DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ALEJANDRO SANCHEZ ORJUELA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ALEJANDRO SANCHEZ ORJUELA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN:

Presidente del Jurado

Jurado

Jurado

Tuluá, Valle del Cauca, 29 de noviembre de 2021

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

LAN: Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

WAN: Wide Area Network (“Red de Área Amplia”). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial.

NAT: (Network Address Translation ó Traducción de Dirección de Red) es un mecanismo utilizado por routers y equipos para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

VLAN: (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

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).

SERVIDOR: Un servidor es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc.

RESUMEN

El presente trabajo escrito, se trata de la solución de 1 único escenario con 6 partes a desarrollar, en la primera se construye la red, se configuran los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces en la segunda parte, se configura la capa 2 de red y el soporte de host, para la tercera parte se configuran los protocolos de enrutamiento, posteriormente en la cuarta parte, se configura la redundancia del primer salto, seguidamente la seguridad en la quinta parte y finalmente en la parte 6 se configurar algunas características de administración de red.

Los protocolos de enrutamiento utilizados en este trabajo final de CISCO CCNP, son, por ejemplo, BGP, que no es más que un protocolo de enrutamiento entre sistemas autónomos, es muy utilizado por proveedores de servicios de internet.

En la parte 2 se emplea LACP para aumentar la capacidad de conmutación, ya que, como lo sabemos, gracias a la agregación de enlaces, podemos además dar redundancia, en el caso de que uno de los enlaces falle, pues tanto el software como la electrónica utilizada en los equipos de comunicación está orientada a cubrir esta necesidad de soporte a fallos.

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

ABSTRACT

The present written work is about the solution of a single scenario with 6 parts to develop, in the first the network is built, the basic settings of each device are configured and the addressing of the interfaces in the second part, the network layer 2 and host support, for the third part the routing protocols are configured, later in the fourth part, the redundancy of the first hop is configured, then the security in the fifth part and finally in part 6 it is configured some network management features.

The routing protocols used in this final CISCO CCNP work are, for example, BGP, which is nothing more than a routing protocol between autonomous systems, it is widely used by internet service providers.

In part 2 LACP is used to increase the switching capacity, since, as we know, thanks to the aggregation of links, we can also provide redundancy, in the event that one of the links fails, since both the software and the electronics used in communication equipment are aimed at meeting this need for fault support.

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

INTRODUCCIÓN

El presente trabajo se refiere al desarrollo o solución de un escenario en el cual, primero construimos la red física, luego configuramos el enrutamiento, que logre hacer que los dispositivos todos se puedan comunicar, seguidamente, se configura la redundancia del último salto con HSRP, cuando todo lo anterior se encuentra configurado, le damos seguridad de acceso a los dispositivos y por último configuramos lo necesario para poder administrar los equipos desplegados.

Este escenario fue construido en GNS3, siguiendo lo solicitado en la primera parte, en la cual se solicita mediante una tabla de direccionamiento, asignar direcciones tanto IP como IPV6, seguidamente, en la capa de red, es donde implementamos, como requerimiento de la parte 2, enlaces troncales, asignamos la VLAN nativa 999, se implementa el spanning tree, supremamente importante en la capa 2 para evitar bucles, para este caso se empleó el rapid stp o RSTP, se fortalecieron los enlaces entre switches principales y de distribución con LACP. En la parte 3 se configuran los protocolos de enrutamiento OSPF y BGP en routers como en switches.

El desarrollo de la cuarta parte, trata de la redundancia del último salto, que permite utilizar redundancia, y así evitar que la red caiga, por algún fallo en un gateway, para esto, se requiere comprobar la disponibilidad de las salidas con IP SLA, luego con el protocolo HSRP, podemos tener esas redundancias necesarias para poder hacer la conmutación en caso de fallos. En la quinta parte realizamos las configuraciones de seguridad, que nos permitirán acceder a los dispositivos, ya sea autenticándonos localmente como a través de RADIUS. Por último, en la parte 6 configuramos las funciones de administración de red, muy necesarias, ellas son, NTP o network time protocol, éste, entrega la hora a los sistemas administrados, seguidamente configuramos el los mensajes syslog, que nos entregan información valiosa cada vez que ocurra una configuración nueva, un fallo o cualquier otro evento, quedará registrado. Ya para finalizar, configuramos el SNMP, en todos los dispositivos para poder administrarlos a través de Software diseñado para tal fin como Nagios, ManageEngine, por mencionar algunos.

ESCENARIO PROPUESTO

Figura 1. Ilustración escenario propuesto

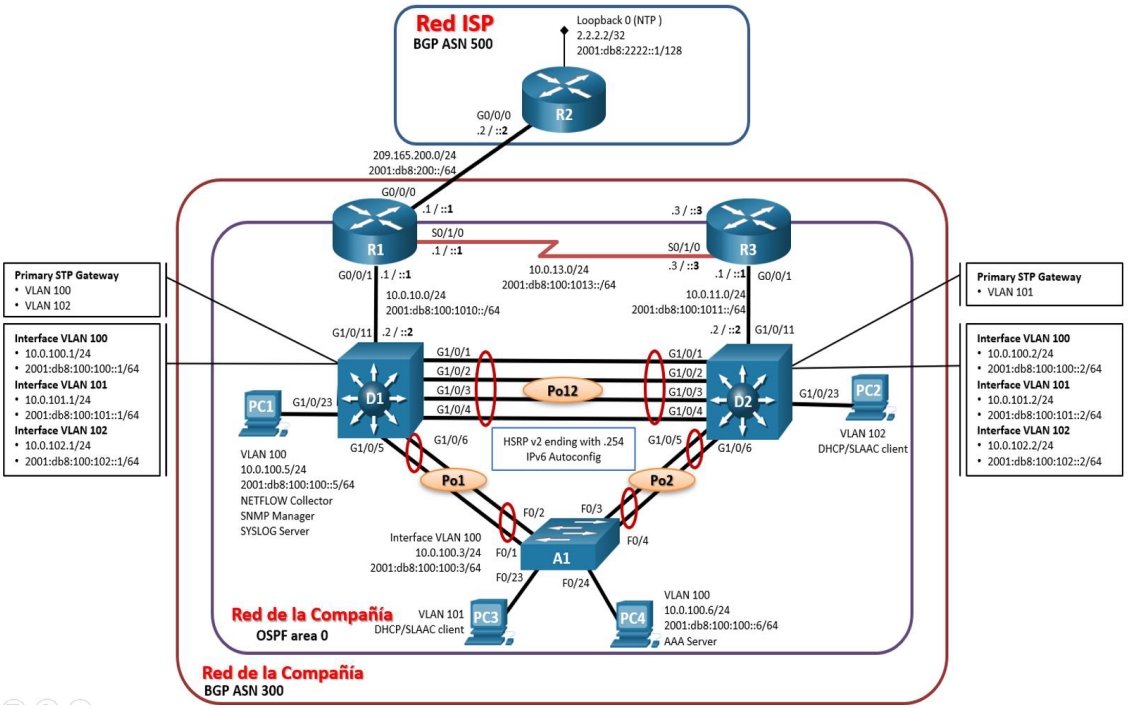


Tabla 1: Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

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

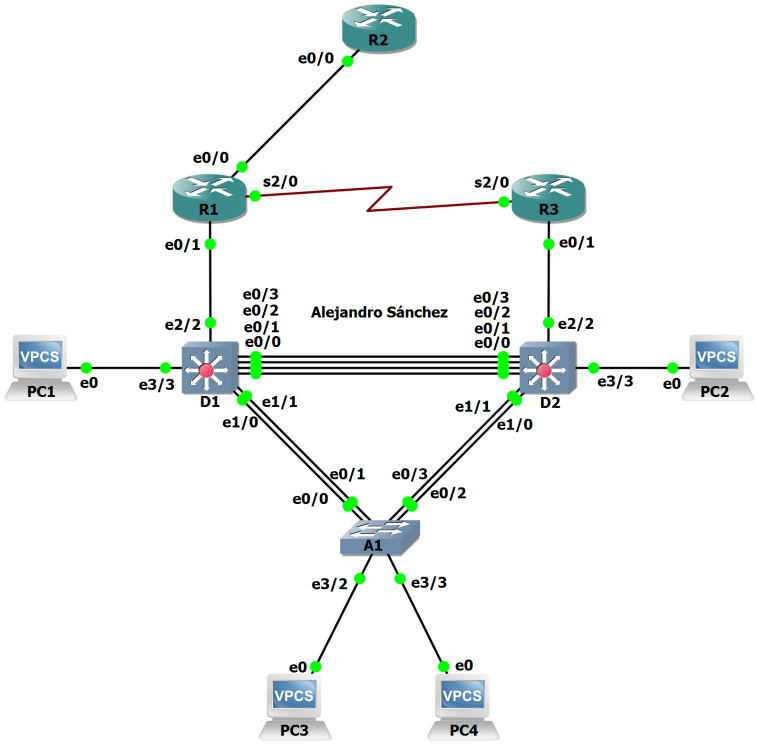
Procederemos entonces a realizar las configuraciones respectivas, teniendo en cuenta que hemos cambiado el nombre de las interfaces ya que lo desarrollamos en GNS3, pero la disposición de los routers y switches es exactamente la misma.

