DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MARCO ALEJANDRO ZAMBRANO BENAVIDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA

PITALITO - HUILA

2021

DIPLOMADO DE PROFUNDIZACION CISCO

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MARCO ALEJANDRO ZAMBRANO BENAVIDES

Diplomado de opción de grado presentado para optar el título de

INGENIERO ELECTRÓNICO

MSC. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA EN TELECOMUNICACIONES

PITALITO - HUILA

2021

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

PITALITO, 29 de noviembre del 2021

AGRADECIMIENTOS

Como primera medida doy infinitas gracias a Dios todo poderoso que es quien ilumina nuestro camino y nos guía por el buen camino y, sin importar los problemas por los que hemos atravesado a lo largo de nuestra existencia, nos ha sabido sacar de la oscuridad y nos brinda las fuerzas necesarias para afrontar cada tropiezo que tenemos.

Un agradecimiento muy especial a mis padres Guillermo Zambrano y Blanca Marina Benavidez, que desde la medida de sus posibilidades me han brindado todo el apoyo que he necesitado, cada uno a su manera, pero con la firme convicción de sacar adelante mi carrera, he recibido mucho apoyo de su parte, me han aconsejado, han confiado en que soy capaz de lograr las cosas que me proponga y me dan la fuerza cuando más la he necesitado; también agradezco a mis hermanos Oscar, Charles y Daniel Zambrano, que me impulsan a surgir, a hacer las cosas bien, a crecer como profesional, pero sobre todo como persona, agradezco también a mi amigo Jhonier David Anacona, que me ha ayudado a lo largo de la carrera, enseñándome muchas de las cosas que desconocía y que fueron de gran valor porque he aprendido cosas que me han ayudado a sacar la carrera de la mejor manera.

Por último, quiero agradecer a los tutores de la universidad que han estado brindando su apoyo y acompañamiento a lo largo de este lindo proceso que está por culminar, especialmente quiero dar gracias al ingeniero Diego Nava del CCAV de Pitalito que me acompañó desde el inicio de mi carrera, tanto en lo académico, como en el semillero de investigación y realizó el acompañamiento por el plan padrino y que siempre estuvo pendiente en cada periodo en todos los procesos que lo requerí.

CONTENIDO

LISTA DE TABLAS

LISTADO DE FIGURAS

GLOSARIO

DHCP: Es un servidor que asigna automáticamente las direcciones IP, puertas de enlace y también otros parámetros que requieren las redes para la transmisión de datos dentro de una red

Dirección IP: Es un conjunto de números que sirven para identificar lógicamente una interfaz en la red, esta dirección la poseen los elementos de comunicación tales como computadores, smartphones, routers, entre otros, que utilicen el protocolo de comunicación que corresponde al modelo TCP/IP.

VLAN: Es la tecnología que permite crear redes lógicas virtuales dentro de la misma red física, pero de manera independiente, puesto que se trata de una subdivisión de la red LAN.

OSPF: Es un protocolo de enrutamiento que ha sido desarrollado para las redes IP, de tipo enlace-estado y que se basa en utilizar la vía más corta para la comunicación aun cuando hay un cambio en la topología de red.

NTP: Es un protocolo que ha sido utilizado ampliamente para sincronizar los ordenadores a los servidores que están conectados a internet o una red telefónica o modem, tiene una alta velocidad de transmisión en la red de área local lo que la hace muy confiable y precisa para el envío de información de un terminal a otro.

SWITCH: Es un dispositivo que se utiliza para interconectar los equipos de una red de área local o LAN, y que está regido por unas especificaciones técnicas bajo el estándar IEEE 802.3

RESUMEN

Este informe contiene la prueba de habilidades propuestas para dar solución a una topología de red de una empresa, la cual sirve como práctica para simular un escenario real y que sus características están estipuladas en detalle en la guía de actividades, en esta topología de redes de conmutación y enrutamiento, se realizan las configuraciones básicas en cada dispositivo que ha sido conectado como lo sugiere el problema.

Los recursos utilizados son 3 Routers, 3 Switches, 4 terminales Host o computadores y cables de conexión que sirven para la comunicación entre los dispositivos, todo este montaje es realizado en el software Packet Tracer de SISCO, puesto que se trata del informe que da como culminado el proceso de aprendizaje propuesto como opción de grado para la carrera de ingeniería Electrónica, mediante el diplomado de profundización CISCO CCNP y que muestra los conocimientos adquiridos a lo largo de los diferentes módulos; en los que se ha realizado la configuración de los protocolos de enrutamiento de IPv4, IPv6 entre otros, se realiza la configuración del HSRP versión 2, protocolos como NTP, AAA, protocolos de enrutamiento como el OSPF, direccionamiento IP y de forma automática con DHCP.

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

ABSTRACT

This report contains the skills test proposed to solve a company network topology, which serves as a practice to simulate a real scenario and that its characteristics are stipulated in detail in the activities guide, in this network topology of switching and routing, basic settings are made on each device that has been connected as suggested by the problem.

The resources used are 3 Routers, 3 Switches, 4 Host terminals or computers and connection cables that serve for communication between the devices, all this assembly is carried out in SISCO's Packet Tracer software, since it is the report that gives as completion of the learning process proposed as a degree option for the Electronic engineering career, through the CISCO CCNP in-depth diploma and showing the knowledge acquired throughout the different modules; In which the configuration of the routing protocols of IPv4, IPv6, among others, has been carried out, the configuration of HSRP version 2, protocols such as NTP, AAA, routing protocols such as OSPF, IP addressing and automatically with DHCP is carried out.

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

INTRODUCCIÓN

En el siguiente informe se relaciona un escenario propuesto para evidenciar lo aprendido en el diplomado de profundización CISCO CCNP, correspondiente a la opción de grado de la carrera Ingeniería Electrónica y que es requisito para los aspirantes al grado; en él se plantea una topología que ha sido implementada en el software de la compañía Cisco, llamado Packet Tracer y que consta de varios terminales como computadores, switches y routers que han sido cableados como lo sugiere la guía y posteriormente configurados con los pasos que se enumeran posterior a la tabla de direccionamiento que también debe ser configurada para continuar con los siguientes pasos.

En el paso 2, se configura la capa 2 de la red y el soporte de Host, para tal caso se realiza la configuración de la interfaz troncal para la interconexión de los switches, usando VLAN 99 como nativa, se habilitan los protocolos y se prueba la conexión haciendo ping entre los dispositivos.

Luego se configuran los protocolos de enrutamiento como OSPF y se asignan las IDs en todos los dispositivos, esto corresponde al paso 3; y luego en el siguiente paso se configura la redundancia, para posteriormente realizar las configuraciones de seguridad que sirven para encriptar la contraseña en cada dispositivo y por último se configuran las funciones de administración de red, dando por finalizados los pasos que permiten una correcta comunicación entre los dispositivos de la red.

