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

JOHN FREDDY MINA MONTENEGRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
PROGRAMA INGENIERÍA SISTEMAS
CALI 2020

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

Trabajo de la opción de grado para optar al título de Ingeniero de Sistemas

JOHN FREDDY MINA MONTENEGRO

TUTOR:
INGENIERO DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
PROGRAMA INGENIERÍA SISTEMAS
CALI 2020

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Santiago de Cali, 12 de diciembre 2020

AGRADECIMIENTOS

Agradezco primero a Dios todo poderoso por ser él el principal responsable de este logro en mi vida, por nunca dejarme solo, por darme su iluminación en momentos difíciles, ser mi guía en cada paso que doy, ser mi fortaleza y así hoy estar a punto de cumplir esta meta en mi vida.

Gracias a mi familia por la confianza, el apoyo, la motivación y nunca dejarme solo y mantener firma la confianza y el cariño para que me esforzara cada vez más en el cumplimiento de este objetivo que sin su compañía no lo hubiese logrado.

Por último, pero no menos agradecido, a todos los miembros de la universidad que de uno u otra forma fueron quienes me apoyaron y dieron fuerza en momentos de dificultad. A todos los tutores de las diferentes asignaturas por compartir su conocimiento y saber guiar mi aprendizaje, a mis compañeros de los cuales aprendí mucho y creo que deja muy buenos amigos y colegas. ¡Infinitas gracias a todos!

CONTENIDO

AGRADECIMIENTOS 4
LISTA DE FIGURAS 7
LISTA DE TABLAS 9
GLOSARIO 10
RESUMEN 11
Palabras clave 11
ABSTRAC 11
Key words: 11
INTRODUCCIÓN 12
OBJETIVOS 13
Objetivo General 13
Objetivos Específicos: 13
DESARROLLO DEL PROYECTO 14
1 ESCENARIO 1 14
Topología 14
Tabla de asignación de direcciones 15
Parte 1: Inicializar y Recargar y Configurar Aspectos Básicos de los Dispositivos 15
Paso 1: Inicializar y volver a cargar el router y el switch 15
Paso 2: Configurar R1 18
Paso 3: Configure S1 y S2 21
Configuración S2 22
Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) 24
Paso 4: Configurar S1 24
Paso 5: Configure el S2 26
Parte 2: Configurar soporte de host. 28
Paso 1: Configure R1 28
Paso 2: Configurar los servidores 29
Parte 3: Probar y verificar la conectividad de extremo a extremo 32
3.2 ESCENARIO 2 37
Topología 37
Parte 1: Inicializar dispositivos 37
Paso 1: Inicializar y volver a cargar los routers y los switches. 37
Parte 2: Configurar los parámetros básicos de los dispositivos 40
Paso 1: Configurar la computadora de Internet 40
Paso 2: Configurar R1 41
Paso 3: Configurar R2 43
Paso 4: Configurar R3 45
Paso 5: Configurar S1 47
Paso 6: Configurar el S3 48

Paso 7: Verificar la conectividad de la red 50
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN .53
Paso 1: Configurar S1 53
Paso 2: Configurar el S3..... 55
Paso 3: Configurar R1 56
Paso 4: Verificar la conectividad de la red 58
Parte 4: Configurar el protocolo de routing dinámico OSPF 61
Paso 1: Configurar OSPF en el R1..... 61
Paso 2: Configurar OSPF en el R2..... 63
Paso 3: Configurar OSPFv3 en el R3..... 64
Paso 4: Verificar la información de OSPF..... 65
Parte 5: Implementar DHCP y NAT para IPv4 66
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 67
Paso 2: Configurar la NAT estática y dinámica en el R2. 68
Paso 3: Verificar el protocolo DHCP y la NAT estática..... 70
Parte 6: Configurar NTP 73
Parte 7: Configurar y verificar las listas de control de acceso (ACL) 74
Paso 1: Restringir el acceso a las líneas VTY en el R2..... 74
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente 76
CONCLUSIONES 1
REFERENCIAS 2
ANEXOS..... 2

LISTA DE FIGURAS

Figura 1: topología escenario 1 14
Figura 2: recarga de los switch 16
Figura 3:topologia terminada 17
Figura 4:configuración r1 20
Figura 5:configuración s1 y s2 24
Figura 6:configuración dela infraestructura. 27
Figura 7:configuración r1 29
Figura 8: configuración de red del host a 30
Figura 9: configuración de red del host b 31
Figura 10: verificación de conectividad del pc-a de extremo a extremo 35
Figura 11: verificación de conectividad del pc-b de extremo a extremo 35
Figura 12 topología escenario 2 37
Figura 13:reinicio de los dispositivos 38
Figura 14: configuración terminada 39
Figura 15:configuración servidor de internet. 40
Figura 16:configuración r1 42
Figura 17:configuración r2 45
Figura 18: configuración r3 47
Figura 19: configuración s1 48
Figura 20: configuración s3 49
Figura 21: verificación de la conexión de r1 51
Figura 22 verificación de la conexión de r2 52
Figura 23: verificación de la conexión del servidor de red a su gateway predeterminado 52
Figura 24: seguridad s1 54
Figura 25:configuración de s3 56
Figura 26: configuración r1 57
Figura 27 verificación de conexión de red en s1 59
Figura 28:verificación de s3 59
Figura 29:verificación s1 60
Figura 30: verificación de s3 61
Figura 31:configuración ospf r1 62
Figura 32:configuración en r2 63
Figura 33:configuración r3 65
Figura 34 verificación de la información ospf 66
Figura 35: r1 como servidor dhcp 68
Figura 36:configurar nat en r2 69
Figura 37:dhcp en pc-a 71
Figura 38:dhcp en pc-c 72
Figura 39:ping entre pc-a y pc-c 72

Figura 40: web service. 73
Figura 41: verificación de la configuración ntp en r1. 74
Figura 42.:funcionamiento vty 75
Figura 43:realizar telnet en r3 75

LISTA DE TABLAS

Tabla 1:Asignación de las VLAN.....14
Tabla 2: Asignación de Direcciones.....15
Tabla 3:Inicialización de router y los switches.....16
Tabla 4: Configuraciones básicas en R1 escenario 1 18
Tabla 5: Configuraciones básicas en S1 del primer escenario.....21
Tabla 6: Configuraciones básicas en S2 del primer escenario.....22
Tabla 7 Configuración de la infraestructura de red en S1 24
Tabla 8: Configuración de la infraestructura de red en S2 26
Tabla 9: Configuración de la infraestructura de red en R1.....28
Tabla 10: Configuración de PC-A.....29
Tabla 11: Configuración de PC-B.....30
Tabla 12: verificar la conectividad de extremo a extremo 32
Tabla 13 :Verificación inicial de los dispositivos del segundo escenario 38
Tabla 14: Indicaciones para configurar la computadora red internet.....40
Tabla 15: Configuraciones básicas de R1 en el segundo escenario.....41
Tabla 16: Configuraciones básicas para el R2.....43
Tabla 17: Configuraciones básicas de R3 en el segundo escenario.....45
Tabla 18: Configuraciones básicas de S1 en el segundo escenario 47
Tabla 19: Configuraciones básicas de S3 en el segundo escenario 49
Tabla 20 :Verificación de conectividad en los routers y en el PC. 50
Tabla 21: Configuración de la seguridad del switch y el routing entre las vlan de S1 53
Tabla 22: Configuración de la seguridad del switch y el routing entre las vlan de S3 55
Tabla 23: Configuración de la seguridad del switch y el routing entre las vlan de R1. 57
Tabla 24: verificación de la topología.....58
Tabla 25: Configuración OSPF área 0 en R1.....61
Tabla 26: Configuración OSPF área 0 en R2.....63
Tabla 27: configurar R3.....64
*Tabla 28: Comandos para realizar las verificaciones de las configuraciones. *65
Tabla 29: Configuración de R1 como servidor de DHCP 67
Tabla 30: Configuración NAT en R2 68
Tabla 31 :Verificación del protocolo DHCP y NAT estática en los dispositivos 70
Tabla 32: Configuración NTP en R1 Y R2 73
Tabla 33: Configuración y verificación de las ACL 74
Tabla 34: Comandos para realizar las verificaciones de las configuraciones realizadas en los dispositivos.....76

GLOSARIO

GNS3: simulador grafico de red. Es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Con GNS3 los usuarios tendrán la posibilidad de poder escoger cada uno de los elementos que llegarán a formar parte de una red informática

HOST: ordenador que funciona como punto de inicio y final de la transferencia de datos.

NETWORKING: establecimiento de conexiones de interacción y trabajo. En el mundo de las computadoras, el concepto de networking aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos.

PROTOCOLOS DE RED: conjunto de reglas que rigen el intercambio de información. Los protocolos se muestran en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores.

VLAN: (Virtual local área), Red de área local que agrupa un conjunto de equipos de manera lógica y no física

RESUMEN

La principal característica de un protocolo de enrutamientos es que esta permite compartir información entre los diversos ROUTERS de manera remota y actualizar de manera dinámica la información de enrutamiento a sus propias tablas y compartirlas entre sí.

La ventaja más significativa de los Routers con protocolo dinámico es que este permite hacer un informe en el cambio de la topología (RUTAS) entre los distintos routers de la red y estos a su vez aprenden automáticamente las nuevas redes, así como las bajas de las mismas.

Podemos decir que uno de los primeros protocolos utilizados formalmente es el RIP en su versión, aunque muchos de los algoritmos usados en el son productos directos del abuelo ARPANET. Aun cuando el RIP ha evolucionado a su versión 2, este aun presenta algunos problemas de escalamiento, dejándolo atrás cuando se requiere de redes grandes, una mejor opción es usar versiones de protocolos más avanzados tales como el IGRP y el EIGRP, ambos productos de CISCO

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

ABSTRAC

We can say that one of the first protocols used formally is the RIP in its version, although many of the algorithms used in it are direct products of the grandfather ARPANET. Even though the RIP has evolved to version 2, it still presents some scaling problems, leaving it behind when large networks are required, a better option is to use more advanced protocol versions such as IGRP and EIGRP, both CISCO products.

The main characteristic of a routing protocol is that it allows to share information between the different ROUTERS remotely and dynamically update the routing information to its own tables and share them with each other.

The most significant advantage of routers with dynamic protocol is that it allows reporting in the change of the topology (ROUTES) between the different routers in the network and these in turn automatically learn the new networks, as well as the lows of the same.

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

INTRODUCCIÓN

Las redes modernas continúan evolucionando para adaptarse a la manera cambiante en que las organizaciones realizan sus actividades diarias. Ahora los usuarios esperan tener acceso instantáneo a los recursos de una compañía, en cualquier momento y en cualquier lugar. Estos recursos incluyen no solo datos tradicionales, sino también de video y de voz. También hay una necesidad creciente de tecnologías de colaboración que permitan el intercambio de recursos en tiempo real entre varias personas en sitios remotos como si estuvieran en la misma ubicación física.

Los distintos dispositivos deben trabajar en conjunto sin inconvenientes para proporcionar una conexión rápida, segura y confiable entre los hosts. Los switches LAN proporcionan el punto de conexión a la red empresarial para los usuarios finales y también son los principales responsables del control de la información dentro del entorno LAN. Los routers facilitan la transmisión de información entre redes LAN y, en general, desconocen a los hosts individuales. Todos los servicios avanzados dependen de la disponibilidad de una infraestructura sólida de routing y switching sobre la que se puedan basar. Esta infraestructura se debe diseñar, implementar y administrar cuidadosamente para proporcionar una plataforma estable necesaria.

OBJETIVOS

Objetivo General

“Implementar una solución ante una problemática determinada en una pequeña empresa que quiere establecer un diseño de red que beneficie la conectividad y la eficiencia en el transporte de voz, audio y video en todas sus sucursales.”

Objetivos Específicos:

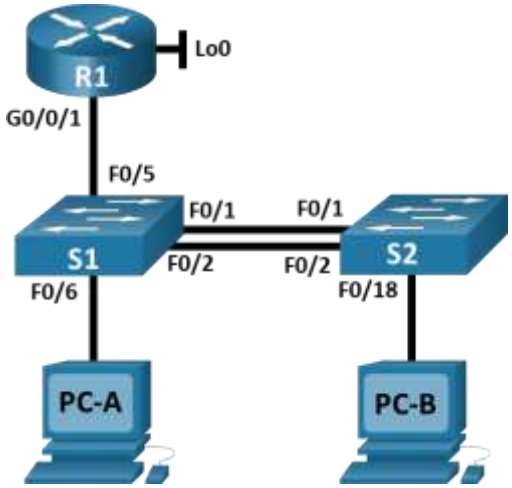
- Realizar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing, de DHCP, NAT, RIP Ver2, dando solución a ciertos problemas, Implementando la debida seguridad en los Router y políticas necesarias.
- Identificar los dispositivos a utilizar para la construcción de una topología de red, configurando los dispositivos a medida que se van implementando instrucciones de configuración.