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

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

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

Figura 2. Conexión entre dispositivos



Paso 2: Configurar los parámetros básicos para cada dispositivo.

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

Configuración R1

Router> enable ingreso al modo EXEC privilegiado
Router#configure terminal entra al modo de configuración global
Router(config)#hostname R1 configuración del nombre del host
R1(config)#ipv6 unicast-routing habilita enrutamiento con ipv6
R1(config)#no ip domain lookup desactiva la traducción de nombres
R1(config)#banner motd # R1, ENCOR Skills Assessment, Scenario 1 # banner
R1(config)#line con 0 configuración de línea de consola
R1(config-line)# exec-timeout 0 0 desconexión por inactividad
R1(config-line)# logging synchronous sincroniza logs
R1(config-line)# exit salida de la configuración de la línea de consola
R1(config)#interface e0/0 entrada en la configuración de la interfaz
R1(config-if)# ip address 209.165.200.225 255.255.255.224 configuración ipv4
R1(config-if)# ipv6 address fe80::1:1 link-local configura el enlace local ipv6
R1(config-if)# ipv6 address 2001:db8:200::1/64 configura ipv6
R1(config-if)# no shutdown enciende la interfaz
R1(config-if)# exit salida de la configuración de la interfaz
R1(config)#interface e0/1 entrada en la configuración de la interfaz
R1(config-if)# ip address 10.0.10.1 255.255.255.0 configuración de ipv4
R1(config-if)# ipv6 address fe80::1:2 link-local configuración de enlace local ipv6
R1(config-if)# ipv6 address 2001:db8:100:1010::1/64 configuración de ipv6
R1(config-if)# no shutdown enciende la interfaz
R1(config-if)# exit salida de la configuración de la interfaz
R1(config)#interface s2/0 entrada en la configuración de la interfaz
R1(config-if)# ip address 10.0.13.1 255.255.255.0 configuración ipv4

R1(config-if)# ipv6 address fe80::1:3 link-local configuración enlace local ipv6
R1(config-if)# ipv6 address 2001:db8:100:1013::1/64 configuración ipv6
R1(config-if)# no shutdown enciende la interfaz
R1(config-if)# exit salida de la configuración de la interfaz
R1(config)#end sale al modo EXEC privilegiado
R1#copy running-config startup-config graba la configuración en la flash

Configuración R2

Router> enable ingreso al modo EXEC privilegiado
Router#configure terminal entra al modo de configuración global
Router(config)#hostname R2 configuración del nombre del host
R2(config)#ipv6 unicast-routing habilita el ipv6
R2(config)#no ip domain lookup desactiva la traducción de nombres
R2(config)#banner motd # R2, ENCOR Skills Assessment, Scenario 1 # banner
R2(config)#line con 0 configura la línea de consola
R2(config-line)# exec-timeout 0 0 desconexión por inactividad
R2(config-line)# logging synchronous sincroniza logs
R2(config-line)# exit salida de la configuración de la línea de consola
R2(config)#interface e0/0 entrada en la configuración de la interfaz
R2(config-if)# ip address 209.165.200.226 255.255.255.224 configuración ipv4
R2(config-if)# ipv6 address fe80::2:1 link-local configuración de enlace local ipv6
R2(config-if)# ipv6 address 2001:db8:200::2/64 configuración ipv6
R2(config-if)# no shutdown encendido de la interfaz
R2(config-if)# exit salida de la configuración de la interfaz
R2(config)#interface Loopback 0 configuración de interfaz virtual Loopback0
R2(config-if)# ip address 2.2.2.2 255.255.255.255 configuración ipv4
R2(config-if)# ipv6 address fe80::2:3 link-local configuración de enlace local ipv6
R2(config-if)# ipv6 address 2001:db8:2222::1/128 configuración ipv6
R2(config-if)# no shutdown encendido de la interfaz
R2(config-if)# exit salida de la configuración de la interfaz

R2(config)#end sale al modo EXEC privilegiado
R2#copy running-config startup-config guarda la configuración en la flash

Configuración R3

Router> enable ingreso al modo EXEC privilegiado
Router#configure terminal entra al modo de configuración global
Router(config)#hostname R3 configuración del nombre del host
R3(config)#ipv6 unicast-routing habilita enrutamiento con ipv6
R3(config)#no ip domain lookup desactiva la traducción de nombres
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 # banner
R3(config)#line con 0 configuración de línea de consola
R3(config-line)# exec-timeout 0 0 desconexión por inactividad
R3(config-line)# logging synchronous sincroniza logs
R3(config-line)# exit salida de la configuración de la línea de consola
R3(config)#interface e0/1
R3(config-if)# ip address 10.0.11.1 255.255.255.0 configuración ipv4
R3(config-if)# ipv6 address fe80::3:2 link-local configuración de enlace local ipv6
R3(config-if)# ipv6 address 2001:db8:100:1011::1/64 configuración ipv6
R3(config-if)# no shutdown encendido de la interfaz
R3(config-if)# exit salida de la configuración de la interfaz
R3(config)#interface s2/0 entrada en la configuración de la interfaz
R3(config-if)# ip address 10.0.13.3 255.255.255.0 configuración ipv4
R3(config-if)# ipv6 address fe80::3:3 link-local configuración de enlace local ipv6
R3(config-if)# ipv6 address 2001:db8:100:1010::2/64 configuración ipv6
R3(config-if)# no shutdown encendido de la interfaz
R3(config-if)# exit salida de la configuración de la interfaz
R3(config)#end sale al modo EXEC privilegiado
R3#copy running-config startup-config guarda la configuración en la flash

Configuración D1

Switch>enable ingreso al modo EXEC privilegiado
Switch#configure terminal entra al modo de configuración global
Switch(config)#hostname D1 configuración nombre del host
D1(config)#ip routing habilita el enrutamiento en el switch
D1(config)#ipv6 unicast-routing habilita el enrutamiento ipv6 en el switch
D1(config)#no ip domain lookup desactiva la traducción de nombres
D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 # banner
D1(config)#line con 0 configuración de línea de consola
D1(config-line)# exec-timeout 0 0 desconexión por inactividad
D1(config-line)# logging synchronous sincroniza logs
D1(config-line)# exit salida de la configuración de la línea de consola
D1(config)#vlan 100 configuración de vlan 100
D1(config-vlan)# name Management nombramiento de la vlan
D1(config-vlan)# exit salida de la configuración de la vlan
D1(config)#vlan 101 configuración de vlan 101
D1(config-vlan)# name UserGroupA nombramiento de la vlan
D1(config-vlan)# exit salida de la configuración de la vlan
D1(config)#vlan 102 configuración de vlan 102
D1(config-vlan)# name UserGroupB nombramiento de la vlan
D1(config-vlan)# exit salida de la configuración de la vlan
D1(config)#vlan 999 configuración vlan 999
D1(config-vlan)# name NATIVE nombramiento de la vlan
D1(config-vlan)# exit salida de la configuración de la vlan
D1(config)#interface e2/2 entrada en la configuración de la interfaz
D1(config-if)# no switchport habilitación como puerto de router
D1(config-if)# ip address 10.0.10.2 255.255.255.0 asignación de dirección ip
D1(config-if)# ipv6 address fe80::d1:1 link-local configuración de link local
D1(config-if)# ipv6 address 2001:db8:100:1010::2/64 configuración de ipv6
D1(config-if)# no shutdown encendido de la interfaz
D1(config-if)# exit salida de la interfaz

D1(config)#interface vlan 100 entrada en la configuración de interfaz de vlan 100

