DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN DAVID MARTINEZ PARRA

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN DAVID MARTINEZ PARRA

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

DIRECTOR:

Msc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma jurado

_____
Firma jurado

Aguachica, Diciembre 06 de 2021

AGRADECIMIENTOS

Primero que todo darles las gracias Dios por permitirme estar en este curso de profundización cisco CCNP a mi tutor que estuvo acompañándome en todo momento, me ayudo a corregir errores, mejorar mi desempeño en el curso, siempre estuvo allí, a mis compañeros del curso y del grupo de Skype, en el cual todos nos apoyábamos y nos colaborábamos. Quiero también darle gracias a mis padres y esposa que me han apoyado para poder terminar mi carrera de ingeniería de telecomunicaciones.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

SWITCH: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet o IEEE 802.3 y este también se le conoce por que proporciona conectividad nivel dos dentro de los tipos de modelo que existen.

ROUTER: Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red. Este dispositivo o enrutador opera en capa 3 y permite que varios ordenadores compartan información o tengan acceso a internet, pero para realizar todas estas funciones se valen de protocolos de enrutamientos creados para cada modelo ya sea OSI o TCP/IP.

ENRUTAMIENTO: El encaminamiento, enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

DHCP: El protocolo de configuración dinámica de host es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

SLAAC: La configuración automática de dirección sin estado es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e información de la dirección de gateway predeterminado de un router IPv6 sin utilizar un servidor de DHCPv6.

RESUMEN

En este trabajo final del diplomado de profundización CCNP, se pusieron a prueba los conocimientos obtenidos en todo el curso, desarrollando una topología de una red completa, utilizando 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), 3 Routers (Cisco 4221 con Cisco IOS XE versión 16.9.4 imagen universal o comparable) y 4 pc. Se realiza la simulación de una red de una compañía, utilizando protocolos de enrutamiento, configurando diferentes tipos de Vlan, configurando la seguridad de los dispositivos, se configura Configurar la capa 2 de la red y el soporte de Host, se utilizan direccionamiento DHCP, SLAAC y estático en cada una de las Vlan y dispositivos de la red de la compañía. Los protocolos de enrutamiento que más se utilizan son IPV4 y IPV6 y también se quiere que la compañía pueda administrar los dispositivos instalado de diferentes formas.

En este trabajo final se quiere demostrar las habilidades prácticas como ingeniero de telecomunicaciones de la universidad nacional abierta y a distancia (UNAD), configurando una topología de red de una compañía la cual consta de una red bastante compleja, en esta nos permite operar, administra la misma y así poder proveer servicios de telecomunicaciones a la empresa.

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

ABSTRACT

In this final work of the CCNP deepening diploma, the knowledge obtained throughout the course was put to the test, developing a topology of a complete network, using 2 Switches (Cisco 3650 with Cisco IOS XE version 16.9.4 universal or comparable image), 1 Switch (Cisco 2960 with Cisco IOS version 15.2 lanbase image or comparable), 3 Routers (Cisco 4221 with Cisco IOS XE version 16.9.4 universal image or comparable) and 4 pc. The simulation of a company network is performed, using routing protocols, configuring different types of Vlan, configuring the security of the devices, configuring Layer 2 of the network and Host support, using DHCP, SLAAC addressing and static in each one of the Vlan and devices of the network of the company. The routing protocols that are most used are IPV4 and IPV6 and the company also wants to be able to manage the installed devices in different ways.

In this final work we want to demonstrate the practical skills as a telecommunications engineer of the national open and distance university (UNAD), configuring a network topology of a company which consists of a rather complex network, in this it allows us to operate, manage the itself and thus be able to provide telecommunications services to the company.

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

INTRODUCCIÓN

Cisco CCNP tiene alta cantidad de información básica y avanzada para configuración e implementación de redes en áreas locales y de amplia cobertura, para la crear diseños avanzados y puedan ser utilizadas en redes escalables de las cuales mucha ISP prestan sus servicios. También se pueden construir topologías de las cuales se pueden monitorear, detectar problemas y poderlos solucionar.

Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking de los cuales estos conocimientos se adquirieron en todo el semestre temas relacionados con protocolos de enrutamiento BGP, EIGRP, OSPF, y direccionamiento de rutas, Dynamic Multi VPN, protocolos en IPv4 y protocolo en IPV6, etc. Este módulo CCNP se quiere mostrar conceptos principales interfaces de swtiches, VLANs, troncales y loopback que es una interfaz de red virtual.

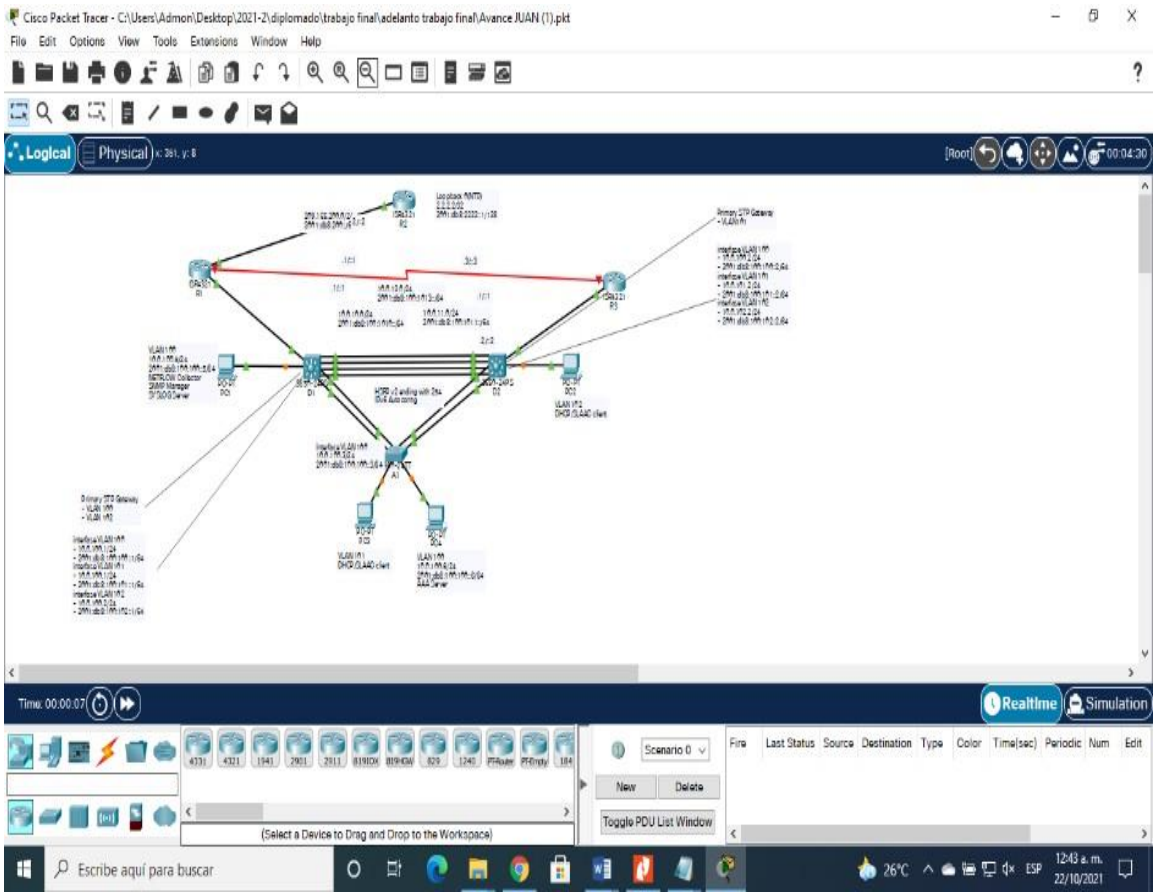
En este documento final se requiere implementar una topología de red en una institución, simulándola mediante GNS3 o Packet Tracer con el fin de demostrar las habilidades aprendida en este curso de profundización, utilizando los materiales teóricos practico que la universidad nacional abierta y a distancia UNAD nos brindó junto a la plataforma de cisco.

