DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DANIELA OCHOA JARAMILLO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DANIELA OCHOA JARAMILLO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Medellín, 29 de noviembre de 2021

AGRADECIMIENTOS

El presente trabajo lo dedico primeramente a Dios, quien fue el que me brindo sabiduría y fuerza para lograr culminar este pregrado y alcanzar este nivel académico.

A mis padres y hermano, quienes me brindaron apoyo y confianza en los momentos más duros y en cuales sentí no poder seguir adelante con mis estudios por situaciones laborales y personales.

Finalmente, a mi Universidad y tutores, quienes a través de su conocimiento lograron transmitirme información que permite que en poco tiempo cumpla el sueño de ser Ingeniera de Telecomunicaciones.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ASN: Número de sistema autónomo.

BGP: Protocolo de puerta de enlace fronteriza. Protocolo de enrutamiento entre dominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP. Está definido por RFC 1163.

CIDR: Itinerario entre recesos. Técnica soportada por BGP4 y basada en agregación de rutas. CIDR permite a los enrutadores agrupar rutas para reducir la cantidad de información de enrutamiento transportada por los enrutadores centrales. Con CIDR, varias redes IP aparecen a las redes fuera del grupo como una entidad única y más grande. Con CIDR, las direcciones IP y sus máscaras de subred se escriben como cuatro octetos, separados por puntos, seguidos de una barra diagonal y un número de dos dígitos que representa la máscara de subred.

HSRP: Protocolo de enrutador Hot Standby. Proporciona una alta disponibilidad de red y cambios transparentes en la topología de la red. HSRP crea un grupo de enrutadores de reserva activa con un enrutador principal que atiende todos los paquetes enviados a la dirección de reserva activa. El enrutador principal es monitoreado por otros enrutadores del grupo. Si falla, uno de los enrutadores en espera hereda tanto la posición principal como la dirección de espera activa.

OSPF: Primero, abra el camino más corto. Algoritmo de enrutamiento IGP jerárquico de estado de enlace propuesto como sucesor de RIP en la comunidad de Internet. Las características de OSPF incluyen enrutamiento de menor costo, enrutamiento de múltiples rutas y equilibrio de carga. OSPF se derivó de una versión anterior del protocolo IS-IS.

PVST +: Por VLAN Spanning Tree Plus. Soporte para troncos dot1q para mapear múltiples árboles de expansión a un solo árbol de expansión.

VLAN: LAN virtual. Grupo de dispositivos en una o más LAN que están configurados (usando software de administración) para que puedan comunicarse como si estuvieran conectados al mismo cable, cuando en realidad están ubicados en varios segmentos de LAN diferentes. Debido a que las VLAN se basan en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

STP: Par trenzado blindado. Medio de cableado de dos pares utilizado en una variedad de implementaciones de red. El cableado STP tiene una capa de aislamiento blindado para reducir la EMI.

RESUMEN

En esta prueba de habilidades, se realiza la configuración completa de la red permitiendo que haya una accesibilidad completa de un extremo a otro, para que los hosts tengan un soporte confiable de la puerta de enlace preterminada y para que los protocolos OSPF y BGP configurados estén operativos dentro de la parte correspondiente a la “Red de la Compañía” en la topología. Estos cambios en las configuraciones son verificados de acuerdo a las especificaciones dadas, cumpliendo cada uno de los detalles y asegurando que los dispositivos funcionen como es requerido.

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

ABSTRACT

In this skills test, the complete network configuration is performed allowing for complete end-to-end accessibility, for hosts to have reliable support of the default gateway, and for configured OSPF and BGP protocols to be operating within the part corresponding to the "Company Network" in the topology. These changes in the configurations are verified according to the given specifications, fulfilling each one of the details and ensuring that the devices work as required.

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

INTRODUCCIÓN

De acuerdo a los desarrollos que deben presentarse al momento de realizar una topología de red, se implementa primeramente la configuración de los dispositivos que conforman esta topología que van desde el cambio en el nombre de host, la desactivación de la búsqueda de dominio, la habilitación del direccionamiento ipv6 unicast y la aplicación de mensaje de bienvenida y verificaciones en la línea de consola. Seguido a esto, se realiza la configucación de las interfaces que conforman el direccionamiento, así como la vinculación de interfaces Loopback, aplicación de DHCP y demás configuraciones que dejan lista la topología para realizar las respectivas verificaciones y aseguran la interconexión entre las redes de la compañía.

Luego, se realiza la configucación de la capa 2 de la red y el soporte de Host, habilitando los enlaces trunk 802.1Q entre los swiches de capa 3 y el switch de capa 2. Enlazando la troncal a la vlan nativa 999, habilitando el protocolo Rapid Spanning-Tree (RSTP), se configuran los puentes raíz RSTP root bridges según la información suministrada del diagrama de topología, complementado por la adición de un respaldo en caso de el puente raiz falle.

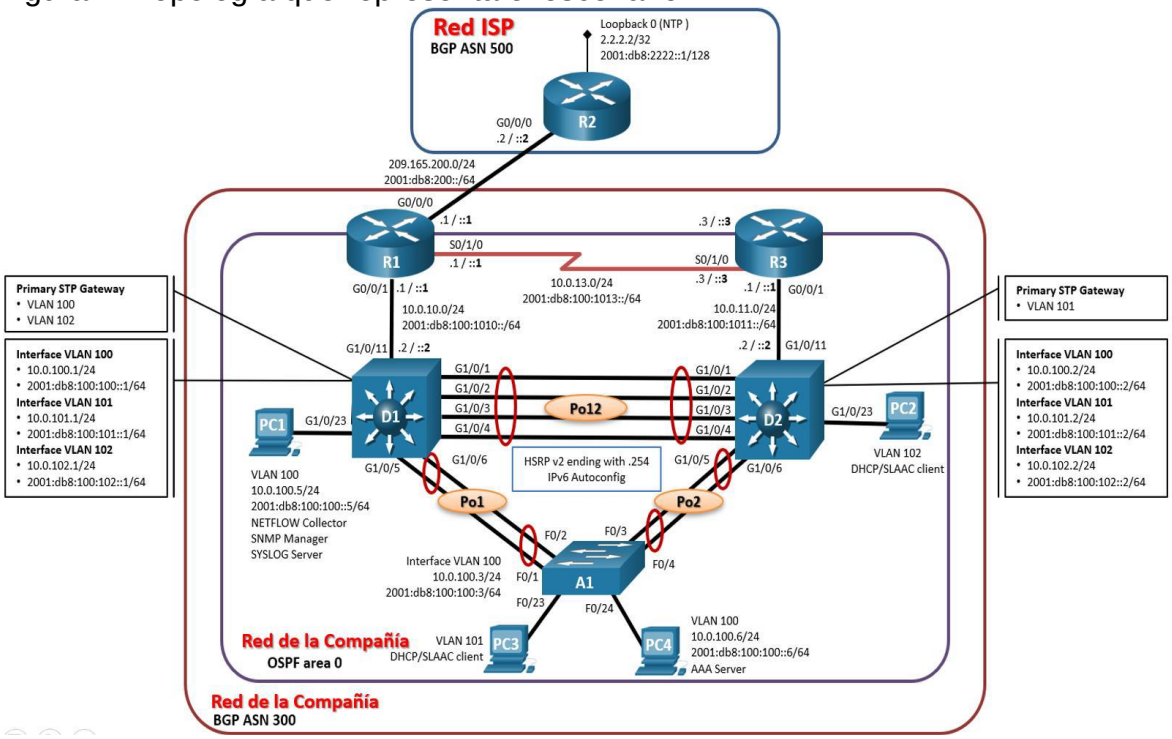
Finalmente se realiza la configuración de los protocolos de enrutamiento en los dispositivos para que la red esté completamente convergente. Para ello se realiza la configuración OSPF tanto para el direccionamiento IPv4 como para el IPv6, se configura MP-BGP en el router R2 y R1.

DESARROLLO

1. Escenario 1

Teniendo en la cuenta la siguiente imagen:

Figura 1. Topología que representa el escenario 1.



Fuente: guía de actividades

1.1. Tabla de direccionamiento

Tabla 1. Tabla de direccionamiento para la topología.

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

	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Fuente: Autora.

1.2. 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 (**no se entrega aún)

Part 5: Configurar la seguridad (**no se entrega aún)
Part 6: Configurar las características de administración de red (** no se entrega aún)

1.3. 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.

1.4. 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

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

1.5.1. 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.

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

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:

Router R1

hostname R1	Se asigna el nombre de host
ipv6 unicast-routing	Se habilita el enrutamiento para ipv6
no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración de la consola
exec-timeout 0 0	Se habilita la desconeción de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
interface g0/0	Se accede a la interface gigabitEthernet
ip address 209.165.200.225 255.255.255.224	Se configura la dirección ip
ipv6 address fe80::1:1 link-local	Se configura la dirección link local
ipv6 address 2001:db8:200::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz gigabitEthernet
exit	

interface g2/0	Se accede a la interface
ip address 10.0.10.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::1:2 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:1010::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface s1/0	Se accede a la interface serial
ip address 10.0.13.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::1:3 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:1013::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	

Router R2

hostname R2	Se asigna el nombre de host
ipv6 unicast-routing	Se habilita el enrutamiento para ipv6
no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración de la consola
exec-timeout 0 0	Se habilita la desconeción de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
interface g0/0	Se accede a la interface gigabitEthernet
ip address 209.165.200.226 255.255.255.224	Se configura la dirección ip
ipv6 address fe80::2:1 link-local	Se configura la dirección link local
ipv6 address 2001:db8:200::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface Loopback 0	Se accede a la interface Loopback
ip address 2.2.2.2 255.255.255.255	Se configura la dirección ip
ipv6 address fe80::2:3 link-local	Se configura la dirección link local

ipv6 address 2001:db8:2222::1/128	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	

Router R3

hostname R3	Se asigna el nombre de host
ipv6 unicast-routing	Se habilita el enrutamiento para ipv6
no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración de la consola
exec-timeout 0 0	Se habilita la desconeción de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
interface g1/0	Se accede a la interface gigabitEthernet
ip address 10.0.11.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::3:2 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:1011::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface s1/0	Se accede a la interface serial
ip address 10.0.13.3 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::3:3 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:1010::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	

Switch D1

hostname D1	Se asigna el nombre de host
ip routing	Se habilita el enrutamiento ipv4

ipv6 unicast-routing	Se habilita el enrutamiento para ipv6
no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración de la consola
exec-timeout 0 0	Se habilita la desconeción de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
vlan 100	Se configura la vlan
name Management	Se configura el nombre de la vlan
exit	
vlan 101	Se configura la vlan
name UserGroupA	Se configura el nombre de la vlan
exit	
vlan 102	Se configura la vlan
name UserGroupB	Se configura el nombre de la vlan
exit	
vlan 999	Se configura la vlan
name NATIVE	Se configura el nombre de la vlan
exit	
interface e2/0	Se accede a la interface Ethernet
no switchport	
ip address 10.0.10.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:1 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:1010::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 100	Se accede a la interface Vlan
ip address 10.0.100.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:2 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:100::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 101	Se accede a la interface Vlan

ip address 10.0.101.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:3 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:101::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 102	Se accede a la interface Vlan
ip address 10.0.102.1 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:4 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:102::1/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.109	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.101.141 10.0.101.254	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.102.1 10.0.102.109	Se excluyen direcciones de la VLAN-102
ip dhcp excluded-address 10.0.102.141 10.0.102.254	Se excluyen direcciones de la VLAN-102
ip dhcp pool VLAN-101	Se crea un pool de direcciones ip
network 10.0.101.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.101.254	Se define la puerta de enlace
exit	
ip dhcp pool VLAN-102	Se crea un pool de direcciones ip
network 10.0.102.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.102.254	Se define la puerta de enlace
exit	
interface range e0/0-3, e1/0-3, e2/1	Se selecciona el rango de interfaces que no se utilizarán
shutdown	Se apagan las interfaces
exit	

Switch D2

hostname D2	Se asigna el nombre de host
ip routing	Se habilita el enrutamiento ipv4
ipv6 unicast-routing	Se habilita el enrutamiento para ipv6

no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración de la consola
exec-timeout 0 0	Se habilita la desconeción de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
vlan 100	Se configura la vlan
name Management	Se configura el nombre de la vlan
exit	
vlan 101	Se configura la vlan
name UserGroupA	Se configura el nombre de la vlan
exit	
vlan 102	Se configura la vlan
name UserGroupB	Se configura el nombre de la vlan
exit	
vlan 999	Se configura la vlan
name NATIVE	Se configura el nombre de la vlan
exit	
interface e2/0	Se accede a la interface Ethernet
no switchport	Se configura como un puerto de capa 3
ip address 10.0.11.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d1:1 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:1011::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 100	Se accede a la interface Vlan
ip address 10.0.100.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d2:2 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:100::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 101	Se accede a la interface Vlan
ip address 10.0.101.2 255.255.255.0	Se configura la dirección ip

ipv6 address fe80::d2:3 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:101::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface vlan 102	Se accede a la interface Vlan
ip address 10.0.102.2 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::d2:4 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:102::2/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
ip dhcp excluded-address 10.0.101.1 10.0.101.209	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.101.241 10.0.101.254	Se excluyen direcciones de la VLAN-101
ip dhcp excluded-address 10.0.102.1 10.0.102.209	Se excluyen direcciones de la VLAN-102
ip dhcp excluded-address 10.0.102.241 10.0.102.254	Se excluyen direcciones de la VLAN-102
ip dhcp pool VLAN-101	Se crea un pool de direcciones ip
network 10.0.101.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.101.254	Se define la puerta de enlace
exit	
ip dhcp pool VLAN-102	Se crea un pool de direcciones ip
network 10.0.102.0 255.255.255.0	Se asigna el rango de hosts
default-router 10.0.102.254	Se define la puerta de enlace
exit	
interface range e0/0-3, e1/0-3, e2/1	Se selecciona el rango de interfaces que no se utilizarán
shutdown	Se apagan las interfaces
exit	

<u>Switch A1</u>

hostname A1	Se asigna el nombre de host
no ip domain lookup	Se desactiva la búsqueda de ip de dominio
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #	Se asigna un mensaje
line con 0	Se accede a la configuración de la consola

exec-timeout 0 0	Se habilita la desconeción de la consola
logging synchronous	Se habilita el logueo sincronico
exit	
vlan 100	Se configura la vlan
name Management	Se configura el nombre de la vlan
exit	
vlan 101	Se configura la vlan
name UserGroupA	Se configura el nombre de la vlan
exit	
vlan 102	Se configura la vlan
name UserGroupB	Se configura el nombre de la vlan
exit	
vlan 999	Se configura la vlan
name NATIVE	Se configura el nombre de la vlan
exit	
interface vlan 100	Se accede a la interface Ethernet
ip address 10.0.100.3 255.255.255.0	Se configura la dirección ip
ipv6 address fe80::a1:1 link-local	Se configura la dirección link local
ipv6 address 2001:db8:100:100::3/64	Se configura la dirección ipv6
no shutdown	Se enciende la interfaz
exit	
interface range e1/2-3, e2/0, e2/1, e2/2, e2/3	Se selecciona el rango de interfaces que no se utilizarán
shutdown	Se apagan las interfaces
exit	

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

Router R1

R1#copy ru st	Copia el archivo running config
R1#	

Router R2

R2#copy ru st config R2#	Copia el archivo running

Router R3

R3#copy ru st config R3#	Copia el archivo running

Switch D1

D1#copy ru st config D1#	Copia el archivo running

Switch D2

D2#copy ru st config D2#	Copia el archivo running

Switch A1

A1#copy ru st config A1#	Copia el archivo running

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.