D1(config-if)# ip address 10.0.100.1 255.255.255.0 asignación de IP en vlan 100

D1(config-if)# ipv6 address fe80::d1:2 link-local configuración de link local

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

D1(config-if)# no shutdown encendido de la interfaz

D1(config-if)# exit salida de interfaz vlan

D1(config)#interface vlan 101 entrada en la interfaz vlan 101

D1(config-if)# ip address 10.0.101.1 255.255.255.0 asignación de IP en vlan 101

D1(config-if)# ipv6 address fe80::d1:3 link-local configuración de link local

D1(config-if)# ipv6 address 2001:db8:100:101::1/64 configuración de ipv6

D1(config-if)# no shutdown encendido de la interfaz

D1(config-if)# exit salida de la interfaz

D1(config)#interface vlan 102 entrada en la interfaz vlan 102

D1(config-if)# ip address 10.0.102.1 255.255.255.0 asignación de IP en vlan 102

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

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

D1(config-if)# no shutdown encendido de la interfaz

D1(config-if)# exit salida de la interfaz

D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109 exclusión ip del pool dhcp

D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254 exclusión ip del pool dhcp

D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109 exclusión ip del pool dhcp

D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254 exclusión ip del pool dhcp

D1(config)#ip dhcp pool VLAN-101 configuración del pool dhcp en la vlan 101

D1(dhcp-config)# network 10.0.101.0 255.255.255.0 configuración red del pool

D1(dhcp-config)# default-router 10.0.101.254 configuración de gateway del pool

D1(dhcp-config)# exit salida de la configuración del pool

D1(config)#ip dhcp pool VLAN-102 configuración del pool dhcp en la vlan 101

D1(dhcp-config)# network 10.0.102.0 255.255.255.0 configuración red del pool

D1(dhcp-config)# default-router 10.0.102.254 configuración de gateway del pool

D1(dhcp-config)# exit salida de la configuración del pool

D1(config)#interface range e0/0-3, e1/0-3, e2/0-1, e2/3, e3/0-3 entrada en un rango de interfaces

D1(config-if-range)# shutdown apagado de interfaces

D1(config-if-range)# exit salida del rango de interfaces

D1(config)#end sale al modo EXEC privilegiado

D1#copy running-config startup-config grabación de la configuración en la flash

Configuración D2

Switch>enable ingreso al modo EXEC privilegiado

Switch#configure terminal entra al modo de configuración global

Switch(config)#hostname D2 configuración del nombre del host

D2(config)#ip routing habilita el enrutamiento en el switch

D2(config)#ipv6 unicast-routing habilita el enrutamiento ipv6 en el switch

D2(config)#no ip domain lookup desactiva la traducción de nombres

D2(config)#banner motd # D2, ENCOR Skills Assessment, Scenario 1 # banner

D2(config)#line con 0 configuración de línea de consola

D2(config-line)# exec-timeout 0 0 desconexión por inactividad

D2(config-line)# logging synchronous sincroniza logs

D2(config-line)# exit salida de la configuración de la línea de consola

D2(config)#vlan 100 configuración de vlan 100

D2(config-vlan)# name Management nombramiento de la vlan

D2(config-vlan)# exit salida de la configuración de la vlan

D2(config)#vlan 101 configuración de vlan 101

D2(config-vlan)# name UserGroupA nombramiento de la vlan

D2(config-vlan)# exit salida de la configuración de la vlan

D2(config)#vlan 102 configuración de vlan 102

D2(config-vlan)# name UserGroupB nombramiento de la vlan

D2(config-vlan)# exit salida de la configuración de la vlan

D2(config)#vlan 999 configuración vlan 999

D2(config-vlan)# name NATIVE nombramiento de la vlan

D2(config-vlan)# exit salida de la configuración de la vlan

D2(config)#interface e2/2 entrada en la configuración de la interfaz

D2(config-if)# no switchport habilitación como puerto de router

D2(config-if)# ip address 10.0.11.2 255.255.255.0 asignación de dirección ip

D2(config-if)# ipv6 address fe80::d1:1 link-local configuración de link local

D2(config-if)# ipv6 address 2001:db8:100:1011::2/64 configuración de ipv6

D2(config-if)# no shutdown encendido de la interfaz

D2(config-if)# exit salida de la configuración de la vlan

D2(config)#interface vlan 100 entrada en la configuración de interfaz de vlan 100

D2(config-if)# ip address 10.0.100.2 255.255.255.0 asignación de IP en vlan 100

D2(config-if)# ipv6 address fe80::d2:2 link-local configuración de link local

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

D2(config-if)# no shutdown encendido de la interfaz

D2(config-if)# exit salida de interfaz vlan

D2(config)#interface vlan 101 entrada en la interfaz vlan 101

D2(config-if)# ip address 10.0.101.2 255.255.255.0 asignación de IP en vlan 101

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

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

D2(config-if)# no shutdown encendido de la interfaz

D2(config-if)# exit salida de la interfaz

D2(config)#interface vlan 102 entrada en la interfaz vlan 102

D2(config-if)# ip address 10.0.102.2 255.255.255.0 asignación de IP en vlan 102

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

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

D2(config-if)# no shutdown encendido de la interfaz

D2(config-if)# exit salida de la interfaz

D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209 exclusión ip del pool dhcp

D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254 exclusión ip del pool dhcp

D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209 exclusión ip del pool dhcp

D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254 exclusión ip del pool dhcp

D2(config)#ip dhcp pool VLAN-101 configuración del pool dhcp en la vlan 101

D2(dhcp-config)# network 10.0.101.0 255.255.255.0 configuración red del pool

D2(dhcp-config)# default-router 10.0.101.254 configuración de gateway del pool

D2(dhcp-config)# exit salida de la configuración del pool

D2(config)#ip dhcp pool VLAN-102 configuración del pool dhcp en la vlan 101

D2(dhcp-config)# network 10.0.102.0 255.255.255.0 configuración red del pool

D2(dhcp-config)# default-router 10.0.102.254 configuración de gateway del pool

D2(dhcp-config)# exit salida de la configuración del pool

D2(config)#interface range e0/0-3, e1/0-3, e2/0-1, e2/3, e3/0-3 entrada en un rango de interfaces

D2(config-if-range)# shutdown apagado de interfaces

D2(config-if-range)# exit salida del rango de interfaces

D2(config)#end sale al modo EXEC privilegiado

D2#copy running-config startup-config grabación de la configuración en la flash

Configuración A1

Switch>enable ingreso al modo EXEC privilegiado

Switch#configure terminal entra al modo de configuración global

Switch(config)#hostname A1 configuración nombre del host

A1(config)#no ip domain lookup desactiva la traducción de nombres

A1(config)#banner motd # A1, ENCOR Skills Assessment, Scenario 1 # banner

A1(config)#line con 0 configuración de línea de consola

A1(config-line)# exec-timeout 0 0 desconexión por inactividad

A1(config-line)# logging synchronous sincroniza logs

A1(config-line)# exit salida de la configuración de la línea de consola

A1(config)#vlan 100 configuración de vlan 100

A1(config-vlan)# name Management nombramiento de la vlan

A1(config-vlan)# exit salida de la configuración de la vlan

A1(config)#vlan 101 configuración de vlan 101

A1(config-vlan)# name UserGroupA nombramiento de la vlan

A1(config-vlan)# exit salida de la configuración de la vlan

A1(config)#vlan 102 configuración de vlan 102

A1(config-vlan)# name UserGroupB nombramiento de la vlan

A1(config-vlan)# exit salida de la configuración de la vlan

A1(config)#vlan 999 configuración vlan 999

A1(config-vlan)# name NATIVE nombramiento de la vlan

A1(config-vlan)# exit salida de la configuración de la vlan

A1(config)#interface vlan 100 entrada en la configuración de interfaz de vlan 100

A1(config-if)# ip address 10.0.100.3 255.255.255.0 asignación de IP en vlan 100

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

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

A1(config-if)# no shutdown encendido de la interfaz

A1(config-if)# exit salida de la interfaz

A1(config)#interface range e0/0-3, e1/0-3, e2/0-3, e3/0-1 entrada en un rango de interfaces

A1(config-if-range)# shutdown apagado de interfaces

A1(config-if-range)# exit salida del rango de interfaces

A1(config)#end sale al modo EXEC privilegiado

A1#copy running-config startup-config grabación de la configuración en la flash

a. Copie el archivo running-config al archivo startup-config en todos los dispositivos.
b. Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

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: Tareas 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.

