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

UBER ALEJANDRO ARAGON VIAFARA

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

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

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

DIPLOMADO DE PROFUNDIZACION CISCO

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

UBER ALEJANDRO ARAGON VIAFARA

DIRECTOR:
DIEGO EDINSON RAMIREZ CLAROS

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma de Jurado

Firma de Jurado

Cali, 30 de noviembre de 2020

AGRADECIMIENTOS

Un agradecimiento especial a la universidad abierta y a distancia (Unad) que, por medio de sus distintos tutores y compañeros, me permiten aprender cada día y poder desarrollar mis habilidades como ingeniero de sistemas

A mis padres y familiares que siempre me apoyan en los momentos más importantes de mi vida, regalándome un buen consejo y guiándome siempre por el bien camino.

CONTENIDO

AGRADECIMIENTOS 4
LISTA DE TABLAS 6
LISTA DE FIGURAS 7
GLOSARIO 8
RESUMEN 9
ABSTRACT 9
INTRODUCCIÓN 10
DESARROLLO 11
1. ESCENARIO 1 11
2. ESCENARIO 2 36
CONCLUSIONES 70
BIBLIOGRÁFIA 71
ANEXOS 72

LISTA DE TABLAS

Tabla 1. Tabla de VLAN 11
Tabla 2. Tabla de asignación de direccionamiento 12
Tabla 3. Tabla de Reinicio de dispositivos 12
Tabla 4. Tabla de configuración R1 13
Tabla 5. Tabla de configuración básica S1/S2 17
Tabla 6. Tabla de configuración Vlan S1 20
Tabla 7. Tabla de configuración Vlan S1 23
Tabla 8. Tabla de configuración Avanzada R1 27
Tabla 9. Tabla de configuración PC-A 29
Tabla 10. Tabla de configuración PC-B 31
Tabla 11. Tabla de conectividad de Red 32
Tabla 12. Tabla de comandos IOS 37
Tabla 13. Tabla de configuración del servidor 37
Tabla 14. Tabla de configuración R1 38
Tabla 15. Tabla de configuración del R2 40
Tabla 16. Tabla de configuración del R3 42
Tabla 17. Tabla de configuración del S1 45
Tabla 18. Tabla de configuración del S3 46
Tabla 19. Pruebas de ping – R1,R2,R3 47
Tabla 20. Configuración Vlans – S1 48
Tabla 21. Configuración Vlans – S3 51
Tabla 22. Configuración subinterfaz – G0/1 53
Tabla 23. Prueba de conectividad – S1,S2,S3,Vlans 53
Tabla 24. Configurar OSPF en el R1 55
Tabla 25. Configurar OSPF en el R2 57
Tabla 26. Configurar OSPF en el R3 58
Tabla 27. Verificación de información OSPF – R1,R2,R3 60
Tabla 28. Configuración de servidor de DHCP 61
Tabla 29. Configuración de NAT estática y dinámica en el R2 63
Tabla 30. Verificar el protocolo DHCP y la NAT estática -PCs 65
Tabla 31. Configuración de NTP 66
Tabla 32. Configuración de ACL 67
Tabla 33. Verificación de ACL 68

LISTA DE FIGURAS

Figura 1. Escenario 1 11
Figura 2. Show running-config R1 16
Figura 3. Show running-config R1 16
Figura 4. Show int vlan S1 19
Figura 5. Show vlan brief 22
Figura 6. Show ip int brief 22
Figura 7. Show vlan brief 26
Figura 8. Show port-security 26
Figura 9. Configuración PC-A 28
Figura 10. Observación Shell PC-A 29
Figura 11. Configuración PC-B 30
Figura 12. Observación Shell PC-B 31
Figura 13. Configuración final Red 32
Figura 14. Ping de R1 a PC-A 33
Figura 15. Ping de R1 a PC-B 34
Figura 16. Ping de PC-B a Lo0 34
Figura 17. Ping de PC-A a PC-B 35
Figura 18. Show ip route en R1 35
Figura 19. Escenario 2 36
Figura 20. Show ip route R1 39
Figura 21. Show ip route R2 42
Figura 22. Show ip route R3 44
Figura 23. Show running-config 45
Figura 24. Ping R1 – R2 47
Figura 25. Ping R2 – R3 47
Figura 26. Ping PC de Internet – Gateway predeterminado 48
Figura 27. Show vlan brief 50
Figura 28. Show ip int brief 50
Figura 29. Show running-config 51
Figura 30. Ping S1 – R1 Vlan 99 54
Figura 31. Ping S3 – R1 Vlan 99 54
Figura 32. Ping S1 – R1 Vlan 21 54
Figura 33. Ping S3 – R1 Vlan 23 55
Figura 34. Show ip protocols 56
Figura 35. Show ip protocols 58
Figura 36. Show ip protocols 59
Figura 37. Show ip route ospf – R2 60
Figura 38. Show run | section ospf – R2 60
Figura 39. Show running-config 62
Figura 40. Show Access-lists 64
Figura 41. Show ip nat translations 64
Figura 42. Show Access-lists 68

GLOSARIO

DIRECCIÓN IP: es un direccionamiento utilizado para identificar un dispositivo en la red.

DHCP: (Protocolo de configuración dinámica de host) de tipo cliente/servidor en el que un servidor cuenta con un listado de direcciones IP dinámicas y las asigna a los clientes en el momento en el que se encuentran disponibles.

PING: comando utilizado para realizar un diagnóstico de estado de comunicación entre dos o más equipos en el cual se puede determinar la velocidad, calidad y estado de red.

PUERTO: Es una interfaz a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

ROUTER: El router es el dispositivo que se encarga de reenviar los paquetes entre distintas redes

SWITCHS: los switchs crean una especie de canal de comunicación exclusiva entre el origen y el destino. Así la red no queda "limitada" a un solo equipo en el envío de información, a diferencia del hub.

VLAN: Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física

RESUMEN

El objetivo principal de esta actividad, practicar lo aprendido a lo largo del diplomado profundización cisco, con los distintos ejercicios realizados en las fases anteriores, temas muy importantes como el enrutamiento (estático y dinámico), configuración DHCP, creación de Vlan, Direccionamiento IP Dinámico y ACL, NAT, PAT y Gestión de equipos de Networking.

Se configuraron 2 escenarios distintos que nos permitieron entender mucho mejor los conceptos mencionados anteriormente, aplicando configuraciones que aplican cada uno de los temas.

Con ayuda de nuestra tabla de enrutamiento establecida previamente, se configuro correctamente toda nuestra red.

Adicionalmente se implementó una seguridad en los distintos dispositivos que conforman la red, tales como contraseñas para poder acceder a estos, apagar los puertos inactivos, creación de distintas Vlan e implementación de ipv4 – ipv6

PALABRAS CLAVES: ENCAPSULACIÓN; ENRUTAMIENTO; ETHERCHANNEL; IPV6; NAT; NTP; OSPF; TRONCAL.

ABSTRACT

The main objective of this activity, to practice what was learned throughout the Cisco deepening diploma, with the different exercises carried out in the previous phases, very important topics such as routing (static and dynamic), DHCP configuration, Vlan creation, Dynamic IP Addressing and ACL, NAT, PAT and Networking Equipment Management.

Two different scenarios were configured that allowed us to understand the concepts mentioned above much better, applying configurations that apply each of the themes.

With the help of our routing table previously, our entire network was correctly configured.

In addition, security was implemented in the different devices that make up the network, such as passwords to access them, turn off the inactive ports, create different Vlan and implement ipv4 - ipv6

KEY WORDS: ENCAPSULATION; ETHERCHANNEL; IPV6; NAT; NTP; OSPF; ROUTING; TRUNK.

INTRODUCCIÓN

En esta primera parte de la actividad trabajaremos el escenario 1 con una topología básica que nos permitirá aplicar mucho de los conocimientos básicos adquiridos en este diplomado a través de los ejercicios de **packet tracer** que solicita la guía de actividades.

Por medio de nuestra tabla de enrutamiento que nos servirá como guía para hacer correctamente la configuración de la red solicitada, creando todas las configuraciones básicas de una red, como son su seguridad y puntos de accesos requeridos, creación de Vlan, entre otros.

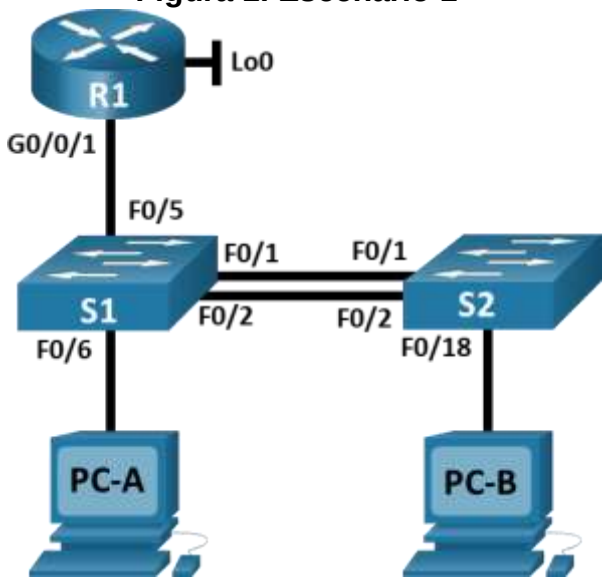
Luego tendremos un segundo escenario que trabajaremos mucho de los temas mencionados en el escenario 1 y adicionalmente temas nuevos como Direccionamiento IP Dinámico y ACL (*Listas de Control de Acceso*), NAT, PAT y Gestión de equipos de Networking

Finalmente, este ejercicio nos servirá como practica y preparación como profesionales en la materia para poderlo implantarlo en campo y la vida laboral.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1



Fuente: UNAD

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. Tabla de VLAN

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

Tabla 2. Tabla de asignación de direccionamiento

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	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
	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
	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
	2001:db8:acad:c: :99 /64	No corresponde
	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
	2001:db8:acad:b: :50 /64	fe80::1

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

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

Lo primero que debemos realizar es borrar toda la configuración anterior que puedan tener nuestros dispositivos, primero que todo procedemos con el borrado de VLAN, luego procedemos con configuración del sdm para poder permitir que nuestro dispositivo funcione con IPV4 – IPV6, finalmente reiniciamos los dispositivos para que se puedan aplicar los cambios realizados en el Router y el Switch.

Tabla 3. Tabla de Reinicio de dispositivos

Función	Comando
Borrado de configuraciones de inicio y las VLAN	Router#erase startup-config Router#delete vlan.dt ***(lo borra en caso que exista el archivo*)** Router#reload

Función	Comando
Configuracion de sdm	S1>enable S1#config t S1(config)#sdm prefer dual-ipv4-and-ipv6 default
Recarga del switch	S1(config)#end S1#reload

Paso 2: Configurar R1

En esta primera configuración del Router implementaremos configuraciones básicas como son la desactivación de la búsqueda DNS, esto con el fin de que cuando escribimos algo que no sea un comando por error el Router no asuma que hemos escrito un nombre de dominio y tarde tratando de resolverlo en una búsqueda DNS, se le asignara un nombre al dispositivo para poderlo identificar más fácil en la red, crearemos un nombre de dominio, implementaremos la seguridad en cada uno de los modos de accesos al dispositivo, configurando contraseñas a cada uno de estos modos, estableceremos una longitud máxima de caracteres en cada una de las contraseñas, implementaremos un mensaje de Advertencia para los intrusos que intenten ingresar de manera fraudulenta y finalmente implementaremos el routing Ipv4 ya que el Ipv4 esta por defecto, esto permitirá que el Router permita trabajar ambos tipos de direccionamiento.

Luego de realizar estas configuraciones básicas de seguridad le asignaremos las direcciones Ip a cada una de las subinterfaces tal como lo indica nuestra tabla de direccionamiento, con el objetivo que el router pueda mantener el tráfico separado de cada una de las Vlan configuradas en la red ya que cada una debe funcionar de manera independiente para un mejor flujo y seguridad de esta.

Se configurará la Loopback que es una interfaz lógica interna del Router el cual también le podemos asignar una dirección Ip tal como una interfaz física y su función principal es servirnos como simulador de punto de red, para la realización de las distintas pruebas de conectividad debido a que estas interfaces nunca se caen y finalmente se deben encriptar todo el tráfico de la red a través de SSH, esto se logra a través de la creación de una llave secreta que se utiliza para encriptar y descifrar datos (**RSA**).

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. Tabla de configuración R1

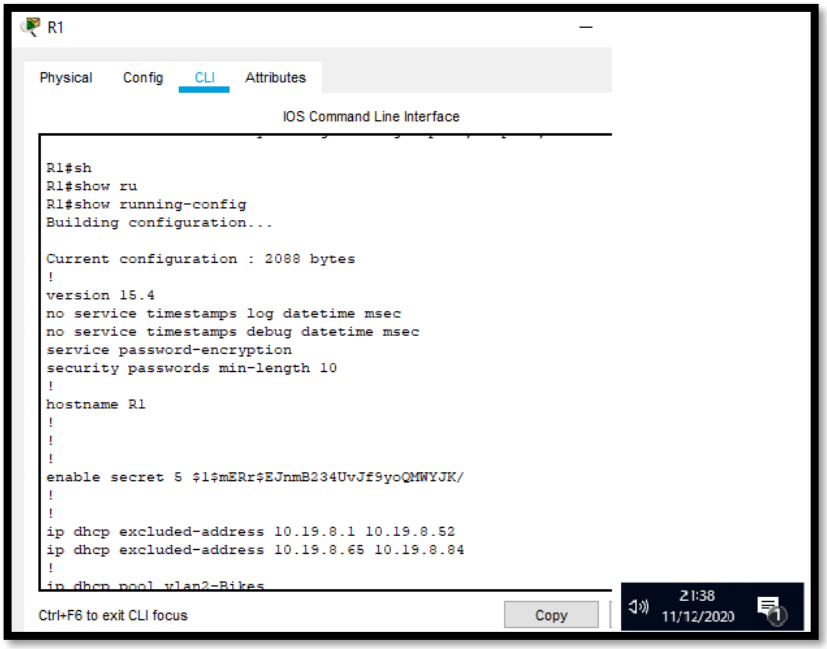
Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1

Tarea	Especificación
Nombre de dominio	R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass R1(config)#exit
Contraseña de acceso a la consola	R1(config)# line console 0 R1(config-line)#password ciscoconpass R1(config-line)# login R1(config-line)# exit R1(config)# exit
Establecer la longitud mínima para las contraseñas (10 caracteres)	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local **Nombre de usuario:** admin **Password:** admin1pass	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	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Solo personal autorizado#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#int g0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#no shutdown R1(config)#int g0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#no shutdown R1(config)#int g0/0/1.4 R1(config-subif)#encapsulation dot1Q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#no shutdown
Configure el Loopback0 interface	R1(config)#int loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
Generar una clave de cifrado RSA **Módulo de 1024 bits**	R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024

Nota: utilizamos el comando **show running-config** para observar las configuraciones realizadas, como la encriptación de las contraseñas, la longitud mínima de los caracteres.

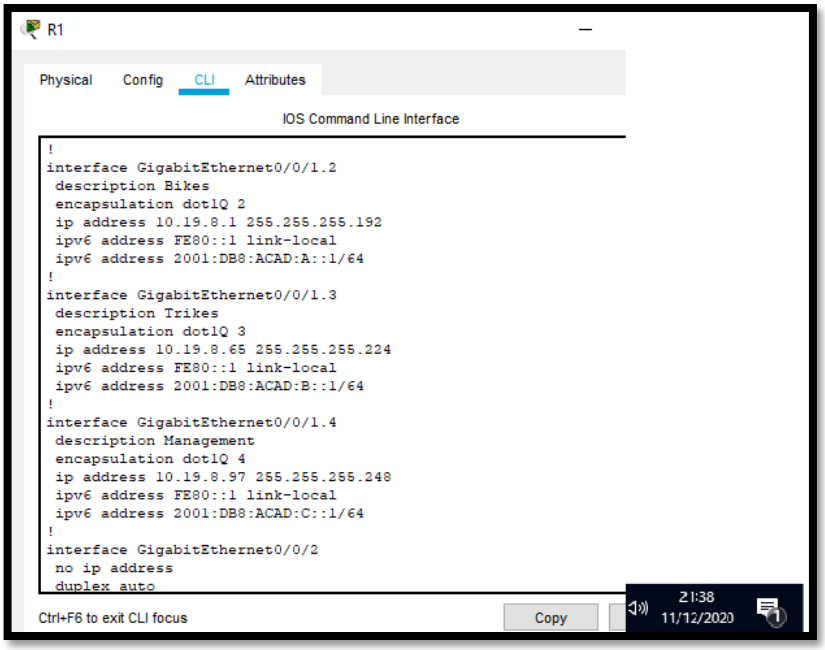
Figura 2. Show running-config R1



Fuente: Autor

Configuraciones de direcciones ip de las subinterfaces según la topología

Figura 3. Show running-config R1



Fuente: Autor

Configuraciones de las direcciones ip de las la sub interfaces realizadas luego de implementar la topología

Paso 3: Configure S1 y S2.

En la configuración de los Switch de utiliza una codificación parecida a la configuración del Router, como son la desactivación de búsqueda DNS, el nombre del dispositivo, la configuración de las contraseñas de acceso, la configuración de conexiones a través de SSH, la encriptación de las contraseñas, la clave de cifrado SSH con RSA.

En esta parte también se deben configurar las direcciones Ip tal como lo indica la tabla de direccionamiento, la creación de las Vlan administrativa para el direccionamiento Ipv4 e Ipv6 y la configuración del Gateway predeterminado.

