SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

JOHN ANDERSON SARMIENTO

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

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

JOHN ANDERSON SARMIENTO

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

DIRECTOR: DIEGO EDINSON RAMIREZ CLAROS
INGENIERO ELECTRÓNICO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRONICA
MOSQUERA
2.020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

MOSQUERA, 30 noviembre de 2020

Contenido

Lista de tablas

Lista de figuras

Glosario

Dirección IP: son un conjunto de números con los cuales se identifica de manera lógica y jerárquica los equipos que están conectados en una red de datos.

Router: en ingles router que traducido seria encaminador, es un dispositivo de red sirve para interconectar computadoras que funcionan en una red, estableciendo la ruta para conectarse con otra de y poder enviar paquetes de datos.

Switch: que traducido al español es interruptor, conmutador es un dispositivo que permite interconectar equipos en una red de datos, trabaja en la capa de enlace de datos y permite interconectar dos o más equipos de una red permitiendo pasar datos de un segmento a otro.

VLAN1: es una interfaz que se usa en el switch, la cual es nativa del switch, y a la que se le asigna una dirección ip para poder administrar el dispositivo remotamente

IPv4: (Protocolo de Internet versión 4), el cual está formado de 32 bits separad en cuatro octetos que son cada uno compuestos de 8 bits, y que se usa en una notación decimal separados por puntos.

IPv6: es una actualización del protocolo IPv4, este tiene un tamaño de 128 bits el cual se separa ocho campos de 16 bits, separado por dos puntos.

SDM: Viene de las siglas (Switching Database Manager), son plantillas de Cisco, con las cuales se puede configurar los switches para poder sacarle el mayor rendimiento, en función de lo que vayan a trabajar

OSPF: De la sigla en inglés Open Shortest Path First que traducen abrir el camino más corto primero, es un protocolo de red para realizar encaminamiento jerárquico de pasarela interior o Interior Gateway.

NAT: el cual significa traducción de direcciones de red y se conoces como enmascaramiento de Ip, se usa en los router para conservar direcciones IP, logrando que se conecten a Internet las redes de con Ip privada.

NTP: de las siglas en ingles Network Time Protocolo, es un protocolo de Internet que se usa para sincronizar los relojes o horas de los dispositivos que componen la red por medio del enrutamiento de paquetes en redes con latencia variable

DHCP: de las siglas en ingles Dynamic Host Configuration Protocol, es un protocolo que sirve para poder asignar ip a los equipos automáticamente.

ACL: de las siglas en ingles access control list, el cual consiste en controlar el flujo del tráfico en equipos de redes filtrando el tráfico para permitir o denegar el tráfico de red de acuerdo a alguna condición o listas creadas.

HTTP: que traduce protocolo de transferencia de hipertexto, el cual es un protocolo de comunicaciones que permite las transferencias de información en la World Wide Web o internet.

Router-on-a-Stick: Consiste en crear interfaces virtuales sobre un puerto físico del router para que atreves de cada interfaz se pueda se pueda transmitir información de una vlan, cuando no se usa Router-on-a-Stick es necesario que por cada vlan se use un puerto físico, esto es un inconveniente pues los router no tiene muchas interfaces.

Enlace troncal o trunk: es la configuración que se le realiza a una interfaz ya sea de un switches o un router para que por este se pueda enviar y recibir el tráfico de las distintas VLANs que se han configurado,

Dot1q: es un protocolo esencial que le da vida a los enlaces que se han configurado como troncal o trunk y pertenece al estándar IEEE 802.1Q.

Vlan Nativa: es una Vlan que se configura para transportar tráfico sin etiquetar o tráfico que no se encapsula 802.1Q, el número de la vlan nativa deber ser igual en ambos extremos de la conexión de los switches o router.

EtherChannel: es una tecnología con estándares 802.3 que permite full-dúplex Fast Ethernet, y con el cual se puede agrupar lógicamente varias interfaces físicas que son tratadas como un único enlace sumando la velocidad nominal de cada puerto físico y enlace troncal de alta velocidad, también sirve como una conexión de respaldo.

Resumen

Se desarrollara el escenario 1 de la prueba de habilidades en el cual se pondrá en práctica los conocimientos adquiridos en el desarrollo del diplomado de profundización Cisco el cual está fundamentado en CCNA que es una certificación Cisco Certified Networking Associate, donde se tendrá que configurar los dispositivos de red con unos parámetros establecidos por la guía, dichos dispositivos será un router con el que se realizar el enrutamiento necesario y dos switches los cuales permitirán montar una red para que haya conectividad en entre dos equipos.

En la segunda actividad se pondrá en práctica los conceptos aprendidos durante el desarrollo de segundo ciclo de CISCI CCNA, donde se abordó y enseño temas como el protocolo OSPF que nos permite compartir y actualizar las tablas de ruteo con los rutes vecinos siempre y cuando todos tengan activo el protocolo OSPF,
El protocolo NTP que se usa para sincronizar los relojes o horas de los dispositivos que componen la red, NAT que nos ayuda a traducir las direcciones de la red permitiendo que los equipos con ip privadas puedan conectarse con los equipos que tiene Ip públicas, ACL que son listas de control de acceso y nos ayudan a controlar el tráfico los paquetes en equipos de redes filtrando el tráfico para permitir o denegarlo, todo esto será aplicado en la segunda parte de la actividad

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

Abstract

Scenario 1 of the skills test will be developed in which the knowledge acquired in the development of the Cisco in-depth diploma will be put into practice, which is based on CCNA, which is a Cisco Certified Networking Associate certification, where the devices will have to be configured network with some parameters established by the guide, these devices will be a router with which the necessary routing will be carried out and two switches which will allow to set up a network so that there is connectivity between two computers.

In the second activity, the concepts learned during the development of the second cycle of CISCI CCNA will be put into practice, where topics such as the OSPF protocol that allows us to share and update the routing tables with neighboring routes as long as everyone has I activate the OSPF protocol,
The NTP protocol that is used to synchronize the clocks or hours of the devices that make up the network, NAT that helps us to translate the network addresses, allowing computers with private IPs to connect with computers that have public IPs, ACL that They are access control lists and help us to control the traffic of the packets in network equipment by filtering the traffic to allow or deny it, all this will be applied in the second part of the activity

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics

Introducción

Las rede de datos cada vez está más integradas en nuestra vida por lo cual hace que todo futuro ingeniero enfocado al área de la informática sepa cómo funciona una red de datos y que elementos conforman una red de datos y como se debe configurar dichos elementos, de ahí la importancia que tiene para nuestro futuro profesional al culminación y aprobación del diplomado de profundización Cisco, donde se aprende a conocer las características, funcionamiento y aplicación de una red de datos.

Con el desarrollo de la actividad propuesta para el escenario se desea poner a prueba los conocimientos adquiridos durante el diplomado de profundización Cisco, nuestro análisis ante una situación como es la de montar una red de datos con una topología en dada y una configuración ya definida la cual se debe poner en practica con packet tracer.

En el escenario 1 se debe configurar un switch y un router desde el inicios empezando por asignar nombre, una dirección Ipv4 y Ipv6 a las interfaces de cada dispositivo, colocar un nivel de seguridad alto, los equipos deben admitir conectividad IPv4 como IPv6 con los pc conectados, colocar una conexión de respaldo por medio de un Ethernetcahnnel con el cual se puede garantizar la redundancia o alta disponibilidad en una conexión de red, también se desea configurar Vlan con lo cual es crean redes lógicas que ayudan a reducir el tamaño del dominio de difusión y para los administradores de redes les facilita la administración redes de gran tamaño, separando segmentos lógicos de una red de área local lo que permite también mejorar el nivel de seguridad de la red separando el tráfico.

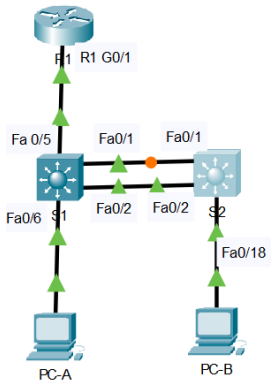
También se aplicaran conceptos como NAT que nos permite traducir las direcciones ipv4 privadas de las redes LAN para que se puedan comunicar con las Ipv4 públicas que se encuentran en internet, otra de las configuraciones en los rotues es la de OSPF que es un protocolo con el cual los routers que estén configurados puedan compartir sus tablas de ruteo para poder encontrar la mejores rutas en el momento que se tenga que enviar los paquetes por la red, el portocolo NTP que nos ayuda a mantener actualizada la horas en los equipos evitando que los administradores tengan que realizar este proceso manualmente y encada dispositivo de red y las ACL que son listas que se realizan para controlar el tráfico de la red filtrándolo y según la configuración realizada permite o niega el acceso.

Desarrollo

Escenario 1

Descripción de escenarios propuestos para la prueba de habilidades

Figura 1Topología



Fuente: Topología que se debe montar para la practica

En este escenario solicitan que los dispositivos de una red pequeña puedan admitir tanto la conectividad IPv4 como IPv6 para los Pc conectados, tanto el router como los dos switch deben administrarse de forma segura, configurando 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 2Tabla de asignación de direcciones

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

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

Tabla 3 Paso 1: Inicializar y volver a cargar el router y el switch

Tarea	Especificación
Se borra configuración R1	Router#erase startup-config
Se vuelve a cargar R1	Router #reload
Se borra configuración S1	Switch#erase startup-config
Se vuelve a cargar S1	Switch#reload
Se borra configuración S2	Switch#erase startup-config
Se vuelve a cargar S2	Switch#reload

Ante todo, siempre que se vaya a configurar un dispositivo de conexión en red de datos nueva se debe borrar la configuración de inicios para que no nos presente problemas más adelante o durante la configuración por tener otros parámetros ya configurados

Tabla 4 Configurar la plantilla SDM

Tarea	Especificación
Configurar la plantilla SDM S1	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Configurar la plantilla SDM S2	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default

Ahora se debe configurar la plantilla SDM para que nuestro switch admita IPv6 como los solicita el escenario propuesto, están plantillas son templates propiedad de Cisco con las cuales se puede llegar a configurar los switch de forma tal que se le saque un mayor rendimiento, dependiendo el uso que se la vaya a dar a switch logrando sacar el mayor rendimiento al dispositivo

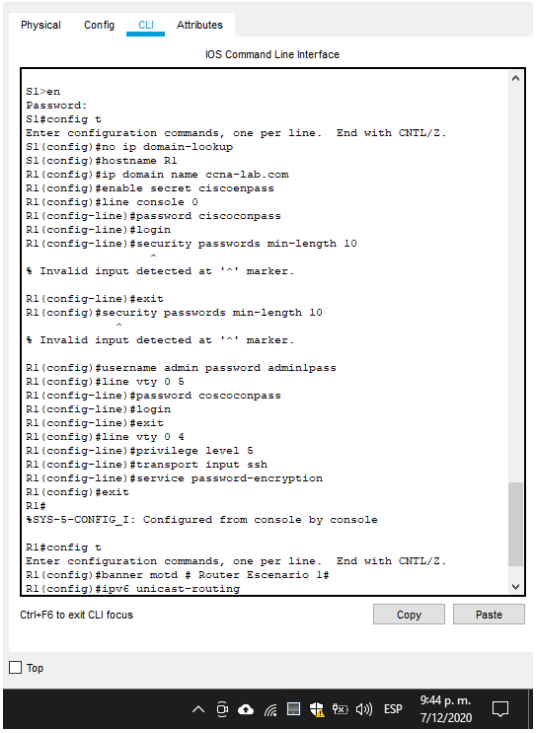
Paso 2: Configurar R1

Tabla 5 Tareas para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1(config-line)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config-line)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 5 R1(config-line)#password coscoconpass R1(config-line)#login R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config-line)#line vty 0 4 R1(config-line)#privilege level 5 R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd # Router Escenario 1#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config-if)#interface g0/0 R1(config-if)#description Red LAN R1(config-if)#ip address 10.19.8.1 255.255.255.192 R1(config-if)#ipv6 address 2001:db8:acad:a::1/6 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shutdown

Configure el Loopback0 interface	R1(config-if)#description lookback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa general-keys modulus 1024

Figura 2 Configuración Básica R1



Fuente: Autor

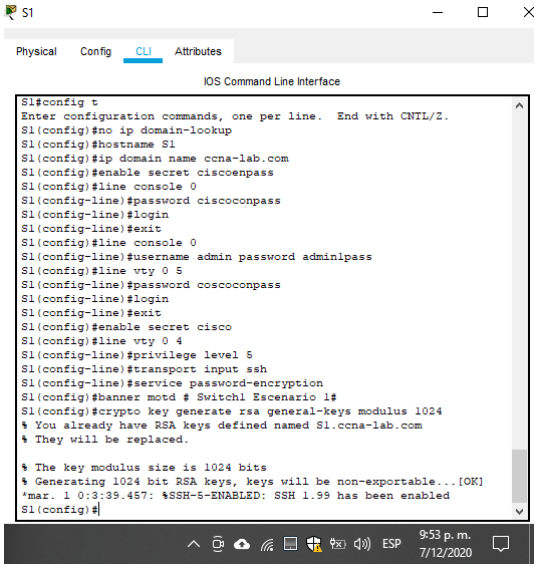
Cuando se va a configurar un router siempre se debe una configuración básica en la que se debe colocar un nombre para para poder lo ubicar en la red, darle seguridad colocando una contraseña mode EXEC, desactivar DNS, bloque las conexiones remotas no seguras, configurar las interfaces y encriptar las contraseñas todo esto se debe realizar en interfaz de línea de comando (CLI) con los siguientes comandos

Paso 3: Configure S1 y S2.