Tabla 3: Tareas Parte 2 (continuación)

Tarea#	Tarea	Especificación
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

Tareas 2.1 a 2.6:

Configuración D1

D1#configure terminal entrada en el modo de configuración global

D1(config)#interface range e0/0-3 entrada en un rango de interfaces

D1(config-if-range)# switchport trunk encapsulation dot1q configuración de puerto troncal

D1(config-if-range)# switchport mode trunk habilitación de puerto troncal

D1(config-if-range)# channel-group 12 mode active creación del port channel

D1(config-if-range)# switchport trunk native vlan 999 asignación de vlan nativa del puerto

D1(config-if-range)# no shutdown encendido el rango de interfaces

D1(config-if-range)# exit salida del rango de interfaces

D1(config)#interface range e1/0-1 entrada en un rango de interfaces

D1(config-if-range)# switchport trunk encapsulation dot1q configuración de puerto troncal

D1(config-if-range)# switchport mode trunk habilitación de puerto troncal

D1(config-if-range)# channel-group 1 mode active creación del port channel

D1(config-if-range)# switchport trunk native vlan 999 asigación de vlan nativa del puerto

D1(config-if-range)# no shutdown encendido el rango de interfaces

D1(config-if-range)# exit salida del rango de interfaces

D1(config)#spanning-tree mode rapid-pvst configuración del modo de spanning tree

D1(config)#spanning-tree vlan 100,102 root primary configuración del root primario

D1(config)#spanning-tree vlan 101 root secondary configuración del root secundario

D1(config)#interface e3/3 entrada en la configuración de la interfaz

D1(config-if)# switchport mode access configuración del modo del puerto

D1(config-if)# switchport access vlan 100 configuración del acceso a la vlan del puerto

D1(config-if)# spanning-tree portfast configuración del puerto para dispositivo terminal

D1(config-if)# no shutdown encendido del puerto

D1(config-if)# exit salida de la configuración del puerto

D1(config)#end sale al modo EXEC privilegiado

D1#copy running-config startup-config grabación de la configuración

Configuración D2

D2#configure terminal entrada en el modo de configuración global

D2(config)#interface range e0/0-3 entrada en un rango de interfaces

D2(config-if-range)# switchport trunk encapsulation dot1q configuración de puerto troncal

D2(config-if-range)# switchport mode trunk habilitación de puerto troncal

D2(config-if-range)# channel-group 12 mode active creación del port channel

D2(config-if-range)# switchport trunk native vlan 999 asignación de vlan nativa del puerto

D2(config-if-range)# no shutdown encendido el rango de interfaces

D2(config-if-range)# exit salida de la interfaz

D2(config)#interface range e1/0-1 entrada en un rango de interfaces

D2(config-if-range)# switchport trunk encapsulation dot1q configuración de puerto troncal

D2(config-if-range)# switchport mode trunk configuración modo de puerto

D2(config-if-range)# channel-group 1 mode active creación de port channel

D2(config-if-range)# switchport trunk native vlan 999 configuración de la vlan nativa

D2(config-if-range)# no shutdown encendido de la interfaz

D2(config-if-range)# exit salida de la interfaz

D2(config)#spanning-tree mode rapid-pvst configuración del modo de spannig tree

D2(config)#spanning-tree vlan 101 root primary configuración del root primario

D2(config)#spanning-tree vlan 100,102 root secondary configuración del root secundario

D2(config)#interface e3/3 entrada en la configuración de la inte

D2(config-if)# switchport mode access configuración del modo del puerto

D2(config-if)# switchport access vlan 102 configuración del acceso a la vlan del puerto

D2(config-if)# spanning-tree portfast configuración del puerto para dispositivo terminal

D2(config-if)# no shutdown encendido del puerto

D2(config-if)# exit salida de la configuración del puerto

D2(config)#end sale al modo EXEC privilegiado

D2#copy running-config startup-config grabación de la configuración

Configuración A1

A1#configure terminal entrada en la configuración global

A1(config)#spanning-tree mode rapid-pvst configuración del modo de spanning tree

A1(config)#interface range e0/0-1 entrada en un rango de interfaces

A1(config-if-range)# switchport trunk encapsulation dot1q configuración de puerto troncal

A1(config-if-range)# switchport mode trunk habilitación de puerto troncal

A1(config-if-range)# channel-group 1 mode active creación del port channel

A1(config-if-range)# switchport trunk native vlan 999 asignación de vlan nativa del puerto

A1(config-if-range)# no shutdown encendido el rango de interfaces

A1(config-if-range)# exit salida del rango de interfaces

A1(config)#interface range e0/2-3 entrada en un rango de interfaces

A1(config-if-range)# switchport trunk encapsulation dot1q configuración de puerto troncal

A1(config-if-range)# switchport mode trunk habilitación de puerto troncal

A1(config-if-range)# channel-group 2 mode active creación del port channel

A1(config-if-range)# switchport trunk native vlan 999 asigación de vlan nativa del puerto

A1(config-if-range)# no shutdown encendido el rango de interfaces

A1(config-if-range)# exit salida del rango de interfaces

A1(config)#interface e3/2 entrada en la configuración de la interfaz

A1(config-if)# switchport mode access configuración del modo del puerto

A1(config-if)# switchport access vlan 101 configuración del acceso a la vlan del puerto

A1(config-if)# spanning-tree portfast configuración del puerto para dispositivo terminal

A1(config-if)# no shutdown encendido del puerto

A1(config-if)# exit salida de la configuración de puerto

A1(config)#interface e3/3 entrada en la configuración de la interfaz

A1(config-if)# switchport mode access configuración del modo del puerto

A1(config-if)# switchport access vlan 100 configuración del acceso a la vlan

A1(config-if)# spanning-tree portfast configuración del puerto para dispositivo terminal

A1(config-if)# no shutdown encendido del puerto

A1(config-if)# exit salida de la configuración del puerto

A1(config)#end sale al modo EXEC privilegiado

A1#copy running-config startup-config grabación de la configuración

Tarea 2.7

Figura 3: Verificación de servicios DHCP IPv4 en PC2

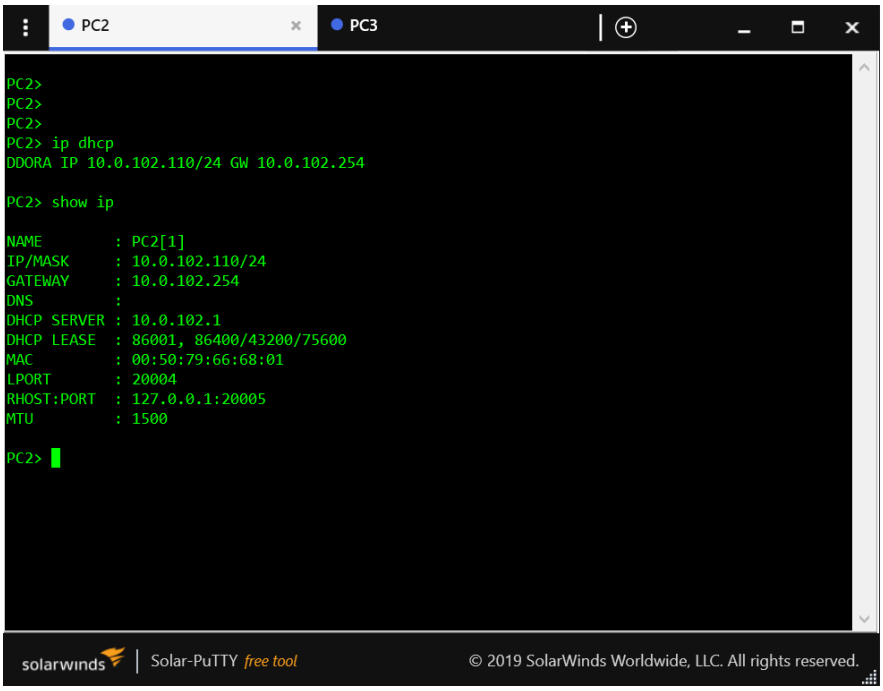
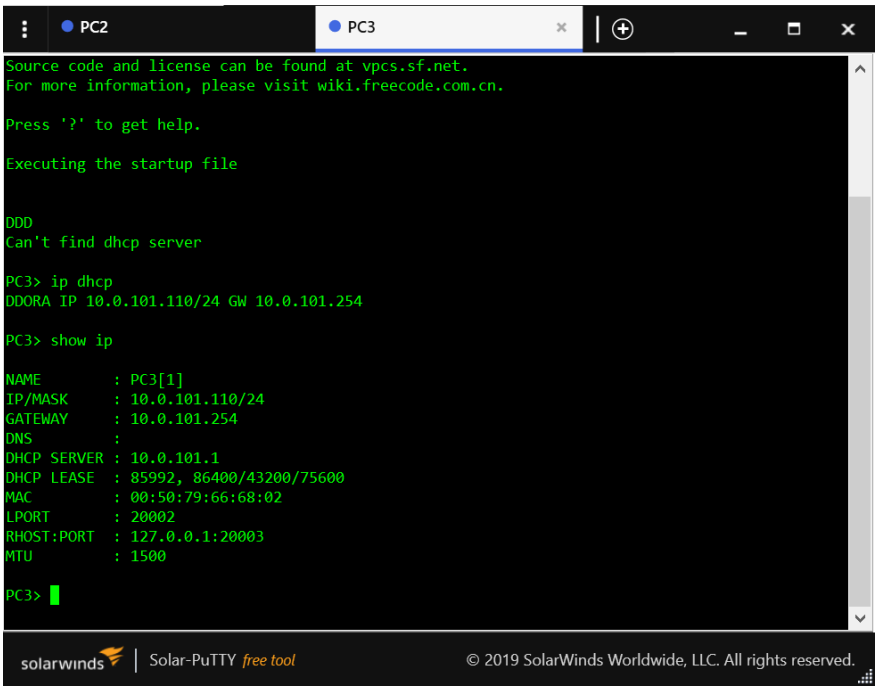


Figura 4: Verificación de servicios DHCP IPv4 en PC3



Tarea 2.8

Figura 5: Verificación de conectividad en PC1

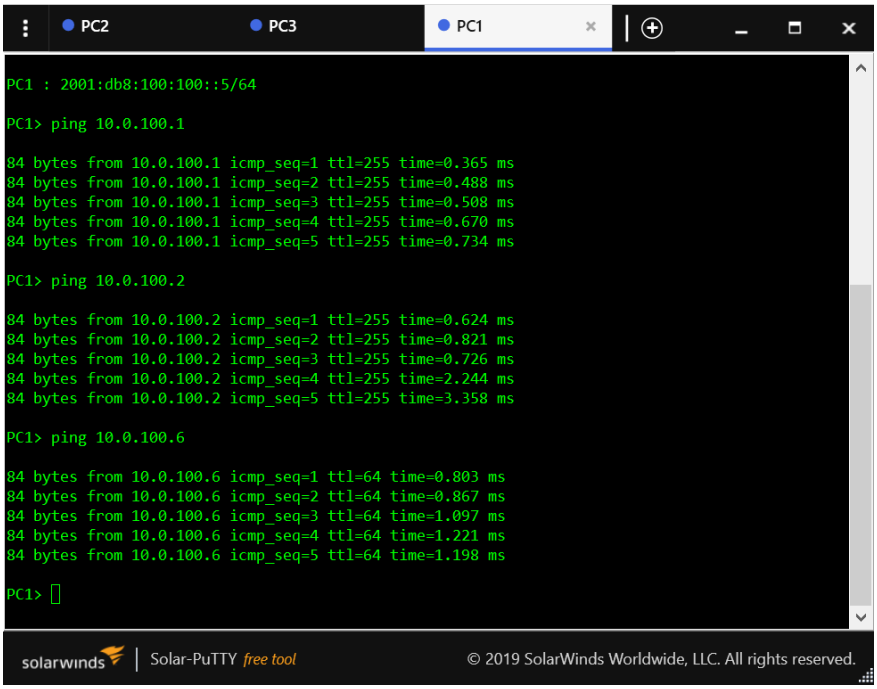


Figura 6: Verificación de conectividad en PC2

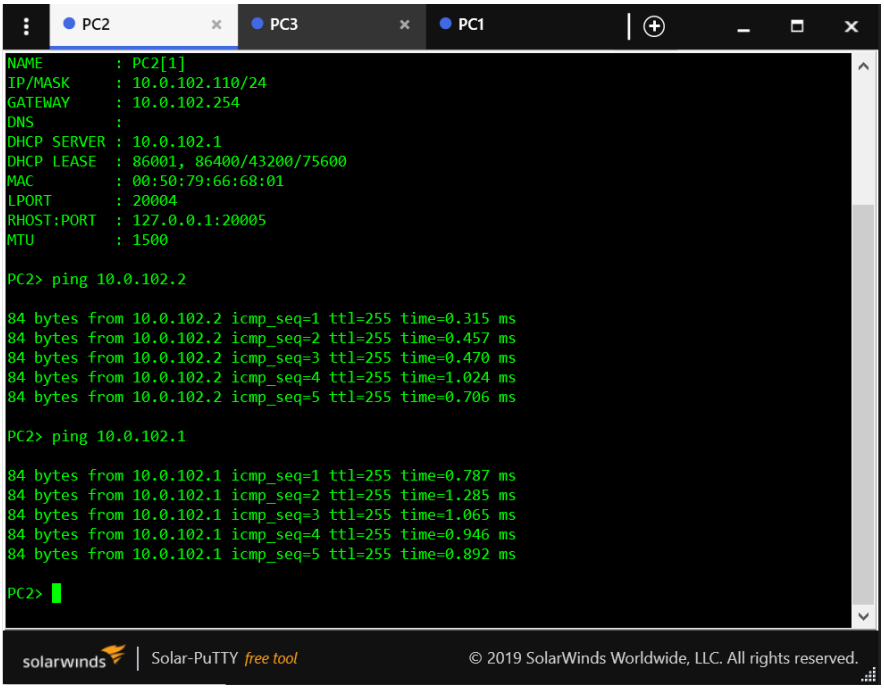


Figura 7: Verificación de conectividad en PC3

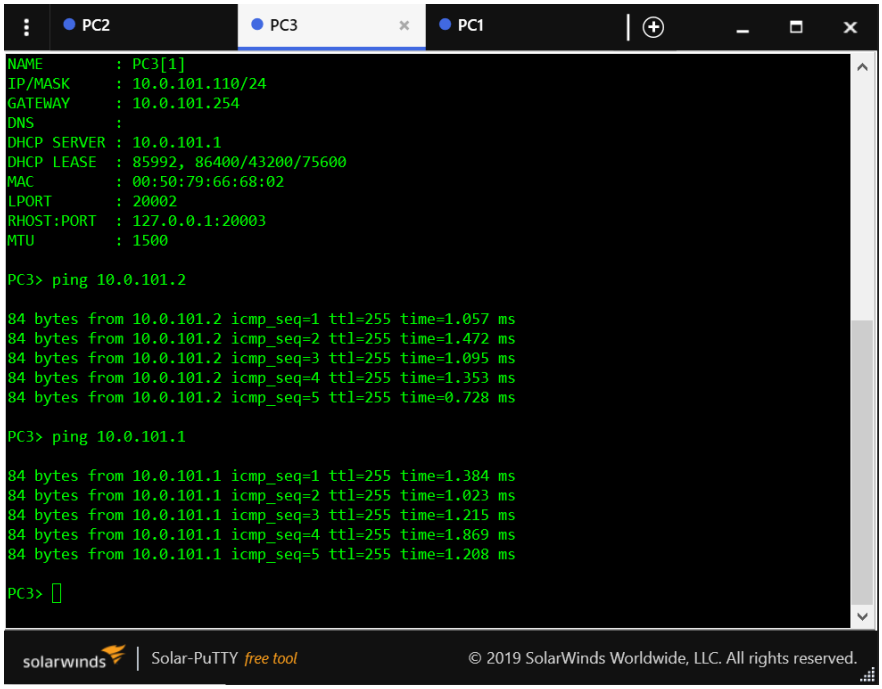
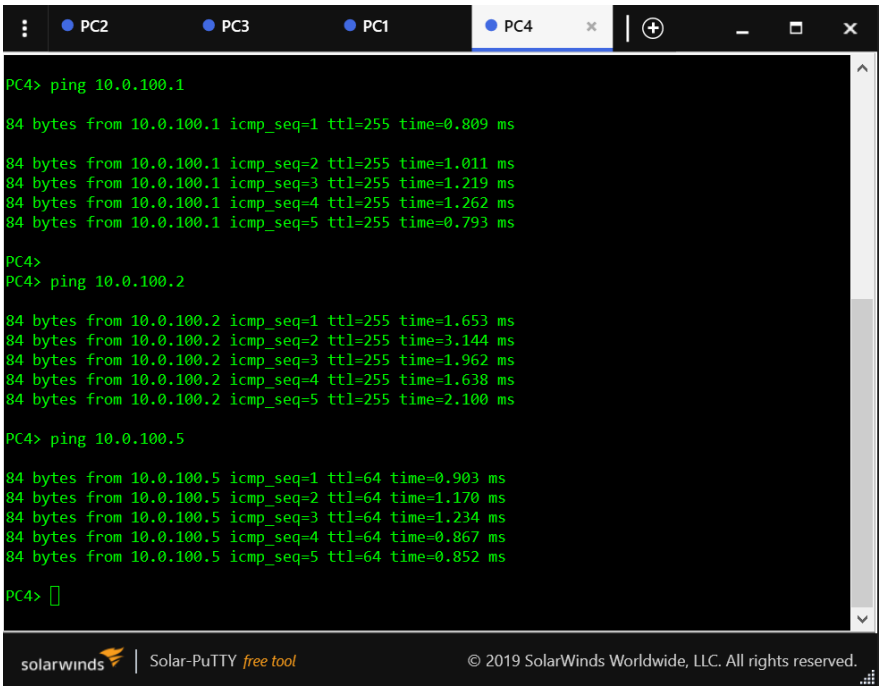


Figura 8: Verificación de conectividad en PC4



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 4: Tareas Parte 3

Tarea#	Tarea	Especificación
3.1	En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.	Use OSPF Process ID **4** y asigne los siguientes router-IDs: • R1: 0.0.4.1 • R3: 0.0.4.3 • D1: 0.0.4.131 • D2: 0.0.4.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • En R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv2 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.2	En la "Red de la Compañia" (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0.	Use OSPF Process ID **6** y asigne los siguientes router-IDs: • R1: 0.0.6.1 • R3: 0.0.6.3 • D1: 0.0.6.131 • D2: 0.0.6.132 En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Area 0. • En R1, no publique la red R1 – R2. • On R1, propague una ruta por defecto. Note que la ruta por defecto deberá ser provista por BGP. Deshabilite las publicaciones OSPFv3 en: • D1: todas las interfaces excepto G1/0/11 • D2: todas las interfaces excepto G1/0/11
3.3	En R2 en la "Red ISP", configure MP-BGP.	Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0: • Una ruta estática predeterminada IPv4. • Una ruta estática predeterminada IPv6. Configure R2 en BGP ASN **500** y use el router-id 2.2.2.2. Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300. En IPv4 address family, anuncie: • La red Loopback 0 IPv4 (/32). • La ruta por defecto (0.0.0.0/0). En IPv6 address family, anuncie: • La red Loopback 0 IPv4 (/128). • La ruta por defecto (::/0).

Tabla 5: Tareas Parte 3 (continuación)

Tarea#	Tarea	Especificación
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.

Tareas 3.1 a 3.4

Configuración R1

R1#configure terminal modo de configuración global

R1(config)#router ospf 4 entrada en OSPF process ID 4

R1(config-router)# router-id 0.0.4.1 asignación de id del router

R1(config-router)# network 10.0.10.0 0.0.0.255 area 0 declaración de la red

R1(config-router)# network 10.0.13.0 0.0.0.255 area 0 declaración de la red

R1(config-router)# default-information originate información de origen por defecto

R1(config-router)# exit salida de la configuración del router

R1(config)#ipv6 router ospf 6 entrada en OSPF process ID 6

R1(config-rtr)# router-id 0.0.6.1 asignación de id del router

R1(config-rtr)# default-information originate información de origen por defecto

R1(config-rtr)# exit salida de la configuración del router

R1(config)#interface e0/1 entrada en la configuración de la interfaz

R1(config-if)# ipv6 ospf 6 area 0 entrada en la configuración ospf ipv6

R1(config-if)# exit salida de la configuración de la interfaz

R1(config)#interface s2/0 entrada en la configuración de la interfaz

R1(config-if)# ipv6 ospf 6 area 0 entrada en la configuración ospf ipv6

R1(config-if)# exit salida de la configuración de la interfaz

R1(config)#ip route 10.0.0.0 255.0.0.0 null0 configuración de ruta nula

R1(config)#ipv6 route 2001:db8:100::/48 null0 configuración de ruta nula ipv6

R1(config)#router bgp 300 entrada en la configuración de bgp

R1(config-router)# bgp router-id 1.1.1.1 configuración de ID

R1(config-router)# neighbor 209.165.200.226 remote-as 500 configuración del sistema autónomo

R1(config-router)# neighbor 2001:db8:200::2 remote-as 500 configuración del sistema autónomo ipv6

R1(config-router)# address-family ipv4 unicast configuración de family address

R1(config-router-af)# neighbor 209.165.200.226 activate configuración del vecino

R1(config-router-af)# no neighbor 2001:db8:200::2 activate configuración del no vecino ipv6

R1(config-router-af)# network 10.0.0.0 mask 255.0.0.0 anuncio de red

R1(config-router-af)# exit-address-family salida de la configuración de familia

R1(config-router)# address-family ipv6 unicast configuración de family ipv6

R1(config-router-af)# no neighbor 209.165.200.226 activate deshabilitar relación vecino

R1(config-router-af)# neighbor 2001:db8:200::2 activate habilitar relación vecino

R1(config-router-af)# network 2001:db8:100::/48 anuncio de red

R1(config-router-af)# exit-address-family salida de configuración familia

R1(config-router)#end salida a configuración global

R1#copy running-config startup-config grabación de configuración a flash

Configuración R2

R2#configure terminal entrada en configuración global

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 configuración de loopback

R2(config)#ipv6 route ::/0 loopback 0 configuración de loopback 0 ipv6

R2(config)#router bgp 500 configuración de bgp

R2(config-router)# bgp router-id 2.2.2.2 configuración de id de router bgp

R2(config-router)# neighbor 209.165.200.225 remote-as 300 configuración de vecino

R2(config-router)# neighbor 2001:db8:200::1 remote-as 300 configuración de sistema remoto

R2(config-router)# address-family ipv4 configuración de family ipv4

R2(config-router-af)# neighbor 209.165.200.225 activate habilitar relación de vecino

R2(config-router-af)# no neighbor 2001:db8:200::1 activate deshabilitar relación de vecino

R2(config-router-af)# network 2.2.2.2 mask 255.255.255.255 anuncio de red

R2(config-router-af)# network 0.0.0.0 anuncio de red

R2(config-router-af)# exit-address-family salida de family

R2(config-router)# address-family ipv6 configuración de family ipv6

R2(config-router-af)# no neighbor 209.165.200.225 activate deshabilitar anuncio de vecino

R2(config-router-af)# neighbor 2001:db8:200::1 activate habilitar relación de vecino

R2(config-router-af)# network 2001:db8:2222::/128 anuncio de red

R2(config-router-af)# network ::/0 anuncio de red

R2(config-router-af)# exit-address-family salida de family

R2(config-router)#end salida a configuración global

R2#copy running-config startup-config grabación de la configuración

Configuración R3

R3#configure terminal entrada en configuración global

R3(config)#router ospf 4 entrada en configuración ospf proceso 4

R3(config-router)# router-id 0.0.4.3 identificación de router
R3(config-router)# network 10.0.11.0 0.0.0.255 area 0 anuncio de red
R3(config-router)# network 10.0.13.0 0.0.0.255 area 0 anuncio de red
R3(config-router)# exit salida de la configuración ospf
R3(config)#ipv6 router ospf 6 entrada en configuración ospf proceso 6
R3(config-rtr)# router-id 0.0.6.3 identificación de router
R3(config-rtr)# exit salida de la configuración ospf
R3(config)#interface e0/1 entrada en la interfaz
R3(config-if)# ipv6 ospf 6 area 0 configuración de ospf en la interfaz
R3(config-if)# exit salida de la interfaz
R3(config)#interface s2/0 entrada en la interfaz
R3(config-if)# ipv6 ospf 6 area 0 configuración de ospf en la interfaz
R3(config-if)# exit salida de la interfaz
R3(config)#end salida a configuración global
R3#copy running-config startup-config grabación de la configuración

Configuración D1

D1#configure terminal
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
D1(config-router)# network 10.0.100.0 0.0.0.255 area 0
D1(config-router)# network 10.0.101.0 0.0.0.255 area 0
D1(config-router)# network 10.0.102.0 0.0.0.255 area 0
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0
D1(config-router)# passive-interface default
D1(config-router)# no passive-interface e2/2
D1(config-router)# exit
D1(config)#ipv6 router ospf 6
D1(config-rtr)# router-id 0.0.6.131
D1(config-rtr)# passive-interface default
D1(config-rtr)# no passive-interface e2/2