DESARROLLO DE LA ACTIVIDAD

Escenario Propuesto

Topología de la Red:

Figura 1. Escenario Propuesto

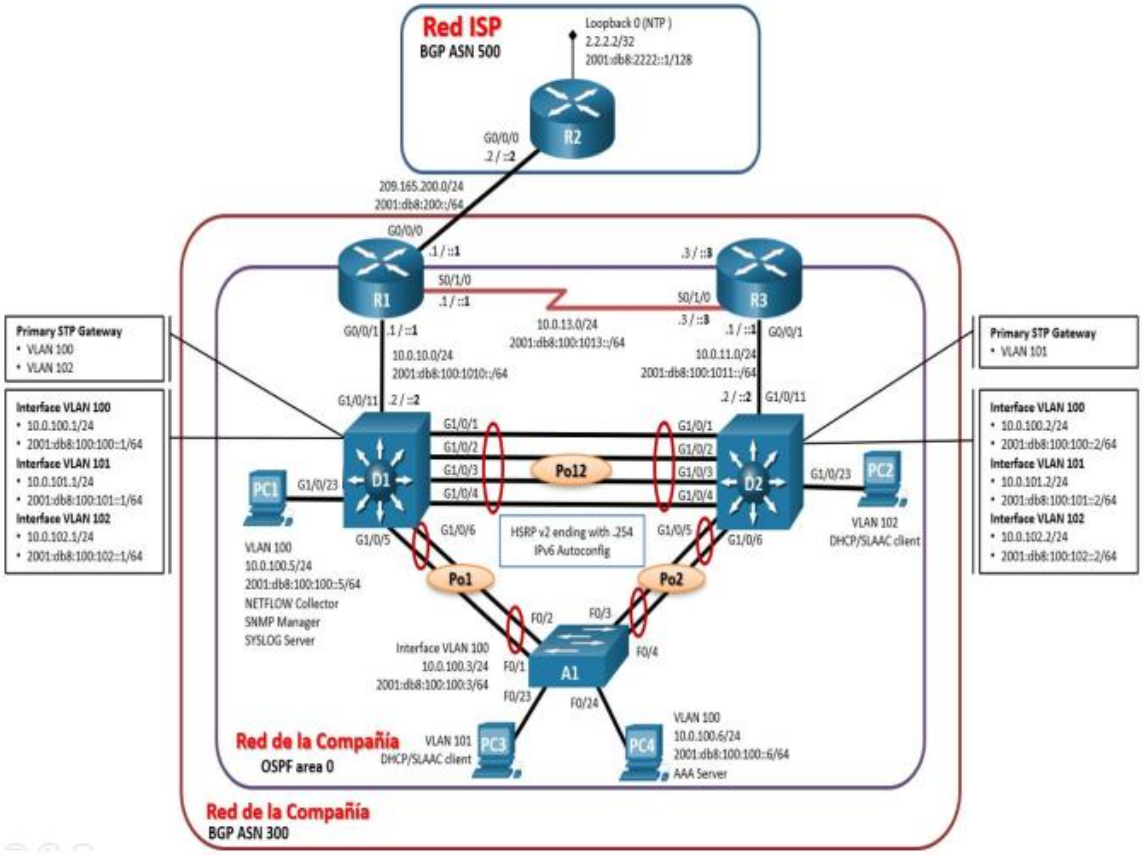


Tabla de direccionamiento

Tabla 1. Direccionamiento para el Escenario

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

Objetivos

Part 1: Construir la red y configurar los ajustes básicos de cada dispositivo y el direccionamiento de las interfaces
Part 2: Configurar la capa 2 de la red y el soporte de Host
Part 3: Configurar los protocolos de enrutamiento
Part 4: Configurar la redundancia del primer salto (no se entrega aún)**
Part 5: Configurar la seguridad (no se entrega aún)**
Part 6: Configurar las características de administración de red (no se entrega aún)**

Escenario

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

Recursos necesarios

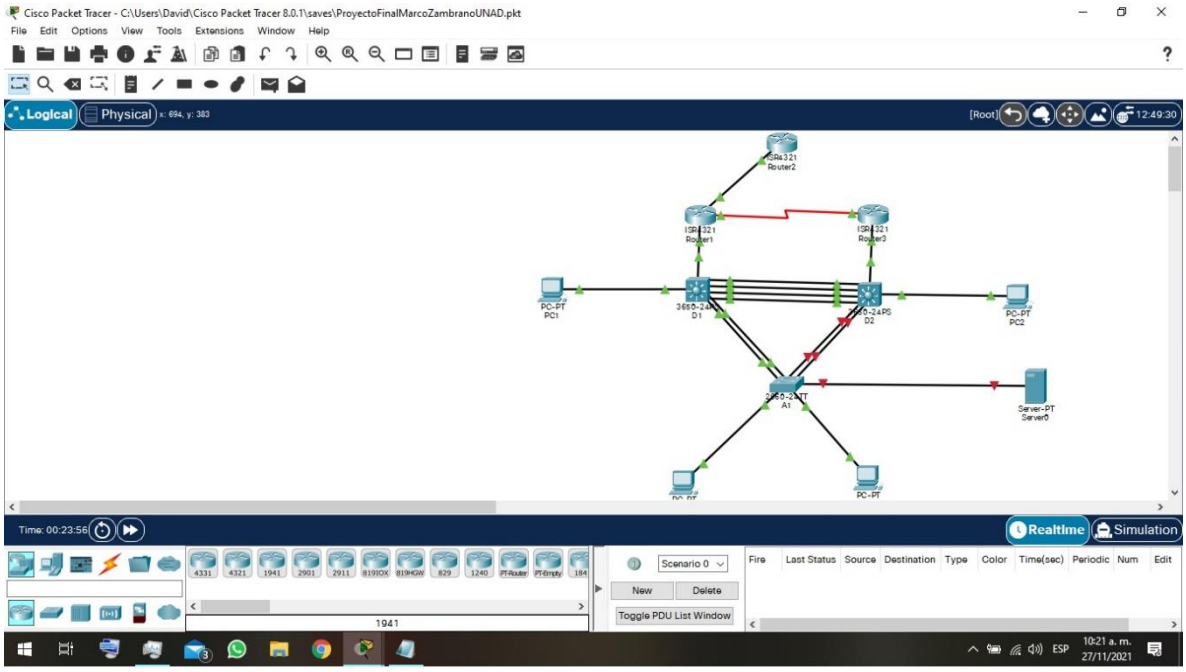
• 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
• 2 Switches (Cisco 3650 con Cisco IOS XE versión 16.9.4 imagen universal o comparable)
• 1 Switch (Cisco 2960 con Cisco IOS versión 15.2 imagen lanbase o comparable)
• 4 PCs (utilice el programa de emulación de terminal)

• Los cables de consola para configurar los dispositivos Cisco IOS van a través de los puertos de consola
• Los cables Ethernet y seriales van como se muestra en la topología

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. Tipología diseñada en Packet Tracer



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 Comando para ingresar a modo privilegiado

Router#configure terminal Comando para ingresar a modo configuración

Router(config)#hostname Comando para nombrar el router R1

R1(config)#ipv6 unicast-routing Tipo de dirección ipv6 unidifusión

R1(config)#no ip domain lookup Evita retrasos al entrar un comando mal escrito

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

R1(config)#line con 0 Comando para ingresar a modo configuración línea

R1(config-line)#exec-timeout 0 0 Comando para retirar el límite de tiempo

R1(config-line)#logging synchronous Para depurar mensajes no solicitados consola

R1(config-line)#exit Salir del modo configuración línea

R1(config)#interface g0/0/0 Configurar interfaces

R1(config-if)# ip address 209.165.200.225 255.255.255.224 Asignar dirección IP

R1(config-if)# ipv6 address fe80::1:1 link-local Asignar direccionamiento ipv6

R1(config-if)# ipv6 address 2001:db8:200::1/64

R1(config-if)# no shutdown Se reinicia una interfaz que está desactivada

R1(config-if)#exit Salir

Posteriormente se procede a realizar la configuración del Router 2

Configuración R2

Router>enable

Router#configure terminal

Router(config)#hostname R2

R2(config)#ipv6 unicast-routing

R2(config)#no ip domain lookup

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

R2(config)#line con 0

R2(config)#exec-timeout 0 0

R2(config)#logging synchronous

```
R2(config)#exit
R2(config)#interface g0/0/0
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
R2(config)#interface Loopback 0
R2(config)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ipv6 address fe80::2:3 link-local
R2(config-if)#ipv6 address 2001:db8:2222::1/128
R2(config-if)#no shutdown
R2(config-if)#exit
```

Ahora se procede a realizar la configuración del Router 3

Configuración R3

```
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#ipv6 unicast-routing
R3(config)#no ip domain lookup
R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
R3(config)#line con 0
R3(config-line)#exec-timeout 0 0
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#interface g0/0/1
```

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 s0/1/0

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

Luego se configura el primer switch

Configuración D1

enable

configure terminal

hostname D1

ip routing

ipv6 unicast-routing

no ip domain lookup

banner motd # D1, ENCOR Skills Assessment, Scenario 1 #

line con 0

exec-timeout 0 0

logging synchronous

exit

vlan 100

name Management

exit

```
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
```

exit

interface vlan 102

ip address 10.0.102.1 255.255.255.0

ipv6 address fe80::d1:4 link-local

ipv6 address 2001:db8:100:102::1/64

no shutdown

exit

ip dhcp excluded-address 10.0.101.1 10.0.101.109

ip dhcp excluded-address 10.0.101.141 10.0.101.254

ip dhcp excluded-address 10.0.102.1 10.0.102.109

ip dhcp excluded-address 10.0.102.141 10.0.102.254

ip dhcp pool VLAN-101

network 10.0.101.0 255.255.255.0

default-router 10.0.101.254

exit

ip dhcp pool VLAN-102

network 10.0.102.0 255.255.255.0

default-router 10.0.102.254

exit

interface range g1/0/1-10, g1/0/12-24, g1/1/1-4

shutdown

exit

Luego se configura el segundo switch

Configuración D2

enable

configure terminal

hostname D2

```
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #line con 0
line con 0
exec-timeout 0 0
logging synchronous
exit
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface g1/0/11
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
```

```
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
ip dhcp pool VLAN-102
```

network 10.0.102.0 255.255.255.0

default-router 10.0.102.254

exit

interface range g1/0/1-10, g1/0/12-24, g1/1/1-4

shutdown

exit

Configuración A1

Para poder realizar la configuración del Switch A1 fue necesario implementar un servidor quien se conectó al switch ya que por medio del servidor se pudo realizar la configuración de la dirección IPV6, puesto que el dispositivo elegido no soporta el comando “sdm prefer dual-ipv4-and-ipv6 default”.

Este procedimiento se realiza con la configuración del servidor y se le asigna una dirección IP 192.168.10.10, para el Switch se le asigna una Vlan e IP con el código:

Switch#enable

Switch#configure terminal

Switch#interface vlan 1

Switch(config-if)#ip address 192.168.10.1 255.255.255.0

Switch(config-if)#no shutdown

Para verificar la conexión entre el switch y el servidor se utiliza el comando ping:

Switch#ping 192.168.10.10

Switch#copy tftp: flash

Address or name of remote host []? 192.168.10.10

Source filename []? c2960-lanbasek9-mz.150-2.SE4.bin Este es el archivo que nos permite configurar la ipv6

Luego se guarda la configuración con el código y se reinicia el switch:

Switch(config)#boot system c2960-lanbasek9-mz.150-2.SE4.bin

Switch#reload

Posteriormente se procede a realizar la configuración de A1:

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
vlan 100
name Management
exit
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
vlan 999
name NATIVE
exit
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown
```

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

R1>enable

R1#copy running-config startup-config — Realizamos la copia de la configuración de la RAM a Nvram

R2>enable — Se ingresa a modo privilegiado

R2#copy running-config startup-config

R3>enable

R3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

D1>enable

D1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

D2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

A1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

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

Figura 3. Configuración Host-PC1

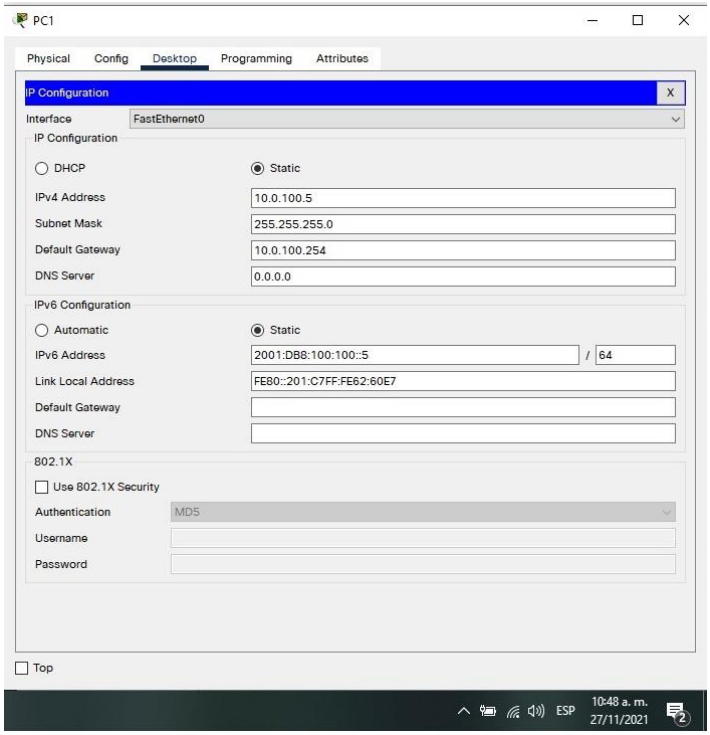
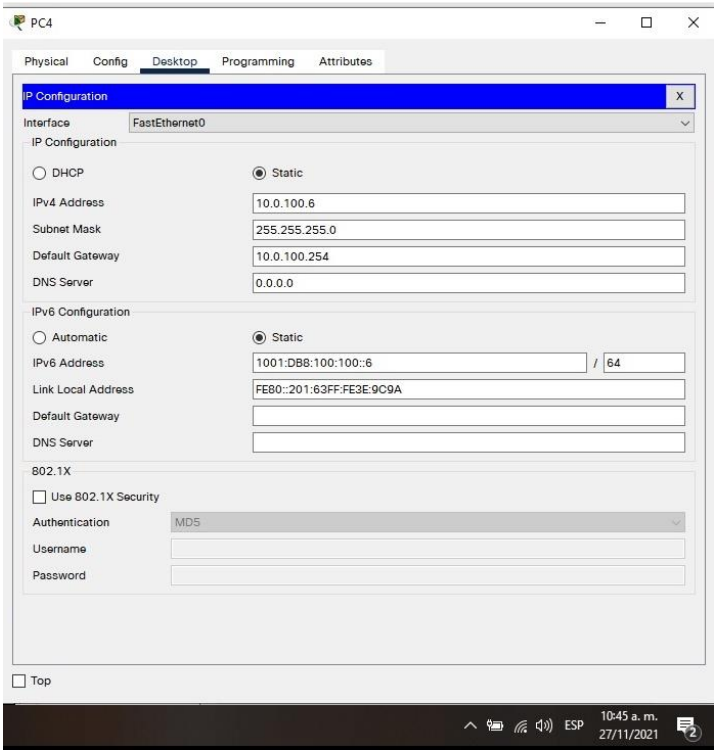


Figura 4. Configuración Host-PC4



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

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

Las tareas de configuración son las siguientes:

Tabla 2. Configuración de protocolos

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

2.1 En todos los Switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre Switches.

Habilitar los enlaces trunk 802.1Q entre:

• D1 and D2

D1>enable Comando para ingresar al modo privilegiado

D1#configure terminal Ingresamos a la configuración del terminal

D1(config)#int g1/0/1 Se indica que conexión se va a configurar

D1(config-if)#switchport trunk encapsulation dot1q Se define la encapsulación protocolo 802.1Q

D1(config-if)#switchport mode trunk Se define modo troncal

• D1 and A1

D1(config)#int range g1/0/5-6

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

D1(config-if-range)#switchport trunk native vlan 999

• D2 and A1

D2(config)#int range g1/0/5-6

D2(config-if-range)#switchport trunk encapsulation dot1q

D2(config-if-range)#switchport mode trunk

D2(config-if-range)#switchport trunk native vlan 999

2.2 En todos los Switches cambie la VLAN nativa en los enlaces troncales.

Use VLAN 999 como la VLAN nativa.

D1(config-if)#switchport trunk native vlan 999 Asignamos la Vlan nativa 999

Realizamos la configuración con cada conexión entre D1 y D2.

D1(config)#int g1/0/2

D1(config-if)#switchport trunk encapsulation dot1q

D1(config-if)#switchport mode trunk

D1(config-if)#switchport trunk native vlan 999

Para g1/0/3 y g1/0/4 se usó la configuración de rango con el código:

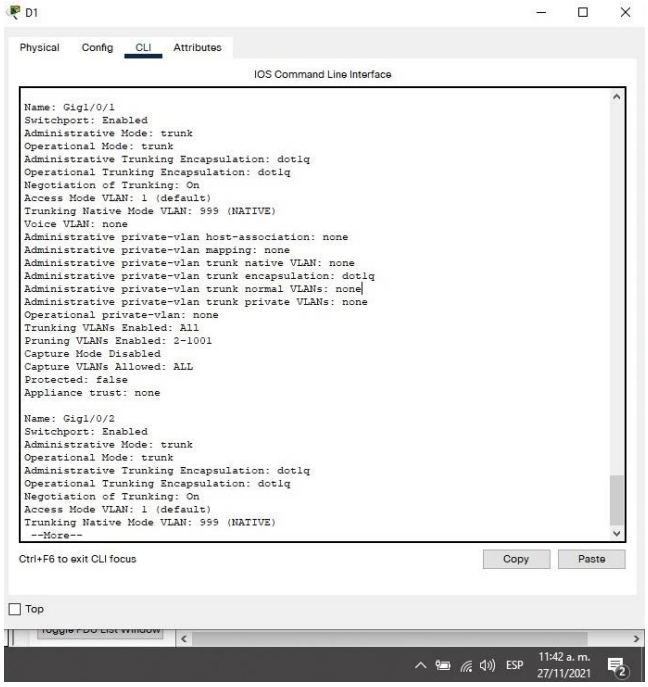
D1(config)#int range g1/0/3-4

D1(config-if-range)#switchport trunk encapsulation dot1q

D1(config-if-range)#switchport mode trunk

D1(config-if-range)#switchport trunk native vlan 999

Figura 5. Resultado de configuración 802.1Q y Vlan Nativa



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

A1#configure terminal Ingresamos al modo de configuración

A1(config)#spanning-tree mode rapid-pvst Cambio de protocolo al RSPT

Esto se realiza en los demás dispositivos.

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.

D1#conf term Ingresamos a modo configuración

D1(config)#spanning-tree vlan 100,102 root primary Se da prioridad 1 Vlan 100-2

D1(config)#spanning-tree vlan 101 root secondary Se da prioridad 2 Vlan 101

D2#configure terminal

D2#spanning-tree mode rapid-pvst

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

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

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

Para establecer un enlace entre el D1 y el D2, se configuran los puertos en el D1 con modo deseado de PAgP y los puertos en el D3 con modo automático de PAgP. Seguidamente se habilitaron los puertos después de que se configuron los modos PAgP.

Se realiza la configuración con el comando channel-goup 12 mode disirable con el objetivo de crear el cannel y seguidamente se inician las interfaces seleccionadas.

D1#configure terminal	Ingresamos al modo configuración
D1(config)#interface range g1/0/1-4	Ingresamos a la interface de rango
D1(config-if-range)#channel-protocol lacp	Asignamos el protocolo lacp
D1(config-if-range)#channel-group 12 mode active	Nombramos grupo
D1#(config-if-range)#no shutdown	Cambiamos el estado de rango de interfaz

Luego se procede a realizar la misma configuración en cada dispositivo según diagrama:

D2#conf term

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

D2(config)#interface range g1/0/1-4

D2(config-if-range)#channel-protocol lacp

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

D2(config-if-range)#Creating a port-channel interface Port-channel 12

D2(config-if-range)#no shutdown

• D1 a A1 – Port channel 1

D1(config)#interface range g1/0/5-6

D1(config-if-range)#channel-protocol lacp

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

A1#configure terminal

A1(config)#interface range f0/1-2

A1(config-if-range)#channel-protocol lacp

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

A1(config-if-range)#no shutdown

• D2 a A1 – Port channel 2

D2(config)#interface range g1/0/1-6

D2(config-if-range)#channel-protocol lacp

D2(config-if-range)#channel-group 2 mode active

A1(config-if-range)#exit

A1(config)#interface range f0/3-4

A1(config-if-range)#channel-protocol lacp

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

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).

D1(config)#int g1/0/23 Seleccionamos el puerto a configurar

D1(config-if)#switchport mode Access Comando para entrar en modo de acceso

D1(config-if)#switchport access vlan 100 Asignamos la vlan 10

D1(config-if)# spanning-tree portfast Configuración de protocolo

De la misma forma se configuran los demás dispositivos

A1(config)#interface f0/23

A1(config-if)#switchport mode access

A1(config-if)#switchport access vlan 101

A1(config-if)#exit

A1(config)#interface f0/24

A1(config-if)#switchport mode access

A1(config-if)#switchport access vlan 100

D2(config)#int g1/0/23

D2(config-if)#switchport mode access

D2(config-if)#switchport access vlan 102

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

Figura 6. DHCP - PC2

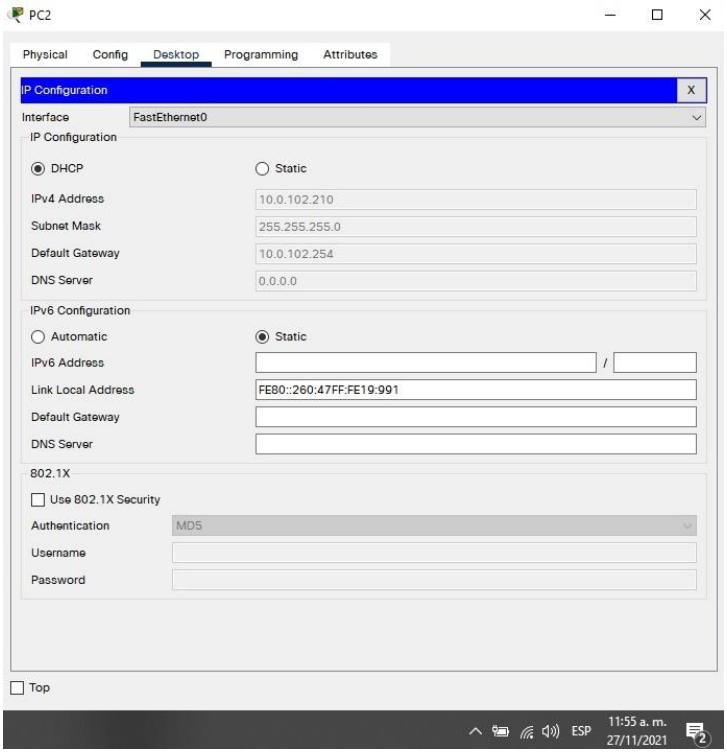
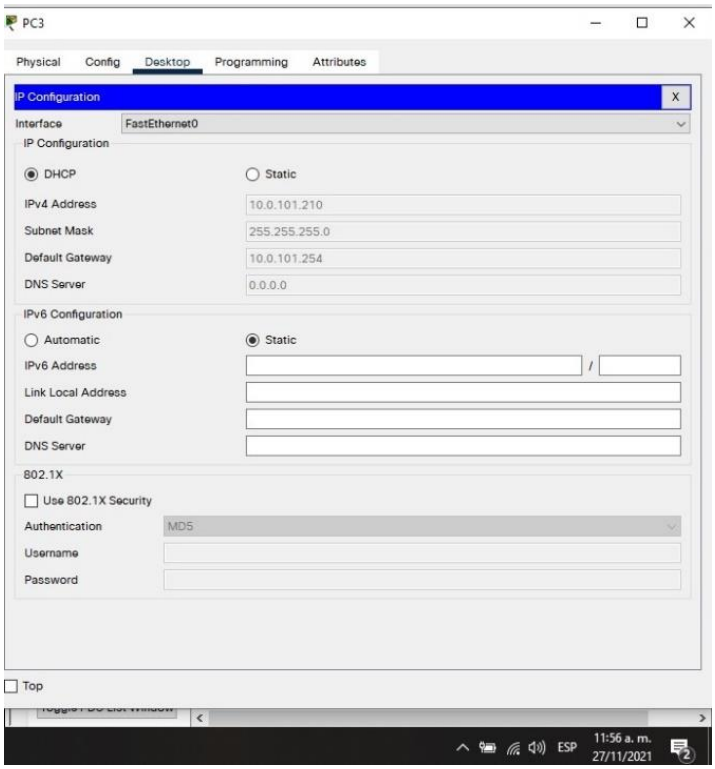


Figura 7. DHCP - PC3



2.8 Verifique la conectividad de la LAN local

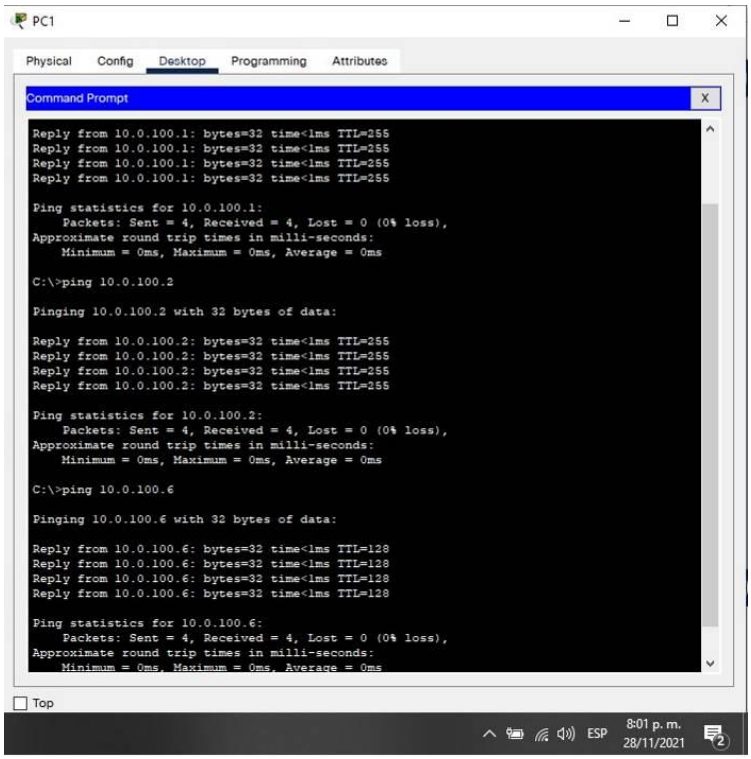
PC1 debería hacer ping con éxito a:

• D1: 10.0.100.1

• D2: 10.0.100.2

• PC4: 10.0.100.6

Figura 8. Verificación pings - PC1

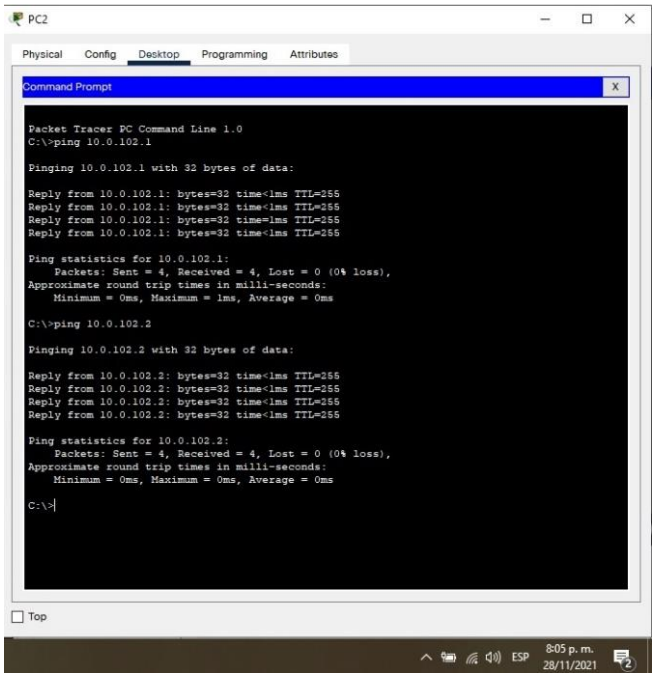


PC2 debería hacer ping con éxito a:

• D1: 10.0.102.1

• D2: 10.0.102.2

Figura 9. Verificación pings - PC2

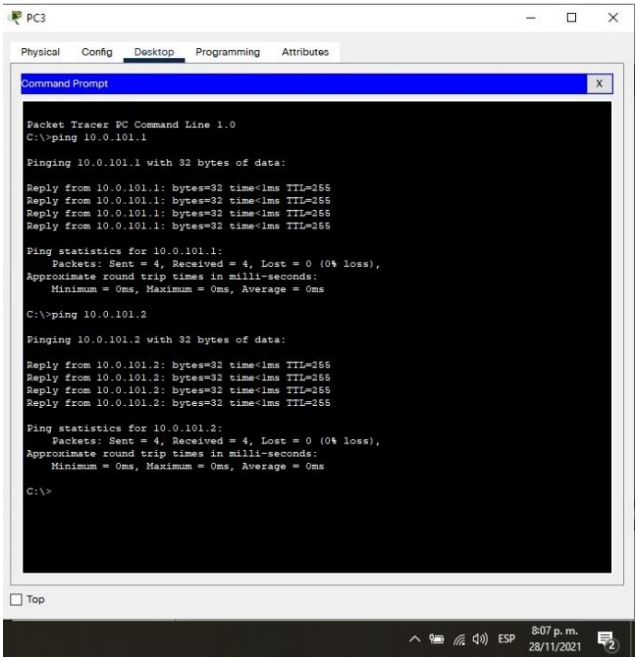


PC3 debería hacer ping con éxito a:

• D1: 10.0.101.1

• D2: 10.0.101.2

Figura 10. Verificación pings - PC3



PC4 debería hacer ping con éxito a:

• D1: 10.0.100.1

• D2: 10.0.100.2

• PC1: 10.0.100.5

Figura 11. Verificación pings - PC4

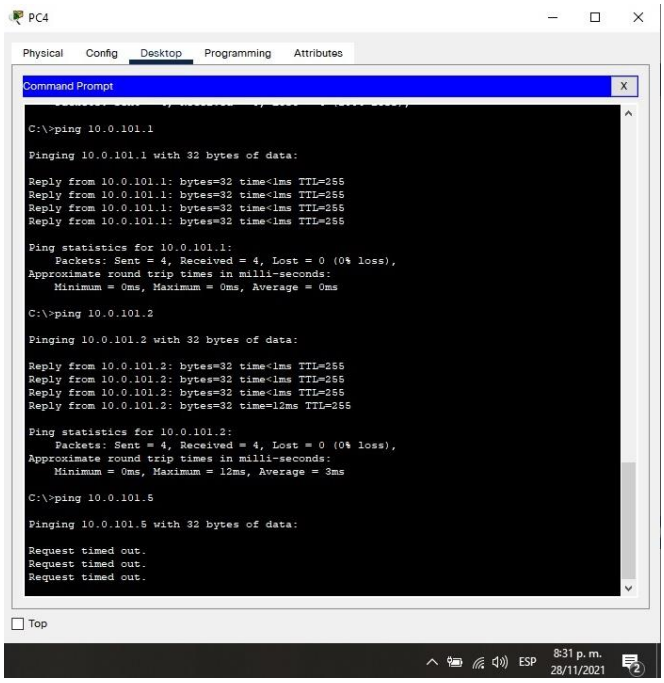
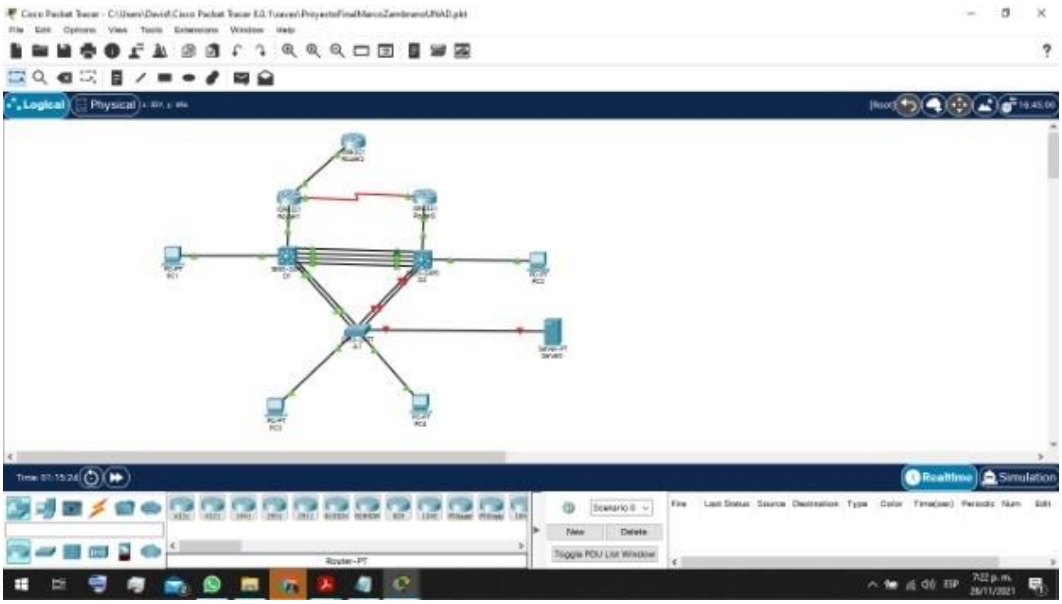


Figura 12. Diagrama final Parte 2



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. Protocolos de enrutamiento 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).
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.

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-área OSPFv2 en área 0.

R1>enable	Ingresamos a la configuración global
R1#configure terminal	Ingresamos a la configuración global
R1(config)#router ospf 4	Le asignamos la ospf e id 4
R1(config-router)#router-id 0.0.4.1	Le asignamos al router ID
R1(config-router)#do show ip route connected	Muestra las interfaces conectadas

C 10.0.10.0/24 is directly connected, GigabitEthernet0/0/1

C 10.0.13.0/24 is directly connected, Serial0/1/0

C 209.165.200.224/27 is directly connected, GigabitEthernet0/0/0

R1(config-router)#network 10.0.10.0 0.0.0.255 area 0	Asignamos área 0 a la interfaz
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0	Asignamos área 0 a la interfaz
R1(config-router)# default-information originate	Declaramos información predeterminada

R1(config-router)#exit

Ahora realizamos la misma configuración en los dispositivos R3, D1 y D2

R3>enable

R3#configure terminal

R3(config)#router ospf 4

R3(config-router)#router-id 0.0.4.3

R3(config-router)#do show ip route connected

C 10.0.11.0/24 is directly connected, GigabitEthernet0/0/1

C 10.0.13.0/24 is directly connected, Serial0/1/0

R3(config-router)#network 10.0.11.0 0.0.0.255 area 0

R3(config-router)#network 10.0.13.0 0.0.0.255 area 0

D1(config)#router ospf 4

D1(config-router)#router-id 0.0.4.131

D1(config-router)#do show ip route connected

C 10.0.10.0/24 is directly connected, GigabitEthernet1/0/11

C 10.0.100.0/24 is directly connected, Vlan100

C 10.0.102.0/24 is directly connected, Vlan102

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 Deshabilita las publicaciones OSPFv2

D1(config-router)#no passive-interface g1/0/11

D2(config)#router ospf 4

D2(config-router)#router-id 0.0.4.132

D2(config-router)#do show ip route connected

C 10.0.11.0/24 is directly connected, GigabitEthernet1/0/11

C 10.0.102.0/24 is directly connected, Vlan102

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 Deshabilita las publicaciones OSPFv2

D2(config-router)#no passive-interface g1/0/11

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-área OSPFv3 en área 0.

Se digita el comando **ipv6 router ospf** para iniciar un proceso OSPFv3 en el router.

Además, se emite el comando **ipv6 ospf 1 area** *id-área* para cada interfaz en R1 que participará en el routing OSPFv3.

R1(config)#ipv6 router ospf 6	Configuramos la OSPF en IPv6
R1(config-rtr)#router-id 0.0.6.1	Le asignamos la id
R1(config-rtr)#default-information originate	Declaramos información por defecto
R1(config-rtr)#exit	Salida del modo de configuración
R1(config)#int g0/0/1	Declaramos la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0	Asignamos área 0 en ipv6
R1(config-if)#exit	Salida del modo de configuración
R1(config)#int s0/1/0	Declaramos la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0	Asignamos área 0 en ipv6

Ahora realizamos la misma configuración en los dispositivos R3, D1 y D2

Router R3:

R3(config)#ipv6 router ospf 6

R3(config-rtr)#router-id 0.0.6.3

R3(config-rtr)#exit

R3(config)# interface g0/0/1

R3(config-if)#ipv6 ospf 6 area 0

R3(config-if)#exit

R3(config)#int s0/1/0

R3(config-if)#ipv6 ospf 6 area 0

R3(config-if)#exit

Switch D1:

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 g1/0/11

D1(config-rtr)#exit

D1(config)# interface g1/0/11

D1(config-if-range)#ipv6 ospf 6 area 0

D1(config-if)#exit

D1(config)#int interface vlan 100

D1(config)#ipv6 ospf 6 area 0

D1(config-if)#exit

D1(config)#int interface vlan 101

D1(config)#ipv6 ospf 6 area 0

D1(config-if)#exit

D1(config)#int interface vlan 102

D1(config)#ipv6 ospf 6 area 0

D1(config-if)#exit

D1(config-if)#end

Switch D2:

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 g1/0/11

D2(config-rtr)#exit

D2(config)#int range g1/0/11

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

```
D2(config-if)#exit
D2(config)#int g1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D2(config-if)#end
```

3.3 En R2 en la “Red ISP”, configure MPBGP.

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

• Una ruta estática predeterminada IPv4.

• Una ruta estática predeterminada IPv6.

```
R2>enable                                   Ingresamos al modo privilegiado
R2#configure terminal                       Configuramos el terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0   Establecemos la ruta a configurar
Loopback 0
R2(config-if)# ipv6 route ::/0 loopback 0   Asignamos los parámetros a configurar
```

Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.

Para esto se configura las redes directamente conectadas en el R2 usando el siguiente código:

R2#enable	Ingresamos al modo privilegiado
R2#configure terminal	Configuramos la terminal
R2(config-router)#router bgp 500	Establecemos el Router con bgp 500
R2(config-router)#bgp router-id 2.2.2.2	Asignamos la id 2.2.2.2

En IPv4 address family, anuncie:

• La red Loopback 0 IPv4 (/32).

• La ruta por defecto (0.0.0.0/0).

R2(config-router)#address-family ipv4	Configuramos la familia ipv4
R2(config-router)# neighbor 209.165.200.225 activate	Red loopback
R2(config-router)# no neighbor 2001:db8:200::1 activate	Red loopback
R2(config-router)# network 2.2.2.2 mask 255.255.255.255	Red y mascara
R2(config-router)#neighbor 0.0.0.0/0	Ruta por defecto
R2(config-router)# exit-address-family	Salir de la configuración de familia

En IPv6 address family, anuncie:

• La red Loopback 0 IPv4 (/128).

• La ruta por defecto (::/0).

R2(config-router)#address-family ipv6

R2(config-router)# no neighbor 209.165.200.225 activate

R2(config-router)# neighbor 2001:db8:200::1 activate

R2(config-router)# network 2001:db8:2222::/128

R2(config-router)# network ::/0

R2(config-router)# exit-address-family

3.4 En R1 en la “Red ISP”, configure MPBGP.

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.

R1#configure terminal	Ingresamos a configuración de terminal
R1(config)#ip route 10.0.0.0 255.255.255.255 null0 ipv4	Configuramos la interfaz null
R1(config)#ip route 2001:db8:100::/48 null0	Interface null opv6

Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.

R1#conf term	Ingresamos a la configuración de terminal
R1(config)#router bgp 300	Asignamos la bgp y ns 300
R1(config-router)#bgp router-id 1.1.1.1	Asignamos la id del router

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

R1(config-router)#neighbor 209.165.200.226 remote-as 500	Definimos la relación vecino ipv4
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500	Definimos la relación vecino ipv6

En IPv4 address family:

• Deshabilite la relación de vecino IPv6.

• Habilite la relación de vecino IPv4.

• Anuncie la red 10.0.0.0/8.

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

R1(config-router)# neighbor 209.165.200.226 activate

R1(config-router)# no neighbor 2001:db8:200::2 activate

R1(config-router)# network 10.0.0.0 mask 255.0.0.0

R1(config-router)# exit-address-family

En IPv6 address family:

• Deshabilite la relación de vecino IPv4.

• Habilite la relación de vecino IPv6.

• Anuncie la red 2001:db8:100::/48.

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

R1(config-router)# no neighbor 209.165.200.226 activate

R1(config-router)# neighbor 2001:db8:200::2 activate

R1(config-router)# network 2001:db8:100::/48

R1(config-router)# exit-address-family

Para verificar los pasos anteriores se a utiliza el comando **Show run**

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

Tabla 4. Configuración de redundancia del primer salto

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

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

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

En este paso realizaremos la implementación del siguiente código:

Para crear dos IP SLAs.

• Use la SLA número 4 para IPv4.

• Use la SLA número 6 para IPv6.

D1>enable	Ingresamos al modo privilegiado
D1#configure terminal	Ingresamos a la configuración del terminal
D1(config)# ip sla 4	Se le asigna el nombre al seguidor del servidor a configurar
D1(config-ip-sla)# icmp-echo 10.0.10.1	Relacionamos la dirección IP a configurar

Las IP SLAs probarán la disponibilidad de la interfaz R1 G0/0/1 cada 5 segundos.

D1(config-ip-sla-echo)# frequency 5

D1(config-ip-sla-echo)# exit

Luego realizamos el mismo código para Ipv6

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

Programe la SLA para una implementación inmediata sin tiempo de finalización.

D1(config-ip-sla)# ip sla schedule 4 life forever start-time now Definimos el tiempo de inicio para que conserve su configuración.

D1(config-ip-sla)# ip sla schedule 6 life-forever start-time now

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.

Para todos los objetos rastreados deben enviar la notificación 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.

D1(config-ip-sla)# track 4 ip sla 4 Comando que permite actualizar el estatus de los cambios en la configuración.

D1(config-ip-sla-track)# delay down 10 up 15 Declaramos el tiempo de respuesta para que se notifiquen los cambios y se actualicen.

D1(config-ip-sla-track)#exit

D1(config-ip-sla)# track 6 ip sla 6

D1(config-ip-sla-track)# delay down 10 up 15

D1(config-ip-sla-track)#exit

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

Se debe implementar el código de 4.1 pero en el switch D2:

Cree dos IP SLAs.

• Use la SLA número 4 para IPv4.

• Use la SLA número 6 para IPv6.

D2>enable /Ingresamos al modo privilegiado

D2#configure terminal Ingresamos a la configuración del terminal

D2(config)# ip sla 4 Nombramos el seguidor del servidor a configurar

D2(config-ip-sla)# icmp-echo 10.0.11.1 Ingresamos la dirección IP a configurar

Las IP SLAs probarán la disponibilidad de la interfaz R3 G0/0/1 cada 5 segundos.

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

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

Luego realizamos el mismo código para Ipv6

D2(config)# ip sla 6

D2(config-ip-sla)# icmp-echo 2001:db8:100:1010::1

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

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

Programe la SLA para una implementación inmediata sin tiempo de finalización.

D2(config-ip-sla)# ip sla schedule 4 life forever start-time now Con este comando damos inicio para que se mantenga implementada

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

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.

Para todos los objetos rastreados deben enviar la notificación a D1 si el estado de IP SLA cambia de Down a Up pasados los 10 segundos, o de Up a Down luego de 15 segundos.

D2(config-ip-sla)# track 4 ip sla 4 Comando que permite actualizar el estatus de los cambios en la configuración.

D2(config-ip-sla-track)# delay down 10 up 15 Declaramos el tiempo para que se notifiquen los cambios y se actualicen

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

D2(config-ip-sla)# track 6 ip sla 6

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

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

Nota: Para el caso del paso 4.1 y 4.2, debido a que el software Packet Tracer no soporta algunos comandos, no se pudo realizar la configuración, solo se documenta como muestra de que se realizan dichos pasos, sin poder dar evidencia de su funcionamiento en la simulación, pero en un escenario real si admite la configuración.

Tarea 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.

En este caso se utilizará el siguiente código:

D1(config)#interface vlan 100 Configuramos la interface Vlan

D1(config-if)#standby version 2	Configuramos HSRP en la Vlan
D1(config-if)#standby 104 ip 10.0.100.254	Asignamos la dirección IP virtual
D1(config-if)#standby 104 priority 150	Establecemos la prioridad en 150
D1(config-if)#standby 104 preempt	Configuramos la preferencia
D1(config-if)#standby 104 track 4 decrement 60	Configuración del rastreo del objeto y decremento 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.

Luego utilizamos el mismo código del paso anterior, y configuramos la Vlan 101, posteriormente cambiamos la dirección IP virtual

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

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.

Posteriormente utilizamos el mismo código del paso anterior, y configuramos la Vlan 102, y luego cambiamos la dirección IP virtual

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

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.

El mismo código que hemos utilizado en los pasos anteriores sirve para esta configuración, luego cambiamos la Vlan y la dirección IP virtual:

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

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.

Esta vez solo cambiamos el grupo y la Vlan y no se establece prioridad:

D1(config-if)#standby 116 ipv6 autoconfig

D1(config-if)# standby 116 preempt

D1(config-if)# standby 116 track 6 decrement 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.

Utilizamos la misma configuración, luego se cambia el grupo y la Vlan y luego se establece prioridad:

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

Tarea 4.4

En D2, configure HSRPv2.

Seguimos utilizando el mismo código de configuración de la tarea 4.3, pero esta vez cambiaremos las direcciones IP y Vlan según corresponda:

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.

D2(config)#interface vlan 100 Ingresamos al modo de configuración Vlan

D2(config-if)# standby version 2 Configuramos la HSRP en la Vlan

D2(config-if)# standby 104 ip 10.0.100.254 Asignamos la dirección IP virtual

D2(config-if)# standby 104 track 4 decrement 60 Configuramos el rastreo del Objeto y decremento 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.

Cambiamos la Vlan, la IP virtual y el grupo. Establecemos la prioridad 150:

D2(config-if)#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

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.

Esta vez solo cambiaremos la dirección Vlan y la IP virtual, sin dar prioridad:

D2(config-if)#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

Haciendo uso del mismo código, solo que ahora se configura la ipv6:

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.

D2(config-if)#standby 106 ipv6 autoconfig

D2(config-if)# standby 106 preempt

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

Cambiamos a ipv6 y se asigna prioridad a la vlan correspondiente:

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

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.

Ahora cambiamos la Vlan y el grupo:

D2(config-if)#standby 126 ipv6 autoconfig

D2(config-if)# standby 126 preempt

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

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. Configuración de seguridad

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.
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**.

Tarea 5.1, 5.2 y 5.3

En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT. Contraseña: cisco12345cisco

Detalles de la cuenta encriptada SCRYPT:

• Nombre de usuario Local: sadmin

• Nivel de privilegio 15

• Contraseña: cisco12345cisco

-Habilite AAA (no en R2).

Para la configuración de la seguridad utilizaremos el siguiente código en cada uno de los dispositivos:

R2>enable Ingresamos a modo privilegiado

R2#configure terminal Ingresamos a la configuración del terminal

R2(config)#enable password cisco12345cisco Asignamos la contraseña

R2(config)#service password-encryption Comando para encriptar la contraseña

R2(config)#exit Salida del modo configuración

R2(config)#enable secret level 15 cisco12345cisco Creamos los privilegios 15

R2(config)#username sadmin privilege 15 secret cisco12345cisco Creación de usuario y contraseña encriptada

Realizamos el mismo procedimiento en los demás dispositivos

R1>enable

R1#configure terminal

R1(config)#enable password cisco12345cisco

R1(config)#service password-encryption

R1(config)#enable secret level 15 cisco12345cisco

R1(config)#username sadmin privilege 15 secret cisco12345cisco

R1(config)#aaa new-model / se declara el modelo AAA

R3(config)#enable password cisco12345cisco

R3(config)#service password-encryption

R3(config)#enable secret level 15 cisco12345cisco

R3(config)#username sadmin privilege 15 secret cisco12345cisco

R3(config)#aaa new-model

D1(config)#enable password cisco12345cisco

D1(config)#service password-encryption

D1(config)#enable secret level 15 cisco12345cisco

D1(config)#username sadmin privilege 15 secret cisco12345cisco

D1(config)#aaa new-model

D2(config)#enable password cisco12345cisco

D2(config)#service password-encryption

D2(config)#enable secret level 15 cisco12345cisco

D2(config)#username sadmin privilege 15 secret cisco12345cisco

D2(config)#aaa new-model

Tarea 5.4, 5.5 y 5.6

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

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.

Cierre e inicie sesión en todos los dispositivos (except R2) con el usuario: raduser y la contraseña: upass123.

Para estos pasos utilizaremos los códigos:

R1(config)#aaa new-model Este es el modelo a configurar

R1(config)#radius server RADIUS Indicamos el servidor a configurar Radius

R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813

Asignamos la dirección IP y puertos del servidor Radius

R1(config-radius-server)#key $trongPass Asignamos la contraseña $trongPass

Usamos los mismos códigos para los demás dispositivos excepto R2:

R3(config)#aaa new-model

R3(config)#radius server RADIUS

R3(config-radius-server)#address ipv4 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

D2(config)#aaa new-model

D2(config)#radius server RADIUS

D2(config-radius-server)#address ipv4 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

D1(config)#aaa new-model

D1(config)#radius server RADIUS

D1(config-radius-server)#address ipv4 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

A1(config)#aaa new-model

A1(config)#radius server RADIUS

A1(config-radius-server)#address ipv4 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

Nota: Para el caso de los switches A1 y D1, los comandos utilizados no fueron aceptados por el software, debido a que muestra un error en la validación de estos códigos, sin embargo, en la práctica se utilizan y son validados por los equipos reales, esta falla se debe a que el Packet Tracer no soporta algunos comandos.

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. Configuración funciones de administración de red

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.

Tarea 6.1

En todos los dispositivos, configure el reloj local a la hora UTC actual.

Empezamos validando en los dispositivos la hora configurada con el código:

R1#show clock Comando para verificar la hora

Si se muestra una hora que no corresponda a la actual se configura con el código:

R1# clock set 20:01:23 Nov 26 2021 Configuramos la fecha y hora actual

Repetimos el código los demás dispositivos:

R2#clock set 20:00:00 Nov 26 2021

R3#clock set 20:00:00 Nov 26 2021

D2#clock set 20:00:00 Nov 26 2021

D1#clock set 20:00:00 Nov 26 2021

A1#clock set 20:00:00 Nov 26 2021

Tarea 6.2

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

En este paso se usará el siguiente comando:

R2(config)#ntp master 3 Configuramos NTP maestro en el nivel de estrato 3

Tarea 6.3, 6.4 y 6.5

Ahora utilizaremos los siguientes comandos:

R1(config)#ntp server 2.2.2.2 Configuramos la NTP

R1(config)#logging trap warning Syslogs en nivel warning

R1(config)#logging host 10.0.100.5 Envío a la PC1 en 10.0.100.5

R1(config)#logging on Cambiamos a estado encendido

R1(config)#ip access-list standard SNMP-NMS Configuración SNMP lectura

R1(config-std-nacl)#permit host 10.0.100.5 Declaramos límite de acceso

R1(config-std-nacl)#exit

R1(config- snmp)#snmp-server contact Cisco AlejandroZ Valor de contacto SNP

R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS

R1(config- snmp)#snmp-server host 10.0.100.5 versión 2c ENCORSA

R1(config- snmp)#snmp-server ifindex persist Habilita el envío de traps

R1(config- snmp)#snmp-server enable traps bgp Habilita el envío de traps bgp

R1(config- snmp)#snmp-server enable traps config Habilita traps

R1(config- snmp)# snmp-server enable traps ospf Habilita el envío de traps osfp

R1(config- snmp)#end Finaliza la configuración

Ahora se usarán los mismos comandos en los demás dispositivos:

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)#snmp-server contact Cisco AlejandroZ
R3(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS
R3(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
R3(config- snmp)#snmp-server ifindex persist
R3(config- snmp)#snmp-server enable traps config
R3(config- snmp)#snmp-server enable traps ospf
R3(config- snmp)#end

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 AlejandroZ
D1(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA
D1(config- snmp)#snmp-server ifindex persist
D1(config- snmp)#snmp-server enable traps config
D1(config- snmp)#snmp-server enable traps ospf
D1(config- snmp)#end

D2(config)#ntp server 10.0.10.1
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)#snmp-server contact Cisco AlejandroZ

D2(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS

D2(config- snmp)#snmp-server host 10.0.100.5 version 2c ENCORSA

D2(config- snmp)# snmp-server enable traps config

D2(config- snmp)#snmp-server enable traps ospf

D2(config- snmp)#end

A1(config)#ntp server 10.0.10.1

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 AlejandroZ

A1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS

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

A1(config- snmp)#snmp-server ifindex persist

A1(config- snmp)#snmp-server enable traps config

A1(config- snmp)#snmp-server enable traps ospf

A1(config- snmp)#end

Nota: En el paso anterior se muestran los comandos que son necesarios para llevar a cabo la configuración de los dispositivos reales, para el caso de la simulación no fue posible realizarlos debido a que el software no soporta algunos comandos, entre ellos el snmp-server, por lo tanto, no se pudo realizar este paso en la simulación.

CONCLUSIONES

Para la realización y montaje del escenario que ha sido sugerido en la guía de actividades se tuvo muchas dificultades con el software sugerido, puesto que luego de realizar la instalación de la máquina virtual y posterior carga da las IOS que contiene la imagen de los switches, no se logra acceder a la consola para realizar las configuraciones iniciales requeridas.

Se trata de configurar realizando varios cambios, entre ellos el aumento de la RAM, notándose un cambio favorable, pero persisten las fallas tanto en el funcionamiento de la máquina virtual, como del computador utilizado para la simulación, esto derivó en un daño al sistema operativo que causó el formateo e instalación nuevamente de los programas, luego de esto siguieron las fallas.

Se procede a realizar el montaje en Packet Tracer, el cual nos permite agregar los dispositivos necesarios para dar conformidad con la topología sugerida, se realiza el cableado y la conexión de los puestos en los diferentes slots, como Fast-Ethernet, Gigabyte, Puerto serial con su respectivo direccionamiento como se muestra en la tabla 1.

Se logra realizar las diferentes configuraciones como la capa 2, protocolo RSTP que permite el correcto direccionamiento de la red por medio de DHCP y SLAAC, dando el libre envío de paquetes entre los dispositivos; también se logra implementar la configuración de los protocolos OSPF para ipv4 e ipv6.

A pesar de que algunos comandos no son soportados por el software, se logra plantear el código que funciona correctamente en escenarios reales con dispositivos en físico, es por esto que se especifica en el documento que no se logra realizar en la simulación, pero se plantea para la implementación en la vida real.

BIBLIOGRAFIA

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). OSPF v3. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Multiple Spanning Tree Protocol. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). VLAN Trunks and EtherChannel Bundles. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Wireless Signals and Modulation. CCNP and CCIE Enterprise Core ENCOR 350-401. Recuperado de https://1drv.ms/b/s!AAIGg5JUgUBthk8

Granados, G. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167

Granados, G. (2019). Registro y acceso a la plataforma Cisco CCNP [OVI]. Recuperado de https://repository.unad.edu.co/handle/10596/24419

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC