DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FILEMAN URIBE BERNAL

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

FILEMAN URIBE BERNAL

Diplomado de opción de grado presentado para optar el título de Ingeniero de Telecomunicaciones

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Cali, 28 de noviembre del 2021

AGRADECIMIENTOS

Presento mi agradecimiento al director de este diplomado como opción de grado, el cual presento para optar por el título de Ingeniero de Telecomunicaciones, Dir. Héctor Julián Parra Mogollón por la consagración y apoyo que ha brindado a este trabajo, por el respaldo y acompañamiento a mis dudas e inquietudes, así como a la fomentación de las ideas, reflejadas con el conocimiento y dirección con que ha facilitado a las mismas. Agradezco la confianza prestada desde que inicie este diplomado.

De igual manera, agradezco a mis compañeros de la carrera de Ingeniería de Telecomunicaciones, por su apoyo personal y calidad humana, especialmente al grupo 18, con quienes he compartido mis avances de los proyectos e durante este tiempo de implementación.

Un diplomado genera una investigación exhaustiva, pero conlleva el fruto de ideas, proyectos y esfuerzos previos que corresponden al apoyo de otras personas. Que para este caso mi más sincero agradecimiento a la UNAD por facilitarme su tiempo y sus ideas plasmadas en documentaciones y apoyo con herramientas tecnológicas, para dar orientación y atención a mis dudas e inquietudes, además por el material facilitado y las sugerencias recibidas.

Finalmente, doy gracias a mi pareja y hermano, por su paciencia, comprensión y solidaridad con este proyecto, por el tiempo que me han concedido, un tiempo que no se dio a la historia familiar. Esto sin su apoyo no lo habría escrito y, por esas razones, este trabajo es también el suyo.

A todos, muchas gracias.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CCNP: decimos que es el nivel intermedio certificación, el cual ofrece la academia de Cisco. Para obtener esta certificación, se han de realizar varios exámenes, clasificados así:

módulos. 1. Enrutamiento (ROUTE), 2. Conmutación (SWITCH), 3. Resolución de problemas (TSHOOT)

OSPF: protocolo de enrutamiento jerárquico de pasarela interior, que usa el algoritmo de Dijkstra enlace-estado para calcular la ruta más corta. Emplea el “cost” como su medida de métrica. Además, construye una base de datos enlace-estado semejante en todos los router de la zona.

RED: agrupación de equipos informáticos y software conectados entre sí mediante dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

SWITCH: Es el dispositivo digital lógico de interconexión de equipos que maniobra en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finaliza la comunicación.

ROUTER: es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, se encarga de interconectar redes.

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local que no deberían intercambiar datos usando la red local.

RESUMEN

Como parte fundamental del diplomado CISCO CCNP, tenemos como objetivo para este estudio es determinar la configuración de plataformas de Conmutación basadas en Switch, mediante el uso de protocolos como STP y la configuración de Vlan en escenarios de red corporativos, para comprender el modo de operación de las subredes y los beneficios de administrar dominios de broadcast independientes, esto para múltiples escenarios al interior de una red jerárquica convergente, que se aplica para la Electrónica de Red, la cual es la parte de la infraestructura que nos permite interconectar ordenadores y periféricos utilizando principalmente dos tipos de equipos: Routers y Switches.

Para alcanzar el aprendizaje de enrutamiento usaremos los comandos IOS de configuración avanzada en routers (con direccionamiento IPv4 e IPv6) para protocolos de Enrutamiento como: OSPF, EIGRP y BGP, en entornos de direccionamiento sin clase, con el fin diseñar e implementar soluciones de red escalables, mediante el uso de los principios de enrutamiento y conmutación de paquetes en ambientes para Redes LAN y WAN.

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

ABSTRACT

As a fundamental part of the CISCO CCNP diplomat, our objective for this study is to determine the configuration of Switch-based Switching platforms, through the use of protocols such as STP and the configuration of VLANs in corporate Networking scenarios, to understand the mode of operation of the subnets and the benefits of managing independent broadcast domains, this for multiple scenarios within a convergent hierarchical network, which is applied to network Electronics, which is the part of the infrastructure that allows us to interconnect computers and peripherals using mainly two types of equipment: Routers and Switch.

To achieve the routing learning, we will use the advanced configuration IOS commands in routers (with IPv4 and IPv6 addressing) for routing protocols such as: OSPF, EIGRP and BGP, in classless addressing environments, to design and implement network solutions scalable, using the principles of Routing and packet switching in LAN and WAN environments

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

INTRODUCCIÓN

Nosotros como estudiantes de ingeniería de Telecomunicaciones, deberemos hacer una entrega oportuna, para llevar a cabo el desarrollo de la temática establecida como alternativa de grado. La modalidad adoptada por el diplomado de profundización se denomina “Proyecto Aplicado”, mecanismo utilizado por el director del curso, que propone escenarios con características y requerimientos específicos, en donde será implementado acorde con las temáticas de las unidades a desarrollar

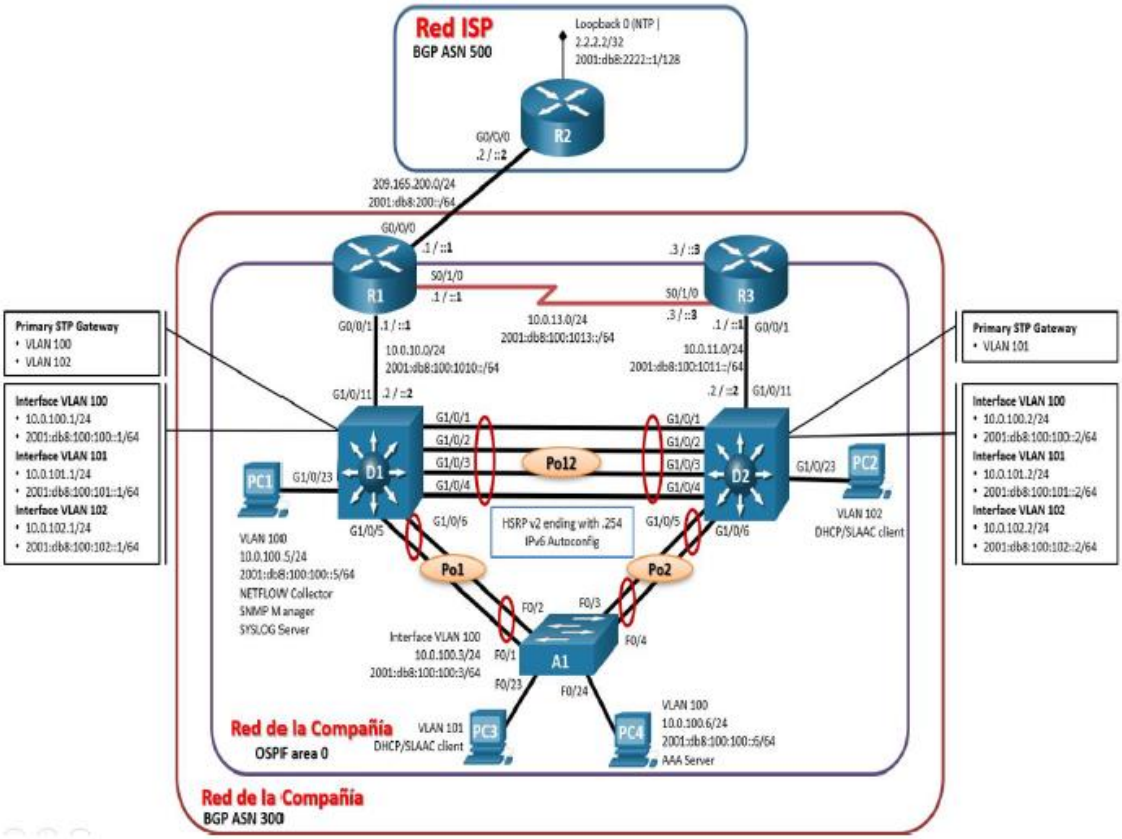
Deberemos configurar de manera correcta cada uno de los dispositivos de Networking que forman parte del primer escenario propuesto en el Simulador de manera adecuada y funcional, dando cumplimiento a cada uno de los lineamientos establecidos en el enunciado.

Como parte de la actividad de implementación, por medio una conexión de consola ingresaremos en cada dispositivo, que crearemos en la topología física y lógica, y procederemos a ingresar al modo de configuración global, para aplicar los parámetros básicos y avanzados. Las configuraciones de inicio para cada dispositivo son fundamentales para generar una comprensión de la actividad Proyecto aplicado.

DESARROLLO

1. ESCENARIO 1

Figura 1 Escenario 1

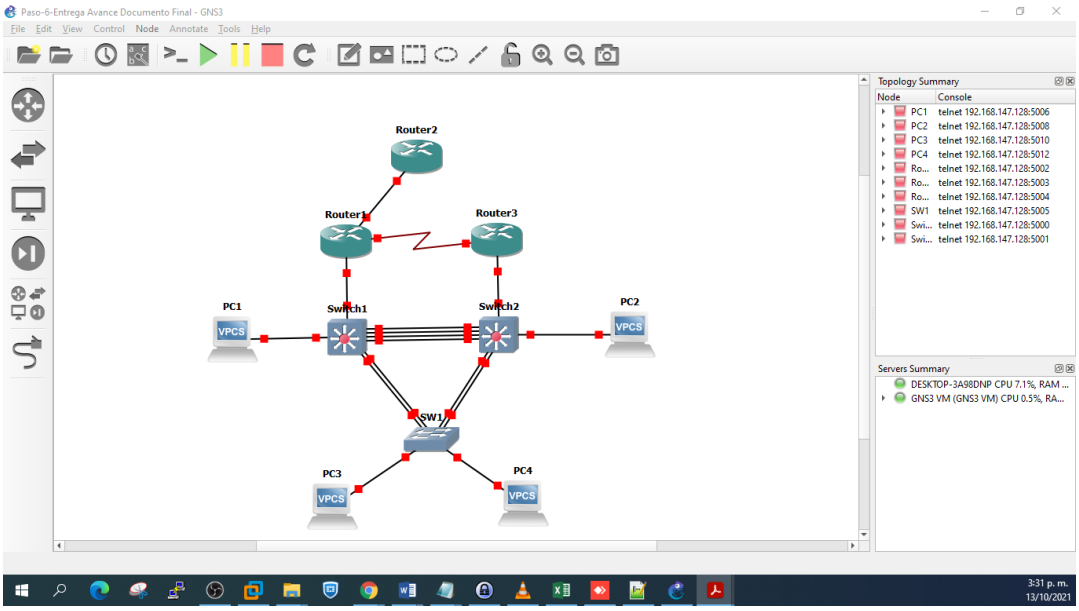


Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

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 Simulación de escenario 1



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.

Tabla 1 Direccionamiento IP

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G1/0	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S2/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R2	G1/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback 0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S2/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/11	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

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

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:

Comandos aplicados en R1 y parámetros de configuración como Nombre de dispositivo, habilitar IPv6 en el router y el mensaje mediante un banner que dice “ENCOR Skills Assessment, Scenario 1”

R1#configure terminal	Ingreso a modo de configuración
R1(config)#hostname R1	Asigno nombre al router
R1(config)#ipv6 unicast-routing	habilitar IPv6 en el router
R1(config)#no ip domain lookup	Deshabilitar el proceso DNS

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

Comandos aplicados en R1 en donde daremos el comando line console 0 para ingresar al modo de configuración de línea de la consola. Decimos que el cero (0), sirve para constituir la primera y en la mayoría de los casos la única interfaz de consola de acceso al Router.

R1(config)#line con 0	Ingreso línea de la consola
R1(config-line)# exec-timeout 0 0	No hay límite de tiempo
R1(config-line)# logging synchronous	Envía mensajes de consola
R1(config-line)# exit	Salir de línea consola

Comandos aplicados en R1 para configuración de la interfaz Ethernet0/0 que comunica con R2.

R1(config)#interface e0/0

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

R1(config-if)# exit

Comandos aplicados en R1 para configuración de la interfaz Ethernet1/0 que comunica con D1.

R1(config)#interface e1/0

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

R1(config-if)# exit

Comandos aplicados en R1 para configuración de la interfaz serial2/0 que comunica con R3

R1(config)#interface s2/0

R1(config-if)# ip address 10.0.13.1 255.255.255.0

R1(config-if)# ipv6 address fe80::1:3 link-local

R1(config-if)# ipv6 address 2001:db8:100:1013::1/64

R1(config-if)# no shutdown

R1(config-if)# exit

Comandos aplicados en R2 y parámetros de configuración como Nombre de dispositivo, habilitar IPv6 en el router y el mensaje mediante un banner que dice “ENCOR Skills Assessment, Scenario 1”

R2#configure terminal

R2(config)#hostname R2

R2(config)#ipv6 unicast-routing

R2(config)#no ip domain lookup

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

Comandos aplicados en R2 en donde daremos el comando line console 0 para ingresar al modo de configuración de línea de la consola. Decimos que el cero (0), sirve para constituir la primera y en la mayoría de los casos la única interfaz de consola de acceso al Router.

R2(config)#line con 0

R2(config-line)# exec-timeout 0 0

R2(config-line)# logging synchronous

R2(config-line)# exit

Comandos aplicados en R2 para configuración de la interfaz Ethernet0/0 que comunica con R1

R2(config)#interface e0/0

R2(config-if)# ip address 209.165.200.226 255.255.255.224

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

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

R2(config-if)# no shutdown

R2(config-if)# exit

Comandos aplicados en R2, para configurar la interfaz de loopback, la cual es una interfaz de red virtual, útil para probar y administrar un dispositivo Cisco IOS, esto debido a que asegura al menos una interfaz esté siempre disponible.

R2(config)#interface Loopback 0

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

R2(config)#

Comandos aplicados en R3 y parámetros de configuración como Nombre de dispositivo, habilitar IPv6 en el router y el mensaje mediante un banner que dice “ENCOR Skills Assessment, Scenario 1”

R3#configure terminal

R3(config)#hostname R3

R3(config)#ipv6 unicast-routing

R3(config)#no ip domain lookup

R3(config)#banner motd # R3, ENCOR Skills Assessment, Scenario 1 #

Comandos aplicados en R3 en donde daremos el comando line console 0 para ingresar al modo de configuración de línea de la consola. Decimos que el cero (0), sirve para constituir la primera y en la mayoría de los casos la única interfaz de consola de acceso al Router.

R3(config)#line con 0

R3(config-line)# exec-timeout 0 0

R3(config-line)# logging synchronous

R3(config-line)# exit

Comandos aplicados en R3 para configuración de la interfaz Ethernet1/0 que comunica con D2.

R3(config)#interface e1/0

R3(config-if)# ip address 10.0.11.1 255.255.255.0

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

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

R3(config-if)# no shutdown

R3(config-if)# exit

Comandos aplicados en R3 para configuración de la interfaz serial2/0 que comunica con R1

R3(config)#interface s2/0

R3(config-if)# ip address 10.0.13.3 255.255.255.0

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

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

R3(config-if)# no shutdown

R3(config-if)# exit

Comandos aplicados en D1 y parámetros de configuración como Nombre de dispositivo, habilitar IPv6 en el Switch capa 3 y el mensaje mediante un banner que dice “ENCOR Skills Assessment, Scenario 1”

IOU1#configure terminal

IOU1(config)#hostname D1

D1(config)#ip routing

D1(config)#ipv6 unicast-routing

D1(config)#no ip domain lookup

D1(config)#banner motd # D1, ENCOR Skills Assessment, Scenario 1 #

Comandos aplicados en D1 en donde daremos el comando line console 0 para ingresar al modo de configuración de línea de la consola. Decimos que el cero (0), sirve para constituir la primera y en la mayoría de los casos la única interfaz de consola de acceso al Switch de capa 3.

