DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

VICTOR ALFOSO GONZALEZ GUZMAN

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

VICTOR ALFONSO GONZALEZ GUZMAN

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

DIRECTOR:

Msc GERARDO GRANADOS ACUÑA

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

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 29 de noviembre de 2021

AGRADECIMIENTOS

Quiero agradecer ante todo a Dios por permitirme alcanzar los logros propuestos ya que ha sido mi guiador en este trayecto educativo la cual me da fortaleza espiritual para continuar con este proyecto tan importante y significativo en mi vida personal y profesional.

Agradecimientos totales y sinceros para mis padres y hermanos la cual han sido un apoyo incondicional tanto económico como emocional, me han brindado el acompañamiento necesario para llevar a cabo los proyectos y metas planteadas, de igual forma a mis compañeros del grupo del diplomado y demás asignaturas que hemos estado en constante comunicación como apoyo fundamental y necesario académicamente.

Nuestros más sinceros agradecimientos a mi tutor del proyecto, quien con su conocimiento y experiencia fue una pieza fundamental para para el desarrollo, teniendo en cuenta que fueron imprescindibles para cada etapa de desarrollo del trabajo la cual se dieron respuestas oportunas a cada uno de los interrogantes.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LACP: La agregación virtual de enlaces, también llamada trunking, es una característica de nivel 2, que une puertos físicos de la red en un único enlace de datos de gran ancho de banda; de este modo se aumenta la capacidad de ancho debanda y se crean enlaces redundantes y de alta disponibilidad.

INTERFAZ LOOPBACK: La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo

REDUNDANCIA: La redundancia consiste en asegurar la supervivencia de la red ante un fallo, proporcionándole rutas de datos alternativas cuando se produce un fallo de enlace. Existen dos técnicas básicas de redundancia que aseguran la comunicación de datos

DHCP: (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de host. Protocolo que usan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin requerir que un administrador configure la información sobre la computadora en la base de datos de un servidor.

DNS: Domain Name System" (sistema de nombre de dominio). DNS es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.

OSPF: Open Shortest Path First (OSPF) es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF).

IP: La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, teléfono inteligente) que utilice el protocolo o (Internet Protocol).

RESUMEN

Con el desarrollo del presente trabajo denominado “documento final”, que realizamos la totalidad de su solución, con la finalidad de culminar el diplomado de profundización CCNP, la cual pondremos en prácticas las habilidades y destrezas que hemos adquirido durante las actividades de laboratorio y demás materias relacionadas con redes, en la actividad que le daremos solución se propone un escenario donde se evidencia las etapas y configuraciones que se deben realizar, que consta de 6 partes, para este escenario se va a utilizar el simulador grafico GNS3, con el manejo del simulador se buscan y se descargan los dispositivos Routers, switch, PCs y cables para empezar con la solución del escenario; tecnologías utilizadas de propiedad de CISCO.

Mediante este ejercicio se debe tener una accesibilidad de red de un extremo a otro que sea robusta y los dispositivos se complementen y tengan un buen funcionamiento, se procedió a cablear la red como se evidencia en el documento guía y posteriormente la respectiva configuración de los routers y switch con los comandos suministrados.

Se realiza la comunicación entre los computadores con todos los switches ofreciéndonos un direccionamiento DHCP y SLAAC para completar la configuración de la capa 2, con interfaces trocales IEEE 802.1Q la cual nos permite que las tramas de Ethernet viajen a través de la red con una etiqueta para poder así llevar la identificación. Con la habilitación del protocolo Rapid Spanning-Tree (RSTP) se busca la negociación en los enlaces eliminando algunos tiempos que tardan los temporizadores teniendo en cuenta que RSTP agrega dos nuevas funciones puerto de respaldo y puerto de borde.

Loa protocolos de enrutamiento IPV4 y IPV6 con la debida configuración con la finalidad de que la red este completamente con multiservicio para así mismo dar ping con D1 y D2 para verificar la comunicación, para D1 y D2 por medio de la configuración HSRP ya que la redundancia es obligatoria para dar continuidad a los servicios ya que desacopla las direcciones IP de la interfaz física y de esta forma permitir el asociamiento al grupo de interfaces en la “RED DE LA COMPAÑÍA”.

Para el desarrollo de la actividad con respecto a los dispositivos de las tecnologías se configuran mecanismos de seguridad usando el algoritmo de encripción SCRYPT con un cifrado de contraseñas basadas en el algoritmo y así crear un usuario local en todos los dispositivos y con nivel de privilegio 15 y con esta configuración permite ofrecer un nivel de seguridad superior.

Es importante y fundamental la administración de la red de esta forma se configura varias funciones como la configuración del reloj local y la configuración en R1, R3, D1, D2, y A1. Con el NTP protocolo de internet para la sincronizar los relojes de estos dispositivos a través del enrutamiento de paquetes.

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

ABSTRACT

With the development of this work called "final document", we carry out the entire solution, in order to complete the CCNP in-depth diploma, which we will put into practice the skills and abilities that we have acquired during laboratory activities and others. matters related to networks, in the activity that we will give a solution, a scenario is proposed where the stages and configurations that must be carried out are evidenced, which consists of 6 parts, for this scenario the GNS3 graphic simulator will be used, with the management of the simulator search and download devices Routers, switches, PCs and cables to start with the solution of the scenario; CISCO proprietary technologies used.

Through this exercise, you must have a robust network accessibility from one end to the other and the devices complement each other and have a good functioning, the network was wired as evidenced in the guide document and subsequently the respective configuration of the routers. and switch with supplied commands.

The communication between the computers is carried out with all the switches, offering us a DHCP and SLAAC addressing to complete the layer 2 configuration, with IEEE 802.1Q trocal interfaces which allows the Ethernet frames to travel through the network with a label. in order to carry the identification. With the enablement of the Rapid Spanning-Tree Protocol (RSTP), negotiation is sought in the links, eliminating some times that the timers take, taking into account that RSTP adds two new functions, backup port and edge port.

Loa routing protocols IPV4 and IPV6 with the proper configuration so that the network is completely with multiservice to also ping with D1 and D2 to verify communication, for D1 and D2 through the HSRP configuration since redundancy It is mandatory to give continuity to the services since it decouples the IP addresses of the physical interface and in this way allows the association to the group of interfaces in the "COMPANY NETWORK".

For the development of the activity with respect to the devices of the technologies, security mechanisms are configured using the encryption algorithm SCRYPT with an encryption of passwords based on the algorithm and thus create a local user on all devices and with privilege level 15 and with this configuration it allows to offer a higher level of security.

It is important and essential to manage the network in this way, several functions are configured such as the local clock configuration and the configuration in R1, R3, D1, D2, and A1. With the NTP internet protocol to synchronize the clocks of these devices through packet routing.

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

INTRODUCCIÓN

En el marco del curso de profundización CCNP, La presentación del trabajo final se evidencia mediante la elaboración del escenario propuesto en la guía del diplomado en CCNP que consta de 6 partes y se realiza el desarrollo utilizando el simulador grafico GNS3 ya que ejerce una copia exacta de los sistemas operativos con imágenes de enrutadores y swiches demostrado una serie de habilidades para realizar el laboratorio de acuerdo con la topografía con la finalidad de que los protocolos utilizados se configuren para una completa accesibilidad de los dispositivos con los computadores utilizados.

Con la configuración de los dispositivos y el direccionamiento de las interfaces para la construcción de la red y posteriormente realizar el cableado correspondiente entre los dispositivos.

Ingresamos mediante una conexión a consola al Router R1 en modo de configuración global aplicando los parámetros básicos, mediante el protocolo HSRP configurado en los dispositivos nos encargamos de proveer redundancia en la “red de la compañía” Con la habilitación del protocolo Rapid Spanning-Tree (RSTP) se busca la negociación en los enlaces, de acuerdo a que agrega dos nuevas funciones puerto de respaldo y puerto de borde para tener en cuneta al momento de realizar el laboratorio montado en le topografía.

DESARROLLO DEL EJERCICIO PROPUESTO

Figura 1: Escenario Propuesto

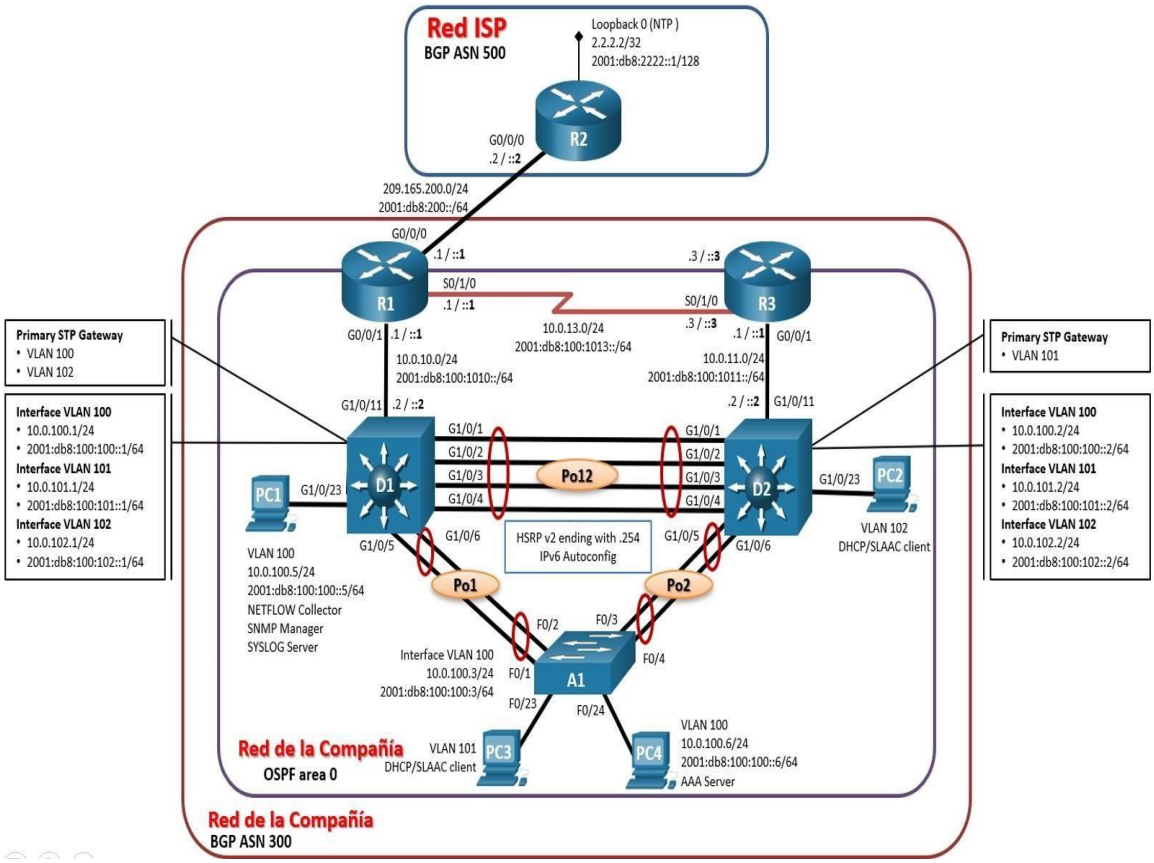


Tabla 1: Tabla de direccionamiento

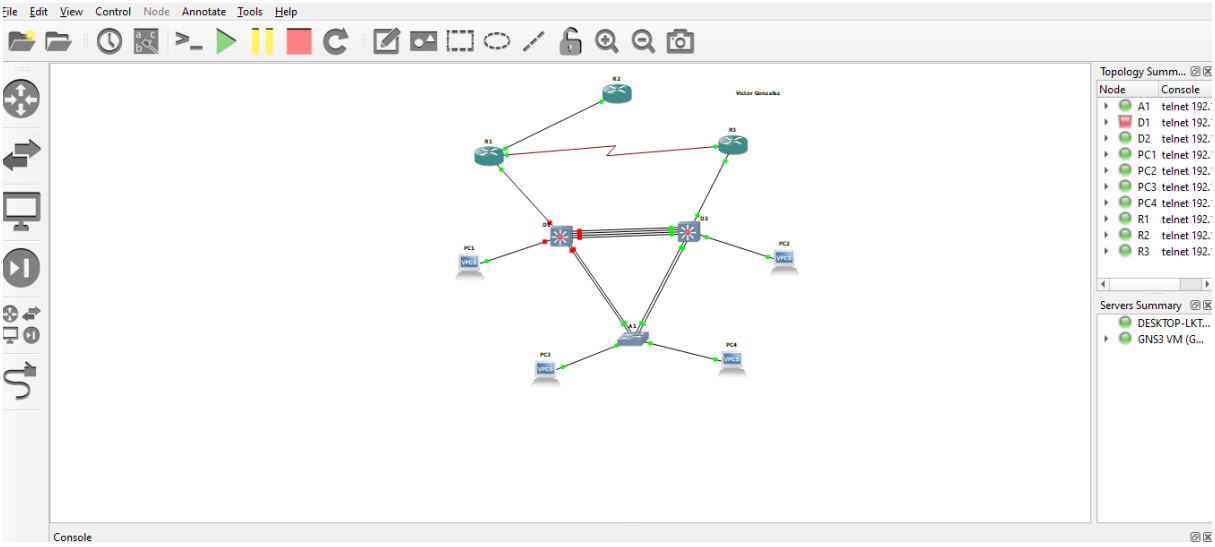
Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 LinkLocal
R1	E0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	E0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S02/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	E0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	E0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	E1/0	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	E1/0	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1

PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Parte 1: Construya la red y configure los ajustes básicos del dispositivo y el direccionamiento de la interfaz

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

Figura 2: Topología de Red a Cablear



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Router R1: Configuración básica.

R2(config)#**hostname R1** *>>Estando en modo configuración terminal con la instrucción hostname se procede a nombrar el equipo en este caso R1.*

R1(config)#**ipv6 unicast-routing** *>> Se habilita el protocolo Ipv6 en el router.*

R1(config)#**no ip domain lookup** *>> Si el comando que se ingrese a partir de esta línea es válido no va a generar ningún mensaje que interrumpa el comando ingresado.*

R1(config)#**banner motd # R1, ENCOR Skills Assessment, Scenario 1** #

R1(config)#**line con 0** *>> Ingreso al modo de configuración línea de consola 0.*

R1(config-line)#**exec-timeout 0 *0*** *>> Se indica que no habrá límite de tiempo por inactividad.*

R1(config-line)#**logging synchronous** *>> Evita que algún mensaje interrumpa la línea o comando ingresado.*

R1(config-line)#**exit** *>> Salir del modo consola.*

R1(config)#i**nterface e0/0** *>> En modo configuración global, se ingresa a la Interface Ethernet 0/0.*

R1(config-if)#**ip address** 209.165.200.225 255.255.255.224 *>> Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la F0/0.*

R1(config-if)#**ipv6 address fe80::1:1 link-local** *>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

R1(config-if)#**ipv6 address 2001:db8:200::1/64** *>> Asignación de la red estática.*

R1(config-if)#**no shutdow** *>> Se sube o enciende la interface.*

R1(config-if)#**exit** *>> Salir de la interface que se está configurando.*

R1(config)#**interface e0/1** *>> Ingreso a la interface Ethernet 0/1, estando en el modo configuración global.*

R1(config-if)#**ip address 10.0.10.1 255.255.255.0** *>> Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la F0/1.*

R1(config-if)#**ipv6 address fe80::1:2 link-local** *>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

R1(config-if)#**ipv6 address 2001:db8:100:1010::1/64** *>> Asignación de la red estática.*

R1(config-if)#**no shutdown** *>> Se sube o enciende la interface***.**

R1(config-if)#**exit** *>> Salir de la interface que se está configurando.*

Las configuraciones realizadas en las interfaces E0/0 y el E0/1, se van a ingresar también para la Interfaz del S2/0, aplican los mismos comandos

R1(config)#**interface s2/0** *>> Ingreso a la interfaz S2/0.*

R1(config-if)#**ip address 10.0.13.1 255.255.255.0** *>> Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la S0/1.*

R1(config-if)#**ipv6 address fe80::1:3 link-local** *>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

R1(config-if)#**ipv6 address 2001:db8:100:1013::1/*64*** *>> Asignación de la red estática.*

R1(config-if)#**no shutdown** *>> Se sube o enciende la interfaz S.*

R1(config-if)#**exit** *>> Salir de la interfaz que se está configurando.*

Router R2: Configuración básica.

R1(config)#**hostname R2** *>> Asignación de nombre al Router como R2.*

R2(config)#**ipv6 unicast-routing** *>> Se Habilita el protocolo Ipv6 en el router.*

R2(config)#**no ip domain lookup** *>> Si el comando que se ingrese a partir de esta línea es válido no va a generar ningún mensaje.*

R2(config)#**banner motd # R2, ENCOR Skills Assessment, Scenario 1** #

R2(config)#**line con 0** *>> Ingreso al modo de configuración línea de consola 0.*

R2(config-line)#**exec-timeout 0 0** *>> Se indica que no habrá límite de tiempo por inactividad.*

R2(config-line)#**logging synchronous** *>> Evita que algún mensaje interrumpa la línea o comando ingresado.*

R2(config-line)#**exit** *>> Salir del modo consola..*

En el Router R2 se aplican las configuraciones aplicadas en las interfaces del R1, para la interfaz E0/0 del R2. (aplica la misma descripción indicada en las líneas anteriores).

R2(config)#**interface e0/0**

R2(config-if)#**ip address 209.165.200.226 255.255.255.224**

R2(config-if)#**ipv6 address fe80::2:1 link-local**

R2(config-if)#**ipv6 address 2001:db8:200::2/64**

R2(config-if)#**no shutdown**

R2(config-if)#**exit**

Se crea una interfaz Loopback, se asigna direccionamiento correspondiente, habilitación del IPV6 y de la interfaz.

R2(config)#**interface Loopback 0** *>> se ingresa al interfaz Loopback 0.*

R2(config-if)#**ip address 2.2.2.2 255.255.255.*255*** *>> Se asigna la Ip y Mascara que usará la Interface Loopback.*

R2(config-if)#**ipv6 address fe80::2:3 link-local** *>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

R2(config-if)#**ipv6 address 2001:db8:2222::1/128** *>> Asignación de la red estática.*

R2(config-if)#**no shutdown** *>> Se sube o enciende la interface Loopback*

R2(config-if)#**exit** *>> Salir de la interface que se está configurando.*

Router R3: Configuración básica.

R3#**confi terminal** *>> Ingreso al modo configuración global.*

R3(config)#**hostname R3** *>>Asignación de nombre al Router.*

R3(config)#**ipv6 unicast-routing** *>> Se Habilita el protocolo Ipv6 en el Router.*

R3(config)#**no ip domain lookup** *>> Si el comando que se ingrese a partir de esta línea es válido no va a generar ningún mensaje.*

R3(config)#**line con 0** *>> Ingreso al modo de configuración línea de consola 0.*

R3(config-line)#**exec-timeout 0 0** *>> Se indica que no habrá límite de tiempo por inactividad.*

R3(config-line)#**logging synchronous** *>> Evita que algún mensaje interrumpa la línea o comando ingresado.*

R3(config-line)#**exit** *>> Salir del modo consola.*

Repetir comandos que se han aplicado en los Router **R1** y **R2** para la Interfaces **E0/0** y la **S2/0**, los cuales comprenden la asignación del direccionamiento a cada interfaz, habilitación del IPV6 y de la interfaz, asignación de la porción de red al prefijo FE80 del IPV6.

R3(config)#**interface e0/0**

R3(config-if)#**ip address 10.0.11.1 255.255.255.0**

R3(config-if)#**ipv6 address fe80::3:2 link-local**

R3(config-if)#**ipv6 address 2001:db8:100:1011::1/64**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

R3(config)#**interface s2/0**

R3(config-if)#**ip address 10.0.13.3 255.255.255.0**

R3(config-if)#**ipv6 address fe80::3:3 link-local**

R3(config-if)#**ipv6 address 2001:db8:100:1010::2/64**

R3(config-if)#**no shutdown**

R3(config-if)#**exit**

Switch D1: Configuración básica.

D1>**enable** *>> Se ingresa a modo privilegiado.*

D1#**configure terminal** *>> Se ingresa a modo configuración global.*

D1(config)#**ip routing** *>> Habilitar enrutamiento IP en el Switch.*

D1(config)#**ipv6 unicast-routing** *>> Se habilita el IPV6 sobre el Switch.*

D1(config)#**no ip domain lookup** *>> Permite que el sistema indiqué que el comando que se está ingresando no es válido, de esta forma no se tiene que esperar un tiempo hasta que salga el mensaje se error de ingreso del comando.*

D1(config)#**line con 0** *>> Ingreso a la línea de consola 0.*

D1(config-line)#**exec-timeout 0 0** *>> Configuración de las excepciones de tiempo.*

D1(config-line)#**logging synchronous** *>> Evita que algún mensaje interrumpa la línea o comando ingresado.*

D1(config-line)#**exit** *>> Salir del modo configuración.*

A continuación, se crean las VLAN 100, 101, 102, y 999 con sus respectivos nombres.

D1(config)#**vlan 100** *>> Ingresar a la Vlan a crear.*

D1(config-vlan)#**name Management** *>> Se nombra la Vlan Managment.*

D1(config-vlan)#**exit** *>> Salir del modo configuración.*

D1(config)#**vlan 101** *>> Ingresar a la Vlan a crear.*

D1(config-vlan)#**name UserGroupA** *>> Se nombra la Vlan UserGroupA.*

D1(config-vlan)#**exit** *>> Salir del modo configuración.*

D1(config)#**vlan 102** *>>Ingresar a la Vlan a crear.*

D1(config-vlan)#**name UserGroupB** *>> Se nombra la Vlan UserGroupB.*

D1(config-vlan)#**exit** *>> Salir del modo configuración.*

D1(config)#**vlan 999** *>> Ingresar a la Vlan a crear.*

D1(config-vlan)#**name NATIVE** *>> Se nombra la Vlan NATIVE.*

D1(config-vlan)#**exit** *>> Salir del modo configuración.*

Aplicación de los comandos ya usados en el **R1**, **R2** y **R3**, en este caso se aplica sobre la Ethernet 1/0

D1(config)#**interface e1/0** *>> Ingreso a la Interfaz Ethernet 1/0.*

D1(config-if)#**no switchport** **>>** *aporta a la interfaz capacidad de Capa 3. La dirección IP se encuentra en la misma subred que el Router predeterminado.*

D1(config-if)#**ip address 10.0.10.2 255.255.255.0** *>> Asignación de direccionamiento a la Ethernet IPV4.*

D1(config-if)#**ipv6 address fe80::d1:1 link-local***>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D1(config-if)#**ipv6 address 2001:db8:100:1010::2/64** *>> Asignación de direccionamiento a la Ethernet IPV6.*

D1(config-if)#**no shutdown** *>> Se enciende la interfaz.*

D1(config-if)#**exit** *>> Salir de la interfaz que se está configurando.*

Asignación de direccionamiento, segmento de red al prefijo **FE80** para **IPV6**, se habilita interfaz para cada Vlan creada antes (Vlan 100, 101, 102).