De acuerdo con la tabla de direccionamiento, se realizará la configuración básica de los switchs.

Las tareas de configuración incluyen lo siguiente:

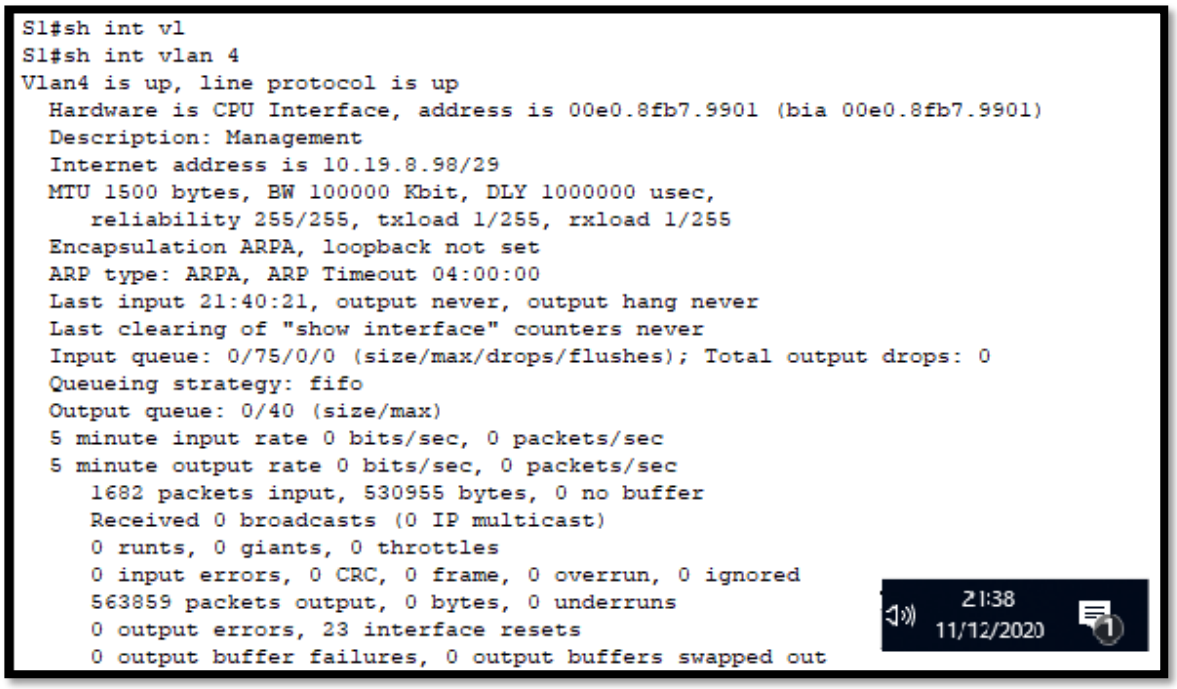
Tabla 5. Tabla de configuración básica S1/S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Nombre de dominio	S1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin** **Password: admin1pass** 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	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh

Tarea	Especificación
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #Solo personal autorizado#
Generar una clave de cifrado RSA	**Módulo de 1024 bits** R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024
Configurar la interfaz de administración (SVI) • Establecer la dirección IPv4 de capa 3 • Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 • Establecer la dirección IPv6 de capa 3	S1(config)#int vlan 4 S1(config-if)#description Management S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S2(config)#int vlan 4 S2(config-if)#description Management S2(config-if)#ip address 10.19.8.99 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::99/64 S1(config-if)#ipv6 address fe80::99 link-local
Configuración del gateway predeterminado	S1(config-if)#exit S1(config)#ip default-gateway 10.19.8.97

Nota: la configuración es similar al router lo único que cambian son las direcciones ip que se requiere para esta parte de la red.

Figura 4. Show int vlan S1



Fuente: Autor

Configuración de la Vlan4 realizada en el S1

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

Paso 4: Configurar S1

En esta parte debemos crear todas la Vlan que se indican en la tabla de direccionamiento, luego de la creación de estas, debemos configurar los enlaces troncales en los puertos que nos indica la tabla de direccionamiento asignándole las Vlan en las cuales debe trabajar esta, luego debe implementar la seguridad en cada uno de los puertos, este caso solo permitiremos el uso de 3 host distintos en cada

punto de interfaz, guardando su MAC en la tabla de Routin y finalmente desactivaremos los puertos que no estén en uso.

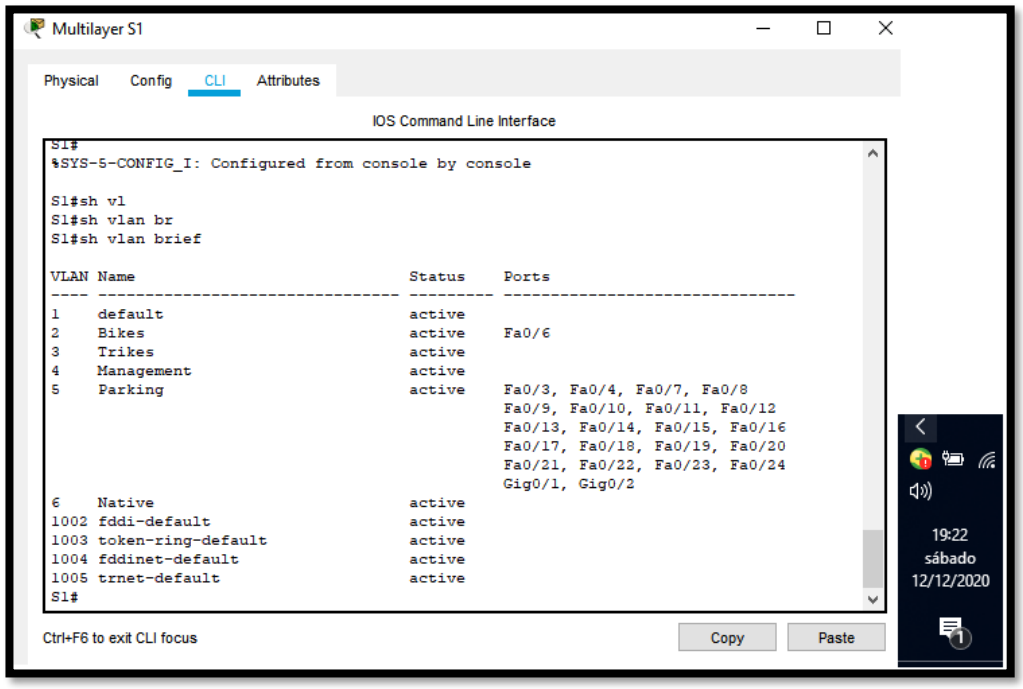
La configuración del S1 incluye las siguientes tareas:

Tabla 6. Tabla de configuración Vlan S1

Tarea	Especificación
Crear VLAN	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)# %LINK-5-CHANGED: Interface Vlan4, changed state to up 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	Interfaces F0/1, F0/2 y F0/5 S1(config)#int fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#shutdown
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** S1(config)#int range fastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#exit S1(config)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6

Tarea	Especificación
Configurar el puerto de acceso de host para VLAN 2	**Interface F0/6** S1(config)#int fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	**Permitir 3 direcciones MAC** S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 S1(config-if)#switchport port-security mac-address sticky S1(config-if)#switchport port-security violation shutdown
Proteja todas las interfaces no utilizadas • Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#int range fastEthernet 0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en Uso este Puerto S1(config-if-range)#shutdown S1(config)#int range fastEthernet 0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en Uso este Puerto S1(config-if-range)#shutdown S1(config)#int range G0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en Uso este Puerto S1(config-if-range)#shutdown

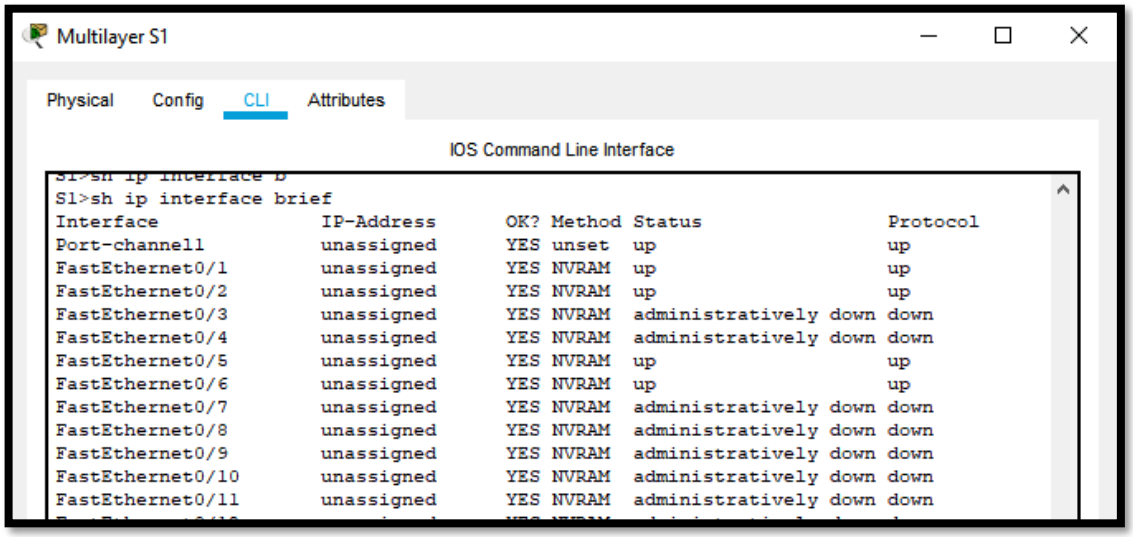
Figura 5. Show vlan brief



Fuente: Autor

Vlans configuradas en S1

Figura 6. Show ip int brief



Fuente: Autor

Como podemos observar las interfaces **1,2,5,6** son las únicas activas el resto las tenemos desactivadas tal como lo indicamos en la configuración anterior

Paso 5: Configure el S2.

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

Se crean las Vlans correspondientes según la topología dada, además de la creación de los enlaces troncales de que permitirán el recorrido de los datos a través de los fastEthernet 0/1 y fastEthernet 0/2, permitiendo también el acceso de todas las Vlans creadas, adicionalmente se crea la seguridad a los puertos de acceso para que guarden un máximo de 3 host conectados a un mismo puerto y finalmente se apaga las interfases que no se utilicen

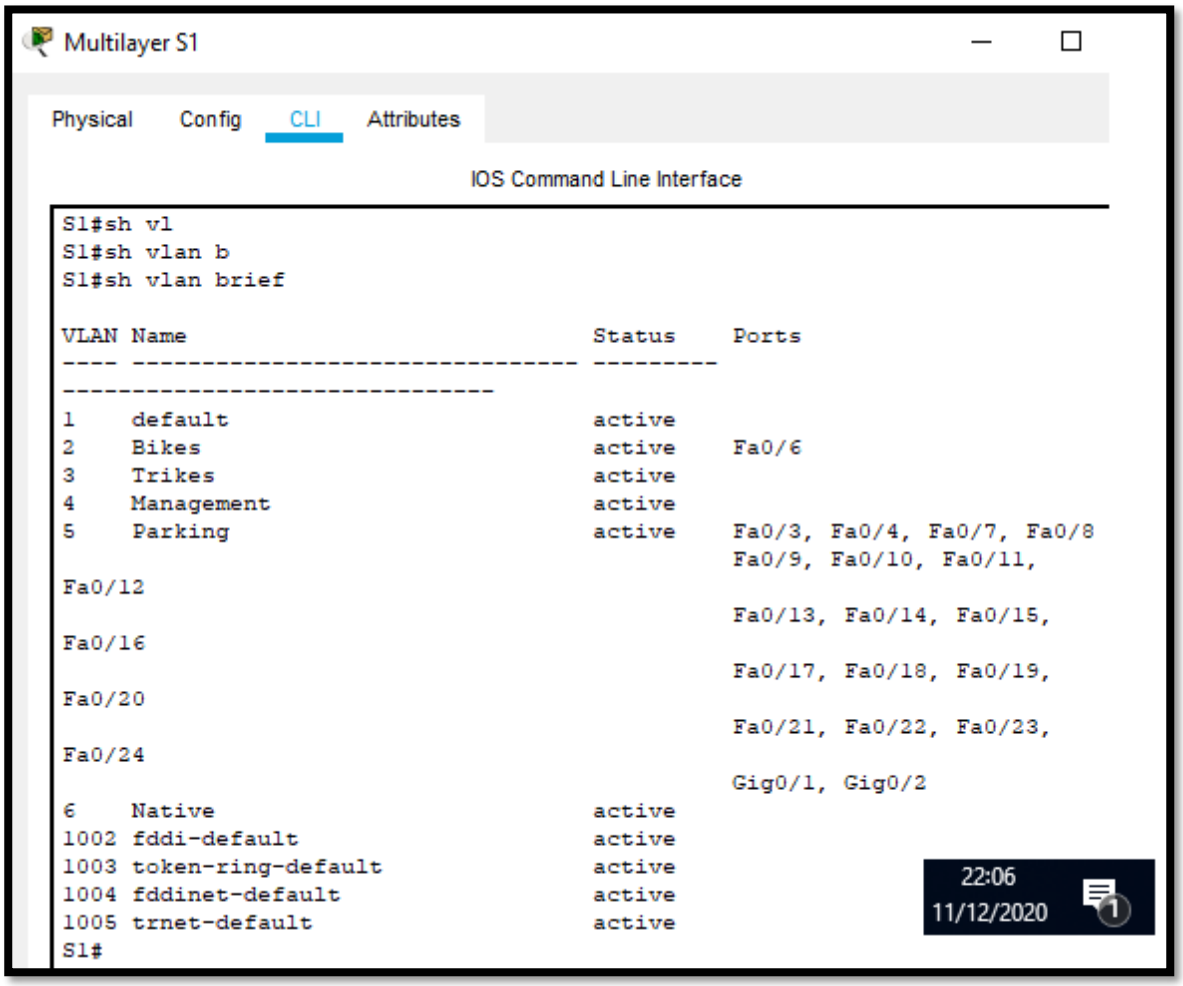
Tabla 7. Tabla de configuración Vlan S1

Tarea	Especificación
Crear VLAN	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)# %LINK-5-CHANGED: Interface Vlan4, changed state to up 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	**Interfaces F0/1 y F0/2** S2(config)#int range fastEthernet 0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#shutdown

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** S2(config)#int range fastEthernet 0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#exit S2(config)#int port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#switchport trunk allowed vlan 2,3,4,5,6
Configurar el puerto de acceso del host para la VLAN 3	**Interfaz F0/18** S2(config)#int fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	**Permite 3 MAC addresses** S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3 S2(config-if)#switchport port-security mac-address sticky S2(config-if)#switchport port-security violation shutdown

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	**Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar** S2(config)#int range fastEthernet 0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en Uso este Puerto S2(config-if-range)#shutdown S2(config)#int range fastEthernet 0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en Uso este Puerto S2(config-if-range)#shutdown S2(config)#int range G0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en Uso este Puerto S2(config-if-range)#shutdown

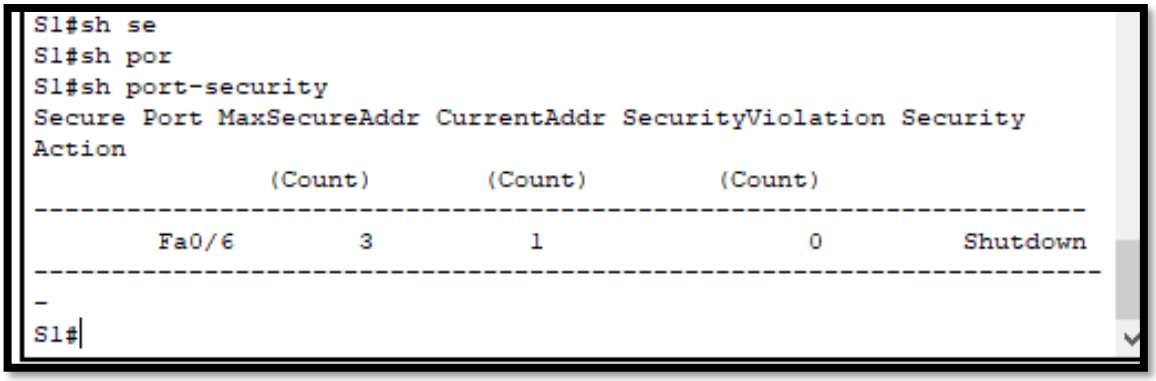
Figura 7. Show vlan brief



Fuente: Autor

Configuración de las Vlans en S1

Figura 8. Show port-security



Fuente: Autor

Seguridad en el puerto Fa0/6 del S1, lo que indica en este caso es que si conectan más de 3 host en este mismo puerto se bloqueara y se apagara

Parte 3: Configurar soporte de host

Paso 1: Configure R1

En esta parte realizaremos las ultimas configuraciones al router, lo primero será la creación de las rutas predeterminadas para redirigir todo el tráfico hacia el Loopback, luego de esto debemos configurar el direccionamiento DHCP para cada una de las Vlan que nos solicitan en la tabla

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Tabla de configuración Avanzada R1

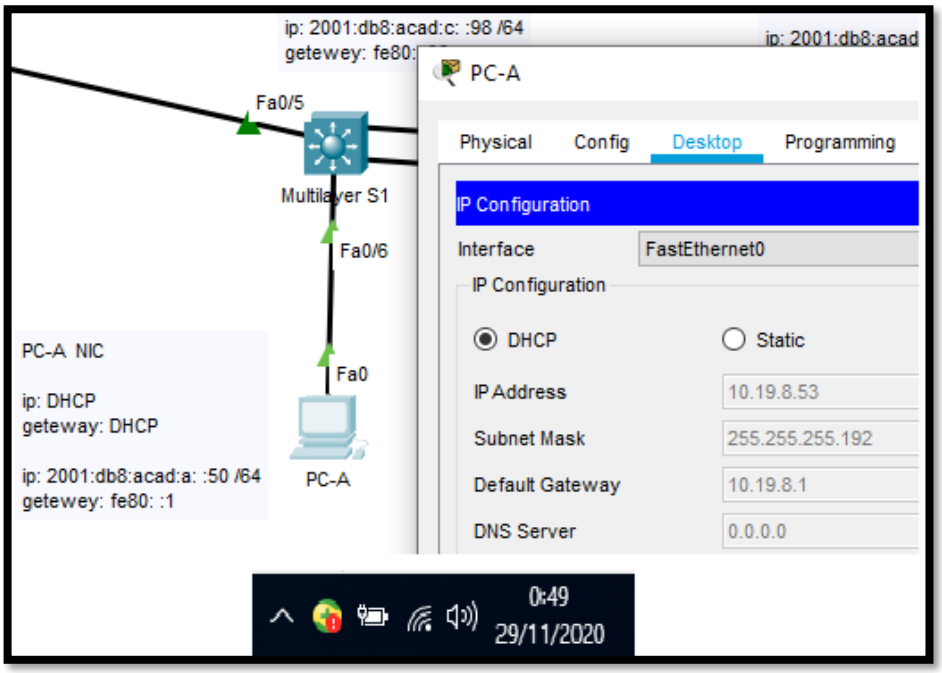
Tarea	Especificación
Configure Default Routing	**Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0** R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	**Cree un grupo DHCP para VLAN 2, compuesto 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** R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool vlan2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	**Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada** R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool vlan3-Trikes R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.56 R1(dhcp-config)#domain-name ccna-b.net

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**.