D1(config-rtr)# exit
D1(config)#interface e2/2
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#interface vlan 100
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#interface vlan 101
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#interface vlan 102
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# exit
D1(config)#end
D1#copy running-config startup-config

Configuración D2

D2#configure terminal
D2(config)#router ospf 4
D2(config-router)# router-id 0.0.4.132
D2(config-router)# network 10.0.100.0 0.0.0.255 area 0
D2(config-router)# network 10.0.101.0 0.0.0.255 area 0
D2(config-router)# network 10.0.102.0 0.0.0.255 area 0
D2(config-router)# network 10.0.11.0 0.0.0.255 area 0
D2(config-router)# passive-interface default
D2(config-router)# no passive-interface e2/2
D2(config-router)# exit
D2(config)#ipv6 router ospf 6
D2(config-rtr)# router-id 0.0.6.132
D2(config-rtr)# passive-interface default
D2(config-rtr)# no passive-interface e2/2

D2(config-rtr)# exit

D2(config)#interface e2/2

D2(config-if)# ipv6 ospf 6 area 0

D2(config-if)# exit

D2(config)#interface vlan 100

D2(config-if)# ipv6 ospf 6 area 0

D2(config-if)# exit

D2(config)#interface vlan 101

D2(config-if)# ipv6 ospf 6 area 0

D2(config-if)# exit

D2(config)#interface vlan 102

D2(config-if)# ipv6 ospf 6 area 0

D2(config-if)# exit

D2(config)#end

D2#copy running-config startup-config

Figura 9: Verificación de conectividad desde D1 a Loopback0

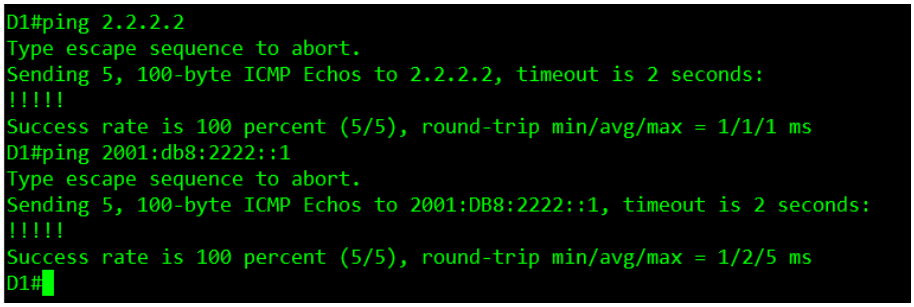
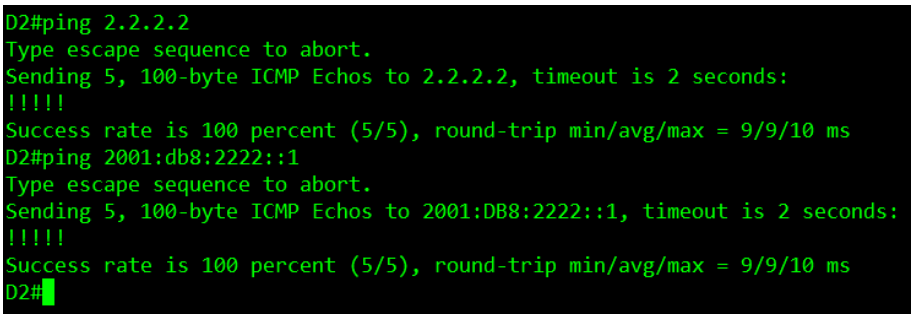


Figura 10: Verificación de conectividad desde D2 a Loopback0



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 hosts en la “Red de la Compañía”.

Las tareas de configuración son las siguientes:

Tabla 6: Tareas Parte 4

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

Tabla 7: Tareas Parte 4 (continuación)

Tarea#	Tarea	Especificación
4.3	En D1 configure HSRPv2.	D1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: • Asigne la dirección IP virtual **10.0.100.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 y decremente en 60. Configure IPv4 HSRP grupo **114** para la VLAN 101: • Asigne la dirección IP virtual **10.0.101.254**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv4 HSRP grupo **124** para la VLAN 102: • Asigne la dirección IP virtual **10.0.102.254**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 4 para disminuir en 60. Configure IPv6 HSRP grupo **106** para la VLAN 100: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **116** para la VLAN 101: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Habilite la preferencia (preemption). • Registre el objeto 6 y decremente en 60. Configure IPv6 HSRP grupo **126** para la VLAN 102: • Asigne la dirección IP virtual usando **ipv6 autoconfig**. • Establezca la prioridad del grupo en **150**. • Habilite la preferencia (preemption). • Rastree el objeto 6 y decremente en 60.

Tareas 4.1 a 4.3

Configuración D1

```
D1#configure terminal
D1(config)#ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
D1(config)#ip sla 6
D1(config-ip-sla)# icmp-echo 2001:db8:100:1010::1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
D1(config)#ip sla schedule 4 life forever start-time now
D1(config)#ip sla schedule 6 life forever start-time now
D1(config)#track 4 ip sla 4
D1(config-track)# delay down 10 up 15
D1(config-track)# exit
D1(config)#track 6 ip sla 6
D1(config-track)# delay down 10 up 15
D1(config-track)# exit
D1(config)#interface vlan 100
D1(config-if)# standby version 2
D1(config-if)# standby 104 ip 10.0.100.254
D1(config-if)# standby 104 priority 150
D1(config-if)# standby 104 preempt
D1(config-if)# standby 104 track 4 decrement 60
D1(config-if)# standby 106 ipv6 autoconfig
D1(config-if)# standby 106 priority 150
D1(config-if)# standby 106 preempt
D1(config-if)# standby 106 track 6 decrement 60
D1(config-if)# exit
```

D1(config)#interface vlan 101
D1(config-if)# standby version 2
D1(config-if)# standby 114 ip 10.0.101.254
D1(config-if)# standby 114 preempt
D1(config-if)# standby 114 track 4 decrement 60
D1(config-if)# standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
D1(config-if)# standby 116 track 6 decrement 60
D1(config-if)# exit
D1(config)#interface vlan 102
D1(config-if)# standby version 2
D1(config-if)# standby 124 ip 10.0.102.254
D1(config-if)# standby 124 priority 150
D1(config-if)# standby 124 preempt
D1(config-if)# standby 124 track 4 decrement 60
D1(config-if)# standby 126 ipv6 autoconfig
D1(config-if)# standby 126 priority 150
D1(config-if)# standby 126 preempt
D1(config-if)# standby 126 track 6 decrement 60
D1(config-if)# exit
D1(config)#end
D1#copy running-config startup-config

Configuración D2

D2#configure terminal
D2(config)#ip sla 4
D2(config-ip-sla)# icmp-echo 10.0.11.1
D2(config-ip-sla-echo)# frequency 5
D2(config-ip-sla-echo)#exit
D2(config)#ip sla 6
D2(config-ip-sla)# icmp-echo 2001:db8:100:1011::1

D2(config-ip-sla-echo)# frequency 5

D2(config-ip-sla-echo)#exit

D2(config)#ip sla schedule 4 life forever start-time now

D2(config)#ip sla schedule 6 life forever start-time now

D2(config)#track 4 ip sla 4

D2(config-track)# delay down 10 up 15

D2(config-track)# exit

D2(config)#track 6 ip sla 6

D2(config-track)# delay down 10 up 15

D2(config-track)# exit

D2(config)#interface vlan 100

D2(config-if)# standby version 2

D2(config-if)# standby 104 ip 10.0.100.254

D2(config-if)# standby 104 preempt

D2(config-if)# standby 104 track 4 decrement 60

D2(config-if)# standby 106 ipv6 autoconfig

D2(config-if)# standby 106 preempt

D2(config-if)# standby 106 track 6 decrement 60

D2(config-if)# exit

D2(config)#interface vlan 101

D2(config-if)# standby version 2

D2(config-if)# standby 114 ip 10.0.101.254

D2(config-if)# standby 114 priority 150

D2(config-if)# standby 114 preempt

D2(config-if)# standby 114 track 4 decrement 60

D2(config-if)# standby 116 ipv6 autoconfig

D2(config-if)# standby 116 priority 150

D2(config-if)# standby 116 preempt

D2(config-if)# standby 116 track 6 decrement 60

D2(config-if)# exit

D2(config)#interface vlan 102

D2(config-if)# standby version 2

D2(config-if)# standby 124 ip 10.0.102.254

D2(config-if)# standby 124 preempt

D2(config-if)# standby 124 track 4 decrement 60

D2(config-if)# standby 126 ipv6 autoconfig

D2(config-if)# standby 126 preempt

D2(config-if)# standby 126 track 6 decrement 60

D2(config-if)# exit

D2(config)#end

D2#copy running-config startup-config

Parte 5: Seguridad

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

Las tareas de configuración son las siguientes:

Tabla 8: Tareas Parte 5

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

Tabla 9: Tareas Parte 5 (continuación)

Tarea#	Tarea	Especificación
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**.