D1(config)#**interface vlan 100** *>>Ingresar a la Vlan.*

D1(config-if)#**ip address 10.0.100.1 255.255.255.0** *>> Asignación de direccionamiento a la Ethernet IPV4.*

D1(config-if)#**ipv6 address fe80::d1:2 link-local** *>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D1(config-if)#**ipv6 address 2001:db8:100:100::1/64** *>> Asignación de direccionamiento a la Ethernet IPV6.*

D1(config-if)#**no shutdown** *>> Se enciende la interfaz.*

D1(config-if)#**exit** *>> Salir de la interfaz que se está configurando.*

Se configura la interfaz Vlan 101 y 102, la descripción de cada una de las líneas es la misma del paso anterior Vlan 100.

D1(config)#**interface vlan 101**

D1(config-if)#**ip address 10.0.101.1 255.255.255.0** *>> Asignación del direccionamiento IP con su respectiva mascara de subred a la Vlan.*

D1(config-if)#**ipv6 address fe80::d1:3 link-local** *>> Activación de una porción de red estática al prefijo FE80 protocolo Ipv6.*

D1(config-if)#**ipv6 address 2001:db8:100:101::1/64***>> Asignación de la red estática.*

D1(config-if)#**no shutdown** *>> Se enciende la interfaz.*

D1(config-if)#**exit** *>> Salir de la interfaz que se está configurando.*

D1(config)#**interface vlan 102**

D1(config-if)#**ip address 10.0.102.1 255.255.255.0**

D1(config-if)#**ipv6 address fe80::d1:4 link-local**

D1(config-if)#**ipv6 address 2001:db8:100:102::1/64**

D1(config-if)#**no shutdown**

D1(config-if)#**exit**

Exclusión de direcciones IP en el DHCP

D1(config)#**ip dhcp excluded-address 10.0.101.1 10.0.101.109**

D1(config)#**ip dhcp excluded-address 10.0.101.141 10.0.101.254**

D1(config)#**ip dhcp excluded-address 10.0.102.1 10.0.102.109**

D1(config)#**ip dhcp excluded-address 10.0.102.141 10.0.102.254**

Creación de pool en cada Vlan.

D1(config)#**ip dhcp pool VLAN-*101*** *>> Ingreso a la Vlan-101 para asignación de pool de dirección por DHCP.*

D1(dhcp-config)#**network 10.0.101.0 255.255.255.0** *>> Asignación de IP.*

D1(dhcp-config)#**default-router 10.0.101.254** *>> Gateway default.*

D1(dhcp-config)#**exit** *>> Salir del modo configuración* DHCP pool VLAN-101.

D1(config)#**ip dhcp pool VLAN-102** *>> Ingreso a la Vlan-102 para asignación de pool de dirección por DHCP.*

D1(dhcp-config)#**network 10.0.102.0 255.255.255.0** *>> Asignación de IP al pool de la Vlan.*

D1(dhcp-config)#**default-router 10.0.102.254** *>> Gateway default.*

D1(dhcp-config)#**exit** *>> Salir del modo configuración DHCP pool VLAN-102.*

Se ingresa al rango de interfaces Ethernet 0/0-3 y la 3/0-3 y se inhabilitan

D1(config)#**interface range e0/0-3, e3/0-3** *>> Ingreso al rango de interfaces Ethernet o las Ethernet que se apagaran.*

D1(config-if-range)#**shutdown** *>> Comando para apagar las interfaces.*

D1(config-if-range)#**exit** *>> Salir de las interfaces Ethernet*.

D1(config)#

Configuración inicial **Switch D2:**

Switch>**enable** *>> Ingreso a modo privilegiado.*

Switch#**configure terminal** *>> Ingreso a modo configuración global.*

Switch(config)#**hostname D2** *>> darle nombre el Sswitch.*

D2(config)#**ip routing** *>> Habilitar enrutamiento IP en el Switch.*

D2(config)#**ipv6 unicast-routing** *>> Se habilita el IPV6 sobre el Switch.*

D2(config)#**no ip domain lookup** *>> Permite que el sistema indique que el comando que se está ingresando no es válido, de esta forma no se tiene que esperar un tiempo hasta que salga el mensaje se error de ingreso del comando.*

D2(config)#**line con 0** *>> Ingreso a la línea de consola 0.*

D2(config-line)#**exec-timeout 0 0** *>> Configuración de las excepciones de tiempo.*

D2(config-line)#**logging synchronous** *>> Evita que algún mensaje interrumpa la línea o comando ingresado.*

D2(config-line)#**exit** *>> Salir del modo configuración line con 0.*

Creación de VLAN 100, 101, 102, y 999 con sus respectivos nombres.

D2(config)#**vlan 100** *>> Ingreso de la Vlan a crear 100.*

D2(config-vlan)#**name Management** *>> Se nombra la Vlan Managment.*

D2(config-vlan)#**exit** *>> Salir de la configuración de la Vlan 100.*

D2(config)#**vlan 101** *>> Ingreso de la Vlan a crear 101.*

D2(config-vlan)#**name UserGroupA** *>> Se nombra la Vlan UserGroupA.*

D2(config-vlan)#**exit** *>> Salir de la configuración de la Vlan 101.*

D2(config)#**vlan 102** *>> Ingresar a la Vlan a crear 102.*

D2(config-vlan)#**name UserGroupB** *>> Se nombra la Vlan UserGroupB.*

D2(config-vlan)#**exit** *>> Salir de la configuración de la Vlan 102.*

D2(config)#**vlan 999** *>> Ingresar a la Vlan a crear 999.*

D2(config-vlan)#**name NATIVE** *>> Se nombra la Vlan NATIVE.*

D2(config-vlan)#**exit** *>> Salir de la configuración de la Vlan 99.*

Los comandos de configuración ingresados en R1, R2 y R3 ahora se repite en la interfaz e1/0

D2(config)#**interface e1/0** *>> En modo configuración global, se ingresa a la Interface Ethernet 1/0.*

D2(config-if)#**no switchport >>** *aporta a la interfaz capacidad de Capa 3. La dirección IP se encuentra en la misma subred que el Router predeterminado.*

D2(config-if)#**ip address 10.0.11.2 255.255.255.0** *>> Asignación del direccionamiento IP con su respectiva mascara de subred que tendrá la E1/0.*

D2(config-if)#**ipv6 address fe80::d1:1 link-local***>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D2(config-if)#**ipv6 address 2001:db8:100:1011::2/64** *>> Asignación de la red estática.*

D2(config-if)#**no shutdown** *>> Se enciende la interfaz.*

D2(config-if)#**exit** *>> Salir de la interfaz que se está configurando.*

D2(config-if)#**ip address 10.0.100.2 255.255.255.0** *>> Asignación de la red estática IPV4.*

D2(config-if)#**ipv6 address fe80::d2:2 link-local** *>> Activación de una porción de red estática al prefijo FE80 del protocolo Ipv6.*

D2(config-if)#**ipv6 address 2001:db8:100:100::2/64** *>> Asignación de la red estática.*

D2(config-if)#**no shutdown** *>> Se enciende la interfaz.*

D2(config-if)#**exit** *>> Salir de la interfaz que se está configurando.*

Direccionamiento IPV6 de las Vlan

D2(config)#**interface vlan 101**

D2(config-if)#**ip address 10.0.101.2 255.255.255.0**

D2(config-if)#**ipv6 address fe80::d2:3 link-local**

D2(config-if)#**ipv6 address 2001:db8:100:101::2/64**

D2(config-if)#**no shutdown**

D2(config-if)#**exit**

D2(config)# **interface vlan 102**

D2(config-if)#**ip address 10.0.102.2 255.255.255.0**

D2(config-if)#**ipv6 address fe80::d2:4 link-local**

D2(config-if)#**ipv6 address 2001:db8:100:102::2/64**

D2(config-if)#**no shutdown**

D2(config-if)#**exit**

Exclusión de direcciones IP en el DHCP

D2(config)#**ip dhcp excluded-address 10.0.101.1 10.0.101.209**

D2(config)#**ip dhcp excluded-address 10.0.101.241 10.0.101.254**

D2(config)#**ip dhcp excluded-address 10.0.102.1 10.0.102.209**

D2(config)#**ip dhcp excluded-address 10.0.102.241 10.0.102.254**

Con las líneas de comandos anteriores se excluyen las direcciones IP especificadas en cada línea para que no sean asignadas de forma automática

Creación de pool en cada Vlan.

D2(config)#**ip dhcp pool VLAN-101**

D2(dhcp-config)#**network 10.0.101.0 255.255.255.0**

D2(dhcp-config)#**default-router 10.0.101.254**

D2(dhcp-config)#**exit**

D2(config)#**ip dhcp pool VLAN-102**

D2(dhcp-config)#**network 10.0.102.0 255.255.255.0**

D2(dhcp-config)#**default-router 10.0.102.254**

D2(dhcp-config)#**exit**

D2(config)#**interface range e0/0-3, e3/0-3**

D2(config-if-range)#**shutdown**

D2(config-if-range)#**exit**

Configuración básica **Switch A1:**

Router(config)#**hostname A1** *>> Se nombra al Swicth como A1.*

A1(config)#**no ip domain lookup** *>> Permite que el sistema indique que el comando que se está ingresando no es válido, de esta forma no se tiene que esperar un tiempo hasta que salga el mensaje se error de ingreso del comando.*

A1(config)#**line con 0** *>> Ingreso al modo de configuración línea de consola 0.*

A1(config-line)#**exec-timeout 0 0** *>> Se indica que no habrá límite de tiempo por inactividad.*

A1(config-line)#**logging synchronous** *>> Evita que algún mensaje interrumpa la línea o comando ingresado.*

A1(config-line)#**exit** *>> Salir del modo consola.*

Creación de las VLAN 100, 101, 102, 999

A1(config)#**vlan 100** *>> Ingresar a la Vlan a crear.*

A1(config-vlan)#**name Management** *>> Se nombra la Vlan Managment.*

A1(config-vlan)#**exit** *>> Salir del modo configuración.*

A1(config)#**vlan 101**

A1(config-vlan)#**name UserGroupA**

A1(config-vlan)#**exit**

A1(config)#**vlan 102**

A1(config-vlan)#**name UserGroupB**

A1(config-vlan)#**exit**

A1(config)#**vlan 999**

A1(config-vlan)#**name NATIVE**

A1(config-vlan)#**exit**

Direccionamiento IPV6 para Vlan 100

A1(config)#**interface vlan 100**

A1(config-if)#**ip address 10.0.100.3 255.255.255.0**

A1(config-if)#**ipv6 address fe80::a1:1 link-local**

A1(config-if)#**ipv6 address 2001:db8:100:100::3/64**

A1(config-if)#**no shutdown**

A1(config-if)#**exit**

A1(config)#**interface range e1/2-3, e2/0-3, e3/0-3**

A1(config)#**shutdown**

A1(config)#**exit**

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

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

Las tareas de configuración son las siguientes:

