SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

EDWARD TRIANA MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

FACATATIVÁ

2020

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

EDWARD TRIANA MORENO

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

PRESENTADO A:

MSc. DIEGO ÉDISON RAMÍREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA ELECTRÓNICA

FACATATIVÁ

2020

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Facatativá, 20 de octubre de 2020

AGRADECIMIENTOS

Agradezco infinitamente a Dios, por brindarme la oportunidad de culminar una meta más en mi vida. Por siempre estar a mi lado, por dame el entendimiento y la sabiduría en cada una de las etapas de la carrera.

A mi familia, que es el motor de mi vida, por darme las fuerzas, el apoyo, y el entusiasmo para el logro de cada una de las metas. A ellos y para ellos es este nuevo logro.

A mis amigos, compañeros y todo el cuerpo de tutores de la universidad que fueron parte activa en esta etapa de mi vida. Por compartir su tiempo y conocimientos conmigo, para hoy dar un escalón más lleno de conocimiento y confianza como ingeniero Electrónico.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

DNS: proviene del término inglés Domain Name System: que significa, Sistema de Nombres de Dominio. Se emplea para denominar a los dispositivos que se conectan a una red por medio de una IP (Internet Protocol o Protocolo de Internet).

INTERFAZ: se conoce como el medio que realiza la interconexión de dos procesos diferentes con un propósito común. Se define como Interfaz a los medios utilizados para la conexión de un computador como medio de transporte de la red.

MÁSCARA DE SUBRED: es especialmente necesaria al momento de señalar la dirección de red correspondiente a cada subred, es la que se encuentra referenciada en la tabla de enrutamiento.

PREFIJO IP: Es una forma especial de expresar las direcciones de red y sus máscaras de red, se identifica la cantidad de bits que aparecen en la máscara de subred.

PROTOCOLOS DE RED: conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a la red. Se componen de instrucciones que permiten a los dispositivos vincularse entre sí, además de emplear reglas de formateo, para que los mensajes viajen de forma adecuada de inicio a fin. Dichas reglas determinan si los datos son recibidos, rechazados o ha ocurrido algún tipo de problema en el transporte de la información.

ROUTER: Dispositivo hardware o software de interconexión de redes para equipos de cómputo, que opera en la capa tres del modelo OSI. Este dispositivo conecta partes de red o redes enteras.

RESUMEN

La actividad denominada “Prueba de habilidades prácticas”, hace parte de las actividades evaluativas del Diplomado de Profundización CCNA, que identifica el grado de desarrollo de competencias y habilidades que se consiguieron a lo largo del curso. Lo esencial es identificar los niveles de comprensión y solución de problemas relacionados con diferentes aspectos de Networking que se pueden enfrentar en la realidad.

Palabras clave: CISCO, Conmutación, Enrutamiento, Redes, Sistemas.

ABSTRAC

The activity called “Practical skills test” is part of the evaluative activities of the CCNA Deepening Diploma, which identifies the degree of development of skills and abilities that were achieved throughout the course. The essential thing is to identify the levels of understanding and solution of problems related to different aspects of Networking that can be faced in reality.

Key words: cisco, Switching, Routing, Networks, Systems.

INTRODUCCIÓN

La realización de la evaluación final del diplomado de profundización en cisco CCNA, nos permite desarrollar dos escenarios especificando los comandos utilizados en el proceso de configuración y verificación de la conexión, por puertos ethernet o seriales de los distintos dispositivos como router, switch y PC's por medio del programa de Cisco Packet Tracer.

Inicialmente, en cada uno de los ejercicios, se realiza la topología de red y las configuraciones básicas de los dispositivos. En el primer escenario, se configuran los dispositivos de una red pequeña en enrutamiento entre VLAN, DHCP, Etherchannel y port security y por último se verifican los enrutamientos IP realizados con el comando show ip route.

En el segundo escenario, se realiza la configuración del protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente y por último se verifica este procedimiento de seguridad de switches, routing entre VLAN de extremo a extremo.

2. OBJETIVOS

2.1 Objetivo General

Aplicar el enrutamiento, parámetros de seguridad y acceso en diferentes dispositivos de una red, con las configuraciones OSPF, RIP ver 2.0, e implementación DHCP, NAT, verificación de ACL.

2.2 Objetivos Específicos:

- Identificar los dispositivos a utilizar para la construcción de una topología de red, configurando los dispositivos a medida que se van implementando instrucciones de configuración.

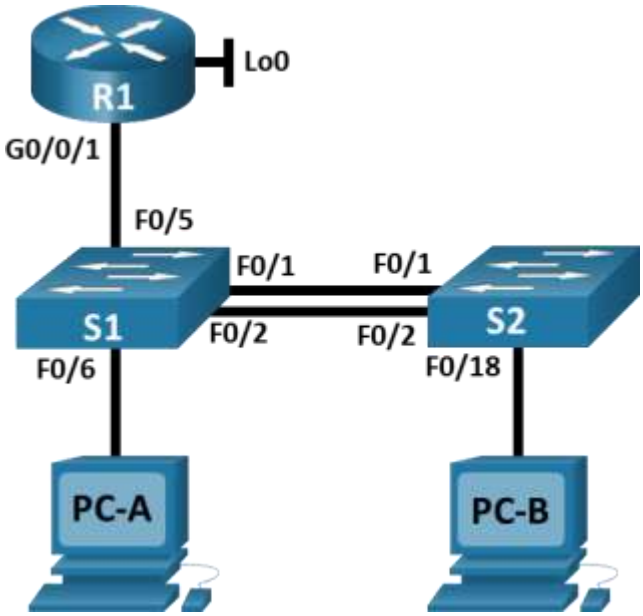
- Realizar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing, de DHCP, NAT, RIP Ver2, dando solución a ciertos problemas, Implementando la debida seguridad en los Router y políticas necesarias.

3. DESARROLLO DEL PROYECTO

3.1 ESCENARIO 1

Topología

Figura 1: Topología Escenario 1



Fuente: imagen de la prueba de habilidades

Topología que se va a desarrollar mediante el software packet tracer.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1: Asignación de las VLAN

Tabla de VLAN**VLAN**	**Nombre de la VLAN**
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Con la tabla 1 nombramos las VLAN que se desarrollaran más adelante.

Tabla de asignación de direcciones

Tabla 2: Asignación de Direcciones

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

La tabla 2 contiene las direcciones IP que se van a asignar en la actividad a cada uno de los dispositivos en la topología.

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

Parte 1: Inicializar y Recargar y Configurar Aspectos Básicos de los Dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

Tabla 3: Inicialización de router y los switches.

Reconfiguración de los dispositivos del escenario 1.	
Tarea	**Comando de ios**
Eliminar el archivo startup-config del router	Para eliminar el archivo startup-config del router, utilizamos el comando: Router#erase startup-config
Volver a cargar el router	Para cargar el router utilizamos: Router#reload

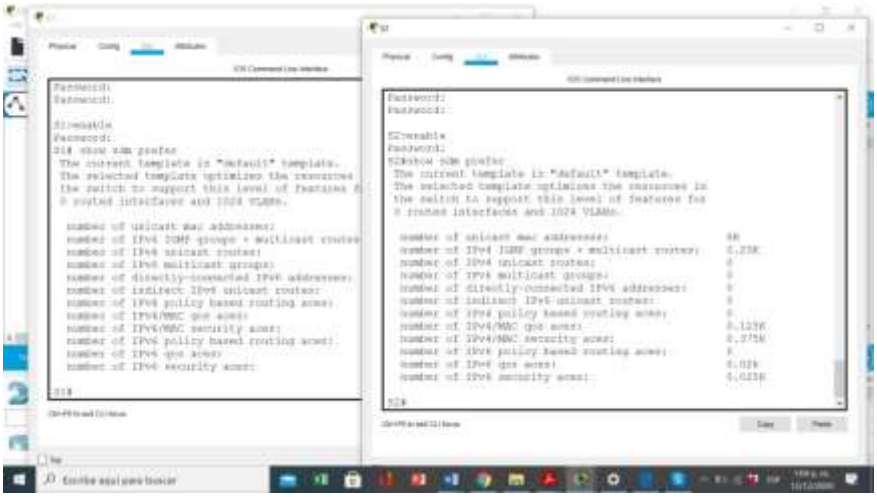
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Se utiliza el comando startup-config, y utilizamos el comando Vlan dat para eliminar bases de datos anteriores. Switch#erase startup-config. Switch#delete vlan.dat
Volver a cargar ambos switches	Para cargar de nuevo los swiches utilizamos el comando reload. Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Con el comando show flash, verificamos la memoria flash de los dos dispositivos. Switch#show flash

Con el desarrollo de la tabla 3 y usando los comando startup-config y VLAN ddat y reload , Borramos las configuraciones de inicio y las VLAN del router y del switch y se vuelve a cargar los dispositivos.

Tareas relacionadas con el reinicio de los dispositivos y su cargue para realizar la lista de comandos para cada uno de los dispositivos que tenemos en la topología.

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

Figura 2: recarga de los switch.



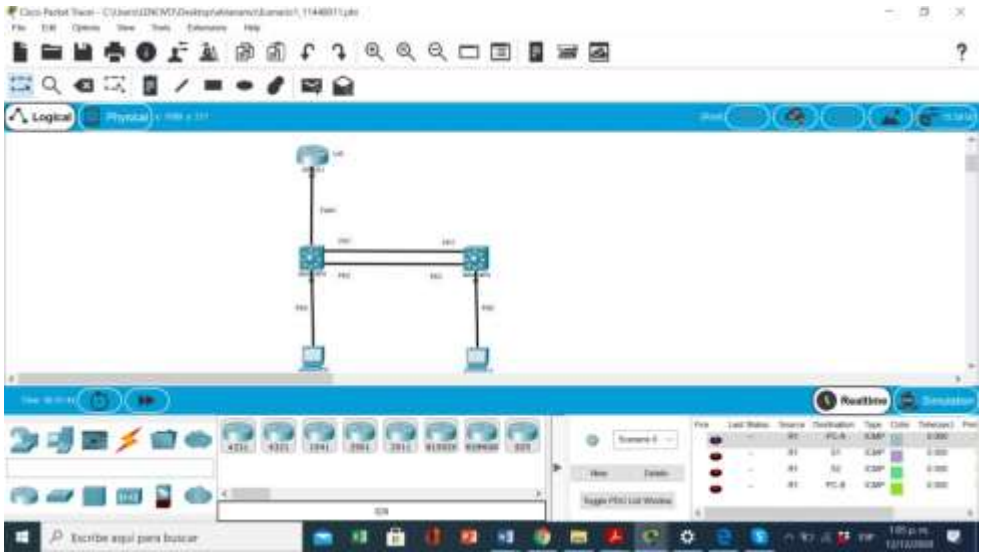
Fuente: Autor

En la figura 2 podemos ver como se recargo el switch y quedaron listo para comenzar a configurar.

Se utiliza el comando SDM, para que reconozca ipv6 que nos permite trabajar con direcciones de este tipo.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Figura 3: topología terminada



Fuente: Autor

En la figura 3 observamos la topología realizada para empezar a configurar de acuerdo a los solicitado.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4: Configuraciones básicas en R1 escenario 1.

Configuración del router 1	
Tarea	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda del DNS utilizamos el comando configure terminal y después indicamos que no busque el dominio. Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Utilizando el comando hostname la damos indicamos cual es nuestro router 1 Router(config)#hostname R1

Nombre de dominio	Para nombrar el dominio donde vamos a trabajar realizamos la configuración con ip domain name. R1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	Para acceder al modo privilegiado, configuramos con Enable secret la contraseña. R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Para ingresar a consola activamos el password y lo logiamos. R1(config)#line con 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	Siempre se debe tener una cantidad de caracteres para la contraseña. R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Creamos un usuario administrativo para que configure los demás dispositivos y establezca seguridad en la red. R1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Para utilizar las bases de datos locales se realizar la configuración VTY para utilizarlas. R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit

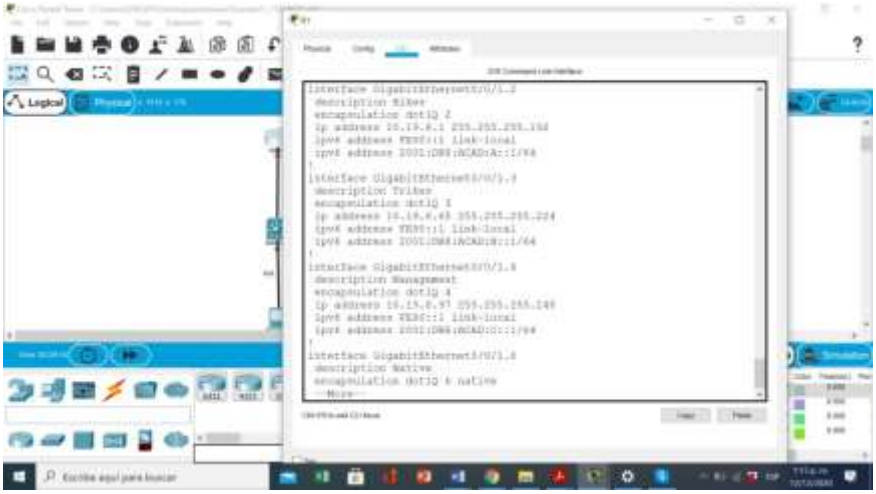
Configurar VTY solo aceptando SSH	Activamos VTY y configuramos SSH establecer sesión de red de modo seguro. R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Al cifrar las contraseñas establecemos una seguridad en la configuración en nuestra topología. R1(config)#service password-encryption
Configure un MOTD Banner	Utilizamos el comando MOTD Banner para establecer su configuración. R1(config)#banner motd #El acceso no autorizado está prohibido#
Habilitar el routing IPv6	Para habilitar las direcciones IPV6 utilizamos el comando unicast-routing. R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Realizamos la configuración de las entradas del router y le asignamos sus direcciones y que van a realizar cada interfaz. R1(config)#interface gi0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description LAN to VLAN2 R1(config-subif)#ip add 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#no shutdown R1(config-if)#no shutdown R1(config-subif)#exit

	R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#ip add 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#description LAN to VLAN3 R1(config-subif)#no shutdown R1(config-subif)#exit
	R1(config)#interface gi0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#ip add 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 add fe80::1 link-local R1(config-subif)#description LAN to VLAN4 R1(config-subif)#no shutdown R1(config-subif)#exit
	R1(config)#interface gi0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#exit
	R1(config)#interface gi0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	Se configure el comando loopback para mantener siempre funcionando el router. R1(config)#interface lo0 R1(config-if)#description LAN to Loopback0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 add 2001:db8:acad:209::1/64 R1(config-if)#ipv6 add FE80::1 link-local R1(config-if)#exit

Generar una clave de cifrado RSA	Generamos una nueva clave RSA para establecer interambio seguro share secret. R1(config)#crypto key generate rsa

Se realiza la lista de comandos para R1 con su conexión a red utilizamos la tabla 4, en la cual esta la asignación, se crean las respectivas sub interfaces, encapsulándolas con su VLAN y asignando los direccionamientos IPv4 e IPv6, además se genera una clave de cifrado RSA, se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de SSH.

Figura 4: configuración R1



Fuente: Autor

En la figura 4 Se realiza la configuración de R1 con las características descritas para el uso del router.

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 5: Configuraciones básicas en S1 del primer escenario.