Tabla 6 Tareas de configuración switch 1-2

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	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config-line)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 5 S1(config-line)#password coscoconpass S1(config-line)#login S1(config-line)#exit S1(config)#enable secret cisco
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#privilege level 5 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd # Switch1 Escenario 1#
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	S1(config-if)#description VLAN4 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 S1(config-if)#no shutdown S2(config)#int vlan 4 S2(config-if)#description VLAN4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#ip default-gateway 10.19.8.97 S2(config-if)#no shutdown
Configuración del gateway predeterminado	S1(config-if)#ip default-gateway 10.19.8.97

Figura 3 Configuración Básica S1



Fuente: Autor

A l igual que se realizó con el router también en un switch siempre se debe realizar una configuración inicial básica para darle la seguridad necesaria al dispositivo, configurar las interfaces, asignarle un nombre, desactivar DNS, conexiones remotas no seguras, asignar la Gateway predeterminada

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

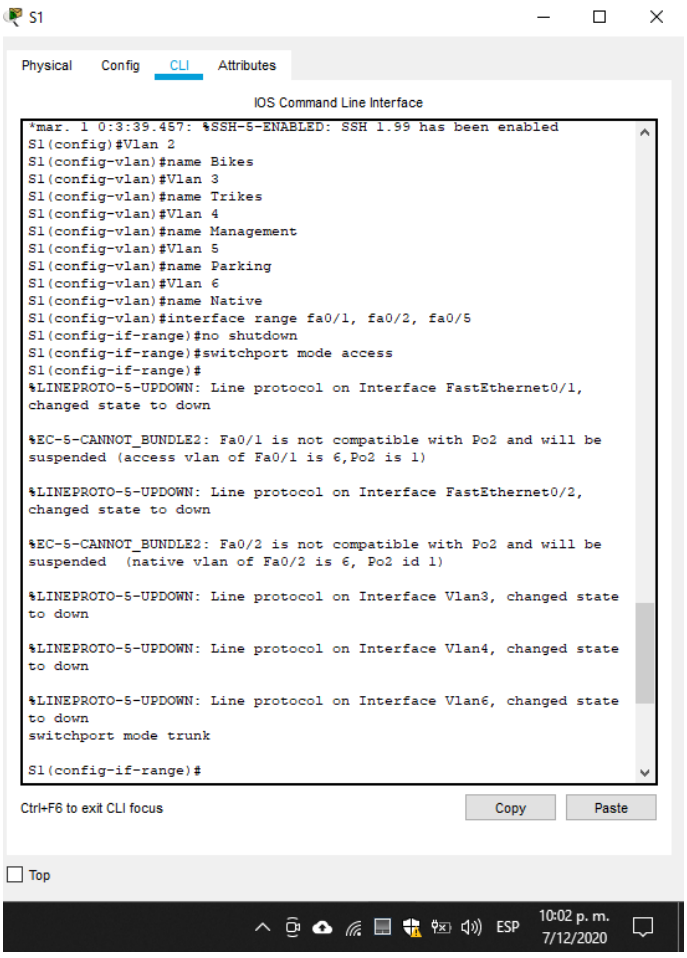
Paso 1: Configurar S1

Tabla 7 Configuración para 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)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	S1(config-if)#interface range fa0/1, fa0/2, fa0/5 S1(config-if-range)#no shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if)#interface range fa0/1,fa0/2 channel-group 2 mode active
Configurar el puerto de acceso de host para VLAN 2	S1(config)#int fa 0/6 S1(config-if)#no shutdown S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1(config)#int fa0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config)#int range fa 0/3-4 S1(config-if-range)#shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport acces vlan 5 S1(config)#int range fa 0/7-24 S1(config-if-range)#shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5

Figura 4 Configuración Vlan y tunk S1



Fuente: Autor

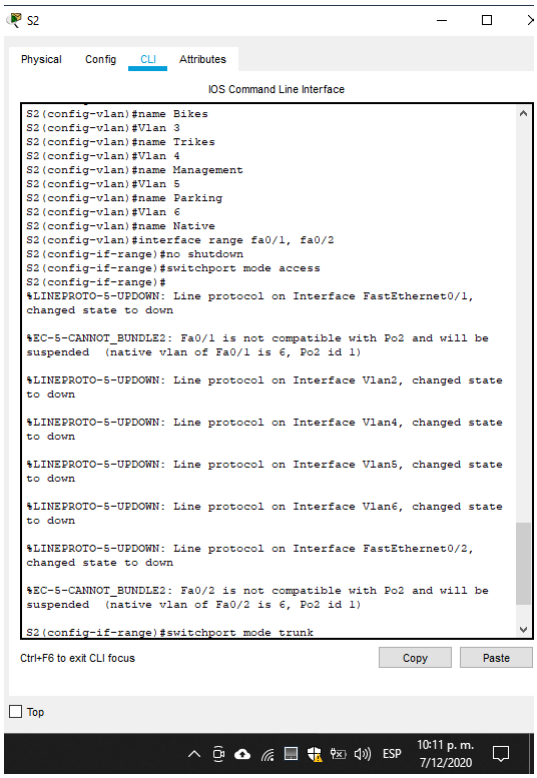
Después de realizar la configuración básica se procede a realizar la configuración ya la configuración detallada dependiendo su entorno y funciones que realizara, para este caso se debe crear las vlan solicitadas en la guía, asignarle un nombre a cada vlan, Crear troncales 802.1Q y asignar la vlan nativa que se va a usar, para nuestro caso en especial se creara un grupo de puertos EtherChannel que solicita la guía, se le asigna que puertos van a trabajar sobre unas vlan ya creadas, configurar la seguridad en los puertos de acceso y proteger las interfaces no utilizadas, todo esto se realizara con los siguientes comandos en la interfaz de línea de comando (CLI)

Paso 2: Configure el S2.

Tabla 8 Configuración para Vlan y trunk S2

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)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	S2(config-if)#interface range fa0/1, fa0/2 S2(config-if-range)#no shutdown S2(config-if-range)#switchport mode access S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if)#switchport trunk encapsulation dot1q
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface range fa0/1, fa0/2 S2(config-if-range)#channel-group 2 mode passive
Configurar el puerto de acceso del host para la VLAN 3	S2(config)#int fa0/18 S2(config-if)#no shutdown S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config)#int fa 0/18 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config)#int range fa 0/3-17, fa 0/19-24, G 0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description puertos sin usa

Figura 5 Configuración para Vlan y trunk S2



Fuente: Autor

Al igual que se hizo con el switch uno1 con el switch dos se procede a realizar la configuración solicitada por la guía como es crear las vlan que se usaran en este switch, asignarle un nombre a cada vlan creada, crear troncales 802.1Q y asignar la vlan nativa, montar los grupos de puertos EtherChannel que estarán en el otro extremo y para este caso se configura modo pasivo, se le asigna que puertos con las vlan, se asegura los puertos que no se usaran, todo esto se realizara con los siguientes comandos en la interfaz de línea de comando (CLI)

Parte 3: Configurar soporte de host

Paso 1: Configure R1

Tabla 9 Configuración para R1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback0 R1(config)#ipv6 route ::/0 Loopback0

Configurar IPv4 DHCP para VLAN 2	R1(dhcp-config)#ip dhcp pool vlan2 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
Configurar DHCP IPv4 para VLAN 3	R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-a.net

Para finalizar la configuración se debe configurar en el Router las turas predeterminadas tanto para IPv4 como para IPv6 con las que se dirigirán el tráfico a la interfaz Loopback 0, también se debe crear un grupo DHCP para la Vlan2 y también para la Vlan3.

Paso 2: Configurar los servidores

Tabla 10 configuración para PC-A

PC-A Network Configuration	
Descripción	Datos tomados por DHCP
Dirección física	0009.7C99.96A8
Dirección IP	10.19.8.59
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19 .8.1
Gateway predeterminado IPv6	FE80::1

En los equipos finales como PC-A y PC-B se debe realizar la configuración tanto Ipv4 como Ipv6 para que pueda estar en el mismo segmento de red y poder tener comunicación tanto entre ellos mismo como con los demás dispositivos de red configurados.

Parte 4: Probar y verificar la conectividad de extremo a extremo

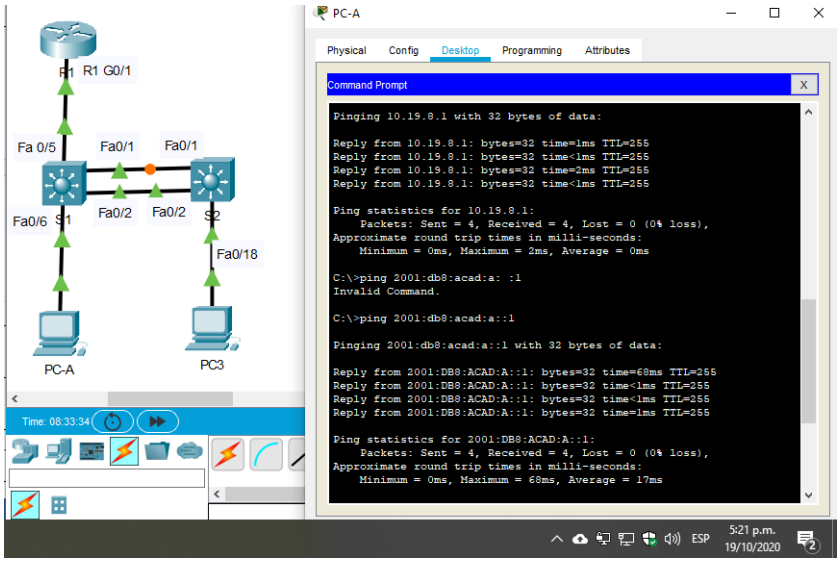
Tabla 11 Prueba de conectividad

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Si hay conexión
		IPv6	2001:db8:acad:a: :1	Si hay conexión
	R1, G0/0/1.3	Dirección	10.19.8.65	Si hay conexión
		IPv6	2001:db8:acad:b: :1	Si hay conexión
	R1, G0/0/1.4	Dirección	10.19.8.97	Si hay conexión
		IPv6	2001:db8:acad:c: :1	Si hay conexión
	S1, VLAN 4	Dirección	10.19.8.98	No hay conexión

		IPv6	2001:db8:acad:c: :98	Si hay conexión
	S2, VLAN 4	Dirección	10.19.8.99.	No hay conexión
		IPv6	2001:db8:acad:c: :99	Si hay conexión
PC-A	PC-B	Dirección	10.19.8.85	Si hay conexión
		IPv6	2001:db8:acad:b: :50	Si hay conexión
	R1 Bucle 0	Dirección	209.165.201.1	Si hay conexión
		IPv6	2001:db8:acad:209: :1	Si hay conexión
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Si hay conexión
		IPv6	2001:db8:acad:209: :1	Si hay conexión
	R1, G0/0/1.2	Dirección	10.19.8.1	Si hay conexión
		IPv6	2001:db8:acad:a: :1	Si hay conexión
	R1, G0/0/1.3	Dirección	10.19.8.65	Si hay conexión
		IPv6	2001:db8:acad:b: :1	Si hay conexión
	R1, G0/0/1.4	Dirección	10.19.8.97	Si hay conexión
		IPv6	2001:db8:acad:c: :1	Si hay conexión
	S1, VLAN 4	Dirección	10.19.8.98	Si hay conexión
		IPv6	2001:db8:acad:c: :98	Si hay conexión
	S2, VLAN 4	Dirección	10.19.8.99.	Si hay conexión
		IPv6	2001:db8:acad:c: :99	Si hay conexión

Para finalizar es necesario realizar pruebas de conectividad entre los PC-a y los demás dispositivos configurados para verificar que las configuraciones realizadas en el Router, Switch 1 y el switch 2 hayan quedado correctamente logrando la conectividad solicitada en la guía, lo mismo se debe realizar con el PC-B, esta verificación se puede realizar por medio del comando ping.

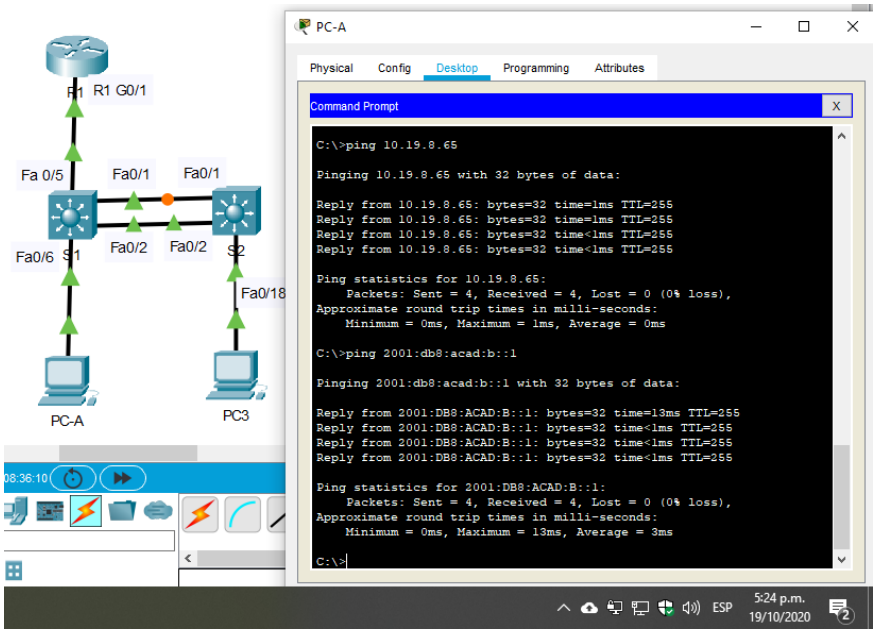
Figura 6 Ping de PC-A a R1, G0/0/1.2



Fuente: Autor

Se inicia command Prompt en el equipo PC-A para se realiza un ping desde el equipo PC-A hacia la interfaz virtual G0/0/1.2 que le pertenece al Router 1, para poder verificar que si tenga conectividad

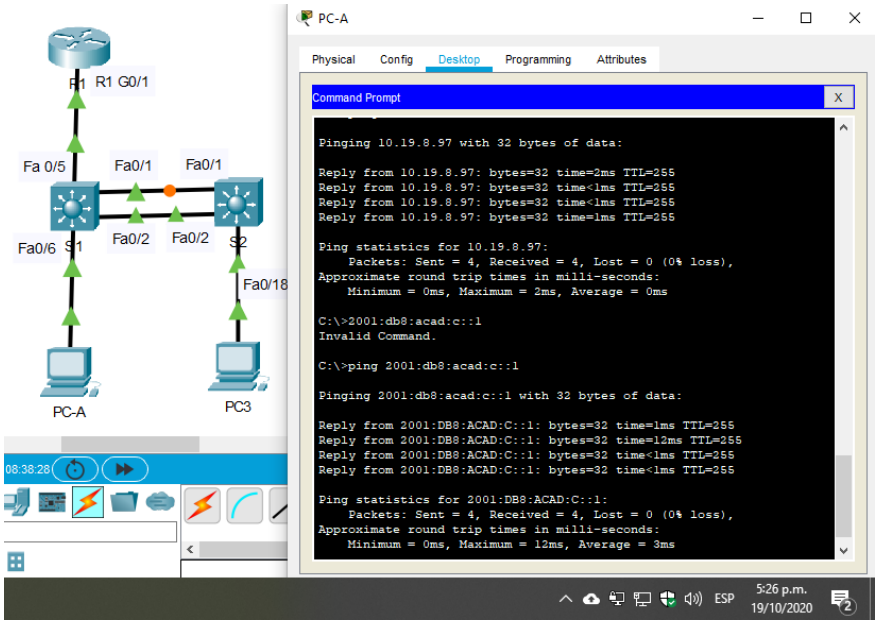
Figura 7 Ping de PC-A a R1, G0/0/1.3



Fuente: Autor

Se inicia command Prompt en el equipo PC-A por medio del comando ping desde el equipo PC-A se verifica conexión con la interfaz virtual G0/0/1.3 que se configuro en el Router 1

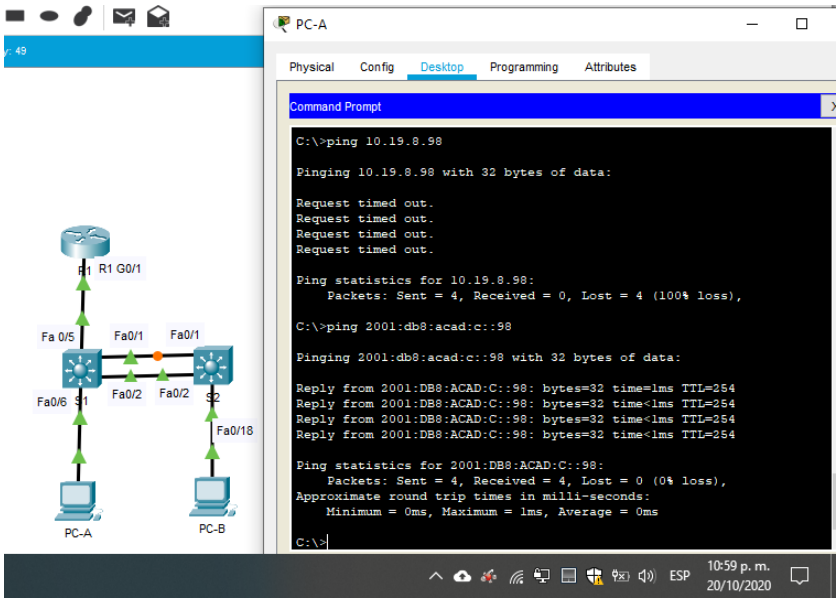
Figura 8 Ping de PC-A a R1, G0/0/1.4



Fuente: Autor

Se inicia command Prompt para realizar pruebas de conexión se realiza un ping desde DOS en el equipo PC-A a las IPV4 e IPV6 que se configuraron en la interfaz virtual G0/0/1.4

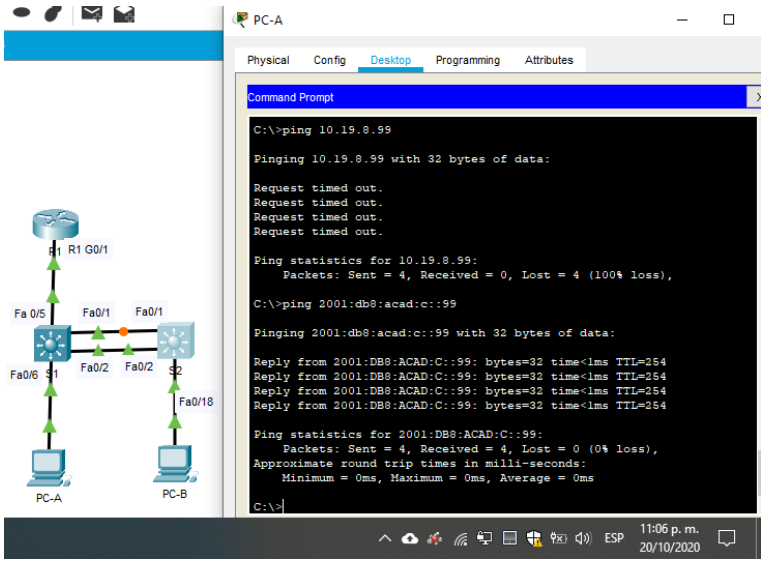
Figura 9 Ping de PC-A a S1, VLAN 4



Fuente: Autor

Se inicia command Prompt para verificar si existe conexión entre el PC-A y la Vlan4 se envía un ping a la ip que se configuraron en las interfaz de Switch 1 ”S1”

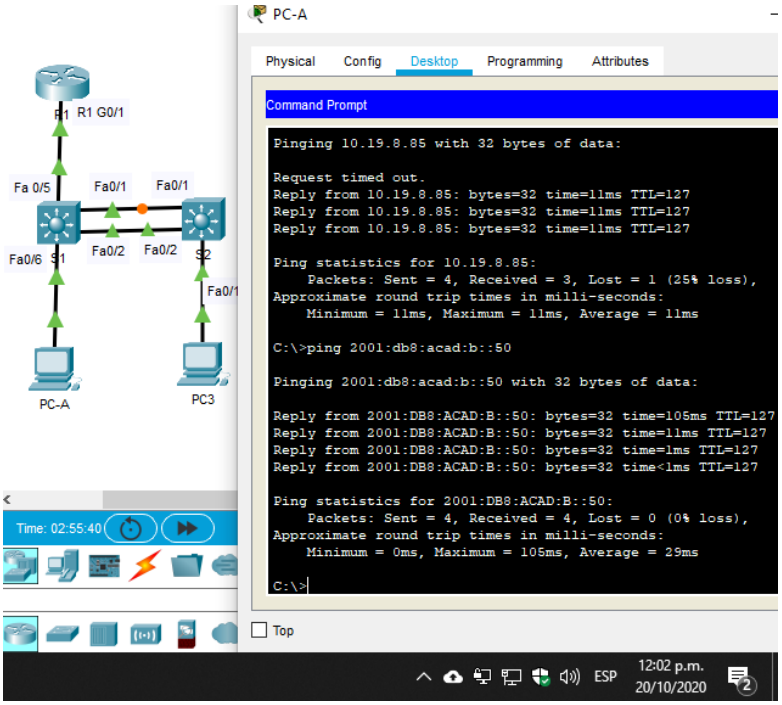
Figura 10 Ping de PC-A a S2, VLAN 4



Fuente: Autor

Se inicia command Prompt para verificar si existe conexión entre el PC-A y la Vlan4 se envía un ping a la ip que se configuraron en las interfaz de Switch ”S2”

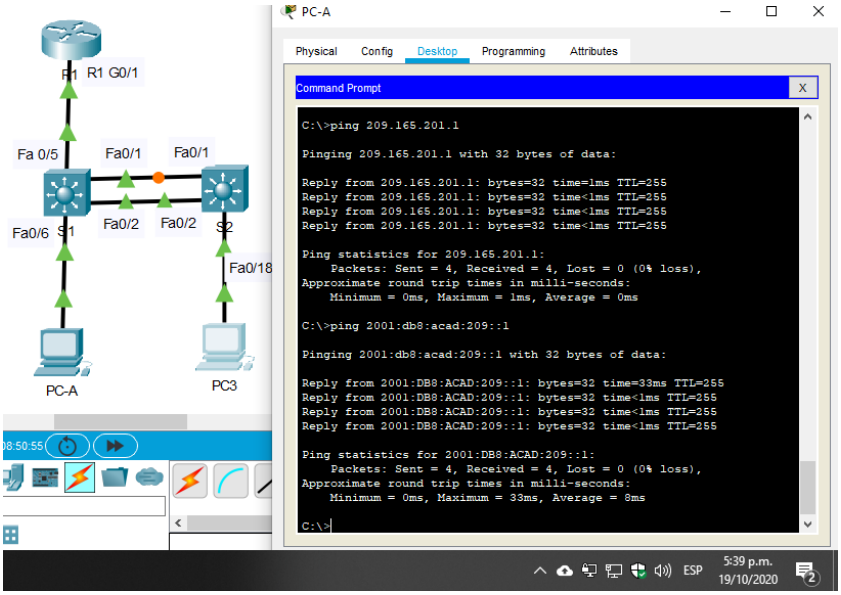
Figura 11 Ping de PC-A a PC-B



Fuente: Autor

Se inicia command Prompt se realiza un ping a 10.19.8.85 y 2001:DB8:ACAD:B::50 para verificar que exista conectividad entre PAC-A y PC-B

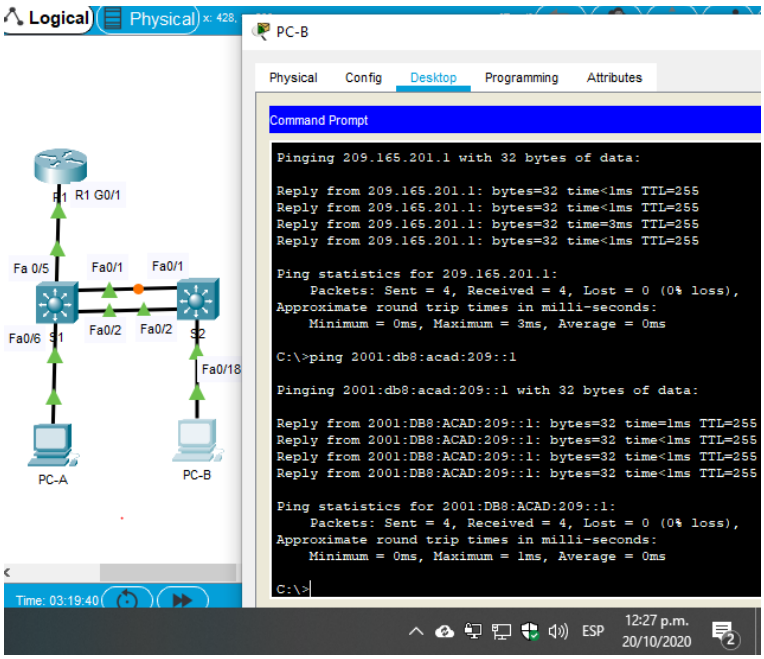
Figura 12 Ping de PC-A a R1 Bucle 0



Fuente: Autor

Se inicia command Prompt se realizar prueba de conexión entre el PC-A y R1 Buble0 o loopback

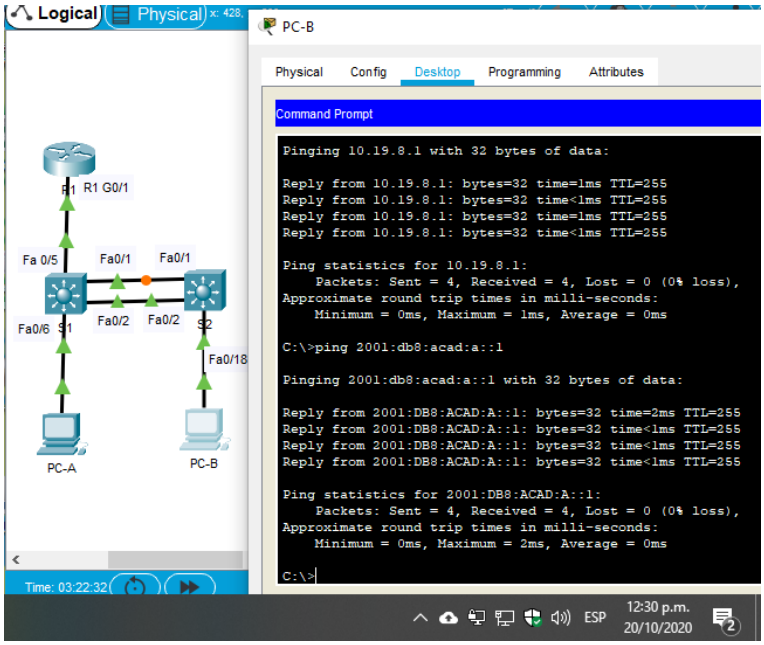
Figura 13 Ping de PC-B a R1 Bucle 0



Fuente: Autor

Se inicia command Prompt se realiza una revisión de conectividad con el comando ping desde PC-B a R1Bucle0