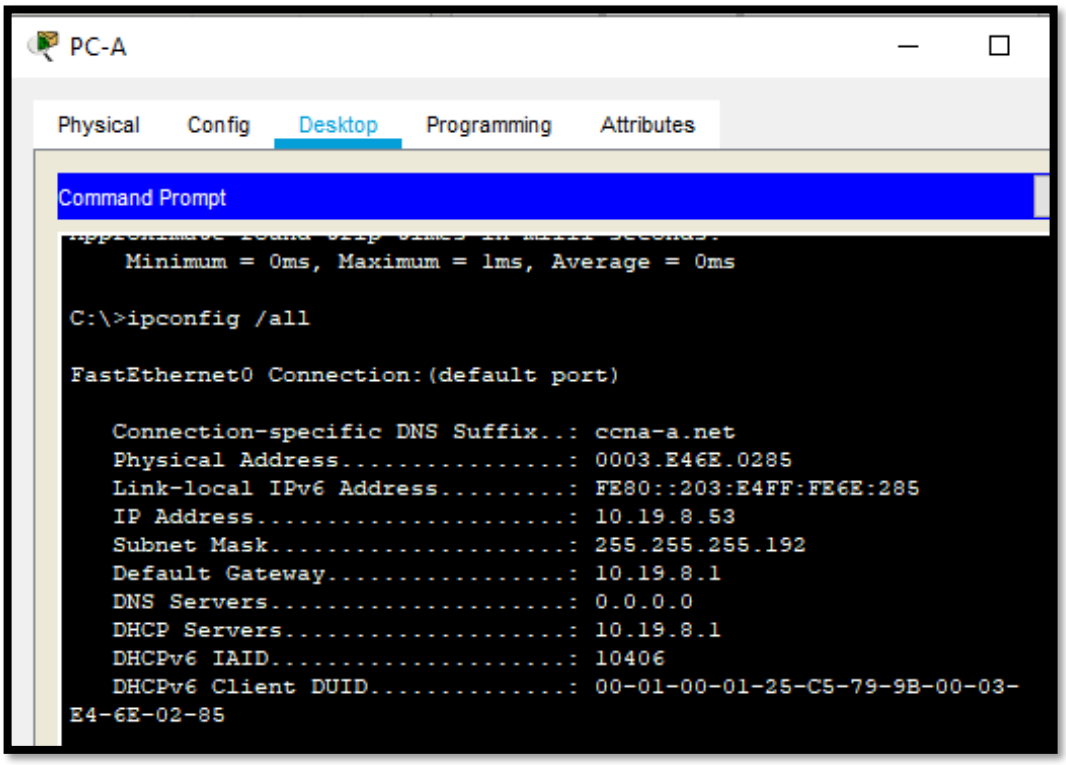
Figura 9. Configuración PC-A



Fuente: Autor

El pc-a obtiene su dirección ip por medio del servicio DHCP

Figura 10. Observación Shell PC-A



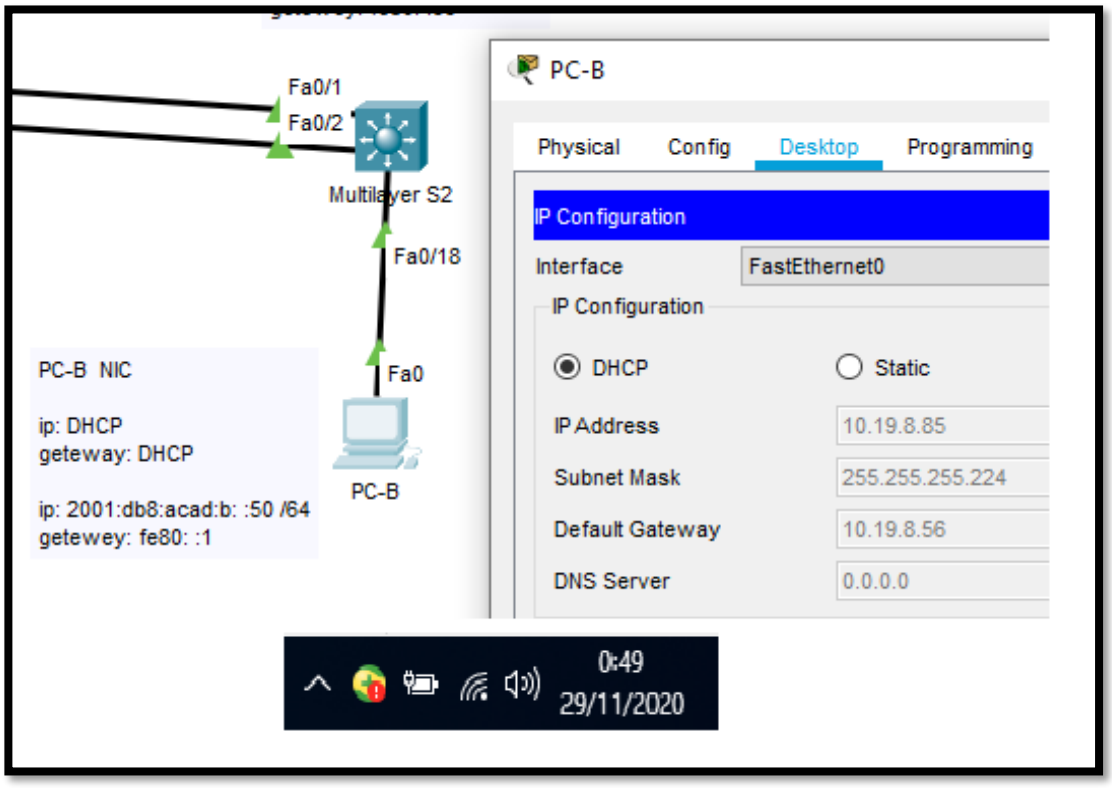
Fuente: Autor

Se observa la configuración del pc-a

Tabla 9. Tabla de configuración PC-A

Configuración de red de PC-A	
Descripción	*PC-A*
Dirección física	*0003.E46E.0285*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

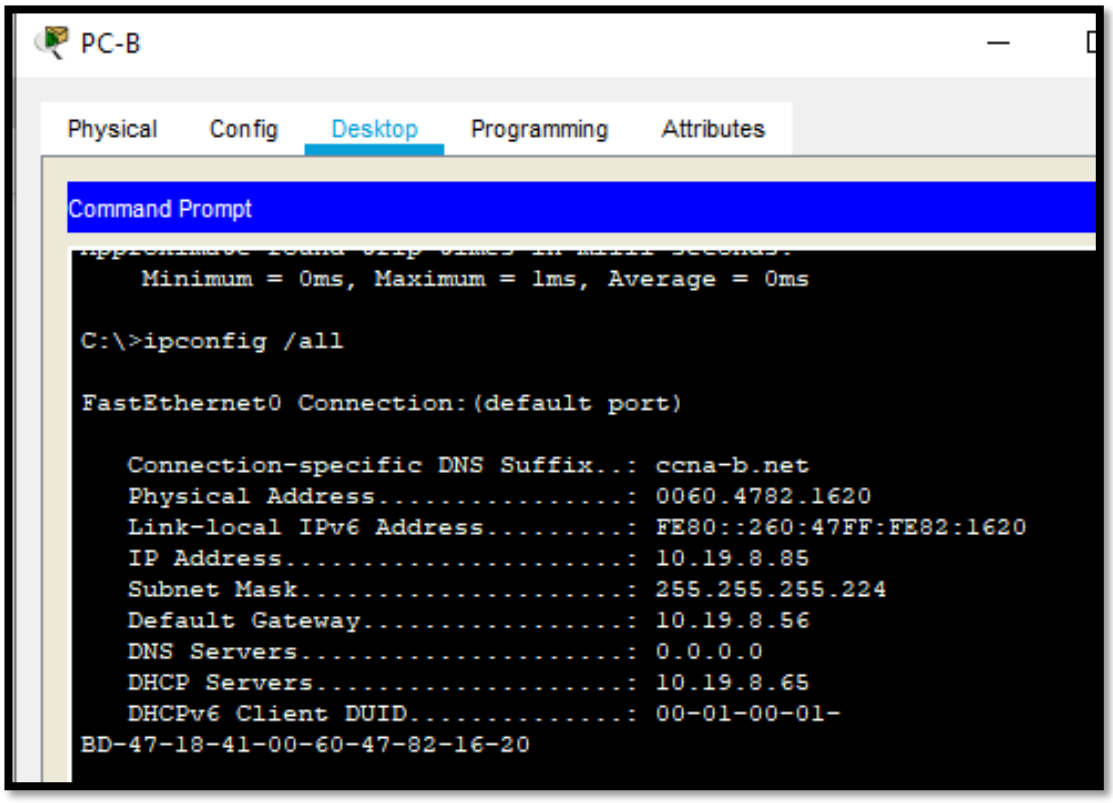
Figura 11. Configuración PC-B



Fuente: Autor

El pc-b obtiene su dirección ip por medio del servicio DHCP

Figura 12. Observación Shell PC-B



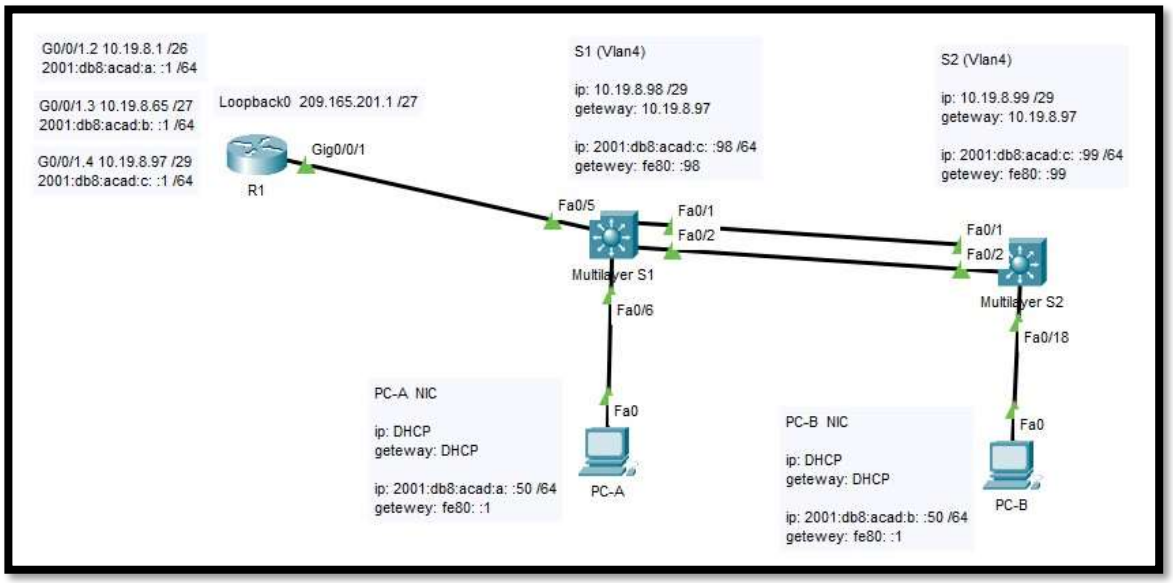
Fuente: Autor

Configuración final del pc-b

Tabla 10. Tabla de configuración PC-B

Configuración de red de PC-B	
Descripción	*PC-B*
Dirección física	*0060.4782.1620*
Dirección IP	*10.19.8.85*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.56*
Gateway predeterminado IPv6	*FE80::1*

Figura 13. Configuración final Red



Fuente: Autor

Aquí podemos observar la topología final del escenario 1 con todas sus configuraciones

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

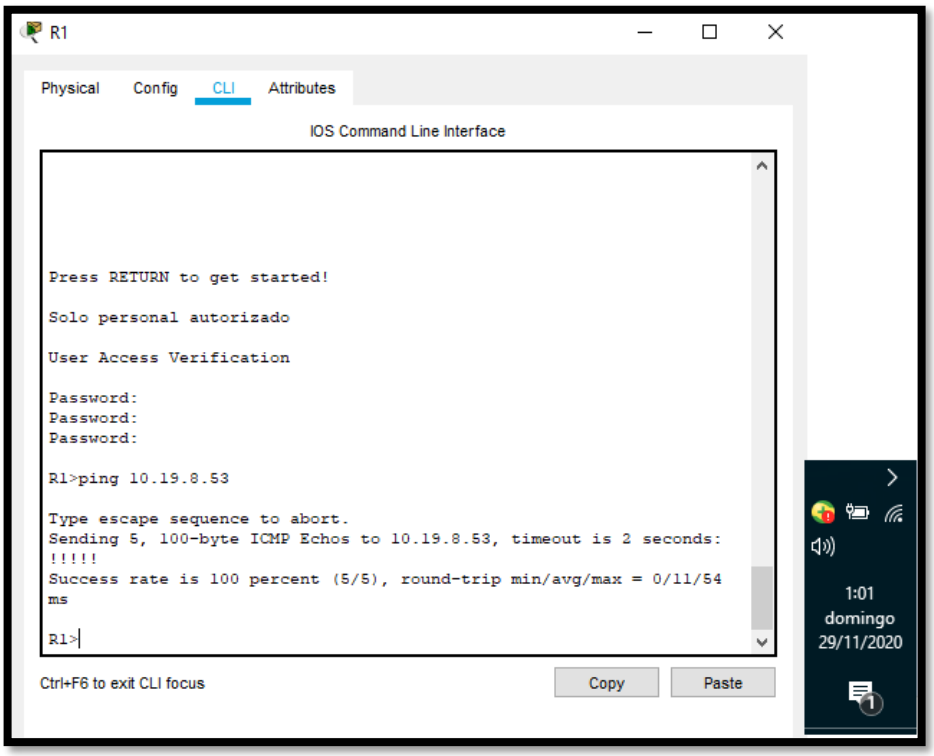
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 11. Tabla de conectividad de Red

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	IP address will vary.	*OK*
PC-A	*PC-B*	IPv6	2001:db8:acad:b: :50	*OK*
PC-A	R1 Bucle 0	Dirección	209.165.201.1	*OK*

Desde	A	de Internet	Dirección IP	Resultados de ping
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:acad: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:acad: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:acad: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:acad: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*