1. DESARROLLO DEL PROYECTO

1.1 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

Nombre de 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
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

Direcciones 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

Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

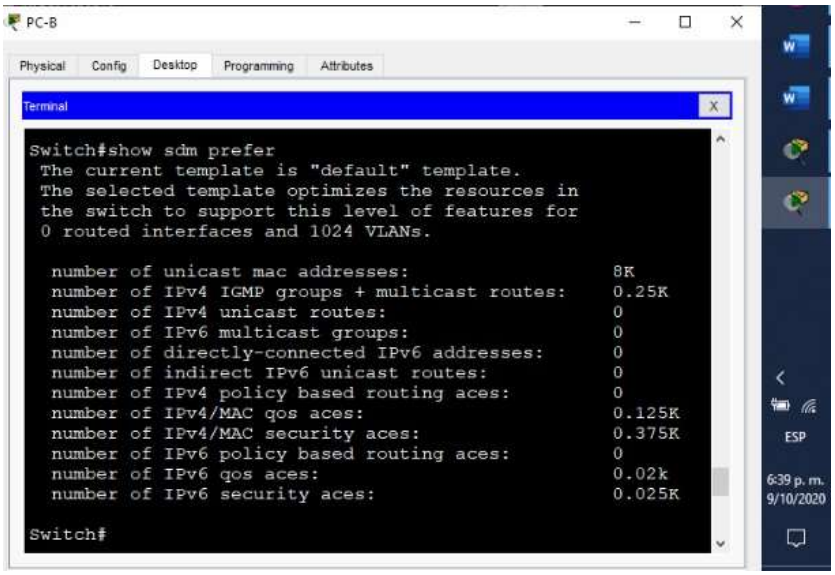
Tabla 3:Inicialización de router y los switches.

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
Configuración de sdm	S1>enable S1#config t S1(config)#sdm prefer dual-ipv4-and-ipv6 default

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.

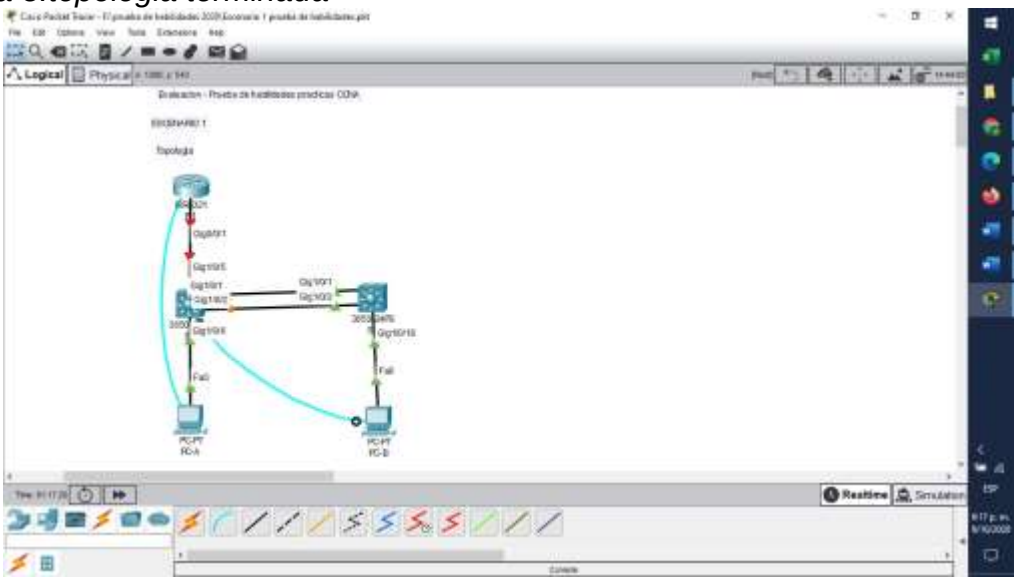


Fuente: Autor

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:topologia terminada



Fuente: Autor

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.

En esta 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

Figura: Autor

se configura R1 con las características descritas para el uso del router 1.

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

Configuraciones requeridas para la conexión del S1 a la topología.

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

Configuración del S2 para su conexión en la topología.

Figura 5:configuración S1 y S2

Fuente: Autor

se realiza la configuración de S1 y S2 para conectar con R1 y los respectivos computadores.

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

Configuración que se realiza para la infraestructura de S1utilizando los comandos respectivos para una buena conexión de la topología.

Paso 5: Configure el S2

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

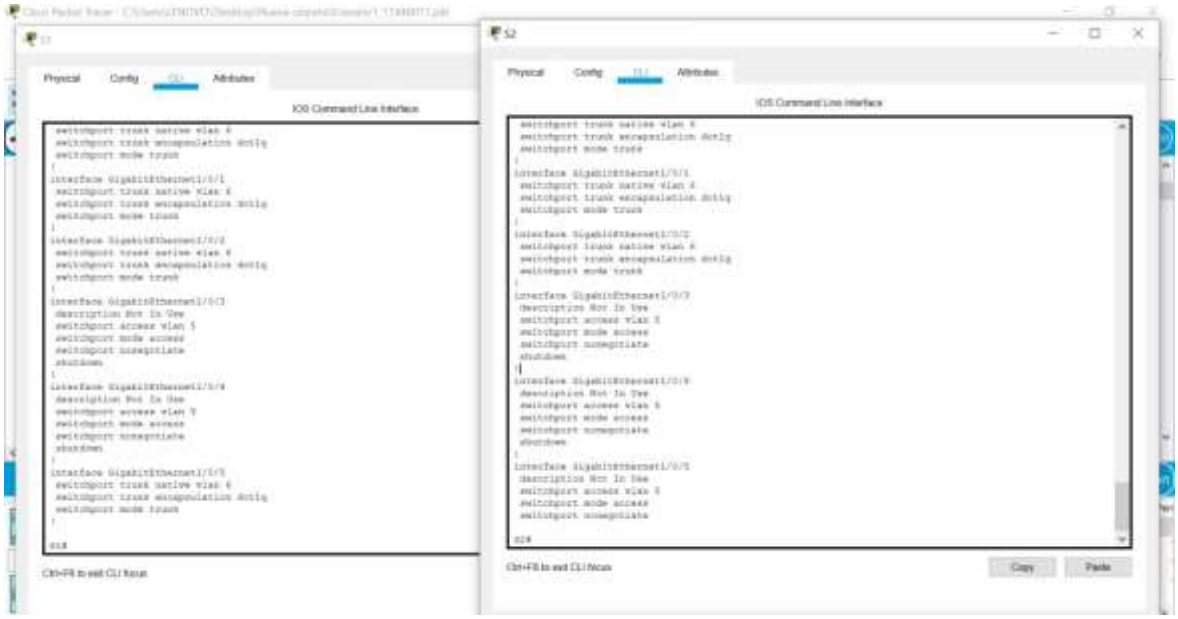
Tabla 8: Configuración de la infraestructura de red en S2.

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 elmaximo 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

Realización de la configuración en la red en S2 instalada.

figura 6:configuración dela infraestructura.



Fuente: Autor

se crea la infraestructura de VLAN, Trunking, EtherChannel de los switch y se verifica que están configuradas correctamente.

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

Se configura la estructura del R1 para su conexión en la topología que venimos desarrollando en este escenario.

Figura 7: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

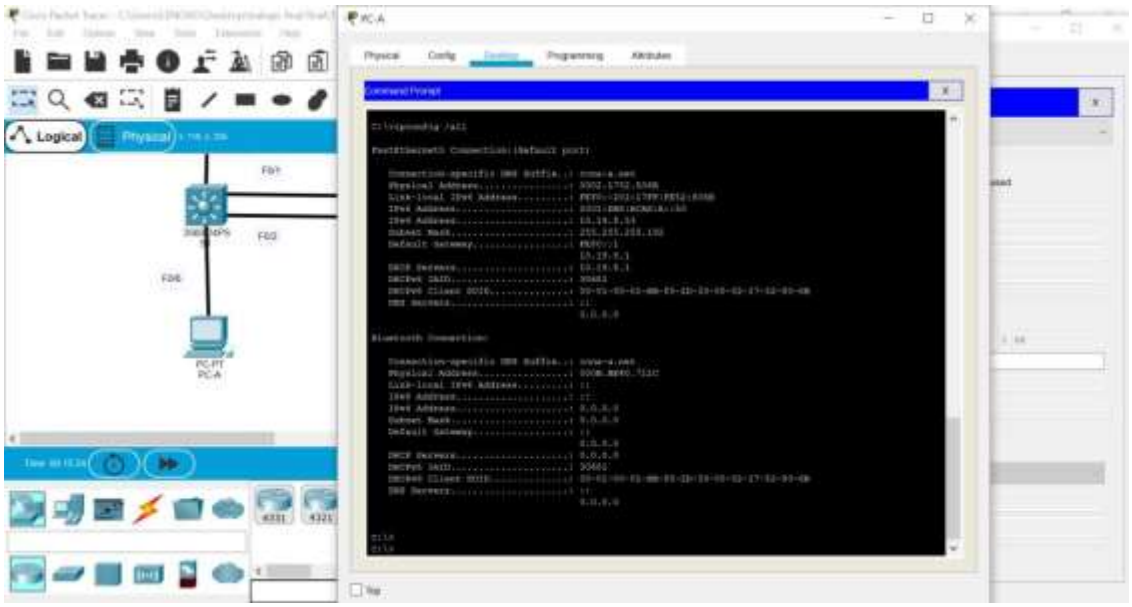
Se realiza configuración del PC-A para obtener conexión de red en los equipos que están conectados en la topología realizada.

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.

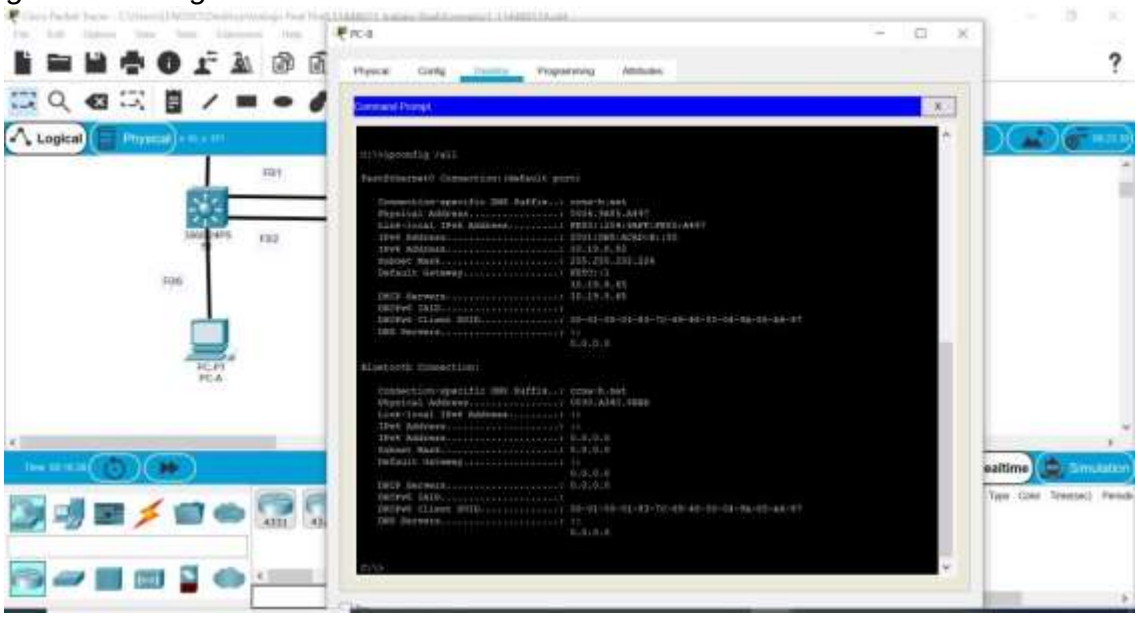
Figura 8: Configuración de red del host A.