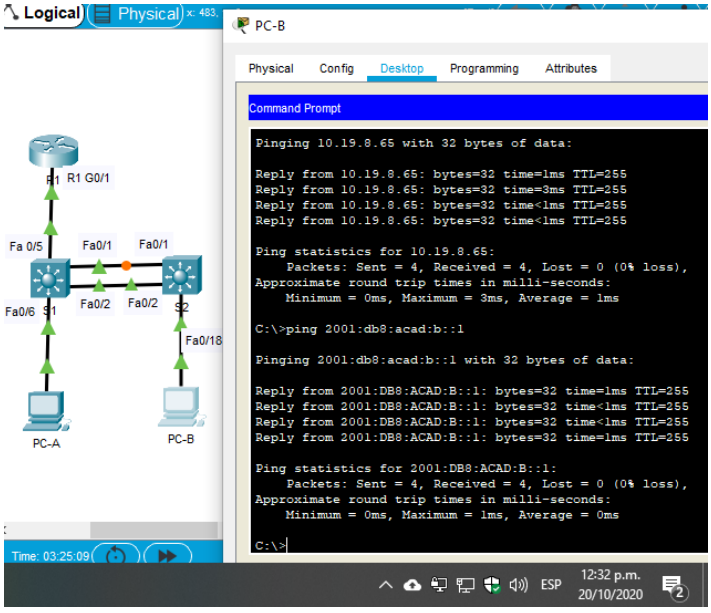
Figura 14 Ping de PC-B a R1, G0/0/1.2



Fuente: Autor

Se inicia command Prompt desde el PC-B se envia un ping a las interfaz configuada en R1, G0/0/1.2

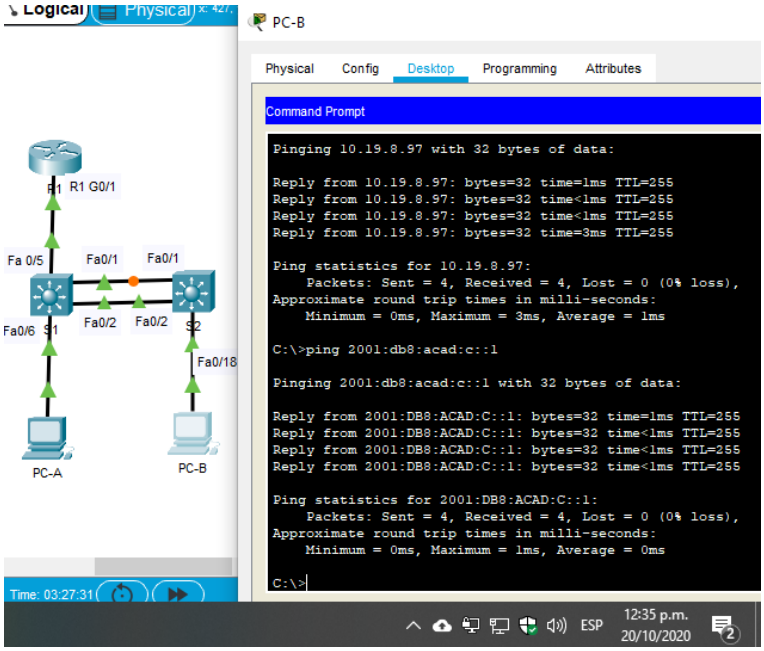
Figura 15 Ping de PC-B a R1, G0/0/1.3



Fuente: Autor

Se inicia command Prompt con el comando Ping desde PC-B se verifica que haya conectividad con la interfaz virtual de R1 G0/0/1.3

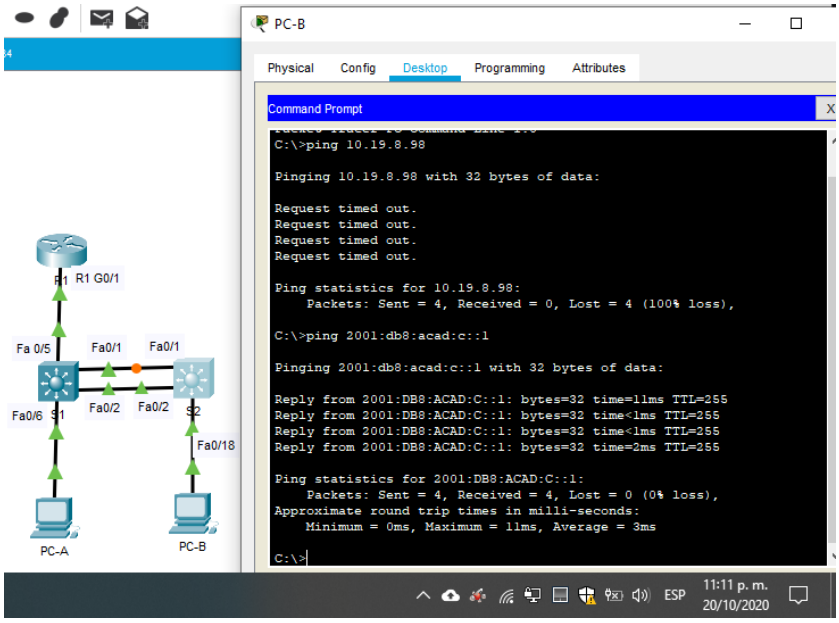
Figura 16 Ping de PC-B a R1, G0/0/1.4



Fuente: Autor

Se inicia command Prompt se ingesa desde a DOS desde PC-B y se envia un ping a las ips configuradas en la interfaz del virtual R1, G0/0/1.4

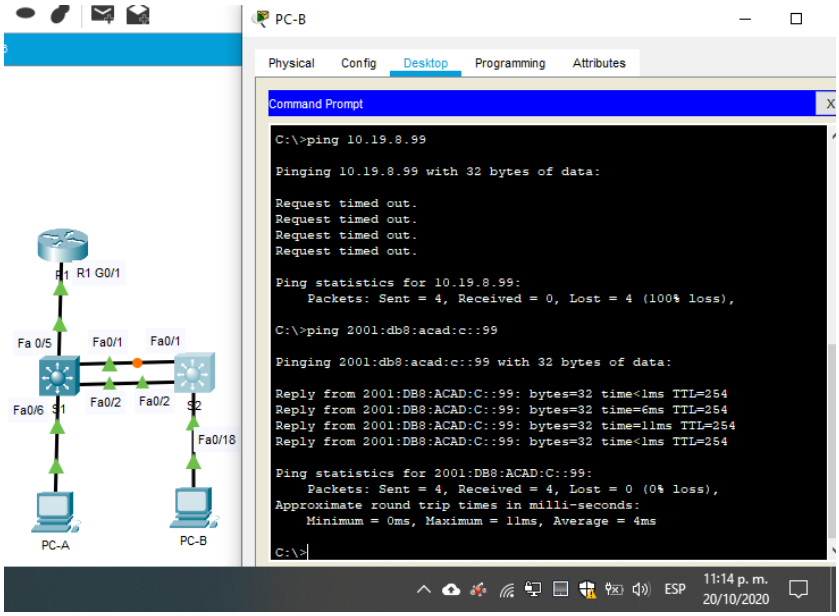
Figura 17 Ping de PC-B a S1, VLAN 4



Fuente: Autor

Se inicia command Prompt se envia Ping para verificar la conectividad entre el PC-B y el switch2

Figura 18 Ping de PC-B a S2, VLAN

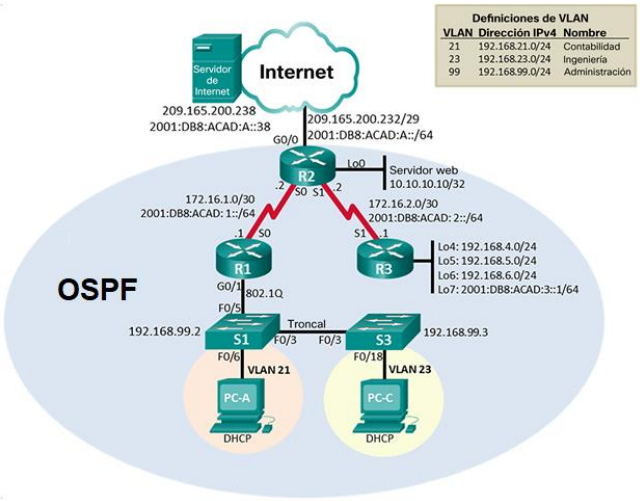


Fuente: Autor

Se inicia command Prompt se envia Ping para verificar la conectividad entre el PC-B y el switch2

Escenario 2

Figura 19 Topología escenario 2



Parte 1: Inicializar dispositivos

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

Tabla 12 Configuración Inicial

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.dat
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 vlan brief

Antes de iniciar cualquier configuración en una red de datos lo primero que se debe hacer es iniciar los dispositivos para poder eliminar todas las configuraciones que se hayan realizado antes y puedan llegar afectar la red que se va a montar.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Tabla 13 Configurar los parámetros básicos de los dispositivos

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

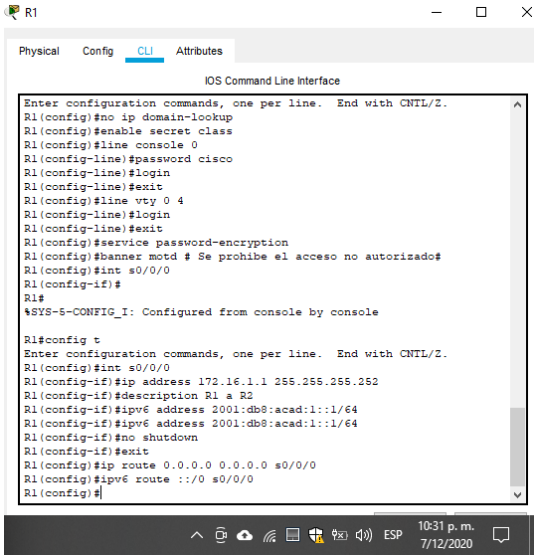
Para la configuracion que se esta realizando se debe configurar el servidor de internet con los siguientes datos de ip, mascara de subred, puerta de enlace, direccion ipv6 y puerta de enlace Ipv6

Paso 2: Configurar R1

Tabla 14 Configurar Router R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#login R1(config-line)#end
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd # Se prohibe el acceso no autorizado#
Interfaz S0/0/0	R1(config)#int s0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#description R1 a R2 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 Router(config)#ipv6 route ::/0 s0/0/0

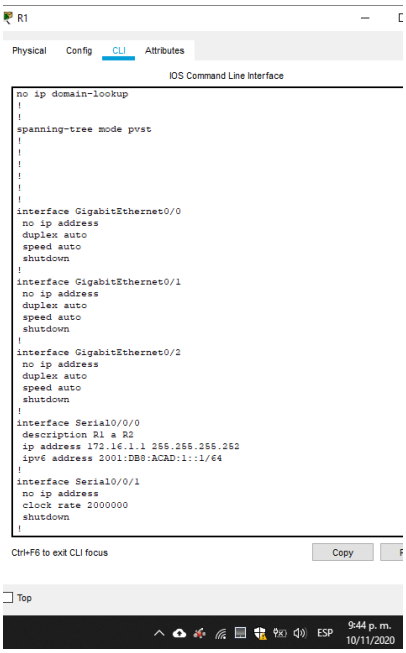
Figura 20 Configuración básica R1



Fuente: Autor

En el router R1 se debe realizar una configuracion basicar donde se cofigure las contraseña para el modo privilegiado, modo de cosoloa, acceso remoto y la condiguracion de red como ip y Ipv6 los cuales son necesario para darle seguridad a los dispositivos de red y configurar la red.

Figura 21 Comando Show Run Router R1



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando Show Run Router R1

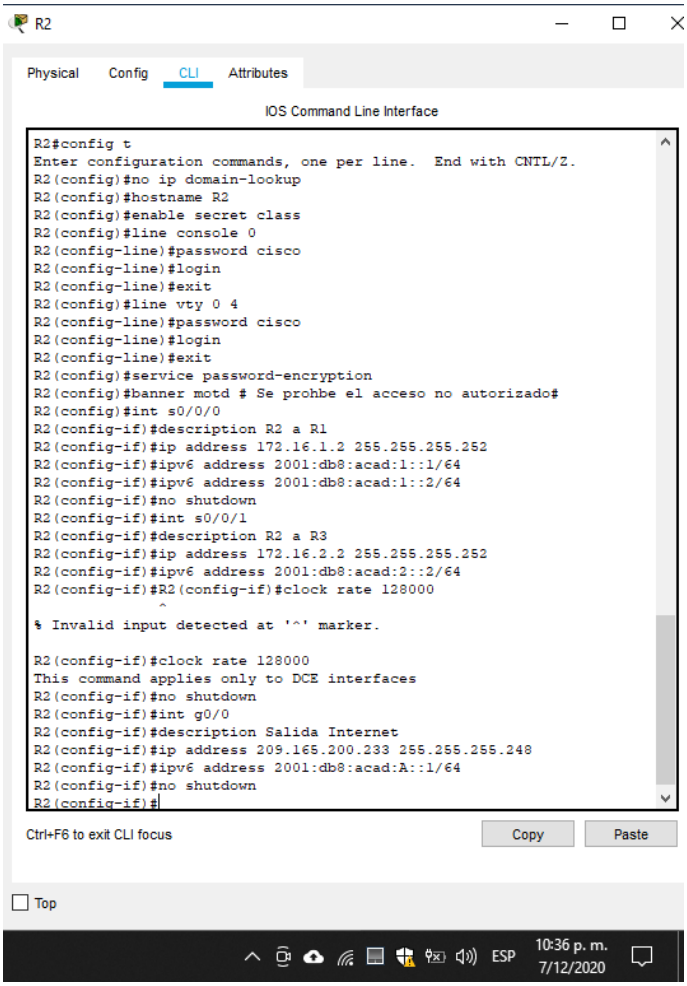
Paso 3: Configurar R2

Tabla 15 Configuración básica R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2 R2(config)#
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	R2(config)#line vty 0 4 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	R2(config)# ip http server

Mensaje MOTD	R2(config)#banner motd # Se prohíbe el acceso no autorizado#
Interfaz S0/0/0	R2(config)#interface S0/0/0 R2(config-if)#description R2 a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::1/64 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)Int S0/0/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description Salida Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.0 R2(config-if)#no shutdown R2(config-if)#description Web Serve simulado
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

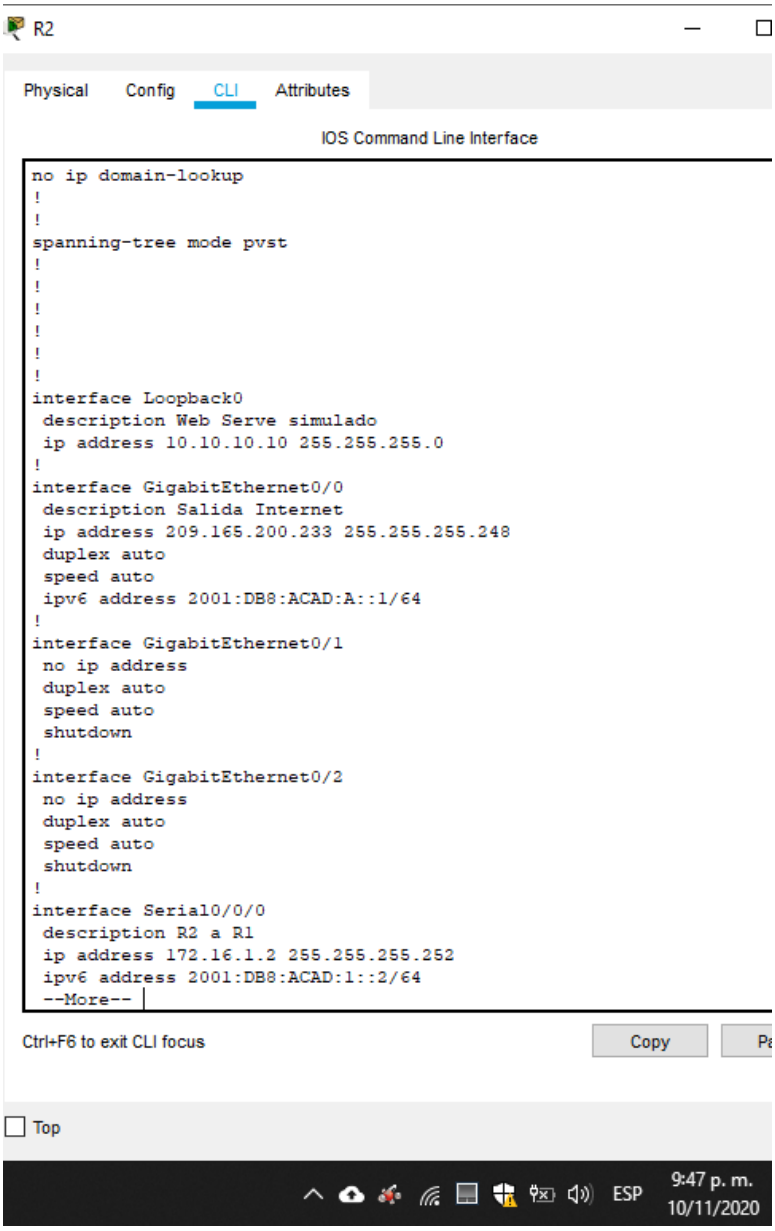
Figura 22 Configuración básica R2



Fuente: Autor

En el segundo router tambien es necesario realizar una configuracion basica para poder aumentar la seguridad de este dispositivo evitando que puedna ingresar y modificar su configuracion ya sea por consola o remotamente, tambien se debe realizar la configuracion de red como ipv4, ipv6 en sus interfaces a usar, para la configuracion solicitada tambien se debe establecer una rutas y configurar unas interfaces loopback

Figura 23 Comando Show run Router R2



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando Show run Router R2

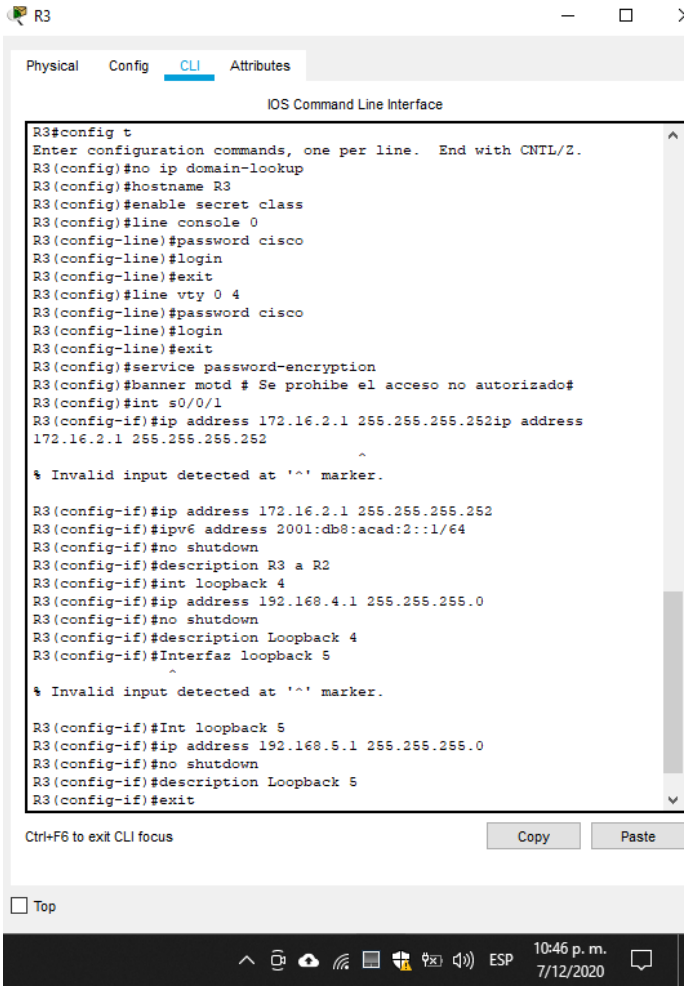
Paso 4: Configurar R3

Tabla 16 Configuración Router R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3 R3(config)#
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 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 prohibe el acceso no autorizado#
Interfaz S0/0/1	R3(config)#int s 0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#clock rate 128000 R3(config-if)#no shutdown R3(config-if)#description R3 a R2
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#description Loopback 4 R3(config-if)#exit
Interfaz loopback 5	R3(config-if)#Interfaz loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#description Loopback 5 R3(config-if)#exit

Interfaz loopback 6	R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#description Loopback 6 R3(config-if)#exit
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#no shutdown R3(config-if)#description Loopback 7 Ipv6 R3(config-if)#exit
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

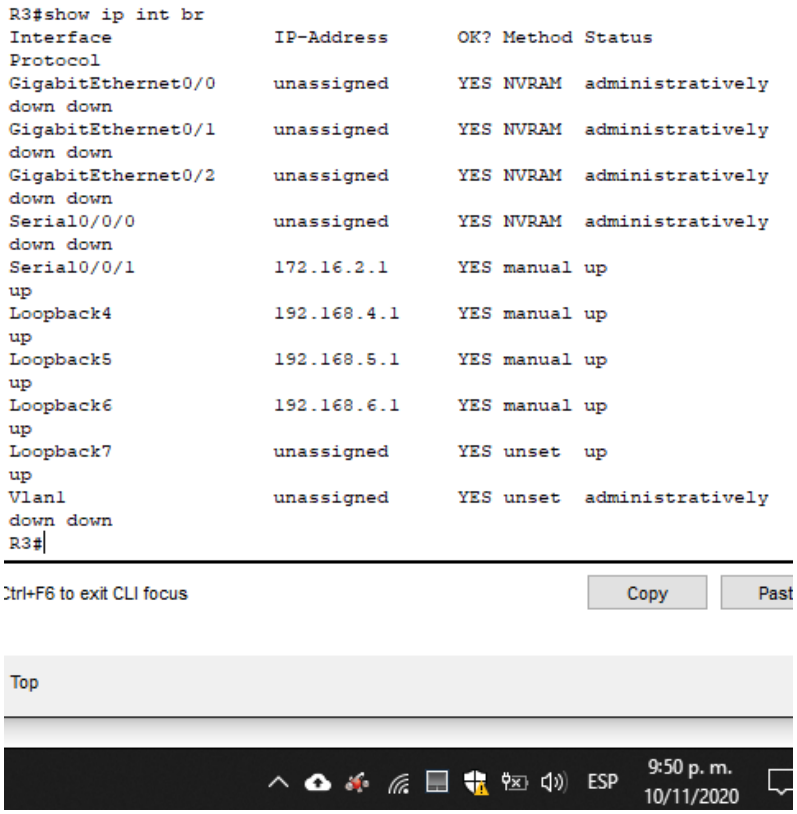
Figura 24 Configuración básica R3



Fuente: Autor

En el router R3 al igual que en los dispositivos anteriores se debe realizar una configuración básica para poder brindar seguridad a los dispositivos, también es necesario poder configurar las interfaces que se utilizaran con los datos de red brindados en la imagen de la topología, para este dispositivo también se configura unas interfaces loopback con los datos brindados

Figura 25 Comando show ip int br Router R3



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show ip int br Router R3

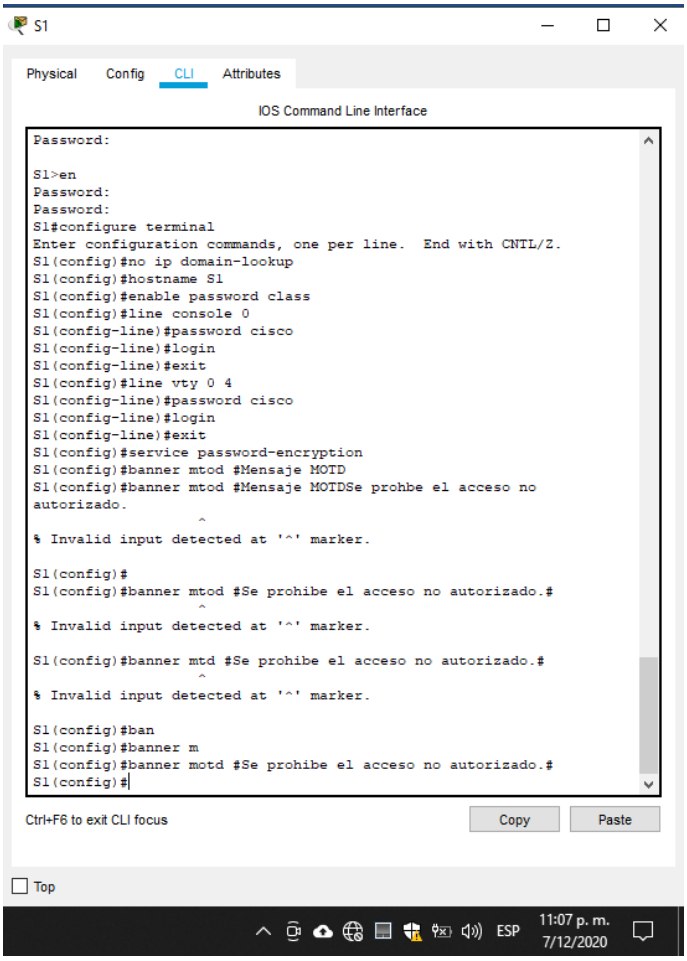
Paso 5: Configurar S1

Tabla 17 Configuración Switch 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 password class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#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 prohibe el acceso no autorizado.#

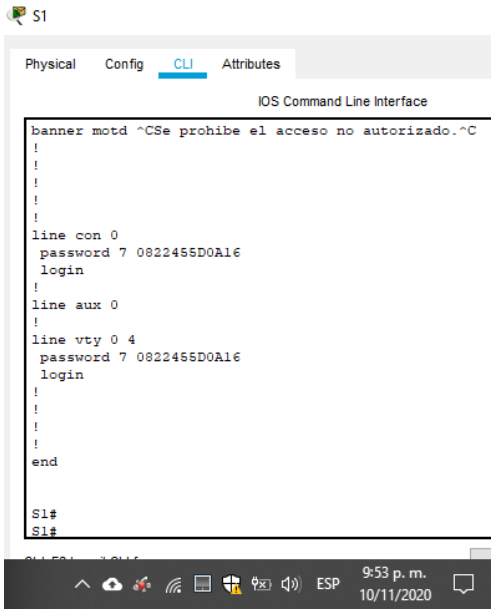
Figura 26 Configuración Básica S1



Fuente: Autor

El switch S1 se le deber realizar la configuracion basica como desactivar DNS, asignar un nombre para poder reconocer en la red, colocar seguridad a la conexión por consola y remotamente

Figura 27 comando Show run Switch S1



Fuente: Autor, para verificar que se haya configurado correctamente se ingresa el comando Show run Switch S1

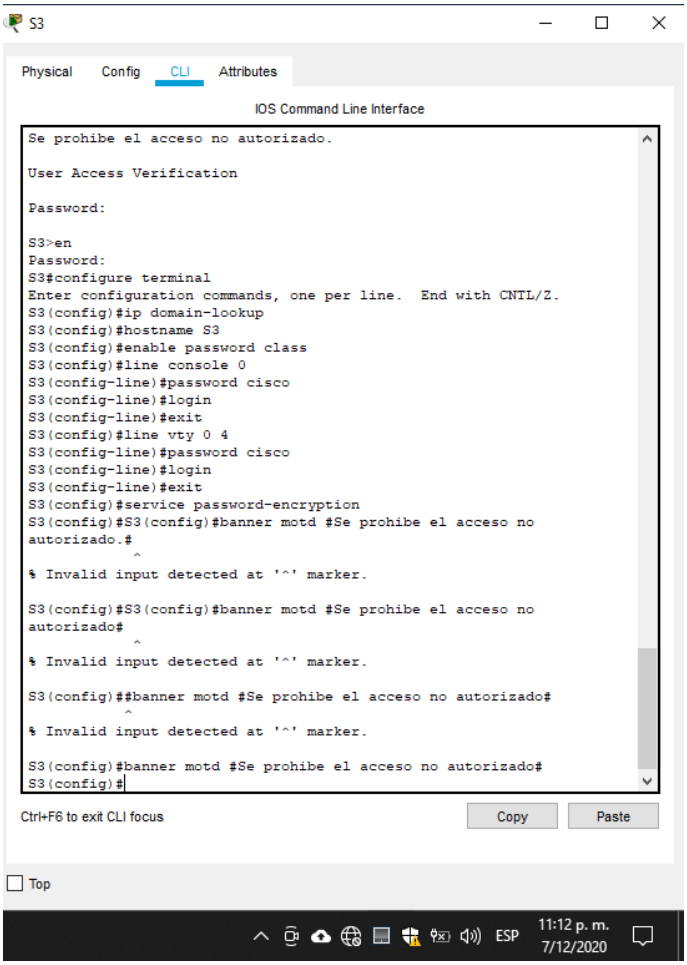
Paso 6 Configurar el S3

Tabla 18 Configuración el Switch S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#ip domain-lookup
Nombre del switch	Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	S3(config)#enable password class
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 4 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 prohibe el acceso no autorizado.#

