D1: 10.73.101.1
- D2: 10.73.101.2

Figura 15. Ping desde PC3 a D1,D2.



```
PC3> ping 10.73.101.1
84 bytes from 10.73.101.1 icmp_seq=1 ttl=255 time=0.695 ms
84 bytes from 10.73.101.1 icmp_seq=2 ttl=255 time=1.150 ms
84 bytes from 10.73.101.1 icmp_seq=3 ttl=255 time=1.550 ms
84 bytes from 10.73.101.1 icmp_seq=4 ttl=255 time=0.961 ms
84 bytes from 10.73.101.1 icmp_seq=5 ttl=255 time=0.943 ms

PC3> ping 10.73.101.2
84 bytes from 10.73.101.2 icmp_seq=1 ttl=255 time=0.972 ms
84 bytes from 10.73.101.2 icmp_seq=2 ttl=255 time=1.960 ms
84 bytes from 10.73.101.2 icmp_seq=3 ttl=255 time=1.275 ms
84 bytes from 10.73.101.2 icmp_seq=4 ttl=255 time=1.378 ms
84 bytes from 10.73.101.2 icmp_seq=5 ttl=255 time=2.431 ms

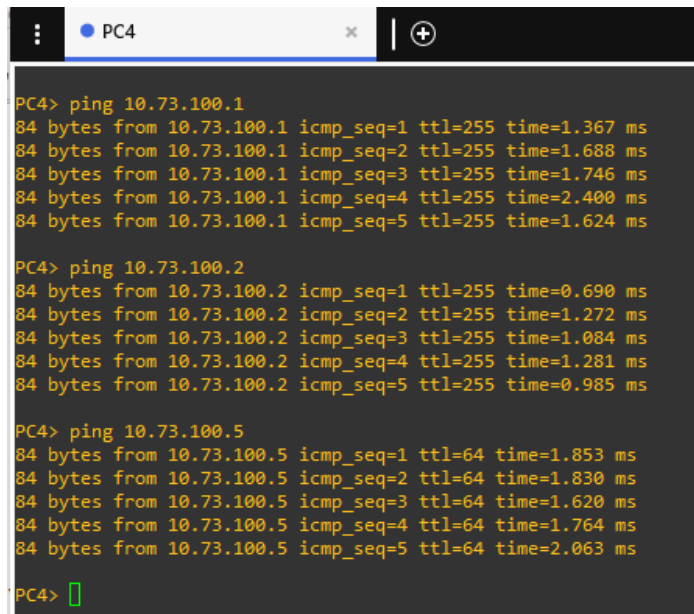
PC3> █
```

Fuente 17. Autoría propia-simulador gns3

Figura 16. Ping desde PC4 a D1,D2, PC1.

Ping desde PC4:

- D1: 10.73.100.1
- D2: 10.73.100.2
- PC1: 10.73.100.5



```
PC4> ping 10.73.100.1
84 bytes from 10.73.100.1 icmp_seq=1 ttl=255 time=1.367 ms
84 bytes from 10.73.100.1 icmp_seq=2 ttl=255 time=1.688 ms
84 bytes from 10.73.100.1 icmp_seq=3 ttl=255 time=1.746 ms
84 bytes from 10.73.100.1 icmp_seq=4 ttl=255 time=2.400 ms
84 bytes from 10.73.100.1 icmp_seq=5 ttl=255 time=1.624 ms

PC4> ping 10.73.100.2
84 bytes from 10.73.100.2 icmp_seq=1 ttl=255 time=0.690 ms
84 bytes from 10.73.100.2 icmp_seq=2 ttl=255 time=1.272 ms
84 bytes from 10.73.100.2 icmp_seq=3 ttl=255 time=1.084 ms
84 bytes from 10.73.100.2 icmp_seq=4 ttl=255 time=1.281 ms
84 bytes from 10.73.100.2 icmp_seq=5 ttl=255 time=0.985 ms

PC4> ping 10.73.100.5
84 bytes from 10.73.100.5 icmp_seq=1 ttl=64 time=1.853 ms
84 bytes from 10.73.100.5 icmp_seq=2 ttl=64 time=1.830 ms
84 bytes from 10.73.100.5 icmp_seq=3 ttl=64 time=1.620 ms
84 bytes from 10.73.100.5 icmp_seq=4 ttl=64 time=1.764 ms
84 bytes from 10.73.100.5 icmp_seq=5 ttl=64 time=2.063 ms

PC4> █
```

Fuente 18. Autoría propia-simulador gns3

3.4 Configurar los protocolos de enrutamiento IPv4 e IPv6.

Realizar las configuraciones de los protocolos de enrutamiento IPv4 - IPv6. Finalizando la actividad, la red debe ser convergente. Los pings IPv4 - IPv6 desde D1 y D2 hacia Loopback 0 se harán correctamente.

los pings de los hosts no serán correctos hasta configurar la dirección HSRP, habilitada en la siguiente parte.

Tabla 3. Tareas de configuración de Enrutamiento IPv4 e IPv6 – ENCOR SKILLS

Tarea #	Tarea	Especificación	Puntos
3.1	En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configurar OSPFv2 de área única en el área 0.	<p>Utilice OSPF Proceso ID 4 y asigne los siguientes ID de router:</p> <ul style="list-style-type: none">• R1: 0.0.4.1• R3: 0.0.4.3• D1: 0.0. 4.131• D2: 0.0.4.132 <p>En R1, R3, D1 y D2, anuncie todas las redes / VLAN conectadas directamente en el Área 0.</p> <ul style="list-style-type: none">• En R1, no anuncie la red R1 – R2.• En R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada. <p>Desactive los anuncios de OSPF v2 en:</p> <ul style="list-style-type: none">• D1: Todas las interfaces excepto E1/2• D2: Todas las interfaces excepto E1/0	8

Tarea #	Tarea	Especificación	Puntos
3.2	En la "Red de la empresa" (es decir, R1, R3, D1 y D2), configure OSPFv3 clásico de área única en el área 0.	<p>Utilice OSPF Proceso ID 6 y asigne los siguientes ID de router:</p> <ul style="list-style-type: none"> • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 <p>En R1, R3, D1 y D2, anuncie todas las redes / VLAN conectadas directamente en el Área 0.</p> <ul style="list-style-type: none"> • En R1, no anuncie la red R1 – R2. • En R1, propague una ruta predeterminada. Tenga en cuenta que BGP proporcionará la ruta predeterminada. <p>Desactive los anuncios de OSPFv3 en:</p> <ul style="list-style-type: none"> • D1: Todas las interfaces excepto E1/2 • D2: Todas las interfaces excepto E1/0 	8

Tarea #	Tarea	Especificación	Puntos
3.3	En R2 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:</p> <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. <p>Configure R2 en BGP ASN 500 y utilice el router-id 2.2.2.2.</p> <p>Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.</p> <p>En la familia de direcciones IPv4, anuncie:</p> <ul style="list-style-type: none"> • La red IPv4 de bucle invertido 0 (/32). • La ruta predeterminada (0.0.0.0/0). <p>En Familia de direcciones IPv6 , anuncie:</p> <ul style="list-style-type: none"> • La red IPv4 de bucle invertido 0 (/128). • La ruta predeterminada (::/0). 	4

Tarea #	Tarea	Especificación	Puntos
3.4	En R1 en la "Red ISP", configure MP-BGP.	<p>Configure dos rutas de resumen estáticas para la interfaz Null 0:</p> <ul style="list-style-type: none"> • Un resumen de la ruta IPv4 para 10.XY.0.0/8. • Un resumen de la ruta IPv6 para 2001:db8:100::/48. <p>Configure R1 en BGP ASN 300 y utilice el router-id 1.1.1.1.</p> <p>Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En la familia de direcciones IPv4:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv6. • Habilite la relación de vecino IPv4. • Anuncie la red 10.XY0.0/8. <p>En la familia de direcciones IPv6:</p> <ul style="list-style-type: none"> • Deshabilite la relación de vecino IPv4. • Habilite la relación de vecino IPv6. • Anuncie la red 2001:db8:100::/48. 	4

Fuente 19. Guía evaluación de habilidades de ENCOR – CCNP (Escenario 2)

3.4.1 Configurar protocolos de enrutamiento IPv4 e IPv6 en R1

TAREA 3.1 Router R1 configurar OSPFv2 de área única en el área 0.	
Especificaciones	Código en R1
Usar OSPF Proceso ID 4 y asignar los siguientes ID de router:	Configure terminal

<ul style="list-style-type: none"> • R1: 0.0.4.1 <p>Anunciar todas las redes VLAN que se conectan directamente en el Área 0.</p> <ul style="list-style-type: none"> • En R1, no anuncie la red R1 – R2. • En R1, propague una ruta predeterminada. BGP proporcionará la ruta predeterminada. 	<pre>router ospf 4 router-id 0.0.4.1 network 10.73.10.0 0.0.0.255 area 0 network 10.73.13.0 0.0.0.255 area 0 default-information originate exit</pre>
TAREA 3.2 Router R1 Configurar OSPFv3 clásico de área única en el área 0.	
Especificaciones	Código en R1
<p>Usar OSPF Proceso ID 6 y asignar los siguientes ID de router:</p> <ul style="list-style-type: none"> • R1: 0.0.6.1 <p>Anuncie todas las redes VLAN que están conectadas directamente en el Área 0.</p> <ul style="list-style-type: none"> • En R1, no anuncie la red R1 – R2. • En R1, propague una ruta predeterminada. BGP proporcionará la ruta predeterminada. 	<pre>Configure terminal ipv6 router ospf 6 router-id 0.0.6.1 default-information originate exit ipv6 router ospf 6 router-id 0.0.6.1 default-information originate exit interface e1/2 ipv6 ospf 6 area 0 exit interface e1/1 ipv6 ospf 6 area 0 exit</pre>
TAREA 3.4 Router R1 En R1 en la "Red ISP", configurar MP-BGP.	
Especificaciones	Código en R1
<p>Configurar dos rutas de resumen estáticas para la interfaz Null 0:</p> <ul style="list-style-type: none"> • Un resumen de la ruta IPv4 para 10.73.0.0/8. 	<pre>Configure terminal ip route 10.73.0.0 255.255.255.255 null0</pre>

<ul style="list-style-type: none"> • Un resumen de la ruta IPv6 para 2001:db8:100::/48. <p>Configurar R1 en BGP ASN 300 y utilice el router-id 1.1.1.1.</p> <p>Configurar una relación de vecino IPv4 e IPv6 con R2 en ASN 500.</p> <p>En la familia de direcciones IPv4:</p> <ul style="list-style-type: none"> • Deshabilitar la relación de vecino IPv6. • Habilitar la relación de vecino IPv4. • Anunciar la red 10.73.0.0/8. <p>En la familia de direcciones IPv6:</p> <ul style="list-style-type: none"> • Deshabilitar la relación de vecino IPv4. • Habilitar la relación de vecino IPv6. <p>Anunciar la red 2001:db8:100::/48.</p>	<pre> ipv6 route 2001:db8:100::/48 null0 router bgp 300 bgp router-id 1.1.1.1 neighbor 209.165.200.226 remote-as 500 neighbor 2001:db8:200::2 remote-as 500 address-family ipv4 unicast neighbor 209.165.200.226 activate no neighbor 2001:db8:200::2 activate network 10.73.0.0 mask 255.255.255.255 exit-address-family address-family ipv6 unicast no neighbor 209.165.200.226 activate neighbor 2001:db8:200::2 activate network 2001:db8:100::/48 exit-address-family </pre>
---	--

3.4.2 Configurar protocolos de enrutamiento IPv4 e IPv6 en R3

<p align="center">TAREA 3.1 Router R3 Configure OSPFv2 de área única en el área 0.</p>	
Especificaciones	Código en R3
<p>Usar OSPF Proceso ID 4 y asignar los siguientes ID de router:</p> <ul style="list-style-type: none"> • R3: 0.0.4.3 	<pre> Configure terminal router ospf 4 router-id 0.0.4.3 </pre>

Anunciar todas las redes VLAN que se conectan directamente en el Área 0.	<pre>network 10.73.11.0 0.0.0.255 area 0 network 10.73.13.0 0.0.0.255 area 0 exit</pre>
TAREA 3.2 Router R3 Configurar OSPFv3 clásico de área única en el área 0	
Especificaciones	Código en R3
Utilice OSPF Proceso ID 6 y asigne los siguientes ID de router: <ul style="list-style-type: none"> • R3: 0.0.6.3 En R3, anuncie todas las redes / VLAN conectadas directamente en el Área 0.	<pre>Configure terminal ipv6 router ospf 6 router-id 0.0.6.3 exit interface e1/0 ipv6 ospf 6 area 0 exit interface e1/1 ipv6 ospf 6 area 0 exit end</pre>

3.4.3 Configurar los protocolos de enrutamiento IPv4 e IPv6 en D1

TAREA 3.1 Switch D1 Configure OSPFv2 de área única en el área 0.	
Especificaciones	Código en D1
Usar OSPF Proceso ID 4 y asignar los siguientes ID de router: <ul style="list-style-type: none"> • D1: 0,0. 4.131 	<pre>Configure terminal router ospf 4 router-id 0.0.4.131</pre>

<p>Anunciar todas las redes / VLAN conectadas directamente en el Área 0.</p> <p>Desactivar los anuncios de OSPF v2 en:</p> <ul style="list-style-type: none"> • Todas las interfaces excepto E1/2 	<pre>network 10.73.10.0 0.0.0.255 area 0 network 10.73.100.0 0.0.0.255 area 0 network 10.73.101.0 0.0.0.255 area 0 network 10.73.102.0 0.0.0.255 area 0 passive-interface default no passive-interface e1/2 exit</pre>
<p>TAREA 3.2 Switch D1 Configurar OSPFv3 clásico de área única en el área 0.</p>	
Especificaciones	Código en D1
<p>Usar OSPF Proceso ID 6 y asignar los siguientes ID de router:</p> <ul style="list-style-type: none"> • D1: 0.0.6.131 <p>Anunciar todas las redes / VLAN conectadas directamente en el Área 0.</p> <p>Desactivar los anuncios de OSPFv3 en:</p> <ul style="list-style-type: none"> • Todas las interfaces excepto E1/2 	<pre>Configure terminal ipv6 router ospf 6 router-id 0.0.6.131 interface e1/2 ipv6 ospf 6 area 0 exit interface vlan 100 ipv6 ospf 6 area 0 exit interface vlan 101 ipv6 ospf 6 area 0 exit interface vlan 102 ipv6 ospf 6 area 0 exit passive-interface default no passive-interface e1/2 exit end</pre>

3.4.4 Configurar los protocolos de enrutamiento IPv4 e IPv6 en D2

TAREA 3.1 Switch D2 Configurar OSPFv2 de área única en el área 0.	
Especificaciones	Código en D2
Usar OSPF Proceso ID 4 y asignar los siguientes ID de router: <ul style="list-style-type: none"> • D2: 0.0.4.132 Anunciar todas las redes VLAN que se conectan directamente en el Área 0.	Configure terminal router ospf 4 router-id 0.0.4.132 network 10.73.11.0 0.0.0.255 area 0 network 10.73.100.0 0.0.0.255 area 0 network 10.73.101.0 0.0.0.255 area 0 network 10.73.102.0 0.0.0.255 area 0
Desactivar los anuncios de OSPF v2 en: <ul style="list-style-type: none"> • Todas las interfaces excepto E1/0 	passive-interface default no passive-interface e1/0 exit
TAREA 3.2 Switch D2 Configurar OSPFv3 clásico de área única en el área 0.	
Especificaciones	Código en D2
Usar OSPF Proceso ID 6 y asignar los siguientes ID de router: <ul style="list-style-type: none"> • D2: 0.0.6.132 Anunciar todas las redes VLAN que se conectan directamente en el Área 0.	Configure terminal ipv6 router ospf 6 router-id 0.0.6.132 interface e1/0 ipv6 ospf 6 area 0 exit interface vlan 100 ipv6 ospf 6 area 0 exit interface vlan 101 ipv6 ospf 6 area 0 exit

Desactivar los anuncios de OSPFv3 en: <ul style="list-style-type: none"> • Todas las interfaces excepto E1/0 	<pre> interface vlan 102 ipv6 ospf 6 area 0 exit passive-interface default no passive-interface e1/0 exit end </pre>
---	---

3.4.5 Configurar los protocolos de enrutamiento IPv4 e IPv6 en R2

TAREA 3.3 Router R2 En R2 en la "Red ISP", configurar MP-BGP.	
Especificaciones	Código en R2
Configurar dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: <ul style="list-style-type: none"> • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configurar R2 en BGP ASN 500 y utilice el router-id 2.2.2.2. Configurar y habilitar una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En la familia de direcciones IPv4, anunciar: <ul style="list-style-type: none"> • La red IPv4 de bucle invertido 0 	<pre> Configure terminal ip route 0.0.0.0 0.0.0.0 loopback 0 ipv6 route ::/0 loopback 0 router bgp 500 bgp router-id 2.2.2.2 neighbor 209.165.200.225 remote-as 300 neighbor 2001:db8:200::1 remote-as 300 address-family ipv4 neighbor 209.165.200.225 activate </pre>

<p>(/32).</p> <ul style="list-style-type: none"> • La ruta predeterminada (0.0.0.0/0). <p>En Familia de direcciones IPv6 , anunciar:</p> <ul style="list-style-type: none"> • La red IPv4 de bucle invertido 0 (/128). • La ruta predeterminada (::/0). 	<pre>no neighbor 2001:db8:200::1 activate network 2.2.2.2 mask 255.255.255.255 network 0.0.0.0 exit-address-family address-family ipv6 no neighbor 209.165.200.225 activate neighbor 2001:db8:200::1 activate network 2001:db8:2222::/128 network ::/0 exit-address-family</pre>
--	--

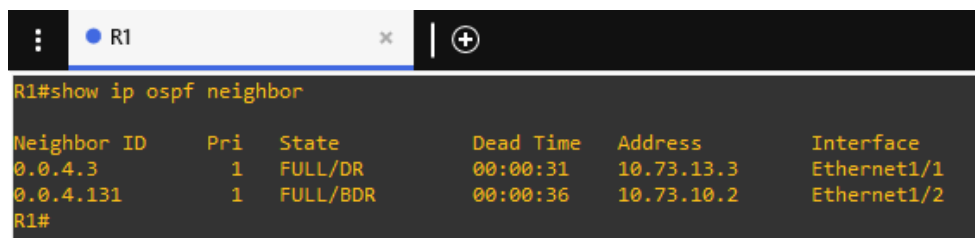
3.4.6 Verificar los protocolos de enrutamiento IPv4 e IPv6.

En este punto se usarán comandos.

- show ip ospf neighbor
- show ip route
- show ipv6 route
- show bgp

- Verificar los protocolos de enrutamiento en R1

Figura 17. Configuración OSPF en R1



```
R1#show ip ospf neighbor
Neighbor ID    Pri  State           Dead Time   Address      Interface
0.0.4.3        1    FULL/DR         00:00:31   10.73.13.3   Ethernet1/1
0.0.4.131     1    FULL/BDR        00:00:36   10.73.10.2   Ethernet1/2
R1#
```

Fuente 20. Autoría propia-simulador gns3

Figura 18. Configuración redes IPv4 en R1

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.165.200.226, 01:02:27
      2.0.0.0/32 is subnetted, 1 subnets
B     2.2.2.2 [20/0] via 209.165.200.226, 01:02:27
      10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
S     10.73.0.0/32 is directly connected, Null0
C     10.73.10.0/24 is directly connected, Ethernet1/2
L     10.73.10.1/32 is directly connected, Ethernet1/2
O     10.73.11.0/24 [110/20] via 10.73.13.3, 00:30:33, Ethernet1/1
C     10.73.13.0/24 is directly connected, Ethernet1/1
L     10.73.13.1/32 is directly connected, Ethernet1/1
O     10.73.100.0/24 [110/11] via 10.73.10.2, 01:02:49, Ethernet1/2
O     10.73.101.0/24 [110/11] via 10.73.10.2, 01:02:49, Ethernet1/2
O     10.73.102.0/24 [110/11] via 10.73.10.2, 01:02:49, Ethernet1/2
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.200.224/27 is directly connected, Ethernet1/0
L     209.165.200.225/32 is directly connected, Ethernet1/0
R1#
```

Fuente 21. Autoría propia-simulador gns3

Figura 19. Configuración redes IPv6 en R1

```
R1#show ipv6 route
IPv6 Routing Table - default - 13 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
       NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP

B ::0 [20/0]
      via FE80::2:1, Ethernet1/0
S 2001:DB8:100::/48 [1/0]
      via Null0, directly connected
O 2001:DB8:100:100::/64 [110/11]
      via FE80::D1:1, Ethernet1/2
O 2001:DB8:100:101::/64 [110/11]
      via FE80::D1:1, Ethernet1/2
O 2001:DB8:100:102::/64 [110/11]
      via FE80::D1:1, Ethernet1/2
C 2001:DB8:100:1010::/64 [0/0]
      via Ethernet1/2, directly connected
L 2001:DB8:100:1010::1/128 [0/0]
      via Ethernet1/2, receive
O 2001:DB8:100:1011::/64 [110/20]
      via FE80::3:3, Ethernet1/1
C 2001:DB8:100:1013::/64 [0/0]
      via Ethernet1/1, directly connected
L 2001:DB8:100:1013::1/128 [0/0]
      via Ethernet1/1, receive
C 2001:DB8:200::/64 [0/0]
      via Ethernet1/0, directly connected
L 2001:DB8:200::1/128 [0/0]
      via Ethernet1/0, receive
L FF00::/8 [0/0]
      via Null0, receive
R1#
```

Fuente 22. Fuente: Autoría propia-simulador gns3

- Verificar los protocolos de enrutamiento en R2

Figura 20. BGP en R2

```

R2#SHOW BGP
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
* > 0.0.0.0          0.0.0.0           0         32768 i
* > 2.2.2.2/32       0.0.0.0           0         32768 i
* > 10.73.0.0/32     209.165.200.225   0         0 300 i
R2#

```

Fuente 23. Autoría propia-simulador gns3

Figura 21. Configuración de redes IPv4 en R2.

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*   0.0.0.0/0 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
C     2.2.2.2 is directly connected, Loopback0
     10.0.0.0/32 is subnetted, 1 subnets
B     10.73.0.0 [20/0] via 209.165.200.225, 01:07:42
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     209.165.200.224/27 is directly connected, Ethernet1/0
L     209.165.200.226/32 is directly connected, Ethernet1/0
R2#

```

Fuente 24. Autoría propia-simulador gns3

Figura 22. Configuración de redes IPv6 en R2

```
R2#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, I - LISP
S  ::/0 [1/0]
   via Loopback0, directly connected
B  2001:DB8:100::/48 [20/0]
   via FE80::1:1, Ethernet1/0
C  2001:DB8:200::/64 [0/0]
   via Ethernet1/0, directly connected
L  2001:DB8:200::2/128 [0/0]
   via Ethernet1/0, receive
LC 2001:DB8:2222::1/128 [0/0]
   via Loopback0, receive
L  FF00::/8 [0/0]
   via Null0, receive
R2#
```

Fuente 25. Autoría propia-simulador gns3

- Verificar los protocolos de enrutamiento en R3

Figura 23. Configuración OSPF en R3

```
R3#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address        Interface
0.0.4.1        1    FULL/BDR        00:00:31   10.73.13.1    Ethernet1/1
0.0.4.132      1    FULL/BDR        00:00:39   10.73.11.2    Ethernet1/0
R3#
```

Fuente 26. Autoría propia-simulador gns3

Figura 24. Configuración de redes IPv4 en R3

```
R3, ENCOR Skills Assessment
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.73.13.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.73.13.1, 01:24:28, Ethernet1/1
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O     10.73.10.0/24 [110/20] via 10.73.13.1, 00:55:59, Ethernet1/1
C     10.73.11.0/24 is directly connected, Ethernet1/0
L     10.73.11.1/32 is directly connected, Ethernet1/0
C     10.73.13.0/24 is directly connected, Ethernet1/1
L     10.73.13.3/32 is directly connected, Ethernet1/1
O     10.73.100.0/24 [110/11] via 10.73.11.2, 01:24:50, Ethernet1/0
O     10.73.101.0/24 [110/11] via 10.73.11.2, 01:24:50, Ethernet1/0
O     10.73.102.0/24 [110/11] via 10.73.11.2, 01:24:50, Ethernet1/0
R3#
```

Fuente 27. Autoría propia-simulador gns3

Figura 25. Configuración de redes IPv6 en R3

```
R3#show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
OE2 ::/0 [110/1], tag 6
      via FE80::1:3, Ethernet1/1
O  2001:DB8:100:100::/64 [110/11]
      via FE80::D1:1, Ethernet1/0
O  2001:DB8:100:101::/64 [110/11]
      via FE80::D1:1, Ethernet1/0
O  2001:DB8:100:102::/64 [110/11]
      via FE80::D1:1, Ethernet1/0
C  2001:DB8:100:1010::/64 [0/0]
      via Ethernet1/1, directly connected
L  2001:DB8:100:1010::2/128 [0/0]
      via Ethernet1/1, receive
C  2001:DB8:100:1011::/64 [0/0]
      via Ethernet1/0, directly connected
L  2001:DB8:100:1011::1/128 [0/0]
      via Ethernet1/0, receive
O  2001:DB8:100:1013::/64 [110/10]
      via Ethernet1/1, directly connected
L  FF00::/8 [0/0]
      via Null0, receive
R3#
```

Fuente 28. Autoría propia-simulador gns3

- Verificar los protocolos de enrutamiento en D1

Figura 26. Configuración OSPF en D1

```

D1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
0.0.4.1          1    FULL/DR         00:00:31   10.73.10.1    Ethernet1/2
D1#

```

Fuente 29. Autoría propia-simulador gns3

Figura 27. Configuración de redes IPv4 en D1

```

D1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.73.10.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.73.10.1, 01:28:00, Ethernet1/2
      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C     10.73.10.0/24 is directly connected, Ethernet1/2
L     10.73.10.2/32 is directly connected, Ethernet1/2
O     10.73.11.0/24 [110/30] via 10.73.10.1, 00:56:06, Ethernet1/2
O     10.73.13.0/24 [110/20] via 10.73.10.1, 01:28:12, Ethernet1/2
C     10.73.100.0/24 is directly connected, Vlan100
L     10.73.100.1/32 is directly connected, Vlan100
C     10.73.101.0/24 is directly connected, Vlan101
L     10.73.101.1/32 is directly connected, Vlan101
C     10.73.102.0/24 is directly connected, Vlan102
L     10.73.102.1/32 is directly connected, Vlan102
D1#

```

Fuente 30. Autoría propia-simulador gns3

Figura 28. Configuración de redes IPv6 en D1

```
D1#
D1#show ipv6 route
IPv6 Routing Table - default - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDP - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
OE2 ::/0 [110/1], tag 6
    via FE80::1:2, Ethernet1/2
C  2001:DB8:100:100::/64 [0/0]
    via Vlan100, directly connected
L  2001:DB8:100:100::1/128 [0/0]
    via Vlan100, receive
C  2001:DB8:100:101::/64 [0/0]
    via Vlan101, directly connected
L  2001:DB8:100:101::1/128 [0/0]
    via Vlan101, receive
C  2001:DB8:100:102::/64 [0/0]
    via Vlan102, directly connected
L  2001:DB8:100:102::1/128 [0/0]
    via Vlan102, receive
C  2001:DB8:100:1010::/64 [0/0]
D1#
```

Fuente 31. Autoría propia-simulador gns3

- Verificar los protocolos de enrutamiento en D2

Figura 29. Configuración OSPF en D2

```
D2#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address        Interface
0.0.4.3        1    FULL/DR         00:00:31   10.73.11.1    Ethernet1/0
D2#
```

Fuente 32. Autoría propia-simulador gns3

Figura 30. Configuración de redes IPv4 en D2

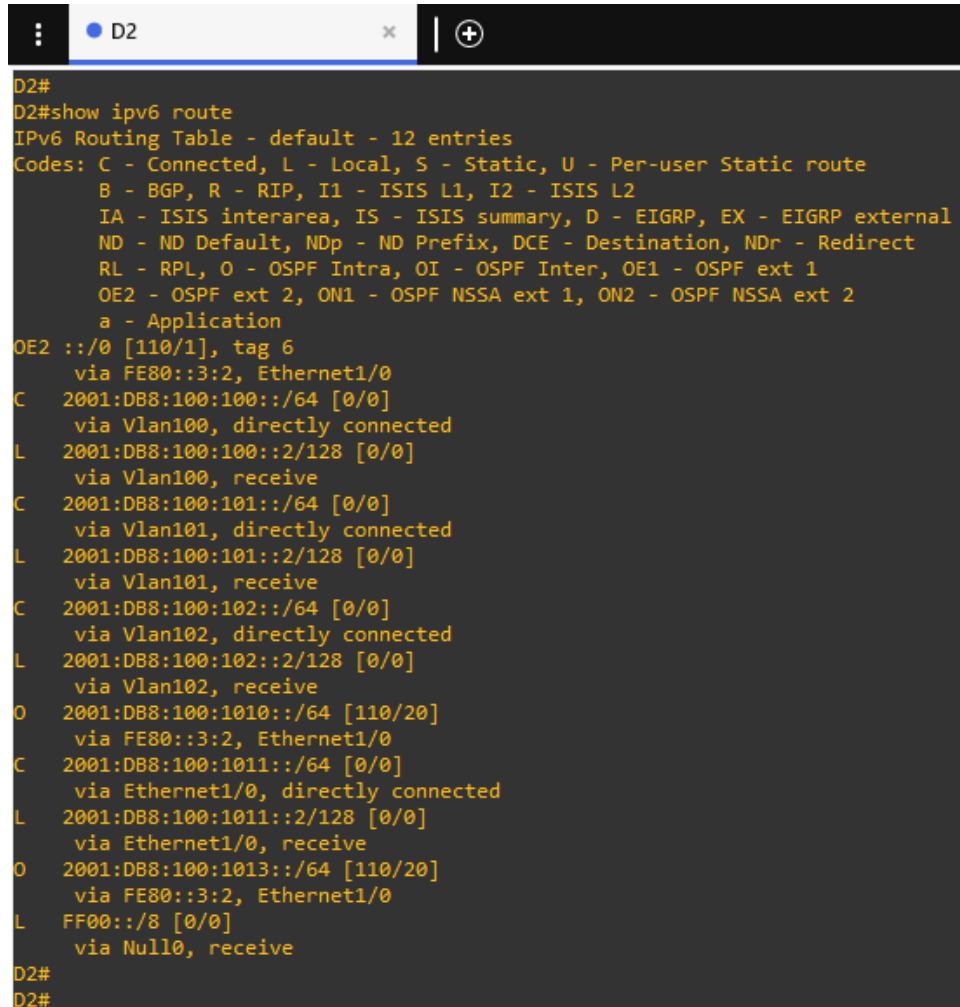
```
D2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.73.11.1 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 10.73.11.1, 01:31:06, Ethernet1/0
      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
O     10.73.10.0/24 [110/30] via 10.73.11.1, 01:02:38, Ethernet1/0
C     10.73.11.0/24 is directly connected, Ethernet1/0
L     10.73.11.2/32 is directly connected, Ethernet1/0
O     10.73.13.0/24 [110/20] via 10.73.11.1, 01:31:28, Ethernet1/0
C     10.73.100.0/24 is directly connected, Vlan100
L     10.73.100.2/32 is directly connected, Vlan100
C     10.73.101.0/24 is directly connected, Vlan101
L     10.73.101.2/32 is directly connected, Vlan101
C     10.73.102.0/24 is directly connected, Vlan102
L     10.73.102.2/32 is directly connected, Vlan102
D2#
```

Fuente 33. Autoría propia-simulador gns3

Figura 31. Configuración de redes IPv6 en D2



```
D2#
D2#show ipv6 route
IPv6 Routing Table - default - 12 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
OE2 ::0 [110/1], tag 6
   via FE80::3:2, Ethernet1/0
C  2001:DB8:100:100::/64 [0/0]
   via Vlan100, directly connected
L  2001:DB8:100:100::2/128 [0/0]
   via Vlan100, receive
C  2001:DB8:100:101::/64 [0/0]
   via Vlan101, directly connected
L  2001:DB8:100:101::2/128 [0/0]
   via Vlan101, receive
C  2001:DB8:100:102::/64 [0/0]
   via Vlan102, directly connected
L  2001:DB8:100:102::2/128 [0/0]
   via Vlan102, receive
O  2001:DB8:100:1010::/64 [110/20]
   via FE80::3:2, Ethernet1/0
C  2001:DB8:100:1011::/64 [0/0]
   via Ethernet1/0, directly connected
L  2001:DB8:100:1011::2/128 [0/0]
   via Ethernet1/0, receive
O  2001:DB8:100:1013::/64 [110/20]
   via FE80::3:2, Ethernet1/0
L  FF00::/8 [0/0]
   via Null0, receive
D2#
D2#
```

Fuente 34. Autoría propia-simulador gns3

3.5 Configurar la redundancia de primer salto.

Configurar HSRP versión 2 para proporcionar redundancia de primer salto para hosts en la "Red de la empresa".

Las tareas de configuración son las siguientes:

Tabla 4. tareas de configuración redundancia de primer salto - ENCOR SKILLS

Tarea #	Tarea	Especificación	Puntos
4.1	En D1, cree SLA IP que prueben la accesibilidad de la interfaz R1 E1/2.	<p>Cree dos SLA IP.</p> <ul style="list-style-type: none"> • Utilice el SLA número 4 para IPv4. • Utilice el SLA número 6 para IPv6. <p>Los SLA IP probarán la disponibilidad de la interfaz R1 E1/2 cada 5 segundos.</p> <p>Programa el SLA para su implementación inmediata sin hora de finalización.</p> <p>Cree un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.</p> <ul style="list-style-type: none"> • Utilice el número de pista 4 para IP SLA 4. • Utilice el número de pista 6 para IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado del SLA IP cambia de abajo a arriba después de 10 segundos , o de arriba a abajo después de 15 segundos.</p>	2

Tarea #	Tarea	Especificación	Puntos
4.2	En D2, cree SLA IP que prueben la accesibilidad de la interfaz R3 E1/0.	<p>Cree dos SLA IP.</p> <ul style="list-style-type: none"> • Utilice el SLA número 4 para IPv4. • Utilice el SLA número 6 para IPv6. <p>Los SLA IP probarán la disponibilidad de la interfaz R3 E1/0 cada 5 segundos.</p> <p>Programa el SLA para su implementación inmediata sin hora de finalización.</p> <p>Cree un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.</p> <ul style="list-style-type: none"> • Utilice el número de pista 4 para IP SLA 4. • Utilice el número de pista 6 para IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado del SLA IP cambia de abajo a arriba después de 10 segundos , o de arriba a abajo después de 15 segundos.</p>	2

Fuente 35. Guía evaluación de habilidades de ENCOR – CCNP (Escenario 2)

3.5.1 Configurar redundancia de primer salto en D1

TAREA 4.1 Switch D1 Crear SLA IP que prueben la accesibilidad de la interfaz R1 E1/2	
Especificaciones	Código en D1
<p>Crear dos SLA IP.</p> <ul style="list-style-type: none"> • Usar el SLA número 4 para IPv4. • Usar el SLA número 6 para IPv6. <p>Los SLA IP prueban la disponibilidad de la interfaz R1 E1/2 cada 5 segundos.</p>	<p>Configure terminal</p> <pre> ip sla 4 icmp-echo 10.73.10.1 frequency 5 exit ip sla 6 icmp-echo 2001:db8:100:1010::1 </pre>

<p>Programar el SLA para su implementación inmediata sin hora de finalización.</p> <p>Crear un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.</p> <ul style="list-style-type: none"> • Usar el número de pista 4 para IP SLA 4. • Usar el número de pista 6 para IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado del SLA IP cambia de abajo a arriba después de 10 segundos , o de arriba a abajo después de 15 segundos</p>	<pre>frequency 5 exit ip sla schedule 4 life forever start-time now ip sla schedule 6 life forever start-time now track 4 ip sla 4 delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit</pre>
<p>TAREA 4.3 Switch D1 Configurar HSRPv2.</p>	
<p>Especificaciones</p>	<p>Código en D1</p>
<p>D1 es el router principal para VLAN 100 y 102; por lo tanto, su prioridad también se cambiará a 150.</p> <p>Configurar HSRP versión 2.</p> <p>Configurar el grupo 104 de HSRP IPv4 para la VLAN 100:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual 10.73.100.254. • Establecer la prioridad del grupo en 150. • Habilitar la preferencia. • Realizar un seguimiento del objeto 4 que disminuya en 60. <p>Configurar el grupo 114 de HSRP IPv4 para la VLAN 101:</p>	<pre>Configure terminal interface vlan 100 standby version 2 standby 104 ip 10.73.100.254 standby 104 priority 150 standby 104 preempt standby 104 track 4 decrement 60 interface vlan 101 standby version 2</pre>

<ul style="list-style-type: none"> • Asignar la dirección IP virtual 10.73.10 1.254. • Habilitar la preferencia. • Realizar un seguimiento del objeto 4 hasta disminuir en 60. <p>Configurar el grupo HSRP IPv4 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual 10.73.10 2.254. • Establecer la prioridad del grupo en 150. • Habilitar la preferencia. • Realizar un seguimiento del objeto 4 hasta disminuir en 60. • <p>Configurar IPv6 HSRP grupo 10 6 para VLAN 100:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual mediante la configuración automática de ipv6. • Establecer la prioridad del grupo en 150. • Habilitar la preferencia. • Realizar un seguimiento del objeto 6 que disminuya en 60. <p>Configurar el grupo HSRP IPv6 11 6 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual mediante la configuración automática de ipv6. • Habilitar la preferencia. • Realizar un seguimiento del objeto 6 que disminuya en 60. <p>Configurar IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual mediante la configuración 	<pre>standby 114 ip 10.73.101.254 standby 114 preempt standby 114 track 4 decrement 60</pre> <p>interface vlan 102</p> <pre>standby version 2 standby 124 ip 10.73.102.254 standby 124 priority 150 standby 124 preempt standby 124 track 4 decrement 60</pre> <p>interface vlan 100</p> <pre>standby 106 ipv6 autoconfig standby 106 priority 150 standby 106 preempt standby 106 track 6 decrement 60 exit</pre> <p>interface vlan 101</p> <pre>standby 116 ipv6 autoconfig standby 116 preempt standby 116 track 6 decrement 60 exit</pre> <p>interface vlan 102</p> <pre>standby 126 ipv6 autoconfig</pre>
--	--

<p>automática de ipv6.</p> <ul style="list-style-type: none"> • Establecer la prioridad del grupo en 150. • Habilitar la preferencia. Realizar un seguimiento del objeto 6 que disminuya en 60. 	<pre>standby 126 priority 150 standby 126 preempt standby 126 track 6 decrement 60 exit end</pre>
---	---

3.5.2 Configurar redundancia de primer salto en D2

TAREA 4.1 Switch D2	
Crear SLA IP que pruebe la accesibilidad de la interfaz R3 E1/0.	
Especificaciones	Código en D2
<p>Crear dos SLA IP.</p> <ul style="list-style-type: none"> • Utilizar el SLA número 4 para IPv4. • Utilizar el SLA número 6 para IPv6. <p>Los SLA IP deberán probar la disponibilidad de la interfaz R3 E1/0 cada 5 segundos.</p> <p>Programar SLA para su implementación inmediata sin hora de finalización.</p> <p>Crear un objeto de SLA de IP para el SLA 4 y otro para el SLA de IP 6.</p> <ul style="list-style-type: none"> • Use el número de pista 4 para IP SLA 4. • Use el número de pista 6 para IP SLA 6. <p>Los objetos rastreados deben notificar a D1 si el estado del SLA IP cambia de abajo a arriba después de 10 segundos , o de arriba a abajo después de 15 segundos</p>	<pre>Configure terminal ip sla 4 icmp-echo 10.73.11.1 frequency 5 exit ip sla 6 icmp-echo 2001:db8:100:1011::1 frequency 5 exit ip sla schedule 4 life forever start-time now ip sla schedule 6 life forever start-time now track 4 ip sla 4 delay down 10 up 15 exit track 6 ip sla 6 delay down 10 up 15 exit</pre>

TAREA 4.3 Switch D2 Configurar HSRPv2.	
Especificaciones	Código en D2
<p>D2 es el router principal para VLAN 101; por lo tanto, la prioridad también se cambiará a 150.</p> <p>Configurar HSRP versión 2.</p> <p>Configurar el grupo 104 de HSRP IPv4 para VLAN 100:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual 10.XY.100.254. • Habilitar la preferencia. • Realizar un seguimiento del objeto 4 y disminuía en 60. • <p>Configurar el grupo 114 de HSRP IPv4 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual 10.73.101.254. • Establecer la prioridad del grupo en 150. • Habilitar la preferencia. • Realizar un seguimiento del objeto 4 hasta disminuir en 60. <p>Configurar el grupo HSRP IPv4 124 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual 10.XY.102.254. • Habilitar la preferencia. • Realizar un seguimiento del objeto 4 hasta disminuir en 60. <p>Configurar IPv6 HSRP grupo 10 6 para VLAN 100:</p>	<p>Configure terminal</p> <p>interface vlan 100 standby version 2 standby 104 ip 10.73.100.254 standby 104 preempt standby 104 track 4 decrement 60</p> <p>interface vlan 101 standby version 2 standby 114 ip 10.73.101.254 standby 114 priority 150 standby 114 preempt standby 114 track 4 decrement 60</p> <p>interface vlan 102 standby version 2 standby 124 ip 10.73.102.254 standby 124 preempt standby 124 track 4 decrement 60</p>