Fuente: Autor

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

Figura 9: 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	ok
PC-A	R1, G0/0/1.2	IPv6	2001:db8:acad:a: :1	ok
PC-A	R1, G0/0/1.3	Dirección	10.19.8.65	ok
PC-A	R1, G0/0/1.3	IPv6	2001:db8:acad:b: :1	ok
PC-A	R1, G0/0/1.4	Dirección	10.19.8.97	ok
PC-A	R1, G0/0/1.4	IPv6	2001:db8:acad:c: :1	ok

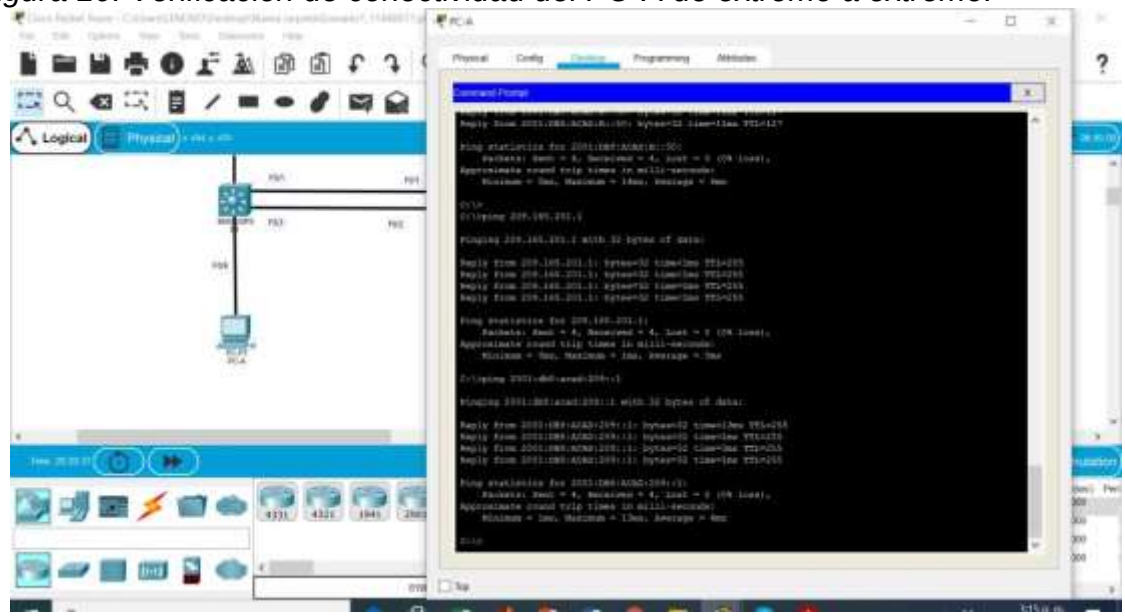
PC-A	S1, VLAN 4	Dirección	10.19.8.98	ok
PC-A	S1, VLAN 4	IPv6	2001:db8:acad:c: :98	ok
PC-A	S2, VLAN 4	Dirección	10.19.8.99.	ok
PC-A	S2, VLAN 4	IPv6	2001:db8:acad:c: :99	ok
PC-A	PC-B	Dirección	10.19.8.85	ok
PC-A	PC-B	IPv6	2001:db8:acad:b: :50	ok
PC-A	R1 Bucle 0	Dirección	209.165.201.1	ok
PC-A	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	ok

PC-B	*R1 Bucle 0*	*Dirección*	*209.165.201 .1*	ok
PC-B	R1 Bucle 0	*IPv6*	*2001:db8:ac ad:209: :1*	ok
PC-B	*R1, G0/0/1. 2*	*Dirección*	*10.19.8.1*	ok
PC-B	R1, G0/0/1. 2	*IPv6*	*2001:db8:ac ad:a: :1*	ok
PC-B	*R1, G0/0/1. 3*	*Dirección*	*10.19.8.65*	ok
PC-B	R1, G0/0/1. 3	*IPv6*	*2001:db8:ac ad:b: :1*	ok
PC-B	*R1, G0/0/1. 4*	*Dirección*	*10.19.8.97*	ok
PC-B	R1, G0/0/1. 4	*IPv6*	*2001:db8:ac ad:c: :1*	ok
PC-B	*S1, VLAN 4*	*Dirección*	*10.19.8.98*	ok

PC-B	S1, VLAN 4	*IPv6*	*2001:db8:acad:c: :98*	ok
PC-B	*S2, VLAN 4*	*Dirección*	*10.19.8.99.*	ok
PC-B	S2, VLAN 4	*IPv6*	*2001:db8:acad:c: :99*	ok

Se verifica la conectividad de los dispositivos.

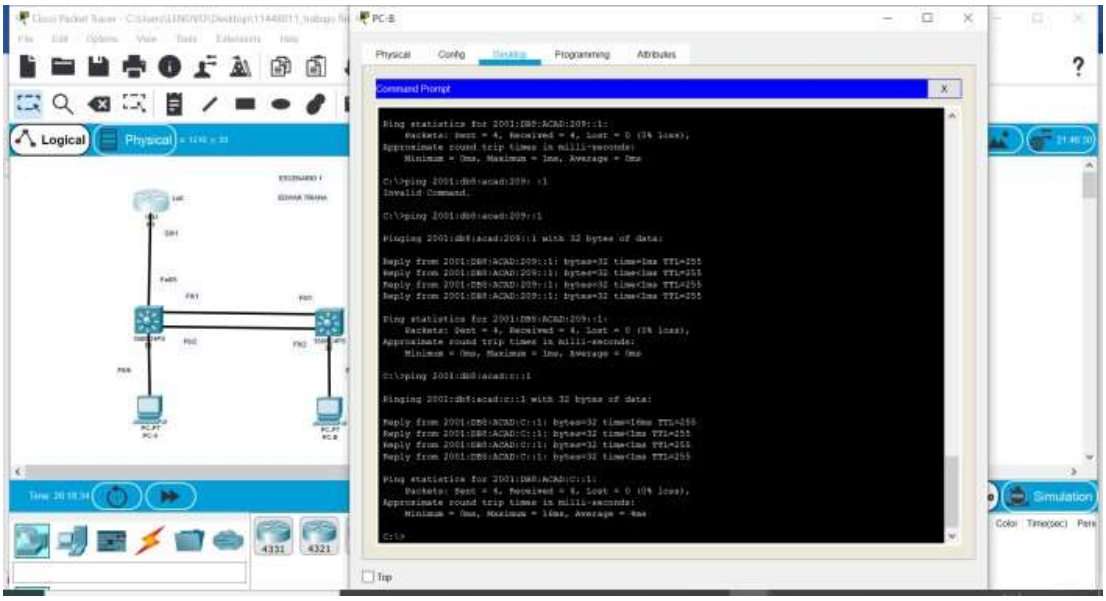
Figura 10: Verificación de conectividad del PC-A de extremo a extremo.



Fuente: Autor

se realiza conexión exitosa de extremo a extremo entre PC-A y PC-B y demás equipos.

Figura 11: Verificación de conectividad del PC-B de extremo a extremo.



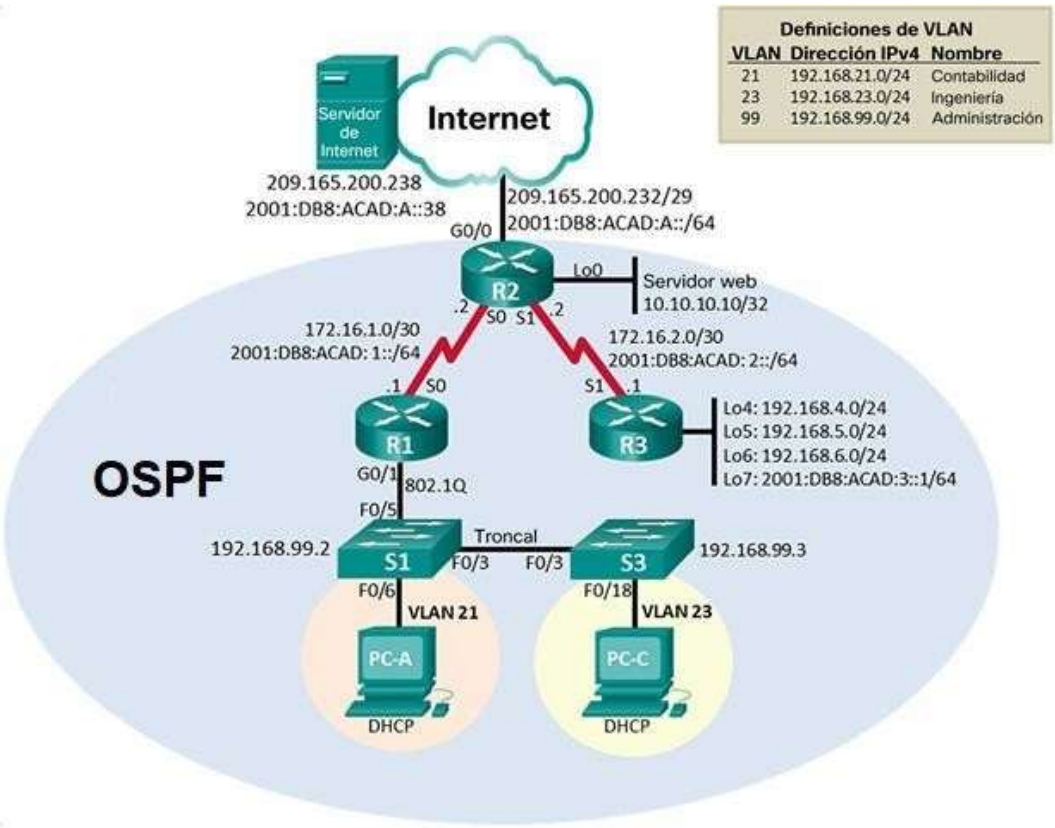
Fuente: Autor

se realiza conexión exitosa entre los diferentes equipos de la topología.

2 ESCENARIO 2

Topología

Figura 12 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.

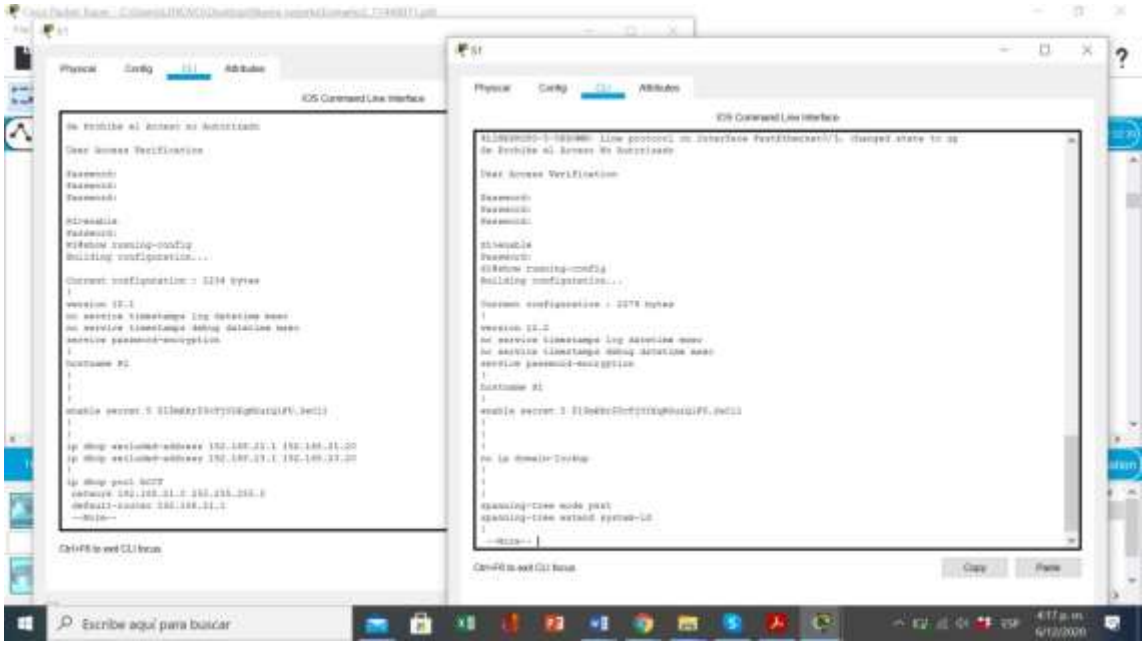
Tabla 13 :Verificación inicial de los dispositivos del segundo escenario

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.

Por medio de los siguientes comandos. Se realizan las configuraciones de formateo y reinicio tanto en los Routers como en los Switch.