Tabla 2: Configuración a aplicar en Switches -Parte 2

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

2.2	En todos los switches cambie la VLAN nativa en los enlaces troncales.	Use VLAN 999 como la VLAN nativa.
2.3	En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)	Use Rapid Spanning Tree (RSPT).
2.4	En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología. D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).	Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch.
2.5	En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.	Use los siguientes números de canales: • D1 a D2 – Port channel 12 • D1 a A1 – Port channel 1 • D2 a A1 – Port channel 2
2.6	En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.	Configure los puertos de acceso con la configuración de VLAN adecuada, como se muestra en el diagrama de topología. Los puertos de host deben pasar
		inmediatamente al estado de reenvío (forwarding).
2.7	Verifique los servicios DHCP IPv4.	PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

2.8	Verifique la conectividad de la LAN local	PC1 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC4: 10.0.100.6 PC2 debería hacer ping con éxito a: • D1: 10.0.102.1 • D2: 10.0.102.2 PC3 debería hacer ping con éxito a: • D1: 10.0.101.1 • D2: 10.0.101.2 PC4 debería hacer ping con éxito a: • D1: 10.0.100.1 • D2: 10.0.100.2 • PC1: 10.0.100.5

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

Figura 3: PC2 Cliente DHCP

Figura 4: PC3 Cliente DHCP

```
PC3> show ip

NAME        : PC3[1]
IP/MASK     : 10.0.101.110/24
GATEWAY     : 10.0.101.254
DNS         :
DHCP SERVER : 10.0.101.1
DHCP LEASE  : 86232, 86400/43200/75600
MAC         : 00:50:79:66:68:02
LPORT       : 10008
RHOST:PORT  : 127.0.0.1:10009
MTU:        : 1500

PC3> ip dhcp
DORA IP 10.0.101.110/24 GW 10.0.101.254

PC3>
```

Verificación de 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

Figura 5: Conectividad PC1

```
PC1> ping 10.0.100.1
84 bytes from 10.0.100.1 icmp_seq=1 ttl=255 time=24.845 ms
84 bytes from 10.0.100.1 icmp_seq=2 ttl=255 time=12.074 ms
84 bytes from 10.0.100.1 icmp_seq=3 ttl=255 time=6.254 ms
84 bytes from 10.0.100.1 icmp_seq=4 ttl=255 time=7.956 ms
84 bytes from 10.0.100.1 icmp_seq=5 ttl=255 time=8.706 ms

PC1> ping 10.0.100.2
84 bytes from 10.0.100.2 icmp_seq=1 ttl=255 time=26.202 ms
84 bytes from 10.0.100.2 icmp_seq=2 ttl=255 time=17.401 ms
84 bytes from 10.0.100.2 icmp_seq=3 ttl=255 time=18.798 ms
84 bytes from 10.0.100.2 icmp_seq=4 ttl=255 time=20.259 ms
84 bytes from 10.0.100.2 icmp_seq=5 ttl=255 time=23.045 ms

PC1> ping 10.0.100.6
84 bytes from 10.0.100.6 icmp_seq=1 ttl=64 time=21.384 ms
84 bytes from 10.0.100.6 icmp_seq=2 ttl=64 time=13.139 ms
84 bytes from 10.0.100.6 icmp_seq=3 ttl=64 time=16.456 ms
84 bytes from 10.0.100.6 icmp_seq=4 ttl=64 time=27.771 ms
84 bytes from 10.0.100.6 icmp_seq=5 ttl=64 time=18.756 ms
```

PC2 debería hacer ping con éxito a:

- D1: 10.0.102.1
- D2: 10.0.102.2

Figura 6: ping desde PC2

```
PC2> ping 10.0.102.1
84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=38.119 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=12.925 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=17.104 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=20.351 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=23.185 ms

PC2> ping 10.0.102.2
84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=14.236 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=4.638 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=6.096 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=12.384 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=7.646 ms
```

PC3 debería hacer ping con éxito a:

- D1: 10.0.101.1
- D2: 10.0.101.2

Figura 7: Conectividad PC3

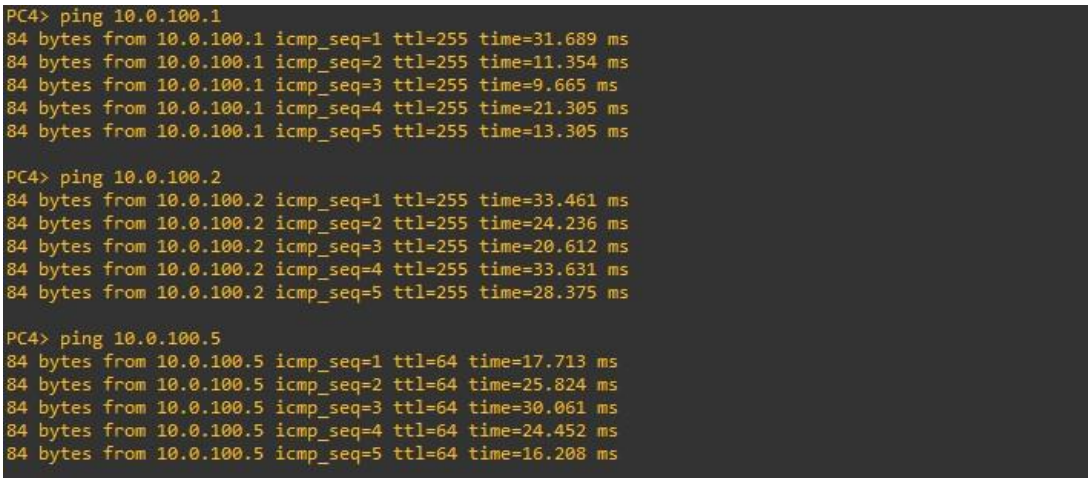
```
PC3> ping 10.0.101.1
84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=33.724 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=21.641 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=24.729 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=25.503 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=31.104 ms

PC3> ping 10.0.101.2
84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=41.112 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=22.212 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=15.939 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=37.948 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=21.162 ms
```

PC4 debería hacer ping con éxito a:

- D1: 10.0.100.1
- D2: 10.0.100.2
- PC1: 10.0.100.5

Figura 8: Conectividad PC4



Configuración de protocolo IEEE 802.1Q con el fin de establecer como troncales las conexiones entre Switches.

Configuración **Switch D1**:

D1(config)#**interface range e1/1-3, e2/0**>> *Ingresar al rango de interfaces Ethernet.*

D1(config-if-range)#**switchport trunk encapsulation dot1q**>> *Se genera el enlace troncal sobre el SW con encapsulación dot1q.*

D1(config-if-range)#**switchport mode trunk**>> *Enlace troncal del SW D1 para interfaces Ethernet.*

D1(config-if-range)#**switchport trunk native vlan 999**>> *Como se habilito la encapsulación con protocolo dot1q se debe indicar la Vlan nativa 999.*

D1(config-if-range)#**channel-group 12 mode active**>>*En modo configuración se activa el grupo de canal 12.*

D1(config-if-range)#**no shutdown**>> *Subir interfaz.*

D1(config-if-range)#exit >> *Salir de la interfaz.*

D1(config)#

D1(config)#**interface range e2/1-2**>> *Ingresar al rango de interfaces Ethernet.*

D1(config-if-range)#**switchport trunk encapsulation dot1q**>> *encapsulación troncal de la interfaz el estándar IEEE 802.1Q.*

D1(config-if-range)#**switchport mode trunk**>> *configuración modo troncal IEEE 802.1Q.*

D1(config-if-range)#**switchport trunk native vlan 999**>> *Vlan nativa.*

D1(config-if-range)#**channel-group 1 mode active**>> *En modo configuración se activa el grupo de canal 1, de D1 a A1.*

D1(config-if-range)#**no shutdown**>> *activar configuración.*

D1(config-if-range)#**exit** >> *salir del interfaz.*

D1(config)#**spanning-tree mode rapid-pvst**>> *Configuración más rápida el PVST.*

D1(config)#**spanning-tree vlan 100,102 root primary**>> *Asignación de prioridad en el Sw para el puente raíz que se designa como primario.*

D1(config)#**spanning-tree vlan 101 root secondary**>> *Asignación de prioridad en el Sw para un segundo puente raíz.*

D1(config)#**interface e2/3**>> *Ingresar al rango de interfaz Ethernet2/3.*

D1(config-if)#**switchport mode access** >> *puerto interface g2/3 de acceso.*

D1(config-if)#**switchport access vlan 100**>> *Fuerza la creación de una VLAN si es que aún no existe en el switch.*

D1(config-if)#**spanning-tree portfast** *>> Habilitación del PortFast global se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.*

D1(config-if)#**no shutdown** *>> Se sube la Vlan.*

D1(config-if)#**exit** *>> salir del interfaz.*

D1(config)#**end***>> salir de modo configuración.*

Configuración **Switch D2:**

D2(config)#**interface range e1/1-3, e2/0***>> rango de interfaces Ethernet.*

D2(config-if-range)#**switchport trunk encapsulation dot1q***>> encapsulación troncal de la interfaz el estándar IEEE 802.1Q.*

D2(config-if-range)#**switchport mode trunk***>> configuración modo troncal IEEE 802.1Q.*

D2(config-if-range)#**switchport trunk native vlan 999***>> Vlan nativa.*

D2(config-if-range)#**channel-group 12 mode active***>>En modo configuración se activa el grupo de canal 12, para D1 a D2.*

D2(config-if-range)#**no shutdown***>> se sube interfaces modo troncal con Vlan nativa.*

D2(config-if-range)#**exit** *>> salir de las interfaces.*

D2(config)#**interface range e2/1-2***>> rango de interfaces Ethernet 2/1-2.*

D2(config-if-range)#**switchport trunk encapsulation dot1q***>> encapsulación troncal de la interfaz el estándar IEEE 802.1Q.*

D2(config-if-range)#**switchport mode trunk***>> configuración modo troncal IEEE 802.1Q.*

D2(config-if-range)#**switchport trunk native vlan 999**>> *configuración Vlan nativa.*

D2(config-if-range)#**channel-group 2 mode active**>>*En modo configuración se activa el grupo de canal 2, para D1 a A1.*

D2(config-if-range)#**no shutdown** >>*Se sube la configuración realizada.*

D2(config-if-range)#**exit** >> *salir del interfaz.*

D2(config)#**spanning-tree mode rapid-pvst** >> *Configuración más rápida el PVST.*

D2(config)#**spanning-tree vlan 101 root primary** >> *Asignación de prioridad en el Sw para el puente raíz que se designa como primario.*

D2(config)#**spanning-tree vlan 100,102 root secondary**>> *Asignación de prioridad en el Sw para un segundo puente raíz.*

D2(config)#**interface e2/3** >> *ingreso a la interfaz Ethernet2/3.*

D2(config-if)#**switchport mode access**>>*puerto interfaz Ethernet2/3 de modo de acceso.*

D2(config-if)#**switchport access vlan 102**>>*Puerto de acceso Vlan102, por lo que otro dispositivo se conecte a este puerto debe tener esta misma Vlan..*

D2(config-if)#**spanning-tree portfast**>> *se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.*

D2(config-if)#**no shutdown**>> *Se sube el puerto en acceso con Vlan 102.*

D2(config-if)#**exit** >> *salir del interfaz.*

D2(config)#**end** >> *salir de modo configuración.*

Configuración **Switch A1:**

A1(config)#**spanning-tree mode rapid-pvst**>> *Configuración más rápida el PVST.*

A1(config)#**interface range e0/0-1**>> *ingreso al rango de las interfaces Ethernet0/0-*

1.

A1(config-if-range)#**switchport mode trunk**>> *configuración modo troncal IEEE 802.1Q.*

A1(config-if-range)#**switchport trunk native vlan 999**>> *configuración Vlan nativa.*

A1(config-if-range)#**channel-group 1 mode active**>>*En modo configuración se activa el grupo de canal 1.*

A1(config-if-range)#**no shutdown** >>*Se sube la configuración realizada.*

A1(config-if-range)#**exit**>> *salgo de la interfaces Etherne0/0-1.*

A1(config)#**interface range e0/2-3**>> *ingreso al rango de interfaces Ethernet0/2-3.*

A1(config-if-range)#**switchport mode trunk**>>*puertos de interfaces Etherne0/2-3 de modo de troncal.*

A1(config-if-range)#**switchport trunk native vlan 999**>>*Puerto troncal con la Vlan 999.*

A1(config-if-range)#**channel-group 2 mode active**>>*En modo configuración se activa el grupo de canal 2.*

A1(config-if-range)#**no shutdown**>>*Se sube la configuración realizada.*

A1(config-if-range)#**exit**>> *salgo de las interfaces Etherne0/2-3.*

A1(config)#**interface e1/0**>> *ingreso al interfaz Ethernet1/0.*

A1(config-if)#**switchport mode access**>>*puerto de interfaz E1/0 de modo de acceso.*

A1(config-if)#**switchport access vlan 101**>>*Puerto acceso con la Vlan 101.*

A1(config-if)#**spanning-tree portfast**>> *se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.*

A1(config-if)#**no shutdown**>>*Se sube la configuración realizada.*

A1(config-if)#**exit**>> *salgo de la interfaz Etherne1/0.*

A1(config)#**interface e1/1**>> *ingreso al interfaz Ethernet1/1.*

A1(config-if)#**switchport mode access**>>*puerto de interfaz E1/1 de modo de acceso.*

A1(config-if)#**switchport access vlan 100**>>*Puerto acceso con la Vlan 100.*

A1(config-if)#**spanning-tree portfast**>> *se usa en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente.*

A1(config-if)#**no shutdown**>>*Se sube la configuración realizada.*

A1(config-if)#**exit**>> *salgo de la interfaz Etherne1/1.*

A1(config)#**end**>> *salgo del modo configuración.*

A1#

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 3: Configuración a aplicar en red - ISP - Parte 3

Tarea#	Tarea	Especificación

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

		provista por BGP. Deshabilite las publicaciones OSPFv3 en: D1: todas las interfaces excepto G1/0/11 D2: todas las interfaces excepto G1/0/11
3.3	En R2 en la “Red ISP”, configure MP- BGP	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: Una ruta estática predeterminada IPv4. Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: La red Loopback 0 IPv4 (/32). La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: La red Loopback 0 Ipv4 (/128). La ruta por defecto (::/0).

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

Router R1: Configuración OSPFv2, OSPFv3.

Se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Routerid 0.0.4.1

R1#**conf terminal** *>> configuración global.*

R1(config)#**router ospf 4** *>> Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

R1(config-router)#**router-id 0.0.4.1** *>> Marcación o identificación del router ID OSPF.*

R1(config-router)#**network 10.0.10.0 0.0.0.255 area 0** *>> Asignación de la red que será ruta del área 0.*

R1(config-router)#**network 10.0.13.0 0.0.0.255 area 0** *>> Asignación de la red que será ruta del área 0.*

R1(config-router)#**default-information originate** *>> Informar una ruta predeterminada en el área.*

R1(config-router)#**exit** *>> Salir de la configuración del router-id 0.0.4.1.*

R1(config)#**ipv6 router ospf 6** *>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

R1(config-rtr)#**router-id 0.0.6.1** *>> Marcación o identificación del router ID OSPF.*

R1(config-rtr)#**default-information originate** *>> Informar una ruta predeterminada en el área.*

R1(config-rtr)#**exit** *>> Salir de la configuración del router-id 0.0.6.1.*

R1(config)#**interface e0/1** *>> En modo configuración global se ingresa en la interface Ethernet0/1.*

R1(config-if)#**ipv6 ospf 6 area *0*** *>> Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R1(config-if)#**exit** *>> Salir de la interfaz E0/1.*

R1(config)#**interface s2/0** *>> En modo configuración global se ingresa en la interfaz S2/0.*

R1(config-if)#**ipv6 ospf 6 area 0** *>> Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R1(config-if)#**exit** *>> Salir de la interfaz S2/0.*

R1(config)#**ip route 10.0.0.0 255.0.0.0 *null0*** *>> Se configura la tabla de rutas en la que se indica que la Ip Route 10.0.0.0 con Submask 255.0.0.0 apunta a la interfaz null0 que es una interfaz virtual.*

R1(config)#**ipv6 route 2001:db8:100::/48 null0** *>> Configuración ruta estática a la interfaz Null 0 para IPv6.*

R1(config)#**router bgp 300** *>> se usa BGP ASN 300.*

R1(config-router)#**bgp router-id 1.1.1.1** *>> Se configura el ID del router en bgp.*

R1(config-router)#**neighbor 209.165.200.226 remote-as 500** *>> Se habilita una relación de vecino IPv4 con R2 en ASN 500.*

R1(config-router)#**neighbor 2001:db8:200::2 remote-as 500***>> Se habilita una relación de vecino IPv6 con R2 en ASN 500.*

R1(config-router)#**address-family ipv4 unicast** *>> Especifica la familia de direcciones, evita intercambio de direcciones IPv4 unicast de forma predeterminada.*

R1(config-router-af)#**neighbor 209.165.200.226 activate***>> Activación de la dirección de vecino en IPv4.*

R1(config-router-af)#**no neighbor 2001:db8:200::2 activate***>> Excluye la dirección de vecino de IPv6 en IPv4.*

R1(config-router-af)#**network 10.0.0.0 mask 255.0.0.0** *>> Anunciado de la red 10.0.0.0/8. En IPv6 address family.*

R1(config-router-af)#**exit-address-family***>> Se sale de la sub interfaz de direcciones vecino IPv4.*

R1(config-router)#**address-family ipv6 unicast***>> Se ingresa de la sub interfaz de direcciones vecino IPv6.*

R1(config-router-af)#**no neighbor 209.165.200.226 activate***>> Excluye la dirección de vecino de IPv4 en IPv6.*

R1(config-router-af)#**neighbor 2001:db8:200::2 activate**>> *Activación de la dirección de vecino en IPv6.*

R1(config-router-af)#**network 2001:db8:100::/48**>> *Dirección de la red Loopback (/48).*

R1(config-router-af)#**exit-address-family**>> *Se sale de la sub interfaz de direcciones vecino IPv6.*

R1(config-router)#**fin** >> *Salir del modo configuración.*

Configuración OSPFv2, OSPFv3 **Router R2:**.

En el R2 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con router-id 2.2.2.2

R2#**conf terminal** >> *Configuración global.*

R2(config)#**ip route 0.0.0.0 0.0.0.0 loopback 0** >> *Configuración rutas estáticas de la interfaz Loopback 0 para IPV4 con ruta por defecto (0.0.0.0/0).*

R2(config)#**ipv6 route ::/0 loopback 0**>> *Configuración rutas estáticas de la interfaz Loopback 0 para IPV6 con ruta por defecto (::/0).*

R2(config)#**router bgp 500** >> *Se usa BGP ASN 500.*

R2(config-router)#**bgp router-id 2.2.2.2**>> *Se usa BGP ASN 500 router-id 2.2.2.2.*

R2(config-router)#**neighbor 209.165.200.225 remote-as 300**>> *Se habilita una relación de vecino IPv4 con R1 en ASN 300.*

R2(config-router)#**neighbor 2001:db8:200::1 remote-as 300**>> *Se habilita una relación de vecino IPv6 con R1 en ASN 300.*

R2(config-router)#**address-family ipv4**>> *Se habilita una relación de vecino IPv4 con R1 en ASN 300 con dirección de familia.*

R2(config-router-af)#**neighbor 209.165.200.225 activate**>> *Activación de la dirección de vecino en IPv4.*

R2(config-router-af)#**no neighbor 2001:db8:200::1 activate**>> *Excluye la dirección de vecino de IPv6 en IPv4.*

R2(config-router-af)#**network 2.2.2.2 mask 255.255.255.255** >> *Router-id 2.2.2.2.*

R2(config-router-af)#**network 0.0.0.0** >> *Ruta por defecto (0.0.0.0/0).*

R2(config-router-af)#**exit-address-family**>> *Se sale de la sub interfaz de direcciones vecino IPv4.*

R2(config-router)#**address-family ipv6**>> *Ingreso de la sub interfaz de direcciones vecino IPv6.*

R2(config-router-af)#**no neighbor 209.165.200.225 activate**>> *Excluye la dirección de vecino de IPv4 en IPv6.*

R2(config-router-af)#**neighbor 2001:db8:200::1 activate**>> *Activación de la dirección de vecino en IPv6.*

R2(config-router-af)#**network 2001:db8:2222::/128** >> *Dirección de la red Loopback (/128).*

R2(config-router-af)#**network ::/0** >> *Ruta por defecto (::/0).*

R2(config-router-af)#**exit-address-family**>> *Se sale de la sub interfaz de direcciones vecino IPv6.*

R2(config-router)#**end** >> *Salir de modo configuración.*

Router R3: Configuración OSPFv2, OSPFv3.

En el R3 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.3

R3#**confi terminal**>> *Configuración global.*

R3(config)#**router ospf 4**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

R3(config-router)#**router-id 0.0.4.3**>> *Marcación o identificación del Router ID OSPF.*

R3(config-router)#**network 10.0.11.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

R3(config-router)#**network 10.0.13.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

R3(config-router)#**exit**>> *Salir de la configuración Router-id 0.0.4.3.*

R3(config)#**ipv6 router ospf 6**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

R3(config-rtr)#**router-id 0.0.6.3**>> *Marcación o identificación del Router ID OSPF*

R3(config-rtr)#**exit**>> *Salir de la configuración Router-id 0.0.6.3*

R3(config)#**interface e0/0**>> *En modo configuración global se ingresa en la interfaz Ethernet0/0.*

R3(config-if)#**ipv6 ospf 6 area 0**>> *Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R3(config-if)#**exit**>> *Salir de la interfaz Ethernet0/0.*

R3(config)#**interface s2/0**>> *En modo configuración global se ingresa en la interfaz S2/0.*

R3(config-if)#**ipv6 ospf 6 area 0**>> *Se habilita el OSPF en el proceso 6 área 0 para publicar rutas.*

R3(config-if)#**exit**>> *Salir de la interfaz S2/0.*

R3(config)#**end**>> *Salir de la configuración.*

Switch D1: Configuración OSPFv2, OSPFv3.

En el D1 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.131.

D1#**conf terminal** *>> Configuración global.*

D1(config)#**router ospf 4**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

D1(config-router)#**router-id 0.0.4.131**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

D1(config-router)#**network 10.0.100.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D1(config-router)#**network 10.0.101.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D1(config-router)#**network 10.0.102.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D1(config-router)#**network 10.0.10.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D1(config-router)#**passive-interface default** *>> Deshabilito las publicaciones OSPFv2, todas las interfaces.*

D1(config-router)#**no passive-interface e1/0**>> *No deshabilito las publicaciones de la interfaz Etherne1/0.*

D1(config-router)#**exit** *>> Salgo de la configuración Router OSPF 4.*

D1(config)#**ipv6 router ospf 6** *>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-rtr)#**router-id 0.0.6.131** *>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-rtr)#**passive-interface default** *>> Deshabilito las publicaciones OSPFv3, todas las interfaces.*

D1(config-rtr)#**no passive-interface e1/0** *>> No deshabilito las publicaciones de la interfaz Etherne1/0.*

D1(config-rtr)#**exit** *>> Salgo de la configuración de router OSPF 6.*

D1(config)#**interface e1/0** *>> Ingreso al interfaz Ethernet1/0.*

D1(config-if)#**ipv6 ospf 6 area 0** *>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit** *>> Salgo de la configuración de router.*

D1(config)#**interface vlan 100** *>> Ingresando a la Vlan.*

D1(config-if)#**ipv6 ospf 6 area 0** *>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit***>> Salir de la configuración vlan 100.*

D1(config)#**interface vlan 101** *>> Ingresando a la Vlan.*

D1(config-if)#**ipv6 ospf 6 area 0***>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit***>> Salir de la configuración vlan 101.*

D1(config)#**interface vlan 102***>> Ingresando a la Vlan.*

D1(config-if)#**ipv6 ospf 6 area 0***>> Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D1(config-if)#**exit***>> Salir de la configuración vlan 102.*

D1(config)**#end**>> *Salir del modo configuración.*

D1#

Configuración OSPFv2, OSPFv3 **Switch D2**:

En el D2 se configura el single- área OSPFv2, OSPFv3 con ID 4, ID 6, en área 0 con Router-id 0.0.4.132.

D2#**conf terminal** >> *Configuración global.*

D2(config)#**router ospf 4**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

D2(config-router)#**router-id 0.0.4.132**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 4.*

D2(config-router)#**network 10.0.100.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D2(config-router)#**network 10.0.101.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D2(config-router)#**network 10.0.102.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D2(config-router)#**network 10.0.11.0 0.0.0.255 area 0**>> *Asignación de la red que será ruta del área 0.*

D2(config-router)#**passive-interface default**>> *Deshabilito las publicaciones OSPFv2, todas las interfaces.*

D2(config-router)#**no passive-interface e1/0**>> *No deshabilito las publicaciones de la interfaz Ethernet1/0.*

D2(config-router)#**exit**>> *Salgo de la configuración.*

D2(config)#**ipv6 router ospf 6**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-router)#**router-id 0.0.6.132**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-router)#**passive-interface default**>> *Deshabilito las publicaciones OSPFv3, todas las interfaces.*

D2(config-router)#**no passive-interface e1/0**>> *No deshabilito las publicaciones de la interfaz Etherne1/0.*

D2(config-router)#**exit** >> *Salgo de la configuración de router.*

D2(config)#**interface e1/0** >> *Ingreso al interfaz Ethernet1/0.*

D2(config-if)#**ipv6 ospf 6 area 0**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-if)#**exit**>> *Salgo de la interfaz Ethernet1/0.*

D2(config)#**interface vlan 100** >> *Ingresando a la Vlan.*

D2(config-if)#ipv6 ospf 6 area 0>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config-if)#**exit** >> *Salir de la configuración vlan 100.*

D2(config)#**interface vlan 101**>> Ingresando a la Vlan.

D2(config)#**ipv6 ospf 6 area 0**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config)#**exit**>> *Salir de la configuración vlan 101.*

D2(config)#**interface vlan 102**>> Ingresando a la Vlan.

D2(config)#**ipv6 ospf 6 area 0**>> *Habilitación del enrutamiento por medio del OSPF en el proceso 6.*

D2(config)#**exit** >> *Salir de la configuración vlan 102.*

Verificación de configuración en ejecución:

Figura 9 R1 # show run | sección ^ router ospf en R1

Figura 10 R3 # show run | sección ^ router ospf en R3

Figura 11 D2s # show run | sección ^ router ospf en D1

Figura 12 D2 # show run | sección ^ router ospf en D2

Figura 13 R1# show run | section ^ipv6 router en A1

```
R1#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.1
 default-information originate
R1#show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se2/0        6     0               6          64    P2P   1/1
Gi1/0        6     0               5          1     DR    0/0
R1#
```

Figura 14 R3# show run | section ^ipv6 router en R3

```
R3#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.3
R3#
```

Figura 15 R3# show ipv6 ospf interface brief en R3

```
R3#show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se2/0        6     0               6          64    P2P   1/1
Gi1/0        6     0               5          1     DR    0/0
R3#
```

Figura 16 D1# show run | section ^ipv6 router en D1

```
D1#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
 no passive-interface Ethernet1/0
D1#
```

Figura 17 D1# show ipv6 ospf interface brief en D1

```
D1#show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Vl102        6     0               25         1     DR    0/0
Vl101        6     0               24         1     DR    0/0
Vl100        6     0               23         1     DR    0/0
Et1/0        6     0               21         10    DOWN  0/0
D1#
```

Figura 18 D2# show run | section ^ipv6 router en D12

```
D2#show run | section ^ipv6 router
ipv6 router ospf 6
 router-id 0.0.6.131
 passive-interface default
 no passive-interface Ethernet1/0
D2#
```

Figura 19 D2# show ipv6 ospf interface brief en D2

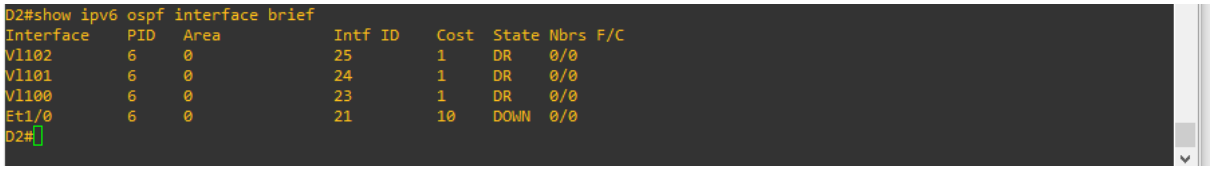
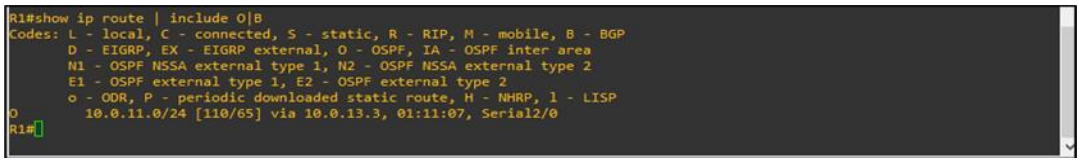


Figura 20 R2# show run | section router bgp en R2

Figura 21 R2# show run | include route en R2

Figura 22 R1# show run | section bgp en R1

Figura 23 R1# show ip route | include O|B en R1



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

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

Las tareas de configuración son las siguientes:

Tabla 4: Configurar la Redundancia del Primer Salto - Parte 4

Tarea#	Tarea	Especificación
4.1	En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 F0/1.	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 F0/1 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 y una para la IP SLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la IP SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

4.2	En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 F0/0.	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 F0/0 cada 5 segundos. Programe la SLA para una implementación inmediata sin tiempo de finalización. Cree una IP SLA objeto para la IP SLA 4 and one for IP SLA 6. • Use el número de rastreo **4** para la IP SLA 4. • Use el número de rastreo **6** para la SLA 6. Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15
		segundos.

4.3	En D1 configure HSRPv2.	D1 es el Router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP versión 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 versión 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 **Switch D1**:

D1#**configure terminal** *>> Se ingresa al modo configuración.*

D1(config)#**ip sla 4** *>> Se crea SLA número 4 para IPv4*.
D1(config-ip-sla)#**icmp-echo 10.0.10.1***>> Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV4.*

D1(config-ip-sla-echo)#**frequency 5***>> IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.*

D1(config-ip-sla-echo)#**exit***>> Salir de la configuración ip sla 4.*

D1(config)#**ip sla 6** *>> Se crea SLA número 4 para IPv6.*

D1(config-ip-sla)#**icmp-echo 2001:db8:100:1010::1** *>> Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV6.*

D1(config-ip-sla-echo)#**frequency 5** *>> IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.*

D1(config-ip-sla-echo)#**exit** *>> Salir de la configuración IP sla 6.*

D1(config)#**ip sla schedule 4 life forever start-time now** *>> Es la IP SLA objeto para la IP SLA 4.*

D1(config)#**ip sla schedule 6 life forever start-time now** *>> Es la IP SLA objeto para la IP SLA 6.*

D1(config)#**track 4 ip sla 4** *>> El número 4 es de rastreo para la IP SLA 4.*
D1(config-track)#**delay down 10 up 15** *>> IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos en IPV4.*

D1(config-track)#**exit** *>> Salir de la configuración IP sla 4.*

D1(config)#**track 6 ip sla 6** *>> El número 6 es de rastreo para la IP SLA 4.*
D1(config-track)#**delay down 10 up 15** *>> IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos en IPV6.*

D1(config-track)#**exit** *>> Salir de la configuración ip sla 6.*

D1 es el Router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150, se Configura HSRP versión 2 en el grupo 104, 114 y 124 para IPV4, los grupos 106, 116 y 126 para IPV6:

D1(config)#**interface vlan 100** *>> Ingreso a la interfaz Vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106.*

D1(config-if)#**standby version 2** *>> Configuración de HSRP versión 2.*

D1(config-if)#**standby 104 ip 10.0.100.254** *>> Se asigna dirección IP virtual (10.0.100.254) en IPv4 HSRP grupo 104.*

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** *>> Rastrea el objeto 4 y decremente en 60.*

D1(config-if)#**standby 106 ipv6 autoconfig** *>> La dirección IP virtual como automática.*

D1(config-if)#**standby 106 priority 150** *>> Prioridad del grupo en 150.*

D1(config-if)#**standby 106 preempt** *>> Se habilita la preferencia.*

D1(config-if)#**standby 106 track 6 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D1(config-if)#**exit** *>> Salir de la configuración Vlan 100.*

D1(config)#**interface vlan 101** *>> Ingreso a la interfaz Vlan 101, para luego configurar IPv4 HSRP grupo 114 e IPV6 HSRP grupo 116.*

D1(config-if)#**standby version 2** *>> Configuración de HSRP versión 2.*

D1(config-if)#**standby 114 ip 10.0.101.254** *>> Se asigna dirección IP virtual (10.0.101.254) en IPv4 HSRP grupo 114.*

D1(config-if)#**standby 114 preempt** *>> Se habilita la preferencia.*

D1(config-if)#**standby 114 track 4 decrement 60** *>> Rastrea el objeto 4 y decremente en 60.*

D1(config-if)#**standby 116 ipv6 autoconfig** *>> La dirección IP virtual como automática.*

D1(config-if)#**standby 116 preempt** *>> Se habilita la preferencia.*

D1(config-if)#**standby 116 track 6 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D1(config-if)#**exit** *>> Salir de la configuración Vlan 101.*

D1(config)#**interface vlan 102** *>> Ingreso a la interfaz Vlan 102, para luego configurar IPv4 HSRP grupo 124 e IPV6 HSRP grupo 126.*

D1(config-if)#**standby version 2** *>> Configuración de HSRP versión 2.*

D1(config-if)#**standby 124 ip 10.0.102.254** *>> Se asigna dirección IP virtual (10.0.102.254) en IPv4 HSRP grupo 124.*

D1(config-if)#**standby 124 priority 150** *>> Se establece la prioridad del grupo en 150.*

D1(config-if)#**standby 124 preempt** *>> Se habilita la preferencia.*

D1(config-if)#**standby 124 track 4 decrement 60** *>> Rastrea el objeto 4 y decremente en 60.*

D1(config-if)#**standby 126 ipv6 autoconfig** *>> La dirección IP virtual como automática.*

D1(config-if)#**standby 126 priority 150** *>> Se establece la prioridad del grupo en 150.*

D1(config-if)#**standby 126 preempt** *>> Se habilita la preferencia*

D1(config-if)#**standby 126 track 6 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D1(config-if)#**exit** *>> Salir de la configuración Vlan 102.*

D1(config)#**end** *>> Salir del modo configuración.*

D1#

Switch D2: Configuración IP SLAs, HSRPv2.

Se crean las dos IP SLAs, número 4 para IPv4 y número 6 para Ipv6:

D2#**configure terminal** *>> Ingresa a modo configuración.*

D2(config)#**ip sla 4** *>> Se crea SLA número 4 para IPv4.*

D2(config-ip-sla)#**icmp-echo 10.0.11.1** *>> Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV4.*

D2(config-ip-sla-echo)#**frequency 5** *>> IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.*

D2(config-ip-sla-echo)#**exit** *>> Salir de la configuración ip sla 4.*

D2(config)#**ip sla 6** *>> Se crea SLA número 4 para IPv6.*

D2(config-ip-sla)#**icmp-echo 2001:db8:100:1011::1** *>> Verificar la conectividad de extremo a extremo entre dispositivos a través de la red (D1 a R1) en IPV6.*

D2(config-ip-sla-echo)#**frequency 5** *>> IP SLAs probarán la disponibilidad de la interfaz R1 F0/1 cada 5 segundos.*

D2(config-ip-sla-echo)#**exit** *>> Salir de la configuración IP sla 6.*

D2(config)#**ip sla schedule 4 life forever start-time now** *>> Es la IP SLA objeto para la IP SLA.*

D2(config)#**ip sla schedule 6 life forever start-time now** *>> Es la IP SLA objeto para la IP SLA.*

D2(config)#**track 4 ip sla 4** *>> El número 4 es de rastreo para la IP SLA 4.*

D2(config-track)#**delay down 10 up 15** *>> IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos en IPV4.*

D2(config-track)#**exit** *>>Salir de la configuración IP SLA 4.*

D2(config)#**interface vlan 100** *>> Ingreso a la interfaz Vlan 100, para luego configurar IPv4 HSRP grupo 104 e IPV6 HSRP grupo 106.*

D2(config-if)#**standby version 2** *>> Configuración de HSRP versión 2.*

D2(config-if)#**standby 104 ip 10.0.100.254** *>> Se establece la prioridad del grupo en 150.*

D2(config-if)#**standby 104 preempt** *>> Se habilita la preferencia.*

D2(config-if)#**standby 104 track 4 decrement 60** *>> Rastrea el objeto 4 y decremente en 60.*

D2(config-if)#**standby 106 ipv6 autoconfig** *>> La dirección IP virtual como automática.*

D2(config-if)#**standby 106 preempt** *>> Se habilita la preferencia.*

D2(config-if)#**standby 106 track 6 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D2(config-if)#**exit** *>> Salir de la configuración Vlan 100.*

D2(config)#**interface vlan 101** *>> Ingreso a la interfaz Vlan 101, para luego configurar IPv4 HSRP grupo 114 e IPV6 HSRP grupo 116.*

D2(config-if)#**standby version 2** *>> Configuración de HSRP versión 2*

D2(config-if)#**standby 114 ip 10.0.101.254** *>> Se asigna dirección IP virtual (10.0.101.254) en IPv4 HSRP grupo 114.*

D2(config-if)#**standby 114 priority 150** *>> Prioridad del grupo en 150.*

D2(config-if)#**standby 114 preempt** *>> Se habilita la preferencia.*

D2(config-if)#**standby 114 track 4 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D2(config-if)#**standby 116 ipv6 autoconfig** *>> La dirección IP virtual como automática.*

D2(config-if)#**standby 116 priority 150** *>> Prioridad del grupo en 150.*

D2(config-if)#**standby 116 preempt** *>> Se habilita la preferencia*. D2(config-if)#**standby 116 track 6 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D2(config-if)#**exit** *>> Salir de la configuración Vlan 101.*

D2(config)#**interface vlan 102** *>> Ingreso a la interfaz Vlan 102, para luego configurar IPv4 HSRP grupo 124 e IPV6 HSRP grupo 126.*

D2(config-if)#**standby version 2** *>> Configuración de HSRP versión 2.*

D2(config-if)#**standby 124 ip 10.0.102.254** *>> Se asigna dirección IP virtual (10.0.102.254) en IPv4 HSRP grupo 124.*

D2(config-if)#**standby 124 preempt** *>> Se habilita la preferencia.*

D2(config-if)#**standby 124 track 4 decrement 60** *>> Rastrea el objeto 4 y decremente en 60.*

D2(config-if)#**standby 126 ipv6 autoconfig** *>> La dirección IP virtual como automática.*

D2(config-if)#**standby 126 preempt** *>> Se habilita la preferencia*

D2(config-if)#**standby 126 track 6 decrement 60** *>> Rastrea el objeto 6 y decremente en 60.*

D2(config-if)#**exit** *>> Salir de la configuración Vlan 102.*

D2(config)#**end** *>> Salir del modo configuración.*

D2#

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 5: Seguridad – Parte 5

Tarea#	Tarea	Especifica ción
5.1	En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.	Contraseña: **cisco12345cisco**
5.2	En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encripción SCRYPT.	Detalles de la cuenta encriptada SCRYPT: • Nombre de usuario Local: **sadmin** • Nivel de privilegio **15** • Contraseña: **cisco12345cisco**
5.3	En todos los dispositivos (excepto R2), habilite AAA.	Habilite AAA.

5.4	En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.	Especificaciones del servidor RADIUS.: • Dirección IP del servidor RADIUS es 10.0.100.6. • Puertos UDP del servidor RADIUS son 1812 y 1813. • Contraseña: **$trongPass**
5.5	En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA	Especificaciones de autenticación AAA: • Use la lista de métodos por defecto • Valide contra el grupo de servidores RADIUS • De lo contrario, utilice la base de datos local.
5.6	Verifique el servicio AAA en todos los dispositivos (except R2).	Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: **raduser** y la contraseña: **upass123**.

En todos los dispositivos, se protege el EXEC privilegiado usando el algoritmo de encriptación SCRYPT, adicional se crea un usuario local con la misma encriptación, con usuario **sadmin** y contraseña **cisco12345cisco**. Para habilita Autenticación, autorización, contabilidad se realiza en R1, R3, D1, D2 y A1.

Configuración SCRYPT, AAA. **Route R1**:

R1# **configure terminal** >> *Ingresa a modo configuración.*

R1(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** >> *Se hace uso del algoritmo de encriptación SCRYPT.*

R1(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** >> *Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

R1(config)#**aaa new-model** >> *Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

R1(config)#**radius server RADIUS** >> *Se ingresa al interfaz del servidor Radius.*

R1(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** >> *Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

R1(config-radius-server)#**key $trongPass** >> *Asignación de la contraseña.*

R1(config-radius-server)#**exit** >> *Salir de la interfaz del servidor Radius.*

R1(config)#**aaa authentication login default group radius local** >> *Se realiza autenticación por defecto.*

R1(config)#**end** >> *Salir del modo configuración.*

R1#

Route R2: Configuración SCRYPT.

R2#**configure terminal** >> *Ingresa a modo configuración.*

R2(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** >> *Se hace uso del algoritmo de encriptación SCRYPT.*

R2(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** >> *Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

R2(config)#**end** >> *Salir del modo configuración.*

R2#

Route R3: Configuración SCRYPT, AAA.

R3#**configure terminal** >> *Ingresa a modo configuración.*

R3(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *>> Se hace uso del algoritmo de encriptación SCRYPT.*

R3(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *>> Por medio de algoritmo de encripción SCRYPT se crea usuario local (sadmin).*

R3(config)#**aaa new-model** *>> Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

R3(config)#**radius server RADIUS** *>> Se ingresa al interfaz del servidor Radius.*

R3(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *>> Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

R3(config-radius-server)# **key $trongPass** *>> Asignación de la contraseña.*

R3(config-radius-server)#**exit** *>> Salir de la interfaz del servidor Radius.*

R3(config)#**aaa authentication login default group radius local** *>> Se realiza autenticación por defecto.*

R3(config)#**end** *>> Salir del modo configuración.*

R3#

Switch D1: Configuración SCRYPT, AAA.

D1#**configure terminal** *>> Ingresa a modo configuración.*

D1(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *>> Se hace uso del algoritmo de encriptación SCRYPT.*

D1(config)# **username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *>> Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

D1(config)#**aaa new-model** *>> Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

D1(config)#**radius server RADIUS** *>> Se ingresa al interfaz del servidor Radius.*

D1(config-radius-server)# **address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *>> Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

D1(config-radius-server)#**key $trongPass** *>> Asignación de la contraseña.*

D1(config-radius-server)#**exit**

D1(config)#**aaa authentication login default group radius local** *>> Se realiza autenticación por defecto.*

D1(config)#**end** *>> Salir del modo configuración.*

D1#

Switch D2: Configuración SCRYPT, AAA.

D2#**configure terminal** *>> Ingresa a modo configuración.*

D2(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *>> Se hace uso del algoritmo de encriptación SCRYPT.*

D2(config)# **username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *>> Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

D2(config)#**aaa new-model** *>> Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

D2(config)#**radius server RADIUS** *>> Se ingresa al interfaz del servidor Radius.*

D2(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *>> Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

D2(config-radius-server)#**key $trongPass** *>> Asignación de la contraseña.*

D2(config-radius-server)#**exit** *>> Salir de la interfaz del servidor Radius.*

D2(config)#**aaa authentication login default group radius local** *>> Se realiza autenticación por defecto.*

D2(config)#**end** *>> Salir del modo configuración.*

D2#

Configuración SCRYPT, AAA. **Switch A1**:

A1#**configure terminal** *>> Ingresa a modo configuración.*

A1(config)#**enable algorithm-type SCRYPT secret cisco12345cisco** *>> Se hace uso del algoritmo de encriptación SCRYPT.*

A1(config)#**username sadmin privilege 15 algorithm-type SCRYPT secret cisco12345cisco** *>> Por medio de algoritmo de encriptación SCRYPT se crea usuario local (sadmin).*

A1(config)#**aaa new-model** *>> Se habilita Autenticación, autorización, contabilidad (AAA), permite el acceso a solo autorizados.*

A1(config)#**radius server RADIUS** *>> Se ingresa al interfaz del servidor Radius.*

A1(config-radius-server)#**address ipv4 10.0.100.6 auth-port 1812 acct-port 1813** *>> Se asigna IP del servidor Radius y los puertos UPD (1812 y 1813).*

A1(config-radius-server)#**key $trongPass** *>> Asignación de la contraseña.*

A1(config-radius-server)#**exit** *>> Salir de la interfaz del servidor Radius.*

A1(config)#**aaa authentication login default group radius local** *>> Se realiza autenticación por defecto.*

A1(config)#**end** *>> Salir del modo configuración.*

A1#

Figura 24 D1# show run | section ip sla en D1

Parte 6: Configure las funciones de Administración de Red.

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

Tabla 6: Configure las funciones de Administración de Red – Parte 6

Tarea#	Tarea	Especificación
6.1	En todos los dispositivos, configure el reloj local a la hora UTC actual.	Configure el reloj local a la hora UTC actual.
6.2	Configure R2 como un NTP maestro.	Configurar R2 como NTP maestro en el nivel de estrato 3.
6.3	Configure NTP en R1, R3, D1, D2, y A1	Configure NTP de la siguiente manera: • R1 debe sincronizar con R2. • R3, D1 y A1 para sincronizar la hora con R1. D2 para sincronizar la hora con R3.
6.4	Configure Syslog en todos los dispositivos excepto R2	Syslogs deben enviarse a la PC1 en 10.0.100.5 en el nivel WARNING.
6.5	Configure SNMPv2c en todos los dispositivos excepto R2	Especificaciones de SNMPv2: • Únicamente se usará SNMP en modo lectura (Read-Only). • Límite 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*.

En todos los dispositivos se configura el reloj local UTC, para el R2 se configura el NTP maestro en estrato 3.

Actualización: De reloj en todos los dispositivos.

clock timezone UTC -5

Router R2: Configuración NTP Máster 3.

R2(config)#**ntp master 3** *>> Se configura el NTP maestro en estrato 3.*
R2(config)#**end** *>> Salir del modo configuración.*

Se realiza configuración de NTP y SNMPv2 en R1, R3, D1, D2 y A1.

Router R1: Configuración NTP y SNMP.

R1#**configure terminal** *>> Ingresa a modo configuración*

R1(config)#**ntp server 2.2.2.2** *>> Se configura NTP para sincronizar con R2 por medio de Loopback 0.*

R1(config)#**logging trap warning** *>> Se configura Syslog en nivel WARNING.*

R1(config)#**logging host 10.0.100.5** *>> Se configura Syslog a la PC1 10.0.100.5.*

R1(config)#**logging on** *>> Se enciende configuración Syslog.*

R1(config)#**ip access-list standard SNMP-NMS** *>> Configuración de SNMPv2c en modo estándar (lectura).*

R1(config-std-nacl)#**permit host 10.0.100.5** *>> Límite de acceso SNMP a la PC1.*

R1(config-std-nacl)#**exit** *>> Salir de la configuración SNMPv2c.*

R1(config)#**snmp-server contact Cisco Milton** *>> Se configura el valor de contacto SNMP con mi nombre.*

R1(config)#**snmp-server community ENCORSA ro SNMP-NMS** *>> Se establece community string en ENCORSA.*

R1(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** *>> Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

R1(config)#**snmp-server ifindex persist** *>> Identifica cada interfaz para la identificación SNMP de esta interfaz.*

R1(config)#**snmp-server enable traps bgp** *>> Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).*

R1(config)#**snmp-server enable traps config** *>> Envía notificaciones de configuración.*

R1(config)#**snmp-server enable traps ospf** *>> Envía notificaciones de OSPF.*

R1(config)#**end** *>> Salir del modo configuración.*

R1#

Router R3: Configuración NTP y SNMP.

R3#**configure terminal** *>> Ingresa a modo configuración*

R3(config)#**ntp server 10.0.10.1** *>> Se configura NTP para sincronizar hora con R1.*

R3(config)#**logging trap warning** *>> Se configura Syslog en nivel WARNING.*

R3(config)#**logging host 10.0.100.5** *>> Se configura Syslog a la PC1 10.0.100.5.*

R3(config)#**logging on** *>> Se enciende configuración Syslog.*

R3(config)#**ip access-list standard SNMP-NMS** *>> Configuración de SNMPv2c en modo estándar (lectura).*

R3(config-std-nacl)#**permit host 10.0.100.5** *>> Límite de acceso SNMP a la PC1.*

R3(config-std-nacl)#**exit** *>> Salir de la configuración SNMPv2c.*

R3(config)#**snmp-server contact Cisco Milton** *>> Se configura el valor de contacto SNMP con mi nombre.*

R3(config)#**snmp-server community ENCORSA ro SNMP-NMS** *>> Se establece community string en ENCORSA.*

R3(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** *>> Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

R3(config)#**snmp-server ifindex persist** *>> Identifica cada interfaz para la identificación SNMP de esta interfaz.*

R3(config)#**snmp-server enable traps config** *>> Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).*

R3(config)#**snmp-server enable traps ospf** *>> Envía notificaciones de configuración.*

R3(config)#**end** *>> Salir del modo configuración.*

R3#

Switch D1: Configuración NTP y SNMP.

D1(config)#**ntp server 10.0.10.1** *>> Se configura NTP para sincronizar hora con R1.*

D1(config)#**logging trap warning** *>> Se configura Syslog en nivel WARNING.*

D1(config)#**logging host 10.0.100.5** *>> Se configura Syslog a la PC1 10.0.100.5.*

D1(config)#**logging on** *>> Se enciende configuración Syslog.*

D1(config)#**ip access-list standard SNMP-NMS** *>> Configuración de SNMPv2c en modo estándar (lectura).*

D1(config-std-nacl)#**permit host 10.0.100.5** *>> Límite de acceso SNMP a la PC1.*

D1(config-std-nacl)#**exit** *>> Salir de la configuración SNMPv2c.*

D1(config)#**snmp-server contact Cisco Student** *>> Se configura el valor de contacto SNMP con mi nombre.*

D1(config)#**snmp-server community ENCORSA ro SNMP-NMS** *>> Se establece community string en ENCORSA.*

D1(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** *>> Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

D1(config)#**snmp-server ifindex persist** *>> Identifica cada interfaz para la identificación SNMP de esta interfaz.*

D1(config)#**snmp-server enable traps** *>> Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).*

D1(config)#**snmp-server enable traps config** *>> Envía notificaciones de configuración.*

D1(config)#**snmp-server enable traps ospf** *>> Envía notificaciones de OSPF*

D1(config)#**end** *>> Salir del modo configuración.*

D1#

Switch D2: Configuración NTP y SNMP.

D2(config)#**ntp server 10.0.10.1** *>> Se configura NTP para sincronizar hora con R1.*

D2(config)#**logging trap warning** *>> Se configura Syslog en nivel WARNING.*

D2(config)#**logging host 10.0.100.5** *>> Se configura Syslog a la PC1 10.0.100.5.*

D2(config)#**logging on** *>> Se enciende configuración Syslog.*

D2(config)#**ip access-list standard SNMP-NMS** *>> Configuración de SNMPv2c en modo estándar (lectura).*

D2(config-std-nacl)#**permit host 10.0.100.5** *>> Límite de acceso SNMP a la PC1.*

D2(config-std-nacl)#**exit** *>> Salir de la configuración SNMPv2c.*

D2(config)#**snmp-server contact Cisco Milton** *>> Se configura el valor de contacto SNMP con mi nombre.*

D2(config)#**snmp-server community ENCORSA ro SNMP-NMS** *>> Se establece community string en ENCORSA.*

D2(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** *>> Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

D2(config)#**snmp-server enable traps config** *>> Envía notificaciones de configuración.*

D2(config)#**snmp-server enable traps ospf** *>> Envía notificaciones de OSPF.*

D2(config)#**end** *>> salir del modo configuración.*

Switch A1: Configuración NTP y SNMP.

A1(config)#**ntp server 10.0.10.1** *>> Se configura NTP para sincronizar hora con R1.*

A1(config)#**logging trap warning** *>> Se configura Syslog en nivel WARNING.*

A1(config)#**logging host 10.0.100.5** *>> Se configura Syslog a la PC1 10.0.100.5.*

A1(config)#**logging on** *>> Se enciende configuración Syslog.*

A1(config)#**ip access-list standard SNMP-NMS** *>> Configuración de SNMPv2c en modo estándar (lectura).*

A1(config-std-nacl)#**permit host 10.0.100.5** *>> Límite de acceso SNMP a la PC1.*

A1(config-std-nacl)#**exit** >> *Salir de la configuración SNMPv2c.*

A1(config)#**snmp-server contact Cisco Milton** >> *Se configura el valor de contacto SNMP con mi nombre.*

A1(config)#**snmp-server community ENCORSA ro SNMP-NMS** >> *Se establece community string en ENCORSA.*

A1(config)#**snmp-server host 10.0.100.5 version 2c ENCORSA** >> *Acceso SNMP a la dirección IP de la PC1 con community string en ENCORSA.*

A1(config)#**snmp-server ifindex persist** >> *Identifica cada interfaz para la identificación SNMP de esta interfaz.*

A1(config)#**snmp-server enable traps** >> *Envía notificaciones del cambio de estado del protocolo de la puerta de enlace de frontera (BGP).*

A1(config)#**snmp-server enable traps ospf** >> *Envía notificaciones de configuración.*

A1(config)#**end** >> *Salir del modo configuración.*

A1#

CONCLUSIONES

Con la creciente evolución de las tecnologías, las redes se vuelven cada vez más importante e imprescindible, la evolución y mejoras continuas que se deben realizar sobre estas tanto en su parte técnica como en la seguridad apunta a que quien tenga una certificación CCNP abre sus puertas y gana una falibilidad en su trabajo.

El simulador GNS3 fue muy importante para el desarrollo de la actividad, siempre y cuando se presentó falencias al momento de configurar los Switchs, no soportaba la capa 3 del modelo OSI; inicialmente se instaló la imagen IOU L2 Versión 15.1a, como alternativa se instala la imagen IOU L2 versión 15.2d, logrando que los Switchs contara con características de capa 2 y capa 3.

Para el protocolo OSPFv2 y v3, duranta la simulación presentó inconveniente de no tomar los comandos de configuración, para la solución, se anticipa con el comando ipv6 unicast-routing, logrando así la actualización de las tablas de enrutamiento.

Al momento de configurar las interfaces de los dispositivos en modo troncal, se evidencio la importancia del comando switchport trunk encapsulation dot1q, sin esta línea de comando, los dispositivos no permitían conectividad.

Para el escenario realizado muestra la importancia del protocolo de autenticación, autorización y auditoría (AAA), proporciona el marco de trabajo necesario para habilitar la seguridad de acceso, como la política de seguridad de red logra la implementación de un sistema de auditoría que registre quién inició sesión y cuándo, y qué hizo mientras permaneció conectado. Es de gran importancia los protocolos Remote Authentication Dial-In User Service (RADIUS) porque permite el acceso solo a personas autorizados.

BIBLIOGRAFÍA

ARIGANELLO, Ernesto. "Redes Cisco CCNP a fondo". {En línea}. {13 septiembre de 2021} disponible en: (https://books.google.com.co/books?id=ZofDwAAQBAJ&lpg=PA796&dq=importancia%20del%20ccnp%20cisco&pg=PP1#v= onepage&q&f=false. Obtenido de Con qué elementos se desarrolla el CCNP en la ingeniería de redes: https://formatalent.com/con-que-elementos-se-desarrolla-elccnp-en-la-ingenieria-de-redes/).

MARCO, Maria. "Escaneando la Informática". {En línea}. {16 septiembre de 2021} disponible en: (https://books.google.com.co/books?id=svpzjkMpdiUC&lpg=PA99&dq=importancia%20del%20ccnp%20cisco&pg=PP1#v=onepage&q=importancia%20del%20ccnp%20cisco&f=false).

RICO, Alberto. "CCNA, la certificación de Cisco (cómo conseguirla)". {En línea}. {16 septiembre de 2021} disponible en: (https://www.ambit-bst.com/blog/ccna-lacertificaci%C3%B3n-de-cisco-c%C3%B3mo-conseguirla).

ROMERO, Christian. "Establecer IOU L2 e IOU L3 en GNS3". {En línea}. {16 Octubre de 2021} disponible en: (www.youtube.com/watch?v=ZXfseiLKIgI).

ROMERO, Christian. "Setup IOU L2 and IOU L3 on GNS3 VM 2.2.14". {En línea}. {16 septiembre de 2021} disponible en: (https://www.youtube.com/watch?v=ivxMfrcMuAk).