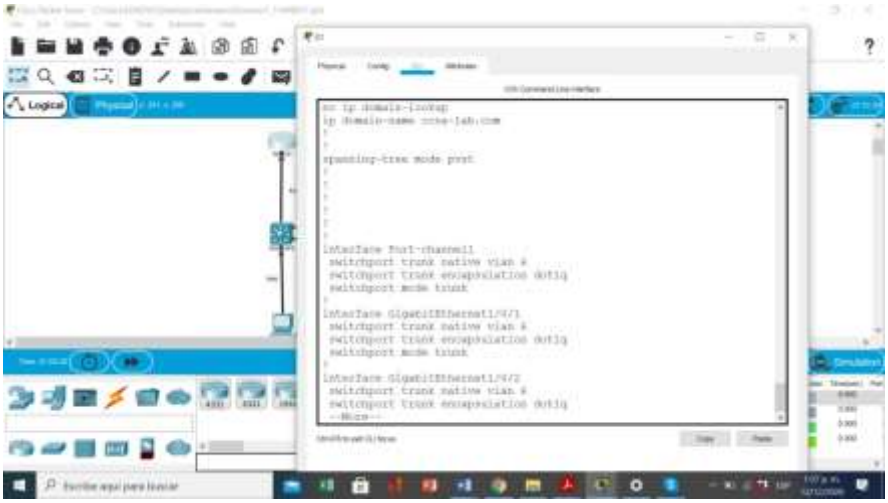
Configuración de S1	
Tarea	**Especificación**
Desactivar la búsqueda DNS.	Utilizando el comando no ip domain desactivamos la busqueda del DNS. S1(config)#no ip domain-lookup

Nombre del switch	Se le coloca nombre al switch para identificarlo en la configuración. Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain-name CCNA-Lab.com
Contraseña cifrada para el modo EXEC privilegiado	Se establece contraseña para el uso del modo privilegiado con su comando: S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Se realiza lista de comando con la contraseña de acceso a la consola y su login para seguridad. S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	Se crea el usuario administrativo para que establezca los comando en la red. S1(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Configuramos VTY para la utilización de datos locales. S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH.	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	Se configure para que se vea cifrado la contraseña y no sea revelada a extraños. S1(config)#service password-encryption
Configurar un MOTD Banner	Se realiza el comando para tener acceso a su configuración. S1(config)# banner motd #El acceso no autorizado está prohibido#
Generar una clave de cifrado RSA	Se configura su clave cifrada para un intercambio seguro de SSH. S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	Utilizando la interfaz SVI podemos crear su interfaz virtual en el switch. S1(config)#interface vlan 4 S1(config-if)#ip add 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 add 2001:db8:acad:c::98/64 S1(config-if)#ipv6 add fe80::98 link-local S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	Realizamos la configuración de su puerta predeterminada para e switch. S1(config)#ip default-gateway 10.19.8.97

En la tabla 5 usando la línea de comandos requeridas para la conexión del S1 a la topología utilizando los comandos del gateway para configurar su puerta predeterminada, su interfaz de administración SVI y generamos claves de intercambio seguro SSH con su nombre de domino CCNA-Lab.com.

Figura 5: configuración S1



Fuente: Autor

Se realiza la configuración de S1 para conectarse con los respectivos dispositivos.

Configuración S2.

Tabla 6: Configuraciones básicas en S2 del primer escenario.

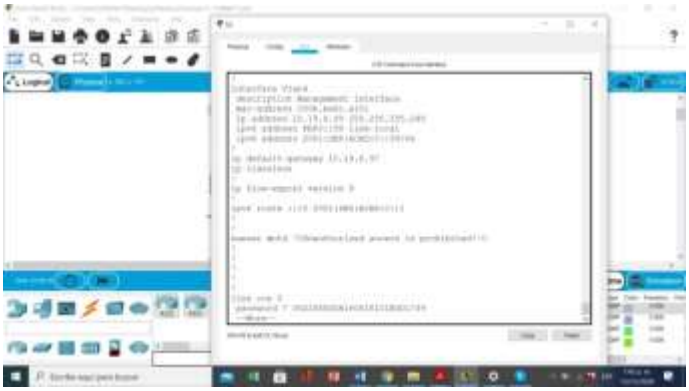
Configuración de switch2	
Tarea	**Especificación**
Desactivar la búsqueda DNS.	Utilizando el comando no ip domain desactivamos la busqueda del DNS S2(config)#no ip domain-lookup
Nombre del switch	Nombramos el switch para identificarlo en la topología. Switch(config)#hostname S1
Nombre de dominio	Le damos nombre al dominio para identificar la red de dominio. S2(config)#ip domain-name CCNA-Lab.com

Contraseña cifrada para el modo EXEC privilegiado	La seguridad que utilizamos es para evitar robo de información. S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	Establecemos contraseña de acceso a la consola para seguridad del dispositivo. S2(config)#line con 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	El usuario administrativo es importante para el manejo de la red. S2(config)#username admin privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se realiza la configuración VTY para el uso de datos locales. S2(config)#username admin privilege 15 secret admin1pass S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Esta configuración es para uso de conexiones SSH unicamente. S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit

Cifrar las contraseñas de texto no cifrado	Se cifran las contraseñas para mantener acceso unico al administrador. S2(config)#service password-encryption
Configurar un MOTD Banner	Se realiza la configuración para el acceso controlado a la topolgia. S2(config)#banner motd #El acceso no autorizado está prohibido#
Generar una clave de cifrado RSA	Generamos la clave RSA para el uso de algoritmos de sincronización simétricos. S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)#interface vlan 4 S2(config-if)#ip add 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db8:acad:c::99/64 S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97

En la tabla 6 realizamos Configuración del S2 para su conexión en la topología con el nombre de dominio CCNA-Lab.com realizando la configuración de cifrado de contraseñas, el inicio de sesión en las líneas VTY para que use la base de datos local y la configuración de su gateway 10.19.8.97.

Figura 6: configuración S2.



Fuente: Autor.

En la figura 6 podemos ver la realización del listado de comandos para la conexión de los puertos que se conectaran con los demás dispositivo en el switch 2.

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 7 Configuración de la infraestructura de red en S1

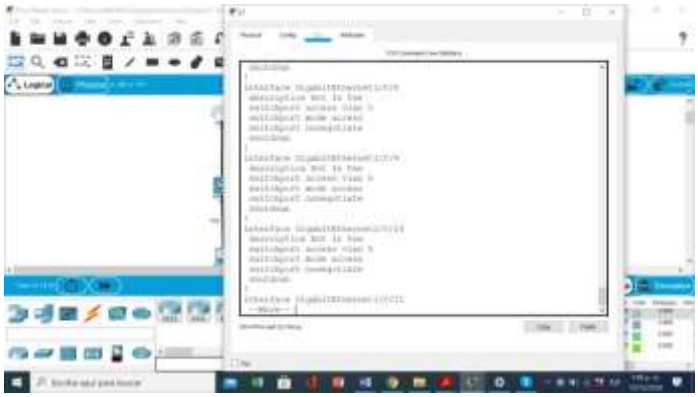
Configuración de S1	
Tarea	**Especificación**
Crear VLAN	La creación de la Vlan nos permite la administración de los dispositivos limitando su conexión. S1(config)#vlan 2,S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	La configuración de roncales, nos permite la conexión en las interfaces Fastethernet y gigabitethernet. S1#configure terminal S1(config)#interface fa0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1#configure terminal,S1(config)#interface fa0/2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit,S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	La creación de este grupo nos proporciona velocidad en los puertos FE y GE, igualando la velocidad en ellos. S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 2 mode active S1(config)#exit S1(config#interface port-channel 2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config)#switchport trunk native vlan 6

Configurar el puerto de acceso de host para VLAN 2	Se configure para la VLAN2 para que el acceso sea exclusivo en el host de la topología. S1(config)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shutdown S1(config-if)#exit
Configurar la seguridad del puerto en los puertos de acceso	Se realiza la configuración par tener un máximo de puertos permitidos de 3. S1(config)#interface fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Se realiza la protección de las interfaces que no usamos apagando los puertos desde el administrador. S1(config)#interface range fa0/3-4, fa0/7-24, gi0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Puertos sin utilizar S1(config-if-range)#shutdown

En la tabla 7 observamos la línea de comandos del switch 1 en la cual realizamos la creación de la VLAN; con la Creación de troncos 802.1Q y la asignación de puertos de acceso tanto como host y puertos de acceso y se apagan las interfaces que no se necesitan en la red.

Figura 7: configuración dela infraestructura.



Fuente: Autor.
Se crea la infraestructura de VLAN, Trunking, EtherChannel del switch 1 y se verifica que están configuradas con lo relacionado a la topología.

Paso 5: Configure el S2

Entre las tareas de configuración de S2 se incluyen las siguientes:

Tabla 8: Configuración de la infraestructura de red en S2.

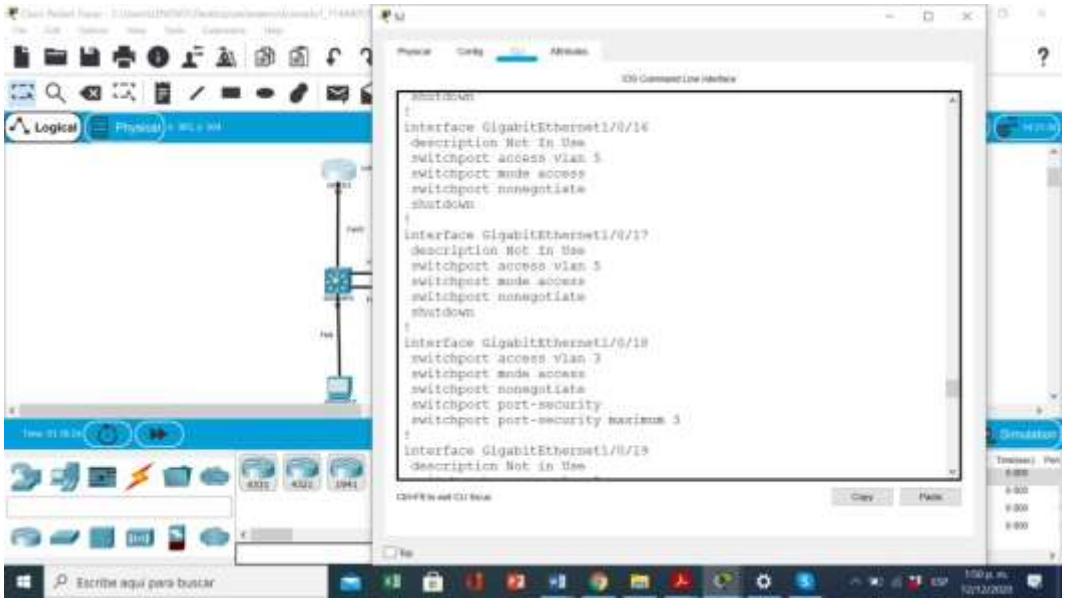
Configuración de S2	
Tarea	**Especificación**
Crear VLAN	La creación de la Vlan nos permite la administración de los dispositivos limitando su conexión siendo más sencilla la administración de los dispositivos. S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3, S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4, S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking, S2(config-vlan)#vlan 6 S2(config-vlan)#name Native

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	La configuración de troncales, nos permite la conexión en las interfaces FE y GE, entre el router y los switches de la topología, agregando una etiqueta a la trama del ethernet en la VLAN en donde pertenece. S2(config)#interface range fa0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	La creación de este grupo nos proporciona velocidad en los puertos FE y GE, igualando la velocidad en ellos. S2(config)#interface port, S2(config)#interface port-channel 2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit, S2(config)#interface range fa0/1-2 channel-group 2 mode passive S2(config-if-range)#no shutdown
Configurar el puerto de acceso del host para la VLAN 3	Se configure para la VLAN3 para que el acceso sea exclusivo en el host de la topología. S2(config)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3,S2(config-if)#exit
Configure port-security en los access ports	Se configure el maximo de puertos permitidos al acceso que son 3. S2(config)#interface fa0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3

Asegure todas las interfaces no utilizadas.	Se realiza apagado administravo para que no realizaen ataques por estas interfaces.S2(config)#interface range fa0/3-17, fa0/19-24, gi0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Puertos no utilizados S2(config-if-range)#shutdown

En la tabla 8 realizamos la configuración de la VLAN en S2, teniendo en cuenta la configuración de puertos EtherChannel de la red en, configurando port-security con un máximo de puertos requeridos que son 3 y el aseguramiento de las interfaces que no se utilizan.

Figura 8: configuración infraestructura switch2.



Fuente: Autor.

En la figura 8 Se realiza la creación la infraestructura de VLAN, Trunking, EtherChannel del switch 1 y se verifica que están configuradas con sus comandos.

Parte 2: Configurar soporte de host.

Paso 1: Configure R1

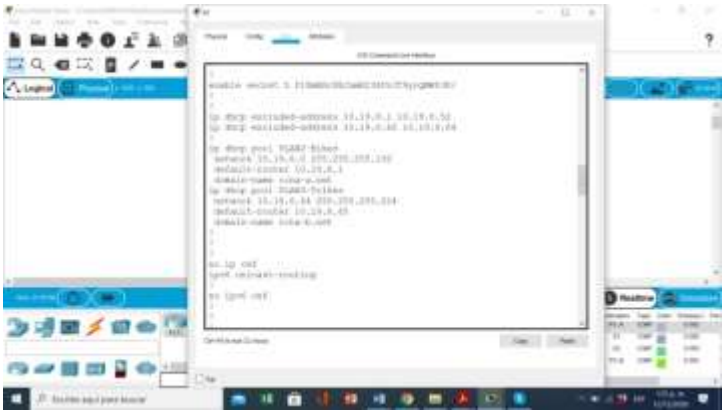
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9: Configuración de la infraestructura de red en R1.

Infraestructura de R1	
Tarea	**Especificación**
Configure Default Routing	Se realiza la configuración por default del R1. R1(config)#ip route 0.0.0.0 0.0.0.0 lo0
Configurar IPv4 DHCP para VLAN 2	Realizando esta operación nos permite asignar las direcciones IP via configuración dinámica en la vlan 2. R1(config)#ip dhcp pool vlan 2, R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.10 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-a.net R1(config)#default-router 10.19.8.1
Configurar DHCP IPv4 para VLAN 3	Realizando esta operación nos permite asignar las direcciones IP via configuración dinámica en la vlan 3. R1(config)#ip dhcp pool vlan 3 R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.10 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-b.net R1(config)#default-router 10.19.8.65

En la tabla 9 Se configura la estructura del R1 para su conexión en la topología que venimos desarrollando en este escenario utilizando los comando para configurar IPV4 en la VLAN 3, utilizando las DNS server 10.10.10.

Figura 9: configuración R1



Fuente: Autor.

Se configura el R1 para soporte de host utilizando líneas de comando y realizando la conexión exitosa con la topología desarrollada, lo que permite una conexión con los dispositivos que se instalaron.

Paso 2: Configurar los servidores

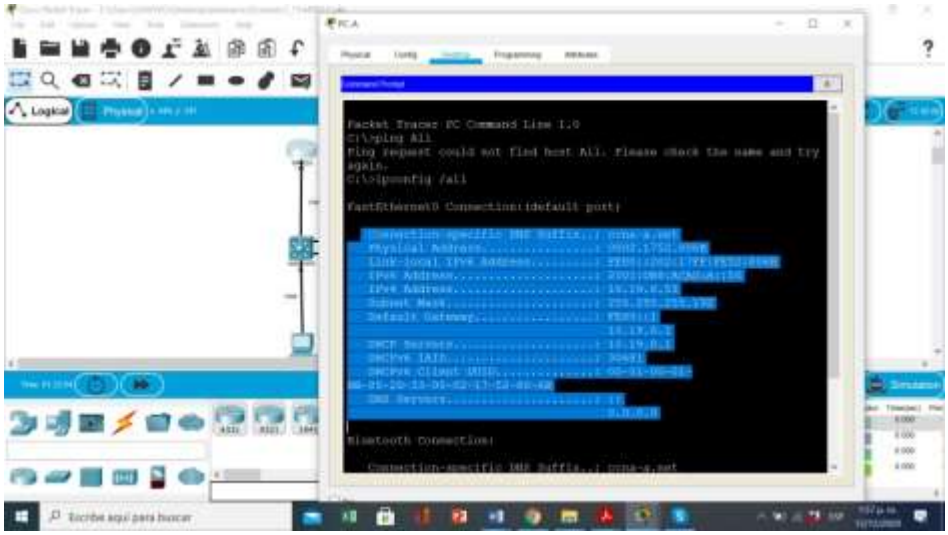
Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando **ipconfig /all**

Tabla 10: Configuración de PC-A.

PC-A Network Configuration	
Descripción	Nombre del pc. CCNA-a.net
Dirección física	La dirección física del PC. 0002.1752.806b
Dirección IP	Dirección que se configuro para el equipo. 10.19.8.53
Máscara de subred	Es la dirección que asigna por defecto el pc. 255.255.255.192
Gateway predeterminado	Puerta de enlace del equipo para conectarse a red.10.19.8.1
Gateway predeterminado IPv6	*Puerta de enlace de IPV6. FE80::1*

Se realiza configuración del PC-A como se observa en la tabla 10, obteniendo conexión de red en los equipos que están conectados en la topología realizada.

Figura 10: Configuración de red del host A.



Fuente: Autor.

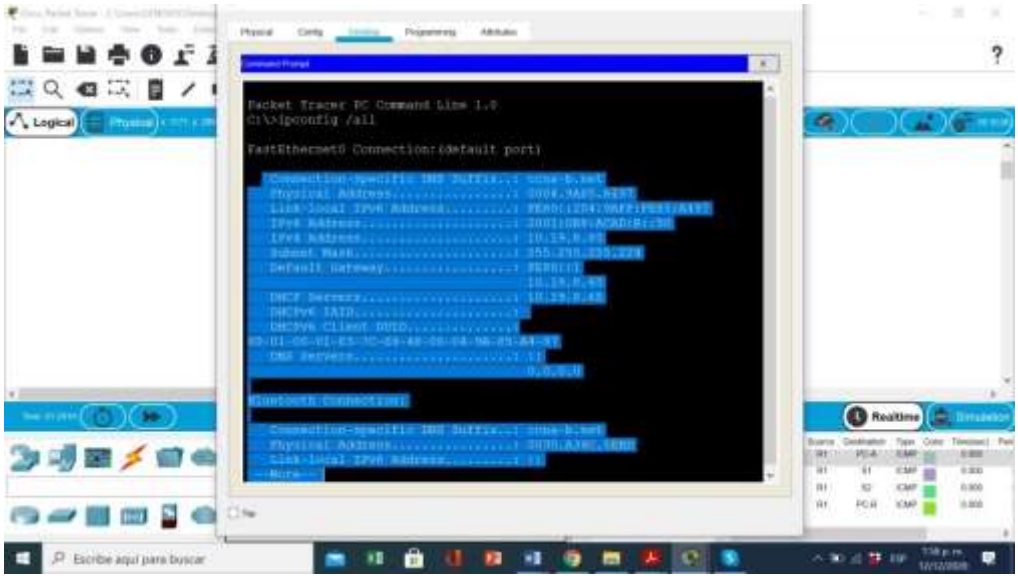
Se utiliza el comando Ipconfig all para verificar la configuración del pc la cual fue exitosa.

Tabla 11: Configuración de PC-B.

Configuración de red de PC-B	
Descripción	*Nombre del pc. Ccna-b.net*
Dirección física	*La dirección física del PC.* 004.9A85.A497
Dirección IP	*Dirección que se configuro para el equipo. 10.19.8.85*
Máscara de subred	Es la dirección que asigna por defecto el pc. 255.255.255.224
Gateway predeterminado	*Puerta de enlace del equipo para conectarse a red.10.19.8.65*
Gateway predeterminado IPv6	Puerta de enlace de IPV6. FE80::1

Se realiza la configuración del PC-B para su conexión con la topología como se muestra en la tabla 11 logrando conexión con los dispositivos.

Figura 11: Configuración de red del host B



Fuente: Autor.

Usando el comando ipconfig all verificamos la configuración del pc.

Parte 3: Probar y verificar la conectividad de extremo a extremo

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12: verificar la conectividad de extremo a extremo.

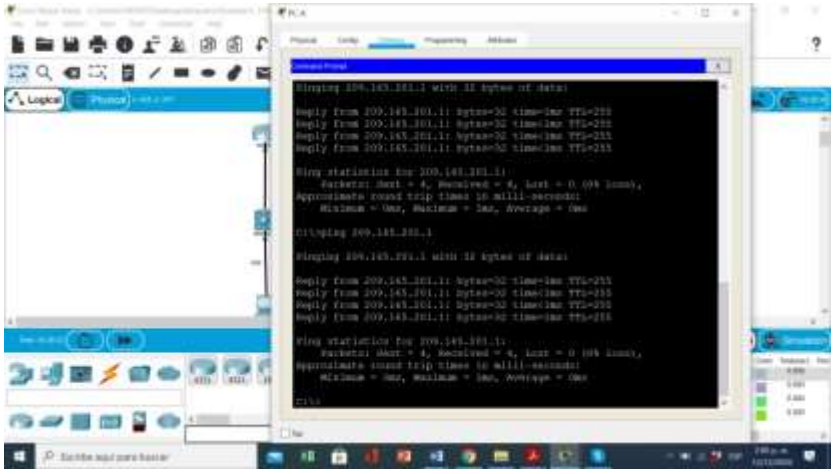
Verificación de la conectividad en la topología				
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Resultado exitoso

PC-A	R1, G0/0/1.2	IPV6	2001:db8:acad:a: :1	Resultado exitoso
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	Resultado exitoso
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	Resultado exitoso
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	Resultado exitoso
PC-A	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	Resultado exitoso
PC-A	S1, VLAN 4	Dirección	10.19.8.98	Resultado exitoso
PC-A	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	Resultado exitoso
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	Resultado exitoso
PC-A	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	Resultado exitoso
PC-A	PC-B	Dirección	10.19.8.85	Resultado exitoso
PC-A	PC-B	IPv6	2001:db8:acad:b: :50	Resultado exitoso
PC-A	R1 Bucle 0	Dirección	209.165.201.1	Resultado exitoso
PC-A	R1 Bucle 0	IPv6	2001:db8:acad:20 9: :1	Resultado exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Resultado exitoso

PC-B	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Resultado exitoso
PC-B	R1, G0/0/1.2	Dirección	10.19.8.1	Resultado exitoso
PC-B	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	Resultado exitoso
PC-B	R1, G0/0/1.3	Dirección	10.19.8.65	Resultado exitoso
PC-B	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	Resultado exitoso
PC-B	R1, G0/0/1.4	Dirección	10.19.8.97	Resultado exitoso
PC-B	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	Resultado exitoso
PC-B	S1, VLAN 4	Dirección	10.19.8.98	Resultado exitoso
PC-B	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	Resultado exitoso
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	Resultado exitoso
PC-B	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	Resultado exitoso

En la tabla 12 podemos ver la conexión exitosa entre PC-A y PC-B obteniendo la conectividad con los demás dispositivos de la red con sus respectivas direcciones Ip las cuales fueron configuradas en la topología que se desarrolló.

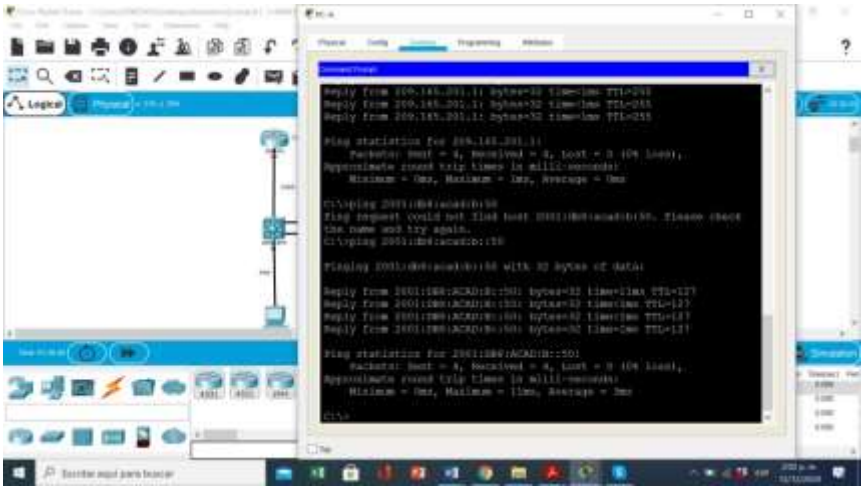
Figura 12: Verificación de conectividad del PC-A de extremo a extremo.



Fuente: Autor

Se realiza conexión exitosa de extremo a extremo entre PC-A y PC-B y demás equipos de la red, utilizando las diferentes direcciones IPV4 e IPV6 que se efectuaron en la configuración de la topología.

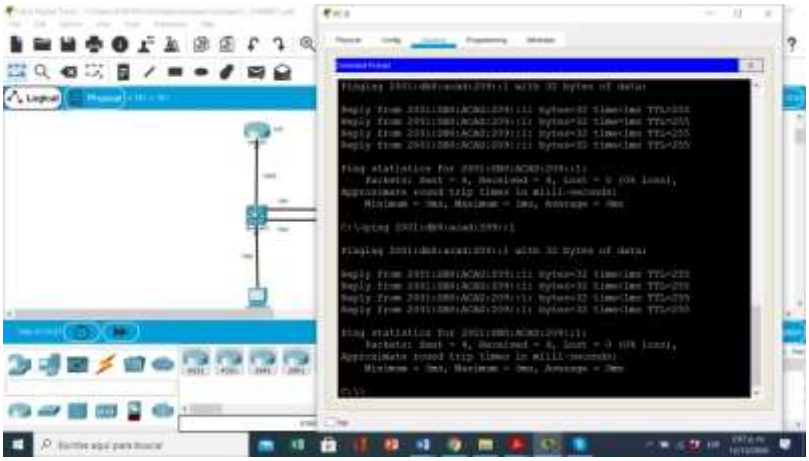
Figura 13: Verificación de conectividad del PC-A con R1 bucle 0.



Fuente: Autor.

En la figura 13, podemos ver la verificación del ping que se realizó al bucle 0 obteniendo la conexión esperada.

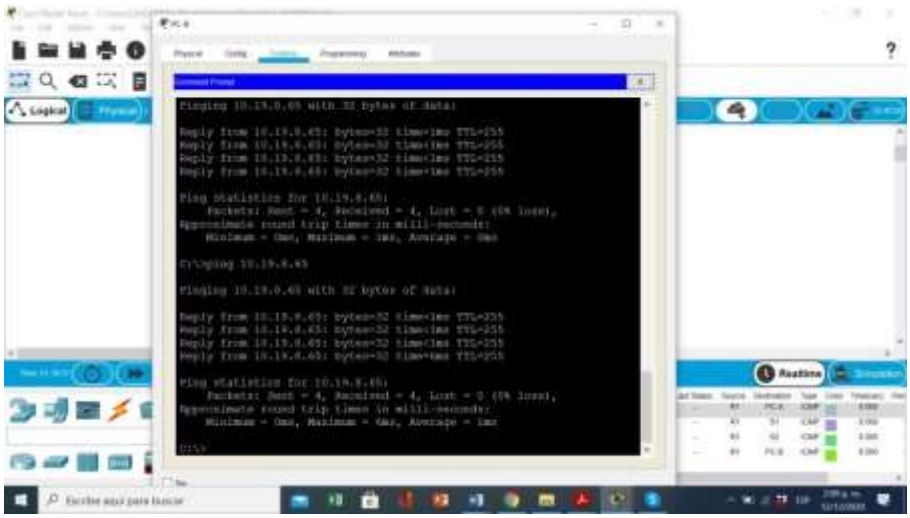
Figura 14: conexión de PC-B con R1 Bucle 0



Fuente: Autor.

En la figura 14 realiza ping utilizando el PC-B bucle 0 resultado satisfactorio.

Figura 15: realizar ping entre PC-B y R1, G0/0/1.3



Fuente: Autor.

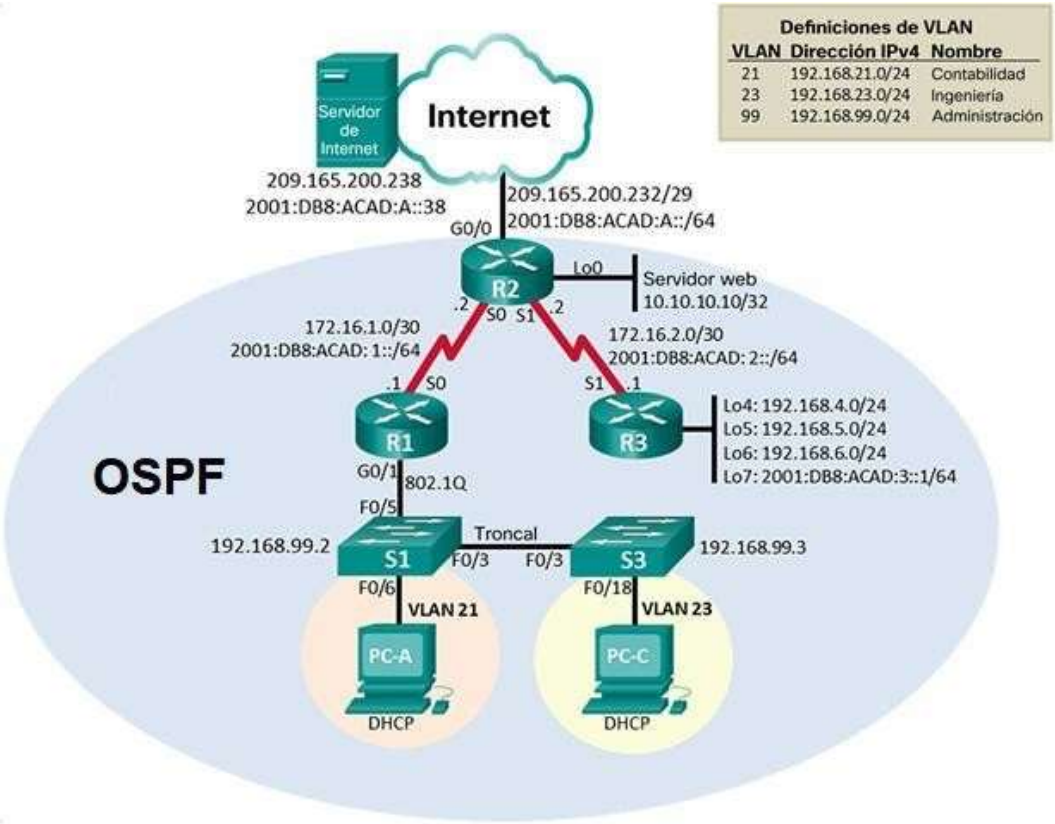
En la figura 15 podemos ver que se realiza la conexión exitosa usando la dirección ip 10.19.8.65 obteniendo conexión sin dificultad.

La comunicación en la topología del escenario se encuentra óptima para trabajo los equipos cuentan con conexión y se muestra que hay comunicación IPV4 e IPV6.

3.2 ESCENARIO 2

Topología

Figura 16: Topología Escenario 2.



Fuente: imagen de la prueba de habilidades

Topología que se va a desarrollar en este escenario.

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches.

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

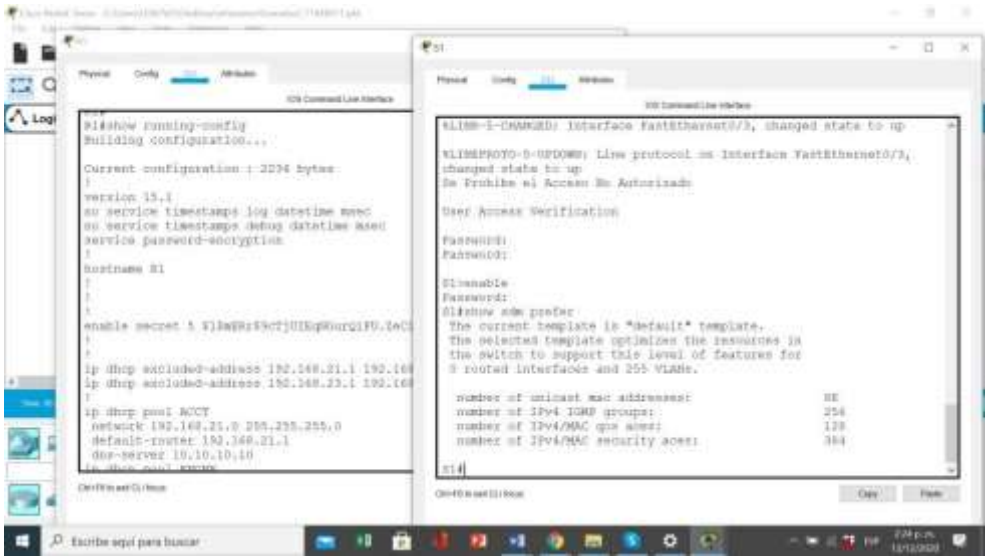
Tabla 13 :Verificación inicial de los dispositivos del segundo escenario

Verificación de los dispositivos.	
Tarea	**Comando de ios**
Eliminar el archivo startup-config de todos los routers	Para eliminar el archivo startup-config del router, utilizamos el comando: Router>enable Router#erase startup-config
Volver a cargar todos los routers	El comando reload nos vuelve a cargat todos los routers. Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Utilizando el comando startup-config, y utilzamos el comando Vlan dat para eliminar bases de datos anteriores Switch>enable Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Volvemos a utilizar el comando reload para cargr los switches. Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Configurando el comando show flash verificamos la memoria de los swiches. Switch#show flash

Se recargan los dispositivos de este escenario.

En la tabla 13 utilizamos los comandos erase startup-config, el cual nos permite eliminar el archivo startup de los routers, también utilizamos el comando delete vlan.dat para eliminar la base de datos de la VlAN y recargamos nuevamente con el comando reload.