D1(config)#line con 0

D1(config-line)# exec-timeout 0 0

D1(config-line)# logging synchronous

D1(config-line)# exit

Comandos aplicados en D1 para creación de Vlan 100 que conecta a PC1 y PC4.

D1(config)#vlan 100	Creación de la Vlan con ID
D1(config-vlan)# name Management	Asignación de nombre para la Vlan
D1(config-vlan)# exit	Salida de config de la Vlan

Comandos aplicados en D1 para creación de Vlan 101 que conecta a PC3.

D1(config)#vlan 101

D1(config-vlan)# name UserGroupA

D1(config-vlan)# exit

Comandos aplicados en D1 para creación de Vlan 102 que conecta a PC2.

D1(config)#vlan 102

D1(config-vlan)# name UserGroupB

D1(config-vlan)# exit

Comandos aplicados en D1 para creación de Vlan 999 la cual será la Nativa.

D1(config)#vlan 999

D1(config-vlan)# name NATIVE

D1(config-vlan)# exit

Comandos aplicados en D1 para configuración de la interfaz Ethernet1/0 que comunica con R1.

D1(config)#interface e1/0	Ingreso a la interfaz ID
D1(config-if)# no switchport	Capacidad Capa 3 a interfaz
D1(config-if)# ip address 10.0.10.2 255.255.255.0	Asigna dirección IPv4
D1(config-if)# ipv6 address fe80::d1:1 link-local	Asigna link-local en IPv6
D1(config-if)# ipv6 address 2001:db8:100:1010::2/64	Dirección IPv6
D1(config-if)# no shutdown	Habilita la interfaz
D1(config-if)# exit	Salir config de la interfaz

VLAN 100 - Red virtual para interconectar PC1 y PC4, con asignación de direccionamiento IPv4 e IPv6

D1(config)#interface vlan 100

D1(config-if)# ip address 10.0.100.1 255.255.255.0

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)# exit

VLAN 101 - Red virtual para interconectar PC3, con asignación de direccionamiento IPv4 e IPv6

D1(config)#interface vlan 101

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

VLAN 102 - Red virtual para interconectar PC2, con asignación de direccionamiento IPv4 e IPv6

D1(config)#interface vlan 102

D1(config-if)# ip address 10.0.102.1 255.255.255.0

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

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

D1(config-if)# no shutdown

D1(config-if)# exit

Exclusión dentro del conjunto de direcciones IP del servicio de DHCP.

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

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

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

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

El comando “ip dhcp pool” con nombre “VLAN-101” crea un conjunto de direcciones IP, con el nombre dado y provoca que el router entre en el modo de configuración de DHCP, el cual se identifica como D1(dhcp-config)#

D1(config)#ip dhcp pool VLAN-101	Creación pool DHCP
D1(dhcp-config)# network 10.0.101.0 255.255.255.0	Dirección de red
D1(dhcp-config)# default-router 10.0.101.254	Puerta de enlace
D1(dhcp-config)# exit	Salir config de la interfaz

El comando “ip dhcp pool” con nombre “VLAN-102” crea un conjunto de direcciones IP, con el nombre dado y provoca que el router entre en el modo de configuración de DHCP, el cual se identifica como D1(dhcp-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

Con el comando “shutdown” se procede apagar interfaces en D1 que no están siendo utilizadas.

D1(config)#interface range e1/1-3 , e1/1-3 , e0/1

D1(config-if-range)# shutdown

D1(config-if-range)# exit

Comandos aplicados en D2 y parámetros de configuración como Nombre de dispositivo, habilitar IPv6 en el Switch capa 3 y el mensaje mediante un banner que dice “ENCOR Skills Assessment, Scenario 1”

IOU2#configure terminal

IOU2(config)#hostname D2

D2(config)#ip routing

D2(config)#ipv6 unicast-routing

D2(config)#no ip domain lookup

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

Comandos aplicados en D2 en donde daremos el comando line console 0 para ingresar al modo de configuración de línea de la consola. Decimos que el cero (0), sirve para constituir la primera y en la mayoría de los casos la única interfaz de consola de acceso al Switch capa 3.

D2(config)#line con 0

D2(config-line)# exec-timeout 0 0

D2(config-line)# logging synchronous

D2(config-line)# exit

Comandos aplicados en D2 para creación de Vlan 100 que conecta a PC1 y PC4.

D2(config)#vlan 100

D2(config-vlan)# name Management

D2(config-vlan)# exit

Comandos aplicados en D2 para creación de Vlan 101 que conecta a PC3.

D2(config)#vlan 101

D2(config-vlan)# name UserGroupA

D2(config-vlan)# exit

Comandos aplicados en D2 para creación de Vlan 102 que conecta a PC2.

D2(config)#vlan 102

D2(config-vlan)# name UserGroupB

D2(config-vlan)# exit

Comandos aplicados en D2 para creación de Vlan 999 la cual será la Nativa.

D2(config)#vlan 999

D2(config-vlan)# name NATIVE

D2(config-vlan)# exit

Comandos aplicados en D2 para configuración de la interfaz Ethernet1/0 que comunica con R3.

D2(config)#interface e1/0

D2(config-if)# no switchport

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

VLAN 100 - Red virtual para interconectar PC1 y PC4, con asignación de direccionamiento IPv4 e IPv6

D2(config)#interface vlan 100

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:db8:100:100::2/64

D2(config-if)# no shutdown

D2(config-if)# exit

VLAN 101 - Red virtual para interconectar PC3, con asignación de direccionamiento IPv4 e IPv6

D2(config)#interface vlan 101

D2(config-if)# ip address 10.0.101.2 255.255.255.0

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

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

D2(config-if)# no shutdown

VLAN 102 - Red virtual para interconectar PC2, con asignación de direccionamiento IPv4 e IPv6

D2(config)#interface vlan 102

D2(config-if)# ip address 10.0.102.2 255.255.255.0

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

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

D2(config-if)# exit

Exclusión dentro del conjunto de direcciones IP del servicio de DHCP.

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

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

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

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

El comando “ip dhcp pool” con nombre “VLAN-101” crea un conjunto de direcciones IP, con el nombre dado y provoca que el router entre en el modo de configuración de DHCP, el cual se identifica como D2(dhcp-config)#

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

El comando “ip dhcp pool” con nombre “VLAN-102” crea un conjunto de direcciones IP, con el nombre dado y provoca que el router entre en el modo de configuración de DHCP, el cual se identifica como D2(dhcp-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

Con el comando “shutdown” se procede apagar interfaces en D2 que no están siendo utilizadas.

D2(config)#interface range 0/0-2 , e1/1-2, e3/1

D2(config-if-range)# shutdown

Comandos aplicados en A1 y parámetros de configuración como Nombre de dispositivo, así como el comando “no ip domain lookup”, el cual permite desactivar la traducción de nombres a dirección del dispositivo, se aplica a un Router o Switch y el mensaje mediante un banner que dice “ENCOR Skills Assessment, Scenario 1”

IOU3#configure terminal

IOU3(config)#hostname A1

A1(config)#no ip domain lookup

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

Comandos aplicados en A1, en donde daremos el comando line console 0 para ingresar al modo de configuración de línea de la consola. Decimos que el cero (0), sirve para constituir la primera y en la mayoría de los casos la única interfaz de consola de acceso al Switch.

A1(config)#line con 0

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

A1(config-line)# logging synchronous

A1(config-line)# exit

Comandos aplicados en A1 para creación de Vlan 100 que conecta a PC1 y PC4.

A1(config)#vlan 100

A1(config-vlan)# name Management

A1(config-vlan)# exit

Comandos aplicados en A1 para creación de Vlan 101 que conecta a PC3.

A1(config)#vlan 101

A1(config-vlan)# name UserGroupA

Comandos aplicados en A1 para creación de Vlan 102 que conecta a PC2.

A1(config)#vlan 102

A1(config-vlan)# name UserGroupB

A1(config-vlan)# exit

Comandos aplicados en A1 para creación de Vlan 999 la cual será la Nativa.

A1(config)#vlan 999

A1(config-vlan)# name NATIVE

A1(config-vlan)# exit

VLAN 100 - Red virtual para interconectar PC1 y PC4, con asignación de direccionamiento IPv4 e IPv6

A1(config)#interface vlan 100

A1(config-if)# ip address 10.0.100.3 255.255.255.0

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

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

A1(config-if)# no shutdown

Con el comando “shutdown” se procede apagar interfaces en A1 que no están siendo utilizadas.

A1(config)#interface range E1/0-3	Selección de rango interfaces
A1(config-if-range)# shutdown	Apagado de interfaces en el rango

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

R1#copy running-config startup-config

R2#copy running-config startup-config

R3#copy running-config startup-config

D1#copy running-config startup-config

D2#copy running-config startup-config

A1#copy running-config startup-config

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.

Configuración en interface para PC1 del Switch D1

D1(config)#interface E3/0

D1(config-if)#switchport mode access

D1(config-if)#switchport access vlan 100

D1(config-if)#no shutdown

Configuración direccionamiento IP del PC1

PC1> ip 10.0.100.5 /24 10.0.100.254

Figura 3 Comando show en PC1

```
PC1> sho

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    10.0.100.5/24        10.0.100.254      00:50:79:66:68:00  20050  127.0.0.1:20051
       fe80::250:79ff:fe66:6800/64
       2001:db8:100:100:2050:79ff:fe66:6800/64 eui-64
```

Configuración en interface para PC4 del Switch A1

A1(config)#interface E3/1

A1(config-if)#switchport mode access

A1(config-if)#switchport access vlan 100

A1(config-if)#no shutdown

Configuración direccionamiento IP del PC4

PC4> ip 10.0.100.6 /24 10.0.100.254

Figura 4 Comando show en PC4

```
PC4> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    10.0.100.6/24        10.0.100.254      00:50:79:66:68:01  20032  127.0.0.1:20033
```

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 Switch deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

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 range ethernet 0/0-3	Rango interfaces
D1(config-if-range)#switchport trunk encapsulation dot1q	Etiquetado de Vlan
D1(config-if-range)#switchport mode trunk	Modo troncal

D1 and A1

D1(config)#interface range e2/0-1

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

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

D2 and A1

D2(config)#interface range e2/0-1

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

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

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

D1 and D2

D1(config)#interface range ethernet 0/0-3

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

D2 and D1

D2(config)#interface range ethernet 0/0-3

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

D1 and A1

D1(config)#interface range ethernet 2/1-2

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

D2 and A1

D2(config)#interface range e2/0-1

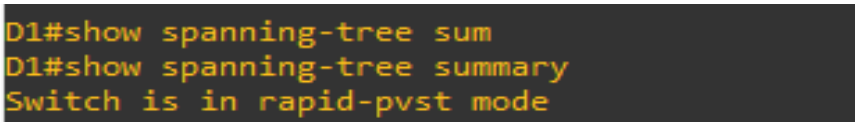
D2(config-if-range)# switchport trunk native vlan 999

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

Decimos que el protocolo de árbol de extensión rápido (RSTP), es la mejora realizada al protocolo de árbol de extensión (STP) y se encarag de proporcionar una convergencia de árbol de extensión más rápida.

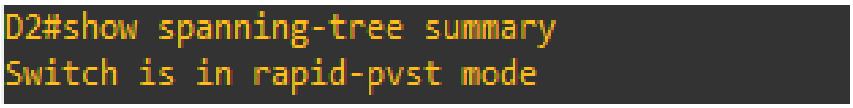
D1(config)#spanning-tree mode rapid-pvst

Figura 5 Comando ver spanning-Tree en D1



D2(config)#spanning-tree mode rapid-pvst

Figura 6 Comando ver spanning-Tree en D2



A1(config)#spanning-tree mode rapid-pvst

Figura 7 Comando ver spanning-Tree en A1

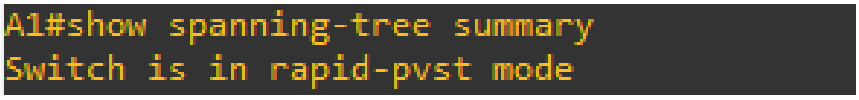


Figura 8 Aplico DHCP para PC3

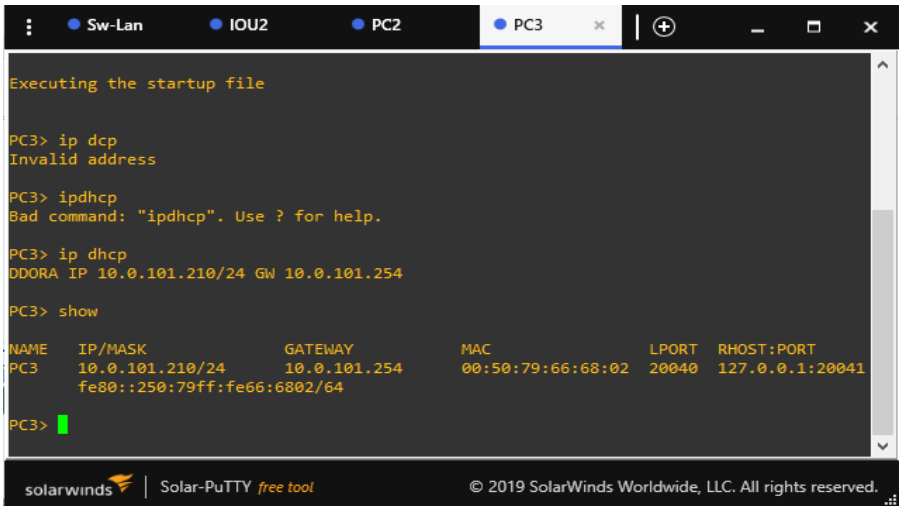
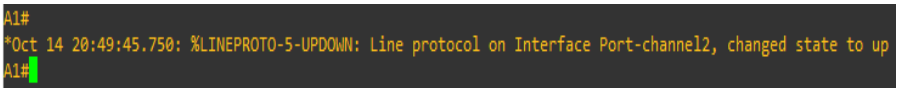


Figura 9 LACP activo entre A1 y D2



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(config)#spanning-tree vlan 100 root primary	Raíz para las VLAN 100
D1#show spanning-tree vlan 102 root primary	Raíz para las VLAN 102
D2(config)#spanning-tree vlan 101 root primary	Raíz para las VLAN 101

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología. Use los siguientes números de canales:

LACP permite la agrupación lógica de varios enlaces físicos Ethernet, dicha agrupación es vista como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado para esta implementación y así obtener un enlace troncal de alta velocidad.

D1 a D2 – Port channel 12

Selección de rango de los enlaces físicos Ethernet 0/0 al 0/3

D1(config)#interface range ethernet 0/0-3

Comando para que la interfaz use la encapsulación 802.1Q y así inserte una etiqueta de VLAN, también sirve para que la interfaz sea usada por el dispositivo como interfaz troncal.

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

Comando para que la interfaz se configura como un enlace trocal.

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

Comando que permite que el enlace trocal, use la vlan 999 como nativa.

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

Comando que permite crear la agrupación de enlaces número 12, LACP en modo activo en dispositivo D1.

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

Creating a port-channel interface Port-channel 12

D1(config-if-range)#

D1(config-if-range)#no shutdown

D1(config-if-range)#exit

Configuración de la interfaz port-channel número 12, como enlace troncal, con todos los parámetros de configuración como: encapsulación 802.1Q, Vlan nativa y estado UP de la interfaz.