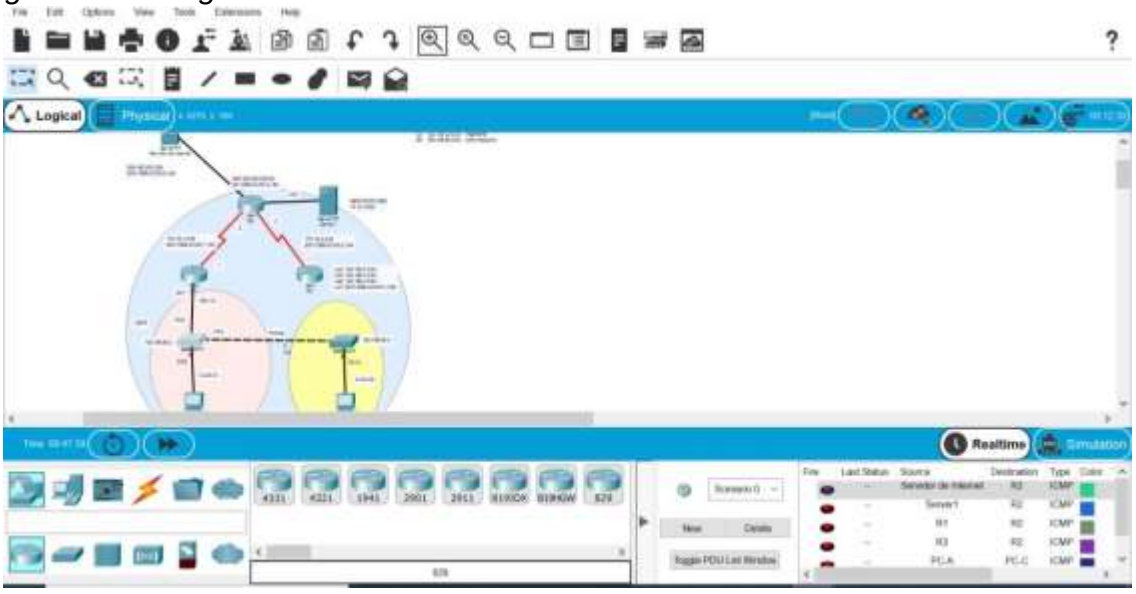
Figura 13:reinicio de los dispositivos.



Fuente: Autor

Autor, se recargan los dispositivos para configurar sus funciones.

Figura 14: configuración terminada.



Fuente: Autor

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):

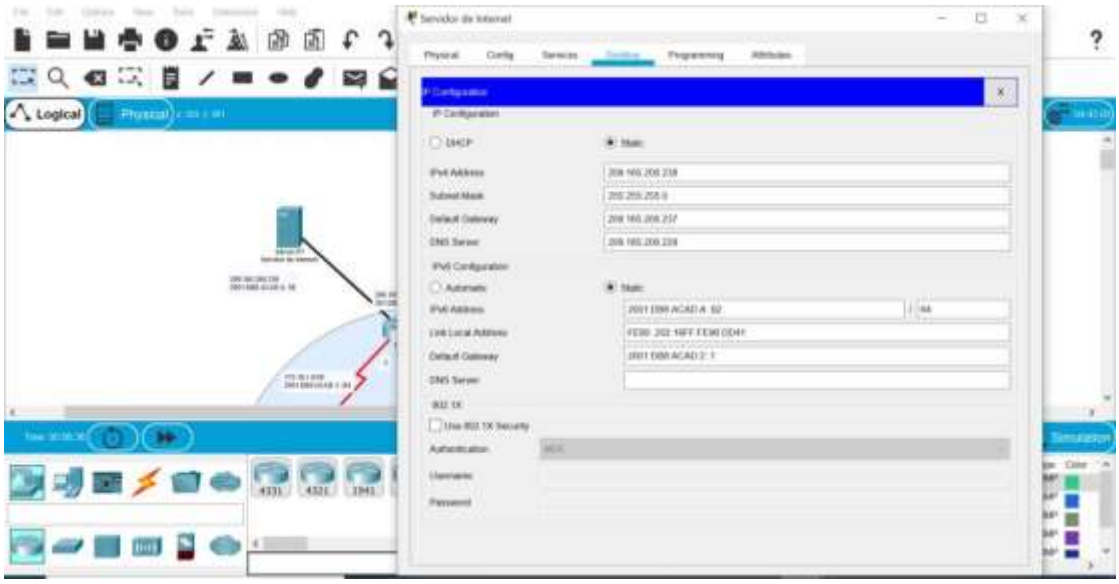
Tabla 14: Indicaciones para configurar la computadora red internet.

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

Tabla de configuración realizada para la conexión del servidor de internet.

Se realiza la configuración de internet para garantizar la conexión de los dispositivos que se van a conectar, garantizando una conexión sin fallas consultando las direcciones que están descritas en la topología que se va a desarrollar.

Figura 15:configuración servidor de internet.



Fuente: Autor

Autor se configura el servidor de internet con la tabla descrita anteriormente.

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:

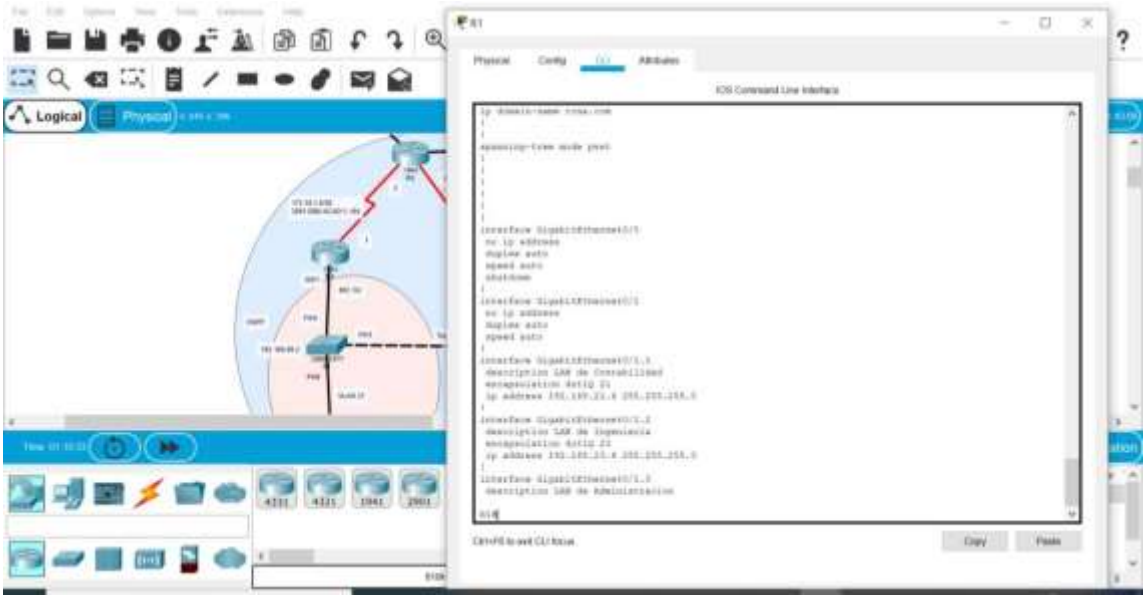
Tabla 15: Configuraciones básicas de R1 en el segundo escenario.

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

Configuración que se utilizara en el router para su conexión 1.

Figura 16:Configuración R1.



Fuente: Autor

se realiza la configuración de R1 para la conexión de los dispositivos.

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

Tareas básicas que utilizara el Router2.

Figura 17:Configuración R2.

Fuente: Autor
se configura el R2 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

Tareas para desarrollar la conexión en el Router 3.

Figura 18: configuración R3.

Fuente: Autor

Autor, se realiza la configuración de R3 para su conexión a la topología.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

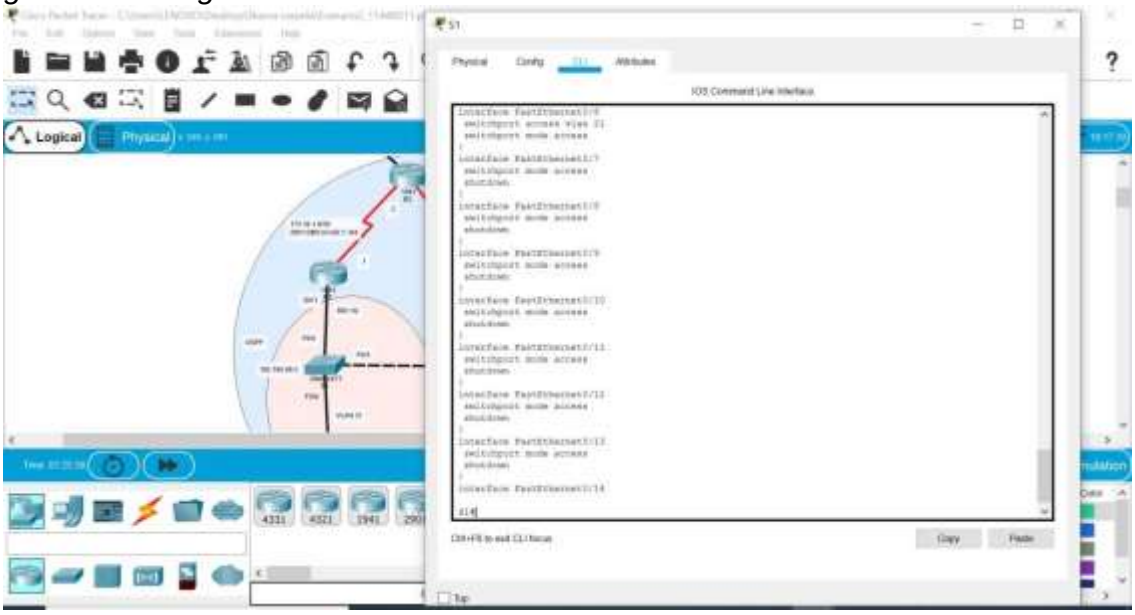
Tabla 18: Configuraciones básicas de S1 en el segundo escenario.

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 para la conexión de S1 a la topología que estamos desarrollando.

Figura 19: configuración S1.



Fuente: Autor

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

Paso 6: Configurar el S3

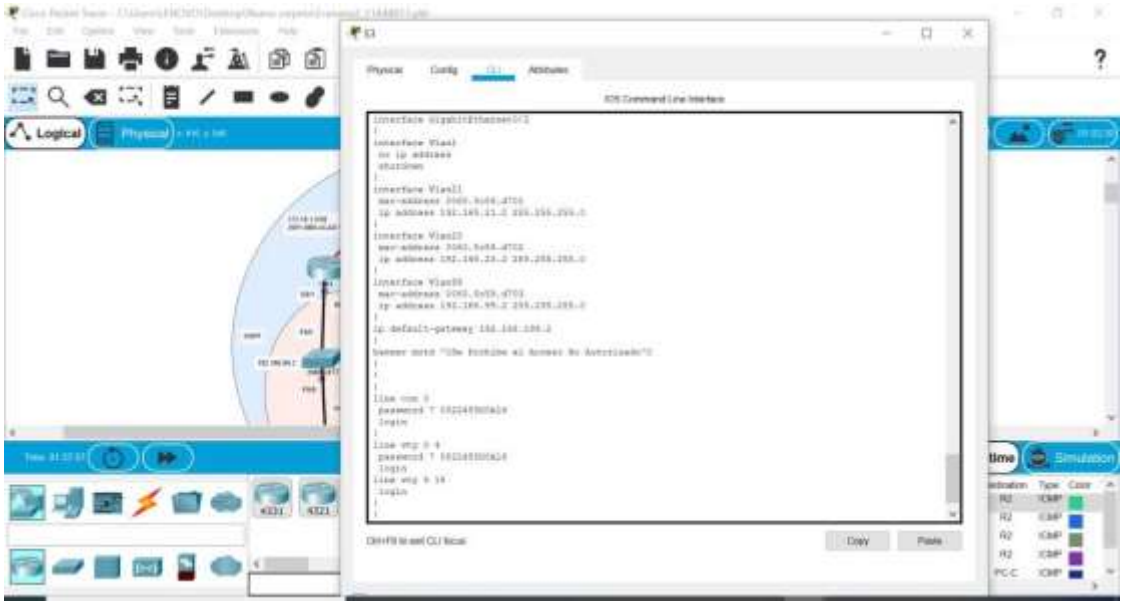
La configuración del S3 incluye las siguientes tareas:

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 $Se prohíbe el acceso no autorizado$

Comandos para la Configuración de S3 en la topología desarrollada.

figura 20: configuración S3



Fuente: Autor

se configura S3 de acurdo al listado de comandos que se indicaron en la tabla número 19.

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.

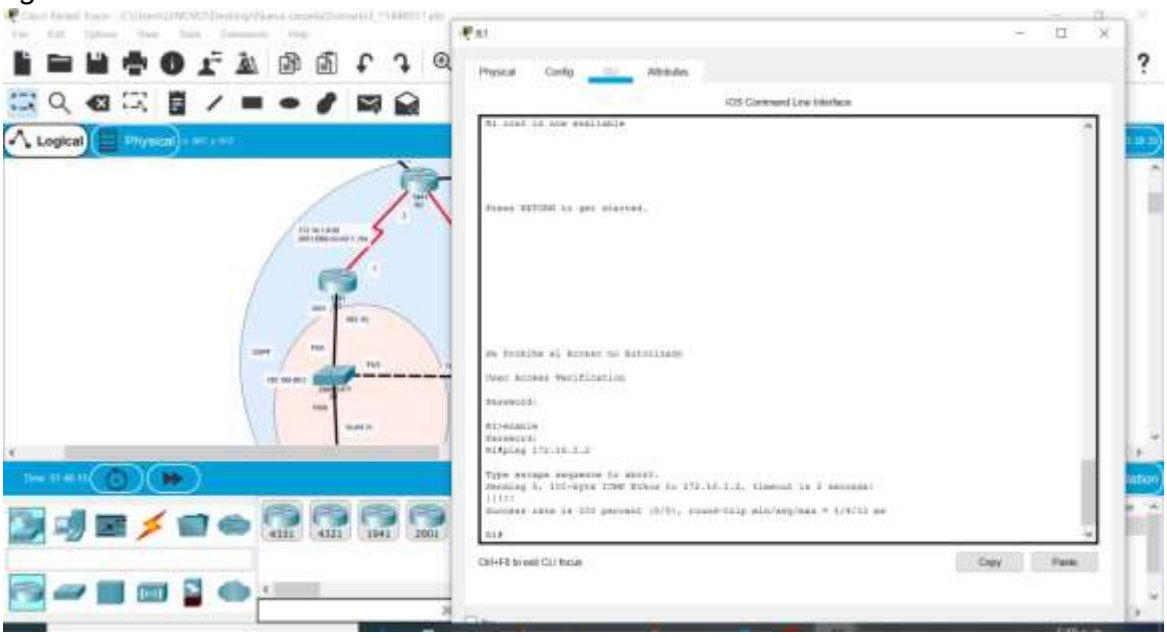
Verificación de la conectividad			
Desde	**A**	**Dirección IP**	**Resultados del ping**
R1	VR2, S0/0/0	172.16.1.2	Conectividad exitosa no presenta mala configuración Success rate is 100 percent(5/5), round-trip min/avg/max = 1/9/38 ms (Ver figura 21)

R2	R3, S0/0/1	172.16.2.1	Conectividad exitosa no presenta mala configuración Success rate is 100 percent(5/5) round-trip min/avg/max = 1/2/8 ms (Ver figura 22)
PC de Internet	Gateway predeterminado	209.165.200.238	Conectividad exitosa no presenta mala configuración Reply from 209.165.200.238: bytes=32 time<1ms TTL=255 (Ver figura 23)

Se realiza los pings y se comprueba la conectividad entre los dispositivos que se configuraron sin tener complicaciones en su configuración.

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

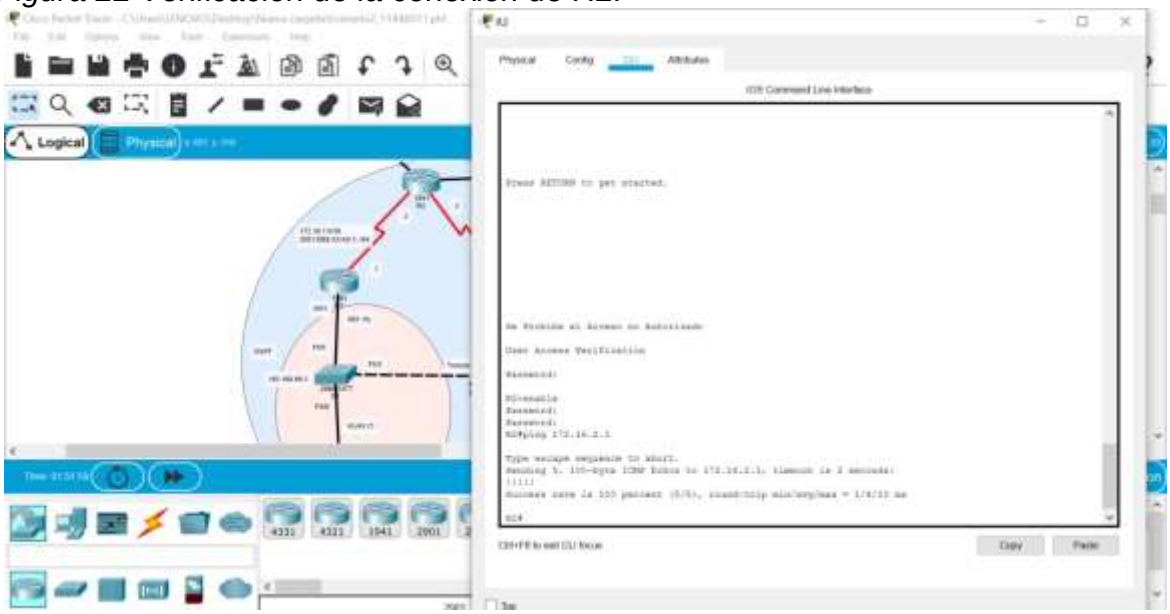
Figura 21: Verificación de la conexión de R1.



Fuente: Autor

se realiza conexión exitosa en R1 R2 y PC de internet.

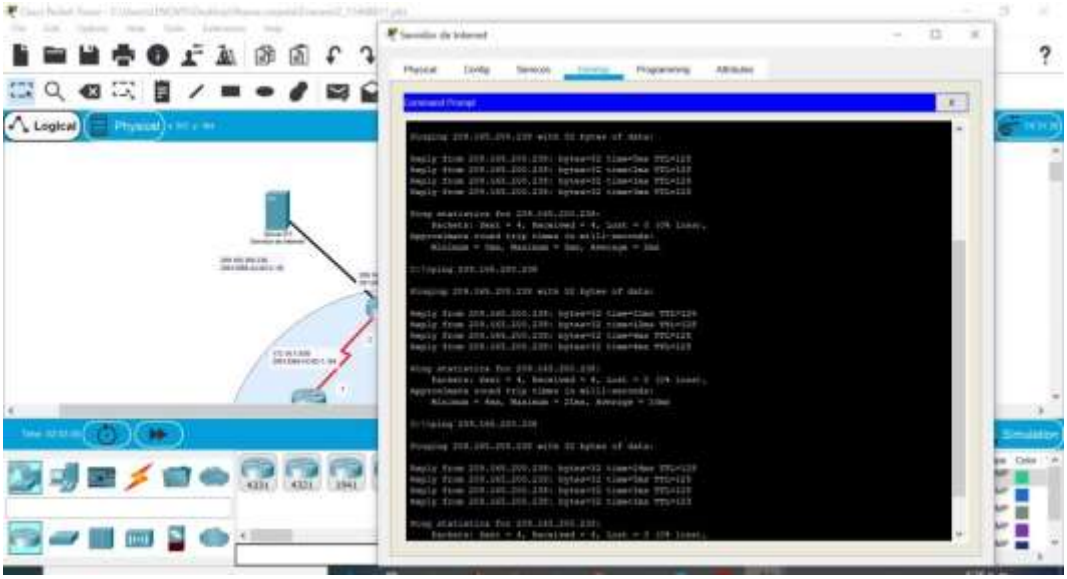
Figura 22 Verificación de la conexión de R2.



Fuente: Autor

conexión de R2 con los diferentes dispositivos.

Figura 23: Verificación de la conexión del servidor de red a su Gateway predeterminado.



Fuente: Autor

verificación exitosa 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:

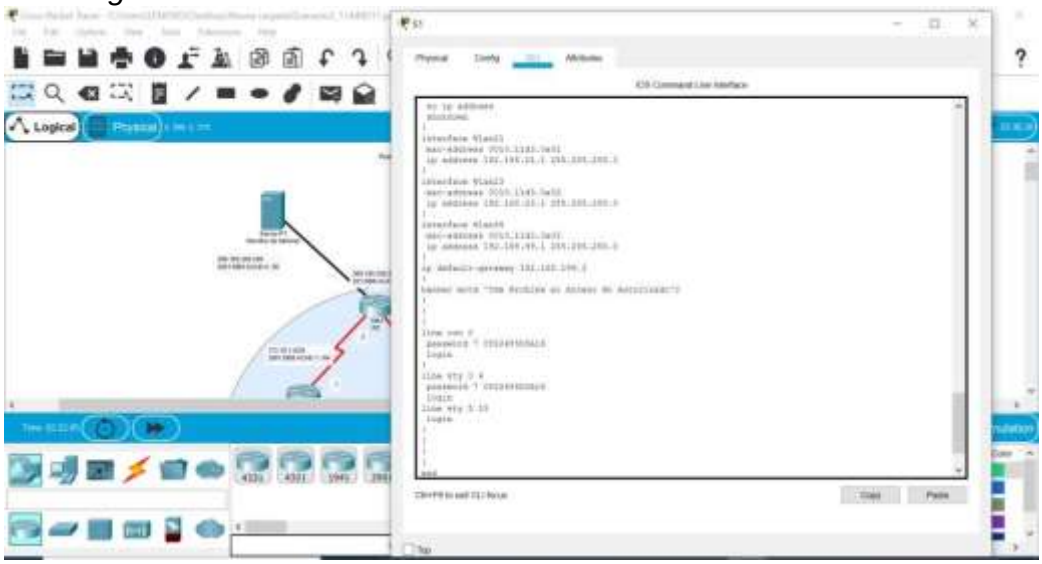
Tabla 21: Configuración de la seguridad del switch y el routing entre las vlan de S1.

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

Tareas para la configuración del S1 manteniendo su conexión.

figura 24: seguridad S1.



Fuente: Autor

se configuro la seguridad de S1 y las vlan respectivas para proteger la información de los equipos.

Paso 2: Configurar el S3.

La configuración del S3 incluye las siguientes tareas:

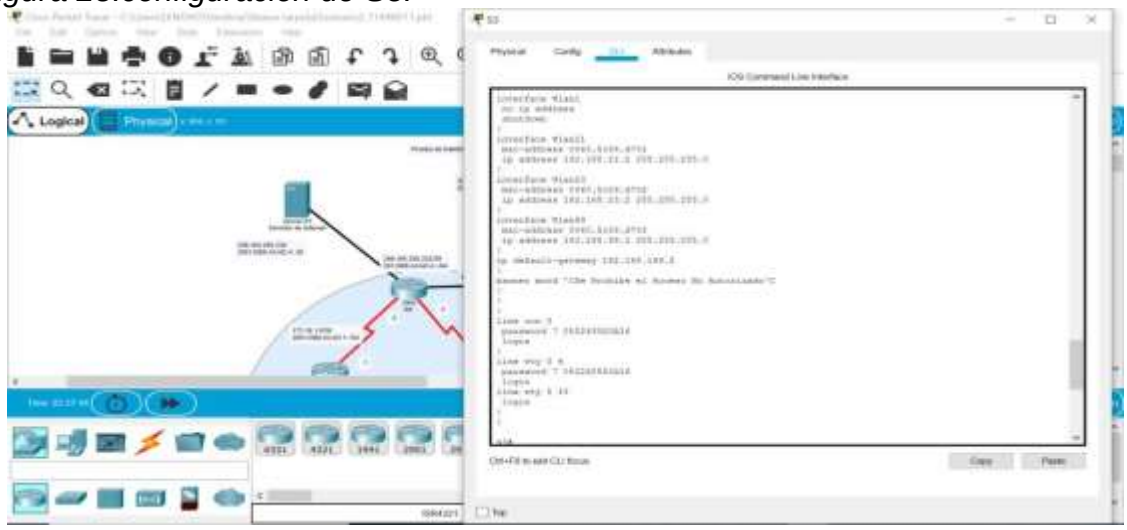
Tabla 22: Configuración de la seguridad del switch y el routing entre las vlan de S3.

Configuración del switch 3	
Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	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 vlan 1

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

Asignación de configuración para S3.

Figura 25:configuración de S3.



Fuente: Autor

se realiza la configuración de seguridad de S3 para garantizar la seguridad de la topología.

Paso 3: Configurar R1

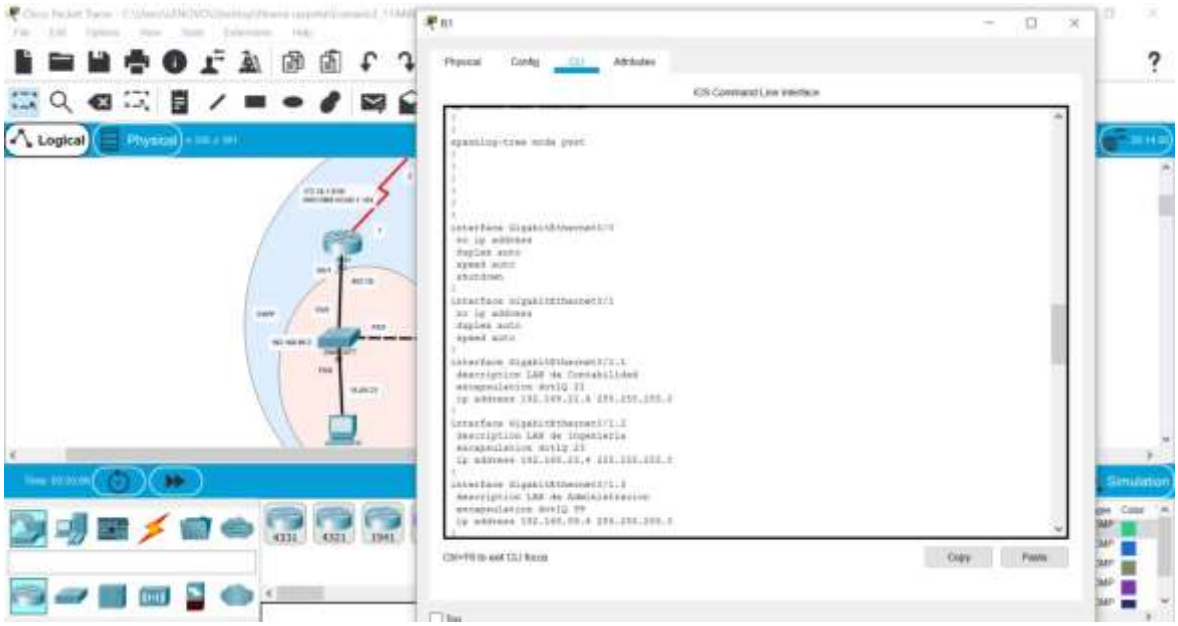
Las tareas de configuración para R1 incluyen las siguientes:

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

Comandos para la configuración de R1 manteniendo la conexión de red.

Figura 26: 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:

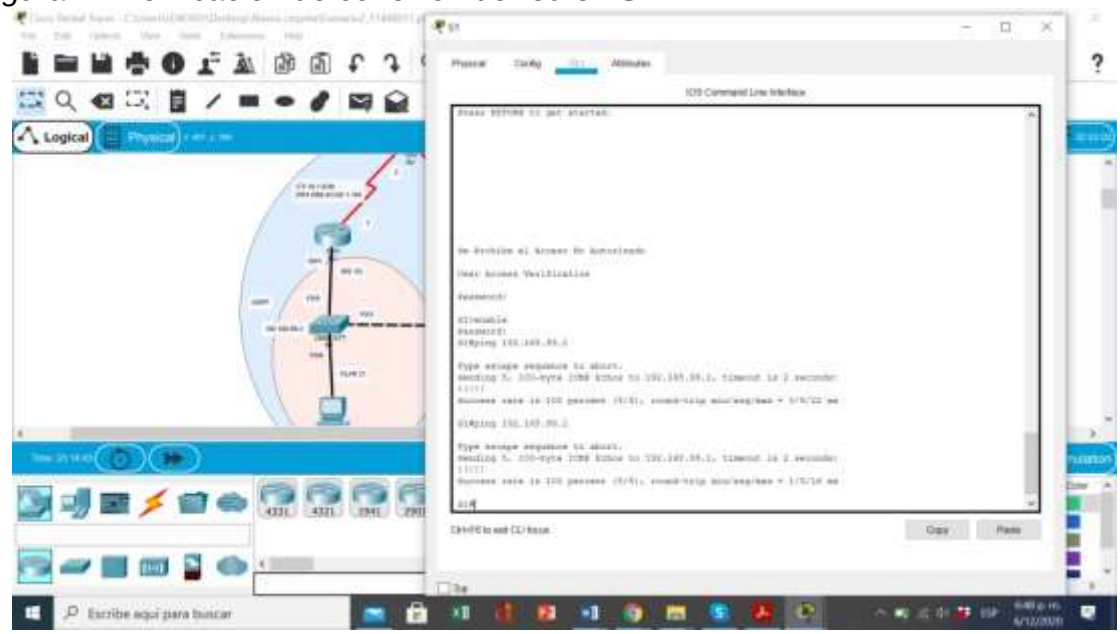
Tabla 24: verificación de la topología.

Verificación de la red			
Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Conexión exitosa en su configuración Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 27)
S3	R1, dirección VLAN 99	192.168.99.1	Conexión exitosa en su configuración Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 28)

S1	R1, dirección VLAN 21	192.168.21.1	Conexión exitosa en su configuración Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 29)
S3	R1, dirección VLAN 23	192.168.23.1	Conexión exitosa en su configuración Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms (Ver figura 30)

Se verifica la conectividad entre S1, S3 y R1 obteniendo los resultados esperados conexión exitosa en los dispositivos.

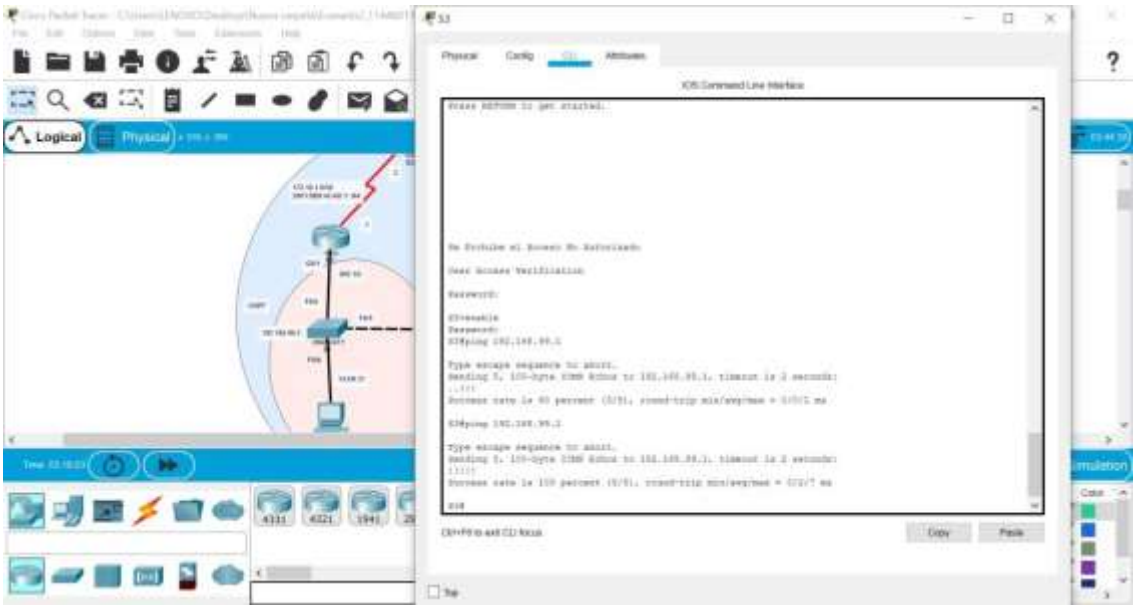
Figura 27 Verificación de conexión de red en S1.



Fuente: Autor.

se realiza ping y se obtiene conectividad exitosa en la red con S1.

Figura 28:verificación de S3.



Fuente: Autor.

se verifica la conexión exitosa de R3 con los diferentes equipos de la topología realizada.

figura 29:verificación S1.

Fuente: Autor.

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

Figura 30: verificación de S3.

Fuente: Autor.

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

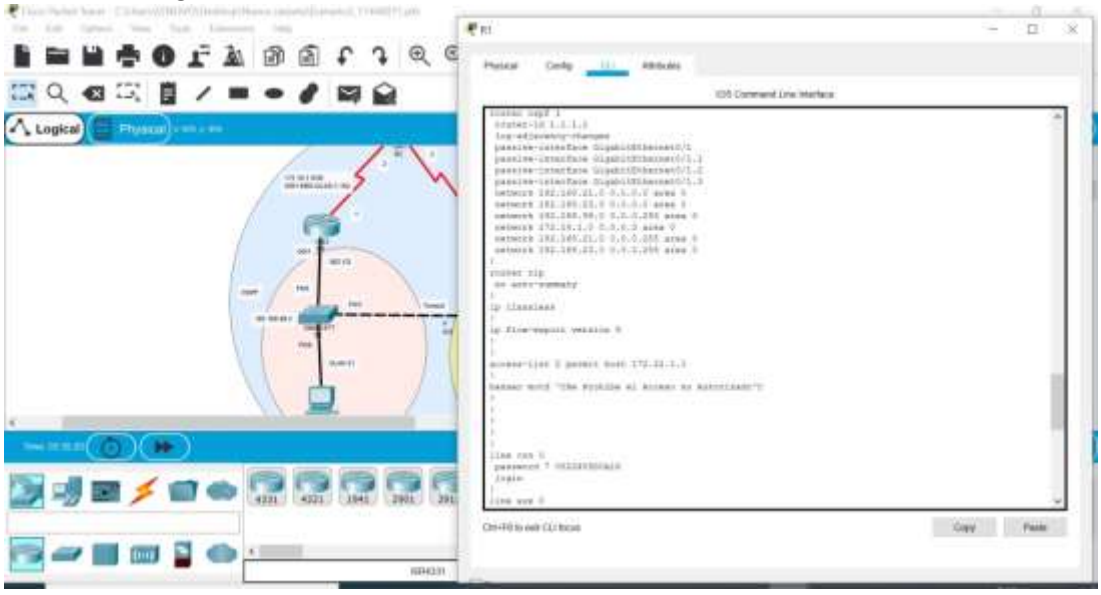
Tabla 25: Configuración OSPF área 0 en R1.

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

Tareas para la Configuración OSPF área 0 en R1 manteniendo su conexión con la topología.

Figura 31:configuración OSPF R1.



Fuente: Autor.

configuración de OSPF completada en el R1 utilizando el comando.

Paso 2: Configurar OSPF en el R2

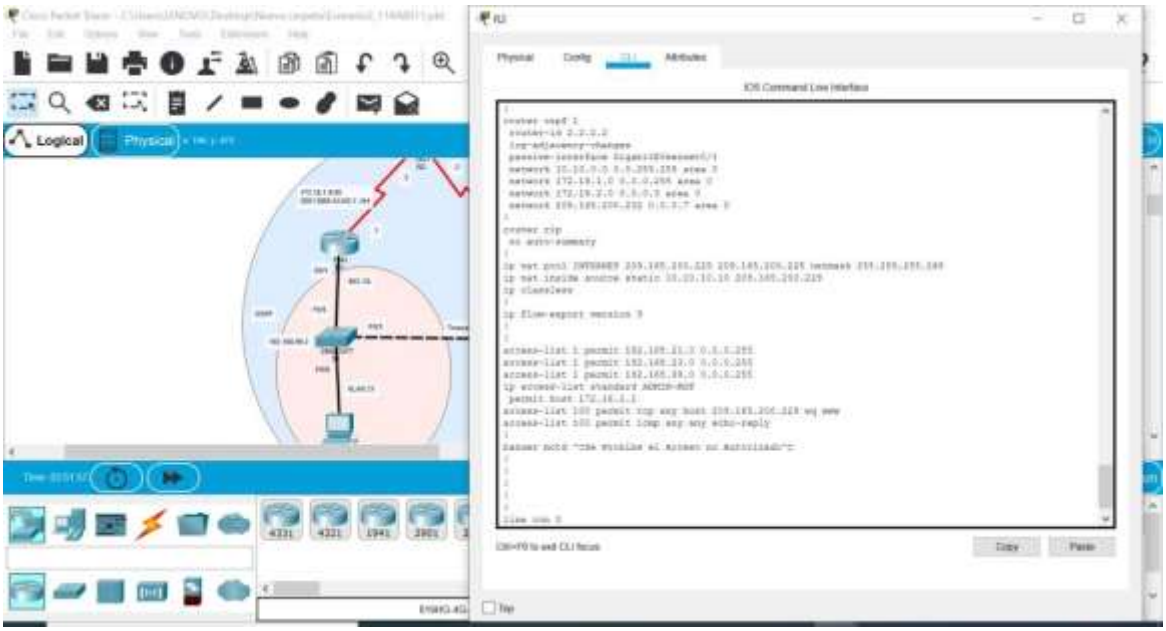
La configuración del R2 incluye las siguientes tareas:

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 de ruta que nos permite conectar directamente a través de la red. R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#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-router)#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 tener su función 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 y sus direcciones. R2(config-router)#no auto-summary

Tareas de configuración OSPF R2 en la topología.

Figura 32:configuración en R2



Fuente: Autor.

configuración en R2 completada mediante el comando 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

Tareas para configurar OSPF en el Router 3 manteniendo conexión.

Figura 33:configuración R3.

Fuente: Autor.

configuración OSPF para el Router 3 utilizando la línea de comandos.