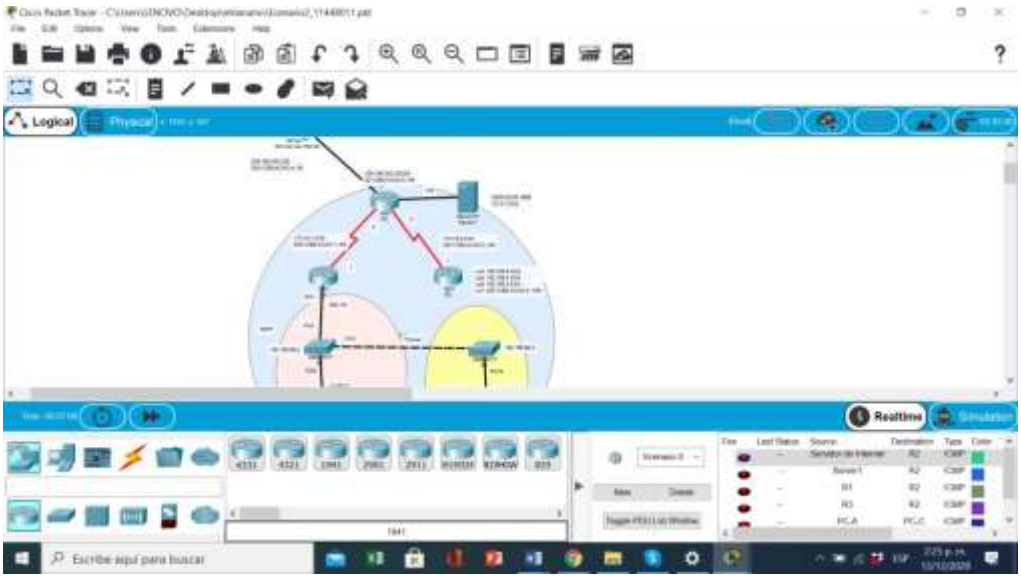
Figura 17:reinicio de los dispositivos.



Fuente: Autor.

En la figura 17 Se recargan los dispositivos para configurar sus funciones.

Figura 18: configuración terminada.



Fuente: Autor.

En la figura 18 observamos que se encuentra topología terminada de los dispositivos para su configuración.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 14: Indicaciones para configurar la computadora red internet.

Configuración de la computadora de internet	
Elemento o tarea de configuración	**Especificación**
Dirección IPv4	Dirección utilizar. 209.165.200.238
Máscara de subred para IPv4	Determina la dirección con los dispositivos a utilizarse. 255.255.255.248
Gateway predeterminado	Puerta de enlace para la conexión a la red. 209.165.200.225
Dirección IPv6/subred	Jerarquía de lad direcciones en IPV6. 2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	Puerta de enlace para la conexión IPV6. 2001:DB8:ACAD:2::1

Como se observa en la Tabla 14 se realiza la configuración para la conexión del servidor de internet, garantizando la conexión de los dispositivos que se van a conectar sin fallas consultando las direcciones que están descritas en la topología que se va a desarrollar.

Figura 19: configuración servidor de internet.

Fuente: Autor.

Como observamos en la figura 19 el servidor de internet ha sido configurado.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15: Configuraciones básicas de R1 en el segundo escenario.

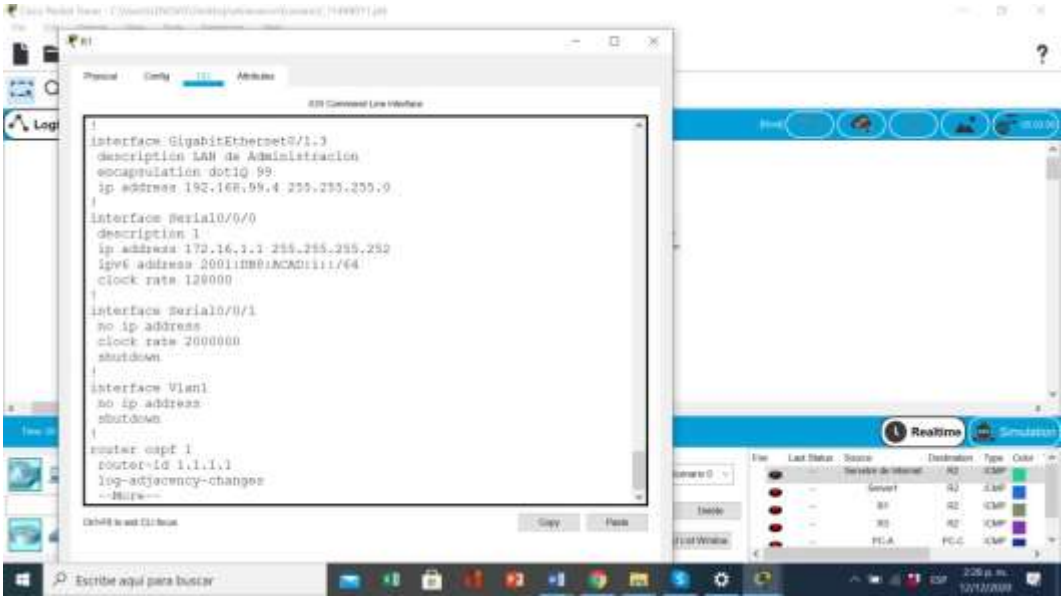
Configuración de R1	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda del DNS utilizamos el comando configure terminal y después indicamos que no busque el dominio. R1(config)#no ip domain-lookup
Nombre del router	Se configura el nombre del router para su identificación en la topología. Router(config)#hostname R1

Contraseña de exec privilegiado cifrada	Colocamos la contraseña cifrada como medida de seguridad en la configuración. R1(config)#enable secret class
Contraseña de acceso a la consola	Se coloca la contraseña de acceso a la consola para seguridad en la red. R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	Se establece esta contraseña para que el administrador de red trabaje remotamente. R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
Cifrar las contraseñas de texto no cifrado	Realizar el cifrado permite que no se conozcan las calves de acceso accidentalmente. R1(config)n#service password-encryption
Mensaje MOTD	Se realiza la configuración para restringuir su acceso a la configuración. R1(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	Se realiza la configuración de la interfaz serial 0/0/0 Con sus direcciones y funciones pertinentes. R1(config)#interface s0/3/0 R1(config-if)#ipaddress172.16.1.1 255.255.255.252 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config)#interface s0/3/0 R1(config-if)#ipvaddress 2001:DB8:ACAD:1::1/64 R1(config-if)#no shutdown

Rutas predeterminadas	Se establecen las rutas que usara la interfaz serial 0/0/0 en IPV6. R1(config)#ip route 0.0.0.0 0.0.0.0 serial s0/3/0 R1(config)#ipv6 route: :/0 serial s0/3/0

En la tabla 15 utilizamos los comandos de configuración DNS para desactivar la búsqueda, y realizamos las configuraciones básicas como son la colocación del nombre configurar sus rutas predeterminadas, el acceso a telnet y el cifrado de contraseñas.

Figura 20: Configuración R1.



Fuente: Autor.

La figura 20 nos muestra la configuración del Router 1 para la conexión de los dispositivos a la topología desarrollada.

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 16: Configuraciones básicas para el R2.

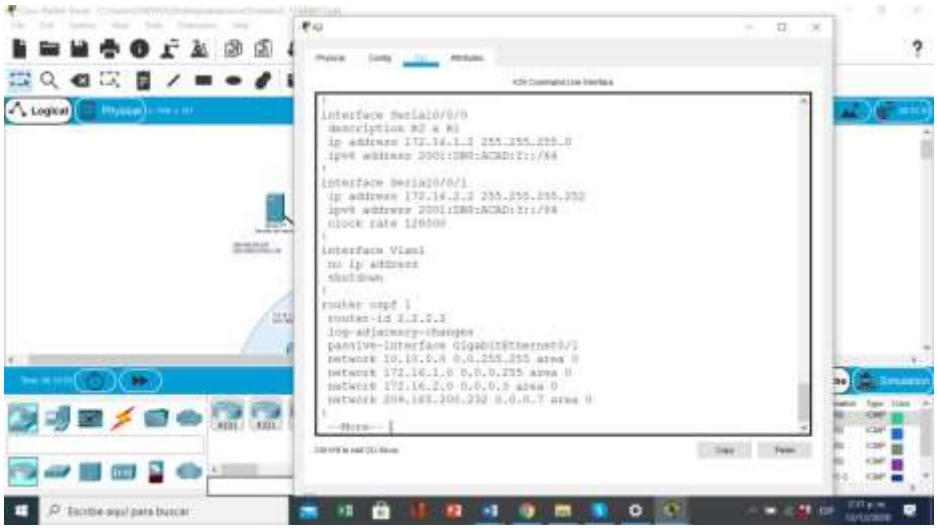
Configuración de R2	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda del DNS utilizamos el comando configure terminal y después indicamos que no busque el dominio. R2(config)#no ip domain-lookup
Nombre del router	Se configura el nombre del router para su identificación en la topología. Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Colocamos la contraseña cifrada como medida de seguridad en la configuración. R2(config)#enable secret class
Contraseña de acceso a la consola	Se coloca la contraseña de acceso a la consola para seguridad en la red. R2(config)#password cisco
Contraseña de acceso Telnet	Se establece esta contraseña para que el administrador de red trabaje remotamente. R2(config)#password cisco
Cifrar las contraseñas de texto no cifrado	Realizar el cifrado permite que no se conozcan las calves de acceso accidentalmente. R2(config)#service password-encryption
Habilitar el servidor HTTP	Se realiza la habilitación de servidor web de red. R2(config)#ip http server
Mensaje MOTD	Se realiza la configuración para reanudar su acceso a la configuración. R2(config)#banner motd $Se prohíbe el acceso no autorizado$

Interfaz S0/0/0	Se realiza la configuración el puerto serial 0/0/0 con sus funciones, direcciones y conexiones. R2(config)#interface s0/3/0R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#clock rate 128000R2(config-if)#no shutdown, R2(config)#interface s0/3/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64, R2(config-if)#no shutdown
Interfaz S0/0/1	Se realiza la configuración el puerto serial 0/0/1 con sus funciones, direcciones y conexiones. R2(config)#interface s0/3/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252, R2(config-if)#clock rate 12800R2 (config-if)#no shutdown, R2(config)#interface s0/3/1, R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64, R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	Se realiza la configuración del Puerto G0/0 que tendrá la función de simulador de red. R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shutdown R2(config)#interface g0/0 R2(config-if)#ipv6 address 2001:DB8:ACAD:/64 R2(config-if)#no shutdown
Interfase loopback 0 (servidor web simulado)	Se establece la interfaz de red virtual para su conexión. R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown

Ruta predeterminada	Se establecen las rutas que usara la interfaz G0/0 en IPV6. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

En la tabla 16 se realizan las Tareas básicas que utilizara el Router2, en las cuales establecemos la búsqueda del DNS, el cifrado de claves la conexión de interfaces serial y gigabit ethernet, y habilitamos el servicio HTTP con el comando http server.

Figura 21: Configuración R2.



Fuente: Autor.

La figura 21 nos enseña la configuración del Router 2 con las tareas indicadas para su conexión a la topología.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 17: Configuraciones básicas de R3 en el segundo escenario.

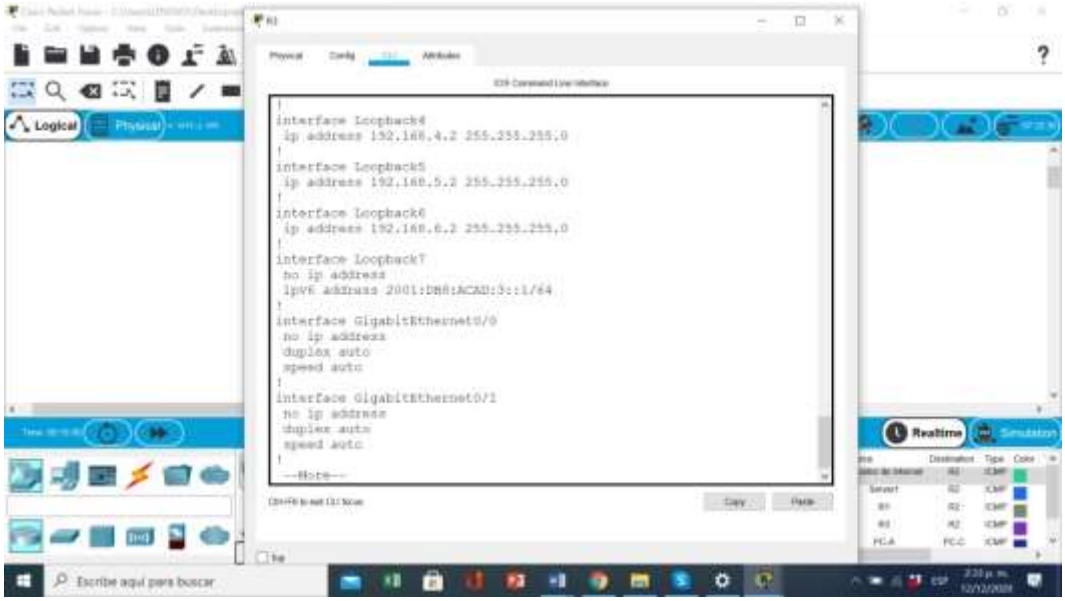
Configuración el router 3	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda del DNS utilizamos el comando configure terminal y después indicamos que no busque el dominio R3(config)#no ip domain-lookup

Nombre del router	Se configura el nombre del router para su identificación en la topología. Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Colocamos la contraseña cifrada como medida de seguridad en la configuración. R3(config)#enable secret class
Contraseña de acceso a la consola	Se coloca la contraseña de acceso a la consola para seguridad en la red. R3(config)#password cisco
Contraseña de acceso Telnet	Se establece esta contraseña para que el administrador de red trabaje remotamente. R3(config)#password cisco
Cifrar las contraseñas de texto no cifrado	Realizar el cifrado permite que no se conozcan las calves de acceso accidentalmente. R3(config)#service password-encryption
Mensaje MOTD	Se realiza la configuración para restringuir su acceso a la configuración. R3(config)#banner motd $Se prohíbe el acceso no autorizado$
Interfaz S0/0/1	Se realiza la configuración el puerto serial 0/0/1 con sus funciones, direcciones y conexiones. R3(config)#interface s0/3/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config)#interface s0/3/1 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	Se establece la interfaz de red virtual para su conexión. R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.0 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 5	Se establece la interfaz de red virtual para su conexión. R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.0 255.255.255.0 R3(config-if)#no shutdown

Interfaz loopback 6	Se establece la interfaz de red virtual para su conexión. R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.0 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 7	Se establece la interfaz de red virtual para su conexión. R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#no shutdown

En la tabla 17 desarrollamos la conexión en el Router 3, realizando las configuraciones básicas como son el nombre del router cifrado de contraseñas configurar la interfaz loopback y desactivar la DNS.

Figura 22: configuración R3.



Fuente: Autor.

La figura 22 nos enseña la configuración de R3 para su conexión a la topología, utilizando la línea de comando que desarrollamos para obtener su conexión a la red.

Paso 5: Configurar S1

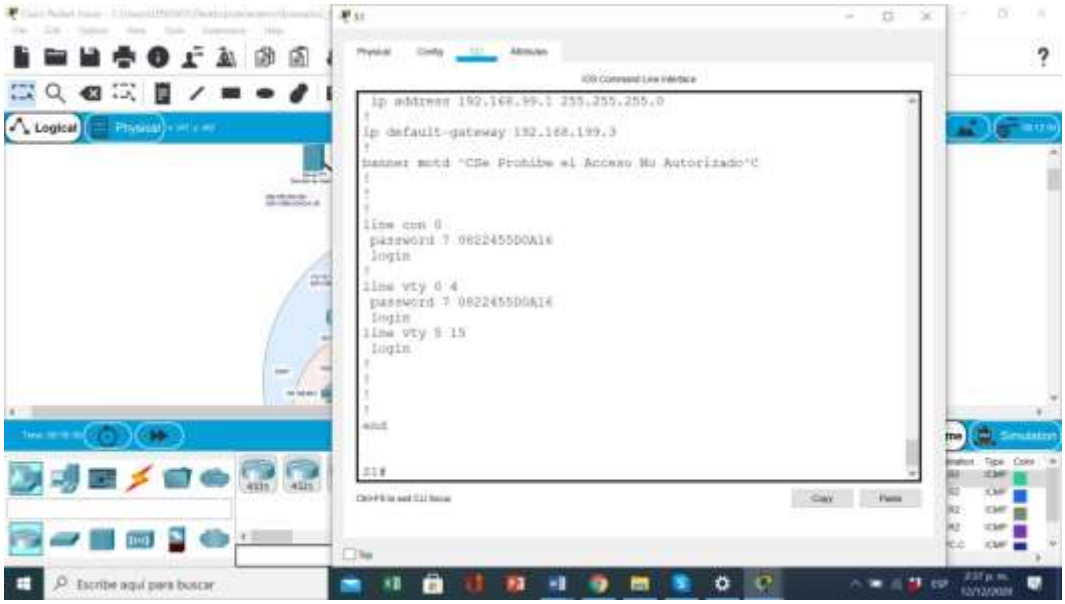
La configuración del S1 incluye las siguientes tareas:

Tabla 18: Configuraciones básicas de S1 en el segundo escenario.

Configuración básica del switch 1	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda del DNS utilizamos el comando configure terminal y después indicamos que no busque el dominio S1(config)#no ip domain-lookup
Nombre del switch	Se le asigna nombre la switch para su reconocimiento en la topología. Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	Utilizamos la contraseña cifrada como medida de seguridad en la configuración. S1(config)#enable secret class
Contraseña de acceso a la consola	Se coloca la contraseña de acceso a la consola para seguridad en la red. S1(config)#password cisco
Contraseña de acceso Telnet	Se establece esta contraseña para que el administrador de red trabaje remotamente. S1(config)#password cisco
Cifrar las contraseñas de texto no cifrado	Realizar el cifrado permite que no se conozcan las calves de acceso accidentalmente. S1(config)#service password-encryption
Mensaje MOTD	Se realiza la configuración para restringuir su acceso a la configuración. S1(config)#banner motd $Se prohíbe el acceso no autorizado$

Asignación de línea de comandos que se observa en la tabla 18 creamos el acceso a la consola y las contraseñas con su cifrado respectivo.

Figura 23: configuración S1.



Fuente: Autor.

Se configura S1 con las tareas indicadas utilizando la lista de comandos indicada.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19: Configuraciones básicas de S3 en el segundo escenario.

Configuración del switch 3	
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda del DNS utilizamos el comando configure terminal y después indicamos que no busque el dominio S3(config)#no ip domain-lookup
Nombre del switch	Se le asigna nombre la switch para su reconocimiento en la topología. Switch(config)#hostname S3

Contraseña de exec privilegiado cifrada.	Utilizamos la contraseña cifrada como medida de seguridad en la configuración. S3(config)#enable secret class
Contraseña de acceso a la consola	Se coloca la contraseña de acceso a la consola para seguridad en la red. S3(config)#password cisco
Contraseña de acceso Telnet	Se establece esta contraseña para que el administrador de red trabaje remotamente. S3(config)#password cisco
Cifrar las contraseñas de texto no cifrado	Realizar el cifrado permite que no se conozcan las calves de acceso accidentalmente. S3(config)#service password-encryption
Mensaje MOTD	Se realiza la configuración para restringuir su acceso a la configuración. S3(config)#banner motd $Se prohíbe el acceso no autorizado$

Los Comandos que se observan en la tabla 19 en la cual realizamos las configuraciones requeridas para l conexión del S3 a la red.

Figura 24: configuración S3

Fuente: Autor.

Se configura S3 de acuerdo al listado de comandos que se indicaron.

Paso 7: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 20 :Verificación de conectividad en los routers y en el PC.

Verificación de la conectividad			
Desde	**A**	**Dirección IP**	**Resultados del ping**
R1	VR2, S0/0/0	172.16.1.2	Conectividad exitosa (Ver figura 25)
R2	R3, S0/0/1	172.16.2.1	Conectividad exitosa (Ver figura 26)
PC de Internet	Gateway predeterminado	209.165.200.238	Conectividad exitosa 5 (Ver figura 27)

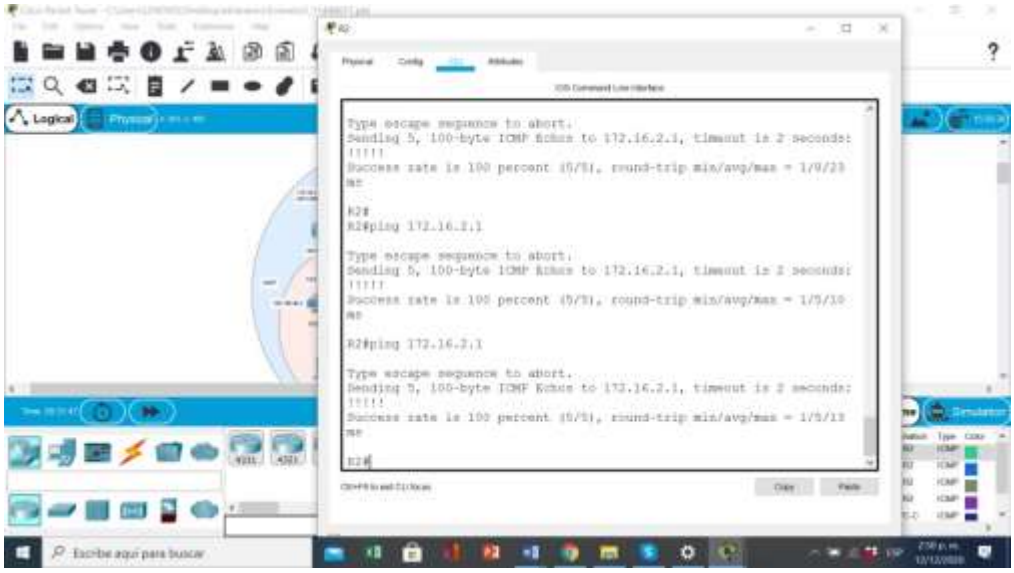
En la tabla 20 Se realiza los pings y se comprueba la conectividad entre los dispositivos que se configuraron sin tener complicaciones en su configuración obteniendo un resultado óptimo en cada uno de ellos.

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 25: Verificación de la conexión de R1.

Fuente: Autor.
Observamos en la figura 25 la conexión exitosa en R1 R2 y PC de internet.

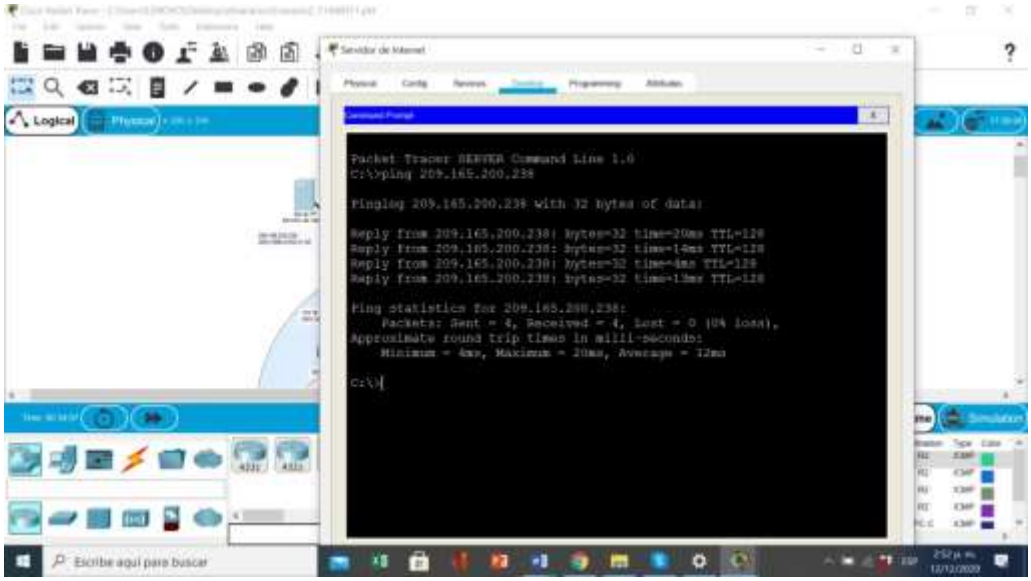
Figura 26 Verificación de la conexión de R2.



Fuente: Autor.

La figura 26 nos enseña la Conexión de R2 con los diferentes dispositivos.

Figura 27: Verificación de la conexión del servidor de red a su Gateway predeterminado.



Fuente: Autor

Con la figura 27, Verificamos la conexión del servidor de internet en su gateway.

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

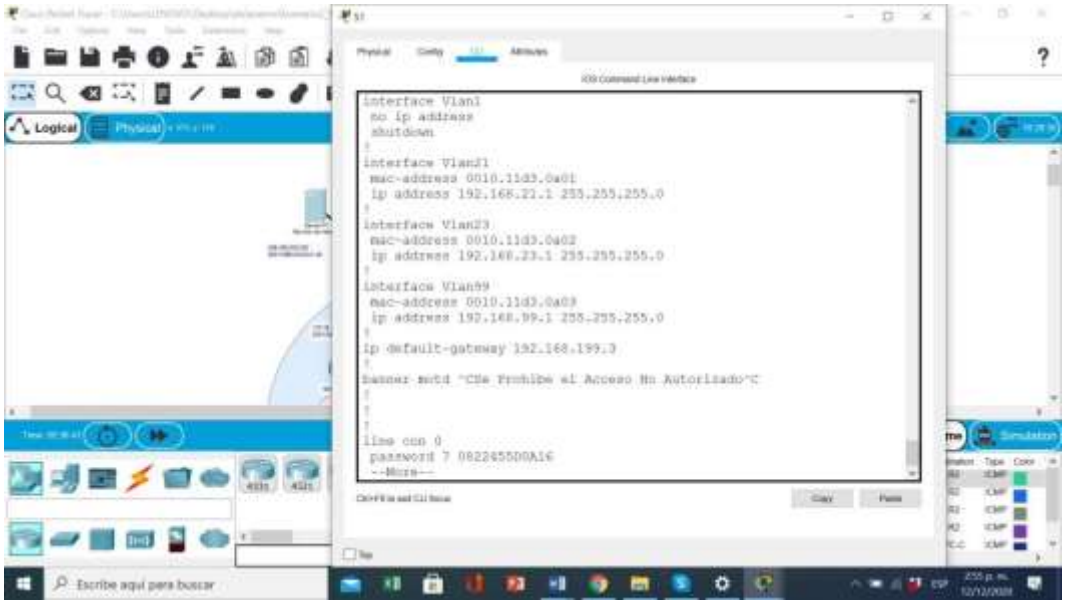
Tabla 21: Configuración de la seguridad del switch y el routing entre las vlan de S1.

Configuración del switch 1	
Tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Se realiza la creación de la VlAN para la conexión entre los diferentes equipos dentro de la topología que desarrollamos. S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administración S1(config-vlan)#exit
Asignar la dirección IP de administración.	Se le asignan las direcciones IP que va a Manejar la administración con sus funciones. S1(config-if)#interface vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el gateway	Se establece la puerta de enlace del switch 1 para su conexión a la red. S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Se asigna el comando trunk para permitir el acceso de las diferentes VlANS configuradas en nuestra topología. S1(config)#interface fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	Se asigna el comando trunk para permitir el acceso de las diferentes VlANS configuradas en nuestra topología. S1(config-if)#interface fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso	Se realiza la lista de comandos correspondiente a los puertos y su designación. S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-rangen)#switchport mode access
Asignar F0/6 a la VLAN 21	Se configura el Puerto Fa0/6 a la vlan21 para su utilización. S1(config-if)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#no shutdown
Apagar todos los puertos sin usar	Se realiza el apagado de los puertos accediendo al nivel administrativo para seguridad de la red. S1(config-if)#interface range fa0/2, fa0/4-24, g0/1-2 S1(config-if-range)#shutdown

Observando la tabla 21 realizamos la configuración para el S1 donde asignamos la gateway 192.168.99.1y realizamos las demás configuraciones de puertos como acceso a la red, apagado de los puertos que no se usan, y la dirección ip de administración.

Figura 28: seguridad S1.



Fuente: Autor.

Se configuro la seguridad de S1 y las vlan respectivas para proteger la información de los equipos manteniendo la conexión de red sin tener pérdidas de conexión en la topología desarrollada.

Paso 2: Configurar el S3.

La configuración del S3 incluye las siguientes tareas:

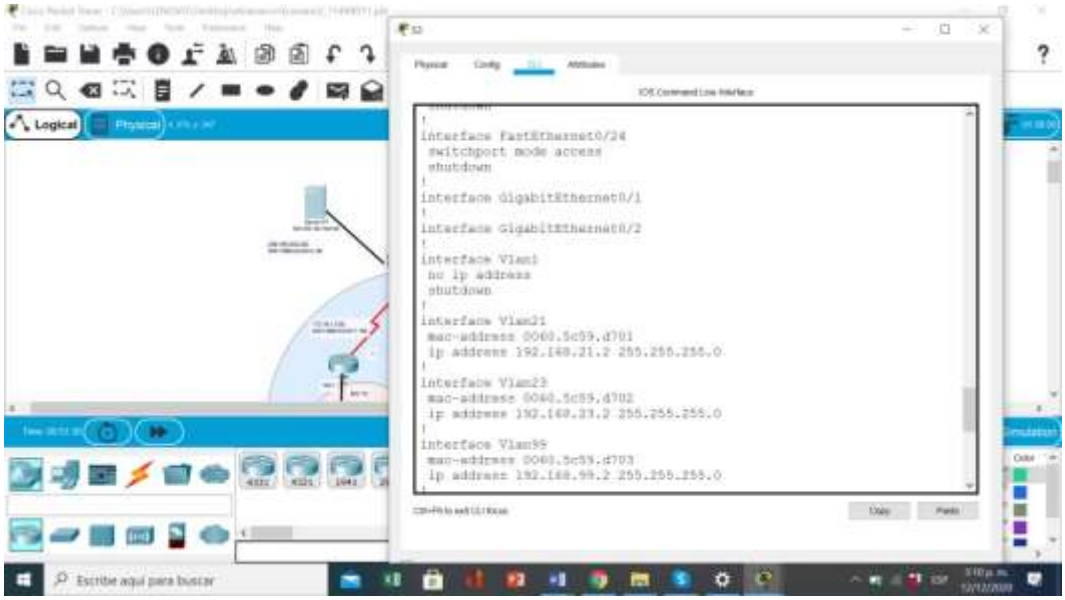
Tabla 22: Configuración de la seguridad del switch y el routing entre las vlan de S3.

Configuración del switch 3	
Elemento o tarea de configuración	**Especificación**
Crear la base de datos de	Se realiza la creación de la VLAN para la conexión entre los diferentes equipos dentro de la topología que desarrollamos. S3(config)#vlan 21, S3(config-vlan)#name contabilidad , S3(config-vlan)#vlan 23, S3(config-vlan)#name ingenieria, S3(config-vlan)#vlan 99, S3(config-vlan)#name administración S3(config-vlan)#exit

Asignar la dirección IP de administración	Se le asignan las direcciones IP que va a Manejar la administración con sus funciones. S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0, S3(config-if)#exit
Asignar el gateway predeterminado.	Se establece la puerta de enlace del switch 3 para su conexión a la red. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Se asigna el comando trunk para permitir el acceso de las diferentes VlANS configuradas en nuestra topología. S3(config)#interface fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan1
Configurar el resto de los puertos como puertos de acceso	Se realiza la lista de comandos correspondiente a los puertos y su designación S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2, S3(config-if)#switchport mode access
Asignar F0/18 a la VLAN 21	Se configura el Puerto Fa0/6 a la vlan21 para su utilización. S3(config-if)#interface fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if-range)#no shutdown
Apagar todos los puertos sin usar	Se realiza el apagado de los puertos accediendo al nivel administrativo para seguridad de la red. S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2, S3(config-if-range)#shutdown

En la tabla 22 asignamos la configuración para S3 realizando la configuración el gateway 192.168.99.1 creamos los puertos de acceso faltantes, y asignamos la dirección IP de administración.

Figura 29: configuración de S3.



Fuente: Autor.

En la figura 29 vemos la configuración de seguridad de S3 para garantizar la seguridad de la topología.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

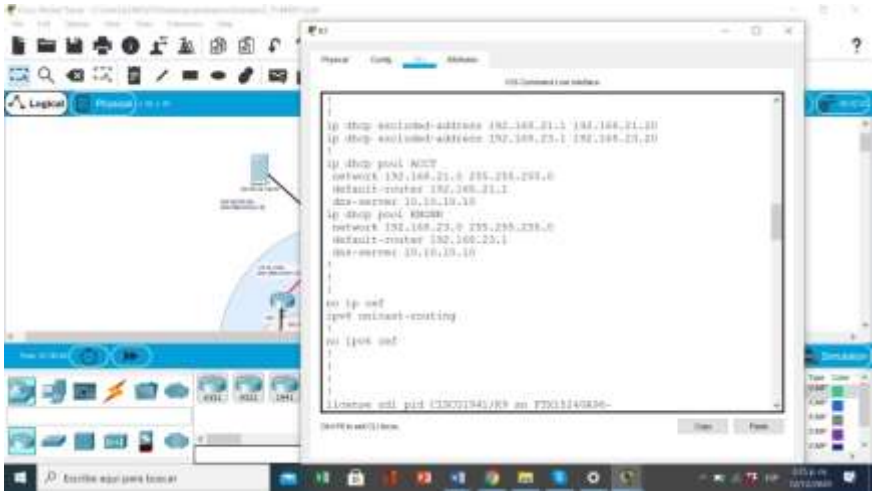
Tabla 23: Configuración de la seguridad del switch y el routing entre las vlan de R1.

Configuración del Router 1	
Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	La configuración de troncales, nos permite la conexión en las interfaces FE y GE, entre el router y los switches de la topología. R1(config)#interface g0/1.1 R1(config-subif)#description accounting LAN

	R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	La configuración de troncales, nos permite la conexión en las interfaces FE y GE, entre el router y los switches de la topología. R1(config-subif)# interface g0/1.2 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.4 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	La configuración de troncales, nos permite la conexión en las interfaces FE y GE, entre el router y los switches de la topología. R1(config-subif)# interface g0/1.3 R1(config-subif)#description accounting LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.4 255.255.255.0
Activar la interfaz G0/1	Realizamos la activación de la interfaz G0/1 y de las configuraciones asignadas para laconexiónde red. R1(config-subif)# interface g0/1 R1(config-subif)#no shutdown

En La Tabla 23 realizamos los comandos para la conexión del Roter 1 activando la subinterfaz 802.1Q .21. y activamos la interfaz G0/1 para obtener acceso ala red en la topología desarrollada.

Figura 30: Configuración R1.



Fuente: Autor.

Se configura correctamente R1 con las conexiones de interfaces requeridas con la su interfaz 802.1Q.

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

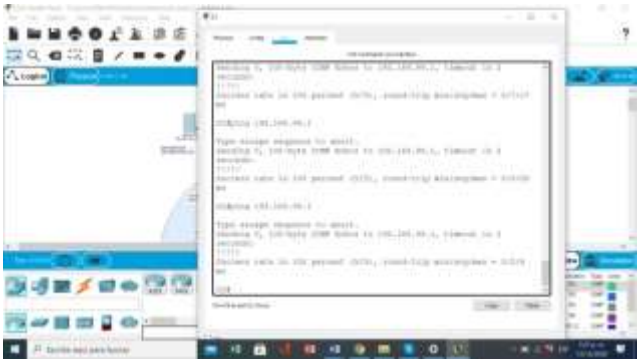
Tabla 24: verificación de la topología.

Verificación de la red			
Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Conexión exitosa (Ver figura 31)
S3	R1, dirección VLAN 99	192.168.99.1	Conexión exitosa (Ver figura 32)

S1	R1, dirección VLAN 21	192.168.21.1	Conexión exitosa (Ver figura 33)
S3	R1, dirección VLAN 23	192.168.23.1	Conexión exitosa (Ver figura 34)

Se verifica la conectividad entre S1, S3 y R1 obteniendo los resultados esperados conexión exitosa en los dispositivos como se observa en la tabla 24.

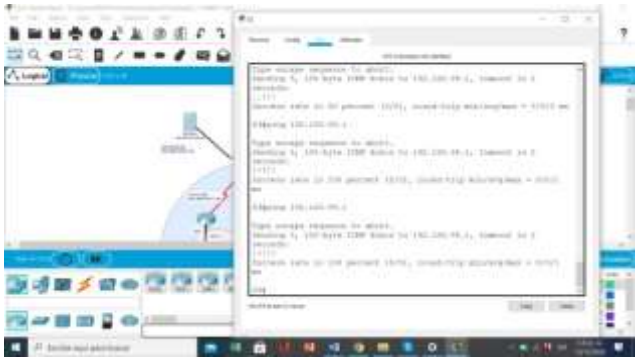
Figura: 31 Verificación de conexión de red en S1.



Fuente: Autor.

La figura 31 nos indica el ping y se obtiene conectividad exitosa en la red con S1.

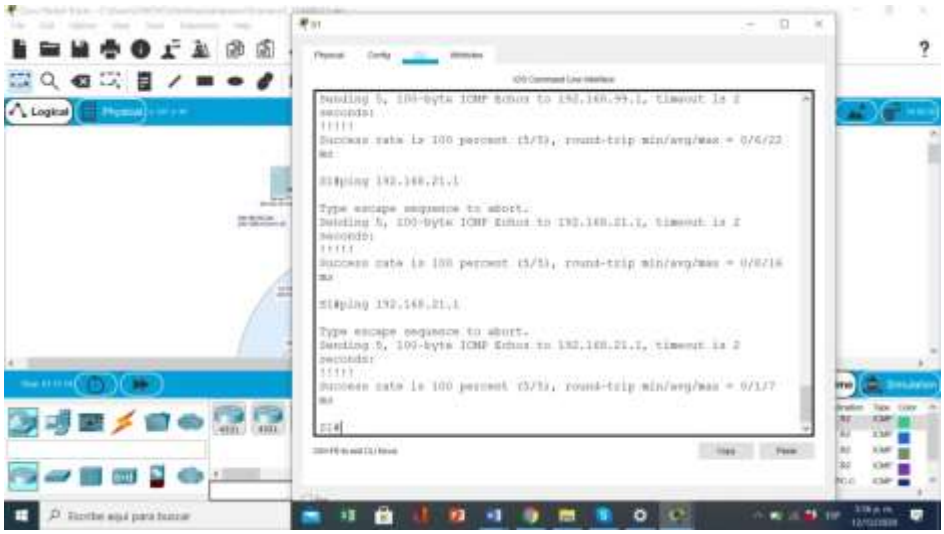
Figura 32: verificación de S3.



Fuente: Autor.

Con la figura 32 verificamos la conexión exitosa de R3 con los diferentes equipos de la topología realizada.

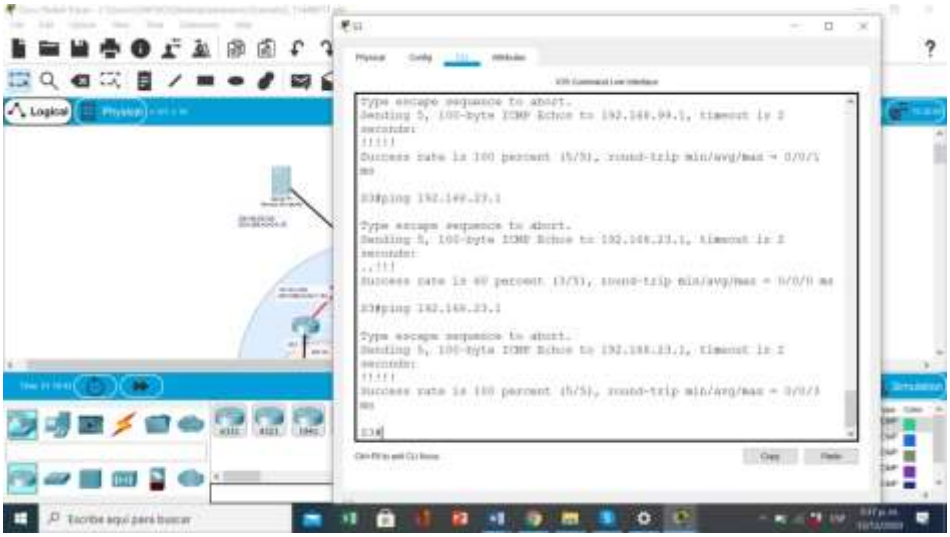
Figura 33: verificación S1.



Fuente: Autor.

La figura 33 confirma la configuración del ping 192.168.21.1 y se encuentra exitosa la conexión de S1.

Figura 34: verificación de S3.



Fuente: Autor.

Observando la figura 34 vemos la Conexión exitosa con la dirección 192.168.23.1 utilizando el S3.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

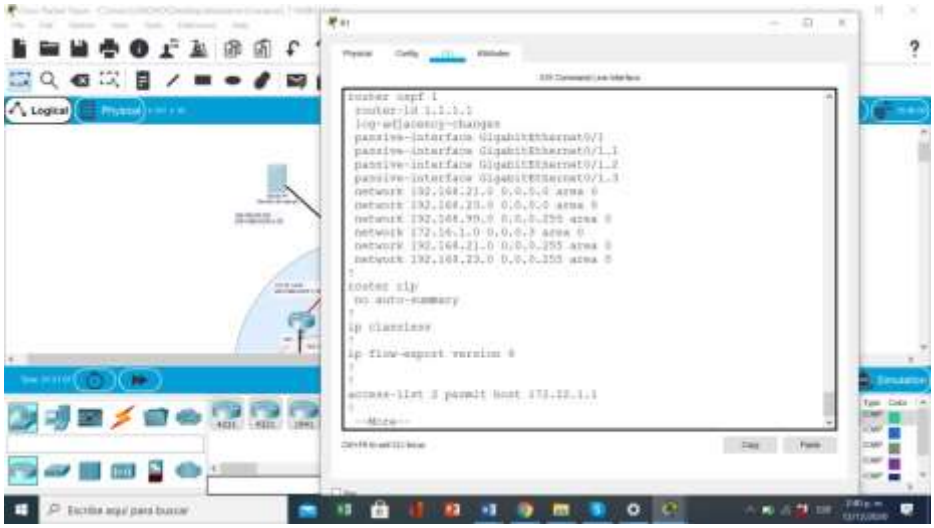
Las tareas de configuración para R1 incluyen las siguientes

Tabla 25: Configuración OSPF área 0 en R1.

Configuración de OSPF en el Router 1	
Elemento o tarea de configuración	**Especificación**
Configurar OSPF area 0	Se configura con el comando OSPF para permitir la autenticación de ruteo en l red. R1(config)#router ospf 1
Anunciar las redes conectadas directamente	Se realiza la instrucción de configuración de ruta que nos permite conectar directamente a través de la red. R1(config-router)#network 172.16.1.0 0.0.0.255 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	Configuramos las redes pasivas en la LAN para tener su función para obtener más velocidad en la transmisión de datos. R1(config-router)#passive-interface g0/1.1 R1(config-router)#passive-interface g0/1.2 R1(config-router)#passive-interface g0/1.3
Desactive la sumarización automática	Desactivamos la sumarización automatic para no tener conflictos entre los dispositivos y sus direcciones. R1(config-router)#no auto-summary

En la tabla 25 vemos como se realizó las Tareas para la Configuración OSPF área 0 en R1 con el comando router ospf 1manteniendo su conexión con la topología.

Figura 35: configuración OSPF R1.



Fuente: Autor.

configuración de OSPF completada en el R1 utilizando el comando.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

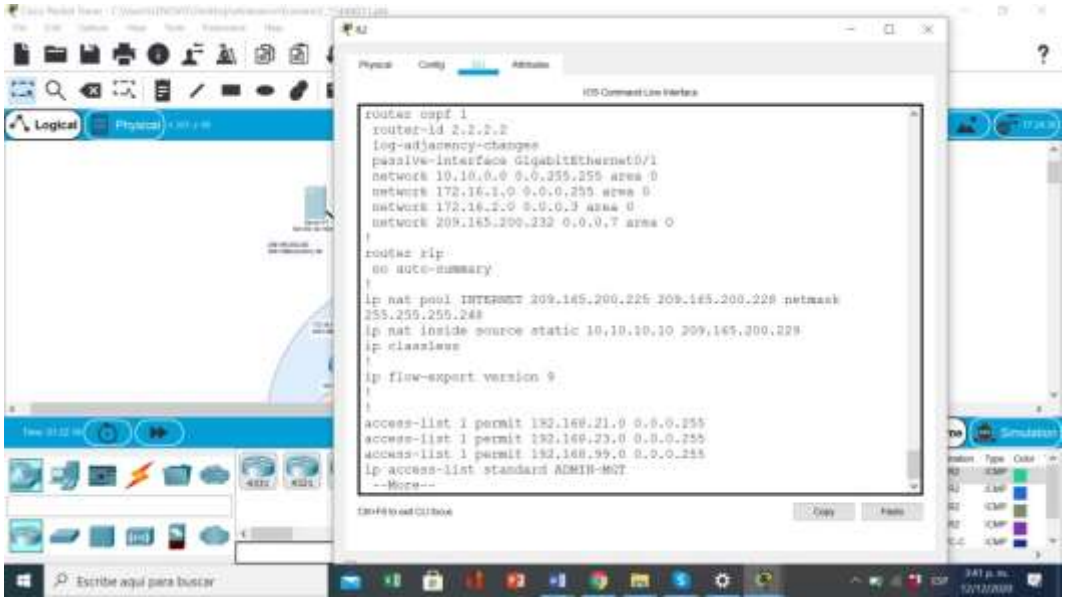
Tabla 26: Configuración OSPF área 0 en R2.

Configuración OSPF en el Router 2	
Elemento o tarea de configuración	**Especificación**
Configurar OSPF area 0	Se configura el comando OSPF para permitir la autenticación de ruteo en la red R2(config)#router ospf 1
Anunciar las redes conectadas directamente	Se realiza la instrucción de configuración para conectar directamente a través de la red. R2(config-router)#network 172.16.1.0 0.0.0.255 area 0, R2(config-outer)#network 172.16.2.0 0.0.0.255 area 0, R2(config-router)#network 10.10.10.10 0.0.0.255 area 0, R2(config-outer)#network 192.168.4.21 0.0.0.255 area 0, R2(config-router)#network 192.168.5.23 0.0.0.255 area 0, R2(config-router)#network 192.168.6.99 0.0.0.255 area 0

Establecer la interfaz LAN (loopback) como pasiva	Configuramos las redes pasivas en la LAN para obtener más velocidad en la transmisión de datos.R2(config-router)#passive-interface lo4 R2(config-router)#passive-interface lo5 R2(config-router)#passive-interface lo6
Desactive la sumarización automática.	Desactivamos la sumarización automática para no tener conflictos entre los dispositivos. R2(config-router)#no auto-summary

En la tabla 26 se observa la configuración de OSPF R2 en la topología realizando la conexión de sus redes directas y desactivando la sumarización con el comando no auto-summary.

Figura 36: configuración en OSPF enR2



Fuente: Autor.

En la figura 36, se observa la Configuración en R2 completada mediante la configuración de OSPF.

Paso 3: Configurar OSPFv3 en el R3

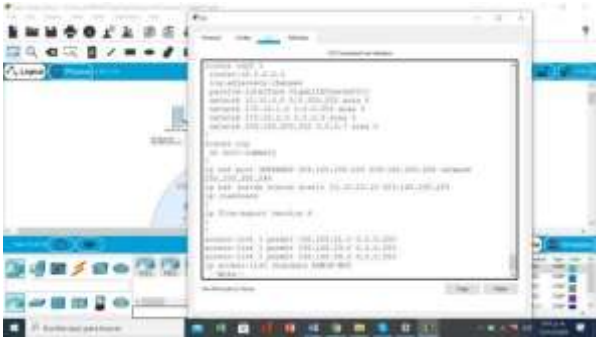
La configuración del R3 incluye las siguientes tareas

Tabla 27: configurar R3.

Configuración OSPF router3	
Elemento o tarea de configuración	**Especificación**
Configurar OSPF area 0	Se configura el comando OSPF para permitir la autenticación de ruteo en la red R3(config)#router ospf 1
Anunciar redes IPv4 conectadas directamente	Se realiza la instrucción de configuración de ruta que nos permite conectar directamente a través de la red. R3(config-router)#network 172.16.2.0 0.0.0.255 area 0 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Configuramos las redes pasivas en la LAN para tener su función para obtener más velocidad en la transmisión de datos. R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	Desactivamos la sumarización automática para no tener conflictos entre los dispositivos y sus direcciones R3(config-router)#no auto-summary

Se realiza la configuración de OSPF en el Router 3 como se observa en la tabla 27 manteniendo conexión y estableciendo las interfaces de LAN IPV4.

Figura 37: configuración R3.



Fuente: Autor.

La Figura 37 nos muestra la configuración OSPF para el Router 3 utilizando la línea de comandos.

Paso 4: Verificar la información de OSPF

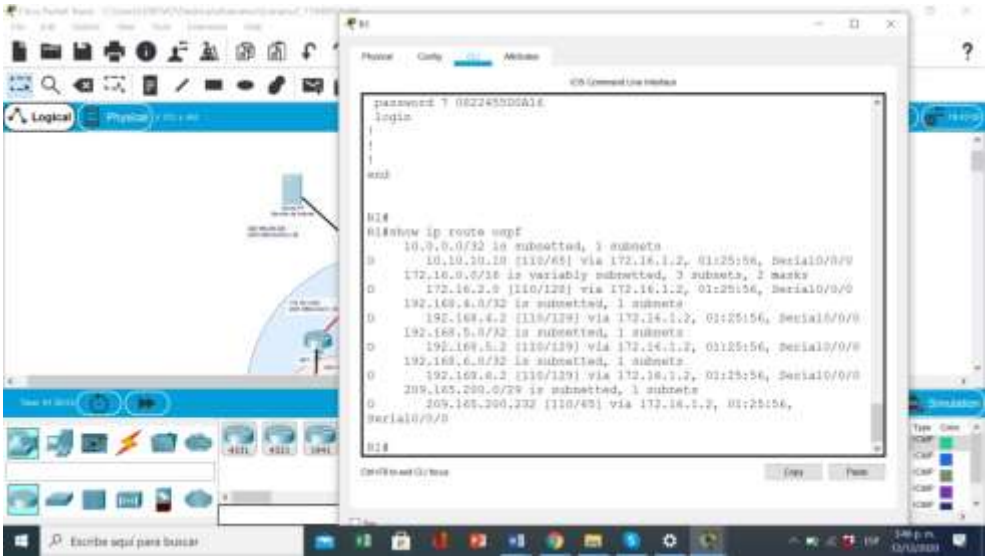
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 28: Comandos para realizar las verificaciones de las configuraciones.

Verificación de OSPF	
Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Para verificar el proceso OSPF utilizamos show ip protocols. R1#Show ip protocols (Figura 38) R2#Show ip protocols (Figura 39) R3#Show ip protocols (Figura 40)
¿Qué comando muestra solo las rutas OSPF?	El comando show ip route Muestra solo las rutas que se trabajan. R1#Show ip route ospf (Figura 38) R2#Show ip route ospf (Figura 39) R3#Show ip route ospf (Figura 40)
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Al digitar el comando show run podemos observar la configuración OSPF en su ejecución. R1#Show run (Figura 38) R2#Show run (Figura 39) R3#Show run (Figura 40)

Como se observa en la tabla 28 la Configuración realizada con OSPF con sus configuraciones es exitosa.

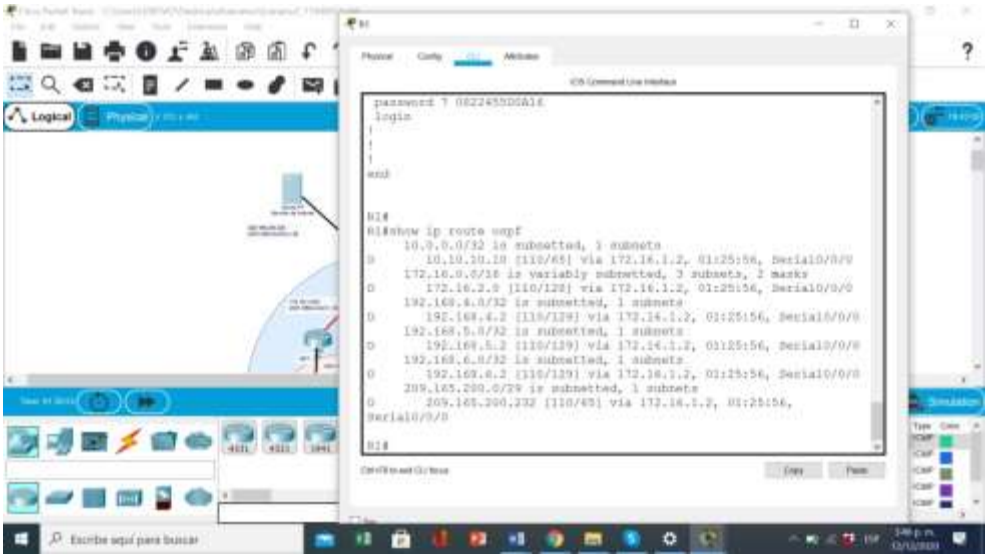
Figura 38 Verificación de la información OSPF en R1



Fuente: Autor.

En la figura 38 Verificación la configuración de OSP exitosa en R1.

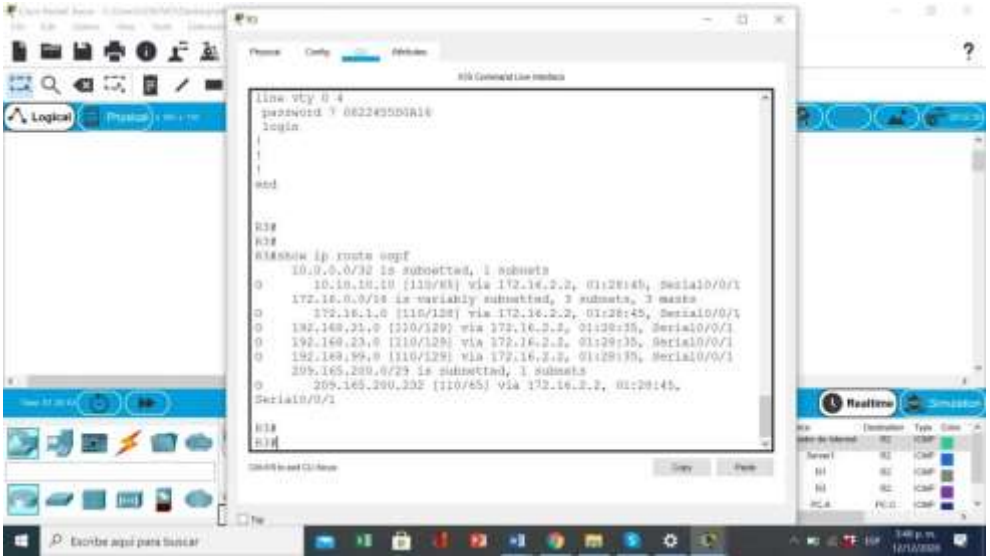
Figura 39: Verificación OSPF en R2



Fuente: Autor.

Con la figura 39 podemos observar la verificación de OSPF en R2.

figura 40: Verificación OSPF en R3.



Fuente: Autor.

En la figura 30 vemos la verificación de OSPF en R3

Parte 5: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

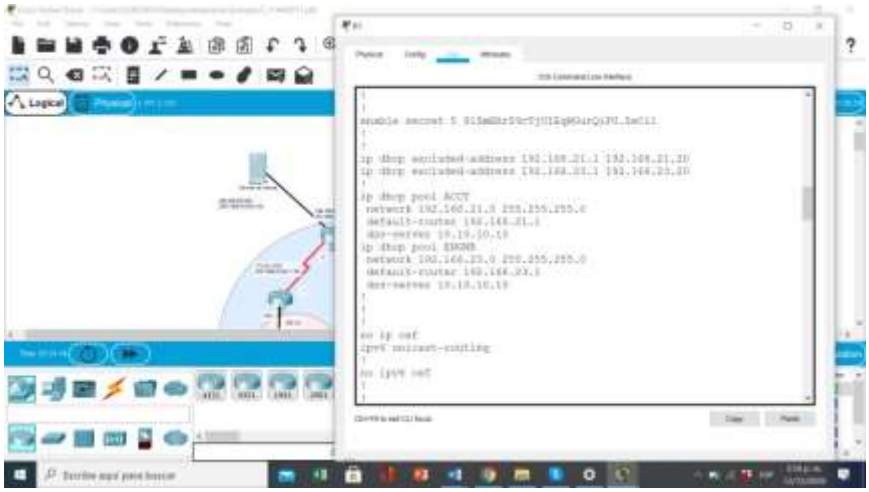
Tabla 29: Configuración de R1 como servidor de DHCP.

Configuración R1 como servidor DHCP	
Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Configuramos con el comando dhcp las direcciones ip que debemos tener en forma estática en la VLAN 21. R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	Configuramos con el comando dhcp las direcciones ip que debemos tener en forma estática en la VLAN 23.

	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Creamos el pool para conectar la VLAN 21 ala que vamos a brindar soporte en la red. R1(config)#ip dhcp pool ACCT R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	Creamos el pool para conectar la VLAN 23 ala que vamos a dar soporte en la red. R1(config)#ip dhcp pool ENGNR R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#default-router 192.168.23.1

En la tabla 29 realizamos la configuración de R1 como servidor de DHCP en la topología desarrollada reservamos direcciones IP en la VLAN 23 y VLAN 21.

Figura 41: R1 como servidor DHCP



Fuente: Autor.

Si observamos la figura 41 Se evidencia la configuración de R1 como servidor DHCP para la asignación de direcciones IP.

Paso 2: Configurar la NAT estática y dinámica en el R2.

La configuración del R2 incluye las siguientes tareas:

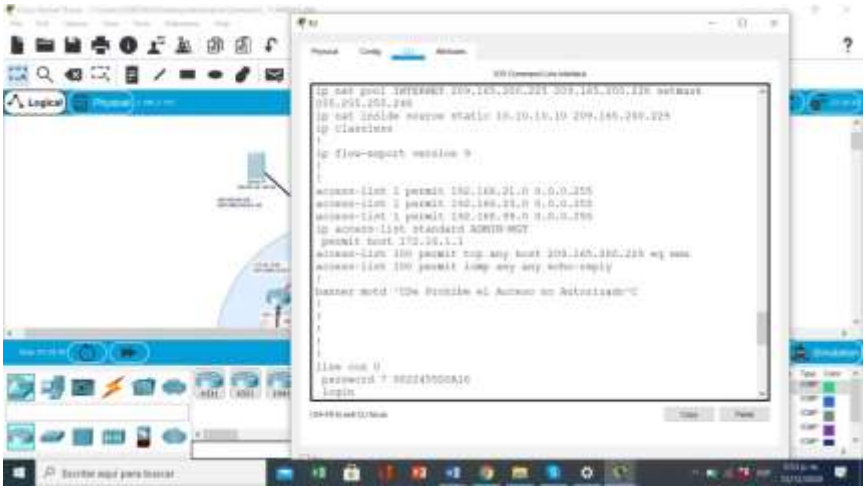
Tabla 30: Configuración NAT en R2

Configuración de NAT en Router 2	
Elemento o tarea de configuración	**especificación**
Crear una base de datos local con una cuenta de usuario	Se realiza la base de datos, y la cuenta de usuario en el router2 con sus caracteristicas. R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	Packet Tracer no procesa la configuración HTTP en su software. R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Se realiza la configuración con los datos requeridos para su autenticación. R2(config)#ip http authentication local
Crear una NAT estática al servidor web.	Se realiza la creación de la NAT para el intercambio de paquetes dentro de la red. R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	Se asigna la interfaz G0/1 para ser utilizada como Nat estatica en la topología desarrollada. R2(config)#interface gi0/1 R2(config)#ip nat outside R2(config)#interface fa0/6 R2(config)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	Se realiza la configuración NAT dinámica la cual os permite tener direcciones ip privadas dentro del acceso local en la topología.

	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Se configure las direcciones públicas las cuales seran utilizadas por los usuarios en la red. R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Configurando la NAT, obtnemos una conexión de red externa para diferentes conexiones internas en la topología. R2(config)#ip nat inside source list 1 pool INTERNET

Se Configura NAT en R2 con sus comandos como se observa en la tabla 30.

Figura 42: configurar NAT en R2



Fuente: Autor.

En la figura 42 vemos la configuración de NAT en R2 correctamente para mejorar la seguridad de la red interna.

Paso 3: Verificar el protocolo DHCP y la NAT estática

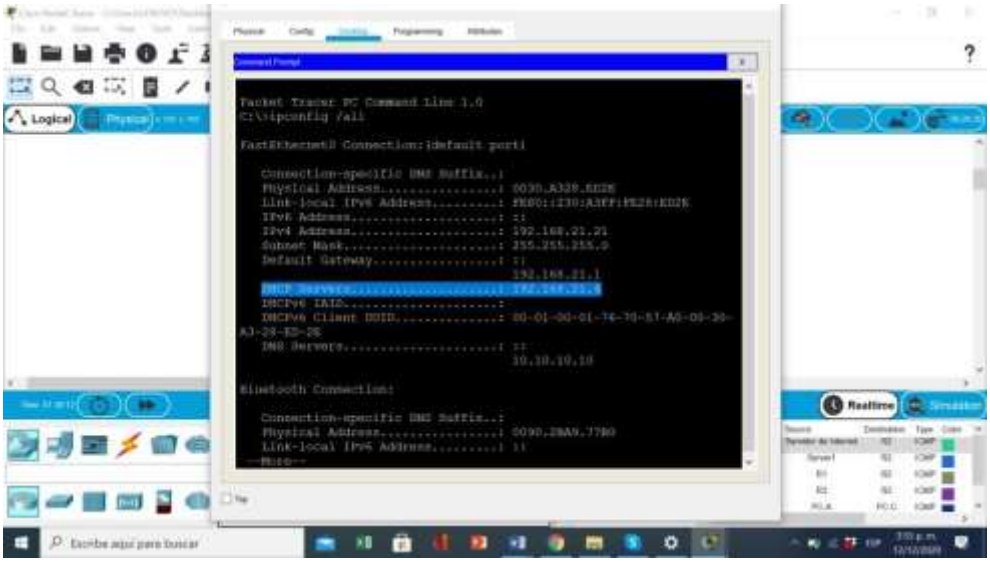
Tabla 31: Verificación del protocolo DHCP y NAT estática en los dispositivos.

Verificación del protocolo DHCP la NAT estática.	
Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Se obtienen resultados óptimos en la configuración. DHCP Servers.....: 192.168.21.4 (figura 43)
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Se verifica que se adquirió la información en DHCP correctamente. DHCP Servers.....: 192.168.21.4 (figura 44)
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	El ping realizado se obtiene conexión exitosa sin interrupciones. Reply from 192.168.21.4: bytes=32 time<1ms TTL=255 (figura 45)
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	La conexión con el servicio de red de la topología se generó con normalidad y sin pérdida de información. Successful (figura 46)

La Configuración de DHCP y NAT exitosa como se puede apreciar en la tabla 31 no hubo afectaciones en la red.

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

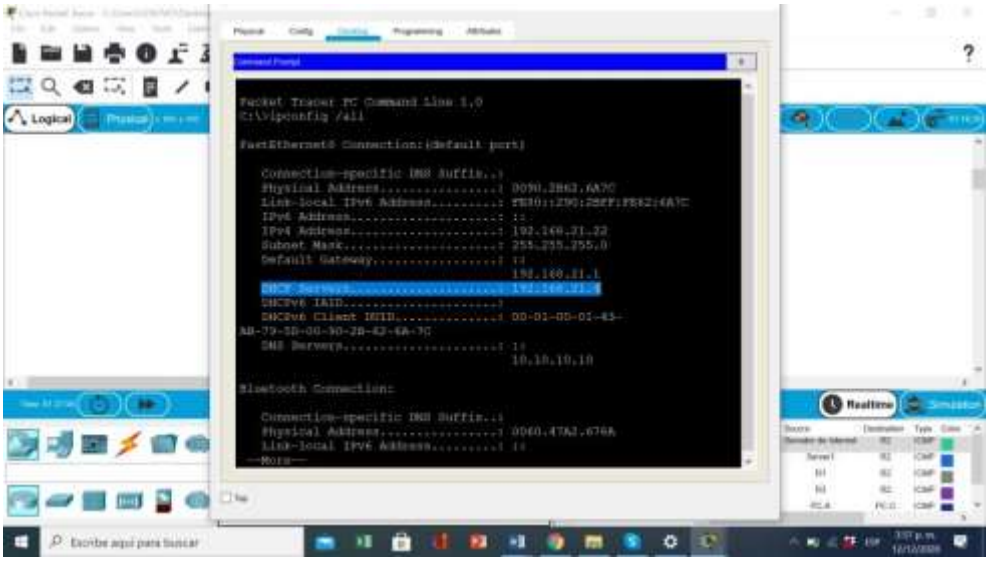
Figura 43:DHCP en PC-A



Fuente: Autor

En la figura 43 vemos la Dirección DHCP en PC-A configurada correctamente para la conexión en la red

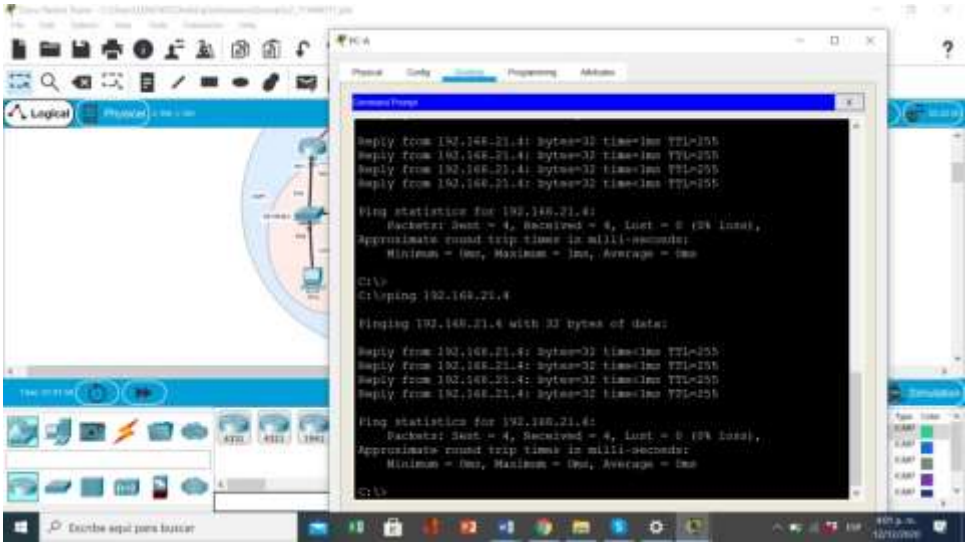
Figura 44:DHCP en PC-C



Fuente: Autor.

La figura 44 evidencia la Configuración DHCP esta correcta en PC-C.

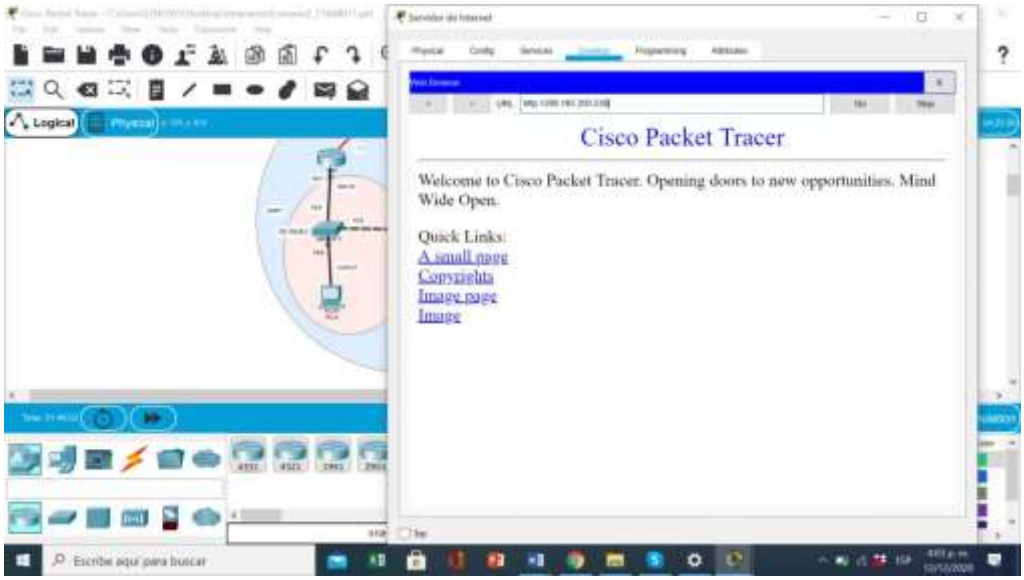
Figura 45:Ping entre PC-A y PC-C



Fuente: Autor.

En la figura 45 Se realizó ping entre PC-A y PC-C sin novedades.

Figura 46: web service.



Fuente: Autor.

Observando la figura 46 vemos la Conexión de red en el servidor de internet exitoso.

Parte 6: Configurar NTP

Tabla 32: Configuración NTP en R1 Y R2.

Configuración de NTP en router 1y 2	
Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	Realizando el comando clock ajustamos fecha y hora del router 2. R2#clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP.	Se configura NTP en el router 2 como maestro para la sincronización de horario. R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	En el router 1 lo utilizamos como cliente y configuramos NTP como servidor. R1(config)#ntp server, 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Al ser servidor R1 configuramos NTP para que actualice el calendario. R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	Se comprueba configuración del NTP en el router 1. R1#show ntp associations R1#show clock

En la tabla 32 se realiza la Tarea de configuración NTP en R1 Y R2 utilizando R1 como cliente y el router 2 como maestro para la sincronización.

Figura 47: Verificación de la configuración NTP en R1.

Fuente: Autor.

En la figura 47 observamos la configuración de NTP correcta en R2 para establecer sincronización en la red.

Parte 7: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 33: Configuración y verificación de las ACL

Configuración y verificación de ACL en R2	
Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Se realiza la lista de acceso para conectar telnet entre el Router 1 y el Router 2. R2(config)#ip access-list standart ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	Se realiza la lista de control de acceso que nos permite denegar o permitir paquetes en la dirección de origen. R2(config-line)#line vty 0 4
Permitir acceso por Telnet a las líneas de VTY	Se realiza la configuración que permita el acceso a telnet otorgando el acceso al dispositivo. R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	Se realizan las pruebas y se obtiene conexión entre los routers. R1#telnet 172.16.1.2 R3#telnet 172.16.1.2

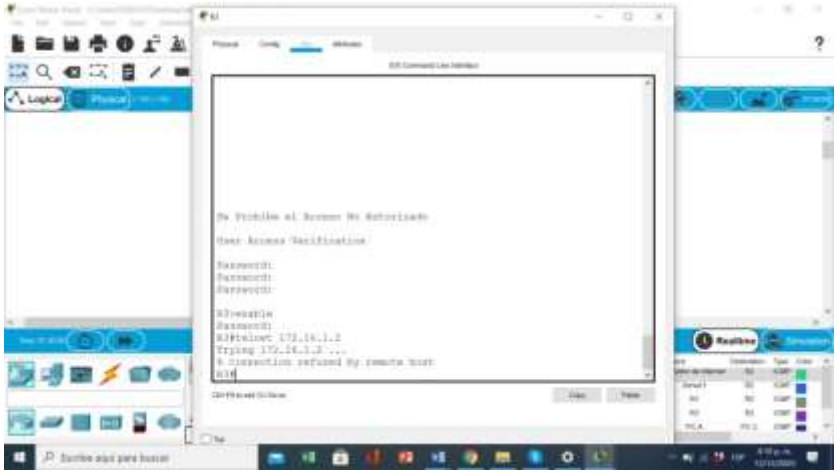
Como observamos en la tabla 33 se realizaron los Pasos para la configuración VTY y telnet con su conexión entre los routers.

Figura 48: funcionamiento VTY

Fuente: Autor.

En la figura 48 se crea la lista ACL con configuración telnet usando VTY.

Figura 49: Realizar telnet en R3



Fuente: Autor.

En la figura 49 vemos como Telnet funciona correctamente en R3 para ser utilizar remotamente los dispositivos de la red.

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

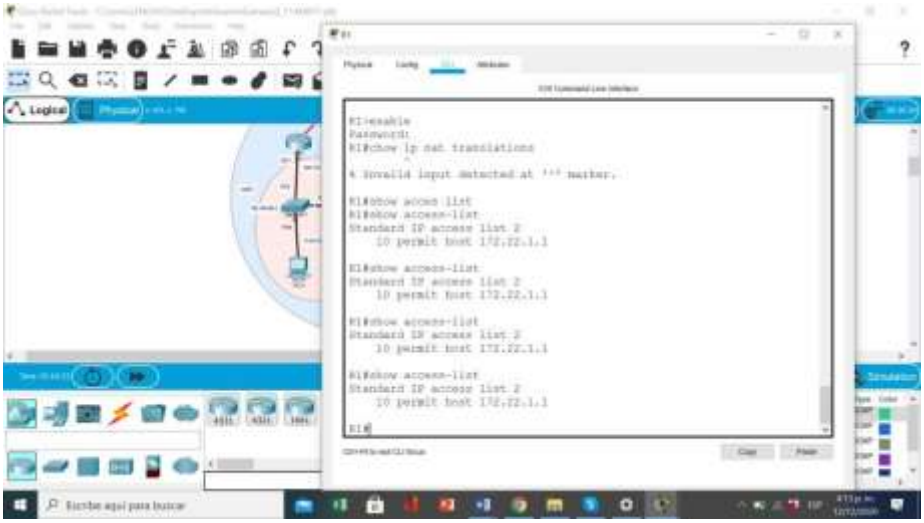
Tabla 34: Comandos para realizar las verificaciones de las configuraciones realizadas en los dispositivos.

Comando CLI	
Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Se realizó la configuración del comando show ip Access list. R1 #show ip access list
Restablecer los contadores de una lista de acceso	Utilizando la configuración Access list, podemos reestablecer los contadores. R1(config)#ip access-list standard 2

	R1(config-std-nacl)#18 permit 172.22.1.1 R1(config-std-nacl)#exit
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Utilizando el comando show ip interface aplicamos la dirección que necesitamos utilizar. #show ip interface
¿Con qué comando se muestran las traducciones NAT?	Con el comando show ip NAT nos muestras el intercambio de paquetes. #show ip nat translations
¿Qué comando se utiliza para eliminar las Traducciones de NAT dinámicas?	Con el comando clear ip NAT borramos la configuraciónde envio de paquetes. #clear ip nat translations

En la tabla 34 observamos Los comandos se realizaron acorde a la actividad.

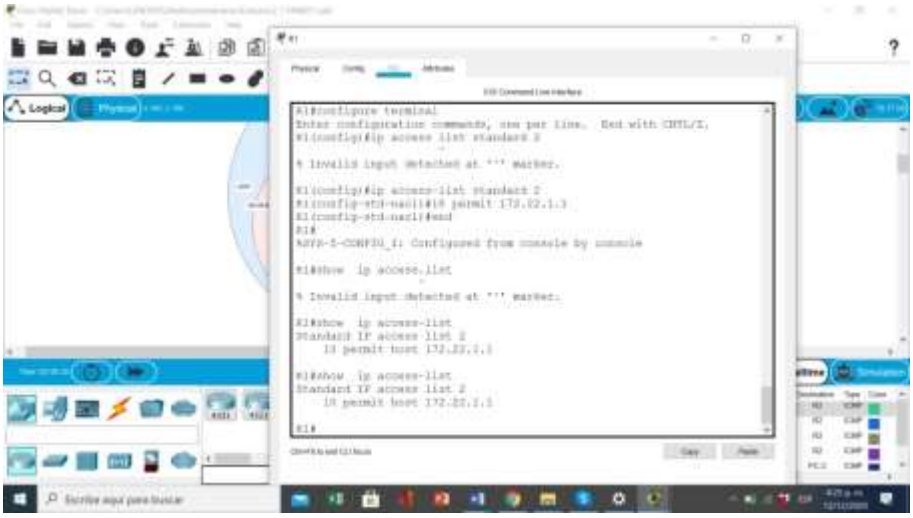
Figura 50 utilización comando show ip Access list.



Fuente: Autor.

En la figura 50 podemos ver el resultado con el comando show Access list, nos muestra la lista de acceso y lo que está permitido.

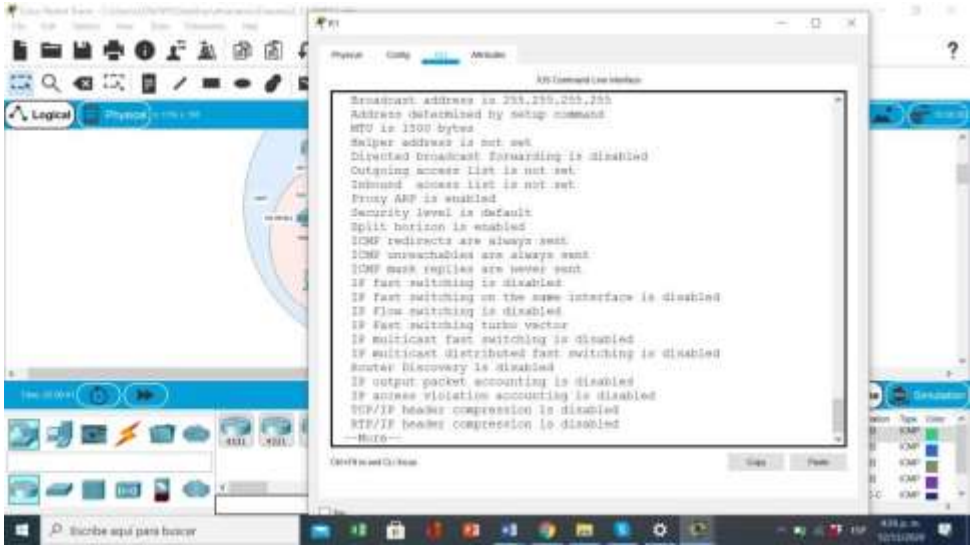
Figura 51: Comando access List.



Fuente: Autor.

Con la figura 50 vemos como se realza el proceso de reestablecer contadores en una lista de acceso.

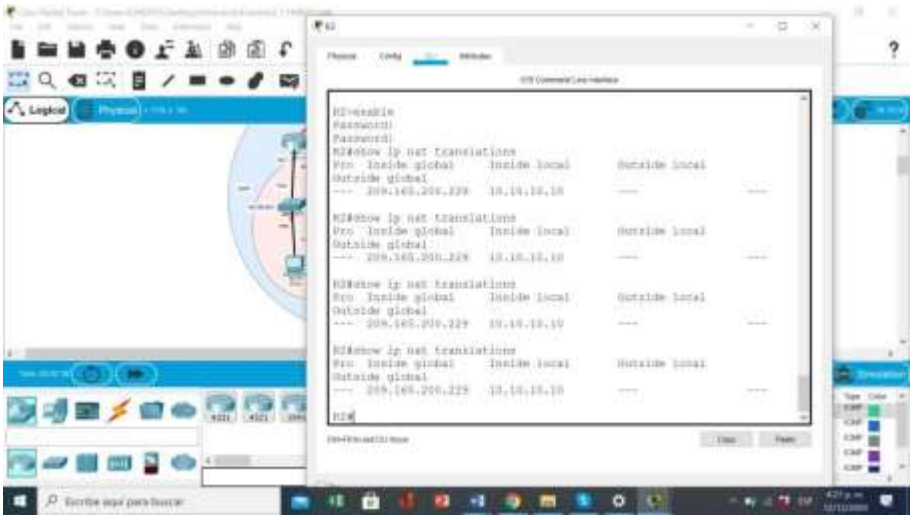
Figura 52:Comando Show ip interface.



Fuente: Autor.

Se realiza la comprobación del comando show ip interface tal y como se muestra en la figura 52.

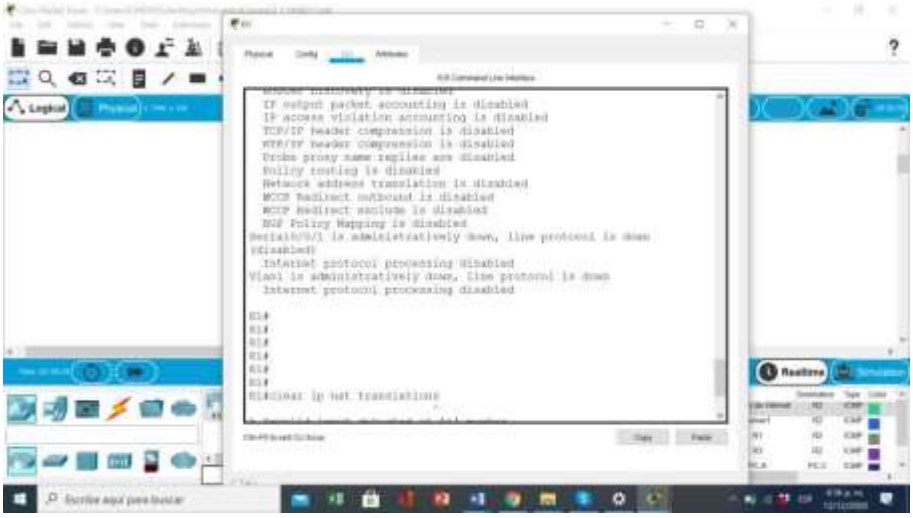
figura 53: comando show ip nat translations



Fuente: Autor.

Con el comando show ip nat translations podemos identificar el puerto local y global del router 2 como se evidencia en la figura 53.

figura 54: borrado de nat dinámicas



Fuente: Autor

en la figura 54 se realiza el borrado de las nat dinámicas.

CONCLUSIONES

En el desarrollo de la prueba se comprende la mayoría de conceptos vistos en el transcurso del curso del diplomado de profundización cisco y nos desarrolla las habilidades básicas para enfrentarnos a problemas de la vida cotidiana, al realizar una descripción de cada una de las etapas realizadas de manera ordenada, registrando cada una de las estructuras de comandos requeridos, permite hacer un mejor manejo de los temas comprendiendo y la función de cada comando.

La topología OSPF es muy utilizada en la actualidad ya que su configuración se puede utilizar en cualquier plataforma tecnológica y es el más recomendado por la sociedad de ingenieros de internet (IETF).

El manejo adecuado de las listas de ACL y NAT nos permite filtrar el tráfico de dispositivos y podemos negarles o permitirles el acceso dependiendo las direcciones de la red, mejoran la administración de redes.

Cuando utilizamos DHCP nos facilita el manejo de las direcciones ip, facilitando la configuración de los dispositivos que se encuentren en la red y permitiendo la conexión entre dispositivos de manera más sencilla, ofreciendo al usuario conectarse rápidamente a distintas redes sin tener que realizar ajuste en su configuración.

IPV6 es la evolución de ipv4, ya que esta nos permite más capacidad en direcciones ip lo cual nos ayuda a mantener la red por más tiempo sin sufrir una falta de direcciones, logrando una evolución en la red y ampliándola para más dispositivos, en la actualidad los dispositivos cuentan con ambos protocolos para su conexión a la red.

REFERENCIAS

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de

https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1
UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

ANEXOS

Anexo1: consolidado trabajo final link google drive:

https://drive.google.com/drive/folders/1Gr6D61nZzvCLpOyJ3f1JLkOoQ0EtdD1X?usp=sharing