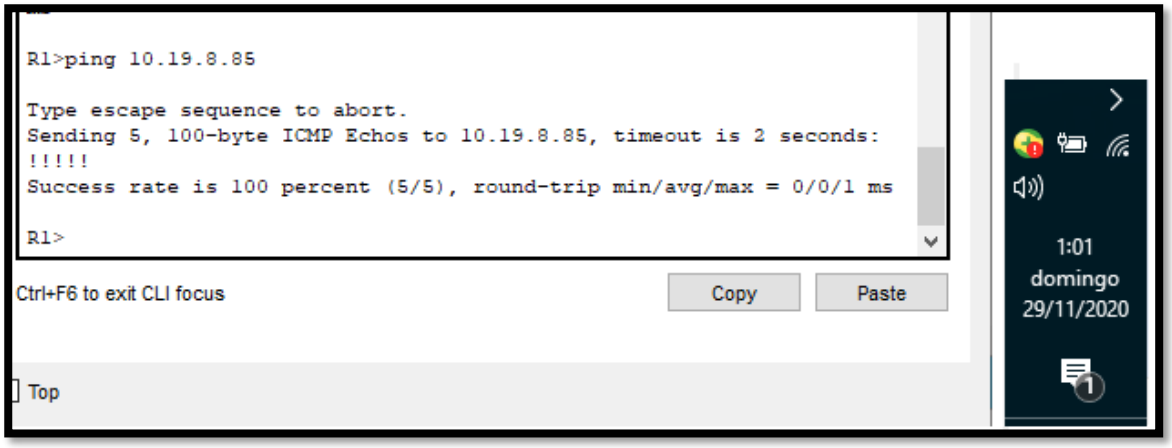
Figura 14. Ping de R1 a PC-A



Fuente: Autor

Ping exitoso de R1 hacia PC-A

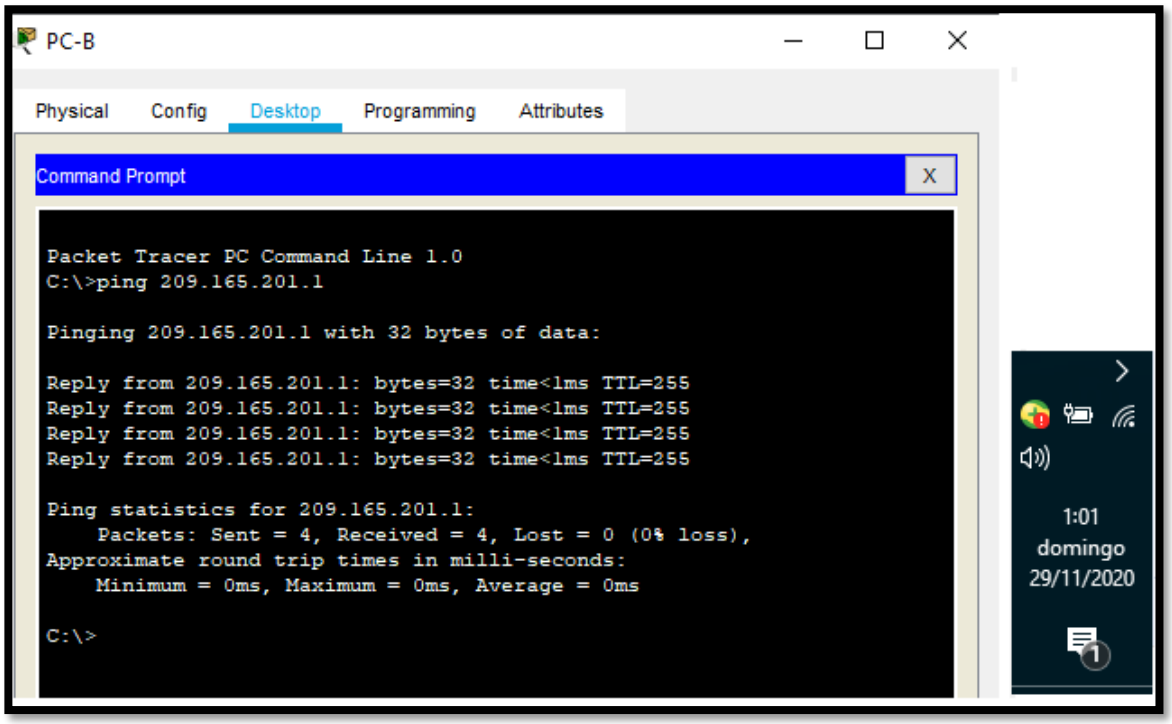
Figura 15. Ping de R1 a PC-B



Fuente: Autor

Ping exitoso de R1 hacia PC-B

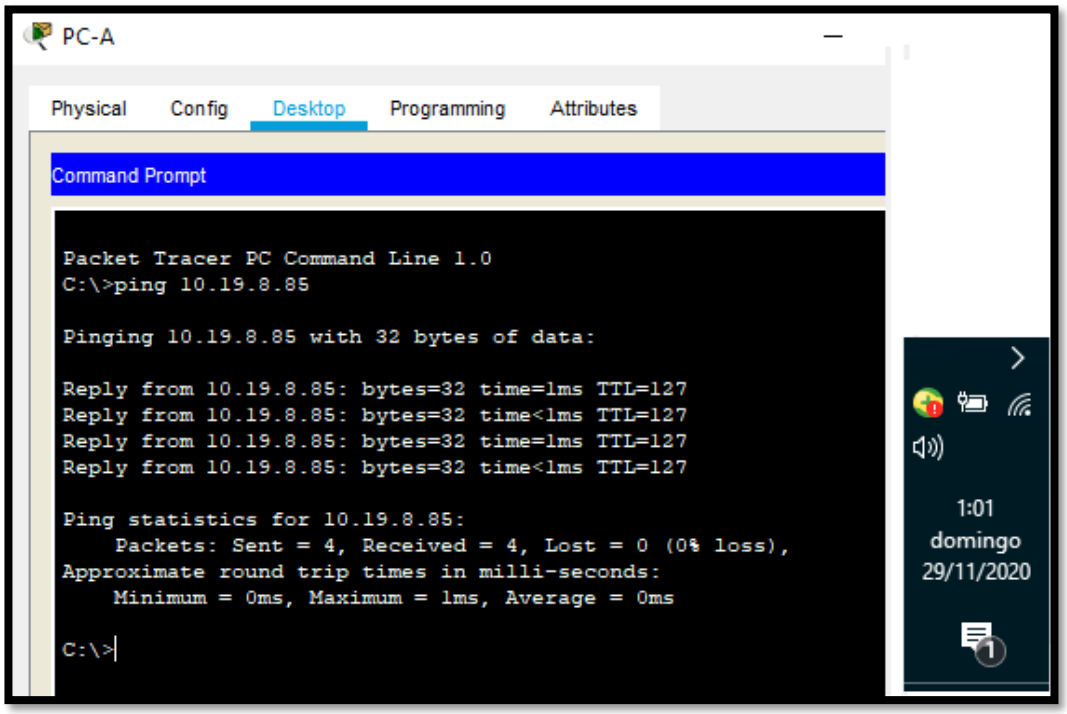
Figura 16. Ping de PC-B a Lo0



Fuente: Autor

Ping exitoso de PC-B hacia Lo0 de R1

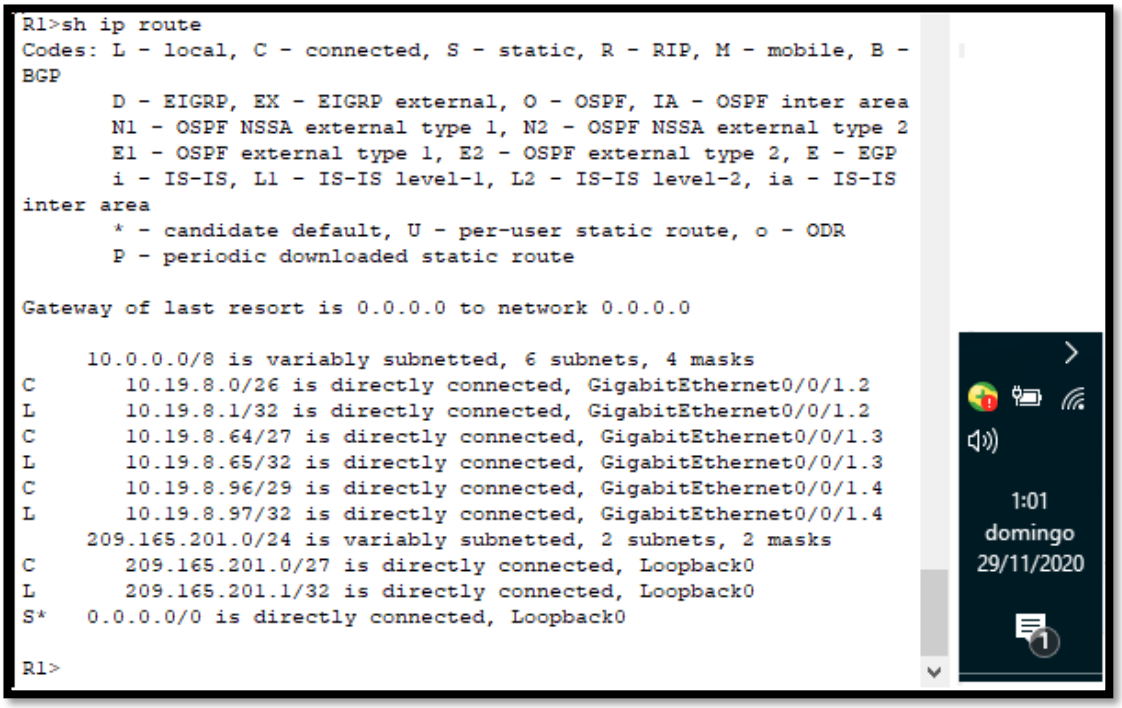
Figura 17. Ping de PC-A a PC-B



Fuente: Autor

Ping exitoso de PC-A hacia PC-B

Figura 18. Show ip route en R1



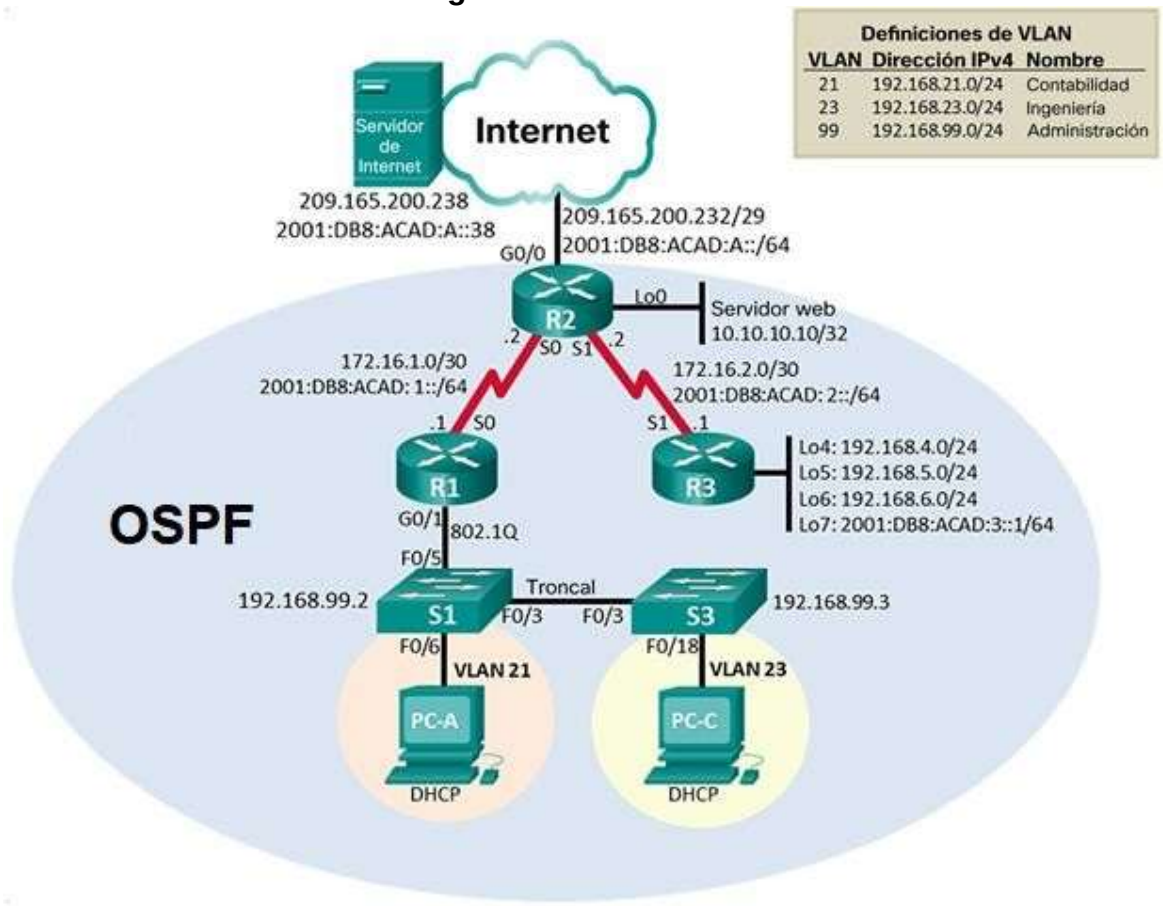
Fuente: Autor

Conexiones físicas de R1

2. ESCENARIO 2

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.
Topología

Figura 19. **Escenario 2**



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.

Lo primero que debemos realizar es borrar cualquier configuración de que tengan los dispositivos capa2 y capa3 que tenemos en nuestra topología, con el fin que no

tengamos ningún problema a la hora de realizar nuestras configuraciones, debemos eliminar el archivo startup-config que están guardados en todos los Router que es el archivo que tiene toda la configuración como las direcciones de red anteriores, después de borrar este archivo debemos reiniciar el Router para poderlo configurar desde cero. El mismo procedimiento debemos realizarlo con los switches pero adicionalmente debemos borrar Vlan.dt que tiene almacenado todas las configuraciones anteriores de cualquier Vlan que ha creado anteriormente y reiniciar el dispositivo.

Tabla 12. Tabla de comandos IOS

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch #erase startup-config Switch #delete vlan.dt
Volver a cargar ambos switches	Switch #reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>show flash:

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

En esta parte nos basaremos en la información que nos muestra la topología que estamos trabajando en este escenario 2, las direcciones ip con sus respectiva mascara subred tanto para Ipv4 como para Ipv6

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

Tabla 13. Tabla de configuración del servidor

Elemento o tarea de configuración	Especificación
Dirección IPv4	**209.165.200.238**
Máscara de subred para IPv4	**255.255.255.248**
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	**2001:DB8:ACAD:A::38 /64**
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Paso 2: Configurar R1

En esta parte debemos realizar las configuraciones básicas de seguridad para el ingreso al router , como la desactivación de la búsqueda DNS, nombrar el dispositivo de tal forma que lo podamos reconocer fácilmente en la topología, creación de contraseñas para cada una de las líneas de acceso, encriptación de todas las contraseñas para evitar que alguna persona la pueda observar al revisar la configuración inicial, creación de mensaje de advertencia para los intrusos, ingreso de la dirección Ip que comunica con el Router2 a través del puerto S0/0/0 y finalmente la creación de las rutas predeterminadas a través del mismo puerto.
Las tareas de configuración para R1 incluyen las siguientes:

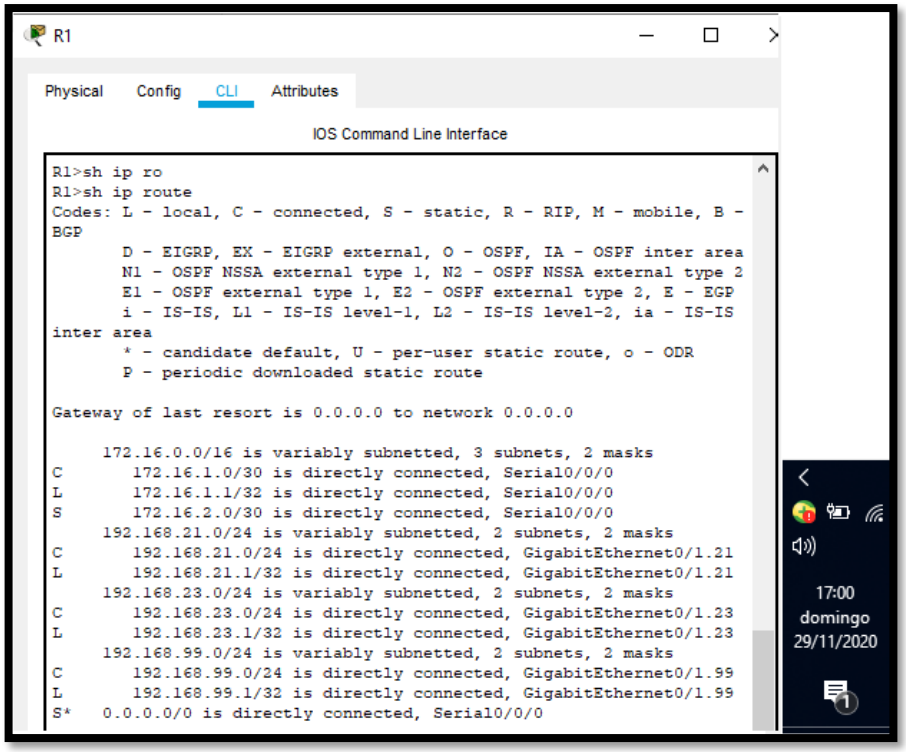
Tabla 14. Tabla de configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class R1(config)#exit
Contraseña de acceso a la consola	R1(config)# line console 0 R1(config-line)#password cisco R1(config-line)# login R1(config-line)# exit R1(config)# exit
Contraseña de acceso Telnet	R1(config)#line vty 0 15 R1(config-line)#password cisco R1(config-line)# login R1(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd # Se prohíbe el acceso no autorizado #

Interfaz S0/0/0 • Establezca la descripción • Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones • Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones • Establecer la frecuencia de reloj en 128000 • Activar la interfaz	R1(config)# ipv6 unicast-routing R1(config)#int s0/0/0 R1(config-subif)#description R1 a R2 R1(config-subif)#ip address 172.16.1.1 255.255.255.252 R1(config-subif)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-subif)# clock rate 128000 R1(config-subif)# no shutdown R1(config-subif)# exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Figura 20. Show ip route R1



Fuente: Autor

En esta parte podemos observar las conexiones físicas que tiene cada uno de los puertos seriales del router 1 con sus respectivas direcciones ip después de realizar las configuraciones.