Paso 4: Verificar la información de OSPF

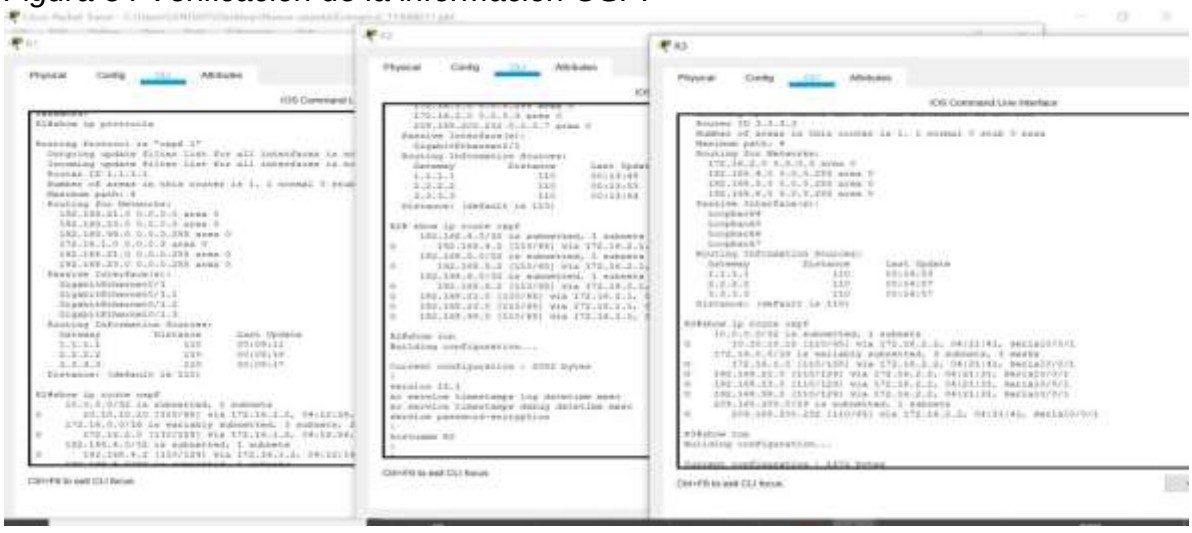
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

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 R2#Show ip protocols R3#Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	El comando show ip route Muestra solo las rutas que se trabajan. R1#Show ip route ospf R2#Show ip route ospf R3#Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Al digirar el comando show run podemos observer la configuración OSPF en su ejecución. R1#Show run R2#Show run R3#Show run

Configuración realizada con OSPF con su conexión exitosa.

Figura 34 Verificación de la información OSPF



Fuente: Autor.

Autor, verificación de OSP exitosa entre R1, R2, 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

Tareas para configurar R1 como servidor de DHCP en la topología desarrollada

figura 35: R1 como servidor DHCP

Fuente: Autor.

se configura 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 bases 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 su línea de comandos.

Figura 36:configurar NAT en R2

Fuente: Autor.

se configura NAT en R2 correctamente para mejorar la seguridad de la red interna.

Paso 3: Verificar el protocolo DHCP y la NAT estática

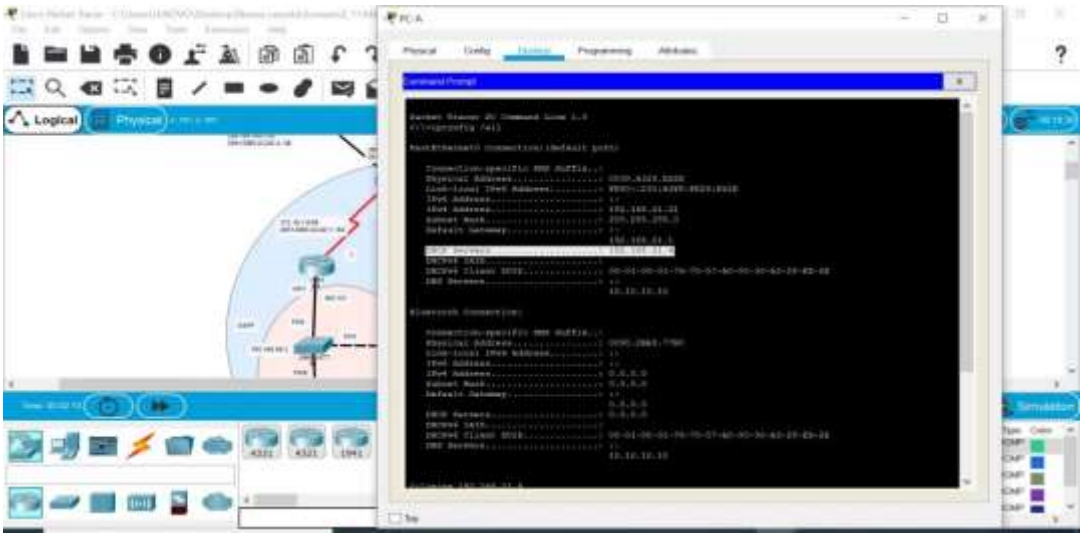
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

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 37)
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 38)
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 39)
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

Configuración de DHCP y NAT exitosa.

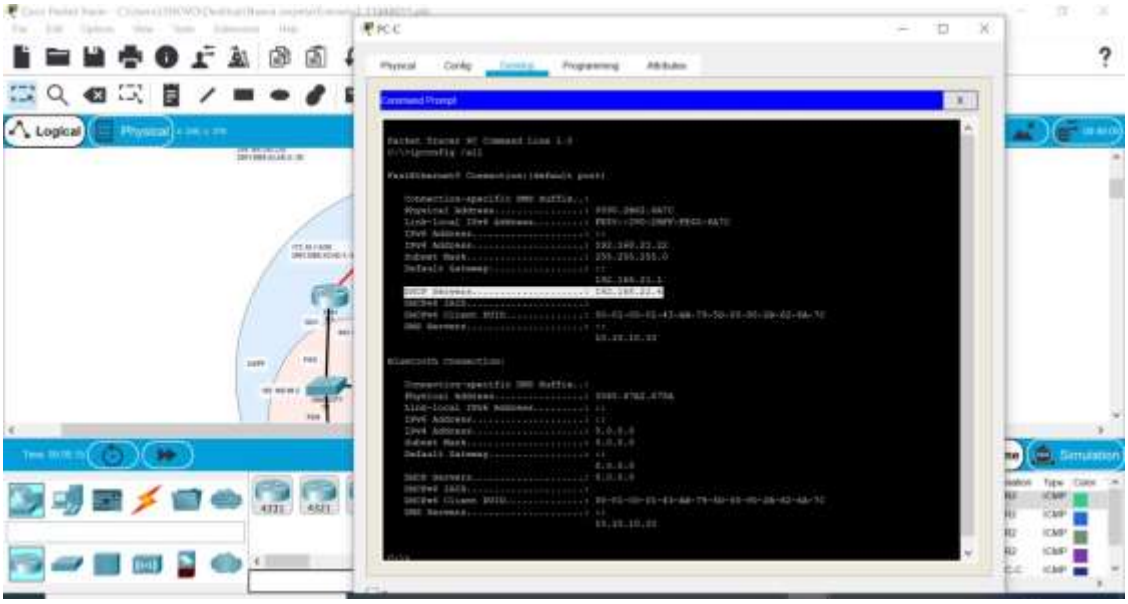
Figura 37:DHCP en PC-A



Fuente: Autor.

dirección DHCP en PC-A configurada correctamente.

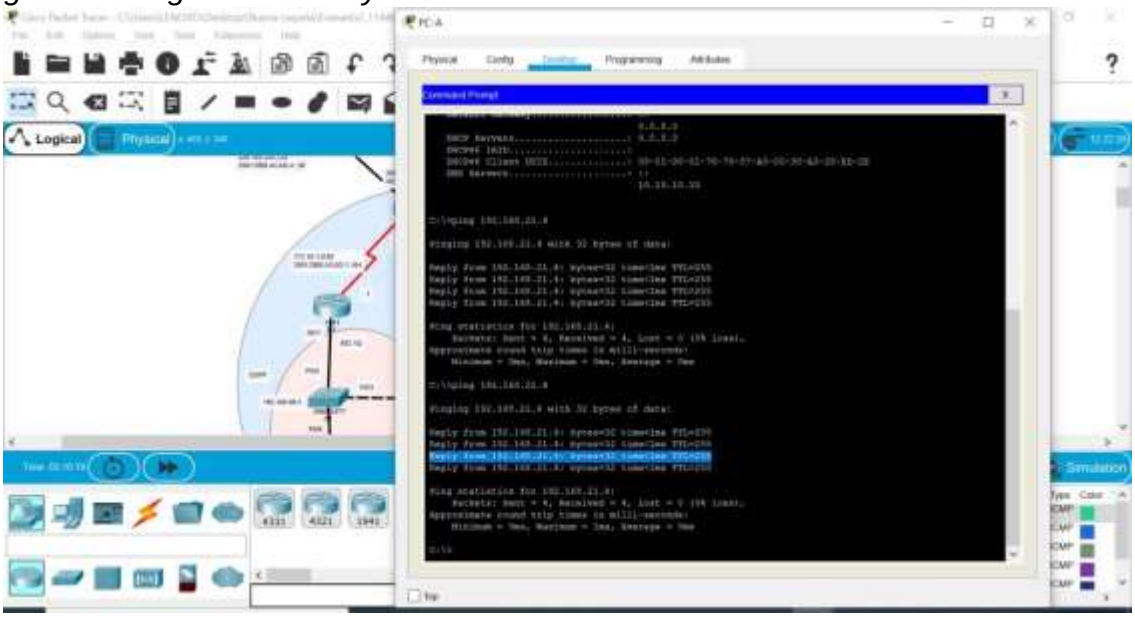
figura 38:DHCP en PC-C



Fuente: Autor.

configuración DHCP esta correcta en PC-C.

Figura 39:Ping entre PC-A y PC-C



Fuente: Autor.

se realiza ping entre PC-A y PC-C sin novedades.

Figura 40: web service.

Fuente: Autor.

conexión de red en el servidor de internet exitoso.

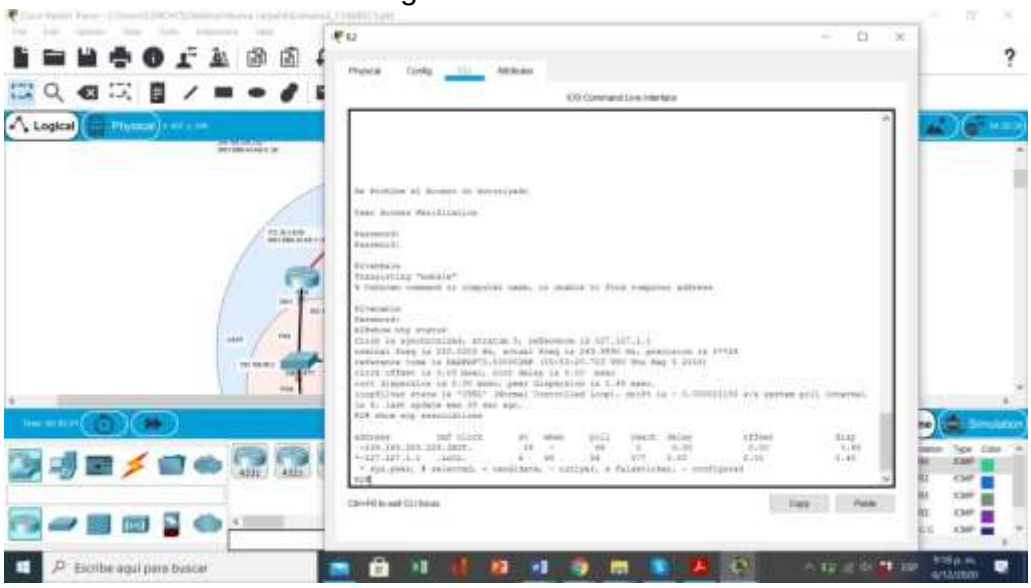
Parte 6: Configurar NTP

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

Tarea de configuración NTP en R1 Y R2

Figura 41: Verificación de la configuración NTP en R1.



Fuente: Autor.

configuración de NTP correcta en R2 para establecer sincronización.