D1(config-if)#interface port-channel 12

D1(config-if)# switchport trunk encapsulation dot1q

D1(config-if)# switchport mode trunk

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

D1(config-if)#no shutdown

D1(config-if)#do wr

D1 a A1 – Port channel 1

Selección de rango de los enlaces físicos Ethernet 2/0 al 2/1 en D1.

D1(config)#interface range e2/0-1

Comando para que la interfaz use la encapsulación 802.1Q y así inserte una etiqueta de VLAN, también sirve para que la interfaz sea usada como troncal.

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

Comando para que la interfaz se configura como un enlace trocal.

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

Comando que permite que el enlace trocal, use la vlan 999 como nativa.

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

Comando que permite crear la agrupación de enlaces número 1, LACP en modo activo en dispositivo D1.

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

Creating a port-channel interface Port-channel 1

D1(config-if-range)# exit

Configuración de la interfaz port-channel número 1, como enlace troncal, con todos los parámetros de configuración como: encapsulación 802.1Q, Vlan nativa y estado UP de la interfaz en D1.

D1(config)#interface port-channel 1

D1(config-if)# switchport trunk encapsulation dot1q

D1(config-if)# switchport mode trunk

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

D2 a D1 – Port channel 2

Selección de rango de los enlaces físicos Ethernet 0/0 al 0/3 en D2.

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

Comando para que la interfaz use la encapsulación 802.1Q y así inserte una etiqueta de VLAN, también sirve para que la interfaz sea usada por el dispositivo como interfaz troncal.

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

Comando para que la interfaz se configura como un enlace trocal.

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

Comando que permite que el enlace trocal, use la vlan 999 como nativa.

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

Comando que permite crear la agrupación de enlaces número 12, LACP en modo activo en dispositivo D2.

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

Creating a port-channel interface Port-channel 12

D2(config-if-range)# exit

Configuración de la interfaz port-channel número 12, como enlace troncal, con todos los parámetros de configuración como: encapsulación 802.1Q, Vlan nativa y estado UP de la interfaz en D2.

D2(config)#interface port-channel 12

D2(config-if)# switchport trunk encapsulation dot1q

D2(config-if)# switchport mode trunk

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

D2(config-if)#do

D2(config-if)#do wr

D2 a A1 – Port channel 2

Selección de rango de los enlaces físicos Ethernet 2/0 al 2/1 en D2.

D2(config)#interface range e2/0-1

Comando para que la interfaz use la encapsulación 802.1Q y así inserte una etiqueta de VLAN, también sirve para que la interfaz sea usada por el dispositivo como interfaz troncal.

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

Comando para que la interfaz se configura como un enlace trocal.

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

Comando que permite que el enlace trocal, use la vlan 999 como nativa.

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

Comando que permite crear la agrupación de enlaces número 2, LACP en modo activo en dispositivo D2.

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

Creating a port-channel interface Port-channel 2

D2(config-if-range)# exit

Configuración de la interfaz port-channel número 2, como enlace troncal, con todos los parámetros de configuración como: encapsulación 802.1Q, Vlan nativa y estado UP de la interfaz en D2.

D2(config)#interface port-channel 2

D2(config-if)# switchport trunk encapsulation dot1q

D2(config-if)# switchport mode trunk

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

D2(config-if)# do wr

D2(config-if)#no shutdown

D2(config-if)#exit

2.6 En todos los Switch, 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 a PC1

D1(config)#interface E3/0	Configuro interfaz ethernet 3/0
D1(config-if)#switchport mode access	Configuro modo acceso en interfaz
D1(config-if)#switchport access vlan 100	Asigno a la Vlan 100
D1(config-if)#no shutdown	Subo interfaz a estado up

D2 a PC2

D1(config)#interface E3/0

D1(config-if)#switchport mode access

D1(config-if)#switchport access vlan 102

D1(config-if)#no shutdown

A1 a PC3

A1(config)#interface E3/0

A1(config-if)#switchport mode access

A1(config-if)#switchport access vlan 101

A1(config-if)#no shutdown

A1 a PC4

A1(config)#interface E3/1

A1(config-if)#switchport mode access

A1(config-if)#switchport access vlan 100

A1(config-if)#no shutdown

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

Figura 10 Aplico DHCP para PC2

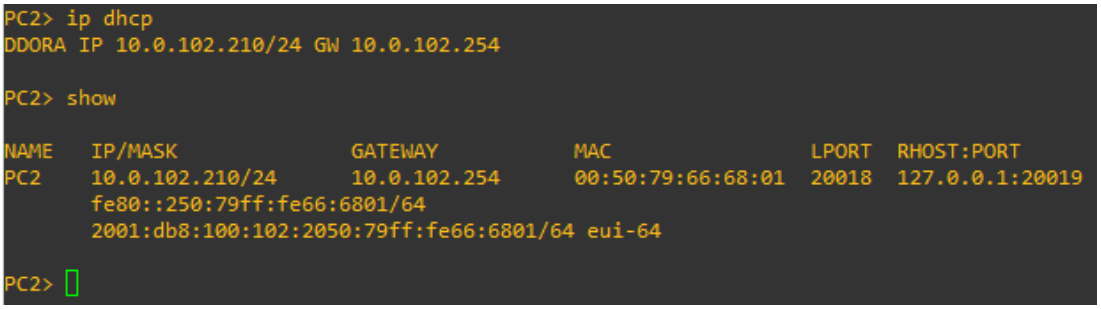
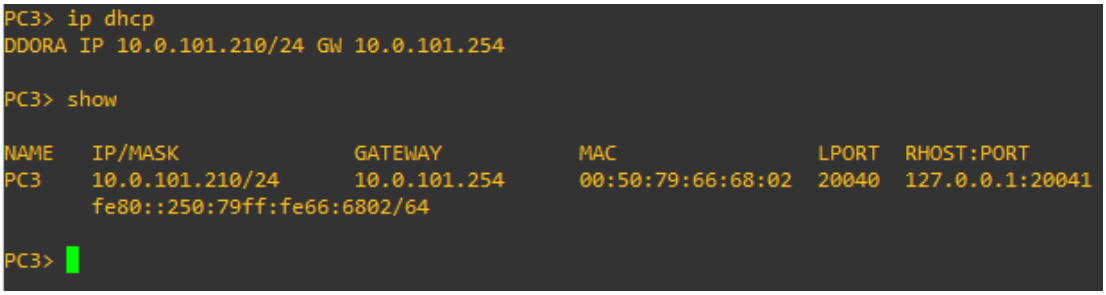


Figura 11 Aplico DHCP para PC3

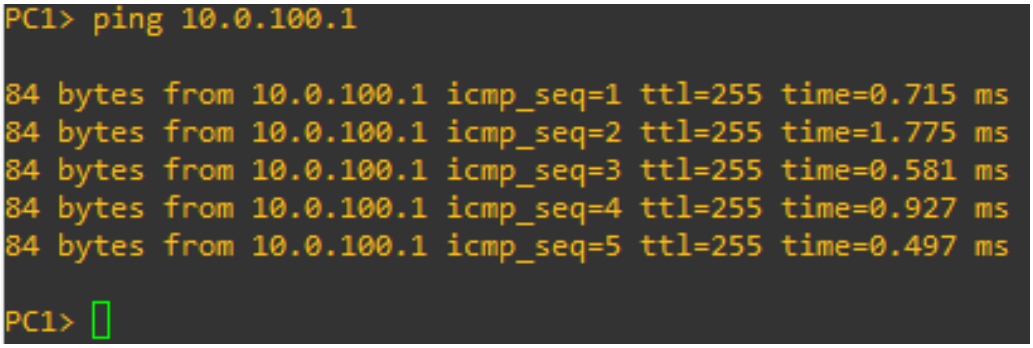


2.8 Verifique la conectividad de la LAN local

PC1 debería hacer ping con éxito a:

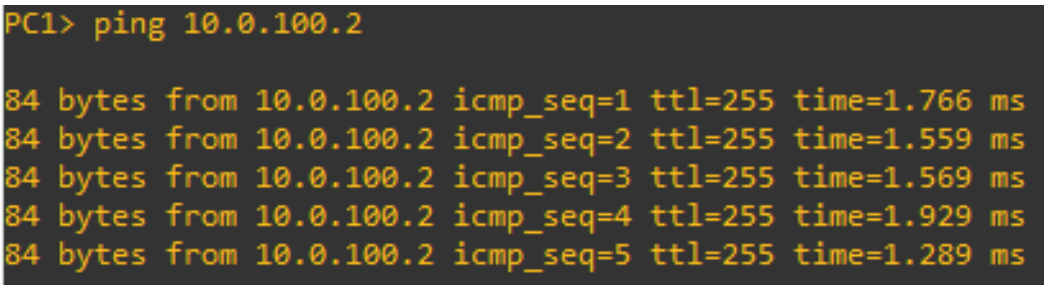
D1: 10.0.100.1

Figura 12 PC1 realiza ping a D1



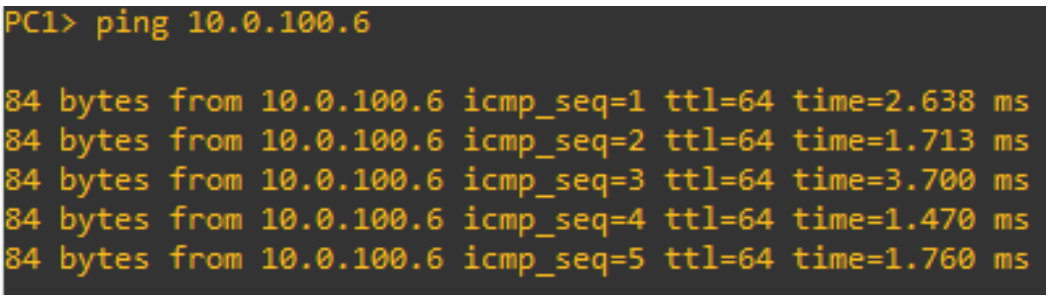
D2: 10.0.100.2

Figura 13 PC1 realiza ping a D2



PC4: 10.0.100.6

Figura 14 PC1 realiza ping a PC4



PC2 debería hacer ping con éxito a:

D1: 10.0.102.1

Figura 15 PC2 realiza ping a D1

```
PC2> ping 10.0.102.1

84 bytes from 10.0.102.1 icmp_seq=1 ttl=255 time=1.092 ms
84 bytes from 10.0.102.1 icmp_seq=2 ttl=255 time=1.249 ms
84 bytes from 10.0.102.1 icmp_seq=3 ttl=255 time=1.504 ms
84 bytes from 10.0.102.1 icmp_seq=4 ttl=255 time=1.524 ms
84 bytes from 10.0.102.1 icmp_seq=5 ttl=255 time=1.856 ms
```

D2: 10.0.102.2

Figura 16 PC2 realiza ping a D2

```
PC2> ping 10.0.102.2

84 bytes from 10.0.102.2 icmp_seq=1 ttl=255 time=0.703 ms
84 bytes from 10.0.102.2 icmp_seq=2 ttl=255 time=0.773 ms
84 bytes from 10.0.102.2 icmp_seq=3 ttl=255 time=0.941 ms
84 bytes from 10.0.102.2 icmp_seq=4 ttl=255 time=0.681 ms
84 bytes from 10.0.102.2 icmp_seq=5 ttl=255 time=0.524 ms
```

PC3 debería hacer ping con éxito a:

D1: 10.0.101.1

Figura 17 PC3 realiza ping a D1

```
PC3> ping 10.0.101.1

84 bytes from 10.0.101.1 icmp_seq=1 ttl=255 time=0.520 ms
84 bytes from 10.0.101.1 icmp_seq=2 ttl=255 time=0.896 ms
84 bytes from 10.0.101.1 icmp_seq=3 ttl=255 time=1.249 ms
84 bytes from 10.0.101.1 icmp_seq=4 ttl=255 time=0.869 ms
84 bytes from 10.0.101.1 icmp_seq=5 ttl=255 time=0.995 ms
```

D2: 10.0.101.2

Figura 18 PC3 realiza ping a D2

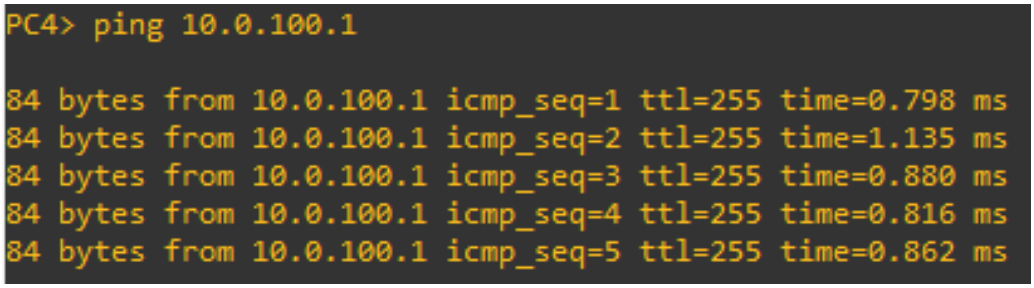
```
PC3> ping 10.0.101.2

84 bytes from 10.0.101.2 icmp_seq=1 ttl=255 time=0.651 ms
84 bytes from 10.0.101.2 icmp_seq=2 ttl=255 time=0.936 ms
84 bytes from 10.0.101.2 icmp_seq=3 ttl=255 time=2.900 ms
84 bytes from 10.0.101.2 icmp_seq=4 ttl=255 time=1.130 ms
84 bytes from 10.0.101.2 icmp_seq=5 ttl=255 time=0.722 ms
```

PC4 debería hacer ping con éxito a:

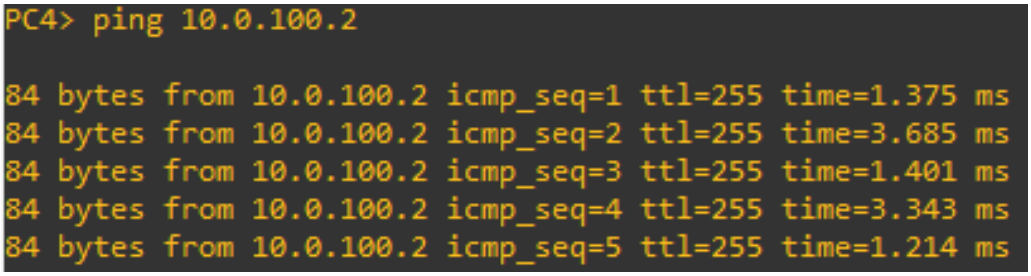
D1: 10.0.100.1

Figura 19 PC4 realiza ping a D1



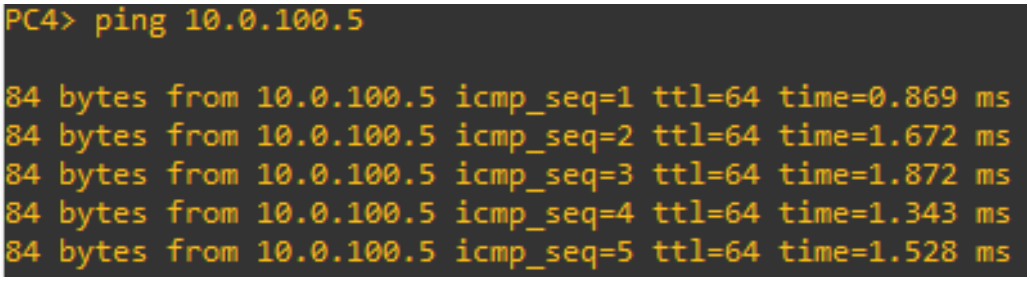
D2: 10.0.100.2

Figura 20 PC4 realiza ping a D2



PC1: 10.0.100.5

Figura 21 PC4 realiza ping a PC1



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.