Paso 3: Configurar R2

En esta parte siguiendo como guía la misma topología, se debe configurar de forma similar como se configuro el Router1 con la diferencia que este Router2 tiene dos redes conectadas y cada una de estas sus direcciones IP son distintas, una está por la interfaz S0/0/0 y la otra por el S0/0/1, también se debe configurar una tercera red que nos proporciona acceso a internet a través del G0/0

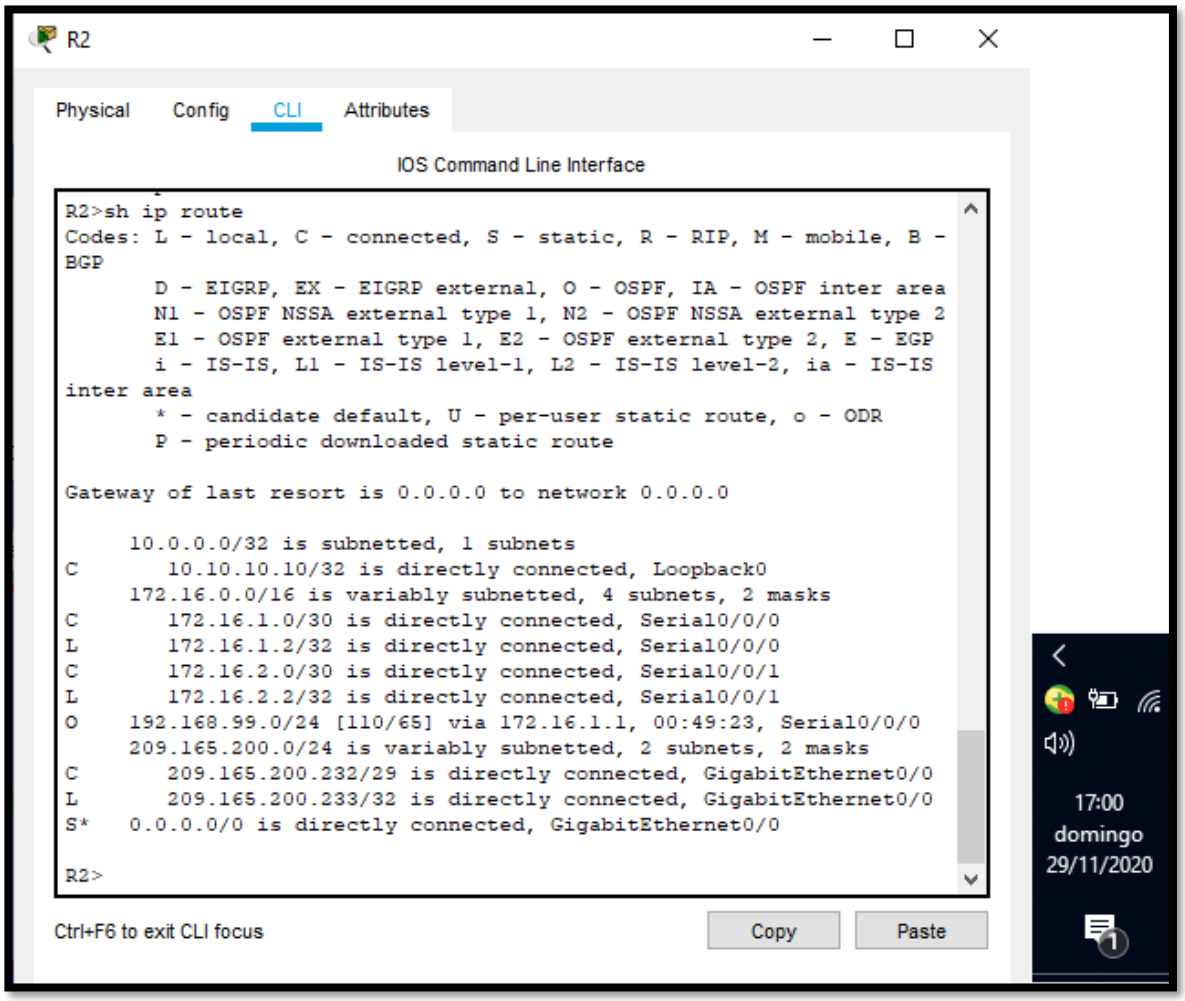
La configuración del R2 incluye las siguientes tareas:

Tabla 15. Tabla de configuración del R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class R2(config)#exit
Contraseña de acceso a la consola	R2(config)# line console 0 R2(config-line)#password cisco R2(config-line)# login R2(config-line)# exit R2(config)# exit
Contraseña de acceso Telnet	R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)# login R2(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	
Mensaje MOTD	R2(config)#banner motd # Se prohíbe el acceso no autorizado #

Interfaz S0/0/0 • Establezca la descripción • Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. • Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. • Activar la interfaz	R2(config)#ipv6 unicast-routing R2(config)#int s0/0/0 R2(config-subif)#description R2 a R1 R2(config-subif)#ip address 172.16.1.2 255.255.255.252 R2(config-subif)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-subif)# no shutdown R2(config-subif)# exit
Interfaz S0/0/1 • Establecer la descripción • Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. • Establecer la frecuencia de reloj en 128000. • Activar la interfaz	R2(config)#int s0/0/1 R2(config-subif)#description R2 a R3 R2(config-subif)#ip address 172.16.2.2 255.255.255.252 R2(config-subif)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-subif)# clock rate 128000 R2(config-subif)# no shutdown R2(config-subif)# exit
Interfaz G0/0 (simulación de Internet) • Establecer la descripción. • Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. • Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. • Activar la interfaz	R2(config)#int G0/0 R2(config-subif)#description via internet R2(config-subif)#ip address 209.165.200.233 255.255.255.248 R2(config-subif)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-subif)# no shutdown R2(config-subif)# exit
Interfaz loopback 0 (servidor web simulado) • Establecer la descripción. • Establezca la dirección IPv4.	R2(config)#int loopback 0 R2(config-subif)#description servidor web R2(config-if)#ip address 10.10.10.10 255.255.255.255
Ruta predeterminada • Configure una ruta IPv4 predeterminada de G0/0. • Configure una ruta IPv6 predeterminada de G0/0.	R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)#ipv6 route ::/0 G0/0

Figura 21. Show ip route R2



Fuente: Autor

En esta parte podemos observar las conexiones físicas que tiene cada uno de los puertos seriales del router 2 con sus respectivas direcciones ip después de realizar las configuraciones.

Paso 4: Configurar R3

En este tercer router se deben realizar configuraciones similares a los dos router anteriores con su respectiva Ip, adicionalmente se configurar cuatro direcciones loopback.

La configuración del R3 incluye las siguientes tareas:

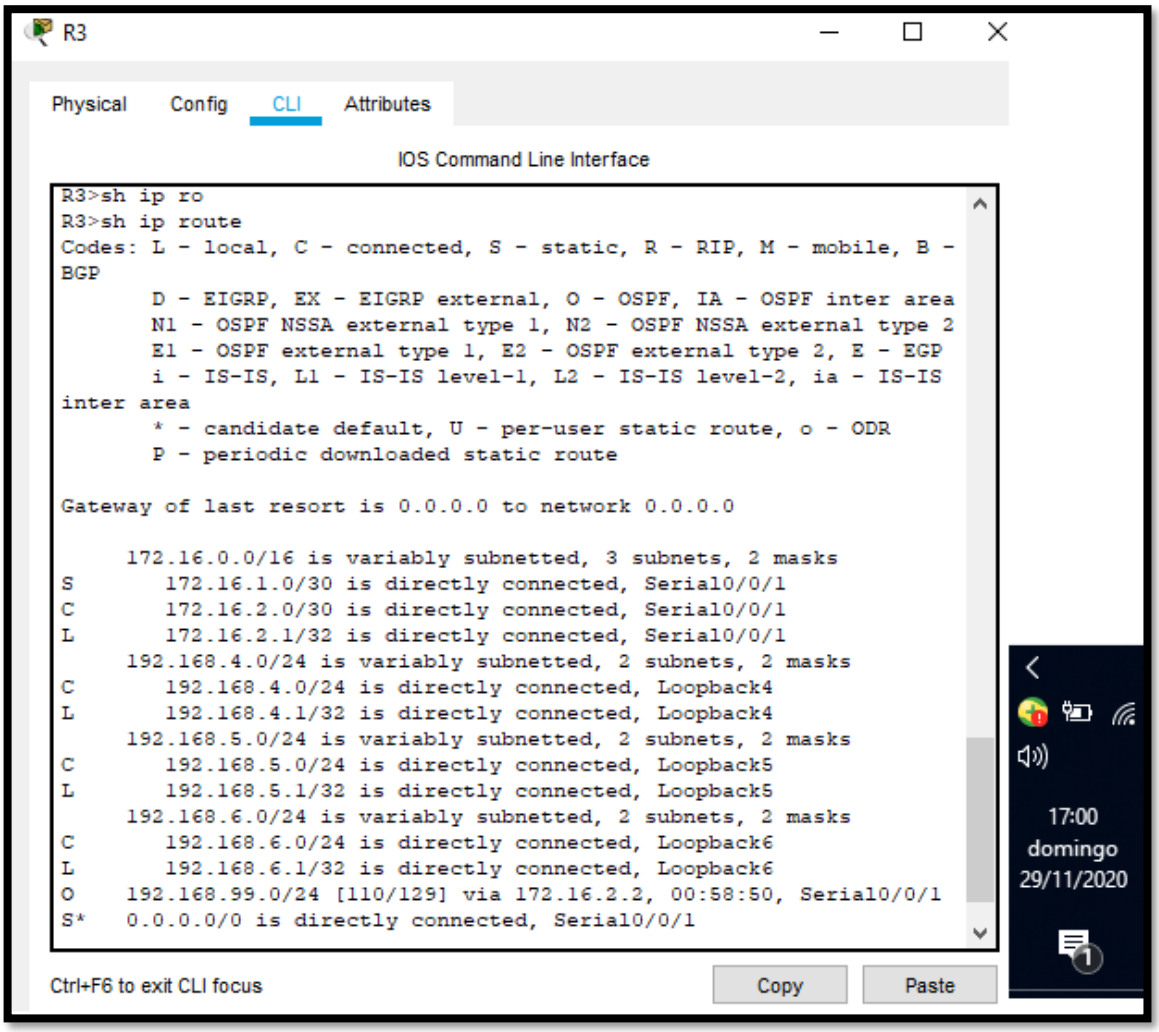
Tabla 16. Tabla de configuración del R3

Elemento o tarea de configuración	Especificación

Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#exit
Contraseña de acceso a la consola	R3(config)# line console 0 R3(config-line)#password cisco R3(config-line)# login R3(config-line)# exit R3(config)# exit
Contraseña de acceso Telnet	R3(config)#line vty 0 15 R3(config-line)#password cisco R3(config-line)# login R3(config-line)# exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd # Se prohíbe el acceso no autorizado #
Interfaz S0/0/1 • Establecer la descripción • Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. • Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. • Activar la interfaz	R3(config)#ipv6 unicast-routing R3(config)#int s0/0/1 R3(config-subif)#description R3 a R2 R3(config-subif)#ip address 172.16.2.1 255.255.255.252 R3(config-subif)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-subif)# no shutdown R3(config-subif)# exit
Interfaz loopback 4 • Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 • Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 • Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7 • Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 S0/0/1 R3(config)#ipv6 route ::/0 S0/0/1

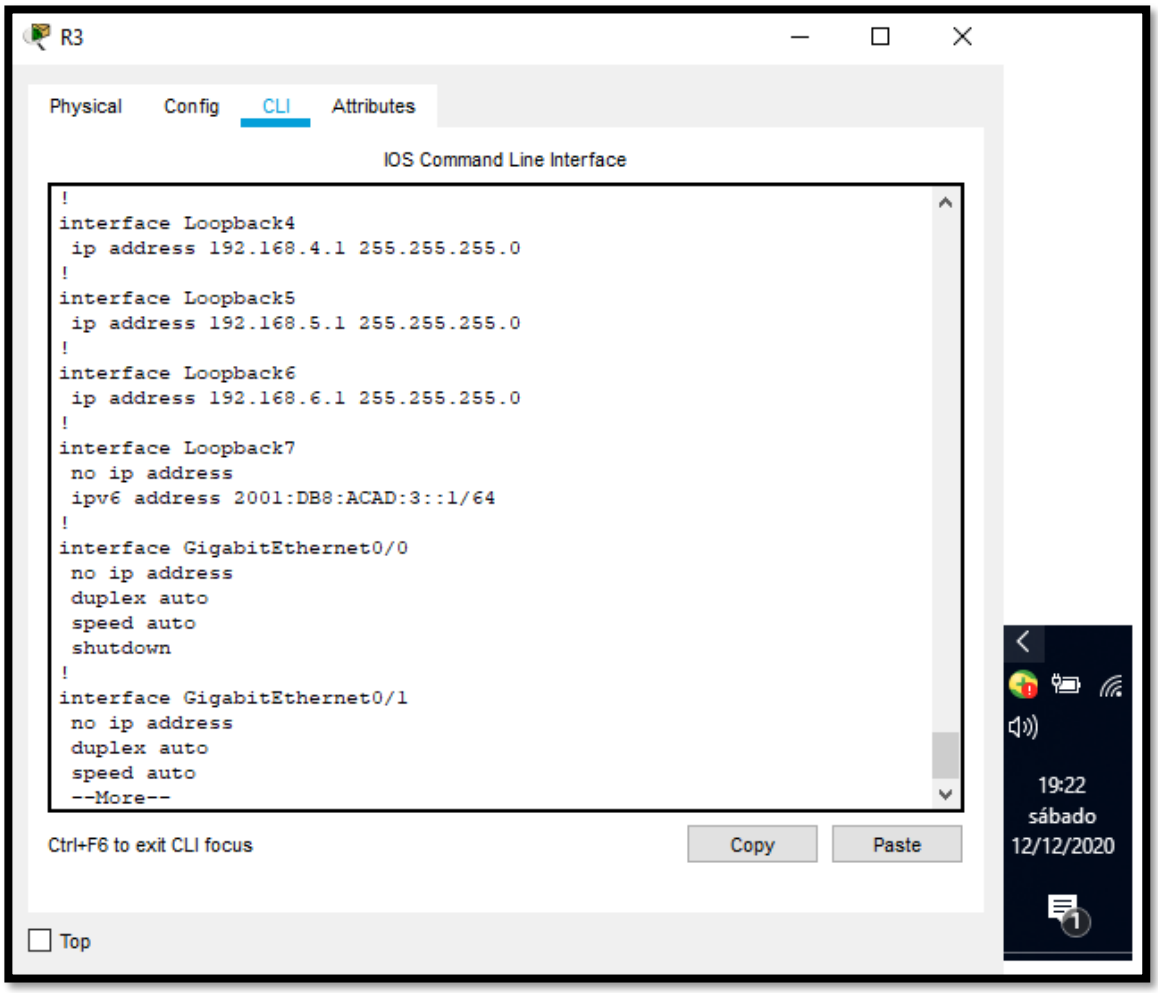
Figura 22. Show ip route R3



Fuente: Autor

En esta parte podemos observar las conexiones físicas que tiene cada uno de los puertos seriales del router 3 con sus respectivas direcciones ip después de realizar las configuraciones.

Figura 23. Show running-config



Fuente: Autor

Configuración de Loopback

Paso 5: Configurar S1

En esta parte configuramos el S1 con las configuraciones básicas que ya hemos realizado anteriormente con los otros dispositivos como son contraseñas, nombre del dispositivo, cifrado de contraseñas, desactivación de búsqueda DNS

La configuración del S1 incluye las siguientes tareas:

Tabla 17. Tabla de configuración del S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch (config)#no ip domain-lookup
Nombre del switch	Switch (config)#hostname S1

Contraseña de exec privilegiado cifrada	S1 (config)#enable secret class S1 (config)#exit
Contraseña de acceso a la consola	S1 (config)# line console 0 S1 (config-line)#password cisco S1 (config-line)# login S1 (config-line)# exit S1 (config)# exit
Contraseña de acceso Telnet	S1 (config)#line vty 0 4 S1 (config-line)#password cisco S1 (config-line)# login S1 (config-line)# exit
Cifrar las contraseñas de texto no cifrado	S1 (config)#service password-encryption
Mensaje MOTD	S1 (config)#banner motd # Se prohíbe el acceso no autorizado #

Paso 6: Configurar el S3

Al igual que el Switch anterior en esta parte configuramos el S3 con las configuraciones básicas que ya hemos realizado anteriormente con los otros dispositivos como son contraseñas, nombre del dispositivo, cifrado de contraseñas, desactivación de búsqueda DNS

La configuración del S3 incluye las siguientes tareas:

Tabla 18. Tabla de configuración del S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch (config)#no ip domain-lookup
Nombre del switch	Switch (config)#hostname S1
Contraseña de exec privilegiado cifrada	S3 (config)#enable secret class S3 (config)#exit
Contraseña de acceso a la consola	S3 (config)# line console 0 S3 (config-line)#password cisco S3 (config-line)# login S3 (config-line)# exit
Contraseña de acceso Telnet	S3 (config)#line vty 0 15 S3 (config-line)#password cisco S3 (config-line)# login S3 (config-line)# exit
Cifrar las contraseñas de texto no cifrado	S3 (config)#service password-encryption
Mensaje MOTD	S3 (config)#banner motd # Se prohíbe el acceso no autorizado #

Paso 7: Verificar la conectividad de la red

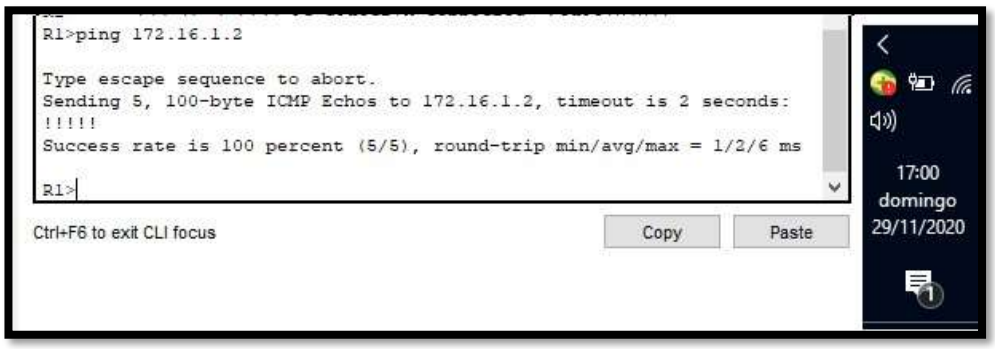
Utilice el comando ping para probar la conectividad entre los dispositivos de red.

