DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HUGO CAMILO SUAREZ MONROY

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA ELECTRÓNICA DE LA CIUDAD CHIQUINQUIRÁ

2021

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

HUGO CAMILO SUAREZ MONROY

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

DIRECTOR:

MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA ELECTRONICA DE LA CIUDAD CHIQUINQUIRA

2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CHIQUINQUIRÁ DICIEMBRE de 2021

Contenido

Lista De Ilustraciones 7

Lista De Tablas 8

Glosario 10

Resumen 12

Introducción 13

Desarrollo con el software Cisco Packet Tracer 14

1. Topología de la Red 14

2. Tabla De Direccionamiento 14

3. Consideraciones del Escenario propuesto 16

3.1 Objetivos 16

3.2 Escenario 16

3.2 Recursos necesarios 16

4. Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces 17

4.1 Paso 1: Cablear la red como se muestra en la topología 17

4.2 Paso 2: Configurar los parámetros básicos para cada dispositivo 18

5. Parte 2: Configurar la capa 2 de la red y el soporte de Host 20

5.1 Código solución 22

6. Parte 3: Configurar los protocolos de enrutamiento 23

6.1 código solución 25

7. Parte 4: Configurar la Redundancia del Primer Salto 27

7.1 Código solución 29

8. Parte 5: Seguridad 29

8.1 código solución 30

9. Parte 6: Configure las funciones de Administración de Red 31

9.1 Código Solución 31

Desarrollo con el software GNS3 32

10. Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces 32

10.2 Paso 2: Configurar los parámetros básicos para cada dispositivo. 34

11. Parte 2: Configurar la capa 2 de la red y el soporte de Host 37

11.1 Código Solución 39

12. Parte 3: Configurar los protocolos de enrutamiento 40

12.1 Código solución 41

13. Parte 4: Configurar la Redundancia del Primer Salto 43

13.1 Código Solución 45

14. Parte 5: Seguridad 46

15. Parte 6: Configure las funciones de Administración de Red 48

15.1 Código solución 48

CONCLUSIONES..... 50

BIBLIOGRAFÍA 53

Lista De Ilustraciones

Ilustración 1 Escenario Propuesto 14

Ilustración 2. Topología del Escenario Cisco Packet Tracer 17

Ilustración 3 Topología del Escenario GNS3 32

Lista De Tablas

Tabla 1. Tabla de Direccionamiento 14

Tabla 2. Codigo Parte 1 paso 2 18

Tabla 3.Indicaciones para la parte 2 21

Tabla 4. Código parte 2 22

Tabla 5. Indicaciones para la parte 3 24

Tabla 6. Código Parte 3 25

Tabla 7. Instrucciones parte 4 27

Tabla 8. Instrucciones parte 5 29

Tabla 9. Código Parte 5 31

Tabla 10. Tabla de enrutamiento para GNS3 33

Tabla 11. Código de configuración inicial 34

Tabla 12. Código configuración inicial PCs 37

Tabla 13. Indicaciones parte 2 37

Tabla 14. Código solución parte 2 39

Tabla 15. Indicaciones para la parte 3 40

Tabla 16. Código Solución Parte 3 42

Tabla 17. Indicaciones para la parte 4 44

Tabla 18. Código Solución parte 4 46

Tabla 19. Código solución parte 5 47

Tabla 20. Instrucciones parte 6 48

Tabla 21. Código solución parte 6 48

Glosario

Configuración automática de dirección sin estado (SLAAC): SLAAC es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP (Cisco, 2021b)

Enrutador: Un enrutador recibe y envía datos en redes informáticas. Los enrutadores a veces se confunden con concentradores de red, módems o conmutadores de red. Sin embargo, los enrutadores pueden combinar las funciones de estos componentes y conectarse con estos dispositivos para mejorar el acceso a Internet o ayudar a crear redes comerciales(Cisco, 2021a).

Protocolo de configuración dinámica de host (DHCP): El DHCP es una extensión del protocolo Bootstrap (BOOTP) desarrollado en 1985 para conectar dispositivos como terminales y estaciones de trabajo sin disco duro con un Bootserver, del cual reciben su sistema operativo. El DHCP se desarrolló como solución para redes de gran envergadura y ordenadores portátiles y por ello complementa a BOOTP, entre otras cosas, por su capacidad para asignar automáticamente direcciones de red reutilizables y por la existencia de posibilidades de configuración adicionales. La asignación de direcciones con DHCP se basa en un modelo cliente-servidor: el terminal que quiere conectarse solicita la configuración IP a un servidor DHCP que, por su parte, recurre a una base de datos que contiene los parámetros de red asignables. Este servidor, componente de cualquier router ADSL moderno, puede asignar los siguientes parámetros al cliente con ayuda de la información de su base de datos: Dirección IP única, Máscara de subred, Puerta de enlace estándar, Servidores DNS, Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol**)** (Digital Guide IONOS, 2020)**.**

Protocolo de enrutamiento: Los protocolos de enrutamiento administran la actividad de enrutamiento en un sistema. Los enrutadores intercambiar información de enrutamiento con otros hosts para mantener las rutas conocidas a las redes remotas. Tanto los enrutadores como los hosts pueden ejecutar protocolos de enrutamientov(ORACLE, 2021).

Switches: Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edicio u ocina. Por ejemplo, un switch puede conectar sus

computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad. Existen dos tipos básicos de switches: administrados y no administrados. Los switches no administrado funcionan de forma automática y no permiten realizar cambios. Los equipos en redes domésticas suelen utilizar switches no administrados. Los switches administrados permiten su programación. Esto proporciona una gran -exibilidad porque el switch se puede supervisar y ajustar de forma local o remota para proporcionarle control sobre el desplazamiento del tráco en la red y quién tiene acceso a la misma (Cisco, 2012).

Resumen

En este documento se encuentra el desarrollo por medio de software Cisco Packet Tracer y GNS3 del escenario propuesto una red con su respectivos protocolos de comunicación la cual permite la configuración de la red para que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace predeterminada (default gateway) y para que los protocolos configurados estén operativos dentro de la parte correspondiente a la "Red de la Compañía" en la topología. Tenga presente verificar que las configuraciones cumplan con las especificaciones proporcionadas y que los dispositivos funcionen como se requiere. Por medio de una solución secuencializada, la primera parte consta de la elaboración de la topología de la red y configuración básica de direccionamiento en la segunda parte se completa la configuración de la capa 2 de la red y establece el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse y los host recibir direccionamiento de DHCP y SLAAC. La parte tres se configura los protocolos de enrutamiento IPv4 e IPv6.

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

Abstract

This document contains the development by means of Cisco Packet Tracer software and GNS3 software of the proposed scenario, a network with its communication protocols which allows the configuration of the network so that there is complete accessibility from one end to the other, so that the hosts have a reliable support for the default gateway and for the configured protocols to be operational within the "Company Network" part of the topology. Please note to verify that the configurations meet the specifications provided and that the devices function as required. By means of a sequential solution, the first part consists of the elaboration of the network topology and basic addressing configuration, in the second part the network layer 2 configuration is completed and the basic host support is established. At the end of this part, all switches should be able to communicate and the hosts will receive the address from DHCP and SLAAC. Part three configures the IPv4 and IPv6 routing protocols.

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

Introducción

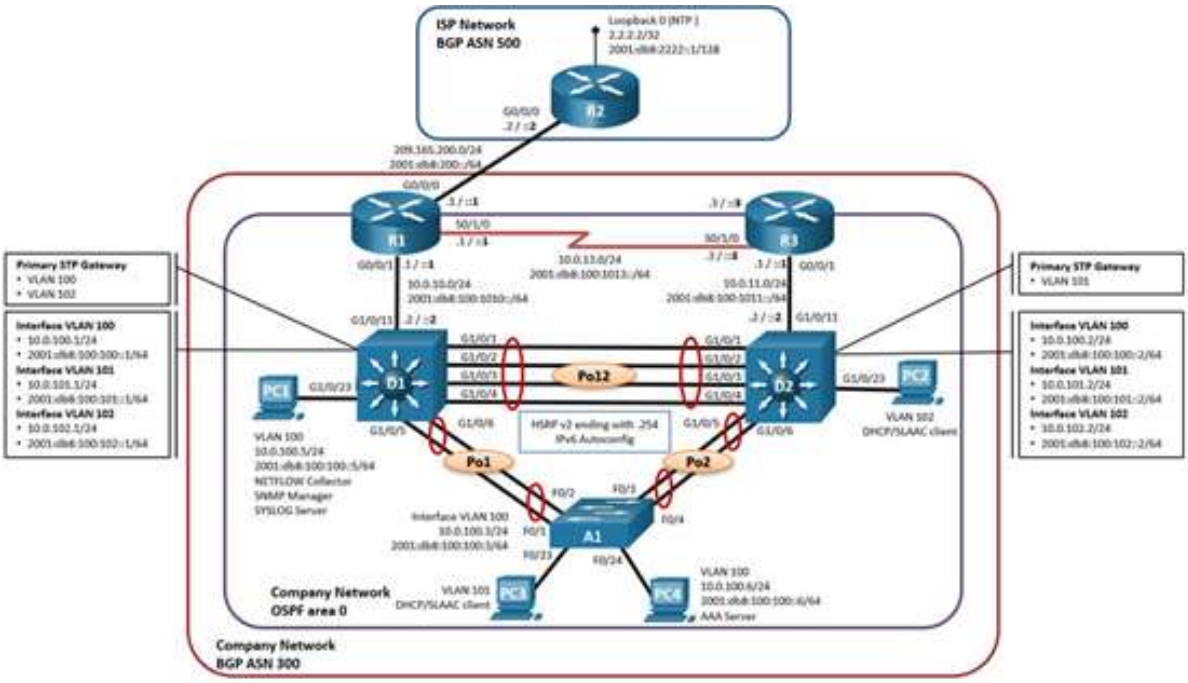
El desarrollo del curso diplomado de profundización cisco se manifiesta la aplicación de diferentes protocolos para la correcta configuración según sea la necesidad de diferentes sistemas de comunicación bajo sus respectivas topologías físicas y lógicas. El siguiente documento muestra el paso a paso de cómo se aplicaron las diferentes competencias adquiridas en el desarrollo según los lineamientos dados del escenario propuesto, el cual tiene como objetivos: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces, Configurar la capa 2 de la red y el soporte de Host, Configurar los protocolos de enrutamiento, Configurar la redundancia del primer salto, Configurar la seguridad y Configurar las características de administración de red. El desarrollo de estos objetivos se mostrara en los respectivos títulos 4, 5, 6, 7 y 8 en adelante y sus respectivos pasos en los subtítulos de cada uno de estos.

El documento presenta el siguiente orden, primero una contextualización del escenario a desarrollar en donde expone la topología de Red, la tabla de direccionamiento, las características de escenario los recursos implementados, el desarrollo del objetivo 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces; El desarrollo del objetivo 2: Configurar la capa 2 de la red y el soporte de Host (En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC) y el desarrollo del objetivo 3 Configurar los protocolos de enrutamiento (En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente; desarrollo del objetivo 4 Configurar la redundancia del primer salto aplicando el Protocolo de redundancia de router virtual versión 2 (VRRPv2) que es un protocolo de elección no exclusivo que asigna de forma dinámica la responsabilidad de uno o más routers virtuales a los routers VRRP en una LAN IPv4. El objetivo 5 Seguridad donde se debe configurar varios mecanismos de seguridad en los dispositivos de la topología crreando bajo el encripción SCRYPT y el algoritmo de encripción SCRYPT usuarios con diferentes prestaciones y extensiones sobre la red y el objetivo 6 donde se configuran varias funciones de administración de red como lo son

Desarrollo con el software Cisco Packet Tracer

1. Topología de la Red

Ilustración 1 Escenario Propuesto



2. Tabla De Direccionamiento.

Tabla 1. Tabla de Direccionamiento

Dis	*Interfaz*	*Dirección IPv4*	*Dirección IPv6*	*IPv6 Link-Local*
R1	*G0/0/0*	*209.165.200.225/27*	*2001:db8:200::1/64*	*fe80::1:1*
	G0/0/1	*10.0.10.1/24*	*2001:db8:100:1010::1/64*	*fe80::1:2*
	S0/1/0	*10.0.13.1/24*	*2001:db8:100:1013::1/64*	*fe80::1:3*

Dis	*Interfaz*	*Dirección IPv4*	*Dirección IPv6*	*IPv6 Link-Local*
R2	*G0/0/0*	*209.165.200.226/27*	*2001:db8:200::2/64*	*fe80::2:1*
	Loopback0	*2.2.2.2/32*	*2001:db8:2222::1/128*	*fe80::2:3*
R3	*G0/0/1*	*10.0.11.1/24*	*2001:db8:100:1011::1/64*	*fe80::3:2*
	S0/1/0	*10.0.13.3/24*	*2001:db8:100:1013::3/64*	*fe80::3:3*
D1	*G1/0/11*	*10.0.10.2/24*	*2001:db8:100:1010::2/64*	*fe80::d1:1*
	VLAN 100	*10.0.100.1/24*	*2001:db8:100:100::1/64*	*fe80::d1:2*
	VLAN 101	*10.0.101.1/24*	*2001:db8:100:101::1/64*	*fe80::d1:3*
	VLAN 102	*10.0.102.1/24*	*2001:db8:100:102::1/64*	*fe80::d1:4*
D2	*G1/0/11*	*10.0.11.2/24*	*2001:db8:100:1011::2/64*	*fe80::d2:1*
	VLAN 100	*10.0.100.2/24*	*2001:db8:100:100::2/64*	*fe80::d2:2*
	VLAN 101	*10.0.101.2/24*	*2001:db8:100:101::2/64*	*fe80::d2:3*
	VLAN 102	*10.0.102.2/24*	*2001:db8:100:102::2/64*	*fe80::d2:4*
A1	*VLAN 100*	*10.0.100.3/23*	*2001:db8:100:100::3/64*	*fe80::a1:1*
PC1	*NIC*	*10.0.100.5/24*	*2001:db8:100:100::5/64*	*EUI-64*
PC2	*NIC*	*DHCP*	*SLAAC*	*EUI-64*
PC3	*NIC*	*DHCP*	*SLAAC*	*EUI-64*
PC4	*NIC*	*10.0.100.6/24*	*2001:db8:100:100::6/64*	*EUI-64*

3. Consideraciones del Escenario propuesto

3.1 Objetivos

- Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
- Part 2: Configurar la capa 2 de la red y el soporte de Host
- Part 3: Configurar los protocolos de enrutamiento
- Part 4: Configurar la redundancia del primer salto
- Part 5: Configurar la seguridad
- Part 6: Configurar las características de administración de red

3.2 Escenario

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

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

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

Nota: La plantilla de Switch Database Manager (SDM) instalada por defecto en un switch Catalyst 2960 no soporta IPv6. Debe cambiar la plantilla SDM por defecto a una plantilla predeterminada dual-ipv4-and-ipv6 utilizando el comando de configuración global sdm prefer dual-ipv4-and-ipv6 default. Cambiar la plantilla requerirá el reinicio del switch.

3.2 Recursos necesarios

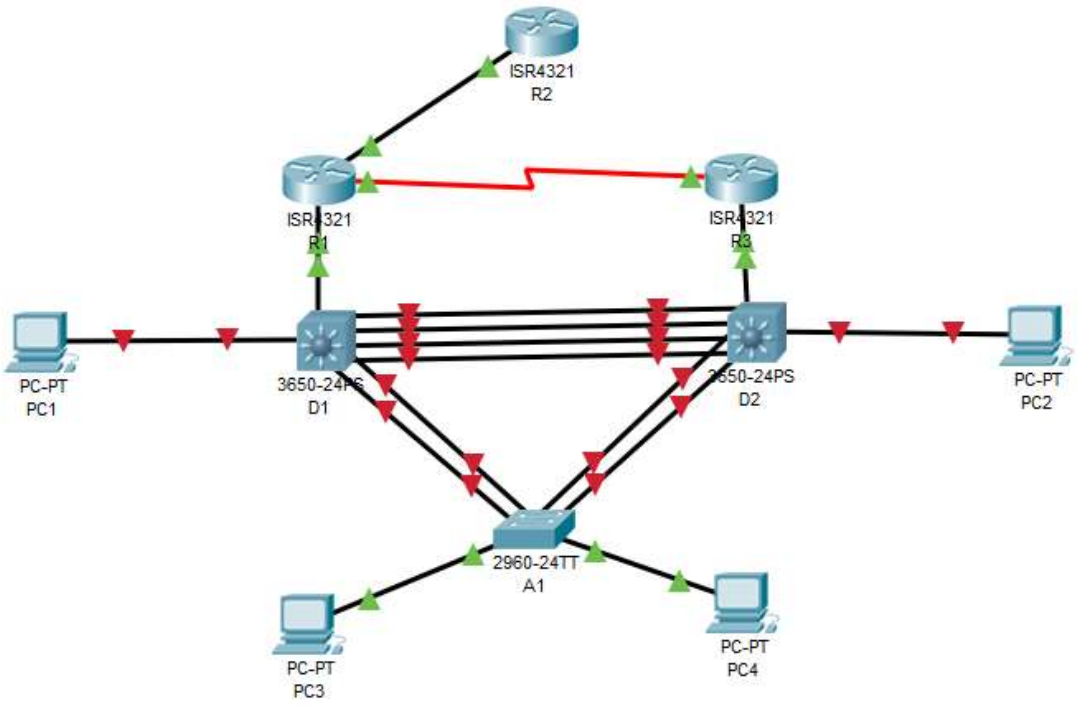
- 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable).
- 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable).
- 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable).
- 4 PCs (utilice el programa de emulación de terminal).
- Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola.
- Los cables Ethernet y seriales van como se muestra en la topología.

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

4.1 Paso 1: Cablear la red como se muestra en la topología

Conecte los dispositivos como se muestra en el diagrama de topología y conecte los cables según sea necesario.

Ilustración 2. Topología del Escenario Cisco Packet Tracer



4.2 Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Tabla 2. Codigo Parte 1 paso 2

Router R1 *hostname R1* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # R1, ENCOR Skills Assessment, Scenario 1 #* *line con 0* *exec-timeout 0 0* *logging synchronous* *exit* *interface g0/0/0* *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 g0/0/1* *ip address 10.0.10.1 255.255.255.0* *ipv6 address fe80::1:2 link-local* *ipv6 address 2001:db8:100:1010::1/64* *no shutdown* *exit* *interface s0/1/0* *ip address 10.0.13.1 255.255.255.0* *ipv6 address fe80::1:3 link-local* *ipv6 address 2001:db8:100:1013::1/64* *no shutdown* *exit*	*Router R2* *hostname R2* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # R2, ENCOR Skills Assessment, Scenario 1 #* *line con 0* *exec-timeout 0 0* *logging synchronous* *exit* *interface g0/0/0* *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*
Router R3 *hostname R3* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # R3, ENCOR Skills Assessment, Scenario 1 #* *line con 0* *exec-timeout 0 0* *logging synchronous* *exit* *interface g0/0/1* *ip address 10.0.11.1 255.255.255.0* *ipv6 address fe80::3:2 link-local* *ipv6 address 2001:db8:100:1011::1/64*	*Switch A1* *sdm prefer dual-ipv4-and-ipv6 default* *hostname A1* *no ip domain lookup* *banner motd # A1, ENCOR Skills Assessment, Scenario 1 #* *line con 0* *exec-timeout 0 0* *logging synchronous* *exit* *vlan 100* *name Management* *exit* *vlan 101*

no shutdown *exit* *interface s0/1/0* *ip address 10.0.13.3 255.255.255.0* *ipv6 address fe80::3:3 link-local* *ipv6 address 2001:db8:100:1010::2/64* *no shutdown* *exit*	*name UserGroupA* *exit* *vlan 102* *name UserGroupB* *exit* *vlan 999* *name NATIVE* *exit* *interface vlan 100* *ip address 10.0.100.3 255.255.255.0* *ipv6 address fe80::a1:1 link-local* *ipv6 address 2001:db8:100:100::3/64* *no shutdown* *exit* *interface range f0/5-22* *shutdown* *exit*
Switch D1 *hostname D1* *ip routing* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # D1, ENCOR Skills Assessment, Scenario 1 #* *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 g1/0/11* *no switchport* *ip address 10.0.10.2 255.255.255.0* *ipv6 address fe80::d1:1 link-local* *ipv6 address 2001:db8:100:1010::2/64* *no shutdown* *exit* *interface vlan 100* *ip address 10.0.100.1 255.255.255.0* *ipv6 address fe80::d1:2 link-local* *ipv6 address 2001:db8:100:100::1/64*	*Switch D2* *hostname D2* *ip routing* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # D2, ENCOR Skills Assessment, Scenario 1 #* *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 g1/0/11* *no switchport* *ip address 10.0.11.2 255.255.255.0* *ipv6 address fe80::d1:1 link-local* *ipv6 address 2001:db8:100:1011::2/64* *no shutdown* *exit* *interface vlan 100* *ip address 10.0.100.2 255.255.255.0* *ipv6 address fe80::d2:2 link-local* *ipv6 address 2001:db8:100:100::2/64*

no shutdown *exit* *interface vlan 101* *ip address 10.0.101.1 255.255.255.0* *ipv6 address fe80::d1:3 link-local* *ipv6 address 2001:db8:100:101::1/64* *no shutdown* *exit* *interface vlan 102* *ip address 10.0.102.1 255.255.255.0* *ipv6 address fe80::d1:4 link-local* *ipv6 address 2001:db8:100:102::1/64* *no shutdown* *exit* *ip dhcp excluded-address 10.0.101.1 10.0.101.109* *ip dhcp excluded-address 10.0.101.141 10.0.101.254* *ip dhcp excluded-address 10.0.102.1 10.0.102.109* *ip dhcp excluded-address 10.0.102.141 10.0.102.254* *ip dhcp pool VLAN-101* *network 10.0.101.0 255.255.255.0* *default-router 10.0.101.254* *exit* *ip dhcp pool VLAN-102* *network 10.0.102.0 255.255.255.0* *default-router 10.0.102.254* *exit* *interface range g1/0/1-10, g1/0/12-24, g1/1/1-4* *shutdown* *exit*	*no shutdown* *exit* *interface vlan 101* *ip address 10.0.101.2 255.255.255.0* *ipv6 address fe80::d2:3 link-local* *ipv6 address 2001:db8:100:101::2/64* *no shutdown* *exit* *interface vlan 102* *ip address 10.0.102.2 255.255.255.0* *ipv6 address fe80::d2:4 link-local* *ipv6 address 2001:db8:100:102::2/64* *no shutdown* *exit* *ip dhcp excluded-address 10.0.101.1 10.0.101.209* *ip dhcp excluded-address 10.0.101.241 10.0.101.254* *ip dhcp excluded-address 10.0.102.1 10.0.102.209* *ip dhcp excluded-address 10.0.102.241 10.0.102.254* *ip dhcp pool VLAN-101* *network 10.0.101.0 255.255.255.0* *default-router 10.0.101.254* *exit* *ip dhcp pool VLAN-102* *network 10.0.102.0 255.255.255.0* *default-router 10.0.102.254* *exit* *interface range g1/0/1-10, g1/0/12-24, g1/1/1-4* *shutdown* *exit*

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

running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

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

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

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

Tabla 3.Indicaciones para la parte 2

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

#	Tarea	Espesificaciones
		Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).
2.7	*Verifique los servicios DHCP IPv4.*	*PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.*
2.8	*Verifique la conectividad de la LAN local.*	*PC1 debería hacer ping con éxito a:* *• D1: 10.0.100.1* *• D2: 10.0.100.2* *• PC4: 10.0.100.6* *PC2 debería hacer ping con éxito a:* *• D1: 10.0.102.1* *• D2: 10.0.102.2* *PC3 debería hacer ping con éxito a:* *• D1: 10.0.101.1* *• D2: 10.0.101.2* *PC4 debería hacer ping con éxito a:* *• D1: 10.0.100.1* *• D2: 10.0.100.2* *• PC1: 10.0.100.5*

5.1 Código solución

Tabla 4. Código parte 2

Switch D1	*Switch D2*
interface range g1/0/1-4 *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 12 mode active* *no shutdown* *exit* *interface range g1/0/5-6* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 1 mode active* *no shutdown* *exit* *spanning-tree mode rapid-pvst* *spanning-tree vlan 100,102 root primary* *spanning-tree vlan 101 root secondary*	*interface range g1/0/1-4* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 12 mode active* *no shutdown* *exit* *interface range g1/0/5-6* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 2 mode active* *no shutdown* *exit* *!* *spanning-tree mode rapid-pvst* *spanning-tree vlan 101 root primary*

interface g1/0/23 *switchport mode access* *switchport access vlan 100* *spanning-tree portfast* *no shutdown* *exit* *end*	*spanning-tree vlan 100,102 root secondary* *!* *interface g1/0/23* *switchport mode access* *switchport access vlan 102* *spanning-tree portfast* *no shutdown* *exit* *end*
Switch A1 *spanning-tree mode rapid-pvst* *interface range f0/1-2* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 1 mode active* *no shutdown* *exit* *interface range f0/3-4* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 2 mode active* *no shutdown* *exit* *interface f0/23* *switchport mode access* *switchport access vlan 101* *spanning-tree portfast* *no shutdown* *exit* *interface f0/24* *switchport mode access* *switchport access vlan 100* *spanning-tree portfast* *no shutdown* *exit* *end*	

6. Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.
Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.
Las tareas de configuración son las siguientes:

Tabla 5. Indicaciones para la parte 3

#	Tarea	Detalle
3.1	*En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.*	*Use OSPF Process ID 4 y asigne los siguientes router-IDs:* *• R1: 0.0.4.1* *• R3: 0.0.4.3* *• D1: 0.0.4.131* *• D2: 0.0.4.132* *En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.* *• En R1, no publique la red R1 – R2.* *• En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.* *Deshabilite las publicaciones OSPFv2 en:* *• D1: todas las interfaces excepto G1/0/11* *• D2: todas las interfaces excepto G1/0/11*
3.2	*En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.*	*Use OSPF Process ID 6 y asigne los siguientes router-IDs:* *• R1: 0.0.6.1* *• R3: 0.0.6.3* *• D1: 0.0.6.131* *• D2: 0.0.6.132* *En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.* *• En R1, no publique la red R1 – R2.* *• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.* *Deshabilite las publicaciones OSPFv3 en:* *• D1: todas las interfaces excepto G1/0/11* *• D2: todas las interfaces excepto G1/0/11*
3.3	*En R2 en la "Red ISP", configure MP-BGP.*	*Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:* *• Una ruta estática predeterminada IPv4.* *• Una ruta estática predeterminada IPv6.* *Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.* *Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.* *En IPv4 address family, anuncie:* *• La red Loopback 0 IPv4 (/32).* *• La ruta por defecto (0.0.0.0/0).* *En IPv6 address family, anuncie:* *• La red Loopback 0 IPv4 (/*

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

6.1 código solución

Tabla 6. Código Parte 3

Router R1	*Router R2*
router ospf 4 *router-id 0.0.4.1* *network 10.0.10.0 0.0.0.255 area 0* *network 10.0.13.0 0.0.0.255 area 0* *default-information originate* *exit* *ipv6 router ospf 6* *router-id 0.0.6.1* *default-information originate* *exit* *interface g0/0/1* *ipv6 ospf 6 area 0* *exit* *interface s0/1/0* *ipv6 ospf 6 area 0* *exit* *!ip route 10.0.0.0 255.0.0.0 null0* *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*	*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* *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*

no neighbor 2001:db8:200::2 activate *network 10.0.0.0 mask 255.0.0.0* *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*	
Router R3 *router ospf 4* *router-id 0.0.4.3* *network 10.0.11.0 0.0.0.255 area 0* *network 10.0.13.0 0.0.0.255 area 0* *exit* *ipv6 router ospf 6* *router-id 0.0.6.3* *exit* *interface g0/0/1* *ipv6 ospf 6 area 0* *exit* *interface s0/1/0* *ipv6 ospf 6 area 0* *exit* *end*	*Switch D1* *router ospf 4* *router-id 0.0.4.131* *network 10.0.100.0 0.0.0.255 area 0* *network 10.0.101.0 0.0.0.255 area 0* *network 10.0.102.0 0.0.0.255 area 0* *network 10.0.10.0 0.0.0.255 area 0* *passive-interface default* *no passive-interface g1/0/11* *exit* *ipv6 router ospf 6* *router-id 0.0.6.131* *passive-interface default* *no passive-interface g1/0/11* *exit* *interface g1/0/11* *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* *end*
Switch D2 *router ospf 4* *router-id 0.0.4.132* *network 10.0.100.0 0.0.0.255 area 0* *network 10.0.101.0 0.0.0.255 area 0* *network 10.0.102.0 0.0.0.255 area 0* *network 10.0.11.0 0.0.0.255 area 0* *passive-interface default* *no passive-interface g1/0/11* *exit* *ipv6 router ospf 6* *router-id 0.0.6.132* *passive-interface default* *no passive-interface g1/0/11* *exit*	

interface g1/0/11 *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* *end*	

7. Parte 4: Configurar la Redundancia del Primer Salto

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

Las tareas de configuración son las siguientes:

Tabla 7. Instrucciones parte 4

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

#	Tarea	Detalle
		• *Use el número de rastreo 4 para la IP SLA 4.* • *Use el número de rastreo 6 para la SLA 6.* *Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos*
4.3	*En D1 configure HSRPv2.*	*D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..* *Configure HSRP version 2.* *Configure IPv4 HSRP grupo 104 para la VLAN 100:* • *Asigne la dirección IP virtual 10.0.100.254.* • *Establezca la prioridad del grupo en 150.* • *Habilite la preferencia (preemption).* • *Rastree el objeto 4 y decremente en 60.* *Configure IPv4 HSRP grupo 114 para la VLAN 101:* • *Asigne la dirección IP virtual 10.0.101.254.* • *Habilite la preferencia (preemption).* • *Rastree el objeto 4 para disminuir en 60.* *Configure IPv4 HSRP grupo 124 para la VLAN 102:* • *Asigne la dirección IP virtual 10.0.102.254.* • *Establezca la prioridad del grupo en 150.* • *Habilite la preferencia (preemption).* • *Rastree el objeto 4 para disminuir en 60.* *Configure IPv6 HSRP grupo 106 para la VLAN 100:* • *Asigne la dirección IP virtual usando ipv6 autoconfig.* • *Establezca la prioridad del grupo en 150.* • *Habilite la preferencia (preemption).* • *Rastree el objeto 6 y decremente en 60.* *Configure IPv6 HSRP grupo 116 para la VLAN 101:* • *Asigne la dirección IP virtual usando ipv6 autoconfig.* • *Habilite la preferencia (preemption).* • *Registre el objeto 6 y decremente en 60.* *Configure IPv6 HSRP grupo 126 para la VLAN 102:* • *Asigne la dirección IP virtual usando ipv6 autoconfig.* • *Establezca la prioridad del grupo en 150.* • *Habilite la preferencia (preemption).* • *Rastree el objeto 6 y decremente en 60*
	En D2, configure HSRPv2.	*D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.* *Configure HSRP version 2.* *Configure IPv4 HSRP grupo 104 para la VLAN 100:* • *Asigne la dirección IP virtual 10.0.100.254.* • *Habilite la preferencia (preemption).* • *Rastree el objeto 4 y decremente en 60.* *Configure IPv4 HSRP grupo 114 para la VLAN 101:* • *Asigne la dirección IP virtual 10.0.101.254.* • *Establezca la prioridad del grupo en 150.* • *Habilite la preferencia (preemption).*

#	Tarea	Detalle
		• Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo 106 para la VLAN 100: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 126 para la VLAN 102: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

7.1 Código solución

Nota; el comando ip sla está fuera de la funciones ofrecidas por cisco packet tracer, y el código presentado aunque correcto no puede ser ejecutado en su totalidad en dicho software.

8. Parte 5: Seguridad

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

Las tareas de configuración son las siguientes:

Tabla 8. Instrucciones parte 5

#	Tarea	Detalle
5.1	*En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.*	*Contraseña: cisco12345cisco*

#	Tarea	Detalle
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: sadmin • Nivel de privilegio 15 • Contraseña: cisco12345cisco
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.
5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: $trongPass
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.

8.1 código solución

Nota; algunos de la funciones ofrecidas por cisco packet tracer, y el código presentado aunque correcto no puede ser ejecutado en su totalidad en dicho software.

R1	R3
aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 key $trongPass exit aaa authentication login default group radius local end	aaa new-model radius server RADIUS address ipv4 10.0.100.6 auth-port 1812 key $trongPass exit aaa authentication login default group radius local end

9. Parte 6: Configure las funciones de Administración de Red

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

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

9.1 Código Solución

Tabla 9. Código Parte 5

R1	*R2*
clock timezone word 23 *ntp server 2.2.2.2* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit*	*ntp master 3* *end*
D1	*D2*
ntp server 10.0.10.1 *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit*	*ntp server 10.0.10.1* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit*

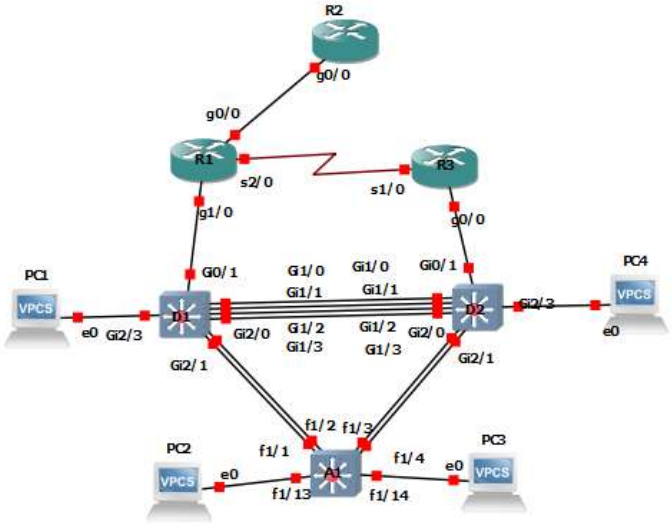
A1	R3
ntp server 10.0.10.1 *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit*	*ntp server 10.0.10.1* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit*

Desarrollo con el software GNS3

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

Sobre el escenario planteado se aclara que aunque GNs3 tiene equivalencias de algunos dispositivos, este permite trabajar con routers y swichets genéricos de diferentes tipos en este caso se han seleccionado aquellos con mayores jerarquías para que ningún comando implementado sea incorrecto porl capa que maneja el dispositivo.

Ilustración 3 Topología del Escenario GNS3



Dada la configuración de los dispositivos implementación de lo equipos y debido que la disposición de la interfaces varia fue necesario modificar la tabla de

enrutamiento en el nombre de algunas de sus interfaces, y eventualmente el código de iniciación respecto al desarrollado en cisco Packet Tracer

Tabla 10. Tabla de enrutamiento para GNS3

Dis	*Interfaz**	*Dirección IPv4*	*Dirección IPv6*	*IPv6 Link-Local*
R1	*G0/0*	*209.165.200.225/27*	*2001:db8:200::1/64*	*fe80::1:1*
	G1/0	*10.0.10.1/24*	*2001:db8:100:1010::1/64*	*fe80::1:2*
	S2/0	*10.0.13.1/24*	*2001:db8:100:1013::1/64*	*fe80::1:3*
R2	*G0/0*	*209.165.200.226/27*	*2001:db8:200::2/64*	*fe80::2:1*
	Loopback0	*2.2.2.2/32*	*2001:db8:2222::1/128*	*fe80::2:3*
R3	*G0/0*	*10.0.11.1/24*	*2001:db8:100:1011::1/64*	*fe80::3:2*
	S1/0	*10.0.13.3/24*	*2001:db8:100:1013::3/64*	*fe80::3:3*
D1	*Gi0/1*	*10.0.10.2/24*	*2001:db8:100:1010::2/64*	*fe80::d1:1*
	VLAN 100	*10.0.100.1/24*	*2001:db8:100:100::1/64*	*fe80::d1:2*
	VLAN 101	*10.0.101.1/24*	*2001:db8:100:101::1/64*	*fe80::d1:3*
	VLAN 102	*10.0.102.1/24*	*2001:db8:100:102::1/64*	*fe80::d1:4*
D2	*Gi0/1*	*10.0.11.2/24*	*2001:db8:100:1011::2/64*	*fe80::d2:1*
	VLAN 100	*10.0.100.2/24*	*2001:db8:100:100::2/64*	*fe80::d2:2*
	VLAN 101	*10.0.101.2/24*	*2001:db8:100:101::2/64*	*fe80::d2:3*

Dis	Interfaz*	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

10.2 Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

nota: para guardar En el switch o router se ejecutar: copy running-config startup-config o “wr”

Tabla 11. Código de configuración inicial

Router R1	Router R2
hostname R1 ipv6 unicast-routing no ip domain lookup banner motd # R1, ENCOR Skills Assessment, Scenario 1 # line con 0 exec-timeout 0 0 logging synchronous exit interface g0/0 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 g1/0	hostname R2 ipv6 unicast-routing no ip domain lookup banner motd # R2, ENCOR Skills Assessment, Scenario 1 # line con 0 exec-timeout 0 0 logging synchronous exit interface g0/0 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 10.0.10.1 255.255.255.0 *ipv6 address fe80::1:2 link-local* *ipv6 address 2001:db8:100:1010::1/64* *no shutdown* *exit* *interface s2/0* *ip address 10.0.13.1 255.255.255.0* *ipv6 address fe80::1:3 link-local* *ipv6 address 2001:db8:100:1013::1/64* *no shutdown* *exit*	*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*
Router R3 *hostname R3* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # R3, ENCOR Skills Assessment, Scenario 1 #* *line con 0* *exec-timeout 0 0* *logging synchronous* *exit* *interface g0/0* *ip address 10.0.11.1 255.255.255.0* *ipv6 address fe80::3:2 link-local* *ipv6 address 2001:db8:100:1011::1/64* *no shutdown* *exit* *interface s1/0* *ip address 10.0.13.3 255.255.255.0* *ipv6 address fe80::3:3 link-local* *ipv6 address 2001:db8:100:1010::2/64* *no shutdown* *exit*	*Switch A1* *hostname A1* *no ip domain lookup* *banner motd # A1, ENCOR Skills Assessment, Scenario 1 #* *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 10.0.100.3 255.255.255.0* *ipv6 address fe80::a1:1 link-local* *ipv6 address 2001:db8:100:100::3/64* *no shutdown* *exit*
Switch D1 *hostname D1* *ip routing* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # D1, ENCOR Skills Assessment, Scenario 1 #* *line con 0* *exec-timeout 0 0* *logging synchronous* *exit* *vlan 100*	*Switch D2* *hostname D2* *ip routing* *ipv6 unicast-routing* *no ip domain lookup* *banner motd # D2, ENCOR Skills Assessment, Scenario 1 #* *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 gi0/1* *no switchport* *ip address 10.0.10.2 255.255.255.0* *ipv6 address fe80::d1:1 link-local* *ipv6 address 2001:db8:100:1010::2/64* *no shutdown* *exit* *interface vlan 100* *ip address 10.0.100.1 255.255.255.0* *ipv6 address fe80::d1:2 link-local* *ipv6 address 2001:db8:100:100::1/64* *no shutdown* *exit* *interface vlan 101* *ip address 10.0.101.1 255.255.255.0* *ipv6 address fe80::d1:3 link-local* *ipv6 address 2001:db8:100:101::1/64* *no shutdown* *exit* *interface vlan 102* *ip address 10.0.102.1 255.255.255.0* *ipv6 address fe80::d1:4 link-local* *ipv6 address 2001:db8:100:102::1/64* *no shutdown* *exit* *ip dhcp excluded-address 10.0.101.1 10.0.101.109* *ip dhcp excluded-address 10.0.101.141 10.0.101.254* *ip dhcp excluded-address 10.0.102.1 10.0.102.109* *ip dhcp excluded-address 10.0.102.141 10.0.102.254* *ip dhcp pool VLAN-101* *network 10.0.101.0 255.255.255.0* *default-router 10.0.101.254* *exit* *ip dhcp pool VLAN-102* *network 10.0.102.0 255.255.255.0* *default-router 10.0.102.254* *exit*	*name Management* *exit* *vlan 101* *name UserGroupA* *exit* *vlan 102* *name UserGroupB* *exit* *vlan 999* *name NATIVE* *exit* *nterface gi0/1* *no switchport* *ip address 10.0.11.2 255.255.255.0* *ipv6 address fe80::d1:1 link-local* *ipv6 address 2001:db8:100:1011::2/64* *no shutdown* *exit* *interface vlan 100* *ip address 10.0.100.2 255.255.255.0* *ipv6 address fe80::d2:2 link-local* *ipv6 address 2001:db8:100:100::2/64* *no shutdown* *exit* *interface vlan 101* *ip address 10.0.101.2 255.255.255.0* *ipv6 address fe80::d2:3 link-local* *ipv6 address 2001:db8:100:101::2/64* *no shutdown* *exit* *interface vlan 102* *ip address 10.0.102.2 255.255.255.0* *ipv6 address fe80::d2:4 link-local* *ipv6 address 2001:db8:100:102::2/64* *no shutdown* *exit* *ip dhcp excluded-address 10.0.101.1 10.0.101.209* *ip dhcp excluded-address 10.0.101.241 10.0.101.254* *ip dhcp excluded-address 10.0.102.1 10.0.102.209* *ip dhcp excluded-address 10.0.102.241 10.0.102.254* *ip dhcp pool VLAN-101* *network 10.0.101.0 255.255.255.0* *default-router 10.0.101.254* *exit* *ip dhcp pool VLAN-102* *network 10.0.102.0 255.255.255.0* *default-router 10.0.102.254* *exit*

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

En este caso se uso el comando “wr” para guardar las configuraciones y establecerla como configuraciones iniciales.

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

Tabla 12. Código configuración inicial PCs

PC1 *Ip 10.0.100.5/24 gateway 10.0.100.254* *Ip 2001:db8:100:100::5/64* *save*	*PC4* *Ip 10.0.100.6/24 gateway 10.0.100.254* *Ip 2001:db8:100:100::6/64* *Save*

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

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

Tabla 13. Indicaciones parte 2

#	Tarea	Espesificaciones
2.1	*En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.*	*Habilite enlaces trunk 802.1Q entre:* *• D1 and D2* *• D1 and A1* *• D2 and A1*
2.2	*En todos los switches cambie la VLAN nativa en los enlaces troncales.*	*Use VLAN 999 como la VLAN nativa.*
2.3	*En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)*	*Use Rapid Spanning Tree (RSPT).*

#	Tarea	Espesificaciones
2.4	*En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología.* *D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).*	*Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.*
2.5	*En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.*	*Use los siguientes números de canales:* *• D1 a D2 – Port channel 12* *• D1 a A1 – Port channel 1* *• D2 a A1 – Port channel 2*
2.6	*En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.*	*Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología.* *Los puertos de host deben pasar inmediatamente al estado de reenvío (forwarding).*
2.7	*Verifique los servicios DHCP IPv4.*	*PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.*
2.8	*Verifique la conectividad de la LAN local.*	*PC1 debería hacer ping con éxito a:* *• D1: 10.0.100.1* *• D2: 10.0.100.2* *• PC4: 10.0.100.6* *PC2 debería hacer ping con éxito a:* *• D1: 10.0.102.1* *• D2: 10.0.102.2* *PC3 debería hacer ping con éxito a:* *• D1: 10.0.101.1* *• D2: 10.0.101.2* *PC4 debería hacer ping con éxito a:* *• D1: 10.0.100.1* *• D2: 10.0.100.2* *• PC1: 10.0.100.5*

11.1 Código Solución

Tabla 14. Código solución parte 2

Switch D1 *interface range gi1/0-3* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 12 mode active* *no shutdown* *exit* *interface range gi2/0-1* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 1 mode active* *no shutdown* *exit* *spanning-tree mode rapid-pvst* *spanning-tree vlan 100,102 root primary* *spanning-tree vlan 101 root secondary* *interface gi2/3* *switchport mode access* *switchport access vlan 100* *spanning-tree portfast* *no shutdown* *exit* *end*	*Switch D2* *interface range gi1/0-3* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 12 mode active* *no shutdown* *exit* *interface range gi2/0-1* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 2 mode active* *no shutdown* *exit* *!* *spanning-tree mode rapid-pvst* *spanning-tree vlan 101 root primary* *spanning-tree vlan 100,102 root secondary* *!* *interface gi2/3* *switchport mode access* *switchport access vlan 102* *spanning-tree portfast* *no shutdown* *exit* *end*
Switch A1 *interface range f1/1* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 1 mode active* *no shutdown* *exit* *interface range f1/2* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 1 mode active* *no shutdown* *exit* *interface range f1/3* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 2 mode active* *no shutdown* *exit* *interface range f1/4* *switchport mode trunk* *switchport trunk native vlan 999* *channel-group 2 mode active*	

no shutdown *exit* *interface f1/13* *switchport mode access* *switchport access vlan 101* *spanning-tree portfast* *no shutdown* *exit* *interface f1/14* *switchport mode access* *switchport access vlan 100* *spanning-tree portfast* *no shutdown* *exit* *end*	

12. Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.
Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4.
Las tareas de configuración son las siguientes:

Tabla 15. Indicaciones para la parte 3

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

#	Tarea	Detalle
	decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	*• R1: 0.0.6.1* *• R3: 0.0.6.3* *• D1: 0.0.6.131* *• D2: 0.0.6.132* *En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0.* *• En R1, no publique la red R1 – R2.* *• On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP.* *Deshabilite las publicaciones OSPFv3 en:* *• D1: todas las interfaces excepto G1/0/11* *• D2: todas las interfaces excepto G1/0/11*
3.3	*En R2 en la "Red ISP", configure MP-BGP.*	*Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:* *• Una ruta estática predeterminada IPv4.* *• Una ruta estática predeterminada IPv6.* *Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.* *Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.* *En IPv4 address family, anuncie:* *• La red Loopback 0 IPv4 (/32).* *• La ruta por defecto (0.0.0.0/0).* *En IPv6 address family, anuncie:* *• La red Loopback 0 IPv4 (/*
3.4	*En R1 en la "Red ISP", configure MP-BGP.*	*Configure dos rutas resumen estáticas a la interfaz Null 0:* *• Una ruta resumen IPv4 para 10.0.0.0/8.* *• Una ruta resumen IPv6 para 2001:db8:100::/48.* *Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.* *Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.* *En IPv4 address family:* *• Deshabilite la relación de vecino IPv6.* *• Habilite la relación de vecino IPv4.* *• Anuncie la red 10.0.0.0/8.* *En IPv6 address family:* *• Deshabilite la relación de vecino IPv4.* *• Habilite la relación de vecino IPv6.* *• Anuncie la red 2001:db8:100::/48.*

12.1 Código solución

Tabla 16. Código Solución Parte 3

Router R1 *router ospf 4* *router-id 0.0.4.1* *network 10.0.10.0 0.0.0.255 area 0* *network 10.0.13.0 0.0.0.255 area 0* *default-information originate* *exit* *ipv6 router ospf 6* *router-id 0.0.6.1* *default-information originate* *exit* *interface g0/0* *ipv6 ospf 6 area 0* *exit* *interface s2/0* *ipv6 ospf 6 area 0* *exit* *!ip route 10.0.0.0 255.0.0.0 null0* *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 10.0.0.0 mask 255.0.0.0* *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*	*Router R2* *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* *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*
Router R3 *router ospf 4* *router-id 0.0.4.3* *network 10.0.11.0 0.0.0.255 area 0* *network 10.0.13.0 0.0.0.255 area 0* *exit* *ipv6 router ospf 6* *router-id 0.0.6.3* *exit* *interface g0/0* *ipv6 ospf 6 area 0* *exit* *interface s1/0* *ipv6 ospf 6 area 0*	*Switch D1* *router ospf 4* *router-id 0.0.4.131* *network 10.0.100.0 0.0.0.255 area 0* *network 10.0.101.0 0.0.0.255 area 0* *network 10.0.102.0 0.0.0.255 area 0* *network 10.0.10.0 0.0.0.255 area 0* *passive-interface default* *no passive-interface gi0/1* *exit* *router ospf 6* *router-id 0.0.6.131* *passive-interface default* *no passive-interface gi0/1*

exit end	exit interface gi0/1 ip ospf 6 area 0 exit interface vlan 100 ip ospf 6 area 0 exit interface vlan 101 ip ospf 6 area 0 exit interface vlan 102 ip ospf 6 area 0 exit
Switch D2 router ospf 4 router-id 0.0.4.132 network 10.0.100.0 0.0.0.255 area 0 network 10.0.101.0 0.0.0.255 area 0 network 10.0.102.0 0.0.0.255 area 0 network 10.0.11.0 0.0.0.255 area 0 passive-interface default no passive-interface gi0/1 exit router ospf 6 router-id 0.0.6.132 passive-interface default no passive-interface gi0/1 exit interface gi0/1 ip ospf 6 area 0 exit interface vlan 100 ip ospf 6 area 0 exit interface vlan 101 ip ospf 6 area 0 exit interface vlan 102 ip ospf 6 area 0 exit	

13. Parte 4: Configurar la Redundancia del Primer Salto

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

Las tareas de configuración son las siguientes:

Tabla 17. Indicaciones para la parte 4

#	Tarea	Detalle
4.1	*En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.*	*Cree dos IP SLAs.* *• Use la SLA número 4 para IPv4.* *• Use la SLA número 6 para IPv6.* *Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.* *Programe la SLA para una implementación inmediata sin tiempo de finalización.* *Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6.* *• Use el número de rastreo 4 para la IP SLA 4.* *• Use el número de rastreo 6 para la IP SLA 6.* *Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.*
4.2	*En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.*	*Cree IP SLAs.* *• Use la SLA número 4 para IPv4.* *• Use la SLA número 6 para IPv6.* *Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.* *Programe la SLA para una implementación inmediata sin tiempo de finalización.* *Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6.* *• Use el número de rastreo 4 para la IP SLA 4.* *• Use el número de rastreo 6 para la SLA 6.* *Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos*
4.3	*En D1 configure HSRPv2.*	*D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150..* *Configure HSRP version 2.* *Configure IPv4 HSRP grupo 104 para la VLAN 100:* *• Asigne la dirección IP virtual 10.0.100.254.* *• Establezca la prioridad del grupo en 150.* *• Habilite la preferencia (preemption).* *• Rastree el objeto 4 y decremente en 60.* *Configure IPv4 HSRP grupo 114 para la VLAN 101:* *• Asigne la dirección IP virtual 10.0.101.254.* *• Habilite la preferencia (preemption).* *• Rastree el objeto 4 para disminuir en 60.* *Configure IPv4 HSRP grupo 124 para la VLAN 102:* *• Asigne la dirección IP virtual 10.0.102.254.* *• Establezca la prioridad del grupo en 150.* *• Habilite la preferencia (preemption).* *• Rastree el objeto 4 para disminuir en 60.* *Configure IPv6 HSRP grupo 106 para la VLAN 100:* *• Asigne la dirección IP virtual usando ipv6 autoconfig.*

#	Tarea	Detalle
		• Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo 126 para la VLAN 102: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60
	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. Configure IPv4 HSRP grupo 104 para la VLAN 100: • Asigne la dirección IP virtual 10.0.100.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo 114 para la VLAN 101: • Asigne la dirección IP virtual 10.0.101.254. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo 124 para la VLAN 102: • Asigne la dirección IP virtual 10.0.102.254. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo 106 para la VLAN 100: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 116 para la VLAN 101: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo 126 para la VLAN 102: • Asigne la dirección IP virtual usando ipv6 autoconfig. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60.

13.1 Código Solución

Tabla 18. Código Solución parte 4

Switch D1	Switch D2
ip sla 4 icmp-echo 10.0.10.1 frequency 5 exit ip sla 6 icmp-echo 2001:db8:100:1010::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 interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 priority 150 standby 104 preempt standby 104 track 4 decrement 60 standby 106 ipv6 autoconfig standby 106 priority 150 standby 106 preempt standby 106 track 6 decrement 60 exit interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 preempt standby 114 track 4 decrement 60 standby 116 ipv6 autoconfig standby 116 preempt standby 116 track 6 decrement 60 exit interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 priority 150 standby 124 preempt standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 priority 150 standby 126 preempt standby 126 track 6 decrement 60 exit	ip sla 4 icmp-echo 10.0.11.1 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 interface vlan 100 standby version 2 standby 104 ip 10.0.100.254 standby 104 preempt standby 104 track 4 decrement 60 standby 106 ipv6 autoconfig standby 106 preempt standby 106 track 6 decrement 60 exit interface vlan 101 standby version 2 standby 114 ip 10.0.101.254 standby 114 priority 150 standby 114 preempt standby 114 track 4 decrement 60 standby 116 ipv6 autoconfig standby 116 priority 150 standby 116 preempt standby 116 track 6 decrement 60 exit interface vlan 102 standby version 2 standby 124 ip 10.0.102.254 standby 124 preempt standby 124 track 4 decrement 60 standby 126 ipv6 autoconfig standby 126 preempt standby 126 track 6 decrement 60 exit

14. Parte 5: Seguridad

En esta parte debe configurar varios mecanismos de seguridad en los dispositivos de la topología. Las tareas de configuración son las siguientes:

Tabla 16. Instrucciones parte 5

#	Tarea	Detalle
5.1	*En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.*	*Contraseña: cisco12345cisco*
5.2	*En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.*	*Detalles de la cuenta encriptada SCRYPT:* *• Nombre de usuario Local: sadmin* *• Nivel de privilegio 15* *• Contraseña: cisco12345cisco*
5.3	*En todos los dispositivos (excepto R2), habilite AAA.*	*Habilite AAA.*
5.4	*En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.*	*Especificaciones del servidor RADIUS.:* *• Dirección IP del servidor RADIUS es 10.0.100.6.* *• Puertos UDP del servidor RADIUS son 1812 y 1813.* *• Contraseña: $trongPass*
5.5	*En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA*	*Especificaciones de autenticación AAA:* *• Use la lista de métodos por defecto* *• Valide contra el grupo de servidores RADIUS* *• De lo contrario, utilice la base de datos local.*
5.6	*Verifique el servicio AAA en todos los dispositivos (except R2).*	*Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.*

14.1 Código solución

Tabla 19. Código solución parte 5

R1	*R3*
enable secret cisco12345cisco *username sadmin privilege 15 secret cisco12345cisco* *aaa new-model* *radius-server HOST 10.0.100.6 auth-port 1812 acct-port 1813 key* *key config-key password-encrypt* *$trongPass* *aaa authentication login default group radius local*	*enable secret cisco12345cisco* *username sadmin privilege 15 secret cisco12345cisco* *aaa new-model* *radius-server HOST 10.0.100.6 auth-port 1812 acct-port 1813* *key config-key password-encrypt* *$trongPass* *aaa authentication login default group radius local*

15. Parte 6: Configure las funciones de Administración de Red

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

Tabla 20. Instrucciones parte 6

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

15.1 Código solución

Tabla 21. Código solución parte 6

R1 *clock timezone word 23* *ntp server 2.2.2.2* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit* *snmp-server contact Cisco Student* *snmp-server community ENCORSA ro SNMP-NMS* *snmp-server host 10.0.100.5 version 2c ENCORSA* *snmp-server ifindex persist* *snmp-server enable traps bgp* *snmp-server enable traps ospf* *end*	*R2* *ntp master 3* *end*
D1 *ntp server 10.0.10.1* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit* *snmp-server contact Cisco Student* *snmp-server community ENCORSA ro SNMP-NMS*	*D2* *ntp server 10.0.10.1* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit* *snmp-server contact Cisco Student* *snmp-server community ENCORSA ro SNMP-NMS*

snmp-server host 10.0.100.5 version 2c ENCORSA *snmp-server ifindex persist* *snmp-server enable traps ospf* *end*	*snmp-server host 10.0.100.5 version 2c ENCORSA* *snmp-server enable traps ospf* *end*
A1 *ntp server 10.0.10.1* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit* *snmp-server contact Cisco Student* *snmp-server community ENCORSA ro SNMP-NMS* *snmp-server host 10.0.100.5 version 2c ENCORSA* *snmp-server ifindex persist* *snmp-server enable traps ospf* *end*	*R3* *ntp server 10.0.10.1* *logging trap warning* *logging host 10.0.100.5* *logging on* *ip access-list standard SNMP-NMS* *permit host 10.0.100.5* *exit* *snmp-server contact Cisco Student* *snmp-server community ENCORSA ro SNMP-NMS* *snmp-server host 10.0.100.5 version 2c ENCORSA* *snmp-server ifindex persist* *snmp-server enable traps ospf* *end*

CONCLUSIONES

La conexión de los dispositivos como se muestra en el diagrama según lo necesario evidencia ya por parte del programador algo de experiencia debido a que algunos de los dispositivos requieren el acondicionamiento para realizarlo de manera correcta desde modificaciones en la parte física, así lo fue en el caso de los 2 Switches en donde su configuración exige la conexión a una fuente de potencia y también los routers en la anexión de una interface para la comunicación serial entre ellos, esto es en alguna medida complicado porque en algunas versiones de Cisco Packet Tracer los dispositivo incluidos en la simulación ya gozan de todas las extensiones que ofrecen y solo es pasar a la conexión y configuración por la interface respetiva. La segunda actividad fue bastante simple en el sentido que se nos ofrece los comandos para realizar los direccionamientos básicos, los comandos utilizados no son desconocidos del todo luego esta parte fue relativamente sencilla.

En la parte 2 se destaca la utilización de los enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN aclarando que Cisco admite IEEE 802.1Q para la coordinación de enlaces troncales en interfaces Fast Ethernet y Gigabit Ethernet. La aplicación del protocolo Rapid Spanning Tree Protocol que gestiona enlaces redundantes.

En la parte 3 el código implementado es bastante genérico según los ejemplos consultados solo es necesario tener cuidado con las IP de la redes, las área y los ip de los demás routers, teniendo en cuenta que los ejemplo consultados eran configuraciones similares al menos en las condiciones topológicas y las conexiones lógicas.

En la parte 4 el código implementado se implementó el comando “ip sla” esta herramienta de cisco no permite analizar en diferente capas los servicios de aplicaciones ip monitorea constantemente el tráfico de en la red en su análisis de performance de red. Respecto al uso de la interface Vlans son claras las ventajas al crear redes de lógicas independientes de las redes física permite la segmentación y mejor gestión de la redes entre sus ventajas tenemos, aumento de la seguridad, partición en subredes flexibilidad al agilizar la comunicación entre dispositivos conectados a la red, optimización de recurso de la red ya con estos aporte se evidencia la necesidad de usar la Vlans en la configuración de una red en la mayor medida de lo posible.

En la parte 5 de código se destaca el uso de la encripción SCRYPT según lo consultado la contraseña implementada es de tipo 9 además podemos concluir que toda configuración de red supone realizar una protección por medio de usuario y contraseña para evitar la manipulación y des configuración por algún usuario

malintencionado o descuido además es indispensable que se use cuando la red lo permite y la implementación de protocolo AAA (RADIUS) trae como beneficios como capacidad de identificar inicio y finalización de sesiones, para el control de y gestión de esta, esto característica es de gran utilidad si partimos del hecho que la red propuesta es una red de carácter empresarial, lo cual permite un mejor control y datos para futuros ajustes o mecanismos de optimación y planeación laboral.

Sobre a la parte 6 del este trabajo la asignación de NTP es clara para conservar los registro no sean contradictorio y permitir una sincronizad cuando se le necesite pero en caso que se presente alguna novedad es necesario la implementación de un protocolo que permita que esta sea notificada la configuración de red propone el uso de “Syslog” que permite que los dispositivos de red envíen los mensajes del sistema a servidores de syslog a través de la red, como se evidencia la aplicación de este protocolo permite normar la interacciones y notificaciones de eventos en la red facilitando su inspección de ser necesaria, respecto al uso del El Protocolo simple de administración de red o SNMPv2 es utilizado para administrar y monitorear dispositivos de red y sus funciones.

Como se pudo mostrar en el desarrollo de escenario es indispensable la asignación de diferentes protocolos para cada posible caso de acción, contingencia o emergencia en donde estos deben poder realizar configuración de la red adecuada para su uso no obstante todos estos protocolos se ven como una conjunción que permite ser la inspección control y supervisión de la red, además parece que se presentan y aplican protocolos para cada posible condición de la red (normal y anormal) que pueda presentarse y todo esto se considera como una configuración estándar o básica, lo cual muestra que la configuración de una red es básicamente la asignación de roles de dispositivos dentro de protocolos de la misma para las condiciones posible en la red.

Respecto al uso de los dos softwares destaquemos sus virtudes, en el caso de cisco Packet Tracer se destacó lo siguiente: su fácil instalación e interface gráfica para la creaciones de topologías de red y la adición de diferentes dispositivos con nombres específicos además con diferentes prestaciones para la fácil adaptación de los equipos por medio de la adición de módulos según la necesidad, también se destaca los pocos requerimientos que pide al sistema y los pocos recurso de software que usa mientras se simula, respecto a los defectos para el desarrollo de este escenario es que algunos comandos y protocolos no los ejecuta impidiendo satisfacer la necesidad que pide la configuración solicitada de la red y la falta de otros da una asignación parcial de algunos protocolos desconociendo como estos afecte a una red real. En el caso de GNS3 su instalación y uso es mucho más complicado, en este caso fue necesario la instalación de otros programas de soporte Máquina virtual, paquetes adicionales de ejecución, archivos para ejecutar elementos equivalente a los dispositivos Cisco entre otros, que además exigen gran

cantidad de recursos computaciones como memoria RAM , otra cualidad es la no existencia de los dispositivos Cisco de diferentes referencias, existen uno pocos Router que según su configuración se adaptan al nivel de su homologo cisco, además de módulos parecidos y limitados puertos. Sobre los códigos las configuraciones o comandos relacionados con “ipv6 “según CLI de cisco no es necesario el programa identifica el protocolo y los ajusta solo por el comando IP, sobre la implemntacion de Swichtes se usa un único tipo que esta habilitados en todos los niveles pero es escaso el número de puerto. El programa es tedioso de manejar y lento en algún caso además las configuraciones no la guarda si no se agrega otro comando y guardar el proyecto es difícil y confuso, pero a diferencia de cisco packet tracer si recibe la inmensa mayoría de condigo implementados en este ejercicio.

BIBLIOGRAFÍA

Cisco. (2012). *Lo que usted necesita saber sobre routers y switches.* Lo que usted necesita saber sobre routers y switches. https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

Cisco. (2021a). *¿Qué es un enrutador?* ¿Cómo funciona un enrutador? https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html

Cisco. (2021b). *Protocolo de configuración dinámica de host v6*. Introducción a SLAAC. https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/10.2.1.1/10.2.1.1.html

Digital Guide IONOS. (2020). *Qué es el DHCP*. El DHCP y la configuración de redes. https://www.ionos.es/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona/

ORACLE. (2021). *Protocolos de enrutamiento*. Configuración del sistema Oracle® Solaris 11.2 como enrutador o equilibrador de carga. https://docs.oracle.com/cd/E56339_01/html/E53805/ipref-13.html