1. DESARROLLO DEL ESCENARIO PROPUESTO TOPOLOGIA DE RED.

PARTE 1: CONSTRUIR LA RED Y CONFIGURAR LOS AJUSTES BÁSICOS DE CADA DISPOSITIVO Y EL DIRECCIONAMIENTO DE LAS INTERFACES.

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

Figura 1. Topología cableada



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:

Tabla 1.Tabla de direccionamiento en toda la topología.

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-
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

Configuración de Router R1

R1>enable R1#configure terminal
R1(config)#hostname R1
R1(config)#line con 0
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config-line)#exit

Configuración de g0/0/0 R1

R1(config)#ipv6 unicast-routin
R1(config)#no ip domain lookup
R1(config)#interface g0/0/0
R1(config-if)#ip address 209.165.200.225 255.255.255.224

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

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

R1(config-if)#no shutdown

Configuración de g0/0/0 R1

R1(config)#interface g0/0/1

R1(config-if)#ip address 10.0.10.1 255.255.255.0

R1(config-if)#ipv6 address fe80::1:2 link-local

R1(config-if)#ipv6 address 2001:db8:100:1010::1/64

R1(config-if)#no shutdown

Configuración de Router R2

Configuración de R2 y g0/0/0

R2>enable
R2#configure terminal
R2(config)#ipv6 unicast-routing
R2(config)#no ip domain lookup
R2(config)#line con 0
R2(config-line)#exec-timeout 0 0

R2(config-line)#logging synchronous

R2(config-line)#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

Configuración de loopback 0

R2(config)#interface loopback 0

%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#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

Configuración de Router R2

R3>enable

R3#configure terminal

Enter configuration commands, one per line. End with

CNTL/Z. R3(config)#ipv6 unicast-routing

R3(config)#no ip domain lookup

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)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R3(config-if)#exit

NOTA: Los códigos mostrados anterior mente nos permitio montar la configuracion global para cada dispositivo y se configuro los parámetros básicos de la topología de red.

Switch D1

D1> D1>enable D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. D1(config)#ip routing
D1(config)#ipv6 unicast-routing
D1(config)#no ip domain lookup
D1(config)#banner motd # D1

Configuración de line y Vlans

D1(config)#line con 0
D1(config-line)#exec-timeout 0 0
D1(config-line)#logging synchronous
D1(config-line)#exit

D1(config)#vlan 100
D1(config-vlan)#name Management
D1(config-vlan)#exit

D1(config)#vlan 101
D1(config-vlan)#name UserGroupA
D1(config-vlan)#exit

D1(config)#vlan 102
D1(config-vlan)#name UserGroupB
D1(config-vlan)#exit

D1(config)#vlan 999
D1(config-vlan)#name NATIVE
D1(config-vlan)#exit

Configuración de g1/0/11

D1(config)#interface g1/0/11
D1(config-if)#no switchport
D1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/11, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/11, changed state to up

D1(config-if)#ip address 10.0.10.2 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address 2001:db8:100:1010::2/64
D1(config-if)#no shutdown
D1(config-if)#exit

Configuración de VLANS

D1(config)#interface vlan 100
D1(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up
D1(config-if)#ip address 10.0.100.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:1 link-local
D1(config-if)#ipv6 address fe80::d1:2 link-local
D1(config-if)#ipv6 address 2001:db8:100:100::1/64
D1(config-if)#no shutdown
D1(config-if)#
D1(config-if)#exit

D1(config)#interface vlan 101
D1(config-if)#
%LINK-5-CHANGED: Interface Vlan101, changed state to up
D1(config-if)#ip address 10.0.101.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:3 link-local
D1(config-if)#ipv6 address 2001:db8:100:101::1/64
D1(config-if)#no shutdown
D1(config-if)#exit

```
D1(config)#interface vlan 102
D1(config-if)#
%LINK-5-CHANGED: Interface Vlan102, changed state to up
D1(config-if)#ip address 10.0.102.1 255.255.255.0
D1(config-if)#ipv6 address fe80::d1:4 link-local
D1(config-if)#ipv6 address 2001:db8:100:102::1/64
D1(config-if)#no shutdown
D1(config-if)#exit

D1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.109
D1(config)#ip dhcp excluded-address 10.0.101.141 10.0.101.254
D1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.109
D1(config)#ip dhcp excluded-address 10.0.102.141 10.0.102.254
D1(config)#ip dhcp pool vlan-101

D1(dhcp-config)#network 10.0.101.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.101.254
D1(dhcp-config)#exit
D1(config)#

D1(config)#ip dhcp pool vlan-102
D1(dhcp-config)#network 10.0.102.0 255.255.255.0
D1(dhcp-config)#default-router 10.0.102.254
D1(dhcp-config)#exit
D1(config)#
```

Switch D2

```
D2>enable
D2#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. D2(config)#ip routing
D2(config)#ipv6 unicast-
routing D2(config)#no ip
domain lookup
D2(config)#exit
D2#
%SYS-5-CONFIG_I: Configured from console by console
```

```
D2#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z. D2(config)#line con 0
D2(config-line)#exec-timeout 0 0
D2(config-line)#
D2(config-line)#logging synchronous
D2(config-line)#exit
D2(config)#vlan 100
D2(config-vlan)#name Management
D2(config-vlan)#exit
D2(config)#vlan 101
D2(config-vlan)#name UserGroupA
D2(config-vlan)#exit
D2(config)#vlan 102
D2(config-vlan)#name UserGroupB
D2(config-vlan)#exit
D2(config)#vlan 999
D2(config-vlan)#name NATIVE
D2(config-vlan)#exit

D2(config)#interface g1/0/11
D2(config-if)#no switchport
D2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/11, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/11, changed state to up

D2(config-if)#ip address 10.0.11.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:1 link-local
D2(config-if)#ipv6 address 2001:db8:100:1011::2/64

D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
D2(config)#
D2(config)#interface vlan 100
```

```
D2(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

D2(config-if)#ip address 10.0.100.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:2 link-local
D2(config-if)#ipv6 address 2001:db8:100:103::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 101
%LINK-5-CHANGED: Interface Vlan101, changed state to up

D2(config-if)#ip address 10.0.101.2 255.255.255.0
D2(config-if)#ipv6 address fe80::d2:3 link-local
D2(config-if)#ipv6 address 2001:db8:100:101::2/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#
D2(config)#interface vlan 102

%LINK-5-CHANGED: Interface Vlan102, changed state to up

D2(config-if)#ip address 10.0.102.1 255.255.255.0
D2(config-if)#ipv6 address fe80::d1:4 link-local
D2(config-if)#ipv6 address 2001:db8:100:102::1/64
D2(config-if)#no shutdown
D2(config-if)#exit
D2(config)#

D2(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.209
D2(config)#ip dhcp excluded-address 10.0.101.241 10.0.101.254
D2(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.209
D2(config)#ip dhcp excluded-address 10.0.102.241 10.0.102.254
D2(config)#ip dhcp pool vlan-101
D2(dhcp-config)#network 10.0.101.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.101.254
D2(dhcp-config)#exit
D2(config)#
```

D2(config)#ip dhcp pool vlan-102
D2(dhcp-config)#network 10.0.102.0 255.255.255.0
D2(dhcp-config)#default-router 10.0.102.254
D2(dhcp-config)#exit
D2(config)#

Switch A1

A1>enable

A1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z. A1(config)#no ip domain lookup

A1(config)#line con 0

A1(config-line)#exec-timeout 0 0

A1(config-line)#logging synchronous

A1(config-line)#exit

A1(config)#vlan 100

A1(config-vlan)#name Management

A1(config-vlan)#exit

A1(config)#vlan 101
A1(config-vlan)#name UserGroupA
A1(config-vlan)#exit

A1(config)#vlan 102

A1(config-vlan)#name UserGroupB
A1(config-vlan)#exit
A1(config)#vlan 999

A1(config-vlan)#name NATIVE
A1(config-vlan)#exit
A1(config)#interface vlan 100

%LINK-5-CHANGED: Interface Vlan100, changed state to up

NOTA: con los codigos anteriores se habilitaron los dispositivos, se nombran los switch, se inabilita la búsqueda de DNS, se le acceso a direccionamiento ipv6, se ingresa al modo configuración 0, se le coloca un tiempo de inactividad y el no desplazamiento. Esto se lñe hace a cada dispositivo es decir a cada switch se nombra las vlan, se configuran como una interfaz y el rango de ellas.

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

R1

R1#copy running-config startup-config Destination filename [startup-config]?

Building configuration...

[OK]

R1#sh start

Using 700 bytes

R2

R2#copy running-config startup-config Destination filename [startup-config]?

Building configuration...

[OK]

R2#sh start

Using 713 bytes

R3

R3#copy running-config startup-config Destination filename [startup-config]?

Building configuration...

[OK]

R3#sh start

Using 700 bytes

D1

D1#copy running-config startup-config Destination filename [startup-config]?

Building configuration...

[OK]

D1#sh start

Using 1341 bytes

D2

D2#copy running-config startup-config Destination filename [startup-config]?

Building configuration...

[OK]

D2#sh start

Using 1341 bytes

A1

A1#copy running-config startup-config Destination filename [startup-config]?

Building configuration...

[OK]

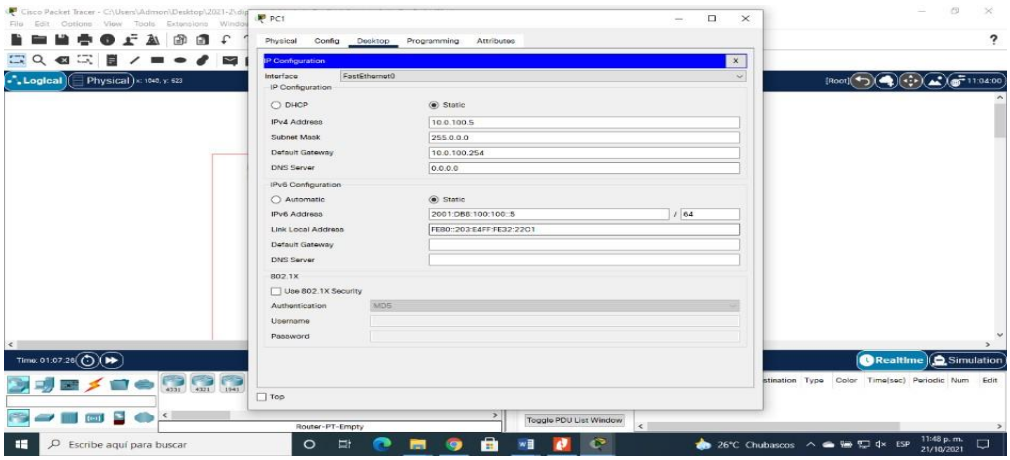
A1#sh start

Using 1076 bytes

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.

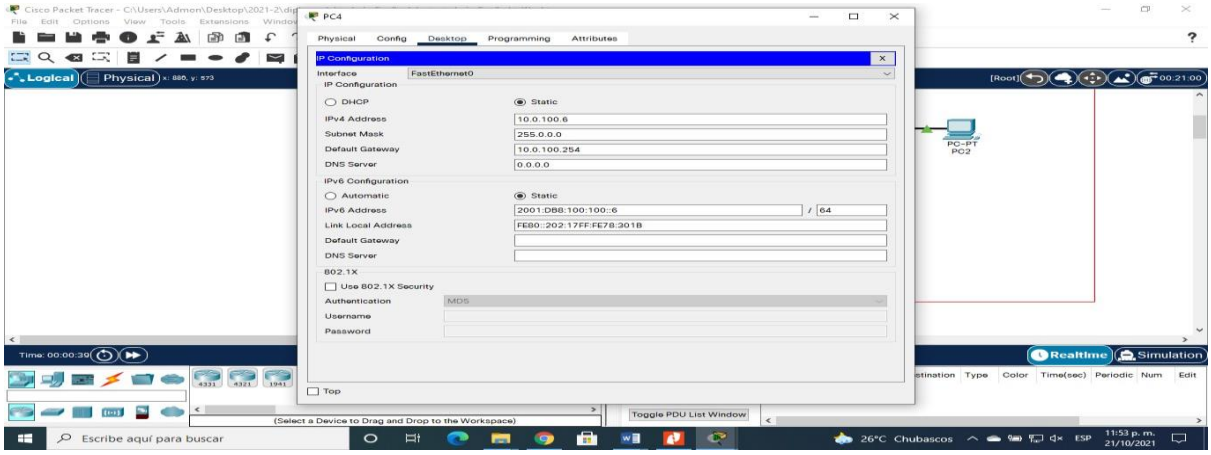
PC1

Figura 2. Direccionamiento IP PC1



PC4

Figura 3. Direccionamiento IP 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.

Tabla 2. Configurar la capa 2 de la red y el soporte de Host

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

		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

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(config)#interface Gig1/0/3

D1(config-if)#switchport mode access

D1(config-if)#switchport access vlan 100

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

D1(config-if)#interface Gig1/0/1

D1(config-if)#switchport mode access

D1(config-if)#switchport access vlan 101

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up

D1(config-if)#interface Gig1/0/2

D1(config-if)#switchport mode access

D1(config-if)#switchport access vlan 102

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/2 (1), with D2 GigabitEthernet1/0/2 (102).

D1(config-if)#switchport access vlan 102

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up

D1(config-if)#interface Gig1/0/4

D1(config-if)#switchport mode access

D1(config-if)#switchport access vlan 999

D2(config)#interface Gig1/0/3

D2(config-if)#switchport mode access

D2(config-if)#switchport access vlan 100

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/3 (1), with D1 GigabitEthernet1/0/3 (100).

D2(config-if)#switchport access vlan 100

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

D2(config-if)#interface Gig1/0/1

D2(config-if)#switchport mode access

D2(config-if)#switchport access vlan 101

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
GigabitEthernet1/0/1 (1), with D1 GigabitEthernet1/0/1 (101).

D2(config-if)#switchport access vlan 101

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up

D2(config-if)#interface Gig1/0/2

D2(config-if)#switchport mode access

D2(config-if)#switchport access vlan 102

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up

D2(config-if)#interface Gig1/0/4

D2(config-if)#switchport mode access

D2(config-if)#switchport access vlan 999

D1 and A1

A1(config-if)#interface Fa0/1
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 101
D1(config)#interface Gig1/0/5
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 101

A1(config-if)#interface Fa0/2
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 100

D1(config)#interface Gig1/0/6
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 100

D2 and A1

A1(config-if)#interface Fa0/3
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 102

D2(config)#interface Gig1/0/6
D2(config-if)#switchport mode access
D2(config-if)#switchport access vlan 102

A1(config-if)#interface Fa0/4
A1(config-if)#switchport mode access
A1(config-if)#switchport access vlan 999

D1(config)#interface Gig1/0/6
D1(config-if)#switchport mode access
D1(config-if)#switchport access vlan 999

2.3 En todos los switches habilite el protocolo Rapid Spanning–Tree (RSTP)

D1# show run | include spanning-
tree spanning-tree mode rapid-

pvst spanning-tree extend system-
id
spanning-tree vlan 100,102 priority
24576 spanning-tree vlan 101 priority
28672 spanning-tree port£fast|

2.4 Configure D1 y D2 como raíz (root) para las VLAN apropiadas, con prioridades de apoyo mutuo en caso de falla del switch

D1(config)#spanning-tree vlan 100 root primary
D1(config)#spanning-tree vlan 101 root primary
D1(config)#spanning-tree vlan 102 root secondary
D1(config)#spanning-tree vlan 999 root secondary
D1(config)#spanning-tree vlan 100 priority 4096
D1(config)#spanning-tree vlan 101 priority 4096
D1(config)#exit

D1#show running-config | include span spanning-tree mode rapid-pvst
spanning-tree vlan 100-101 priority 4096
spanning-tree vlan 102,999 priority 28672
D2(config)#spanning-tree vlan 100 root primary
D2(config)#spanning-tree vlan 101 root primary
D2(config)#spanning-tree vlan 102 root secondary
D2(config)#spanning-tree vlan 999 root secondary
D2(config)#
D2(config)#spanning-tree vlan 100 priority 4096
D2(config)#spanning-tree vlan 101 priority 4096
D2(config)#exit
D2#show running-config | include span spanning-tree mode rapid-pvst

spanning-tree vlan 100-101 priority 4096
spanning-tree vlan 102,999 priority 28672

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(config)#int rang Gig1/0/1-4
D1(config-if-range)#channel-protocol lacp
D1(config-if-range)#channel-port 12 mode active

^
% Invalid input detected at '^' marker. D1(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down

D1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
D1(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down

D1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up

D1(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

D1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

D1(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to down

D1(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up

D1#show etherchannel summary Flags: D - down P - in port-channel I - stand-alone s - suspended
H - Hot-standby (LACP only) R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator u - unsuitable for bundling
w - waiting to be aggregated d - default port

Number of channel-groups in use: 3
Number of aggregators: 3

Group Port-channel Protocol Ports
------+-------------+-----------+---

1 Po1(SD) -
3 Po3(SD) - Gig1/0/5(s) Gig1/0/6(s)
12 Po12(SD) LACP Gig1/0/1(I) Gig1/0/2(I) Gig1/0/3(I) Gig1/0/4(I)

D2(config)#int rang Gig1/0/1-4
D2(config-if-range)#channel-protocol lacp
D2(config-if-range)#channel-group 1 mode passive

Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/1 is not compatible with Po1 and will be suspended (access vlan of Gig1/0/1 is 101,Po1 is 1)

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/2 is not compatible with Po1 and will be suspended (access vlan of Gig1/0/2 is 102,Po1 is 1)

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/3 is not compatible with Po1 and will be suspended (access vlan of Gig1/0/3 is 100,Po1 is 1)

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/4 is not compatible with Po1 and will be suspended (access vlan of Gig1/0/4 is 999,Po1 is 1)

D2(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down

D2(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up

D2(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/4, changed state to down

D2(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up

D2(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

D2(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

D2(config-if-range)#
%LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to down
D2(config-if-range)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

D2(config-if-range)#
D2#show etherchannel summary Flags: D - down P - in port-channel I - stand-alone s - suspended
H - Hot-standby (LACP only) R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated d - default port

Number of channel-groups in use: 2
Number of aggregators: 2

Group Port-channel Protocol Ports
------+-------------+-----------+---
1 Po1(SD) -
12 Po12(SD) LACP Gig1/0/1(I) Gig1/0/2(I) Gig1/0/3(I) Gig1/0/4(I)

D1 a A1 – Port channel 1

D1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#interface range g1/0/5-6
D1(config-if-range)#channel-group 1 mode active
D1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/5 is not compatible with Po3 and will be suspended (access vlan of Gig1/0/5 is 101,Po3 is 1)

%LINEPROTO-5-UPDOWN:
changed state to up Line protocol on Interface GigabitEthernet1/0/6,

%LINEPROTO-5-UPDOWN: changed state to down Line protocol on Interface GigabitEthernet1/0/6,
%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po3 and will be suspended (access vlan of Gig1/0/6 is 100,Po3 is 1)

A1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
A1(config)#interface range Fa0/1-2
A1(config-if-range)#channel-group 1 mode passive
A1(config-if-range)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

A1(config-if-range)#

D2 a A1 – Port channel 2

D2(config)#interface range g1/0/5-6
D2(config-if-range)#channel-group 2 mode active
D2(config-if-range)#
Creating a port-channel interface Port-channel 2

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/5 is not compatible with Po2 and will be suspended (access vlan of Gig1/0/5 is 102,Po2 is 1)

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/6, changed state to down

%EC-5-CANNOT_BUNDLE2: Gig1/0/6 is not compatible with Po2 and will be suspended (access vlan of Gig1/0/6 is 999,Po2 is 1)

A1(config)#interface range Fa0/3-4
A1(config-if-range)#channel-group 2 mode passive
A1(config-if-range)#
Creating a port-channel interface Port-channel 2

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

A1(config-if-range)#

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.

D2# show run interface gl1/0/23
Building configuration...
Current configuration : 115 bytes interface GigabitEthernet1/0/23
switchport access vlan 102
switchport mode access spanning-tree portfast|

A1# show run interface £0/23
Building configuration...
Current configuration : 115 bytes interface FastEthernet0/23
switchport access vlan 101
switchport mode access spanning-tree portfast edge end

Al# show run interface £0/24
Building configuration...
Current configuration : 115 bytes interface FastEthernet0/24
switchport access vlan 100 switchport mode access

epanningzeres portfast edge

2.7 Verifique los servicios DHCP IPv4.

PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

IPv4 PC2 = 10.0.102.210

IPv4 PC3 = 10.0.101.110
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

Packet Tracer PC Command Line 1.0
C:\>ping 10.0.100.1

Pinging 10.0.100.1 with 32 bytes of data:

Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.100.2

Pinging 10.0.100.2 with 32 bytes of data:

Reply from 10.0.100.2: bytes=32 time=1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.100.6

Pinging 10.0.100.6 with 32 bytes of data:

Reply from 10.0.100.6: bytes=32 time=11ms TTL=128
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128
Reply from 10.0.100.6: bytes=32 time<1ms TTL=128
Reply from 10.0.100.6: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.100.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 11ms, Average = 3ms

PC2 debería hacer ping con éxito a:
D1: 10.0.102.1
D2: 10.0.102.1
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.102.1

Pinging 10.0.102.1 with 32 bytes of data:

Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time=15ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.102.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 15ms, Average = 3ms

C:\>ping 10.0.102.1

Pinging 10.0.102.1 with 32 bytes of data:

Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.102.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC3 debería hacer ping con éxito a:
D1: 10.0.101.1
D2: 10.0.101.2

Packet Tracer PC Command Line 1.0
C:\>ping 10.0.101.1

Pinging 10.0.101.1 with 32 bytes of data:

Reply from 10.0.101.1: bytes=32 time=2ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.101.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 2ms, Average = 0ms C:\>ping 10.0.101.2
Pinging 10.0.101.2 with 32 bytes of data:

Reply from 10.0.101.2: bytes=32 time=1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time=12ms TTL=255
Reply from 10.0.101.2: bytes=32 time=15ms TTL=255

Ping statistics for 10.0.101.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 15ms, Average = 7ms

PC4 debería hacer ping con éxito a:
D1: 10.0.100.1
D2: 10.0.100.2
PC1: 10.0.100.5

Packet Tracer PC Command Line 1.0
C:\>ping 10.0.100.1

Pinging 10.0.100.1 with 32 bytes of data:

Reply from 10.0.100.1: bytes=32 time=1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time<1ms TTL=255
Reply from 10.0.100.1: bytes=32 time=3ms TTL=255

Ping statistics for 10.0.100.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 10.0.100.2

Pinging 10.0.100.2 with 32 bytes of data:

Reply from 10.0.100.2: bytes=32 time=1ms TTL=255
Reply from 10.0.100.2: bytes=32 time=1ms TTL=255
Reply from 10.0.100.2: bytes=32 time=16ms TTL=255
Reply from 10.0.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.100.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 16ms, Average = 4ms
C:\>10.0.100.5
Invalid Command. C:\>ping 10.0.100.5

Pinging 10.0.100.5 with 32 bytes of data:

Reply from 10.0.100.5: bytes=32 time=1ms TTL=128
Reply from 10.0.100.5: bytes=32 time=1ms TTL=128
Reply from 10.0.100.5: bytes=32 time<1ms TTL=128
Reply from 10.0.100.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.100.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms

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.

Use OSPF Process ID 4 y asigne los siguientes router- IDs:

Tabla 3. Configuración de los protocolos de enrutamiento

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
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

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).
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:

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

R1: 0.0.4.1

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 4
R1(config-router)#router-id 0.0.4.1
R1(config-router)# network 10.0.10.0 0.0.0.255 area 0
R1(config-router)# network 10.0.13.0 0.0.0.255 area 0
R1(config-router)# default-information originate /    se declara información predeterminada
R1(config-router)#exit
```

R3: 0.0.4.3
R3>enable
R3#conf term

Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
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
R3(config-router)#exit

D1: 0.0.4.131
D1>enable
D1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)# network 10.0.10.0 0.0.0.255 area 0
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)#passive-interface default / se deshabilita las publicaciones OSPFv2
D1(config-router)#no passive-interface g1/0/11
D1(config-router)#exit

D2: 0.0.4.132
D2>enable
D2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)# network 10.0.11.0 0.0.0.255 area 0
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)#passive-interface default / se deshabilita las publicaciones OSPFv2
D2(config-router)#no passive-interface g1/0/11
D2(config-router)#exit

3.2 Use OSPF Process ID 6 y asigne los siguientes routerIDs:

R1: 0.0.6.1

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ipv6 router ospf 6
R1(config-router)#router-id 0.0.6.1
R1(config-router)# default-information originate / se declara información predeterminada
R1(config-router)#exit / se sale del modo configuracion
R1(config)#int g0/0/1 / se declara la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0 / se asigna área 0 en ipv6
R1(config-if)#exit / se sale del modo configuracion
R1(config)#int s0/1/0 / se declara la interfaz a configurar
R1(config-if)#ipv6 ospf 6 area 0 / se asigna área 0 en ipv6
R1(config-router)#exit
```

R3: 0.0.6.3

```
R3>enable
R3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# ipv6 router ospf 6
R3(config-router)# router-id 0.0.6.3
R3(config-router)#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
```

D1: 0.0.6.131

```
D1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D1(config)#ipv6 router ospf 6
D1(config-router)#router-id 0.0.6.131
D1(config-router)#passive-interface default
D1(config-router)#no passive-interface Gig1/0/11
D1(config-router)#exit
D1(config)# interface g1/0/11
D1(config-if-range)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

D1(config)#int vlan 100
D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int vlan 101
D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit
D1(config)#int vlan 102
D1(config)#ipv6 ospf 6 area 0
D1(config-if)#exit

D2: 0.0.6.132

D2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
D2(config)# ipv6 router ospf 6
D2(config-router)#router-id 0.0.6.132
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface Gig1/0/11
D2(config-router)#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

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

R2>en / Se ingresa al modo privilegiado
R2#conf term / Se ingresa a configurar el terminal
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 0 / Se llama la interfaz a conf. Loopback 0
%Default route without gateway, if not a point-to-point interface, may impact performance

R2(config-if)# ipv6 route ::/0 loopback 0/ se establece los parámetros a configurar con ip y mascara de red, como indica el diagrama del escenario
Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2

R2#en / Se ingresa al modo privilegiado
R2#conf term / Se ingresa a configurar el terminal
R2(config)#router bgp 500 / se establece el router con bgp 500
R2(config-router)#bgp router-id 2.2.2.2 / se asigna el id 2.2.2.2

Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

R2(config-router)#neighbor 209.165.200.225 remote-as 300 / se define la relación vecino ipv4
R2(config-router)#neighbor 2001:db8:200::1/64 remote-as 300/ se define la relación vecino ipv6

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 / se llama a configurar 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 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#conf term / se ingresa a configuración de terminal
R1(config)#ip route 10.0.0.0 255.255.255.255 null0 / se configura interfaz null ipv4
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ip route 2001:db8:100::/48 null0 / interfaz null opv6

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

R1#conf term / se ingresa a la configuración de terminal
R1(config)#router bgp 300 / se asigna bgp y ns 300

R1(config-router)#bgp router-id 1.1.1.1 / se asigan 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 / define la relación vecino ipv4
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 209.165.200.226 Up
R1(config-router)#neighbor 2001:db8:200::2 remote-as 500 / se define 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
```

PARTE 4: CONFIGURAR LA REDUNDANCIA DEL PRIMER SALTO

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

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

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
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

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

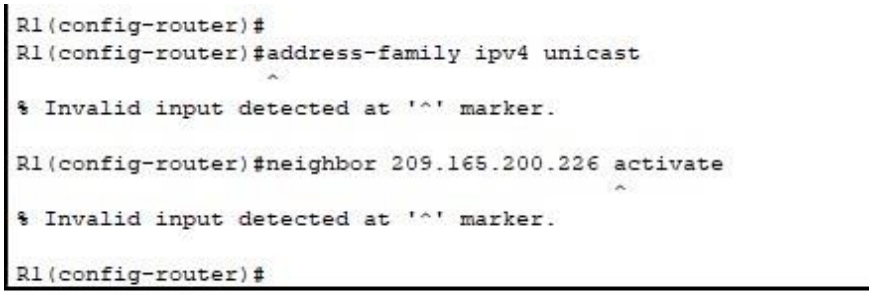
Tarea#	Tarea	Especificación
	En D2, configure HSRPv2.	D2 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150. Configure HSRP version 2. Configure IPv4 HSRP grupo **104** para la VLAN 100: Asigne la dirección IP virtual **10.0.100.254**. Habilite la preferencia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

4.1 Para la solución de esta se implementa el código: Cree dos IP SLAs.

Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6.

D1>en /se ingresa al modo global
D1#conf term /se ingresa a la configuración del dispositivo
D1(config)# ip sla 4 / se nombra el seguidor del servidor a configurar
D1(config-ip-sla)# icmp-echo 10.0.10.1 / se indica la ip a configurar

Figura 4. Se muestra la configuración IP sla 4



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

Se realiza 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 / se define el inicio y que se mantenga implementada.
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.

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.

D1(config-ip-sla)# track 4 ip sla 4 / es el que permite actualizar el estatus de los cambios en la conexión o configuracion.
D1(config-ip-sla-track)# delay down 10 up 15 / se declara el tiempo en el que actualiza los cambios o notifica.
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 Para la solución de esta se implementa el código de 4.1 pero en el terminal D2: Cree dos IP SLAs.

Use la SLA número 4 para IPv4.
Use la SLA número 6 para IPv6

D2>en / se ingresa al modo global
D2#conf term / se ingresa a la configuración del dispositivo
D2(config)# ip sla 4 / se nombra el seguidor del servidor a configurar
D2(config-ip-sla)# icmp-echo 10.0.11.1 / se indica la ip a configurar

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

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

Se realiza 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 / se define el inicio y 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

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.

D2(config-ip-sla)# track 4 ip sla 4 / es el que permite actualizar el estatus de los cambios en la conexión o configuracion.
D2(config-ip-sla-track)# delay down 10 up 15 / se declara el tiempo en el que actualiza los cambios o notifica.
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 la tarea 4.1 y 4.2 packet tracer no reconoce los comandos para realizar esta configuración debería implementarse en un ambiente real con los servidores físicos

4.3 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.

Para esto se utiliza el código:

D1(config)#interface vlan 100 / se ingresa a la vlan a configurar
D1(config-if)#standby version 2 /se configura HSRP en la vlan

D1(config-if)#standby 104 ip 10.0.100.254 /se asigna la ip virtual
D1(config-if)#
%HSRP-6-STATECHANGE: Vlan100 Grp 104 state Init -> Init
%HSRP-6-STATECHANGE: Vlan100 Grp 104 state Standby -> Active
D1(config-if)#standby 104 priority 150 /se establece prioridad en 150
D1(config-if)#standby 104 preempt /se configura como preferencia
D1(config-if)#standby 104 track 4 decrement 60 /se configura 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.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.

Se utiliza el código del paso anterior, y se configura la vlan 101, se cambia la 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)#
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Init -> Init
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan101 Grp 114 state Standby -> Active
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.

Se utiliza el código del paso anterior, y se configura la vlan 102, se cambia la 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)#
%HSRP-6-STATECHANGE: Vlan102 Grp 124 state Init -> Init
%HSRP-6-STATECHANGE: Vlan102 Grp 124 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan102 Grp 124 state Standby -> Active
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.

Para este paso continuamos utilizando el código de configuración anterior y se cambia a ipv6, se cambia la vlan y la ip virtual:

D1(config)#interface vlan 100
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.

Continuamos con los mismos pasos de configuración cambiando el grupo y la vlan y no se establece prioridad:

D1(config)#interface vlan 101
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.

Continuamos con los mismos pasos de configuración cambiando el grupo y la vlan y se establece prioridad:

D1(config)#interface vlan 102
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

4.4 En D2, configure HSRPv2.

Para esta tarea utilizamos el mismo código de configuración de la tarea 4.3 y cambiamos las vlan e ip 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 / se ingresa a la vlan a configurar
D2(config-if)# standby version 2 / se configura HSRP en la vlan
D2(config-if)# standby 104 ip 10.0.100.254 / se asigna la ip virtual
D2(config-if)# standby 104 preempt
D2(config-if)# standby 104 track 4 decrement 60 / se configura 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.

Utilizamos los códigos del paso inmediatamente anterior cambiando la vlan, la ip virtual y el grupo. Se establece 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

D2(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.
Habilite la preferencia (preemption).
Rastree el objeto 4 para disminuir en 60.

Continuamos con la serie de códigos utilizados en el paso anterior cambiando la vlan y la ip virtual en este paso no se establece 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

De acá en adelante se replica el código, pero 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)#interface vlan 100
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.

Utilizamos los comandos anteriores se cambia a ipv6 se determina prioridad a la vlan correspondiente:

D2(config-if)#interface vlan 101
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.

Continuamos con la serie de códigos de configuración cambiando la vlan y grupo:

D2(config-if)#interface vlan 102
D2(config-if)#standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
D2(config-if)# standby 126 track 6 decrement 60

Figura 5. Interfaces Vlans

```
!
interface Vlan100
 mac-address 0002.1654.d801
 ip address 10.0.100.2 255.255.255.0
 ipv6 address FE80::D2:2 link-local
 ipv6 address 2001:DB8:100:103::2/64
 ipv6 ospf 6 area 0
 standby version 2
 standby 104 ip 10.0.100.254
 standby 104 preempt
 standby 106 ipv6 autoconfig
 standby 106 preempt
!
interface Vlan101
 mac-address 0002.1654.d802
 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
 ipv6 ospf 6 area 0
 standby version 2
 standby 114 ip 10.0.101.254
 standby 114 priority 150
 standby 114 preempt
 standby 116 ipv6 autoconfig
 standby 116 priority 150
 standby 116 preempt
!
interface Vlan102
 mac-address 0002.1654.d803
 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
 ipv6 ospf 6 area 0
 standby version 2
 standby 124 ip 10.0.102.254
 standby 124 preempt
 standby 126 ipv6 autoconfig
 standby 126 preempt
!
```

PARTE 5: SEGURIDAD

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

Tabla 5. seguridad

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.
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
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**.

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 esta configuración de seguridad se debe ingresar a cada dispositivo y utilizar el siguiente código:

R2>en / se ingresa a modo privilegiado
R2#conf term / se ingresa a configurar terminal
R2(config)#enable password cisco12345cisco / se asigna contraseña a modo privilegiado
R2(config)#service password-encryption / se encripta la contraseña
R2(config)#exit / se sale del modo configuracion
R2(config)#enable secret level 15 cisco12345cisco / se crea sesión privilegio 15
R2(config)#username sadmin privilege 15 secret cisco12345cisco / se crea usuario y contraseña encriptada para el usuario.

R1>en
R1#conf term
Enter configuration commands, one per line. End with CNTL/Z. 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

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 utilizamos los códigos:

R1(config)#aaa new-model / llamamos el modelo a configurar
R1(config)#radius server RADIUS / se indica el servidor a configurar Radius
R1(config-radius-server)#address ipv4 10.0.100.6 auth-port 1812 acct-port 1813
/se asigna la dirección ip y puertos del servidor Radius
R1(config-radius-server)#key $trongPass / se asigna la contraseña $trongPass

Nota: número de puerto acct-port el cual especifica el Puerto de destino UDP no lo acepta, solo acepta hasta hasta el numero de puerto de autenticacion
Se replica los códigos de configuración para los demás dispositivos exepto 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
D1(config)#end

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: Los dispositivos D1, D2 no aceptan la configuración radius server RADIUS y el dispositivo A1 no acepta la configuración aaa new-model

En en los dispositivos A1 y D1 no fue posible realizar la configuración, ya que genera un error la configuración de packet tracer. cabe decir que estos son los códigos para utilizar en un escenario simulado.

PARTE 6: CONFIGURE LAS FUNCIONES DE ADMINISTRACIÓN DE RED

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

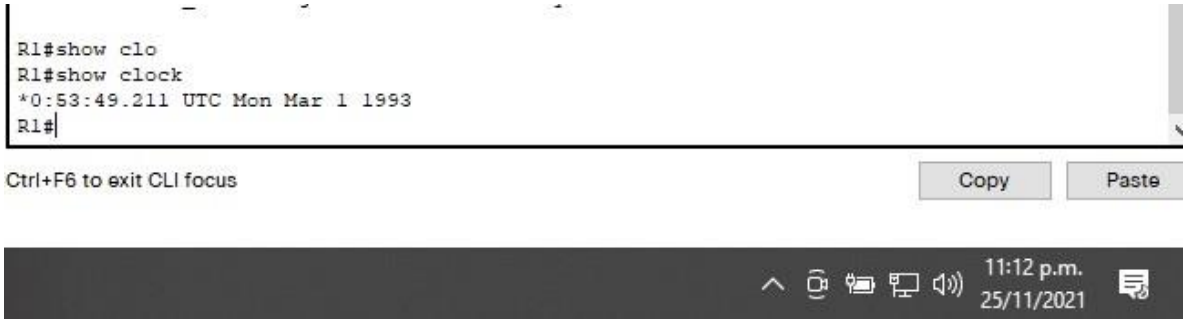
Tabla 6. Configure las funciones de Administración de Red

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*.

6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual. Para esto validamos en los dispositivos la hora configurada con el código:

R1#show clock / verificar la hora configurada

Figura 6. Verificación hora en los dispositivos



Como se evidencia que la hora no corresponde a la actual se configura con el código:

R1# clock set 23:13:00 25 Nov 2021 / se configura fecha y hora actual
R2#clock set 23:14:00 25 Nov 2021
R3#clock set 23:15:00 25 Nov 2021
D1#clock set 23:16:00 25 Nov 2021
D2#clock set 23:16:00 25 Nov 2021
A1#clock set 23:16:00 25 Nov 2021

Figura 7. Verificación de corrección de hora de dispositivos.

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

Para esto utilizamos el código:
R2(config)#ntp master 3 / se configura NTP maestro en el nivel de estrato 3

6.3, 6.4 y 6.5 Para esta parte utilizamos el código:

R1(config)#ntp server 2.2.2.2 / se configura NTP R1(config)#logging trap warning / Syslogs en nivel warning R1(config)#logging host 10.0.100.5 / enviarse a la PC1 en 10.0.100.5
R1(config)#logging on / se cambia a estado encendido
R1(config)#ip access-list standard SNMP-NMS / se cinfigura SNMP lectura
R1(config-std-nacl)#permit host 10.0.100.5 / se declara límite de acceso
R1(config-std-nacl)#exit

R1(config)#snmp-server community ENCORSA ro
R1(config- snmp)#snmp-server contact Cisco Juan / valor de contacto SNP
R1(config- snmp)#snmp-server community ENCORSA ro SNMP-NMS /se establece R1(config- snmp)#snmp-server host 10.0.100.5 versión 2c ENCORSA /se declara el host

R1(config- snmp)#snmp-server ifindex persist / se habilita el envío de traps
R1(config- snmp)#snmp-server enable traps bgp / se habilita el envío de traps bgp
R1(config- snmp)#snmp-server enable traps config / se habilita traps
R1(config- snmp)# snmp-server enable traps ospf / se habilita el envió de traps osfp
R1(config- snmp)#end /se finaliza la configuración

Se replica 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-server community ENCORSA ro
R3(config- snmp)#snmp-server contact Cisco Juan
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

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 community ENCORSA ro
D1(config)#snmp-server contact Cisco Juan
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

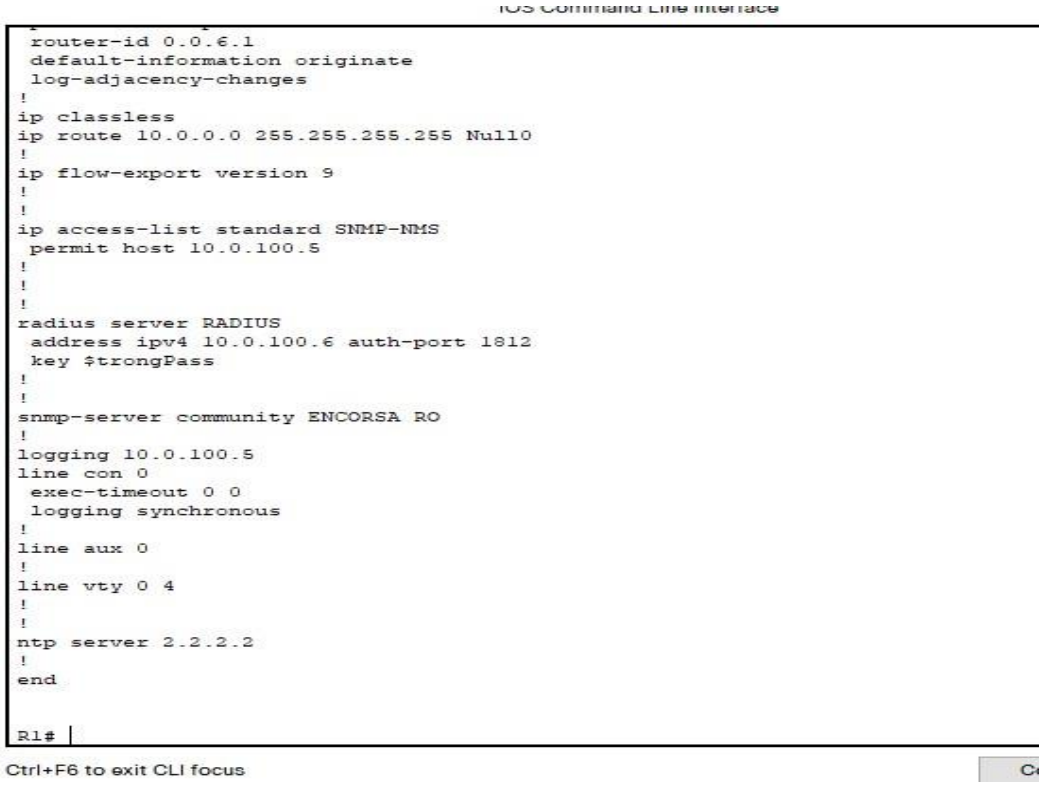
D2(config)#ntp server 10.0.10.1
D2(config)#logging trap warning
D2(config)#logging host 10.0.100.5
D2(config)#logging on
D2(config)#ip access-list standard SNMP-NMS
D2(config-std-nacl)#permit host 10.0.100.5
D2(config-std-nacl)#exit

D2(config)#snmp-server community ENCORSA ro
D2(config)#snmp-server contact Cisco Juan
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

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 community ENCORSA ro
A1(config)#snmp-server contact Cisco Juan
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

figura 8. Configura NTP maestro en el nivel de estrato 3



CONCLUSIONES

En este trabajo final, se realiza la configurando cada uno de los dispositivos utilizados para crear la topología de red completa propuesta por el tutor, se crearon vlans, se direccionaron las interfaces según sus parámetros, se configuro la capa 2 del soporte host, se asignaron unos protocolos de enrutamiento en estos dispositivos, se configuro la redundancia del primer salto, se le configuro la seguridad de cada uno de los dispositivos y por último se configuro las características de administración de red.

La simulación de dicha topología, se realizó en packet tracer, se realizaron las partes 1 , 2 , 3, 4, 5 y 6 del trabajo final. También se verifico la conectividad de los dispositivos simulados mediante los comandos ping, tracerouter, show ip route; este trabajo se realizó con el fin de cumplir con la unidad del periodo y llevar a cabo los conocimientos que hemos obtenido en el transcurso del diplomado de profundización.

El curso de CCNP me permitió obtener conocimientos avanzados de cómo se configura una ISP como la que nos presta estos servicios en nuestros hogares, de cómo es el funcionamiento y cuales problemas se nos pueden presentar y como solucionarlo.

Se implementó la topología con el fin de oponer en prácticas nuestras habilidades teóricas, con el fin de implementar los protocolos de enrutamiento IPV6 y IPV4 en cada uno de los dispositivos puestos por el director del curso y se implementaron ideas de administración de los mismos sistemas.

REFERENCIAS

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). IP Routing Essentials. CCNP and CCIE Enterprise Core ENCOR 350-401. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

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

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

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

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

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Secure Access Control. CCNP and CCIE Enterprise Core ENCOR 350-401. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8

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

Edgeworth, B., Garza Rios, B., Gooley, J., Hucaby, D. (2020). CISCO Press (Ed). Foundational Network Programmability Concepts. CCNP and CCIE Enterprise Core ENCOR 350-401. Disponible en https://1drv.ms/b/s!AAIGg5JUgUBthk8