Tareas 5.1 a 5.5

Configuración R1

R1#configure terminal

R1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

R1(config)#aaa new-model

R1(config)#radius server RADIUS

R1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813

R1(config-radius-server)# key $trongPass

R1(config-radius-server)# exit

R1(config)#aaa authentication login default group radius local

R1(config)#end

R1#copy running-config startup-config

Configuración R2

R2#configure terminal

R2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

R2(config)#end

R2#copy running-config startup-config

Configuración R3

R3#configure terminal

R3(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

R3(config)#aaa new-model

R3(config)#radius server RADIUS

R3(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813

R3(config-radius-server)# key $trongPass

R3(config-radius-server)# exit

R3(config)#aaa authentication login default group radius local

R3(config)#end

R3#copy running-config startup-config

Configuración D1

D1#configure terminal

D1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

D1(config)#aaa new-model

D1(config)#radius server RADIUS

D1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813

D1(config-radius-server)# key $trongPass

D1(config-radius-server)# exit

D1(config)#aaa authentication login default group radius local

D1(config)#end

D1#copy running-config startup-config

Configuración D2

D2#configure terminal

D2(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

D2(config)#aaa new-model

D2(config)#radius server RADIUS

D2(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813

D2(config-radius-server)# key $trongPass

D2(config-radius-server)# exit

D2(config)#aaa authentication login default group radius local

D2(config)#end

D2#copy running-config startup-config

Configuración A1

A1#configure terminal

A1(config)#enable algorithm-type SCRYPT secret cisco12345cisco

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

A1(config)#aaa new-model

A1(config)#radius server RADIUS

A1(config-radius-server)#$v4 10.0.100.6 auth-port 1812 acct-port 1813

A1(config-radius-server)# key $trongPass

A1(config-radius-server)# exit

A1(config)#aaa authentication login default group radius local

A1(config)#end

A1#copy running-config startup-config

Nota: no se puede realizar la verificación RADIUS ya que no existe un servidor con esta funcionalidad, en las configuraciones se realizó, el apuntamiento a la dirección 10.0.100.6, pero este servidor no existe en nuestra topología.

Tabla 10: Tareas 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: • Unicamente se usará SNMP en modo lectura (Read-Only). • Limite el acceso SNMP a la dirección IP de la PC1. • Configure el valor de contacto SNMP con su nombre. • Establezca el *community string* en **ENCORSA**. • En R3, D1, y D2, habilite el envío de *traps config* y *ospf*. • En R1, habilite el envío de *traps bgp, config*, y *ospf*. • En A1, habilite el envío de *traps config*.

Tareas 6.1 a 6.5

Configuración R2

R2#configure terminal

R2(config)#ntp master 3

R2(config)#end
R2#copy running-config startup-config

Configuración R1

R1#configure terminal
R1(config)#ntp server 2.2.2.2
R1(config)# logging trap warning
R1(config)# logging host 10.0.100.5
R1(config)# logging on
R1(config)#ip access-list standard SNMP-NMS
R1(config-std-nacl)# permit host 10.0.100.5
R1(config-std-nacl)# exit
R1(config)# snmp-server contact Cisco Student
R1(config)# snmp-server community ENCORSA ro SNMP-NMS
R1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R1(config)# snmp-server ifindex persist
R1(config)# snmp-server enable traps bgp
R1(config)# snmp-server enable traps config
R1(config)# snmp-server enable traps ospf
R1(config)#end
R1#copy running-config startup-config

Configuración R3

R3#configure terminal
R3(config)#ntp server 2.2.2.2
R3(config)# logging trap warning
R3(config)# logging host 10.0.100.5
R3(config)# logging on
R3(config)#ip access-list standard SNMP-NMS

R3(config-std-nacl)# permit host 10.0.100.5
R3(config-std-nacl)# exit
R3(config)# snmp-server contact Cisco Student
R3(config)# snmp-server community ENCORSA ro SNMP-NMS
R3(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config)# snmp-server ifindex persist
R3(config)# snmp-server enable traps bgp
R3(config)# snmp-server enable traps config
R3(config)# snmp-server enable traps ospf
R3(config)#end
R3#copy running-config startup-config

Configuración D1

D1#configure terminal
D1(config)#ntp server 2.2.2.2
D1(config)# logging trap warning
D1(config)# logging host 10.0.100.5
D1(config)# logging on
D1(config)#ip access-list standard SNMP-NMS
D1(config-std-nacl)# permit host 10.0.100.5
D1(config-std-nacl)# exit
D1(config)# snmp-server contact Cisco Student
D1(config)# snmp-server community ENCORSA ro SNMP-NMS
D1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config)# snmp-server ifindex persist
D1(config)# snmp-server enable traps bgp
D1(config)# snmp-server enable traps ospf
D1(config)#end
D1#copy running-config startup-config

Configuración D2

```
D2#configure terminal
D2(config)#ntp server 2.2.2.2
D2(config)# logging trap warning
D2(config)# logging host 10.0.100.5
D2(config)# logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#  permit host 10.0.100.5
D2(config-std-nacl)#  exit
D2(config)# snmp-server contact Cisco Student
D2(config)# snmp-server community ENCORSA ro SNMP-NMS
D2(config)# snmp-server host 10.0.100.5 version 2c ENCORSA
D2(config)# snmp-server ifindex persist
D2(config)# snmp-server enable traps bgp
D2(config)# snmp-server enable traps ospf
D2(config)#end
D2#copy running-config startup-config
```

Configuración A1

```
A1#configure terminal
A1(config)#ntp server 2.2.2.2
A1(config)# logging trap warning
A1(config)# logging host 10.0.100.5
A1(config)# logging on
A1(config)#ip access-list standard SNMP-NMS
A1(config-std-nacl)#  permit host 10.0.100.5
A1(config-std-nacl)#  exit
A1(config)# snmp-server contact Cisco Student
A1(config)# snmp-server community ENCORSA ro SNMP-NMS
```

A1(config)# snmp-server host 10.0.100.5 version 2c ENCORSA

A1(config)# snmp-server ifindex persist

A1(config)# snmp-server enable traps bgp

A1(config)# snmp-server enable traps ospf

A1(config)#end

A1#copy running-config startup-config

CONCLUSIONES

El uso de protocolos de enrutamiento dinámico nos permite el aprendizaje rápido de la topología de red por la cual estemos pasando y la cantidad de saltos posibles para alcanzar un destino.

Como elemento de seguridad el uso de Vlan nos permite la segmentación adecuada de una red limitando el acceso a los recursos que sean absolutamente necesarios y logrando una división basada en departamentos, servicios o localidades.

El empleo del protocolo LACP, garantiza una conexión redundante y confiable, ya que suma las velocidades de los enlaces que participen, es fundamental en la implementación de una topología de core.

Gracias el RADIUS, podemos lograr una autenticación que no se aloje directamente en el dispositivo consultado, y se realice dicho proceso con un equipo remoto en el cual se encuentren los datos del usuario, nombre, contraseña, nivel de uso, entre otros.

BIBLIOGRAFIA

Configuración DHCP en Router (s.f), 27 de mayo de 2018, recuperado de https://apuntesdecisco.blogspot.com/2008/07/configuracin-de-dhcp-en-lrouter.html

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

Gerometta Oscar, (2015), 28 de junio, Que es una SVI, recuperado de http://librosnetworking.blogspot.com/2015/06/que-es-una-svi.html

HSRP Versión 2 (s.f), 27 mayo de 2018, recuperado de https://www.cisco.com/c/en/us/td/docs/ios-ml/ios/ipapp_fhrp/configuration/xe3s/fhp-xe-3s-book/fhp-hsrp-v2.html

Morales, J. M. Introduccción al CLI en routers y switches cisco. Recuperado de: https://pics.unlugarenelmundo.es/hechoencasa/CLI%20en%20Routers%20y%20Switches%20Cisco.pdf