Host PC1

PC1> ip 10.0.100.5 255.255.255.0 10.0.100.254	Se configura el direccionamiento en el VPC

PC1 : 10.0.100.5 255.255.255.0 gateway 10.0.100.254

PC1> ip 2001:db8:100:100::5/64 Se configura el direccionamiento IPV6 en el VPC
PC1 : 2001:db8:100:100::5/64

PC1>

Host PC4

PC4> ip 10.0.100.6 255.255.255.0 10.0.100.254 Se configura el direccionamiento en el VPC
PC4 : 10.0.100.6 255.255.255.0 gateway 10.0.100.254
PC4> ip 2001:db8:100:100::6/64 Se configura el direccionamiento IPV6 en el VPC
PC1 : 2001:db8:100:100::6/64

PC4>

1.6. 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 2. Tabla de asingación de tareas 2.1.

Tarea#	**Tarea**	**Especificación**
2.1	En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.	Habilite enlaces trunk 802.1Q entre: • D1 and D2 • D1 and A1 • D2 and A1

Fuente: Autora.

Switch D1

D1#configure terminal
D1(config)# interface range e0/0-3, e1/0-1 Se seleccionan las interfaces troncales

D1(config-if-range)#switchport trunk encapsulation dot1q Se habilita la encapsulación dot1q en el puerto
D1(config-if-range)#switchport mode trunk Se habilita el puerto en modo troncal
D1(config-if-range)#no shutdown Se enciende la interfaz
D1(config-if-range)#

Switch D2

D2#configure terminal
D2(config)#interface range e0/0-3, e1/0-1 Se seleccionan las interfaces troncales
D2(config-if-range)#switchport trunk encapsulation dot1q Se habilita la encapsulación dot1q en el puerto
D2(config-if-range)#switchport mode trunk Se habilita el puerto en modo troncal
D2(config-if-range)#no shutdown Se enciende la interfaz
D2(config-if-range)#exit
D2(config)#

Switch A1

A1#configure terminal
A1(config)#interface range e0/0-3 Se seleccionan las interfaces troncales
A1(config-if-range)#switchport trunk encapsulation dot1q Se habilita la encapsulación dot1q en el puerto
A1(config-if-range)#switchport mode trunk Se habilita el puerto en modo troncal
A1(config-if-range)#no shutdown Se enciende la interfaz
A1(config-if-range)#exit
A1(config)#

Tabla 3. Tabla de asingación de tareas 2.2.

2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.

Fuente: Autora.

Switch D1

D1(config-if-range)#switchport trunk native vlan 999	Se configura la vlan nativa en el puerto troncal

Switch D2

D2(config-if-range)#switchport trunk native vlan 999	Se configura la vlan nativa en el puerto troncal

Switch A1

A1(config-if-range)#switchport trunk native vlan 999	Se configura la vlan nativa en el puerto troncal

Tabla 4. Tabla de asingación de tareas 2.3.

2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).

Fuente: Autora.

Switch D1

D1(config)#spanning-tree mode rapid-pvst	Se habilita Rapid Spanning Tree en el switch

Switch D2

D2(config)#spanning-tree mode rapid-pvst	Se habilita Rapid Spanning Tree en el switch

Switch A1

A1(config)#spanning-tree mode rapid-pvst	Se habilita Rapid Spanning Tree en el switch

Tabla 5. Tabla de asingación de tareas 2.4.

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.

Fuente: Autora.

Switch D1

D1(config)#spanning-tree vlan 100,102 root primary — Se configura el puente raíz RSTP
D1(config)#spanning-tree vlan 101 root secondary — Se configura el puente de respaldo

Switch D2

D2(config)#spanning-tree vlan 101 root primary — Se configura el puente raíz RSTP
D2(config)#spanning-tree vlan 100,102 root secondary — Se configura el puente de respaldo

Tabla 6. Tabla de asingación de tareas 2.5.

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

Fuente: Autora.

Switch D1

D1(config)#interface range e0/0-3 — Se seleccionan las interfaces
D1(config-if-range)#channel-group 12 mode active — Se configura el canal del grupo y en modo activo

D1(config-if-range)#exit
D1(config)#interface range e1/0-1 Se seleccionan las interfaces
D1(config-if-range)#channel-group 1 mode active Se configura el canal del grupo y en modo activo
D1(config-if-range)#exit

Switch D2

D2(config)#interface range e0/0-3 Se seleccionan las interfaces
D2(config-if-range)#channel-group 12 mode active Se configura el canal del grupo y en modo activo
D2(config-if-range)#exit
D2(config)#interface range e1/0-1 Se seleccionan las interfaces
D2(config-if-range)#channel-group 2 mode active Se configura el canal del grupo y en modo activo
D2(config-if-range)#exit

Switch A1

A1(config)#interface range e0/0-1 Se seleccionan las interfaces
A1(config-if-range)#channel-group 1 mode active Se configura el canal del grupo y en modo activo
A1(config-if-range)#exit
A1(config)#interface range e0/2-3 Se seleccionan las interfaces
A1(config-if-range)#channel-group 2 mode active Se configura el canal del grupo y en modo activo
A1(config-if-range)#exit

Tabla 7. Tabla de asingación de tareas 2.6.

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).

Fuente: Autora.

Switch D1

D1(config)#interface e2/1	Se selecciona la interfaz
D1(config-if)#switchport mode Access acceso	Se configura en modo de
D1(config-if)#switchport access vlan 100	Se asigna la vlan al puerto
D1(config-if)#spanning-tree portfast	Se habilita portfast
D1(config-if)#no shutdown	Se enciende la interfaz
D1(config-if)#exit	

Switch D2

D2(config)#interface e2/1	Se selecciona la interfaz
D2(config-if)#switchport mode Access acceso	Se configura en modo de
D2(config-if)#switchport access vlan 102	Se asigna la vlan al puerto
D2(config-if)#spanning-tree portfast	Se habilita portfast
D2(config-if)#no shutdown	Se enciende la interfaz
D2(config-if)#exit	

Switch A1

A1(config)#interface e1/0	Se selecciona la interfaz
A1(config-if)#switchport mode Access acceso	Se configura en modo de
A1(config-if)#switchport access vlan 101	Se asigna la vlan al puerto
A1(config-if)#spanning-tree portfast	Se habilita portfast
A1(config-if)#no shutdown	Se enciende la interfaz
A1(config-if)#exit	
A1(config)#interface e1/1	Se selecciona la interfaz
A1(config-if)#switchport mode Access acceso	Se configura en modo de
A1(config-if)#switchport access vlan 100	Se asigna la vlan al puerto
A1(config-if)#spanning-tree portfast	Se habilita portfast
A1(config-if)#no shutdown	Se enciende la interfaz
A1(config-if)#exit	

Tabla 8. Tabla de asingación de tareas 2.7.

2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

Fuente: Autora.

Host PC2

PC2> dhcp — Se configura ipv4 por DHCP
DDORA IP 10.0.102.210/24 GW 10.0.102.254
PC2>

Figura 2. Verificación de los servicios DHCP IPv4 en PC2.

Fuente: Autora.

Host PC3

PC3> dhcp
DDORA IP 10.0.101.210/24 GW 10.0.101.254 — Se configura ipv4 por DHCP
PC3>

Figura 3. Verificación de los servicios DHCP IPv4 en PC3.

Fuente: Autora.

Tabla 9. Tabla de asingación de tareas 2.8.

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

Fuente: Autora.

Prueba ping PC1

Figura 4. Prueba de ping desde PC3 a D1, D2 y PC4.

Fuente: Autora.

Prueba ping PC2

Figura 5. Prueba de ping desde PC2 a D1 y D2.

Fuente: Autora.

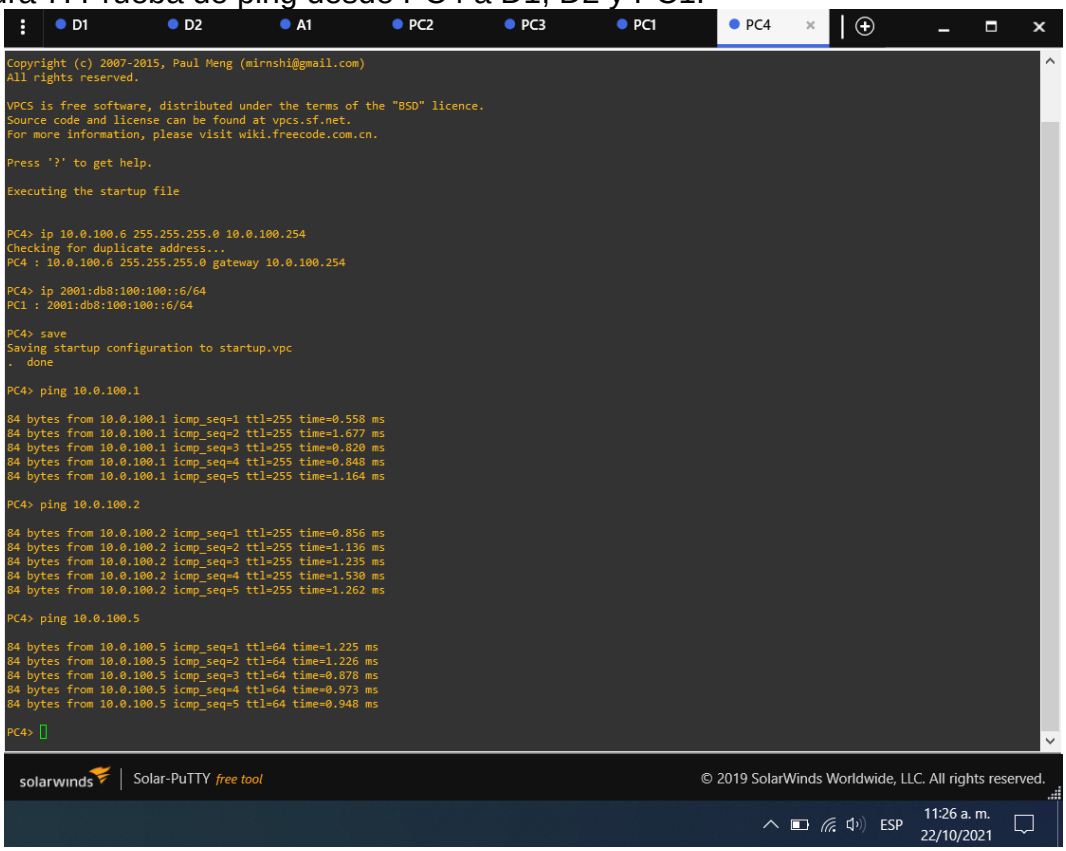
Prueba ping PC3

Figura 6. Prueba de ping desde PC3 a D1 y D2.

Fuente: Autora.

Prueba ping PC4

Figura 7. Prueba de ping desde PC4 a D1, D2 y PC1.



Fuente: Autora.

1.7. 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 10. Tabla de asingación de tareas 3.1.

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

Fuente: Autora.

Router R1

R1#configure terminal
R1(config)#router ospf 4 — Se habilita OSPF con su indicador
R1(config-router)#router-id 0.0.4.1 — Se configura el identificador

R1(config-router)#network 10.0.10.0 0.0.0.255 area 0 Se configura las redes y su área
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0 Se configura las redes y su área
R1(config-router)#default-information originate Se genera una ruta predetermina
R1(config-router)#exit
R1(config)#

Router R3

R3#configure terminal
R3(config)#router ospf 4 Se habilita OSPF con su indicador
R3(config-router)#router-id 0.0.4.3 Se configura el identificador
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0 Se configura las redes y su área
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0 Se configura las redes y su área
R3(config-router)#exit
R3(config)#

Switch D1

D1#configure terminal
D1(config)#router ospf 4 Se habilita OSPF con su indicador
D1(config-router)#router-id 0.0.4.131 Se configura el identificador
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0 Se configura las redes y su área
D1(config-router)#passive-interface default Se configuran las interfaces como pasivas
D1(config-router)#no passive-interface e2/0 Se excluye la interfaz de estar pasiva
D1(config-router)#exit

Switch D2

D2#configure terminal
D2(config)#router ospf 4 Se habilita OSPF con su indicador
D2(config-router)#router-id 0.0.4.132 Se configura el identificador
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0 Se configura las redes y su área
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0 Se configura las redes y su área
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0 Se configura las redes y su área
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0 Se configura las redes y su área
D2(config-router)#passive-interface default Se configuran las interfaces como pasivas
D2(config-router)#no passive-interface e2/0 Se excluye la interfaz de estar pasiva
D2(config-router)#exit

Tabla 11. Tabla de asingación de tareas 3.2.

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

Fuente: Autora

Router R1

R1(config)#ipv6 router ospf 6	Se habilita OSPF con su indicador
R1(config-rtr)#router-id 0.0.6.1	Se configura el identificador
R1(config-rtr)#default-information originate	Se genera una ruta predetermina
R1(config-rtr)#exit	
R1(config)#interface gi2/0	Se accede a la interfaz
R1(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 en la interfaz y se configura el área
R1(config-if)#exit	
R1(config)#interface se1/0	Se accede a la interfaz
R1(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 en la interfaz y se configura el área
R1(config-if)#exit	

Router R3

R3(config)#ipv6 router ospf 6	Se habilita OSPF con su indicador
R3(config-rtr)#router-id 0.0.6.3	Se configura el identificador
R3(config-rtr)#exit	
R3(config)#interface gi2/0	Se accede a la interfaz
R3(config-if)#ipv6 ospf 6 area 0	Se habilita OSPFv6 en la interfaz y se configura el área
R3(config-if)#exit	
R3(config)#interface se1/0	Se accede a la interfaz

R3(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
R3(config-if)#exit	

Switch D1

D1(config)#ipv6 router ospf 6 indicador	Se habilita OSPF con su
D1(config-rtr)#router-id 0.0.6.131	Se configura el identificador
D1(config-rtr)#passive-interface default como pasivas	Se configuran las interfaces
D1(config-rtr)#no passive-interface e2/0 estar pasiva	Se excluye la interfaz de
D1(config-rtr)#exit	
D1(config)#interface e2/0	Se accede a la interfaz
D1(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D1(config-if)#exit	
D1(config)#interface vlan 100	Se accede a la interfaz
D1(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D1(config-if)#exit	
D1(config)#interface vlan 101	Se accede a la interfaz
D1(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D1(config-if)#exit	
D1(config)#interface vlan 102	Se accede a la interfaz
D1(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D1(config-if)#exit	
D1(config)#	

Switch D2

D2(config)#ipv6 router ospf 6 indicador	Se habilita OSPF con su
D2(config-rtr)#router-id 0.0.6.132	Se configura el identificador
D2(config-rtr)#passive-interface default como pasivas	Se configuran las interfaces
D2(config-rtr)#no passive-interface e2/0 estar pasiva	Se excluye la interfaz de
D2(config-rtr)#exit	
D2(config)#interface e2/0	Se accede a la interfaz

D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#interface vlan 100	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#interface vlan 101	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#interface vlan 102	Se accede a la interfaz
D2(config-if)#ipv6 ospf 6 area 0 interfaz y se configura el área	Se habilita OSPFv6 en la
D2(config-if)#exit	
D2(config)#	

Tabla 12. Tabla de asingación de tareas 3.3.

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

		En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).

Fuente: Autora.