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 19. Pruebas de ping – R1,R2,R3

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	**172.16.1.2** **2001:DB8:ACAD:1::2**	**5/5**
R2	R3, S0/0/1	**172.16.2.1** **2001:DB8:ACAD:2::1**	**5/5**
PC de Internet	Gateway predeterminado	**209.165.200.233**	**4/4**

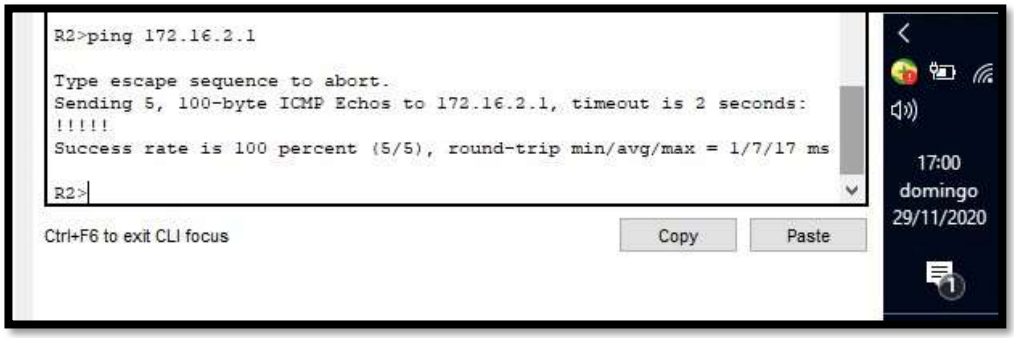
Figura 24. Ping R1 – R2



Fuente: Autor

Ping exitoso del R1 hacia el R2

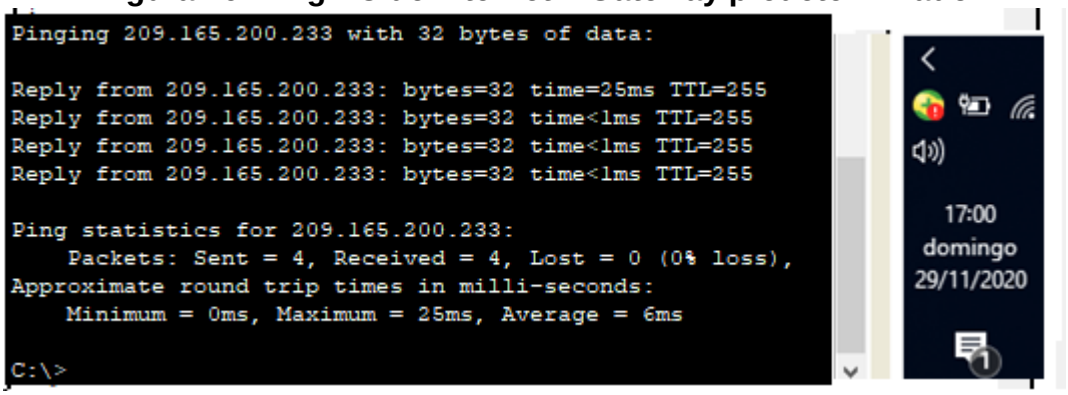
Figura 25. Ping R2 – R3



Fuente: Autor

Ping exitoso del R2 hacia el R3

Figura 26. Ping PC de Internet – Gateway predeterminado



Fuente: Autor

Ping exitoso del PC de Internet hacia su Gateway predeterminado

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

Paso 1: Configurar S1

En esta parte debemos crear todas la Vlan que se indican en la tabla de direccionamiento, luego de la creación de estas, debemos configurar los enlaces troncales en los puertos que nos indica la tabla de direccionamiento asignándole las Vlan en las cuales debe trabajar esta, y finalmente desactivaremos los puertos que no estén en uso.

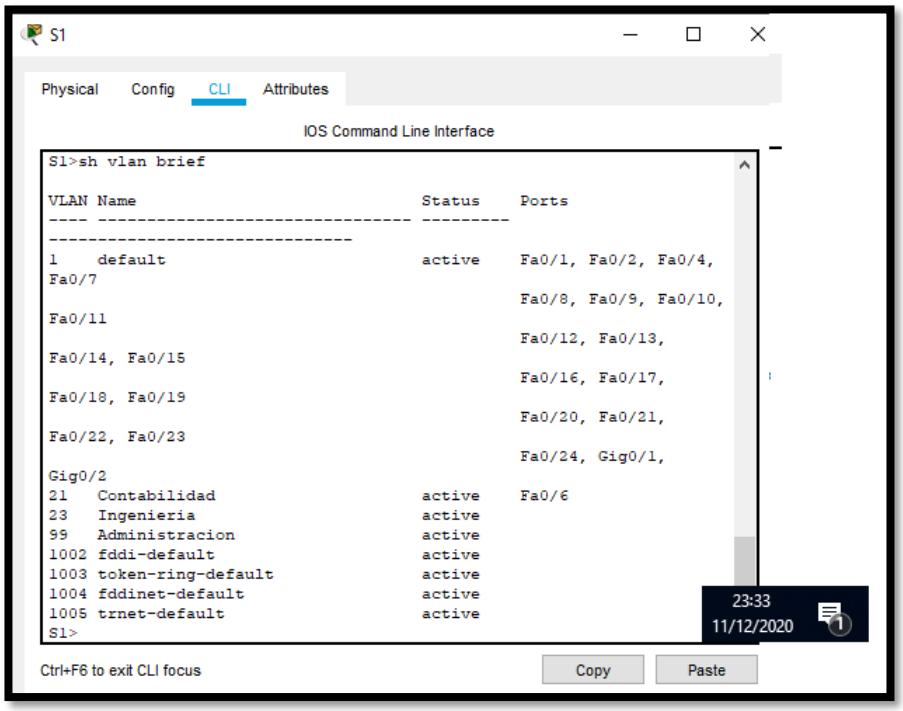
La configuración del S1 incluye las siguientes tareas:

Tabla 20. Configuración Vlans – S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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 Administracion
Asignar la dirección IP de administración. • Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#int vlan 99 S1(config)#ip address 192.168.99.2 255.255.255.0 S1 (config-subif)# no shutdown S1 (config-subif)# exit

Asignar el gateway predeterminado • Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-Gateway 192.168.99.1 S1(config)#exit
Forzar el enlace troncal en la interfaz F0/3 • Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5 • Utilizar la red VLAN 1 como VLAN nativa	S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso • Utilizar el comando interface range	S1(config)#int range f0/1-2,f0/4,f0/7-24,G0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config)#int range f0/1-2,f0/4,f0/7-24,G0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#exit

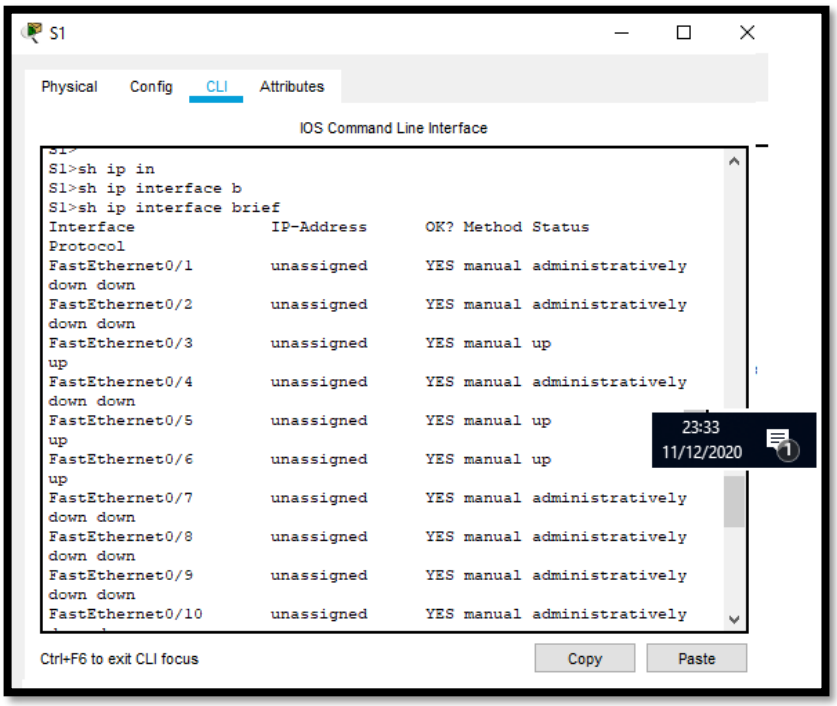
Figura 27. Show vlan brief



Fuente: Autor

Vlans configuradas en S1

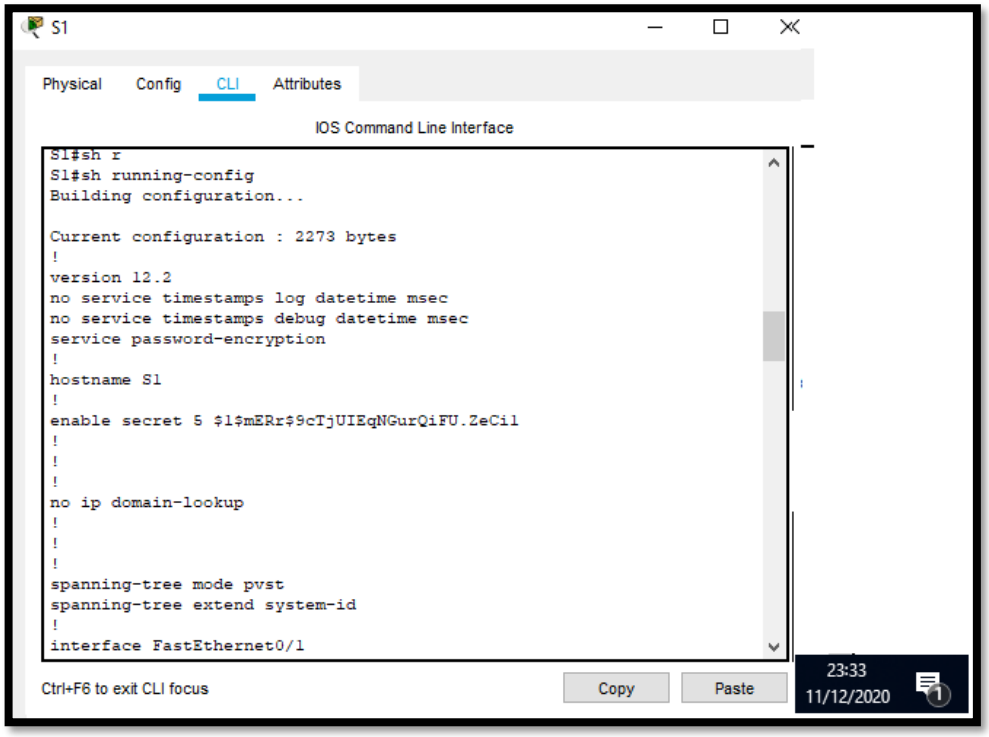
Figura 28. Show ip int brief



Fuente: Autor

Interfases activas en el S1

Figura 29. Show running-config



Fuente: Autor

Configuraciones iniciales del S1

Paso 2: Configurar el S3

En esta parte debemos crear todas la Vlan que se indican en la tabla de direccionamiento, luego de la creación de estas, debemos configurar los enlaces troncales en los puertos que nos indica la tabla de direccionamiento asignándole las Vlan en las cuales debe trabajar esta, y finalmente desactivaremos los puertos que no estén en uso.

La configuración del S3 incluye las siguientes tareas:

Tabla 21. Configuración Vlans – S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	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 Administracion

Asignar la dirección IP de administración • Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3 (config-subif)# no shutdown S3(config-if)#exit
Asignar el gateway predeterminado. • Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-Gateway 192.168.99.1 S1(config)#exit
Forzar el enlace troncal en la interfaz F0/3 • Utilizar la red VLAN 1 como VLAN nativa	S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config)#int range f0/1-2,f0/4-17,f0/19-24,G0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2,f0/4-17,f0/19-24,G0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit

Nota: esta configuración utilizamos las mismas configuraciones que el S1-2, solo cambiarias las direcciones ip

Paso 3: Configurar R1

Luego de realizar estas configuraciones básicas de seguridad le asignaremos las direcciones Ip a cada una de las subinterfaces tal como lo indica nuestra tabla de direccionamiento, con el objetivo que el router pueda mantener el tráfico separado de cada una de las Vlan configuradas en la red ya que cada una debe funcionar de manera independiente para un mejor flujo y seguridad de esta, finalmente debemos levantar el servicio en esta interfaz G0/1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración subinterfaz – G0/1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 • Descripción: LAN de Contabilidad • Asignar la VLAN 21 • Asignar la primera dirección disponible a esta interfaz	R1(config)#int G0/1.21 R1(config-subif)#description LAN de Contabilidad R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1 • Descripción: LAN de Ingeniería • Asignar la VLAN 23 • Asignar la primera dirección disponible a esta interfaz	R1(config)#int G0/1.23 R1(config-subif)#description LAN de Ingeniera R1(config-subif)#encapsulation dot1Q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1 • Descripción: LAN de Administración • Asignar la VLAN 99 • Asignar la primera dirección disponible a esta interfaz	R1(config)#int G0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#encapsulation dot1Q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown

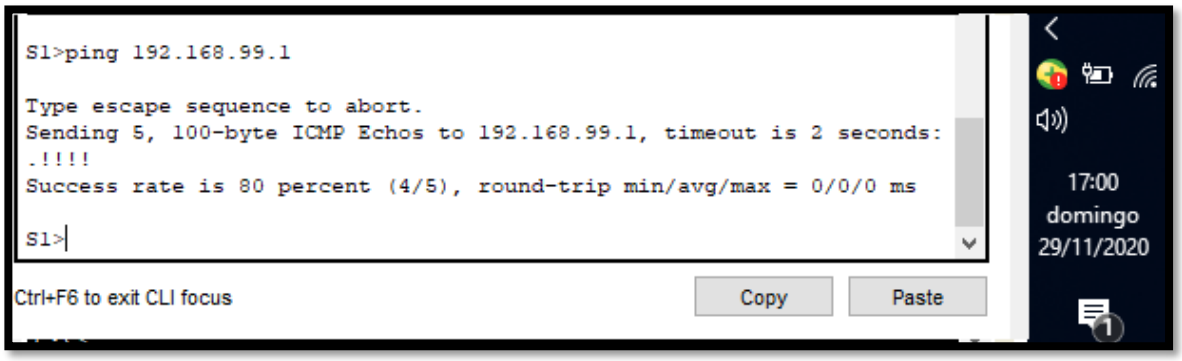
Paso 4: Verificar la conectividad de la red

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 23. Prueba de conectividad – S1,S2,S3,Vlans

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	**192.168.99.1**	**4/5**
S3	R1, dirección VLAN 99	**192.168.99.1**	**4/5**
S1	R1, dirección VLAN 21	**192.168.22.1**	**5/5**
S3	R1, dirección VLAN 23	**192.168.23.1**	**5/5**

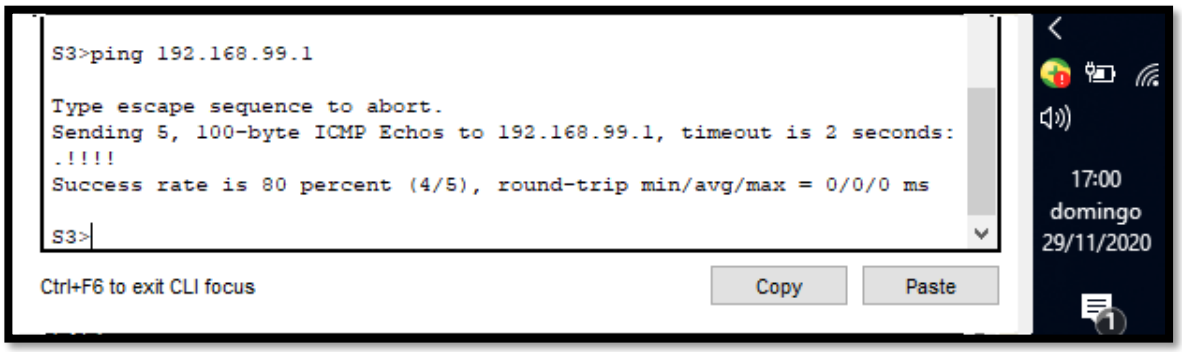
Figura 30. Ping S1 – R1 Vlan 99



Fuente: Autor

Ping exitoso de S1 hacia Vlan 99 de R1

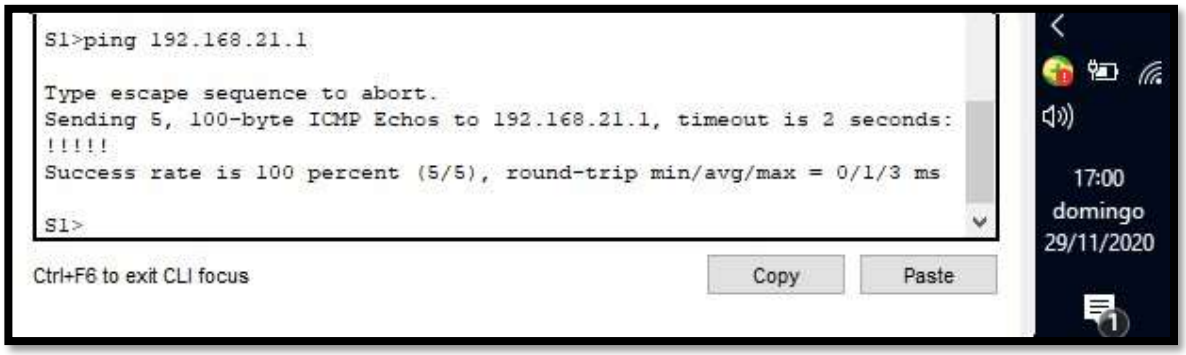
Figura 31. Ping S3 – R1 Vlan 99



Fuente: Autor

Ping exitoso de S3 hacia Vlan 99 de R1

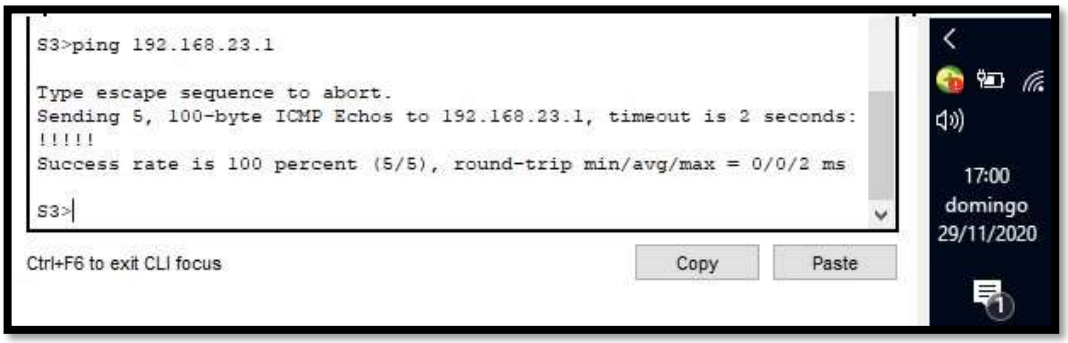
Figura 32. Ping S1 – R1 Vlan 21



Fuente: Autor

Ping exitoso de S1 hacia Vlan 21 de R1

Figura 33. Ping S3 – R1 Vlan 23



Fuente: Autor

Ping exitoso de S3 hacia Vlan 23 de R1

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:
El objetivo de la configuración el los dispositivos conozcan toda la red y puedan tomar el camino más corto hacia la su objetivo, en este caso el dispositivos que deseen conectarse.

El comando **passive** lo utilizamos para poder evitar que dichos dispositivos que tengan esta configuración puedan obtener algún tipo de actualización que requiera el sistema en general

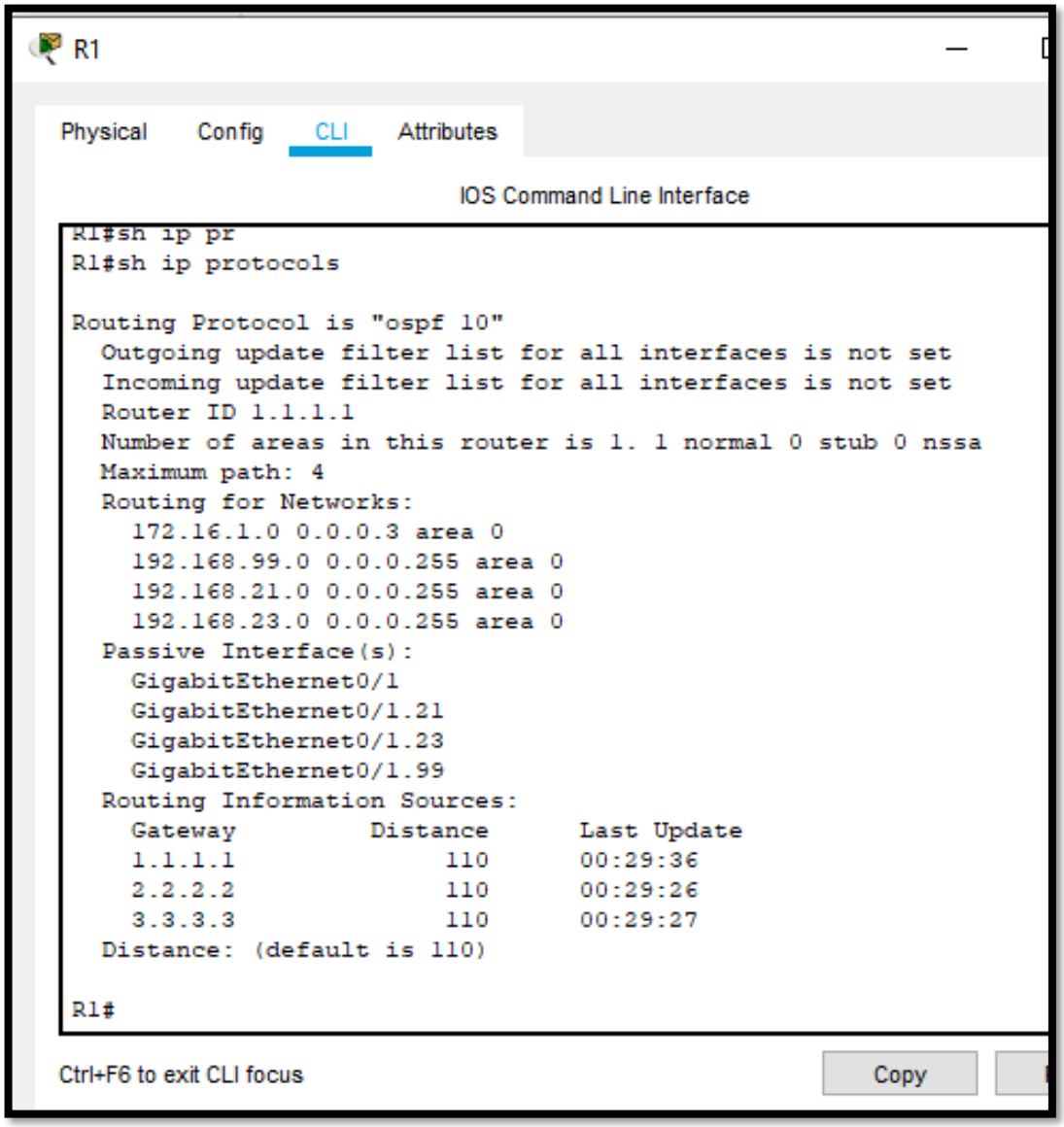
Tabla 24. Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 10 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente • Asigne todas las redes conectadas directamente.	R1(config-router)#network 172.16.1.0 0.0.0.3 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	R1(config-router)#passive-interface gigabitEthernet 0/1 R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	(Solo aplica en Protocolo Rip)

Luego de realizar las configuraciones podemos observar las redes que quedaron configuradas con ayuda del comando **show ip protocols**

Figura 34. Show ip protocols



Fuente: Autor

Configuración de OSPF en el R1 podemos observar la red que conduce al S1 que es la 192.168.99.0, la red que conduce al R2 172.16.1.0 y las otras dos redes internas que conducen a las Vlans de contabilidad 192.168.21.0 y la que conduce a ingeniería 192.168.23.0, finamente las interfaces que configuramos de forma pasiva para que no puedan recibir actualizaciones.

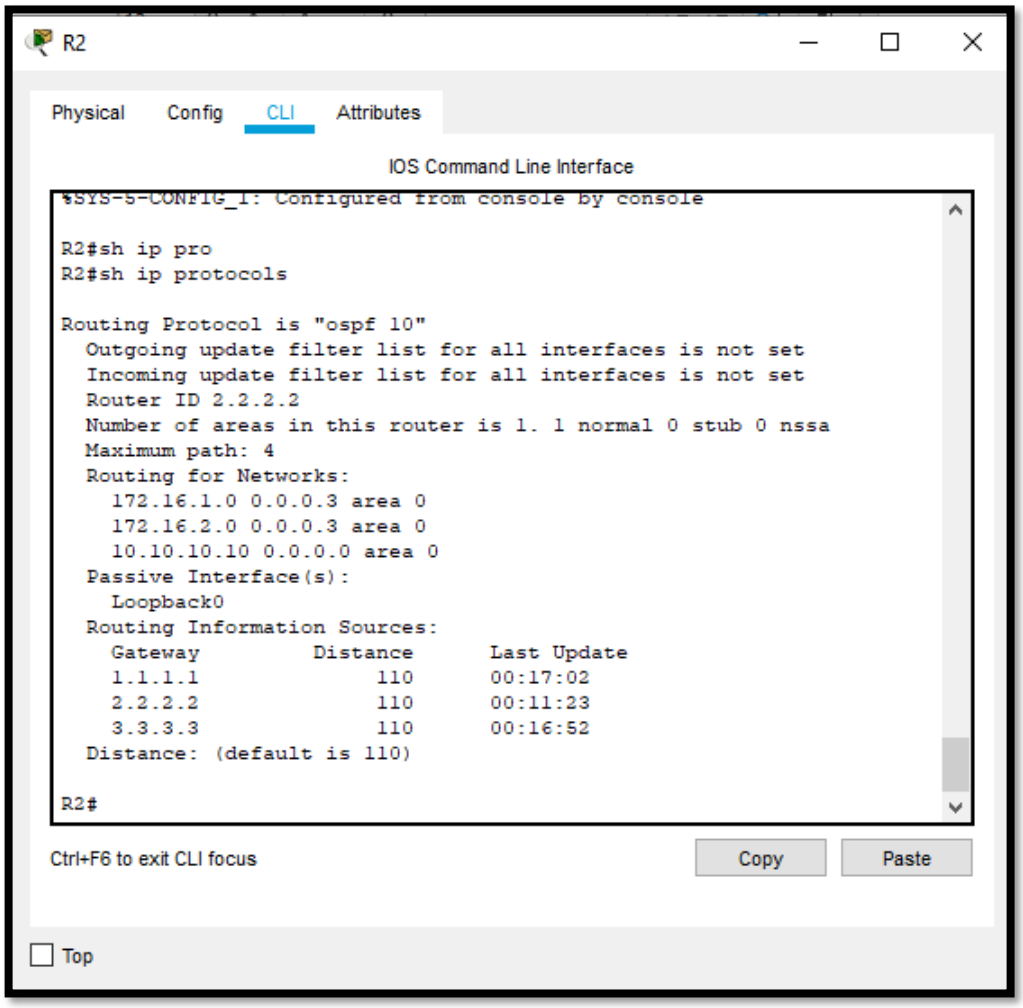
Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:
En esta parte también anunciaremos las redes que están conectadas directamente a este Router2

Tabla 25. Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 10 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente Nota: Omitir la red G0/0.	R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface Loopback 0
Desactive la sumarización automática.	(Solo aplica en Protocolo Rip)

Figura 35. Show ip protocols



Fuente: Autor

Paso 3: Configurar OSPFv3 en el R3

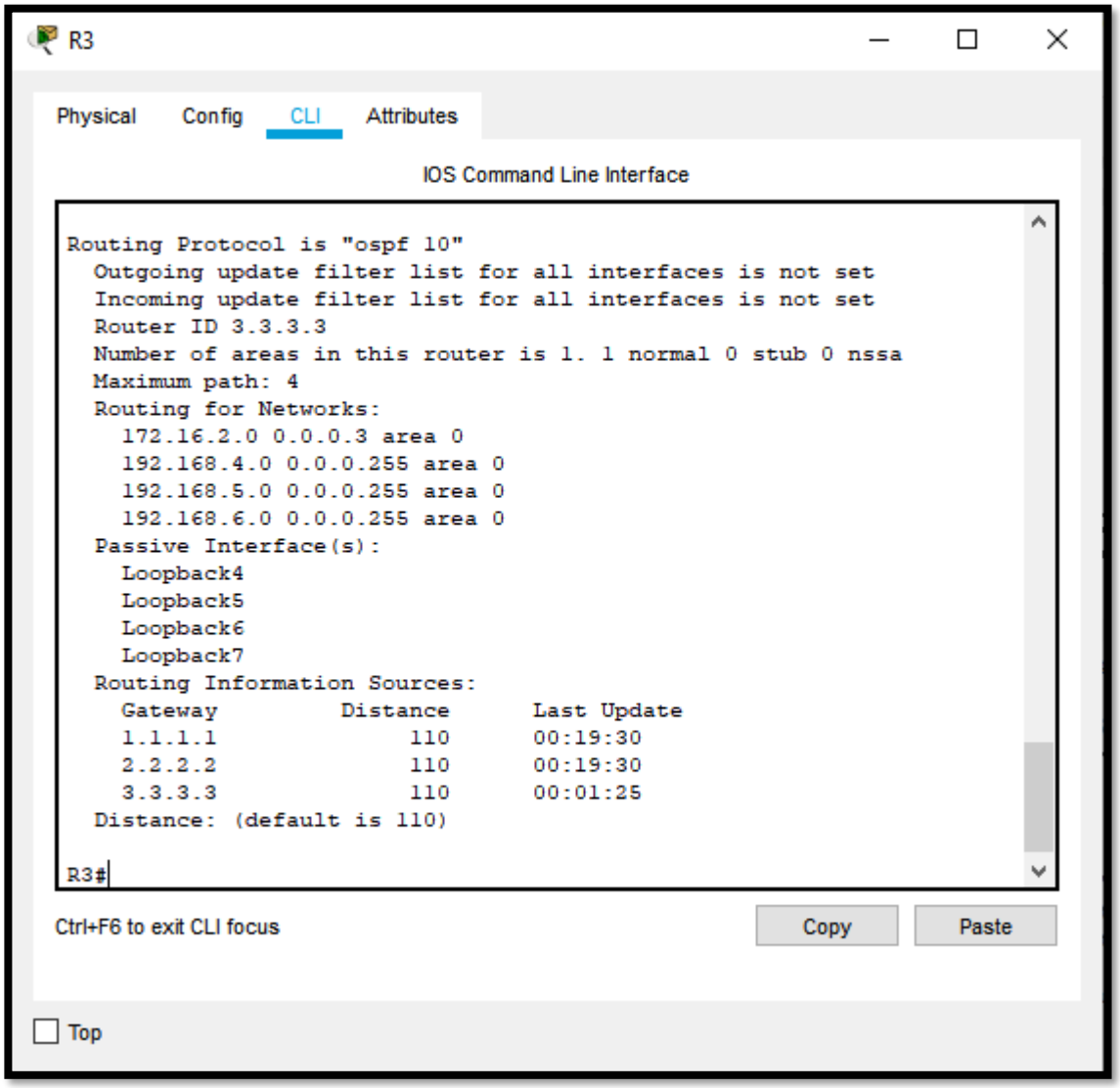
La configuración del R3 incluye las siguientes tareas:

Tabla 26. Configurar OSPF en el R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config-if)#ipv6 ospf 10 area 0 Router(config-if)#exit R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 10 R3(config)#router ospf 10 R3(config-rtr)#router-id 3.3.3.3

Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 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	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6
Desactive la sumarización automática.	(Solo aplica en Protocolo Rip)

Figura 36. Show ip protocols



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:

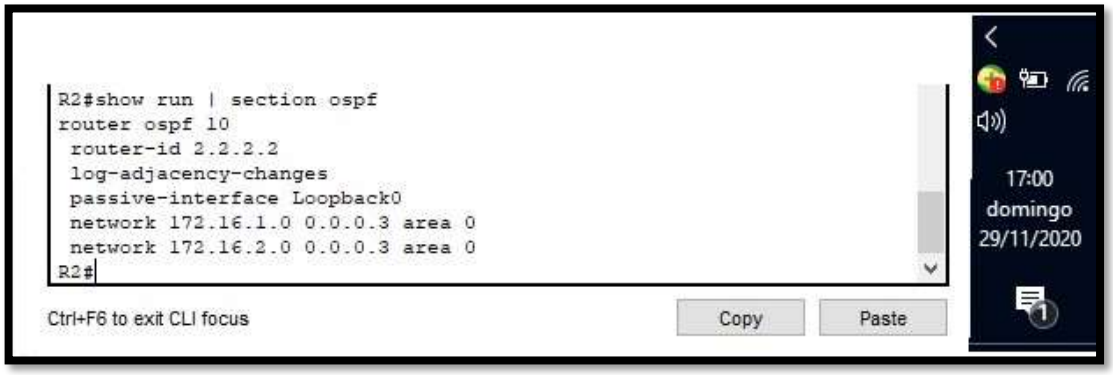
Tabla 27. Verificación de información OSPF – R1,R2,R3

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?	R3#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show run | section ospf

Figura 37. Show ip route ospf – R2

Fuente: Autor

Figura 38. Show run | section ospf – R2



Fuente: Autor

Parte 5: Implementar DHCP y NAT para IPv4

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

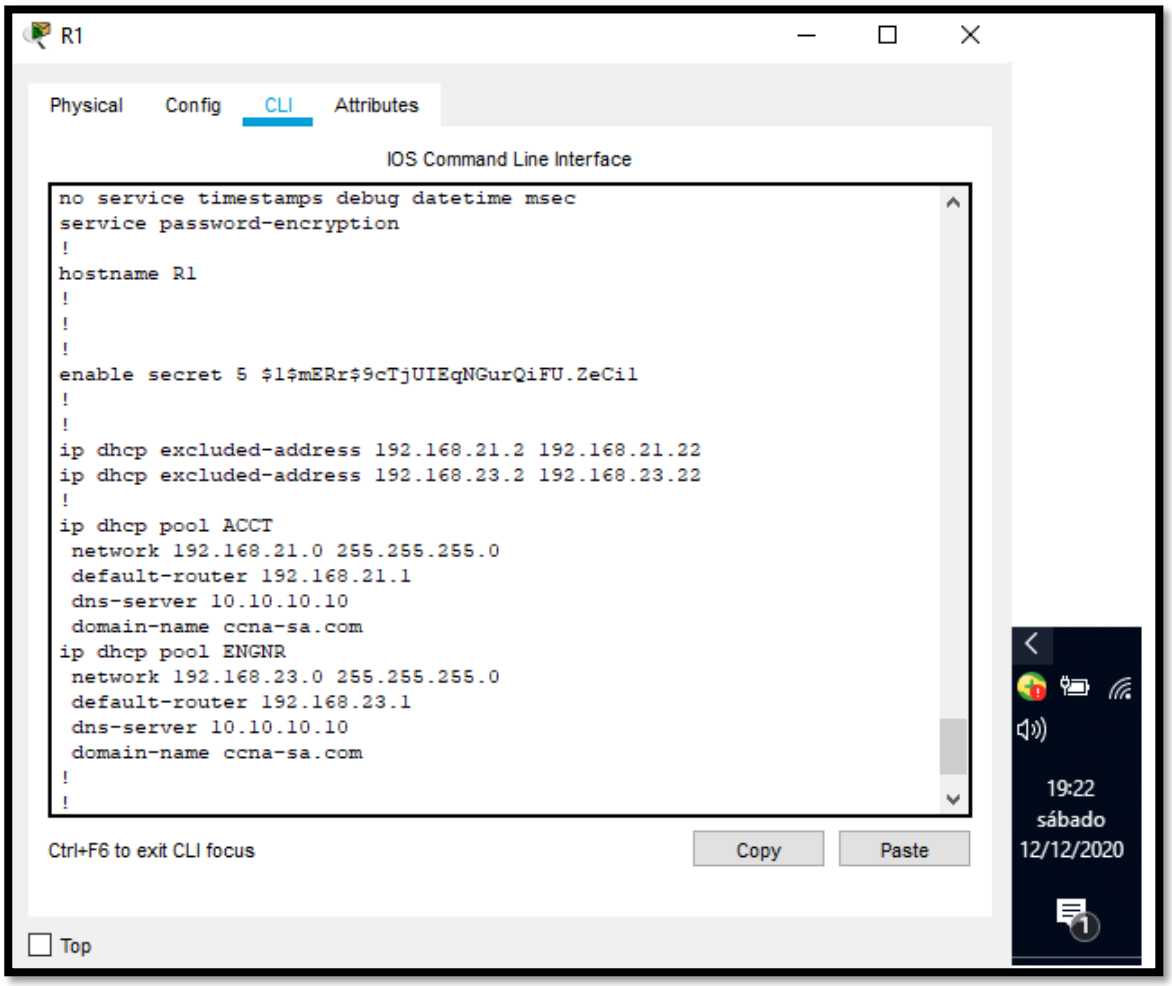
Las tareas de configuración para R1 incluyen las siguientes:

Para esta parte se creo un rango de direcciones ip para poder configurar el direccionamiento DHCP para los Host que están en la topología, el primero se crea para la Vlan 21 que corresponde al área de contabilidad y el segundo grupo corresponde al área de a la Vlan 23 de ingeniería,

Tabla 28. Configuración de servidor de DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.2 192.168.21.22
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.2 192.168.23.22
Crear un pool de DHCP para la VLAN 21. • Nombre: ACCT • Servidor DNS: 10.10.10.10 • Nombre de dominio: ccna-sa.com • Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23 • Nombre: ENGNR • Servidor DNS: 10.10.10.10 • Nombre de dominio: ccna-sa.com • Establecer el gateway predeterminado	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

Figura 39. Show running-config



Fuente: Autor

Configuración de dhcp pool en R1

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

La configuración del R2 incluye las siguientes tareas:

La **NAT** es un tipo de enmascaramiento de las direcciones IP que tengamos en nuestra red interna, sirve principalmente para cambiar nuestra dirección IP de nuestros equipos una vez que llegan al router salgan hacia la internet para evitar cualquier tipo de amenaza de seguridad que puedan ocasionar terceros.

Esta configuración se realiza con el fin de que los dispositivos cambien su dirección ip una vez llega al Router y se dirige hacia la red pública, esto con el fin de proteger

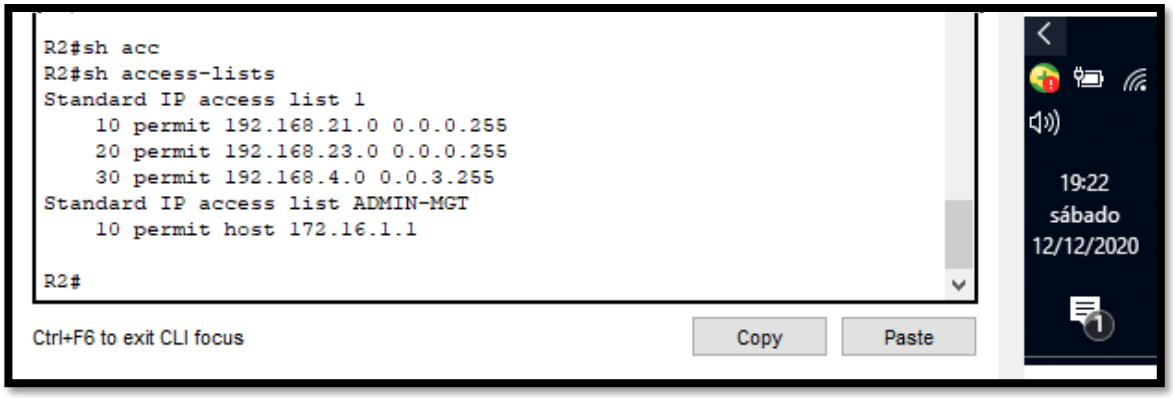
nuestros equipos y evitar posibles hackeos por parte de terceros exponiendo nuestras direcciones ip internas.

Tabla 29. Configuración de NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario • Nombre de usuario: webuser • Contraseña: cisco12345 • Nivel de privilegio: 15	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	(No aplica en Paket Tracer)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	(No aplica en Paket Tracer)
Crear una NAT estática al servidor web. • Dirección global interna: 209.165.200.229	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int loopback 0 R2(config-if)#ip nat outside R2(config-if)#exit R2(config)#int S0/0/0 R2(config-if)#ip nat in R2(config-if)#ip nat inside R2(config-if)#int S0/0/1 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada • Lista de acceso: 1 • Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 • Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	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. • Nombre del conjunto: INTERNET • El conjunto de direcciones incluye: • 209.165.200.225 – 209.165.200.228	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	R2(config)#ip nat inside source list 1 pool INTERNET

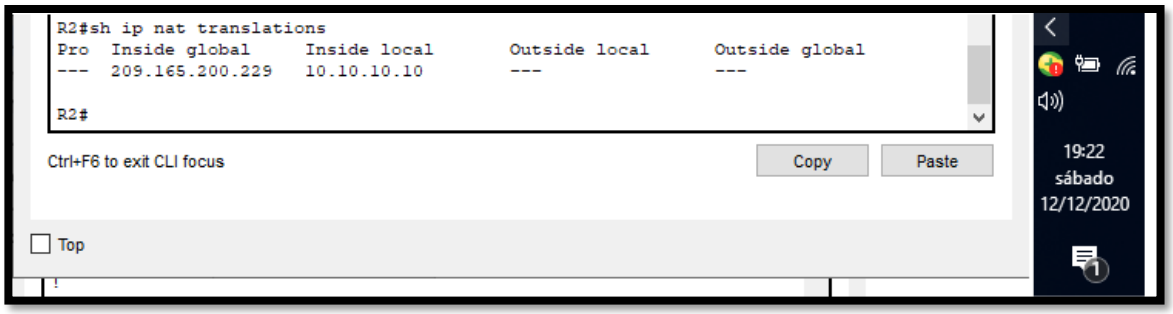
Figura 40. Show Access-lists



Fuente: Autor

Aquí podemos ver la lista de control de acceso creada

Figura 41. Show ip nat translations



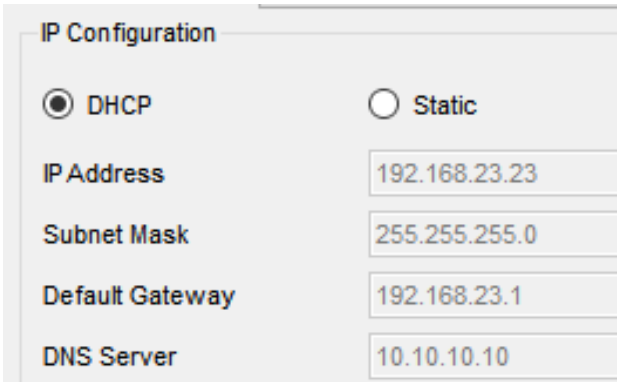
Fuente: Autor

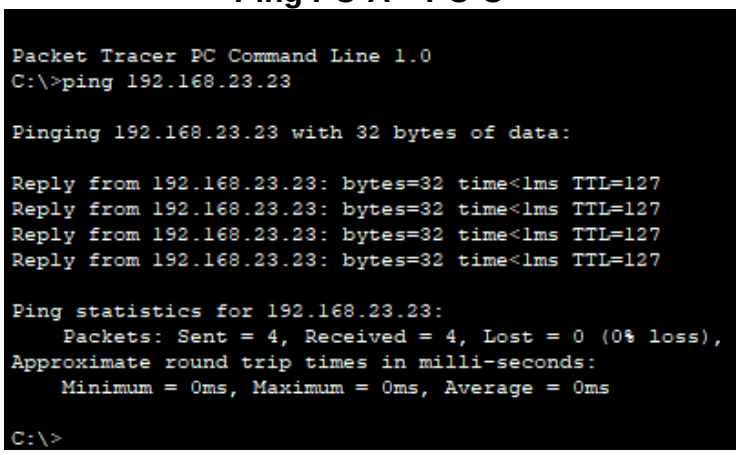
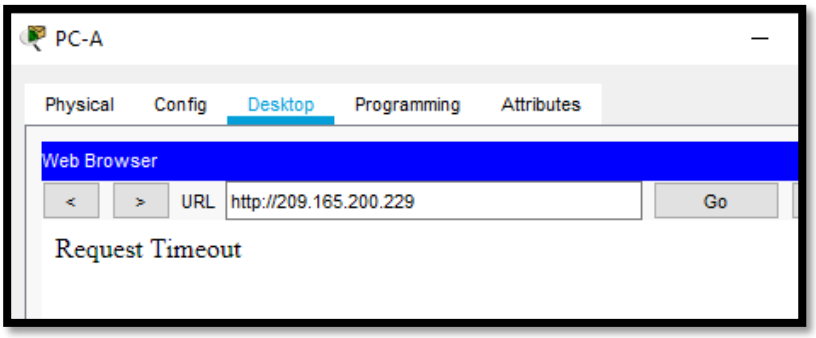
Dirección ip Nat creada para la traducción de ip interna, para cuando salga al exterior (internet), para buscar cualquier tipo de solicitud

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 30. Verificar el protocolo DHCP y la NAT estática -PCs

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**DHCP – PC-A**  *Fuente: Autor*
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**DHCP – PC-C**  *Fuente: Autor*

Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	**Ping PC-A – PC-C**  *Fuente: Autor*
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	(No se puede realizar este paso ya que packet tracer no soporta comandos para http en routers.) **Falla de conexion – Servidor web**  *Fuente: Autor*

Parte 6: Configurar NTP

En esta parte realizaremos algunas configuraciones básicas como la fecha y hora, activamos el NTP para sincronizar los relojes de los sistemas informáticos a través del enrutamiento, activamos las actualizaciones periódicas

Tabla 31. Configuración de NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. • 5 de marzo de 2016, 9 a. m.	R2#clock set 09:00:00 05 mar 2016

Configure R2 como un maestro NTP. • Nivel de estrato: 5	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. • Servidor: R2	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#sh ntp associations …. R1#sh clock detail 9:11:26.714 UTC Sat Mar 5 2016 Time source is NTP

Nota: cómo podemos observar la configuración de la fecha y hora que realizamos en el R2 automáticamente se actualizo en el R1 una vez aplicamos las configuraciones NPT

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

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

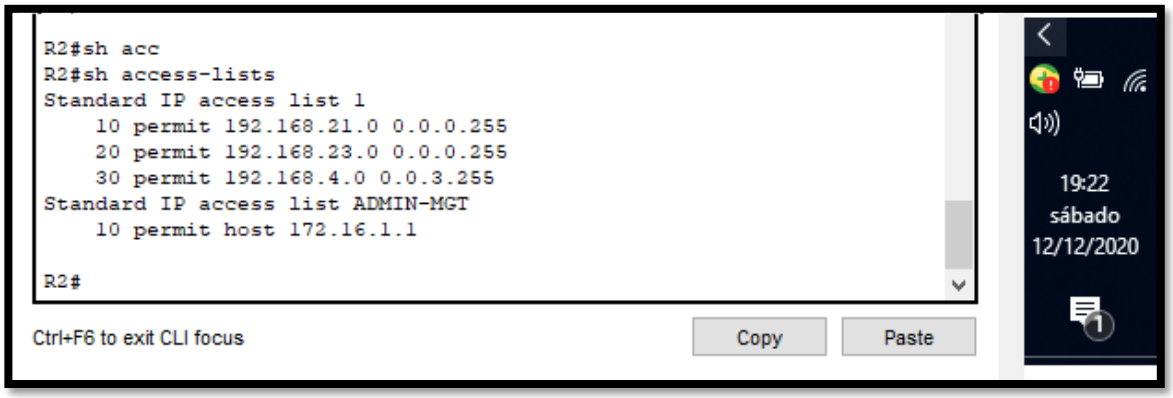
en esta parte debemos crear las **ACL** para permitir que ciertos dispositivos puedan acceder a los quipos que configuremos, en el caso de un administrador de red pueda obtener acceso remoto a el Router y pueda realizar las configuraciones requeridas.

Tabla 32. Configuración de ACL

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 • Nombre de la ACL: ADMIN-MGT	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet

Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...Open Se prohibe el acceso no autorizado User Access Verification Password:

Figura 42. Show Access-lists



Nos muestra la lista de acceso configuradas en R2

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

En esta parte podemos llevar un control de los accesos que tengan cada usuario a la red, como podemos observar en esta parte hay un total de 4 accesos realizados desde las distintas redes que tenemos configuradas.

Tabla 33. Verificación de ACL

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#sh access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 (2 match(es)) 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (4 match(es))
Restablecer los contadores de una lista de acceso	R2#clear access-list counters

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#sh ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#sh ip nat translations tcp 209.165.200.225:1025192.168.21.23:1025 209.165.200.229:80 209.165.200.229:80
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation *

Como podemos observar con el comando **clear** podemos reiniciar las listas de acceso para poder llevar un control periódico de los ingresos de todos los usuarios que se encuentren conectados, además podemos observar la lista de traducciones de NAT el cual es la IP que utilizan nuestro pc en internet.

CONCLUSIONES

Finalmente se logra cumplir con el principal objetivo de la actividad que fue la configuración correcta de las dos topologías dadas, configurando toda la red basándonos en la tabla de direccionamiento entregada para el desarrollo de esta actividad.

Este trabajo nos sirvió como base para tener muchos más claros algunos conceptos y su aplicación dentro de una red real, aprendimos conceptos muy importantes como por ejemplo las configuraciones básicas de seguridad para los dispositivos de capa 2 y de capa 3, para evitar que un intruso pueda acceder fácilmente a nuestra red y modificar nuestras configuraciones, creando y encriptando todas las contraseñas, se aprendieron conceptos como las vlans que son muy importantes dentro de la red ya que nos permite proteger y limitar el acceso entre una red u otra por temas de seguridad, se aprendieron temas de enrutamiento estático y dinámico y las ventajas que se tiene en utilizar uno u otro, temas como el DHCP que nos permite la utilización de direcciones Ip de forma automática, la configuración de los enlaces troncales que es la vía la cual nos permite la comunicación entre una red distinta, prendimos sobre la listas de control de acceso (ACL) la cual nos permite bloquear el tráfico de las direcciones especificas dentro de la red.

Se logro conocer acerca del tema de NAT, que nos sirve principalmente para la encapsulación de direcciones IP que salen de nuestra red interna hacia el internet, también estudiamos el tema de direccionamiento DHCP que nos permite principalmente la adquisición de direcciones IP de forma automática para todos los hosts que se encuentren conectados en la red. Con el tema de las Vlans aprendimos a dividir las redes en pequeñas subredes que nos permitan mejorar el tema de la seguridad y direccionamiento de los datos y se trabajo el tema de las ACL que nos sirven principalmente para mejorar la seguridad en creando listas de accesos y evitando ataques via remota que puedan vulnerar la seguridad de nuestra red.

BIBLIOGRÁFIA

CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

UNAD (2017). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgTCtKY-7F5KIRC3

ANEXOS

Anexo 1

Enlace del archivo de simulación escenario 1:
https://drive.google.com/drive/folders/1SU14vhDgBr0oruksN5YmliBE7m0Z3BX-?usp=sharing

Anexo 2

Enlace del archivo de simulación escenario 2:
https://drive.google.com/drive/folders/1tHkO-NtnCMbXoiwKvpXGPgBDz8vFDnZ_?usp=sharing

Anexo 3

Articulo Científico:
https://drive.google.com/file/d/1tkJR5mjowMkgHrTQenzz_EsWTJLCadez/view?usp=sharing