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

En R1, R3, D1, y D2, anuncie todas las redes directamente conectadas / VLANs en Área 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

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

R1: 0.0.4.1

R1(config)#router ospf 4

R1(config-router)# router-id 0.0.4.1

En R1, anunciar todas las redes directamente conectadas / VLANs en Área 0.

R1(config-router)# network 10.0.13.0 0.0.0.255 area 0

R1(config-router)# network 10.0.10.0 0.0.0.255 area 0

R1(config-router)#do wr

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

R3: 0.0.4.3

R3(config)#router ospf 4

R3(config-router)# router-id 0.0.4.3

En R3, anunciar todas las redes directamente conectadas / VLANs en Área 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
R3(config-router)#do wr

Use OSPF Process ID 4 y asigne los siguientes router-IDs:
D1: 0.0.4.131
D1(config)#router ospf 4
D1(config-router)# router-id 0.0.4.131
En D1, anunciar todas las redes directamente conectadas / VLANs en Área 0.
D1(config-router)# network 10.0.0.0 0.0.255.255 area 0
D1(config-router)#do wr

Use OSPF Process ID 4 y asigne los siguientes router-IDs:
D2: 0.0.4.132
D2(config)#router ospf 4
D2(config-router)# router-id 0.0.4.132
En D2, anunciar todas las redes directamente conectadas / VLANs en Área 0.
D2(config-router)# network 10.0.0.0 0.0.255.255 area 0
D2(config-router)#do wr

3.2 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure classic single-area OSPFv3 en area 0. Use OSPF Process ID 6 y asigne los siguientes router-IDs:

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 OSPFv3 en:

D1: todas las interfaces excepto G1/0/11

D2: todas las interfaces excepto G1/0/11

Use OSPF Process ID 6 y asigne los siguientes router-IDs:

R1: 0.0.6.1

R1(config)#ipv6 router ospf 6	Configuración OSPF proceso ID 6
R1(config-rtr)# router-id 0.0.6.1	ID de router
R1(config-rtr)# exit	Salir de configuración
R1(config)#interface e1/0	Configurar ethernet 1/0
R1(config-if)# ipv6 ospf 6 area 0	Configure OSPFv3 en area 0
R1(config-if)# exit	Salir de configuración

R1(config)#interface s2/0

R1(config-if)# ipv6 ospf 6 area 0

R1(config-if)# do wr

Use OSPF Process ID 6 y asigne los siguientes router-IDs:

R3: 0.0.6.3

R3(config)#ipv6 router ospf 6

R3(config-rtr)# router-id 0.0.6.3

R3(config-rtr)# exit

R3(config)#interface e1/0

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

R3(config-if)# exit
R3(config)#interface s2/0
R3(config-if)# ipv6 ospf 6 area 0
R3(config-if)# exit
R3(config)#do wr

Use OSPF Process ID 6 y asigne los siguientes router-IDs:
D1: 0.0.6.131
D1(config)#ipv6 router ospf 6
D1(config-rtr)# router-id 0.0.6.131
D1(config-rtr)# exit
D1(config)#interface e1/0
D1(config-if)# ipv6 ospf 6 area 0
D1(config-if)# do wr

Use OSPF Process ID 6 y asigne los siguientes router-IDs:
D2: 0.0.6.132
D2(config)#ipv6 router ospf 6
D2(config-rtr)# router-id 0.0.6.132
D2(config-rtr)# exit
D2(config)#interface e1/0
D2(config-if)# ipv6 ospf 6 area 0
D2(config-if)# exit

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.

R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 0

Una ruta estática predeterminada IPv6.

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

Podemos decir que el protocolo BGP, denominado puerta de enlace de frontera, es un protocolo por el cual se intercambia información de enrutamiento entre sistemas autónomos (AS). Es muy común ver su implementación con ISP denominados prestadores de servicios de Internet.

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).

R2(config)#router bgp 500	Configuro ASN 500
R2(config-router)#bgp router-id 2.2.2.2	ID de router
R2(config-router)#bgp log-neighbor-changes	Mensaje de vecino
R2(config-router)#network 209.165.200.224 mask 255.255.255.224	
R2(config-router)#redistribute connected	Redistribuir las rutas
R2(config-router)#neighbor 209.165.200.225 remote-as 300	Vecino con AS 300
R2(config-router)#no auto-summary	No sumarización
R2(config-router)#do wr	Salvar configuración
R2(config-router)#address-family ipv4	Configurar IPv4
R2(config-router-af)#network 0.0.0.0 mask 0.0.0.0	Ruta por defecto
R2(config-router-af)#network 2.2.2.2 mask 255.255.255.255	Ruta de red IPv4
R2(config-router)#address-family ipv6	Configurar IPv6
R2(config-router-af)#network 2001:db8:2222::1/128	Ruta de red IPv6

R2(config-router-af)#network ::/0	Ruta por defecto
R2(config-router-af)#exit	Salir
R2(config-router)#do wr	Salvar configuración

Figura 22 Configuración BGP en R2

```
R2#
*Oct 16 16:06:25.646: %BGP-5-ADJCHANGE: neighbor 209.165.200.225 Up
R2#sh
R2#show ip rou
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
B        10.0.0.0/8 [20/0] via 209.165.200.225, 00:47:06
B        10.0.10.0/24 [20/0] via 209.165.200.225, 00:49:42
B        10.0.13.0/24 [20/0] via 209.165.200.225, 00:49:42
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Ethernet0/0
L        209.165.200.226/32 is directly connected, Ethernet0/0
R2#
```

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.

R1(config)#ip route 10.0.0.0 255.0.0.0 null 0

Una ruta resumen IPv6 para 2001:db8:100::/48.

R1(config)#ipv6 route 2001:db8:100::/48 null 0

Podemos decir que el protocolo BGP, denominado puerta de enlace de frontera, es un protocolo por el cual se intercambia información de enrutamiento entre sistemas autónomos (AS). Es muy común ver su implementación con ISP denominados prestadores de servicios de Internet.

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.

R1(config)#router bgp 300

R1(config-router)#bgp router-id 1.1.1.1

R1(config-router)#bgp log-neighbor-changes

R1(config-router)#network 209.165.200.224 mask 255.255.255.224

R1(config-router)#network 10.0.10.0 mask 255.255.255.0

R1(config-router)#network 10.0.13.0 mask 255.255.255.0

R1(config-router)#redistribute connected

R1(config-router)#neighbor 209.165.200.226 remote-as 500

R1(config-router)#neighbor 2001:db8:200::2 remote-as 500

R1(config-router)#no auto-summary

R1(config-router)#do wr

R1(config-router)#address-family ipv4

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

R1(config-router-af)#neighbor 209.165.200.226 activate

R1(config-router)#address-family ipv6

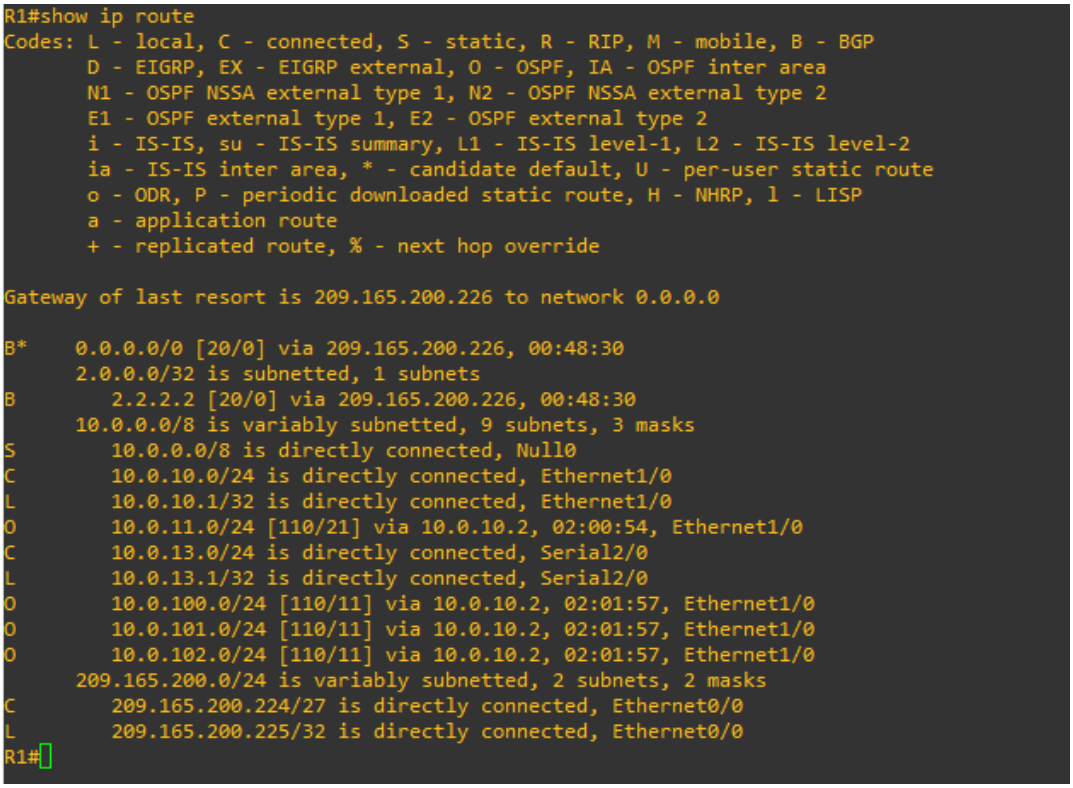
R1(config-router-af)#network 2001:db8:100::/48

R1(config-router-af)#neighbor2001:db8:200::2 activate

R1(config-router-af)#exit

R1(config-router)#do wr

Figura 23 Configuración BGP en R1.



En la figura 23, las rutas que tiene (B*) son las que está anunciando BGP

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

En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 e1/0.

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 e1/0 cada 5 segundos.

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

Cree una IP SLA objeto para la IP SLA 4 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.

Tenemos que al hacer seguimiento de objetos de SLA de IP para una ruta estática, también se fundamenta en operaciones de IP SLA para detectar la conectividad a las redes de destino. La operación de IP SLA posterior a esto, inicia el proceso de monitoreo ya sea en el éxito o fracaso de las respuestas del host destino.

En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 e1/0.

Primero deberemos establecer comunicación entre R1 y D1 por la interfaz Ethernet 1/0 en ambos dispositivos, Debemos tener en cuenta que un puerto enrutado se crea en un switch de Capa 3 deshabilitando la función switchport de un switch de Capa 2 que está conectado a otro dispositivo de Capa 3. Específicamente, al configurar el comando de configuración interfaz no switchport en un puerto de Capa 2, se convierte en una interfaz de Capa 3.

D1(config)#interface ethernet 1/0

D1(config-if)#no switchport

D1(config-if)#ip address 10.0.10.2 255.255.255.0

D1(config-if)#ipv6 address 2001:db8:100:1010::2/64

Cree dos IP SLAs.

Use la SLA número 4 para IPv4.

Para iniciar la configuración de una operación IP SLA e ingresar al modo de configuración ingresamos así:

D1(config)#ip sla 4

Configurar operaciones de eco ICMP, las IP SLAs probarán la disponibilidad de la interfaz R1 e1/0 cada 5 segundos, mediante la interfaz ethernet 1/0 del dispositivo D1 con IP 10.0.10.2.

D1(config-ip-sla)#icmp-echo 10.0.10.1 source-ip 10.0.10.2

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

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

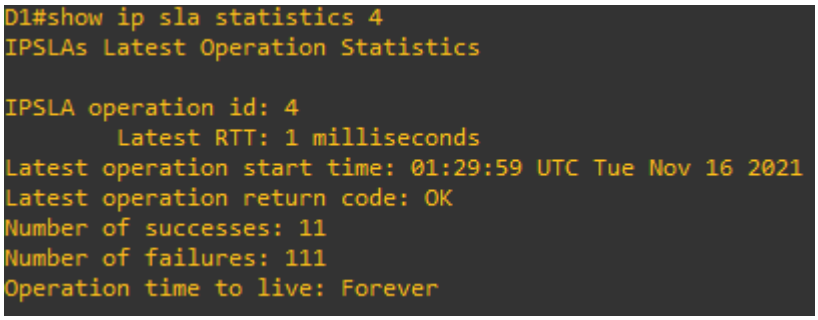
Programe la SLA para una implementación inmediata sin tiempo de finalización.

D1(config)#ip sla schedule 4 start-time now life forever

Para ver la configuración de IP SLA 4

D1(config)#show ip sla statistics 4

Figura 24 Comando verifica la sla 4



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.

D1(config)#track 4 ip sla 4 state

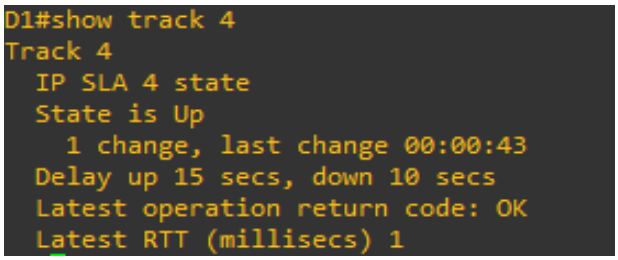
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Después de la creación del objeto, el estado se establece primero en Up.

(config-track)#delay up 15 down 10

D1#show track 4

Figura 25 Comando ver objeto 4 en D1



Use la SLA número 6 para IPv6.

Para iniciar la configuración de una operación IP SLA e ingresar al modo de configuración ingresamos así:

D1(config)#ip sla 6

Configurar operaciones de eco ICMP, las IP SLAs probarán la disponibilidad de la interfaz R1 f0/0/0 cada 5 segundos.

D1(config-ip-sla)#icmp-echo 2001:db8:100:1010::1 source-ip 2001:db8:100:1010::2

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

D1(config)#exit

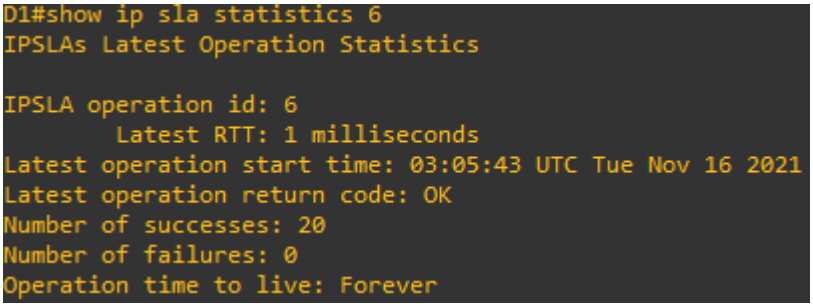
Programe la SLA para una implementación inmediata sin tiempo de finalización.

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

Para ver la configuración de IP SLA 6

D1#show ip sla statistics 6

Figura 26 Comando ver sla 6 en D1



Use el número de rastreo 6 para la IP SLA 6.

D1(config)#track 6 ip sla 6 state

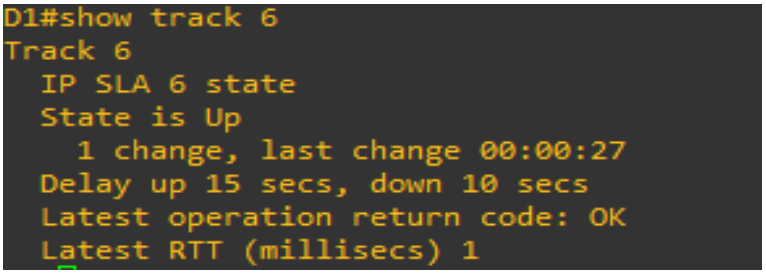
Los objetos rastreados deben notificar a D1 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Después de la creación del objeto, el estado se establece primero en Up.

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

D1#show track 6

Figura 27 Comando ver objeto 6 en D1



En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 e1/0.

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 e1/0 cada 5 segundos.

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

Cree una IP SLA objeto para la IP SLA 4 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 D2 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)#interface ethernet 1/0

D2(config-if)#no switchport

D2(config-if)#ip address 10.0.11.2 255.255.255.0

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

Cree dos IP SLAs.

Use la SLA número 4 para IPv4.

Para iniciar la configuración de una operación IP SLA e ingresar al modo de configuración ingresamos así:

D2(config)#ip sla 4

Configurar operaciones de eco ICMP, las IP SLAs probarán la disponibilidad de la interfaz R3 e1/0 cada 5 segundos, mediante la interfaz ethernet 1/0 del dispositivo D2 con IP 10.0.11.2.

D2(config-ip-sla)#icmp-echo 10.0.11.1 source-ip 10.0.11.2

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

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

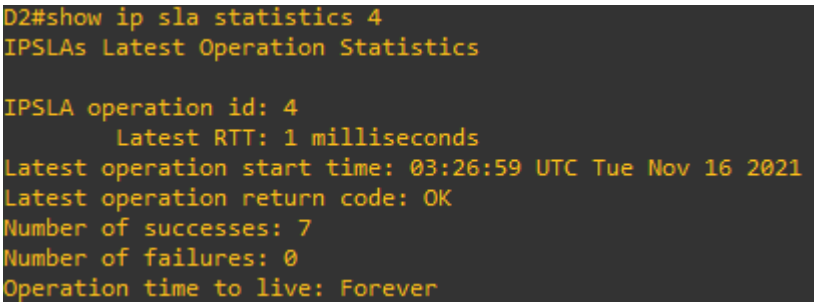
Programe la SLA para una implementación inmediata sin tiempo de finalización.

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

Para ver la configuración de IP SLA 4

D2(config)#show ip sla statistics 4

Figura 28 Comando ver sla 4 en D2



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.

D2(config)#track 4 ip sla 4 state

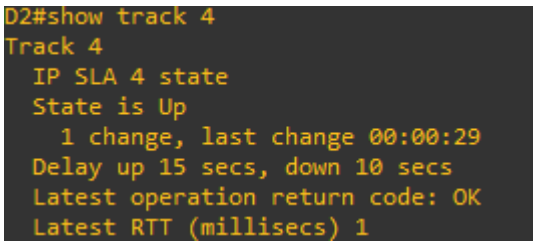
Los objetos rastreados deben notificar a D2 si el estado de IP SLA cambia de Down a Up después de 10 segundos, o de Up a Down después de 15 segundos.

Después de la creación del objeto, el estado se establece primero en Up.

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

D2#show track 4

Figura 29 Comando ver objeto 4 en D2



Use la SLA número 6 para IPv6.

Para iniciar la configuración de una operación IP SLA e ingresar al modo de configuración ingresamos así:

D2(config)#ip sla 6

Configurar operaciones de eco ICMP, las IP SLAs probarán la disponibilidad de la interfaz R1 f0/0/0 cada 5 segundos.

D2(config-ip-sla)#icmp-echo 2001:db8:100:1011::1 source-ip 2001:db8:100:1011::2

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

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

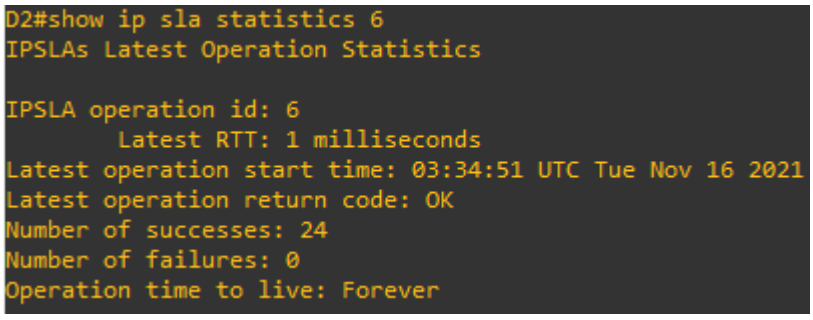
Programe la SLA para una implementación inmediata sin tiempo de finalización.

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

Para ver la configuración de IP SLA 6

D1#show ip sla statistics 6

Figura 30 Comando ver sla 6 en D2



Use el número de rastreo 6 para la IP SLA 6.

D2(config)#track 6 ip sla 6 state

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.

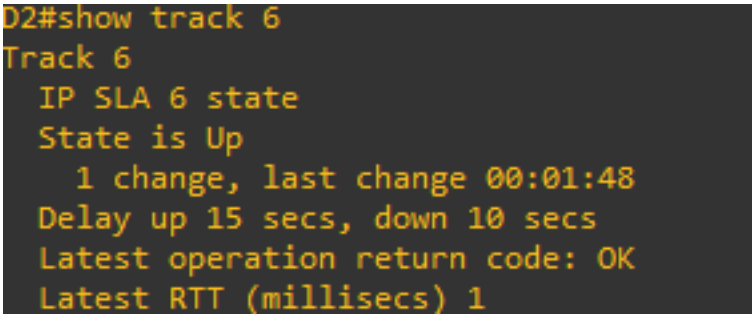
Después de la creación del objeto, el estado se establece primero en Up.

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

D2(config-track)#exit

D2#show track 6

Figura 31 Comando ver objeto 6 en D2



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

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

Las tareas de configuración son las siguientes:

Primero deberemos establecer un enlace trocal entre R1 y D1, esto lo haremos en R1 mediante la interfaz Ethernet 1/0 y D1 Ethernet 1/0

Creación de Subinterfaces para Vlan 100, 101, 102 en dispositivo R1.

R1, Creamos subinterfaces las cuales se utilizan en el enrutamiento no tradicional, esto sobre una misma interfaz física se realizan varias subinterfaces virtuales en enlaces troncales. Cada subinterfaz se configura con su dirección IP, máscara de subred y VLAN.

Subinterfaz Vlan 100

R1(config)#interface ethernet1/0.100

R1(config-subif)#encapsulation dot1Q 100

R1(config-subif)#ip address 10.0.100.3 255.255.255.0

R1(config-subif)#ipv6 address 2001:db8:100:100::3/64

R1(config-subif)#no shutdown

Figura 32 Comando subinterfaces en R1

```
R1#show interfaces ethernet1/0.100
Ethernet1/0.100 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc00.0401 (bia aabb.cc00.0401)
  Internet address is 10.0.100.3/24
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive set (10 sec)
  Last clearing of "show interface" counters never
```

Subinterfaz Vlan 101

R1(config)#interface ethernet1/0.101

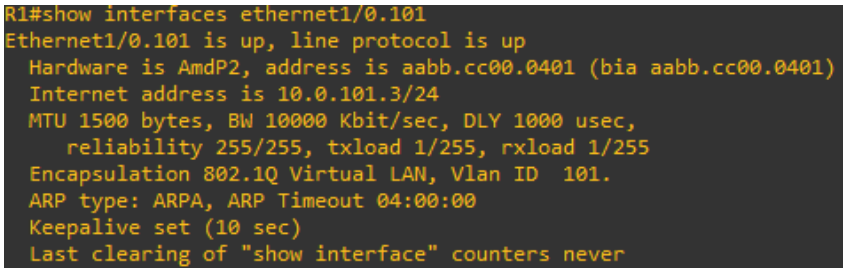
R1(config-subif)#encapsulation dot1Q 101

R1(config-subif)#ip address 10.0.101.3 255.255.255.0

R1(config-subif)#ipv6 address 2001:db8:100:101::3/64

R1(config-subif)#no shutdown

Figura 33 Comando subinterfaces en R1.



Subinterfaz Vlan 102

R1(config)#interface ethernet1/0.102

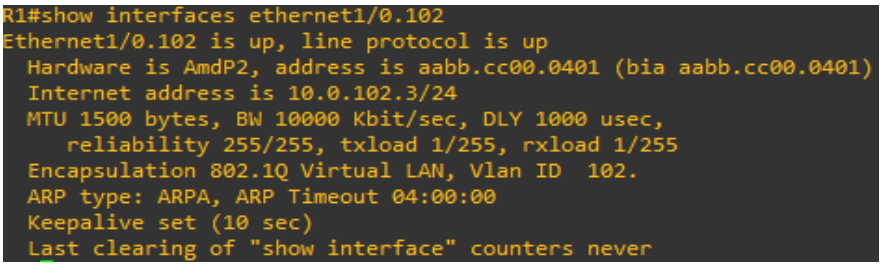
R1(config-subif)#encapsulation dot1Q 102

R1(config-subif)#ip address 10.0.102.3 255.255.255.0

R1(config-subif)#ipv6 address 2001:db8:100:102::3/64

R1(config-subif)#no shutdown

Figura 34 Comando subinterfaces en R1



D1, habilitamos el comando “ip routing”, para habilitar previamente el ruteo IP, posteriormente debemos dar el comando “switchport” consiste en una combinación en la forma del sistema de troncalizado de VLAN y enlaces de acceso. Los enlaces generales pueden tener tramas etiquetadas y sin etiquetar. Podemos decir que todas las tramas que se envían a una VLAN específica deben etiquetarse. A su vez todas las tramas sin etiquetar se envían a la VLAN nativa. También en la configuración debemos dar el comando “encapsulation dot1q” para habilitar 802.1Q y asociar una VLAN específica VLAN a la subinterfaz, así mismo configurar las Vlan permitidas y la Vlan nativa.

D1(config)#ip routing

D1(config-if)#intergafe e1/0

D1(config-if)#switchport

D1(config-if)#switchport trunk encapsulation dot1q

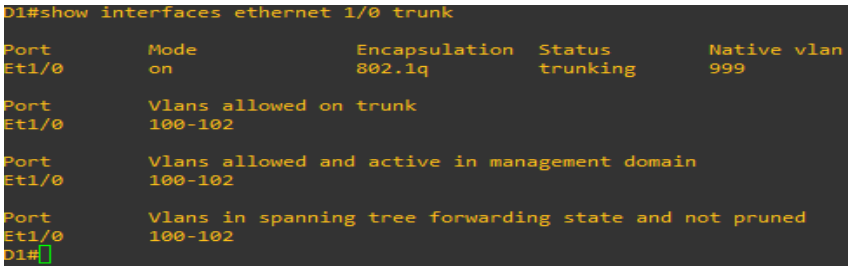
D1(config-if)#switchport mode trunk

D1(config-if)#switchport trunk allowed vlan 100,101,102

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

D1#show interfaces ethernet 1/0 trunk

Figura 35 Comando ver interface en D1



Creación de Subinterfaces para Vlan 100, 101, 102 en dispositivo R3.

R3, Creamos subinterfaces las cuales se utilizan en el enrutamiento no tradicional, esto sobre una misma interfaz física se realizan varias subinterfaces virtuales en enlaces troncales. Cada subinterfaz se configura con su dirección IP, máscara de subred y VLAN.

Subinterfaz Vlan 100

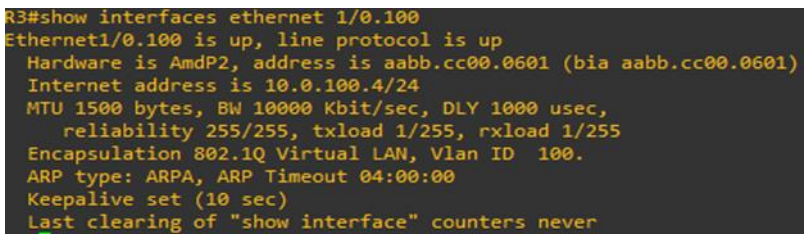
R3(config)#interface ethernet1/0.100

R3(config-subif)#encapsulation dot1Q 100

R3(config-subif)#ip address 10.0.100.4 255.255.255.0

R3(config-subif)#ipv6 address 2001:db8:100:100::4/64

Figura 36 Comando subinterfaces en R3



Subinterfaz Vlan 101

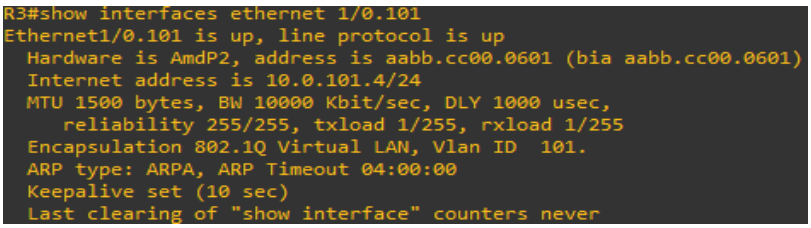
R3(config)#interface ethernet1/0.101

R3(config-subif)#encapsulation dot1Q 101

R3(config-subif)#ip address 10.0.101.4 255.255.255.0

R3(config-subif)#ipv6 address 2001:db8:100:101::4/64

Figura 37 Comando subinterfaces en R3.



Subinterfaz Vlan 102

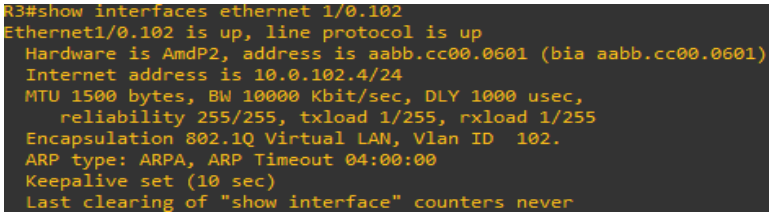
R3(config)#interface ethernet1/0.102

R3(config-subif)#encapsulation dot1Q 102

R3(config-subif)#ip address 10.0.102.4 255.255.255.0

R3(config-subif)#ipv6 address 2001:db8:100:102::4/64

Figura 38 Comando subinterfaces en R3.



D2, habilitamos el comando “ip routing”, para habilitar previamente el ruteo IP, posteriormente debemos dar el comando “switchport” consiste en una combinación en la forma del sistema de troncalizado de VLAN y enlaces de acceso. Los enlaces generales pueden tener tramas etiquetadas y sin etiquetar. Podemos decir todas las tramas que se envían a una VLAN específica deben etiquetarse. Así todas las tramas sin etiquetar se envían a VLAN nativa. También en la configuración debemos dar el comando “encapsulation dot1q” para habilitar 802.1Q y asociar la VLAN específica a la subinterfaz, así mismo configurar las Vlan permitidas y la Vlan nativa.

D2(config)#ip routing

D2(config-if)#intergafe e1/0

D2(config-if)#switchport

D2(config-if)#switchport trunk encapsulation dot1q

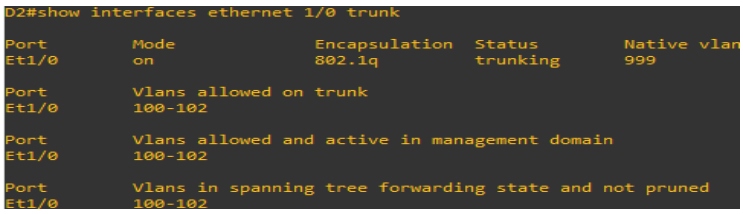
D2(config-if)#switchport mode trunk

D2(config-if)#switchport trunk allowed vlan 100,101,102

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

D2#show interfaces ethernet 1/0 trunk

Figura 39 Comando interface en D2.



Configuración de HSRPv2 en R1

Tenemos que el protocolo de enrutamiento de espera activa (HSRP) se encarga de desacoplar las direcciones IP de la interfaz física y las asocia a grupos de interfaces, habilitando la redundancia del hardware. La principal característica del HSRP es la posibilidad de asignar direcciones IP virtuales a cada grupo. Si el Router primario deja de funcionar, el secundario ocupará su lugar, mientras que la dirección IP virtual continua igual sin cambiar.

R1 es el router primario para las VLANs 100 y 102; por lo tanto, su prioridad también se cambiará a 150.

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.

Configuramos el router HSRP grupo 104 para la VLAN 100

R1(config)#interface Ethernet 1/0.100	Configuro subinterfaz
R1(config-if)#standby version 2	Configura el HSRP versión 2
R1(config-if)#standby 104 ip 10.0.100.254	Define IP virtual grupo 104
R1(config-if)#standby 104 priority 150	Identifica prioridad del router
R1(config-if)#standby 104 preempt	Prioridad en el router activo
R1(config-if)#standby 104 track 4 decrement 60	Rastree el objeto 4

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.

R1(config)#interface Ethernet 1/0.101

R1(config-if)#standby version 2

R1(config-if)#standby 114 ip 10.0.101.254

R1(config-if)#standby 114 preempt

R1(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.

R1(config)#interface Ethernet 0/0.102

R1(config-if)#standby version 2

R1(config-if)#standby 124 ip 10.0.102.254

R1(config-if)#standby 124 priority 150

R1(config-if)#standby 124 preempt

R1(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.

R1(config)# ipv6 unicast-routing

1(config)#interface Ethernet 1/0.100

R1(config-if)#standby 106 ipv6 autoconfig

R1(config-if)#standby 106 priority 150

R1(config-if)#standby 106 preempt

R1(config-if)#standby 106 track 6 decrement 60

R1(config-if)#ipv6 address 2001:db8:100:100::254/64

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.

R1(config)#interface Ethernet 1/0.101

R1(config-if)#standby 116 ipv6 autoconfig

R1(config-if)#standby 116 preempt

R1(config-if)#standby 116 track 6 decrement 60

R1(config-if)#ipv6 address 2001:db8:100:101::254/64

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.

R1(config)#interface fastEthernet 1/0.102

R1(config-if)#standby 126 ipv6 autoconfig

R1(config-if)#standby 126 priority 150

R1(config-if)#standby 126 preempt

R1(config-if)#standby 126 track 6 decrement 60

R1(config-if)#ipv6 address 2001:db8:100:102::254/64

R1# show ipv6 interface FastEthernet 0/0/1

Comando show standby brief, para ver la subinterfaz, grupo y prioridad HSRP, podemos ver como se encuentra correcta configuración con los estados de Vlan 100 y 102 Activo-Standby, para la Vlan 101 Standby-Activo en HSRP en R3.

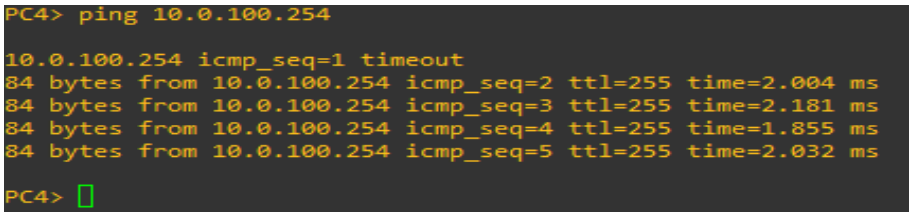
Figura 40 Comando ver subinterfaces en R3

```
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et1/0.100   104  150 P Active  local           10.0.100.4      10.0.100.254
Et1/0.100   106  150 P Active  local           FE80::A8BB:CCFF:FE00:601
                                                                FE80::5:73FF:FEA0:6A
Et1/0.101   114  100 P Standby 10.0.101.4      local           10.0.101.254
Et1/0.101   116  100 P Standby FE80::A8BB:CCFF:FE00:601
                                                local           FE80::5:73FF:FEA0:74
Et1/0.102   124  150 P Active  local           10.0.102.4      10.0.102.254
Et1/0.102   126  150 P Active  local           FE80::A8BB:CCFF:FE00:601
                                                                FE80::5:73FF:FEA0:7E
```

Pruebas de R1 a D1

Cortamos el enlace de R1 a D1, para verificar la redundancia del enlace HSRP para la Vlan 100 IP 10.0.100.254, Vlan 101 IP 10.0.101.254 y Vlan 102 10.0.102.254.

Figura 41 Comando ping PC4



Después de cortar el enlace de R1 a D1, al hacer el Trace hacia la IP HSRP 10.0.100.254, nos muestra cómo se establece conexión mediante la PC4 a la interfaz 10.0.100.4 quien es la subinterfaz 100 en R3 y conecta mediante D2. Esto se repite desde PC3 y PC2

Figura 42 Trace desde PC4

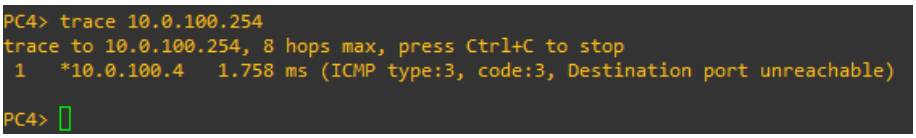


Figura 43 Trace desde PC3

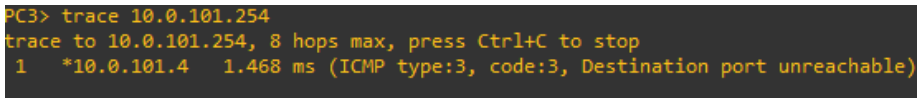
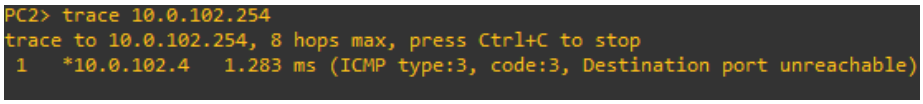


Figura 44 Trace desde PC2



Configuración de HSRPv2 en R3

Tenemos que el protocolo de enrutamiento de espera activa (HSRP) se encarga de desacoplar las direcciones IP de la interfaz física y las asocia a grupos de interfaces, habilitando la redundancia del hardware. La principal característica del HSRP es la posibilidad de asignar direcciones IP virtuales a cada grupo. Si el Router primario deja de funcionar, el secundario ocupará su lugar.

R3 es el router primario para la VLAN 101; por lo tanto, su prioridad también se cambiará a 150.

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.

Rastree el objeto 4 y decremente en 60.

Configuramos el router HSRP grupo 104 para la VLAN 100

R3(config)#interface Ethernet 1/0.100

R3(config-if)#standby version 2

R3(config-if)#standby 104 ip 10.0.100.254

R3(config-if)#standby 104 preempt

R3(config-if)#standby 104 track 4 decrement 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.

R3(config)#interface Ethernet 1/0.101

R3(config-if)#standby version 2

R3(config-if)#standby 114 ip 10.0.101.254

R3(config-if)#standby 114 priority 150

R3(config-if)#standby 114 preempt

R3(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.

```
R3(config)#interface Ethernet 0/0.102
R3(config-if)#standby version 2
R3(config-if)#standby 124 ip 10.0.102.254
R3(config-if)#standby 124 preempt
R3(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.

Habilite la preferencia (preemption).

Rastree el objeto 6 para disminuir en 60.

```
R3(config)# ipv6 unicast-routing                    Habilita HSRP para IPv6
R3(config)#interface Ethernet 1/0.100               Configuro interfaz
R3(config-if)#standby 106 ipv6 autoconfig           Define IP virtual grupo 106
R3(config-if)#standby 106 preempt                   Prioridad router activo
R3(config-if)#standby 106 track 6 decrement 60      Rastrear objeto 6
R3(config-if)#ipv6 address 2001:db8:100:100::4/64
```

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.

```
R3(config)#interface Ethernet 1/0.101
R3(config-if)#standby 116 ipv6 autoconfig
R3(config-if)#standby 116 priority 150
R3(config-if)#standby 116 preempt
```

R3(config-if)#standby 116 track 6 decrement 60

R3(config-if)#ipv6 address 2001:db8:100:101::4/64

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.

R3(config)#interface fastEthernet 1/0.102

R3(config-if)#standby 126 ipv6 autoconfig

R3(config-if)#standby 126 preempt

R3(config-if)#standby 126 track 6 decrement 60

R3(config-if)#ipv6 address 2001:db8:100:102::4/64

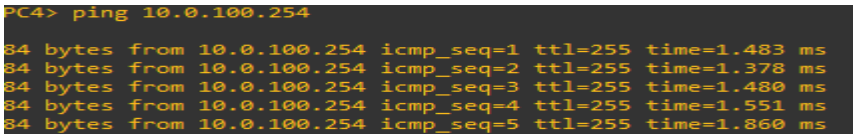
El comando show standby brief, para ver la subinterfaz, grupo y prioridad HSRP, podemos ver como se encuentra en correcta configuración con los estados de para la Vlan 101 Activo-Standby y para las Vlan 100 y 102 Standby-Activo en el HSRP en R1.

Figura 45 Comando subinterfaces en R3.

```
R3#sho standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et1/0.100   104  100 P Standby 10.0.100.3      local           10.0.100.254
Et1/0.100   106  100 P Standby FE80::A8BB:CCFF:FE00:401
                                               local           FE80::5:73FF:FEA0:6A
Et1/0.101   114  150 P Active  local           10.0.101.3      10.0.101.254
Et1/0.101   116  150 P Active  local           FE80::A8BB:CCFF:FE00:401
                                                               FE80::5:73FF:FEA0:74
Et1/0.102   124  100 P Standby 10.0.102.3      local           10.0.102.254
Et1/0.102   126  100 P Standby FE80::A8BB:CCFF:FE00:401
                                               local           FE80::5:73FF:FEA0:7E
```

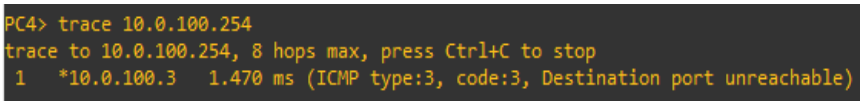
Pruebas de conectividad, para validar aplicación de HSRP en R3, Cortamos el enlace de R3 a D2, para verificar la redundancia del enlace HSRP para la Vlan 100 IP 10.0.100.254, Vlan 101 IP 10.0.101.254 y Vlan 102 10.0.102.254.

Figura 46 Comando ping desde PC4



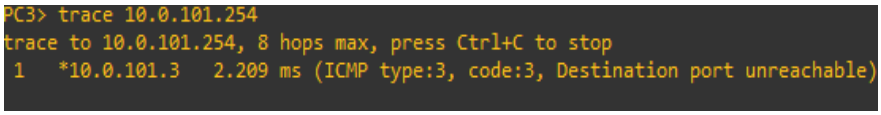
Trace hacia la PC4 a la IP HSRP 10.0.100.254 pertenece a Vlan100, nos muestra cómo se establece la conexión mediante la interfaz 10.0.100.3 quien es la subinterfaz 100 en R1 y conecta mediante D1.

Figura 47 Comando trace desde PC4



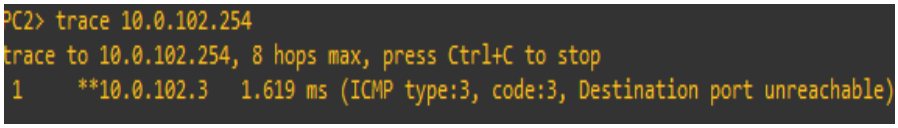
Trace desde PC3 a la IP HSRP 10.0.101.254 pertenece a Vlan101, nos muestra cómo se establece la conexión mediante la interfaz con IP 10.0.101.3 quien es la subinterfaz 101 en R1 y conecta mediante D1. Vemos la aplicación de la prioridad aplicada en R3.

Figura 48 Comando trace desde PC3



Trace hacia la PC2 a IP HSRP 10.0.102.254 pertenece a Vlan102, nos muestra cómo se establece la conexión mediante la interfaz con IP 10.0.102.3 quien es la subinterfaz 102 en R1 y conecta mediante D1

Figura 49 Comando trace desde PC2



Parte 5: Seguridad

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

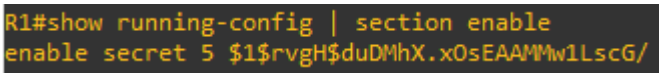
5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encripción SCRYPT.

EL comando enable secret se utiliza para restringir el acceso al modo EXEC privilegiado. Se recomienda habilitar para que la contraseña este cifrada.

R1(config)#enable secret cisco12345cisco

R1#show running-config | section enable

Figura 50 Comando verifica running config de R1



R2(config)#enable secret cisco12345cisco

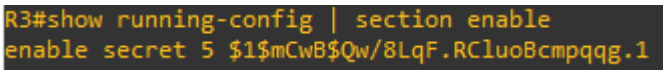
R2#show running-config | section enable

Figura 51 Comando verifica running config de R2

R3(config)#enable secret cisco12345cisco

R3#show running-config | section enable

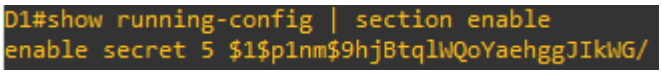
Figura 52 Comando verifica running config de R3



D1(config)#enable secret cisco12345cisco

D1#show running-config | section enable

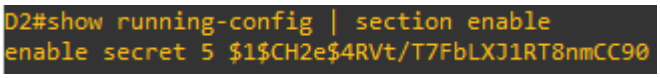
Figura 53 Comando verifica running config de D1



D2(config)#enable secret cisco12345cisco

D2#show running-config | section enable

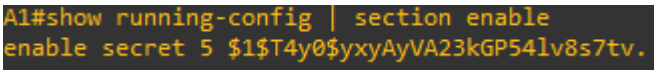
Figura 54 Comando verifica running config de D2



A1(config)#enable secret cisco12345cisco

A1#show running-config | section enable

Figura 55 Comando verifica running config de A1



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

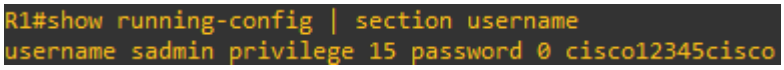
Nivel de privilegio 15

Contraseña: cisco12345cisco

R1(config)#username sadmin privilege 15 password cisco12345cisco

R1#show running-config | section username

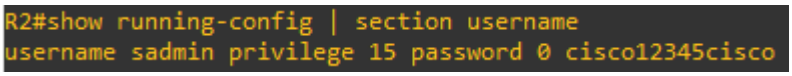
Figura 56 Comando verifica running config de R1



R2(config)#username sadmin privilege 15 password cisco12345cisco

R2#show running-config | section username

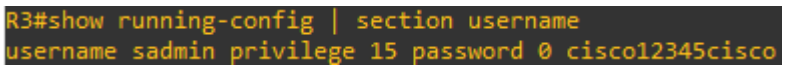
Figura 57 Comando verifica running config de R2



R3(config)#username sadmin privilege 15 password cisco12345cisco

R3#show running-config | section username

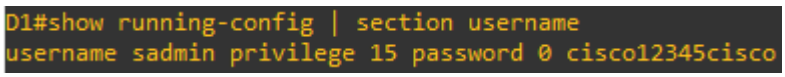
Figura 58 Comando verifica running config de R3



D1(config)#username sadmin privilege 15 password cisco12345cisco

D1#show running-config | section username

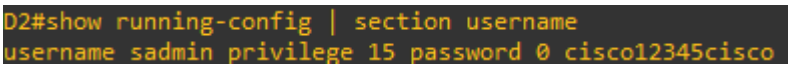
Figura 59 Comando verifica running config de D1



D2(config)#username sadmin privilege 15 password cisco12345cisco

D2#show running-config | section username

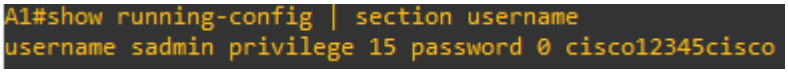
Figura 60 Comando verifica running config de D2



A1(config)#username sadmin privilege 15 password cisco12345cisco

A1#show running-config | section username

Figura 61 Comando verifica running config en A1

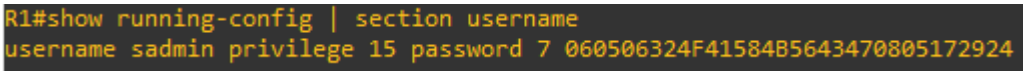


El comando de configuración global service password-encryption le indica a Cisco IOS Software que cifre las contraseñas, los secretos de Challenge Handshake Authentication Protocol (CHAP) y datos similares que se guardan en su archivo de configuración. Dicho cifrado es útil para evitar que observadores casuales lean las contraseñas

R1(config)#service password-encryption

R1#show running-config | section username

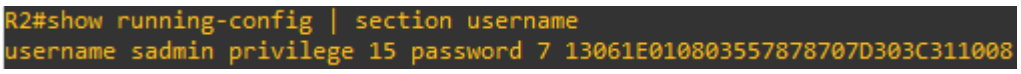
Figura 62 Comando verifica running config en R1



R2(config)#service password-encryption

R2#show running-config | section username

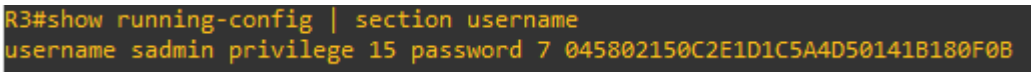
Figura 63 Comando verifica running config en R2



R3(config)#service password-encryption

R3#show running-config | section username

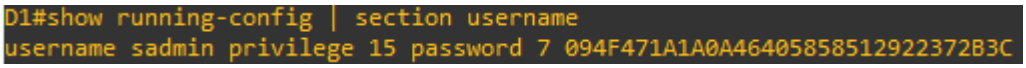
Figura 64 Comando verifica running config en R3



D1(config)#service password-encryption

D1#show running-config | section username

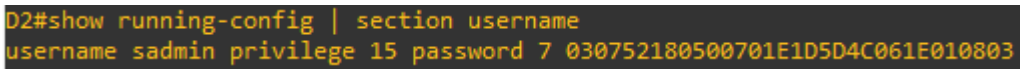
Figura 65 Comando verifica running config en D1



D2(config)#service password-encryption

D2#show running-config | section username

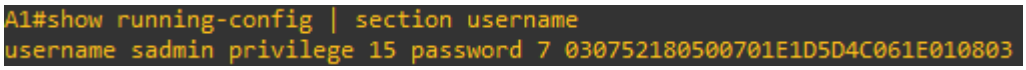
Figura 66 Comando verifica running config de D2



A1(config)#service password-encryption

A1#show running-config | section username

Figura 67 Comando verifica running config en A1



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

R1(config)#aaa new-model

R3(config)#aaa new-model

D1(config)#aaa new-model

D2(config)#aaa new-model

A1(config)#aaa new-model

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

Password compartida entre servidor Radius y dispositivos de red.

R1(config)# radius-server host 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass

R3(config)# radius-server host 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass

D1(config)# radius-server host 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass

D2(config)# radius-server host 10.0.100.6 auth-port 1812 acct-port 1813 key $trongPass

A1(config)# radius-server host 10.0.100.6 auth-port 1812 acct-port 1813 key $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.

Todos los usuarios que quieran iniciar una sesión de acceso deben estar autorizados mediante Radius (primer método) o mediante la base de datos local (segundo método). Entonces este comando indica primero que se hará la autenticación por Radius y si falla se hará local.

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

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

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

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

A1(config)# aaa authentication login default group RADIUS 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.

Nota: para realizar las pruebas de acceso, de forma adecuada por recomendaciones del tutor basta en la imagen que solicite usuario y contraseña para verificar aplicación del servidor Radius implementado.

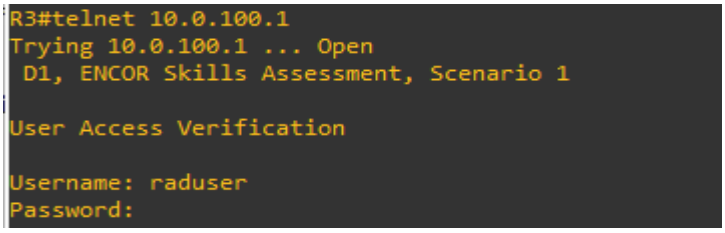
Configuración de línea vty para hacer pruebas de acceso en dispositivos de red.

R1(config)# line vty 0 4

R1(config)# login authentication RADIUS

R1(config)# exit

Figura 68 Acceso por telnet R3 a R1

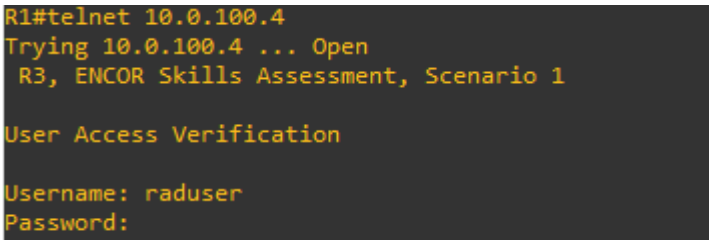


R3(config)# line vty 0 4

R3(config)# login authentication RADIUS

R3(config)# exit

Figura 69 Acceso por telnet R1 a R3

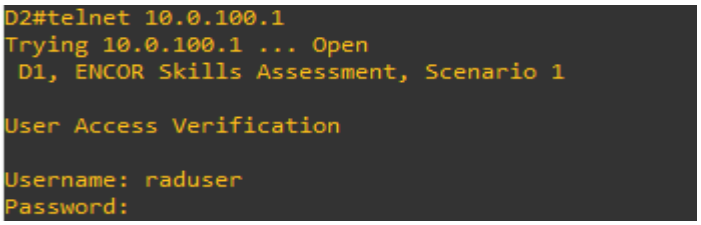


D1(config)# line vty 0 4

D1(config)# login authentication RADIUS

D1(config)# exit

Figura 70 Acceso por telnet D2 a D1

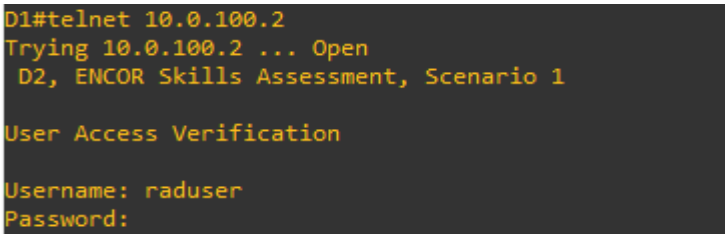


D2(config)# line vty 0 4

D2(config)# login authentication RADIUS

D2(config)# exit

Figura 71 Acceso por telnet D1 a D2

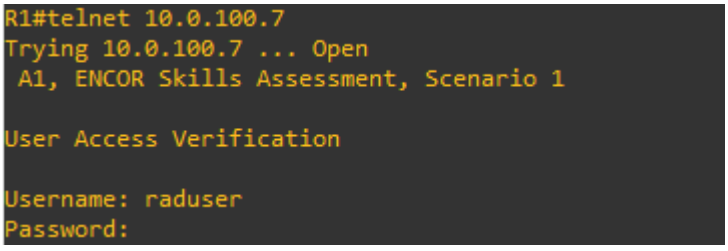


A1(config)# line vty 0 4

A1(config)# login authentication RADIUS

A1(config)# exit

Figura 72 Acceso por telnet R1 a A1



Parte 6: Configure las funciones de Administración de Red

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

Configure el reloj local a la hora UTC actual.

Nota importante: este comando debe ser dado en modo de usuario privilegiado

R1#clock set 20:59:42 19 nov 2021

R1# show clock detail

Figura 73 verifica la hora del sistema en R1

```
R1#show clock detail
21:01:02.915 UTC Fri Nov 19 2021
Time source is user configuration
```

R2#clock set 20:59:42 19 nov 2021

R2# show clock detail

Figura 74 verifica la hora del sistema en R2

```
R2#show clock detail
21:01:02.985 UTC Fri Nov 19 2021
Time source is user configuration
```

R3#clock set 20:59:42 19 nov 2021

R3# show clock detail

Figura 75 verifica la hora del sistema en R3

```
R3#show clock detail
21:01:03.220 UTC Fri Nov 19 2021
Time source is user configuration
```

D1#clock set 20:59:42 19 nov 2021

D1# show clock detail

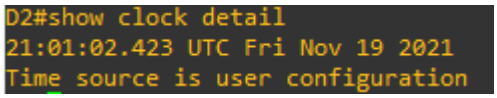
Figura 76 verifica la hora del sistema en D1

```
D1#show clock detail
21:01:01.869 UTC Fri Nov 19 2021
Time source is user configuration
```

D2#clock set 20:59:42 19 nov 2021

D2# show clock detail

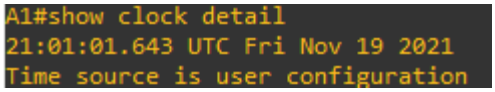
Figura 77 verifica la hora del sistema en D2



A1#clock set 20:59:42 19 nov 2021

A1# show clock detail

Figura 78 verifica la hora del sistema en A1



6.2 Configure R2 como un NTP maestro.

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

Podríamos considerarlo como un sistema que es usado para lograr un sincronismo de la hora a través de redes de comunicaciones. A nivel de estructura de protocolos, hay que decir que NTP está basado en UDP a nivel de transporte (User Datagram Protocol), por lo que va a permitir optimizar las comunicaciones sin necesidad de establecer una conexión previa como sucede en TCP.

Además, otro signo característico de NTP es que usa el puerto 123, aspecto a considerar para permitir comunicaciones a través de firewalls.

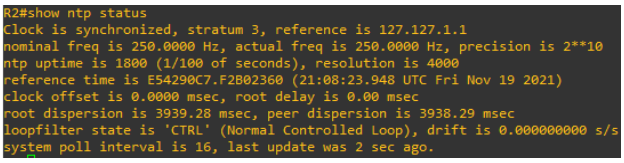
El fundamento del mecanismo de NTP se basa fundamentalmente en el uso de una fuente de tiempo, que va a permitir actualizar y sincronizar la hora en los dispositivos que están trabajando en una red.

Los diferentes niveles de estrato (Stratum) definen la distancia desde el reloj de referencia. Entonces Un servidor de stratum 2 está conectado al servidor de stratum 1. Por otro lado, un servidor de stratum 3 se conectaría al servidor de stratum 2 y así sucesivamente, para concluir un servidor de stratum 3 obtiene su tiempo a través de solicitudes de paquetes NTP de un servidor de stratum 2.

R2(config)#ntp master 3

R2#show ntp status

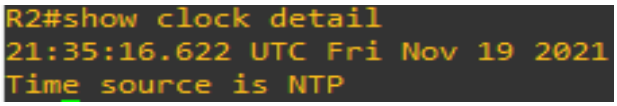
Figura 79 Comando ntp en R2



Vemos la hora actual en el reloj. Con la opción detail, vemos el tiempo está configurado por el usuario. Esto significa que la hora se configuró manualmente.

R2# show clock detail

Figura 80 comando verifica la hora en R2



6.3 Configure NTP en R1, R3, D1, D2, y A1.

Configure NTP de la siguiente manera:

R1 debe sincronizar con R2.

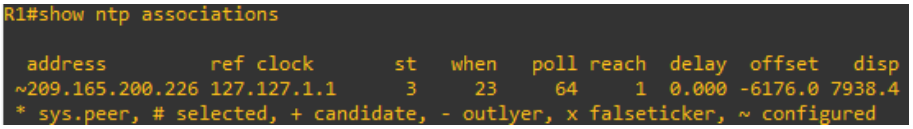
Se configuro con ntp server, para sincronizar con R2.

R1(config)#ntp server 209.165.200.226

Permite validar con quien se está sincronizando y ver el estrato, que para nuestro ejercicio R2 es de estrato st 3.

R1#show ntp associations

Figura 81 verifica ntp en R1



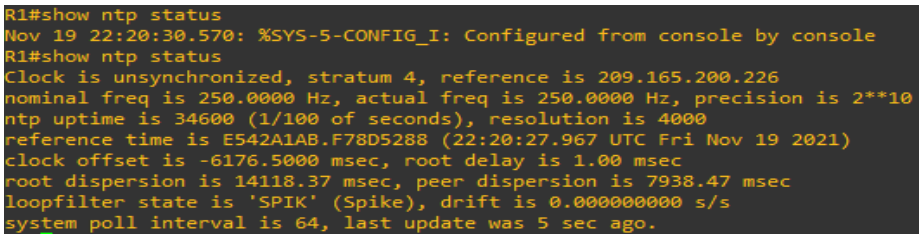
R3, D1 y A1 para sincronizar la hora con R1.

R1(config)#ntp master 4

R1 cambia de estrato 4, por estar asociado de R2, quien pertenece al estrato 3, por implementación NTP, toma un cambio en la jerarquía, aumentado el número según orden en la ramificación.

R1#show ntp status

Figura 82 verifica ntp en R1



R3(config)#ntp server 10.0.10.1

Podemos ver R1 con la dirección IP del servidor ntp 10.0.10.1 y estrato 4, quien a su vez toma referencia de R2 con IP 209.165.200.226.

R3#show ntp associations

Figura 83 verifica asociación ntp en R3

```
R3#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~10.0.10.1       209.165.200.226  4      0     64     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

D1(config)#ntp server 10.0.10.1

Podemos ver D1, sincronizando con la dirección IP del servidor ntp R1 10.0.10.1.

D1#show ntp associations

Figura 84 verifica asociación ntp en D2

```
D2#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~10.0.10.1       .INIT.          16      -     64     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

A1(config)#ntp server 10.0.10.1

Podemos ver A1, sincronizando con la dirección IP del servidor ntp R1 10.0.10.1.

A1#show ntp associations

Figura 85 verifica asociación ntp en A1

```
A1#show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~10.0.10.1       .INIT.          16      -     64     0  0.000   0.000 15937.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

D2 para sincronizar la hora con R3.

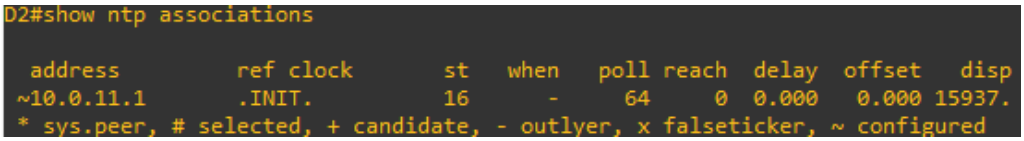
R3(config)#ntp master 5

Podemos ver D2, sincronizando con la dirección IP del servidor ntp R3 10.0.11.1.

D2(config)#ntp server 10.0.11.1

D2#show ntp associations

Figura 86 verifica asociación ntp en D2



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.

Para ver los mensajes de syslog, se debe instalar un servidor quien será el syslog en una estación de trabajo en la red. Hay diferentes versiones de freeware y shareware de syslog, y versiones de pago o empresariales.

El servidor de syslog proporciona una interfaz intuitiva y amigable de usar para que el administrador pueda ver el resultado de syslog. El servidor analiza el resultado y organiza los mensajes en columnas predefinidas para que se puedan interpretar con facilidad.

Par enviar mensajes de registro a un servidor syslog remoto. Al usar esto, podemos enviar mensajes a un dispositivo externo para almacenar estos registros y el tamaño de almacenamiento depende del espacio disponible en disco del servidor.

Tenemos los niveles de Syslog:

Emergency: 0, Alert: 1, Critical: 2, Error: 3, Warning: 4, Notice: 5, Informational: 6, Debug: 7

Utilice el nivel de depuración con precaución, ya que puede generar una gran cantidad de tráfico de syslog en una red ocupada.

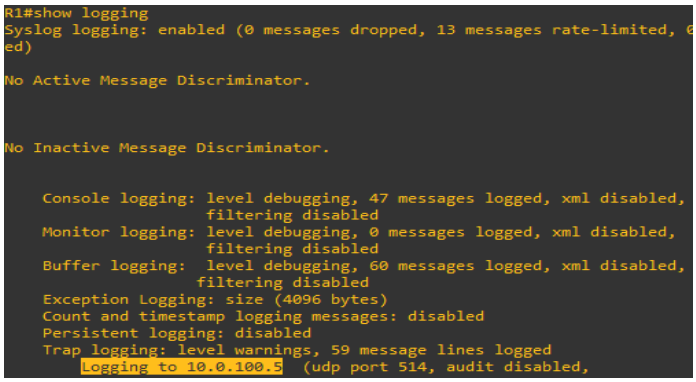
R1#conf t

R1(config)#logging host 10.0.100.5

R1(config)#logging trap warnings

R1#show logging

Figura 87 Comando ver syslog en R1



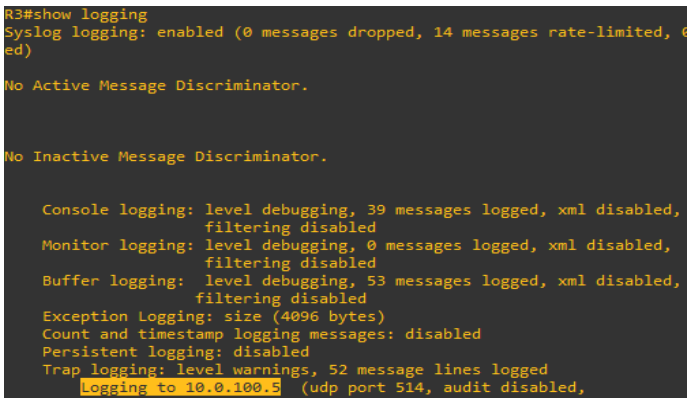
R3#conf t

R3(config)#logging host 10.0.100.5

R3(config)#logging trap warnings

R3#show logging

Figura 88 Comando ver syslog en R3



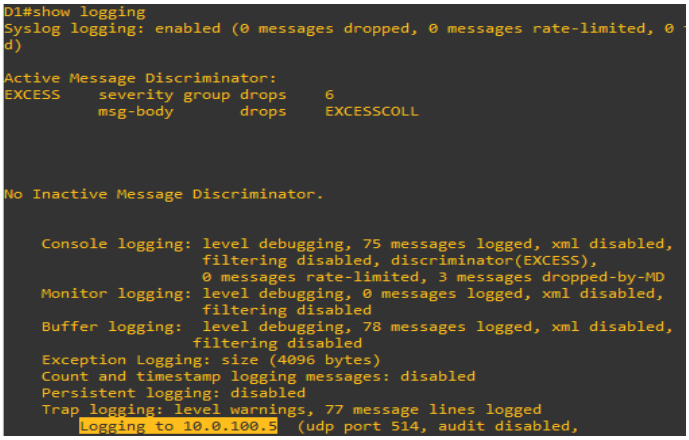
D1#conf t

D1(config)#logging host 10.0.100.5

D1(config)#logging trap warnings

D1#show logging

Figura 89 Comando ver syslog en D1



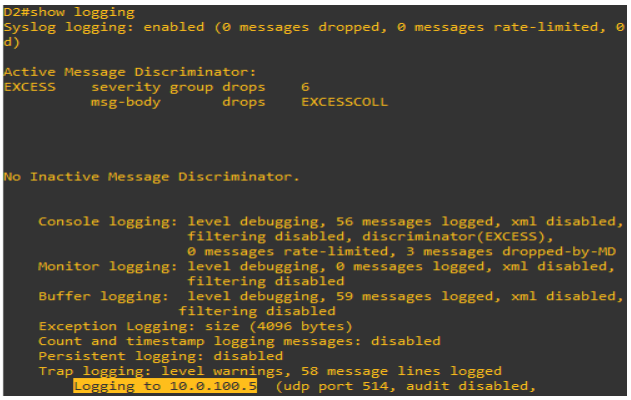
D2#conf t

D2(config)#logging host 10.0.100.5

D2(config)#logging trap warnings

D2#show logging

Figura 90 Comando ver syslog en D2



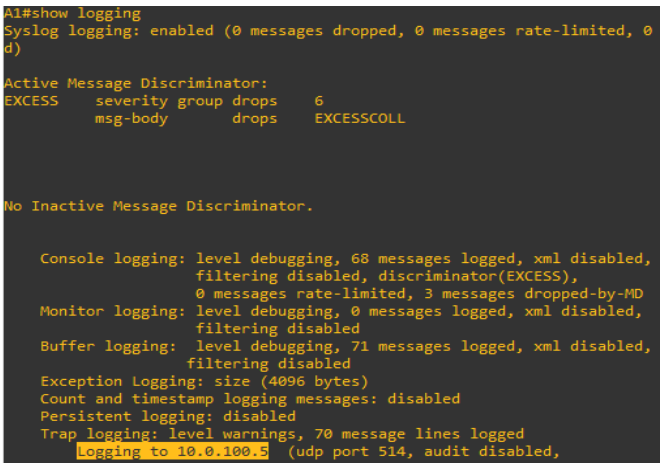
A1#conf t

A1(config)#logging host 10.0.100.5

A1(config)#logging trap warnings

A1#show logging

Figura 91 Comando ver syslog en A1



6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Especificaciones de SNMPv2:

Únicamente 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 habilite el envío de traps ipsla y ospf.

Se establece la comunidad snmp ENCORSA, tambien configuramos snmp en modo lectura Read-Only, además de la configuración con el valor de contacto SNMP con mi nombre “FILEMAN” y se habilita el envío de traps isla y ospf,

R3(config)#snmp-server host 10.0.100.5 version 2c ENCORSA

R3(config)#snmp-server community private ro

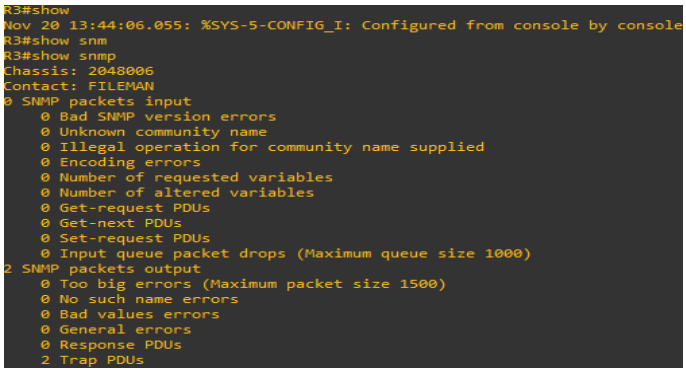
R3(config)#snmp-server contact FILEMAN

R3(config)#snmp-server enable traps ipsla

R3(config)#snmp-server enable traps ospf

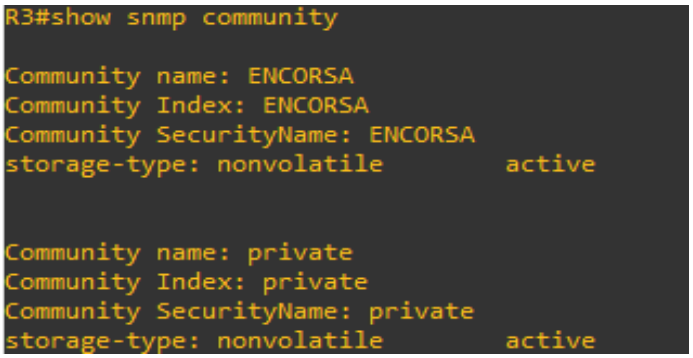
R3#show snmp

Figura 92 Comando ver snmp en R3



R3#show snmp community

Figura 93 Comando ver snmp en R3



R3#show snmp contact

Figura 94 Comando ver snmp en R3

En D1, habilite el envío de traps ipsla y ospf.

D1(config)#snmp-server host 10.0.100.5 version 2c ENCORSA (Se establece el community string en ENCORSA.

D1(config)#snmp-server community private ro	Modo lectura Read-Only
D1(config)#snmp-server contact FILEMAN	Configuración contacto
D1(config)#snmp-server enable traps isla	Habilito el envío de traps.
D1(config)#snmp-server enable traps ospf	Habilito el envío de traps.

D1#show snmp

Figura 95 Comando ver snmp en D1

```
SNMP logging: enabled
    Logging to 10.0.100.5.162, 0/10, 0 sent, 0 dropped.
D1#
```

D1#show snmp community

Figura 96 Comando ver snmp en D1

```
D1#show snmp community

Community name: ENCORSA
Community Index: ENCORSA
Community SecurityName: ENCORSA
storage-type: nonvolatile        active
```

D1#show snmp contact

Figura 97 Comando ver snmp en D1

```
D1#show snmp contact
FILEMAN
```

En D2, habilite el envío de traps ipsla y ospf.

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

D2(config)#snmp-server community private ro

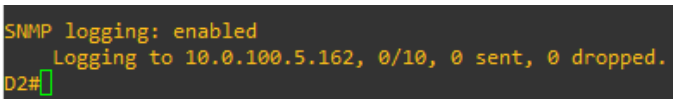
D2(config)#snmp-server contact FILEMAN

D2(config)#snmp-server enable traps ipsla

D2(config)#snmp-server enable traps ospf

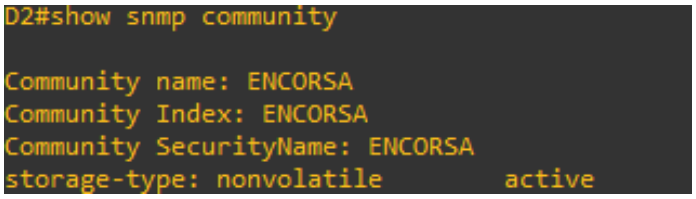
D2#show snmp

Figura 98 Comando ver snmp en D2



D2#show snmp community

Figura 99 Comando ver snmp en D2



D2#show snmp contact

Figura 100 Comando ver snmp en D2

En R1, habilite el envío de traps ipsla, bgp y ospf.

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

R1(config)#snmp-server community private ro

R1(config)#snmp-server contact FILEMAN

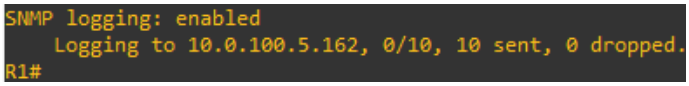
R1(config)#snmp-server enable traps ipsla

R1(config)#snmp-server enable traps bgp

R1(config)#snmp-server enable traps ospf

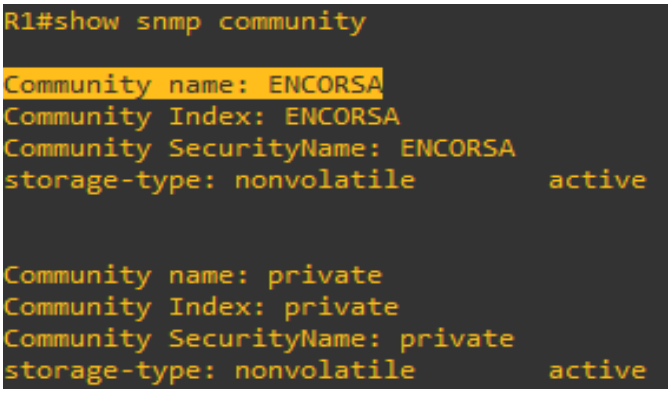
R1#show snmp

Figura 101 Comando ver snmp en R1



R1#show snmp community

Figura 102 Comando ver snmp en R1



R1#show snmp contact

Figura 103 Comando ver snmp en R1

En A1, habilite el envío de traps config.

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

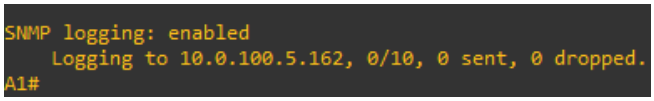
A1(config)#snmp-server community private ro

A1(config)#snmp-server contact FILEMAN

A1(config)#snmp-server enable traps ipsla

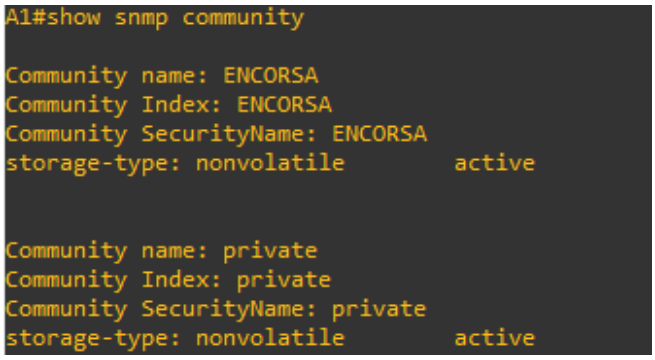
A1#show snmp

Figura 104 Comando ver snmp en A1



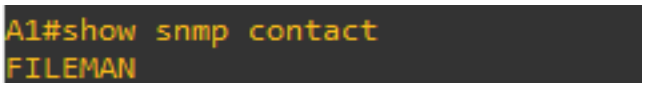
A1#show snmp community

Figura 105 Comando ver snmp en A1



R1#show snmp contact

Figura 106 Comando ver snmp en A1



CONCLUSIONES

Con la implementación de las distintas técnicas de Networking empleadas en el presente trabajo, se logra la reducción de fallos en la de red con enlaces redundantes, regalando adicionalmente un mayor ancho de banda en el transporte de la información, para satisfacer las necesidades de conectividad de la organización.

Regalar una capa adicional de seguridad para la organización, empleado técnicas de segmentación de red, dividiendo las redes planas de Capa 2 en múltiples grupos lógicos de trabajo denominados (dominios de broadcast), los cuales permiten reducir el tráfico en la red y potencia el rendimiento de la red, mitigando tormentas que puedan afectar las comunicaciones.

Conseguimos realizar un enrutamiento adecuado, presentando las redes que necesitamos publicar con el uso del protocolo BGP, entre los router de la compañía y del ISP, permitiendo realizar un control adecuado y administración idónea para hacer una red redundante y de bajo costo.

Conseguimos Construir la red de forma segura, con la debida utilización de diversos mecanismos de seguridad, aplicado a los dispositivos de la topología el acceso a los mismos, mediante un servidor Radius regalando Autenticación, autorización, contabilidad (AAA), además de mecanismos como Syslog, NTP y SNMP para contar con visibilidad para eventos en la Red, de esta forma poder hacer seguimiento con información de fecha y hora actualizadas.

BIBLIOGRÁFIA

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

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

CISCO. (2020). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

Configuración DHCP en Router (s.f), 27 de mayo de (2018), Recuperado de

https://apuntesdecisco.blogspot.com/2008/07/configuracin-de-dhcp-en-elrouter.html

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ

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

OSPFv3 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

Security Cisco. (2018). Guía de Cisco para fortalecer los dispositivos Cisco IOS. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/13608-21.html

SNMPv2 Edgeworth, Cisco. (2005). How to Configure SNMP Community Strings. SNMP v2. CCNP. Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html