Router R2

R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 Se configura una ruta predeterminada con interfaz de salida loopback
R2(config)#ipv6 route ::/0 loopback 0 Se configura una ruta IPv6 predeterminada con interfaz de salida loopback
R2(config)#router bgp 500 Se configura bgp 500
R2(config-router)# bgp router-id 2.2.2.2 Se asigna un identificador bgp
R2(config-router)# neighbor 209.165.200.225 remote-as 300 Se configura la relación con R1 en ASN 300
R2(config-router)# neighbor 2001:db8:200::1 remote-as 300 Se configura la relación con R1 en ASN 300
R2(config-router)# address-family ipv4
R2(config-router-af)# neighbor 209.165.200.225 activate Se configura la relación con el vecino activa
R2(config-router-af)# no neighbor 2001:db8:200::1 activate Se excluye la dirección IPv6
R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255 Se configura la relación con la interface loopback de R2
R2(config-router-af)# network 0.0.0.0 Redes predeterminadas
R2(config-router-af)# exit-address-family
R2(config-router)# address-family ipv6
R2(config-router-af)# no neighbor 209.165.200.225 activate Se configura la relación con el vecino activa
R2(config-router-af)# neighbor 2001:db8:200::1 activate Se incluye la dirección IPv6
R2(config-router-af)# network 2001:db8:2222::/128 Se excluye la dirección IPv6
R2(config-router-af)# network ::/0 Redes predeterminadas
R2(config-router-af)# exit-address-family
R2(config-router)#

Tabla 13. Tabla de asingación de tareas 3.4.

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.

Fuente: Autora.

Router R1

R1(config)#ip route 10.0.0.0 255.0.0.0 null0	Se configura una ruta predeterminada con interfaz de salida
R1(config)#ipv6 route 2001:db8:100::/48 null0	Se configura una ruta IPv6 predeterminada con interfaz de salida
R1(config)#router bgp 300	Se configura bgp 300

R1(config-router)# bgp router-id 1.1.1.1 Se asigna un identificador bgp
R1(config-router)# neighbor 209.165.200.226 remote-as 500 Se configura la relación con R2 en ASN 500
R1(config-router)# neighbor 2001:db8:200::2 remote-as 500 Se configura la relación con R2 en ASN 500
R1(config-router)# address-family ipv4 unicast
R1(config-router-af)# neighbor 209.165.200.226 activate Se configura la relación con el vecino activa
R1(config-router-af)# no neighbor 2001:db8:200::2 activate
R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0
R1(config-router-af)# exit-address-family
R1(config-router)# address-family ipv6 unicast
R1(config-router-af)# no neighbor 209.165.200.226 activate Se deshabilita la relación con el vecino activa
R1(config-router-af)# neighbor 2001:db8:200::2 activate Se configura la relación con el vecino activa
R1(config-router-af)# network 2001:db8:100::/48 Se configura la dirección ipv6
R1(config-router-af)# exit-address-family
R1(config-router)#exit
R1(config)#

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

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

Las tareas de configuración son las siguientes:

Tabla 14. Tabla de asingación de tareas 4.1.

Tarea#	Tarea	Especificación

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

Fuente: Autora.

<u>Configuración en D1.</u>

```
D1#configure terminal
D1(config)#ip sla 4                                   Se configura sla
D1(config-ip-sla)#icmp-echo 10.0.10.1                 Se configura la interfaz a probar
D1(config-ip-sla-echo)#frequency 5                    Se configura la frecuencia
D1(config-ip-sla-echo)#exit
D1(config)#ip sla 6                                   Se configura sla
D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1      Se configura la interfaz a probar
D1(config-ip-sla-echo)#frequency 5                    Se configura la frecuencia
D1(config-ip-sla-echo)#exit
D1(config)#ip sla schedule 4 life forever start-time now      Se activa la operación del sla
D1(config)#ip sla schedule 6 life forever start-time now      Se activa la operación del sla
D1(config)#track 4 ip sla 4                           Se configura un verificador de estado de IP SLA
D1(config-track)#delay down 10 up 15                 Cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos
D1(config-track)#exit
```

D1(config)#track 6 ip sla 6 Se configura un verificador de estado de IP SLA
D1(config-track)#delay down 10 up 15 Cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos
D1(config-track)#exit
D1(config)#

Tabla 15. Tabla de asingación de tareas 4.2.

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.

Fuente: Autora.

<u>Configuración en D2.</u>

D2#configure terminal
D2(config)#ip sla 4 Se configura sla
D2(config-ip-sla)#icmp-echo 10.0.11.1 Se configura la interfaz a probar
D2(config-ip-sla-echo)#frequency 5 Se configura la frecuencia
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6 Se configura sla
D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 Se configura la interfaz a probar

D2(config-ip-sla-echo)#frequency 5 Se configura la frecuencia
D2(config-ip-sla-echo)#exit
D2(config)#ip sla schedule 4 life forever start-time now Se activa la operación del sla
D2(config)#ip sla schedule 6 life forever start-time now Se activa la operación del sla
D2(config)#track 4 ip sla 4 Se configura un verificador de estado de IP SLA
D2(config-track)#delay down 10 up 15 Cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos
D2(config-track)#exit
D2(config)#track 6 ip sla 6 Se configura un verificador de estado de IP SLA
D2(config-track)#delay down 10 up 15 Cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos
D2(config-track)#exit
D2(config)#

Tabla 16. Tabla de asingación de tareas 4.3.

4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. • Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. • Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Establezca la prioridad del grupo en 150. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60.

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

		• Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Rastree el objeto 6 para disminuir en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • 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.

Configuración en D1.

D1(config)#interface vlan 100	Se accede a la interfaz
D1(config-if)#standby version 2	Se habilita HSRPv2
D1(config-if)#standby 104 ip 10.0.100.254	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 104 priority 150	Se establece la prioridad del grupo en 150
D1(config-if)#standby 104 preempt	Se habilita la preferencia
D1(config-if)#standby 104 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#standby 106 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 106 priority 150	Se establece la prioridad del grupo en 150
D1(config-if)#standby 106 preempt	Se habilita la preferencia
D1(config-if)#standby 106 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#exit	
D1(config)#interface vlan 101	Se accede a la interfaz
D1(config-if)#standby version 2	Se habilita HSRPv2
D1(config-if)#standby 114 ip 10.0.101.254	Se asigna la dirección IP virtual para el respectivo grupo

D1(config-if)#standby 114 preempt	Se habilita la preferencia
D1(config-if)#standby 114 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#standby 116 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 116 preempt	Se habilita la preferencia
D1(config-if)#standby 116 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#exit	
D1(config)#interface vlan 102	Se accede a la interfaz
D1(config-if)#standby version 2	Se habilita HSRPv2
D1(config-if)#standby 124 ip 10.0.102.254	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 124 priority 150	Se configura la prioridad del grupo
D1(config-if)#standby 124 preempt	Se habilita la preferencia
D1(config-if)#standby 124 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#standby 126 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D1(config-if)#standby 126 priority 150	Se configura la prioridad del grupo
D1(config-if)#standby 126 preempt	Se habilita la preferencia
D1(config-if)#standby 126 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D1(config-if)#exit	

Configuración en D2.

D2(config)#interface vlan 100	Se accede a la interfaz
D2(config-if)# standby version 2	Se habilita HSRPv2
D2(config-if)# standby 104 ip 10.0.100.254	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 104 preempt	Se habilita la preferencia
D2(config-if)# standby 104 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# standby 106 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 106 preempt	Se habilita la preferencia
D2(config-if)# standby 106 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# exit	
D2(config)#interface vlan 101	Se accede a la interfaz
D2(config-if)# standby version 2	Se habilita HSRPv2

D2(config-if)# standby 114 ip 10.0.101.254	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 114 priority 150	Se establece la prioridad del grupo en 150
D2(config-if)# standby 114 preempt	Se habilita la preferencia
D2(config-if)# standby 114 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# standby 116 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 116 priority 150	Se establece la prioridad del grupo en 150
D2(config-if)# standby 116 preempt	Se habilita la preferencia
D2(config-if)# standby 116 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# exit	
D2(config)#interface vlan 102	Se accede a la interfaz
D2(config-if)# standby version 2	Se habilita HSRPv2
D2(config-if)# standby 124 ip 10.0.102.254	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 124 preempt	Se habilita la preferencia
D2(config-if)# standby 124 track 4 decrement 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# standby 126 ipv6 autoconfig	Se asigna la dirección IP virtual para el respectivo grupo
D2(config-if)# standby 126 preempt	Se habilita la preferencia
D2(config-if)# standby 126 track 6 decrement 60	Se rastrea el objeto y decrementa en 60
D2(config-if)# exit	

1.9. 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 17. Tabla de asingación de tareas 5.1.

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

Fuente: Autora.

Configuración en R1.

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encryptación SCRYPT

Configuración en R2.

R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encryptación SCRYPT

Configuración en R3.

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encryptación SCRYPT

Configuración en D1.

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encryptación SCRYPT

Configuración en D2.

D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encryptación SCRYPT

Configuración en A1.

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco Se protege el EXEC privilegiado usando el algoritmo de encryptación SCRYPT

Tabla 18. Tabla de asingación de tareas 5.2.

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**

Fuente: Autora.

Configuración en R1.

R1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Se crea un usuario local protegido con el algoritmo de encriptación SCRYPT

Configuración en R2.

R2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Se crea un usuario local protegido con el algoritmo de encriptación SCRYPT

Configuración en R3.

R3(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Se crea un usuario local protegido con el algoritmo de encriptación SCRYPT

Configuración en D1.

D1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Se crea un usuario local protegido con el algoritmo de encriptación SCRYPT

Configuración en D2.

D2(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Se crea un usuario local protegido con el algoritmo de encriptación SCRYPT

Configuración en A1.

A1(config)#username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco Se crea un usuario local protegido con el algoritmo de encriptación SCRYPT

Tabla 19. Tabla de asingación de tareas 5.3.

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

Fuente: Autora.

Configuración en R1.

R1(config)#aaa new-model Se habilita AAA

Configuración en R3.

R3(config)#aaa new-model Se habilita AAA

Configuración en D1.

D1(config)#aaa new-model Se habilita AAA

Configuración en D2.

D2(config)#aaa new-model Se habilita AAA

Configuración en A1.

A1(config)#aaa new-model Se habilita AAA

Tabla 20. Tabla de asingación de tareas 5.4.

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**

Fuente: Autora.

Configuración en R1.

R1(config)#radius server RADIUS Se configura servidor Radius
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
Se configura la dirección RADIUS con sus respectivos puertos
R1(config-radius-server)#key $trongPass Se asigna la contraseña
R1(config-radius-server)#exit

Configuración en R3.

R3(config)#radius server RADIUS Se configura servidor Radius
R3(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
Se configura la dirección RADIUS con sus respectivos puertos
R3(config-radius-server)#key $trongPass Se asigna la contraseña
R3(config-radius-server)#exit

Configuración en D1.

D1(config)#radius server RADIUS Se configura servidor Radius

D1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
Se configura la dirección RADIUS con sus respectivos puertos
D1(config-radius-server)#key $trongPass Se asigna la contraseña
D1(config-radius-server)#exit
D1(config)#

Configuración en D2.

D2(config)#radius server RADIUS Se configura servidor Radius
D2(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
Se configura la dirección RADIUS con sus respectivos puertos
D2(config-radius-server)#key $trongPass Se asigna la contraseña
D2(config-radius-server)#exit

Configuración en A1.

A1(config)#radius server RADIUS Se configura servidor Radius
A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813 Se configura la dirección RADIUS con sus respectivos puertos
A1(config-radius-server)# key $trongPass Se asigna la contraseña
A1(config-radius-server)# exit

Tabla 21. Tabla de asingación de tareas 5.5.

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.

Fuente: Autora.

Configuración en R1.

R1(config)#aaa authentication login default group radius local — Se configura la lista de métodos de autenticación AAA

Configuración en R3.

R3(config)#aaa authentication login default group radius local — Se configura la lista de métodos de autenticación AAA

Configuración en D1.

D1(config)#aaa authentication login default group radius local — Se configura la lista de métodos de autenticación AAA

Configuración en D2.

D2(config)#aaa authentication login default group radius local — Se configura la lista de métodos de autenticación AAA

Configuración en A1.

A1(config)#aaa authentication login default group radius local — Se configura la lista de métodos de autenticación AAA

Tabla 22. Tabla de asingación de tareas 5.6.

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**.

Fuente: Autora.

1.10. 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 23. Tabla de asingación de tareas 6.1.

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.

Fuente: Autora.

Configuración en R1.

R1(config)#clock timezone utc -5 Se configura el reloj a la hora UTC actual

Configuración en R2.

R2(config)#clock timezone utc -5 Se configura el reloj a la hora UTC actual

Configuración en R3.

R3(config)#clock timezone utc -5 Se configura el reloj a la hora UTC actual

Configuración en D1.

D1(config)#clock timezone utc -5 Se configura el reloj a la hora UTC actual

Configuración en D2.

D2(config)#clock timezone utc -5 Se configura el reloj a la hora UTC actual

Configuración en A1.

A1(config)#clock timezone utc -5 Se configura el reloj a la hora UTC actual

Tabla 24. Tabla de asingación de tareas 6.2.

6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.

Fuente: Autora.

Configuración en R2.

R2(config)#ntp master 3 Se configura como NTP maestro

Tabla 25. Tabla de asingación de tareas 6.3.

6.3	Configure NTP en R1, R3, D1, D2, y A1.	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. • D2 para sincronizar la hora con R3.

Fuente: Autora.

Configuración en R1.

R1(config)#ntp server 2.2.2.2 Se sincroniza NTP

Configuración en R3.

R3(config)#ntp server 10.0.10.1 Se sincroniza NTP

Configuración en D1.

D1(config)#ntp server 10.0.10.1 Se sincroniza NTP

Configuración en D2.

D2(config)#ntp server 10.0.10.1 Se sincroniza NTP

Configuración en A1.

A1(config)#ntp server 10.0.10.1 Se sincroniza NTP

Tabla 26. Tabla de asingación de tareas 6.4.

6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.

Fuente: Autora.

Configuración en R1.

R1(config)#logging trap warning Se configura el Syslog de peligro
R1(config)#logging host 10.0.100.5 Se configura el envío del syslog a la PC1
R1(config)#logging on Se habilita el syslog

Configuración en R3.

R3(config)#logging trap warning Se configura el Syslog de peligro
R3(config)#logging host 10.0.100.5 Se configura el envío del syslog a la PC1
R3(config)#logging on Se habilita el syslog

Configuración en D1.

D1(config)#logging trap warning	Se configura el Syslog de peligro
D1(config)#logging host 10.0.100.5	Se configura el envío del syslog a la PC1
D1(config)#logging on	Se habilita el syslog

Configuración en D2.

D2(config)#logging trap warning	Se configura el Syslog de peligro
D2(config)#logging host 10.0.100.5	Se configura el envío del syslog a la PC1
D2(config)#logging on	Se habilita el syslog

Configuración en A1.

A1(config)#logging trap warning	Se configura el Syslog de peligro
A1(config)#logging host 10.0.100.5	Se configura el envío del syslog a la PC1
A1(config)#logging on	Se habilita el syslog

Tabla 27. Tabla de asingación de tareas 6.5.

6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *traps config* y *ospf*.

		• En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

Fuente: Autora.

Configuración en R1.

R1(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
R1(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
R1(config-std-nacl)#exit	
R1(config)#snmp-server contact Daniela Ochoa	Se configura el valor de contacto SNMP
R1(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura
R1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la dirección donde se envían los traps
R1(config)# snmp-server ifindex persist	Se habilita la persistencia de index
R1(config)# snmp-server enable traps bgp	Se habilita el envío de traps bgp
R1(config)# snmp-server enable traps config	Se habilita el envío de traps config
R1(config)# snmp-server enable traps ospf	Se habilita el envío de traps ospf

Configuración en R3.

R3(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
R3(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
R3(config-std-nacl)#exit	
R3(config)#snmp-server contact Daniela Ochoa	Se configura el valor de contacto SNMP
R3(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura

R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA Se configura la dirección donde se envían los traps
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#

Configuración en D1.

D1(config)#ip access-list standard SNMP Se configura una lista de acceso estándar
D1(config-std-nacl)#permit host 10.0.100.5 Se permite SNMP a la dirección del PC1
D1(config-std-nacl)#exit
D1(config)#snmp-server contact Daniela Ochoa Se configura el valor de contacto SNMP
D1(config)#snmp-server community ENCORSA ro SNMP Se configura el nombre de comunidad y se habilita de solo lectura
D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA Se configura la dirección donde se envían los traps
D1(config)# snmp-server ifindex persist Se habilita la persistencia de index
D1(config)# snmp-server enable traps config Este comando no es soportado por la imagen utilizada
D1(config)# snmp-server enable traps ospf Se habilita el envío de traps ospf

Configuración en D2.

D2(config)#ip access-list standard SNMP Se configura una lista de acceso estándar
D2(config-std-nacl)#permit host 10.0.100.5 Se permite SNMP a la dirección del PC1
D2(config-std-nacl)# exit
D2(config)# snmp-server contact Daniela Ochoa Se configura el valor de contacto SNMP
D2(config)#snmp-server community ENCORSA ro SNMP Se configura el nombre de comunidad y se habilita de solo lectura
D2(config)#snmp-server host 10.0.100.5 version 2c ENCORSA Se configura la dirección donde se envían los traps
D2(config)# snmp-server enable traps config Este comando no es soportado por la imagen utilizada

D2(config)# snmp-server enable traps ospf	Se habilita el envío de traps ospf

Configuración en A1.

A1(config)#ip access-list standard SNMP	Se configura una lista de acceso estándar
A1(config-std-nacl)#permit host 10.0.100.5	Se permite SNMP a la dirección del PC1
A1(config-std-nacl)# exit	
A1(config)# snmp-server contact Daniela Ochoa	Se configura el valor de contacto SNMP
A1(config)#snmp-server community ENCORSA ro SNMP	Se configura el nombre de comunidad y se habilita de solo lectura
A1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA	Se configura la dirección donde se envían los traps
A1(config)# snmp-server ifindex persist	Se habilita la persistencia de index
A1(config)# snmp-server enable traps config	Este comando no es soportado por la imagen utilizada
A1(config)# snmp-server enable traps ospf	Se habilita el envío de traps ospf

CONCLUSIONES

CCNP permite adquirir a los estudiantes conocimientos y habilidades necesarios para que planifiquen, implementen, protejan, mantengan y solucionen fallas de red. CCNP tiene como objetivo reflejar habilidades y responsabilidades laborales relacionadas con los roles profesionales de ingeniero de redes, ingeniero de sistemas, ingeniero de soporte de redes, administrador de redes Ingeniero de telecomunicaciones de red, consultor de redes e integrador de sistemas y otras carreras relacionadas.

Esta prueba permite comprender como sería la aplicación de varios conceptos de redes, la implementación de técnicas y la verificación de aplicaciones realizadas a los dispositivos, que van desde la implementación de vlans en dispositivos switch capa 3, la habilitación del enrutamiento ipv6 y la ejecución de bgp con un asn designado.

La enseñanza a través de ejercicios desarrollados permite la simulación de los mismos, de como sería en un entorno real, ya que en un futuro al realizar la aplicación y desarrollo de redes y demás elementos se hace menos complicado, al mismo tiempo que algunas de ellas son de aplicación constante en el sector industrial de los sistemas y las Telecomunicaciones.

BIBLIOGRAFÍA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

ANEXO 1. CONFIGURACION DE LOS DISPOSITIVOS

Router R1

```
R1#show run
Building configuration...

Current configuration : 3853 bytes
!
! Last configuration change at 20:46:54 utc Mon Nov 22 2021
! NVRAM config last updated at 20:46:56 utc Mon Nov 22 2021
! NVRAM config last updated at 20:46:56 utc Mon Nov 22 2021
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 9
$9$dfwXI1xDuveXUx$OZ0Csr52RsD89lH/PH4YB6cdpxbF3F2HENhzjoEQSuE
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
```

```
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username sadmin privilege 15 secret 9
$9$ySf7MFNP/zTcUa$JilyD90i2vc7QcJg55K6SIqM7U4BnWn55cnulWLij7Q
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 209.165.200.225 255.255.255.224
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address FE80::1:1 link-local
```

```
 ipv6 address 2001:DB8:200::1/64
!
interface Serial1/0
 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
 ipv6 ospf 6 area 0
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface GigabitEthernet2/0
 ip address 10.0.10.1 255.255.255.0
 negotiation auto
 ipv6 address FE80::1:2 link-local
 ipv6 address 2001:DB8:100:1010::1/64
 ipv6 ospf 6 area 0
!
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
!
router bgp 300
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 2001:DB8:200::2 remote-as 500
 neighbor 209.165.200.226 remote-as 500
 !
 address-family ipv4
  network 10.0.0.0
```

```
  no neighbor 2001:DB8:200::2 activate
  neighbor 209.165.200.226 activate
 exit-address-family
 !
 address-family ipv6
  network 2001:DB8:100::/48
  neighbor 2001:DB8:200::2 activate
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 10.0.0.0 255.0.0.0 Null0
!
ip access-list standard SNMP
 permit 10.0.100.5
!
logging trap warnings
logging host 10.0.100.5
no cdp log mismatch duplex
ipv6 route 2001:DB8:100::/48 Null0
ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate
!
!
snmp-server community ENCORSA RO SNMP
snmp-server ifindex persist
snmp-server contact Daniela Ochoa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps bgp
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
```

```
!
!
!
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
 shutdown
!
banner motd ^C R1, ENCOR Skills Assessment, Scenario 1 ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 transport input all
!
ntp server 2.2.2.2
!
end

R1#
```

Router R2

```
R2#show run
Building configuration...

Current configuration : 2534 bytes
!
! Last configuration change at 20:46:48 utc Mon Nov 22 2021
! NVRAM config last updated at 20:46:51 utc Mon Nov 22 2021
! NVRAM config last updated at 20:46:51 utc Mon Nov 22 2021
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable secret 9
$9$zO4aNmattL7hxh$NU5xf8eT3TJbTHc/hiEBUMCxUaiJbFVaIdT0poMantU
!
no aaa new-model
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
```

```
!
!
!
!
username sadmin privilege 15 secret 9
$9$wzXUi5yMQE2HUK$SO.PYoD/NsEcwyBHq/YvPMy1Z.4.Z59wlSJfONT//Gc
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ipv6 address FE80::2:3 link-local
 ipv6 address 2001:DB8:2222::1/128
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 209.165.200.226 255.255.255.224
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address FE80::2:1 link-local
 ipv6 address 2001:DB8:200::2/64
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
```

```
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router bgp 500
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 neighbor 2001:DB8:200::1 remote-as 300
 neighbor 209.165.200.225 remote-as 300
 !
 address-family ipv4
  network 0.0.0.0
  network 2.2.2.2 mask 255.255.255.255
  no neighbor 2001:DB8:200::1 activate
  neighbor 209.165.200.225 activate
 exit-address-family
 !
 address-family ipv6
  network ::/0
  network 2001:DB8:2222::/128
  neighbor 2001:DB8:200::1 activate
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 Loopback0
```

```
!
no cdp log mismatch duplex
ipv6 route ::/0 Loopback0
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
 shutdown
!
banner motd ^C R2, ENCOR Skills Assessment, Scenario 1 ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
!
ntp master 3
!
end

R2#
```

Router R3

```
R3#show run
Building configuration...

Current configuration : 3214 bytes
!
! Last configuration change at 20:46:42 utc Mon Nov 22 2021
! NVRAM config last updated at 20:46:45 utc Mon Nov 22 2021
! NVRAM config last updated at 20:46:45 utc Mon Nov 22 2021
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
enable secret 9
$9$YOt0sly5FMi/ex$cAj3bV7J70QpOK3Y.XwfFMIsA/DUzuC7IMqkLbcQGbc
!
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
```

```
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username sadmin privilege 15 secret 9
$9$OClK0Ljh3JdgM4$7hDevnTiV/t1DUHsqRqun9I9Ilm.tEPgECi4Rgpp3uw
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface Serial1/0
 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
 ipv6 ospf 6 area 0
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface GigabitEthernet2/0
 ip address 10.0.11.1 255.255.255.0
 negotiation auto
 ipv6 address FE80::3:2 link-local
 ipv6 address 2001:DB8:100:1011::1/64
 ipv6 ospf 6 area 0
!
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
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ip access-list standard SNMP
 permit 10.0.100.5
!
logging trap warnings
logging host 10.0.100.5
no cdp log mismatch duplex
ipv6 router ospf 6
```

```
 router-id 0.0.6.3
!
!
snmp-server community ENCORSA RO SNMP
snmp-server ifindex persist
snmp-server contact Daniela Ochoa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps entity-sensor threshold
snmp-server enable traps config
snmp-server host 10.0.100.5 version 2c ENCORSA
!
!
!
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
 shutdown
!
banner motd ^C R3, ENCOR Skills Assessment, Scenario 1 ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 transport input all
!
ntp server 10.0.10.1
!
end

R3#
```

Switch D1

```
D1#show run
Building configuration...

Current configuration : 6495 bytes
!
! Last configuration change at 23:32:22 utc Mon Nov 22 2021
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname D1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 9
$9$N18ZH2rCsPNw23$qfuuLw/pfgMLvpCbqg7sD2ImaCxbUB4.N4v7KYccNIE
!
username sadmin privilege 15 secret 9
$9$uwioLkOU.Li0vp$3zFmF.2XJSJ5TW8nTrduv4Aoqn/216BYybTRpN.K.Tg
aaa new-model
```

```
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
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
!
ip dhcp pool VLAN-102
 network 10.0.102.0 255.255.255.0
 default-router 10.0.102.254
!
!
no ip domain-lookup
ip cef
!
!
!
!
!
ipv6 unicast-routing
ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
track 4 ip sla 4
 delay down 10 up 15
!
```

```
track 6 ip sla 6
 delay down 10 up 15
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
 shutdown
!
interface Ethernet0/1
 shutdown
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet1/0
 shutdown
!
interface Ethernet1/1
 shutdown
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
interface Ethernet2/0
 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
!
interface Ethernet2/1
 shutdown
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Vlan1
 no ip address
```

```
 shutdown
!
interface Vlan100
 ip address 10.0.100.1 255.255.255.0
 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
 ipv6 address FE80::D1:2 link-local
 ipv6 address 2001:DB8:100:100::1/64
!
interface Vlan101
 ip address 10.0.101.1 255.255.255.0
 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
 ipv6 address FE80::D1:3 link-local
 ipv6 address 2001:DB8:100:101::1/64
!
interface Vlan102
 ip address 10.0.102.1 255.255.255.0
 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
 ipv6 address FE80::D1:4 link-local
 ipv6 address 2001:DB8:100:102::1/64
!
ip forward-protocol nd
!
no ip http server
```

```
!
ip access-list standard SNMP
 permit 10.0.100.5
!
!
ip sla 4
 icmp-echo 10.0.10.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1010::1
 frequency 5
ip sla schedule 6 life forever start-time now
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Daniela Ochoa
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps eigrp
snmp-server enable traps tty
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps bfd
snmp-server enable traps bgp cbgp2
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-
change inconsistency
snmp-server enable traps dlsw
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps msdp
```

```
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-
message
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps syslog
snmp-server enable traps event-manager
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop
config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown
service-up
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps energywise
snmp-server enable traps pw vc
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps ether-oam
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps mpls vpn
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
!
!
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
!
!
control-plane
```

```
!
banner motd ^C D1, ENCOR Skills Assessment, Scenario 1 ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
!
ntp server 10.0.10.1
!
end
D1#
```

Switch D2

```
D2#show run
Building configuration...

Current configuration : 4304 bytes
!
! Last configuration change at 23:32:17 utc Mon Nov 22 2021
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname D2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 9
$9$/PCvwoh3y4BKV3$wpyFV9SGzE8fN93er0QYLat6Z0I7ow3Dh0rghvNGcgg
!
```

```
username sadmin privilege 15 secret 9
$9$2.rPJuq6WKvRBp$0CymCH.cstsyvnGA5vqImngoizHoeh07NksNwChPjEA
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
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
!
ip dhcp pool VLAN-102
 network 10.0.102.0 255.255.255.0
 default-router 10.0.102.254
!
!
no ip domain-lookup
ip cef
!
!
!
!
!
ipv6 unicast-routing
ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
```

```
track 4 ip sla 4
 delay down 10 up 15
!
track 6 ip sla 6
 delay down 10 up 15
!
ip tcp synwait-time 5
!
!
!
!
interface Ethernet0/0
 shutdown
!
interface Ethernet0/1
 shutdown
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet1/0
 shutdown
!
interface Ethernet1/1
 shutdown
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
interface Ethernet2/0
 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
!
interface Ethernet2/1
 shutdown
!
interface Ethernet2/2
```

```
!
interface Ethernet2/3
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 ip address 10.0.100.2 255.255.255.0
 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
 ipv6 address FE80::D2:2 link-local
 ipv6 address 2001:DB8:100:100::2/64
!
interface Vlan101
 ip address 10.0.101.2 255.255.255.0
 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
 ipv6 address FE80::D2:3 link-local
 ipv6 address 2001:DB8:100:101::2/64
!
interface Vlan102
 ip address 10.0.102.2 255.255.255.0
 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
 ipv6 address FE80::D2:4 link-local
 ipv6 address 2001:DB8:100:102::2/64
!
```

```
ip forward-protocol nd
!
!
no ip http server
!
ip access-list standard SNMP
 permit 10.0.100.5
!
!
ip sla 4
 icmp-echo 10.0.11.1
 frequency 5
ip sla schedule 4 life forever start-time now
ip sla 6
 icmp-echo 2001:DB8:100:1011::1
 frequency 5
ip sla schedule 6 life forever start-time now
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Daniela Ochoa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
!
!
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
!
!
control-plane
!
banner motd ^C D2, ENCOR Skills Assessment, Scenario 1 ^C
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
!
ntp server 10.0.10.1
!
end

D2#
```

Switch A1

```
A1#show run
Building configuration...

Current configuration : 2736 bytes
!
! Last configuration change at 23:32:12 utc Mon Nov 22 2021
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname A1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 9
$9$W/1/gBOKadZ5wJ$dfxyC82BOcPNnpXlLuHeRLyglVx9V05lYgzvLa0z.HA
!
username sadmin privilege 15 secret 9
$9$vV/1VA/oZc1N8Z$GHJJcWBrzZhs8x/jFZqDMB7Cnj1iqDBUFkryaToSblQ
```

```
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
!
!
!
aaa session-id common
clock timezone utc -5 0
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup
ip cef
!
!
!
!
!
no ipv6 cef
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
```

```
interface Ethernet1/1
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
interface Ethernet2/0
 shutdown
!
interface Ethernet2/1
 shutdown
!
interface Ethernet2/2
 shutdown
!
interface Ethernet2/3
 shutdown
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 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
!
ip forward-protocol nd
!
!
no ip http server
!
ip access-list standard SNMP
 permit 10.0.100.5
!
```

```
!
logging trap warnings
logging host 10.0.100.5
!
!
snmp-server community ENCORSA RO SNMP
snmp-server contact Daniela Ochoa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server host 10.0.100.5 version 2c ENCORSA
snmp ifmib ifindex persist
!
!
radius server RADIUS
 address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
 key $trongPass
!
!
control-plane
!
banner motd ^C A1, ENCOR Skills Assessment, Scenario 1 ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
!
ntp server 10.0.10.1
!
end

A1#
```