<ul style="list-style-type: none"> • Asignar la dirección IP virtual mediante la configuración automática de ipv6. • Habilitar la preferencia. • Realizar un seguimiento del objeto 6 que disminuya en 60. <p>Configurar el grupo HSRP IPv6 11 6 para la VLAN 101:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual mediante la configuración automática de ipv6. • Establecer la prioridad del grupo en 150. • Habilitar la preferencia. • Realizar un seguimiento del objeto 6 que disminuya en 60. <p>Configurar IPv6 HSRP grupo 126 para la VLAN 102:</p> <ul style="list-style-type: none"> • Asignar la dirección IP virtual mediante la configuración automática de ipv6. • Habilitar la preferencia. • Realizar un seguimiento del objeto 6 que disminuya en 60. 	<pre> interface vlan 100 standby 106 ipv6 autoconfig standby 106 preempt standby 106 track 6 decrement 60 exit interface vlan 101 standby 116 ipv6 autoconfig standby 116 priority 150 standby 116 preempt standby 116 track 6 decrement 60 exit interface vlan 102 standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60 exit end </pre>
---	---

3.5.3 Verificar configuración de redundancia de primer salto.

En este punto se usará el comando:

- Show standby brief
 - Verificar redundancia de primer salto en D1

Figura 32. HSRP en D1

```
D1#
D1#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Vl100     104  150 P Active local         10.73.100.2     10.73.100.254
Vl100     106  150 P Active local         FE80::D2:2     FE80::5:73FF:FEA0:6A
Vl101     114  100 P Standby 10.73.101.2    local           10.73.101.254
Vl101     116  100 P Standby FE80::D2:3     local           FE80::5:73FF:FEA0:74
Vl102     124  150 P Active local         10.73.102.2     10.73.102.254
Vl102     126  150 P Active local         FE80::D2:4     FE80::5:73FF:FEA0:7E
D1#
D1#
```

Fuente 36. Autoría propia-simulador gns3

- Verificar redundancia de primer salto en D2

Figura 33. HSRP en D2

```
D2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State  Active          Standby          Virtual IP
Vl100     104  100 P Standby 10.73.100.1    local           10.73.100.254
Vl100     106  100 P Standby FE80::D1:2     local           FE80::5:73FF:FEA0:6A
Vl101     114  150 P Active local         10.73.101.1     10.73.101.254
Vl101     116  150 P Active local         FE80::D1:3     FE80::5:73FF:FEA0:74
Vl102     124  100 P Standby 10.73.102.1    local           10.73.102.254
Vl102     126  100 P Standby FE80::D1:4     local           FE80::5:73FF:FEA0:7E
D2#
```

Fuente 37. Autoría propia-simulador gns3

4. CONCLUSIONES

Este laboratorio tuvo como objetivo implementar una red convergente con características jerárquicas. En la implementación se usaron configuraciones de protocolos de enrutamiento para lograr configurar servicios IP de calidad; en el proceso realizado en el simulador gráfico GNS3 se presentaron problemas de configuración IPv4 que se identificaron usando los comandos: *show ip route* y *show ip protocols*.

Además, se identificó un error en la discrepancia de GNS Duplex (DUPLEX_MISMATCH) entre R1 - D1 y R3 - D2, en donde los enrutadores tenían configuración de Full Duplex y los conmutadores Half Duplex, estos errores se identificaron en los puertos usando los comandos "*show interfaces* y *show interfaces status*", no obstante aunque se intentó configurar los equipos con los mismos parámetros, GNS3 continuó mostrando el error, el cual fue solucionado silenciando los mensajes con el comando, "*no cdp log mismatch duplex*", concluyendo que se debe a un error del simulador, y no a la negociación entre dispositivos.

En la configuración de los conmutadores D1 y D2, se utilizó el protocolo RSTP para prevenir bucles de capa 2, permitiendo mejorar la convergencia de 50 segundos aproximadamente que toma STP a 10 segundos de RSTP, logrando el objetivo tener una red completamente convergente.

Se implementó correctamente el protocolo de enrutamiento dinámico (OSPF), concluyendo que es el protocolo idóneo para funcionar entre redes heterogéneas de gran tamaño, ya que recalcula las rutas más rápido si se llega a presentar un cambio en la topología de la red; dando como resultado una efectividad mayor que la de otros protocolos como por ejemplo el RIP.

Se realizó correctamente la configuración del protocolo HSRP, con una prioridad de router activo en D1 y D2 de 150 versus la predeterminada de 100 para los otros dispositivos. Siendo D1 el router principal de las VLAN 100 -102, y D2 el router principal de la VLAN 101. En el proceso se reconoció que el método que utiliza HSRP para identificar un fallo en la red y en consecuencia un enrutador en estado de espera (standby) debe asumir el papel de estado activo, está basado en el envío de paquetes Hello a la dirección multicast 224.0.0.2.

Finalmente, el desarrollo de la actividad y el uso del simulador grafico GNS3 permitió generar habilidades prácticas en “*Cisco Networking*” mejorando la destreza en el diseño, la configuración y el mantenimiento de redes. Además, se fortalecieron conceptos como: VLAN, DHCP, SLAAC, HSRP, OSPF, SLA IP, etc.

Para culminar se toma en consideración la importancia de seguir profundizando en los conocimientos demandados en el ámbito de redes hoy en día, reconociendo el valor que tiene el “*Networking*” en generar oportunidades de crecimiento laboral y profesional.

5. BIBLIOGRAFÍA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). [Packet Forwarding](#). CCNP and CCIE Enterprise Core ENCORA 350-401. <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 ENCORA 350-401. <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 ENCORA 350-401. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). [OSPFv3](#). CCNP and CCIE Enterprise Core ENCORA 350-401. <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 ENCORA 350-401. <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 ENCORA 350-401. <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 ENCORA 350-401. <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 ENCORA 350-401. <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. <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. <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. <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. <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. <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. <https://1drv.ms/b/s!AAIGg5JUgUBthk8>