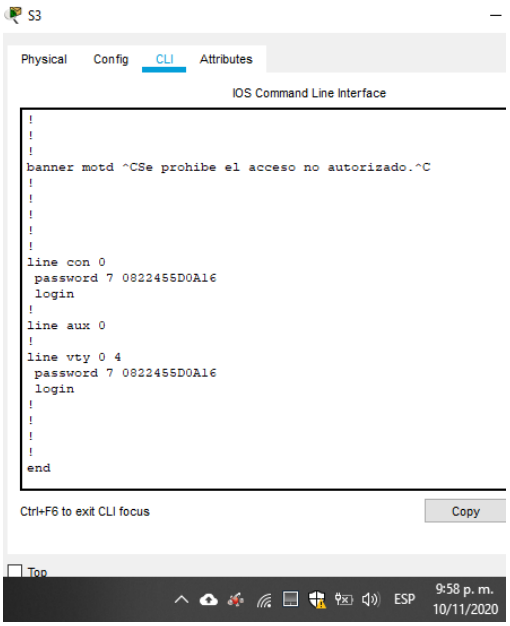
Figura 28 Configuración básica S3



Fuente: Autor

En el Swtich S3 se debe configurar el nombre del dispositivo para poderlo ubicar en la red, asegurar el dispositivo colocando contraseña de ingreso y un mensaje de advertencia, contraseña en el modo remoto,

Figura 29 comando Show run Switch S3



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando Show run Switch S3

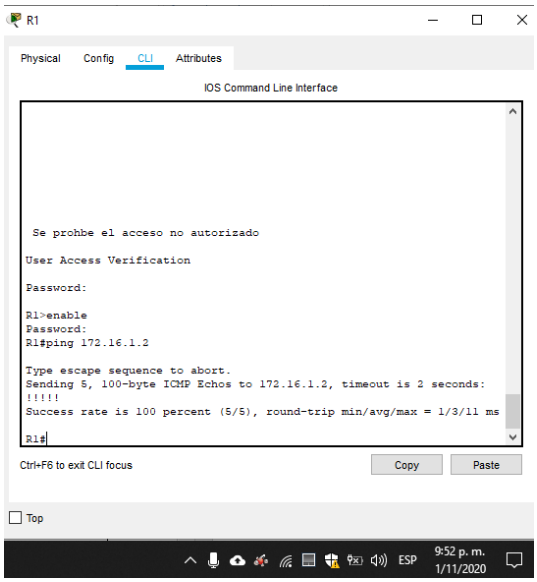
Paso 7: Verificar la conectividad de la red

Tabla 19 Verificación de Conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Ping responde
R2	R3, S0/0/1	172.16.2.1	Ping responde
PC de Internet	Gateway predeterminado	209.165.200.233	Ping Responde

Para veririfcar que los datos configurados han quedado correctamente y verificar que exista conectividad entre los dispositivos con el comando ping se envia paquetes a R1 y R2

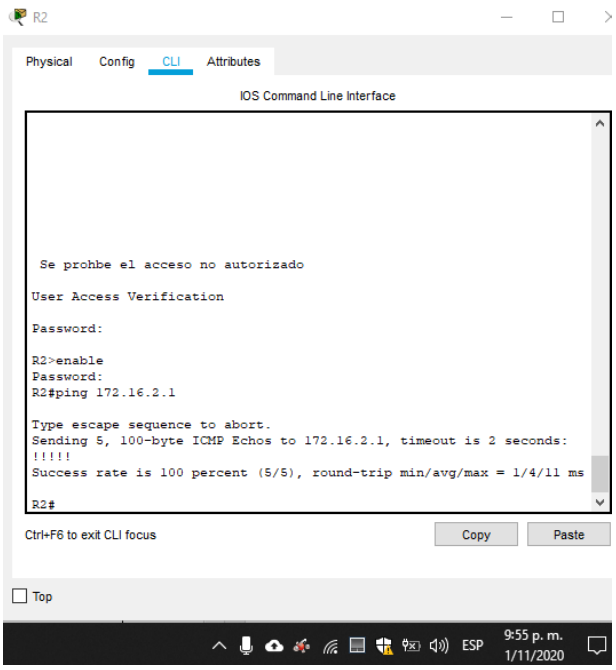
Figura 30 Ping desde R1 a R2 S0/0/0



Fuente: Autor

Para verificar que exista conectividad correctamente se ingresa el comando ping desde R1 a R2 S0/0/0

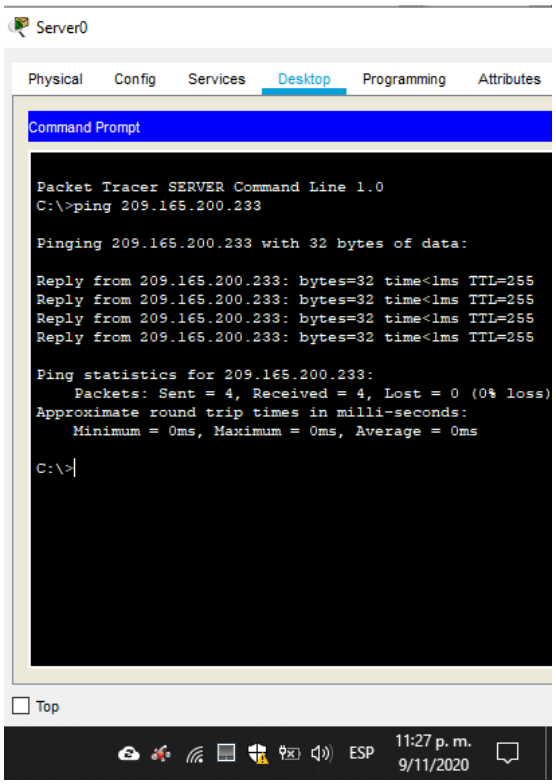
Figura 31 Ping de R2 a R3 S0/0/1



Fuente: Autor

Para verificar que exista conectividad correctamente se ingresa el comando, ping de R2 a R3 S0/0/1

Figura 32 Ping desde Pc internet a Gateway



Fuente: Autor

Para verificar que exista conectividad correctamente se ingresa el comando ping desde Pc internet a Gateway

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

Paso 1: Configurar S1

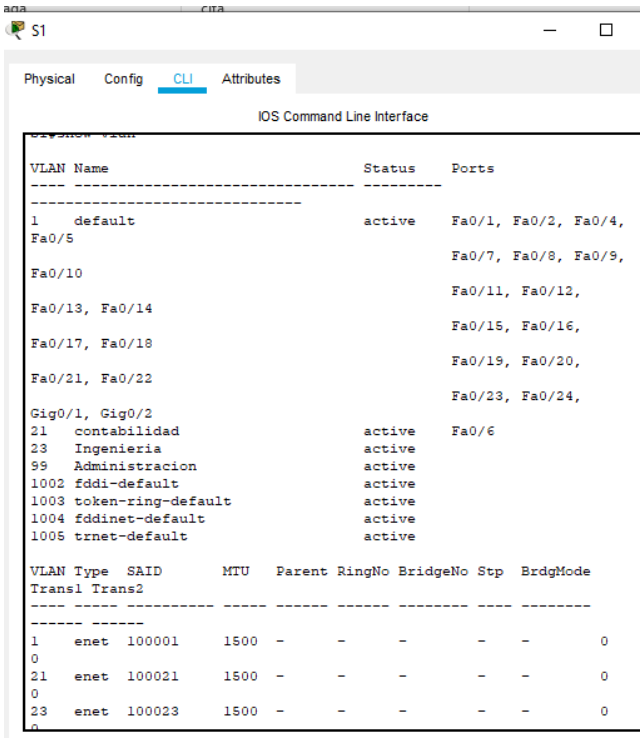
Tabla 20 Configuración Vlan, puertos troncales y Routing S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1#vlan database S1(vlan)#vlan 21 name Contabilidad S1(vlan)#vlan 23 name Ingenieria S1(vlan)#vlan 99 Administracion

Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#Description Vlan Administracion
Asignar el gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#switchport mode access S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#no shutdown S1(config-if)#description Conexion a R1
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 access S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#no shutdown S1(config-if)#description Conexion S1 a S3 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-if)#int range F0/1-2, f0/4, F0/6-24 S1(config-if-range)#switch mode access S1(config-if-range)#shutdow
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 S1(config-if)#no shutdown
Apagar todos los puertos sin usar	Utilizar el comando interface range S1(config-if)#int range F0/1-2, f0/4, F0/7-24 S1(config-if-range)#shutdow

Procedemos a realizar configuracion de las Vlan que solicita la actividad propuesta y con la cual jabamos los dominios de broadcast separando las redes por areas de trabajo, tambien realizamos la configuracion de los puertos troncal sobre el switch S1 para que se pueda pasar el trafico de las diferentes Vlan que se usaran en el swtich.

Figura 33 Comando show vlan switch S1



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show vlan en el switch S1

Paso 2: Configurar el S3

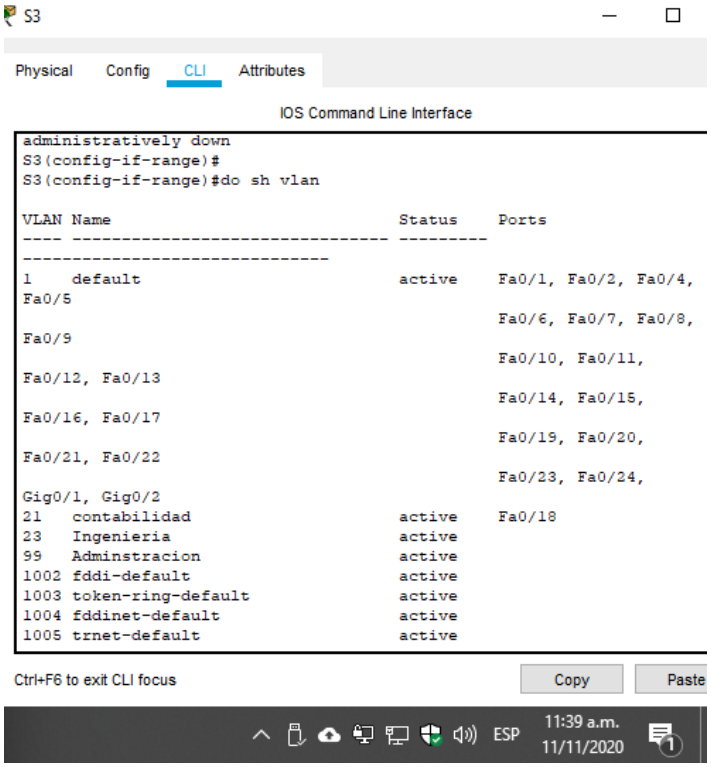
Tabla 21 Configuración Vlan, puertos troncal y routing S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3#vlan database S3(vlan)#Vlan 21 name contabilidad S3(vlan)#vlan 23 name Ingenieria S3(vlan)#vlan 99 name Adminstracion

Asignar la dirección IP de administración	S3(config-if)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#description Vlan Ingenieria
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#switchport mode access S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#Switchport trunk encapsulation dot1q S3(config-if)#description Conexion a S1 S3(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso	S3(config)#int range F0/1-2, F0/4-24 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 21 S3(config-if)#no shutdown
Apagar todos los puertos sin usar	S3(config)#int range f0/1-2, F0/4-17, f0/19-24 S3(config-if-range)#shutdown

Sobre el swith S3 tambien se debe realizar al configuracio de las Vlan, puertos troncales y ruoting para que pueda cominicar se los swtches por la vlan configuradas

Figura 34 Configuración Vlan e interfaces S3



Fuente: Autor, para verificar que se haya configurado correctamente se ingresa el comando show vlan en el switch S3

Paso 3: Configurar R1

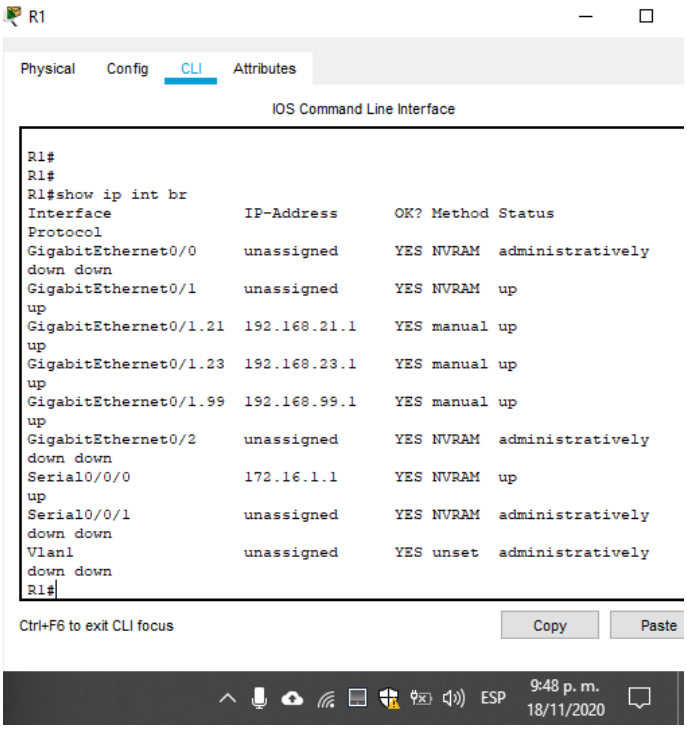
Tabla 22 Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.21 R1(config-subif)#description Lan Contabilidad R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#encapsulation dot1q 21
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#int g0/1.23 R1(config-subif)#description Lan de Ingenieria R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#encapsulation dot1q 23

Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/1.99 R1(config-subif)#description LAN de Administracion R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#encapsulation dot1q 99
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown

Para que R1 pueda recibir el trafico de las vlan por el mismo puerto es necesario configurar interfaces virtuales para cada vlan y configurar el encapsulado todo en la inerfaz G0/1

Figura 35 show ip interface br en R1



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show ip interface br en R1

Paso 4: Verificar la conectividad de la red

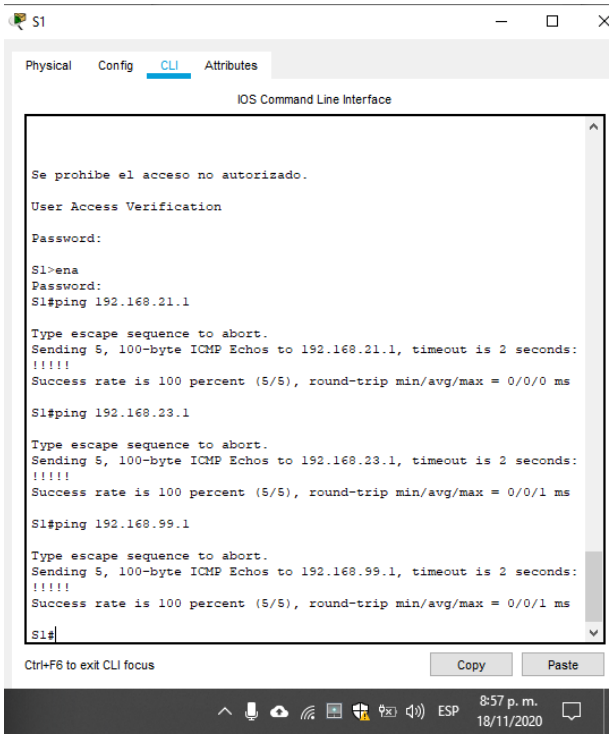
Tabla 23 Verificación interfaces virtuales R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Ok

S3	R1, dirección VLAN 99	192.168.99.1	Ok
S1	R1, dirección VLAN 21	192.168.21.1	Ok
S3	R1, dirección VLAN 23	192.168.23.1	Ok

Para verificar que la interfaces virtuales creadas quedaron configuradas correctamente se realiza un ping desde el switch S1 y S2 a router R1 comprobando que si halla conexión.

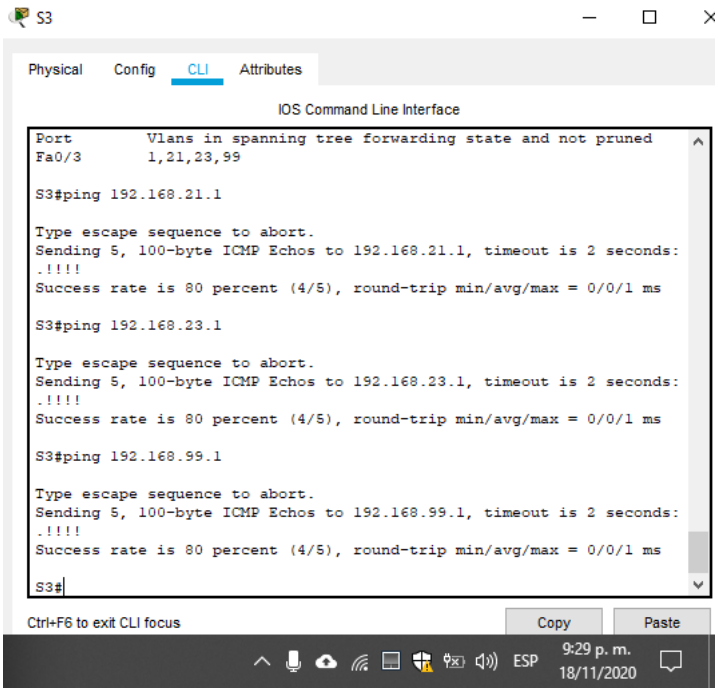
Figura 36 Verificación conexión de S1 a R1 vlan 99 y vlan 21



Fuente: Autor

Para verificar que exista conectividad correctamente se ingresa el comando ping conexión de S1 a R1 vlan 99 y vlan 21

Figura 37 Verificación conexión de S1 a R1 vlan 99 y vlan 23



Fuente: Autor

Para verificar que exista conectividad correctamente se ingresa el comando ping de S1 a R1 vlan 99 y vlan 23

Parte 4: Configurar el protocolo de routing dinámico OSPF

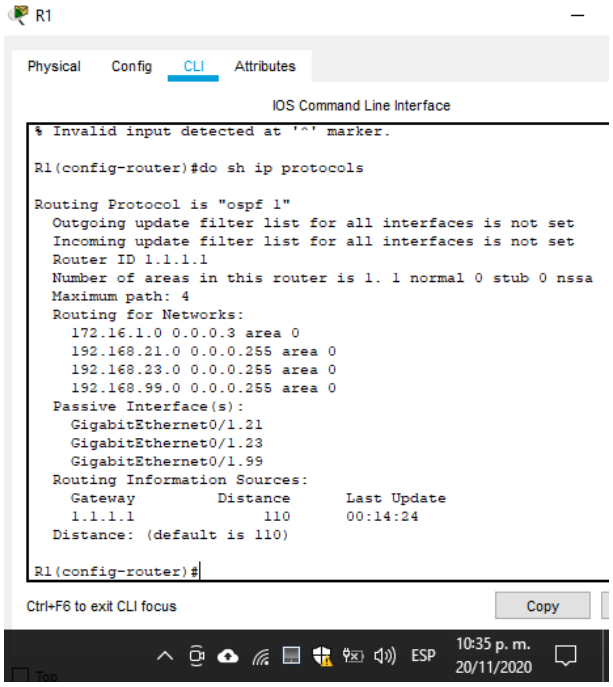
Paso 1: Configurar OSPF en el R1

Tabla 24 Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar 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)#router ospf 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 R1(config-router)#end
Desactive la sumarización automática	R1(config)#router ospf 1 R1(config-router)#no auto-summary

En los router se configurar OSPF para que entre ellos cree adyacencia entre vecinos, intercambie informacion de routing y calcular las mejores rutas

Figura 38 show ip protocols en R1



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show ip protocols en R1

Paso 2: Configurar OSPF en el R2

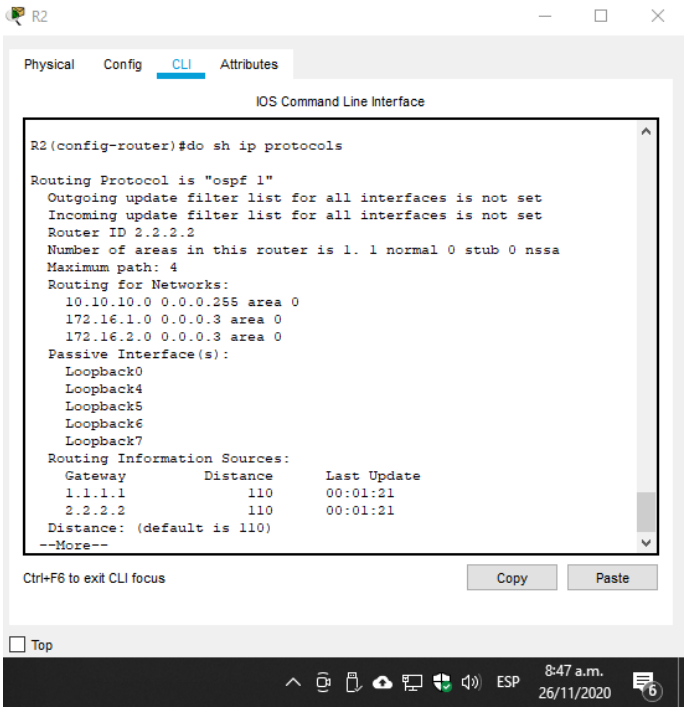
Tabla 25 Configurar OSPF en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.0 0.0.0.255 area 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
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#route ospf 1 R2(config-router)#passive-interface loopback 4 R2(config-router)#passive-interface loopback 5 R2(config-router)#passive-interface loopback 6 R2(config-router)#passive-interface loopback 7

Desactive la sumarización automática.	R2(config)#router ospf 1 R2(config-router)#no auto-summary

Para que el protocolo OSPF pueda acutalizar y compartir si lista de rutas tambien se debe configurar en R2 OSPF, area y anunciar las redes conectada directamente

Figura 39 show ip protocols en R2



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show ip protocols en R2

Paso 3: Configurar OSPFv3 en el R2

Tabla 26 Configurar OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)# ipv6 router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar redes IPv4 conectadas directamente	R2(config-router)#network 10.10.10.0 0.0.0.255 area 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

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config)# ipv6 router ospf 1 R2(config-router)#passive-interface loopback 4 R2(config-router)#passive-interface loopback 5 R2(config-router)#passive-interface loopback 6 R2(config-router)#passive-interface loopback 7
Desactive la sumarización automática.	R2(config)# ipv6 router ospf 1 R2(config-router)#no auto-summary

El protocolo OSPFv3 se utiliza para configurar adyacencia entre vecinos, intercambie informacion de routing y calcular las mejores rutas en direccionamiento Ipv6

Figura 40 Configurar OSPFv3 en el R2

Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show ip protocols

Paso 4: Verificar la información de OSPF

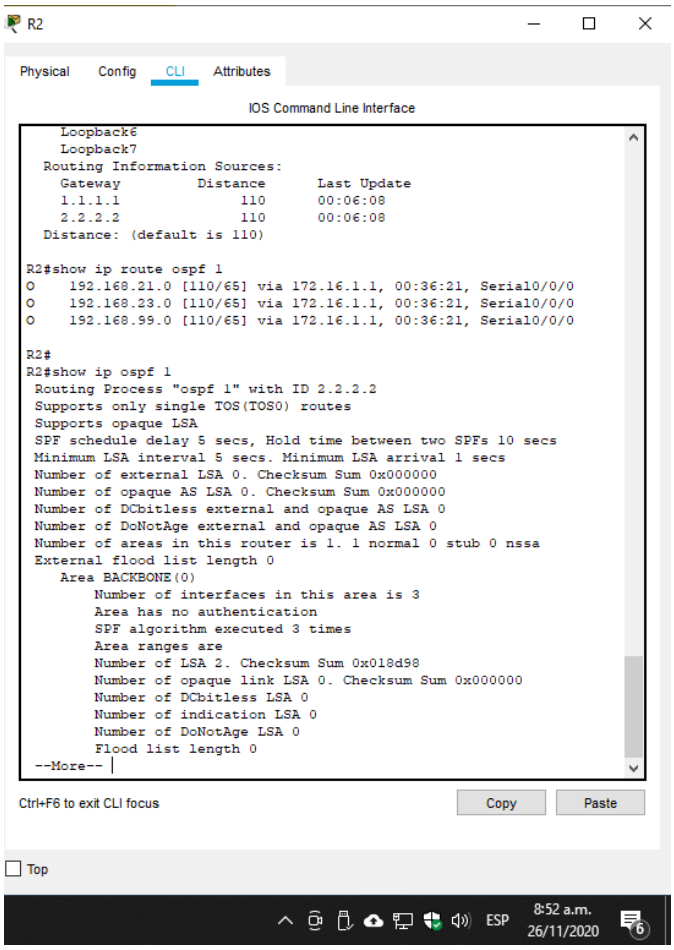
Tabla 27 Verificación OSPF por medio de comando

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de	R2#show ip protocols

routing y las interfaces pasivas configuradas en un router?	
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf 1
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show ip ospf 1

Se verifica e que OSPF esté funcionando como se espera por medio de los comandos show descritos en la tabla anterior

Figura 41 Comandos Show



Fuente: Autor

para verificar que se haya configurado correctamente se ingresa el comando show ip ospf 1

Parte 5: Implementar DHCP y NAT para IPv4

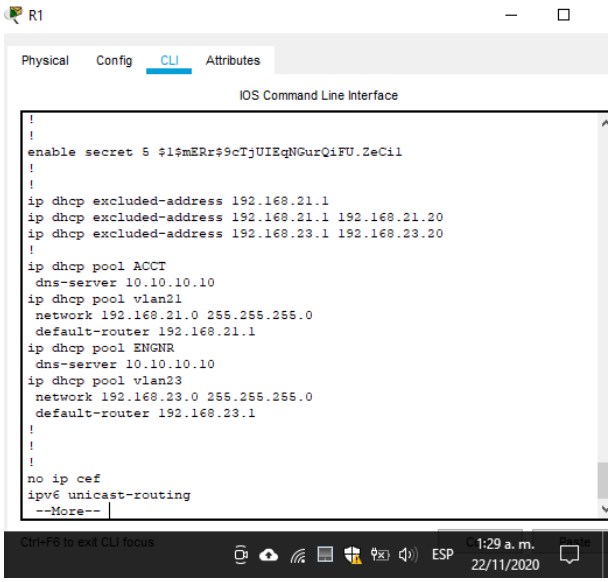
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Figura 42 Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#Ip dhcp excluded-add 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#Ip dhcp excluded-add 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	R1(config)#Int g0/1.21 R1(config-subif)#Ip dhcp pool ACCT R1(dhcp-config)#Dns-server 10.10.10.10 R1(dhcp-config)#Ip domain-name ccna-sa.com R1(config)#ip dhcp pool vlan21 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1
Crear un pool de DHCP para la VLAN 23	R1(config-subif)#int g0/1.23 R1(config-subif)#ip dhcp pool ENGNR R1(dhcp-config)#Dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(config)#ip dhcp pool vlan23 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-route 192.168.23.1

Para que los quipos conectados al los switches tomen una ip automatica se debe configurar en el router R1 el protocolo DHCP, este protocolo asigna una direcion Ip automatica a los equipos que se conecten a la red, y se evita tener que asignarle una ip manual a cada equipo que se conecte a la red

Figura 43 Comando show run en R1



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show run en R1

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

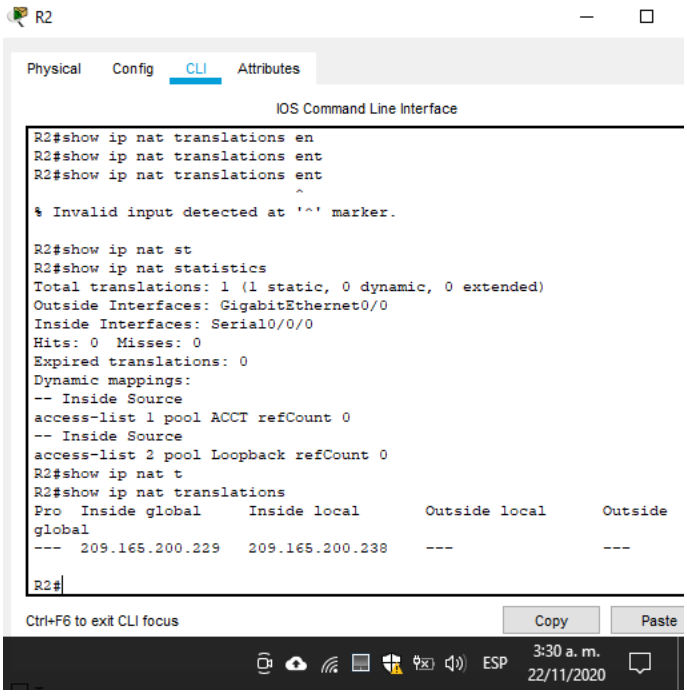
Tabla 28Configurar la NAT estática y dinámica en el R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)# ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	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 192.168.99.0 0.0.0.255
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 209.165.200.238 209.165.200.229

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 S0/0/0 R2(config-if)#ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#Ip nat inside source list 1 pool ENGNR R2(config)#Ip nat inside source list 1 pool ACCT R2(config)#Ip nat inside source list 2 pool Loopback
Defina el pool de direcciones IP públicas utilizables.	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	Show ip nat statistics

En ipv4 es necesario traducir las direciones ip publicas a privadas con el protocolo NAT el cual ayuda a que no todos los equipos de una red tenga direcciones publicas para poder navegar por internet, en esta paso se realizara la configuracion del router R2 que es nuestro rotuer de frontera para que realice NAT

Figura 44 show ip nat statistics /translations



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show ip nat statistics /translations

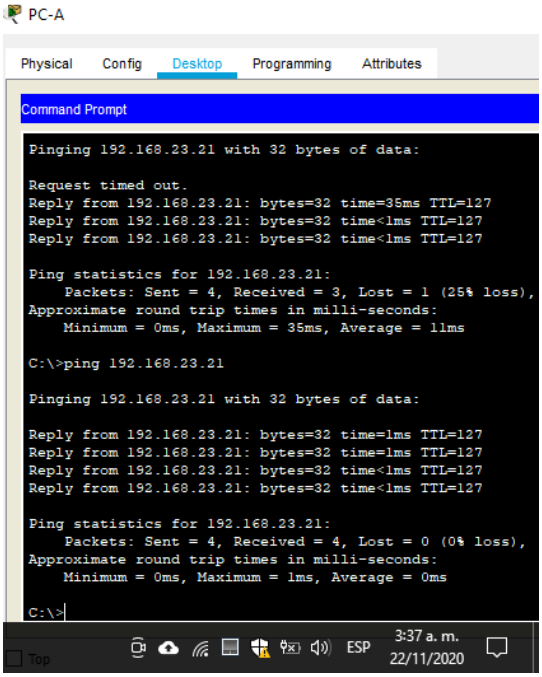
Paso 3: Verificar el protocolo DHCP y la NAT estática

Figura 45 Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix..: Physical Address.....: 0001.635A.244E Link-local IPv6 Address.....: FE80::201:63FF:FE5A:244E IP Address.....: 192.168.21.21 Subnet Mask.....: 255.255.255.0 Default Gateway.....: 192.168.21.1 DNS Servers.....: 0.0.0.0 DHCP Servers.....: 192.168.21.1 DHCPv6 Client DUID.....: 00-01-00-01-05-51-0A-90-00-01-63-5A-24-4E
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix..: Physical Address.....: 0060.2F68.1DD0 Link-local IPv6 Address.....: FE80::260:2FFF:FE68:1DD0 IP Address.....: 192.168.23.21 Subnet Mask.....: 255.255.255.0 Default Gateway.....: 192.168.23.1 DNS Servers.....: 0.0.0.0 DHCP Servers.....: 192.168.23.1 DHCPv6 Client DUID.....: 00-01-00-01-62-20-64-E7-00-60-2F-68-1D-D0
Verificar que la PC-A pueda hacer ping a la PC-C	Si responde
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**	Si responde página web http://209.165.200.229 Server Reset Connection por servicio del servidor HTTP no funciona en Packet tracert

Se realiza una verificacion de que la configuracion de protoclo DHCP y NAT esten funcionado correctamente en los equipos configurados como se ve en la tabla anterior

Figura 46 Ping desde PC-A a PC-C



Fuente: Autor

Para verificar que exista conectividad correctamente se ingresa el comando ping desde PC-A a PC-C

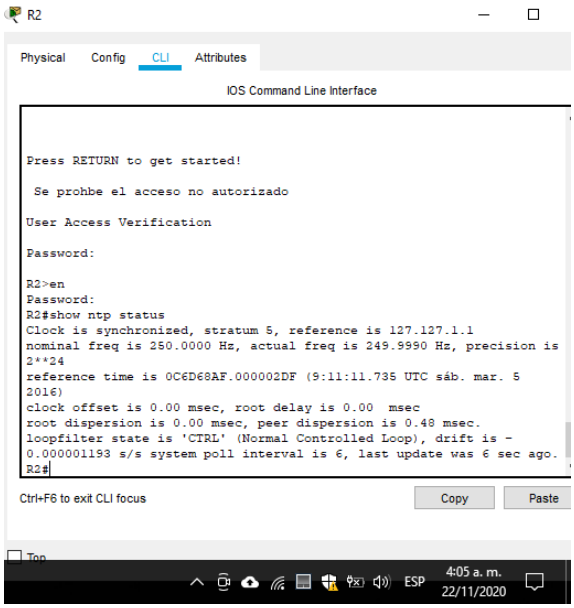
Parte 6: Configurar NTP

Tabla 29 Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#Clock set 09:00:00 March 5 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#Ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#Ntp update-calendar
Verifique la configuración de NTP en R1.	R1#Show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 10 16 17 6.00 1.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

En los router es necesario configurar el protocolo NTP el cual es un protocolo de Internet que sirve para sincronizar la hora de los equipos, acontinuacion se configurara NTP en router R1 y R2

Tabla 30 Show ntp status



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando Show ntp status

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

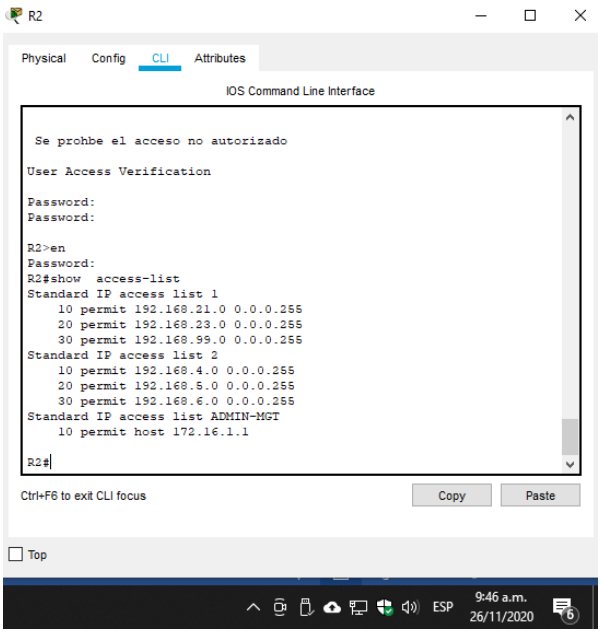
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 31 Restringir el acceso a las líneas VTY en el 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	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	line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Verificar que la ACL funcione como se espera	R2#show access-list

Se realizara la configuración de las lista ACL para poder controlar el tráfico y que solo el router R1 pueda tener una conexión por telnet hacia el rotuter R2

Figura 47 Comando show access-list R2



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show access-list R2

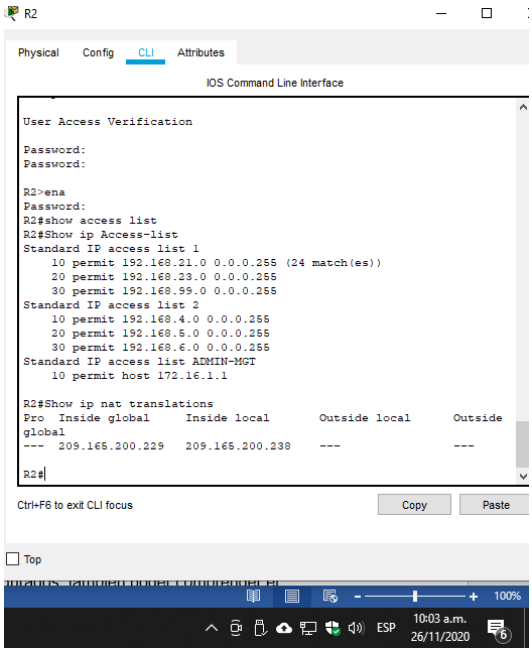
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Tabla 32 Comandos Show para mirar configuración

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip Access-list
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat traslation

Por medio del comando Show podemos consultar la configuración que tiene los dispositivos como router y switches, esto no sirve para poder ver la configuración actual del equipo o si se realiza algún cambio poder revisar que si se haya tomado los cambios realizados

Figura 48 Verificación configuración comandos Show



Fuente: Autor

Para verificar que se haya configurado correctamente se ingresa el comando show Access list, show ip nat trasnlations

Conclusiones

Después de haber realizado el desarrollo del escenario1 configuro en la práctica los comandos aprendidos en el desarrollo de las unidades de Cisco y también entender cómo funciona cada comando como se verifica que ya sea en el router o el los switches configurados, también poder comprender el funcionamiento de las configuraciones solicitadas como las Vlan que nos ayuda a separar el tráfico de las redes, el ethernetcahnnel con el cual podemos tener un enlace de respaldo, las configuraciones necesarias para lograr que un router trabaje con distintas Vlan.

Se monta una red de datos con varias Vlan y una conexión de respaldo o redundancia entre los switches, con la cual se puede llegar a proteger la red de datos en caso que se produzca una falla en las interfaces que realizan el enlace los dos switches o una falla del cable de conexión, también se logra poder realizar una comunicación entre todas las Vlan que se crearon.

Con esta actividad propuesta se logró conocer las configuraciones y funciones que puede llegar a tener un switch y un router y con la cuales se puede administra una red de datos dándole seguridad y mejorando el rendimiento de esta separando las redes en grupos para que mantengan si flujo de datos o información separados.

Se virtualizo la interfaz de un rotuer para poder manejar sobre cada una de estas interfaces virtuales una vlan diferente, con lo cual se evita usar una interfaz física para cada vlan, también se aumentó la seguridad de los router y switches que se usaron generando una contraseña para el ingreso y para las conexiones remotas, un mensaje de alerta

Bibliografía

calvear84. (10 de Febrero de 2020). *learningnetwork*. Obtenido de https://learningnetwork.cisco.com/s/question/0D53i00000KsOwt/vlan-nativa-puerto-trunk-y-subinterfaces

cisco. (30 de Agosto de 2005). *cisco*. Obtenido de cisco: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

cisco. (4 de Marzo de 2014). *cisco*. Obtenido de https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default.html

cisco. (17 de Marzo de 2015). *cisco*. Obtenido de https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/port_sec.pdf

cisco. (27 de Marzo de 2015). *cisco*. Obtenido de https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25sg/configuration/guide/conf/port_sec.pdf

cisco. (16 de Julio de 2017). *cisco*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-2950-series-switches/24042-158.html

cisco. (16 de Julio de 2017). *Cisco*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-2950-series-switches/24042-158.html

Cisco. (1 de Mayo de 2017). *Cisco*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/dynamic-address-allocation-resolution/22920-dhcp-ser.html

Duarte, E. (9 de Abril de 2019). *cloudacia*. Obtenido de https://blog.cloudacia.com/2019/04/10/ccna-como-configurar-un-puerto-trunk-en-cisco-switch/

Rugama, A. (19 de Julio de 2015). *youtube*. Obtenido de https://www.youtube.com/watch?v=lAgDtUKnbf0&ab_channel=AlvaroRugama

youtube. (24 de Mayo de 2014). Obtenido de https://www.youtube.com/watch?v=lfZMR3zjaTs&ab_channel=gustavoLobatoclara

Anexos

Archivo simulación Escenario 1 en Packet Tracer
https://drive.google.com/file/d/1XVVs9730yLyw8myQlGvLovfrcHgpWubV/view?usp=sharing

Archivo simulación Escenario 2 en Packet Tracer
https://drive.google.com/file/d/16BZJf8FXX2b0HsLPFc_K7RH6qHcIgbof/view?usp=sharing

Artículo Científico escenario 1 solución de dos estudios de caso bajo el uso de tecnología cisco
https://drive.google.com/file/d/1GduvoVca_OID7_i4BAMipzYTIW3HY5nu/view?usp=sharing