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

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

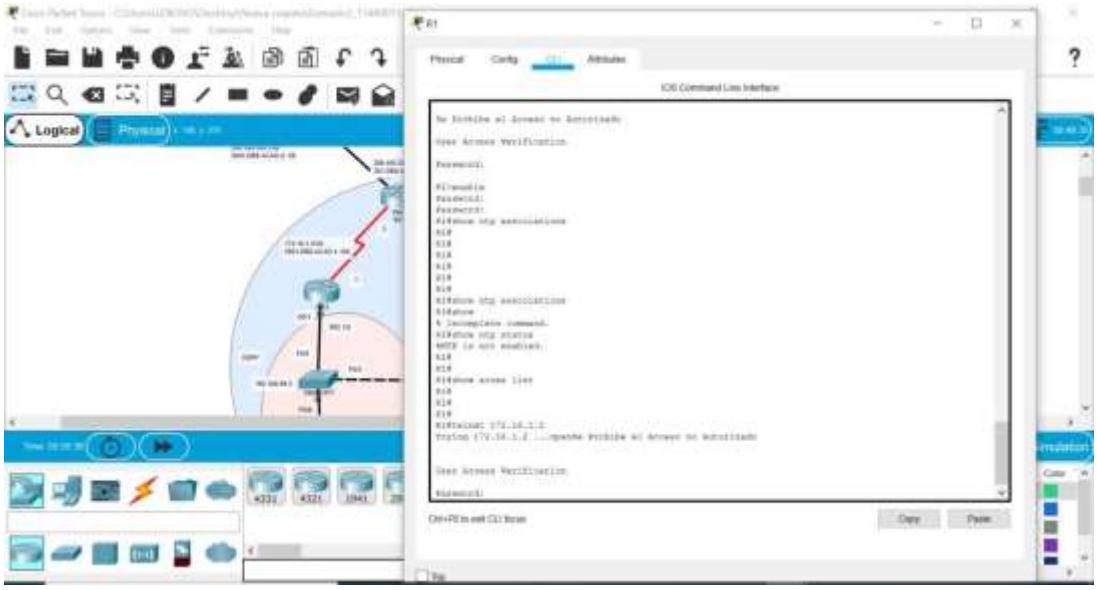
Configuración y verificación de ACL en R2	
Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Se realiza la lista de acceso para conectar telnet entre el Router 1 y el Router 2. R2(config)#ip access-list 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

Tabla 33: Configuración y verificación de las ACL

Pasos para la configuración VTY y telnet con su conexión entre los routers.

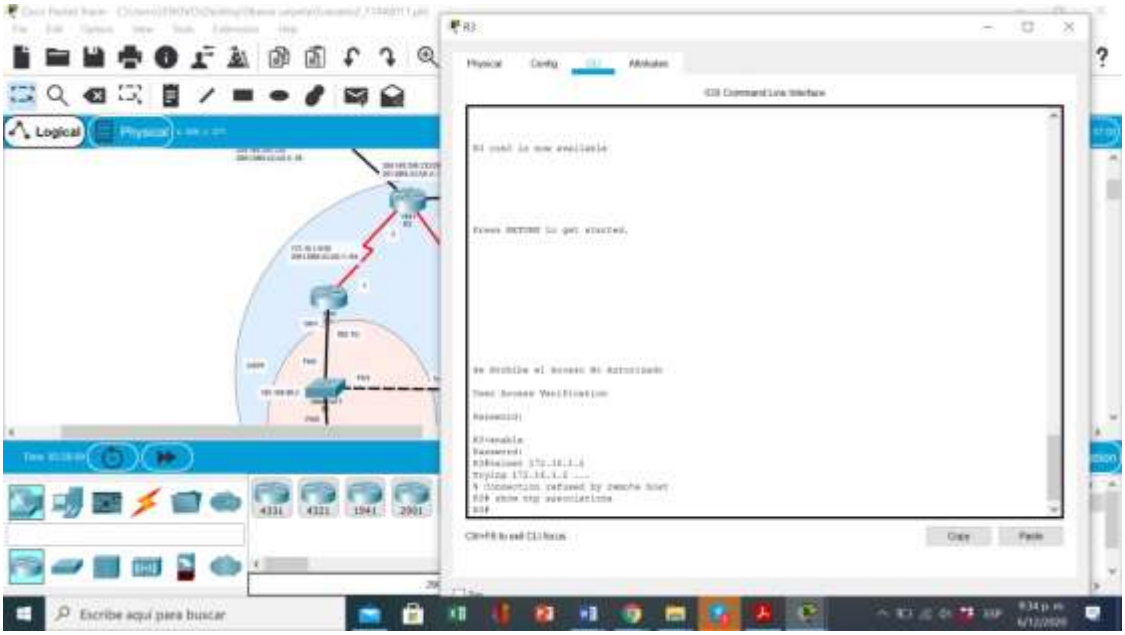
figura 42:funcionamiento VTY



Fuente: Autor.

se crea en R1 la lista de control de acceso ACL con la configuración de telnet utilizando el comando VTY.

Figura 43:realizar telnet en R3



Fuente: Autor.

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. #show ip access list
Restablecer los contadores de una lista de acceso	Con el comando clear ip borramos los contadores. #clear ip
¿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

Los comandos se realizaron acorde a la actividad.

CONCLUSIONES

- En el escenario 2 al verificar los equipos se puede detallar un direccionamiento entre los R1, R2 y R3, mediante la configuración previa utilizando un direccionamiento OSPF.

- En el desarrollo de los diferentes escenarios se ha aplicado el conocimiento adquirido en el curso de profundización del CCNA

- 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.

- 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.

REFERENCIAS

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

LUCAS, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

ODOM, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

SONIA, M., n.d. 7.2.5.4 Configuración De Direcciones Ipv6 En Dispositivos De Red - CCNA CISCO Sitio Wiki De Maria Sonia. [online] Sites.google.com. Recuperado de: https://sites.google.com/site/redesintroduccion/7-2-5-4-configuracion-de-direcciones-ipv6-en-dispositivos-de-red

SUÁREZ, M., 2019. Seguridad En El Switch: Puertos Y Acceso - CCNA Desde Cero. [online] CCNA Desde Cero. Recuperado de: https://ccnadesdecero.com/curso/seguridad-switch-puertos-acceso/

W0LF_F4NG, 2020. Configuración Básica Ipv6 Router Cisco. [online] WF-Networking. Recuperado de: https://www.w0lff4ng.org/configuracion-basica-ipv6-router-cisco/

WALTON, A., 2017. Configuración De NAT Dinámica. [online] ccnadesdecero.es. Recuperado de: https://ccnadesdecero.es/configuracion-nat-dinamica/

WILLEMVWYK, 2007. Err-Disabled On Fastethernet Port. [online] Community.cisco.com. Recuperado de: https://community.cisco.com/t5/switching/err-disabled-on-fastethernet-port/td-p/716827

ANEXOS

Enlace de descarga de archivo de simulación del escenario 1:
https://1drv.ms/u/s!Am8K_vEvL9LKgRW_TGKSlp-6Xb6a?e=u0yA2n

ANEXO 2

Enlace de descarga de archivo de simulación del escenario 2:
https://1drv.ms/u/s!Am8K_vEvL9LKgRbOuPycubT8kP_7?e=99QNcm

ANEXO 3

Enlace de descarga del artículo científico alojado en Google drive:

https://1drv.ms/u/s!Am8K_vEvL9LKgRkGTzRcooB_KQuX?e=28oMlA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN7

John Freddy Mina Montenegro

Universidad Nacional Abierta y a Distancia UNAD

jfmm1028@outlook.es

Resumen

"La principal característica de un protocolo de enrutamientos es que esta permite compartir información entre los diversos ROUTERS de manera remota y actualizar de manera dinámica la información de enrutamiento a sus propias tablas y compartirlas entre sí.

La ventaja más significativa de los Routers con protocolo dinámico es que este permite hacer un informe en el cambio de la topología (RUTAS) entre los distintos routers de la red y estos a su vez aprenden automáticamente las nuevas redes, así como las bajas de las mismas.

Podemos decir que uno de los primeros protocolos utilizados formalmente es el RIP en su versión, aunque muchos de los algoritmos usados en el son productos directos del abuelo ARPANET. Aun cuando el RIP ha evolucionado a su versión 2, este aun presenta algunos problemas de escalamiento, dejándolo atrás cuando se requiere de redes grandes, una mejor opción es usar versiones de protocolos más avanzados tales como el IGRP y el EIGRP, ambos productos de CISCO

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

Abstract:

"We can say that one of the first protocols used formally is the RIP in its version, although many of the algorithms used in it are direct products of the grandfather ARPANET. Even though the RIP has evolved to version 2, it still presents some scaling problems, leaving it behind when large networks are required, a better option is to use more advanced protocol versions such as IGRP and EIGRP, both CISCO products.

Keywords— *CISCO, CCNP, Routing, Swicthing, Networking, Electronics.*

I. Introducción

"Las redes modernas continúan evolucionando para adaptarse a la manera cambiante en que las organizaciones realizan sus actividades diarias. Ahora los usuarios esperan tener acceso instantáneo a los recursos de una compañía, en cualquier momento y en cualquier lugar. Estos recursos incluyen no solo datos tradicionales, sino también de video y de voz. También hay una necesidad creciente de tecnologías de colaboración que permitan el intercambio de recursos en tiempo real entre varias personas en sitios remotos como si estuvieran en la misma ubicación física. "

"Los distintos dispositivos deben trabajar en conjunto sin inconvenientes para proporcionar una conexión rápida, segura y confiable entre los hosts. Los switches LAN proporcionan el punto de conexión a la red empresarial para los usuarios finales y también son los principales responsables del control de la información dentro del entorno

LAN. Los routers facilitan la transmisión de información entre redes LAN y, en general, desconocen a los hosts individuales. Todos los servicios avanzados dependen de la disponibilidad de una infraestructura sólida de routing y switching sobre la que se puedan basar. Esta infraestructura se debe diseñar, implementar y administrar cuidadosamente para proporcionar una plataforma estable necesaria."

II. DESARROLLO.

ESCENARIO 1.

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."

Ilustración 1-Ecenario 1

En la siguiente tabla se presenta de manera ordenada la debida asignación de direcciones donde se puede detallas el dispositivo o interfa la dirección IP o prefijo y lapuerta de enlace predeterminada

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
	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
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
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
	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

Tabla 1 Tabla de asignación de direcciones.

En el ejercicio se puede evidenciar que no hay ninguna interfaz en el router que admita VLAN 5.

Instrucciones para inicializar y recargar y configurar aspectos básicos de los dispositivos.

Inicializar y volver a cargar el router y el switch

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos.

PC_A

Router>enable

Router#erase startup-config

En la siguiente ilustración se puede observar los datos de la instalación de equipos

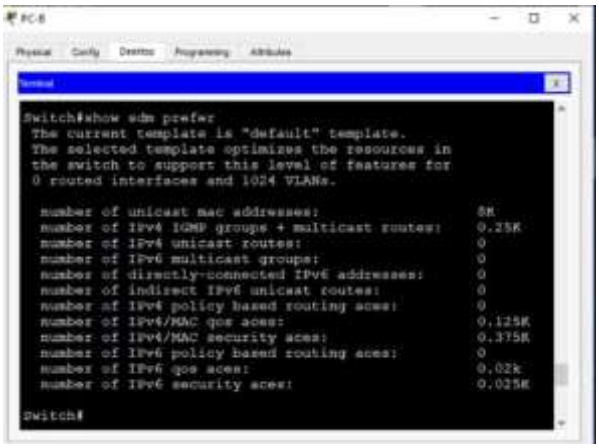


Ilustración 2 PC-B

A continuación, se presentan las partes con sus respectivos pasos para la configuración de cada uno de los

Parte 1 configuración.

Paso 1 Configuración de R1.

Para esta configuración se deben cumplir una serie de tareas con sus respectivas especificaciones algunas de estas son: desactivar la búsqueda DNS, nombre del router, nombre de dominio, contraseña cifrada para el modo EXEC privilegiado, las cuales, Contraseña de acceso a la consola, Establecer la longitud mínima para las contraseñas, crear un usuario administrativo en la base de datos local, configurar el inicio de sesión en las líneas VTY para que use la base de datos local configurar VTY solo aceptando SSH entro otras. Las culés permiten una configuración correcta de la última tarea para finiquitar la configuración es la generación de una clave de cifrado RSA y como modo de ejemplo para las anteriores tareas que no se describe la especificación, a continuación, presente la de esta ultima tarea de configuración.

Especificación:

Módulo de 1024 bits

R1(config)#crypto key generate RSA

The name for the keys will be: R1.ccna-lab.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

- Configurar IPv4 DHCP para VLAN 2

Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Paso 2: Configurar los servidores.

PC-A Network Configuration	
Descripción	*DHCP resquest successful.*
Dirección física	*en 10.19.8.1*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Tabla 3 PC-A

Configuración de red de PC-A	
Descripción	*Connection-specific DNS Suffix*
Dirección física	*10.19.8.1*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::202:17FF : FE52:806B*

Tabla 4 Red-PC-A.

Tabla 35: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
Configuración de sdm	S1>enable S1#config t S1(config)#sdm prefer dual-ipv4-and-ipv6 default

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.

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:

Se realiza la lista de comandos para R1 con su conexión a red.

En esta 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 44:configuración R1

Figura: Autor

se configura R1 con las características descritas para el uso del router 1.

Bibliografía

Mi nombre es John Fredy Mina tengo 37 años actualmente vivo en la ciudad de Santiago de Cali Me considero una persona responsable, creativa, con iniciativa y responsabilidad, asumo con agrado los retos y metas en cualquier organización que me pudiera plantear; con buen manejo de relaciones interpersonales, facilidad para trabajar en equipo, en condiciones de alta presión, así como para resolver problemas eficientemente y lograr las metas trazadas por parte de la empresa y mi grupo de trabajo.

III. Referencias

[1] CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

[2] CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

[3] LUCAS, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

[4] ODOM, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf