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

ANDREA DEL PILAR VARGAS COMETA

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
POPAYÁN
2020

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

ANDREA DEL PILAR VARGAS COMETA

Diplomado de opción de grado presentado para optar el título de DE INGENIERO DE SISTEMAS

DIRECTOR:
DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
POPAYÁN
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Popayán, 28 de Noviembre de 2020

TABLA DE CONTENIDO

LISTA DE TABLA

LISTA DE FIGURAS

GLOSARIO

DIRECCIÓN IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.

MASCAR DE SUBRED: es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

ENRUTAMIENTO: es el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.

VLAN: acrónimo de virtual LAN (red de área local virtual), 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.

DHCP: (Dynamic Host Configuration Protocol) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red

RESUMEN

En el presente documento se da solución a dos escenarios que consisten en la configuración de cada uno de los dispositivos de una red pequeña, permitiendo el establecimiento de conexiones para cada elemento conectado a la red, que son las conexiones IPv4 del protocolo de Internet, la cual, es la forma de uso general de IP Addressing usada para identificar los host y utiliza un formato de 32 bits y la versión 6 (IPv6) del protocolo de Internet que es el estándar de la dirección IP de la última generación, previsto para substituir el formato del IPv4; es decir, que se realizan las configuraciones del IPv4 y del IPv6 en el dispositivo del punto de acceso de las redes y se hace el diagnóstico con el comando ping, para verificar el estado de determinada conexión de host local.

Palabras claves: Conexiones IPv4, host, ping. Protocolo de internet

ABSTRACT

This document provides a solution to two scenarios consisting of the configuration of each of the devices of a small network, allowing the establishment of connections for each element connected to the network, which are the Ipv4 connections of the Internet protocol, the which, is the general use form of IP Addressing used to identify the hosts and uses a 32-bit format and version 6 (Ipv6) of the Internet protocol which is the next generation IP address standard, intended to replace the Ipv4 format; that is, the Ipv4 and Ipv6 configurations are made on the network access point device and the diagnosis is made with the ping command, to verify the status of a certain local host connection.

Keywords: Ipv4 connections, host, ping, the Internet protocol

INTRODUCCIÓN

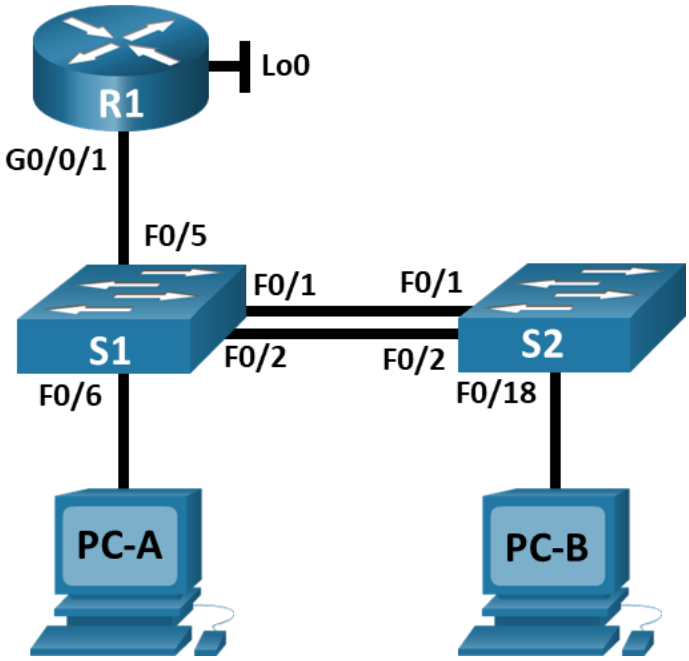
En un contexto donde la comunicación es una necesidad para transmitir y recibir información de manera segura es importante utilizar la tecnología, las redes dan la posibilidad de conectarse ofreciendo mejores servicios al alcance de toda una comunidad a fin de estimular y ofrecer mejores oportunidades para el desarrollo social.

En el siguiente documento se encuentran dos escenarios relacionados con redes y el objetivo es aplicar cada uno de los conceptos adquiridos en el diplomado de cisco para la adecuada configuración de los dispositivos y de esta manera obtener el establecimiento de una conexión efectiva.

DESARROLLO DE LA ACTIVIDAD

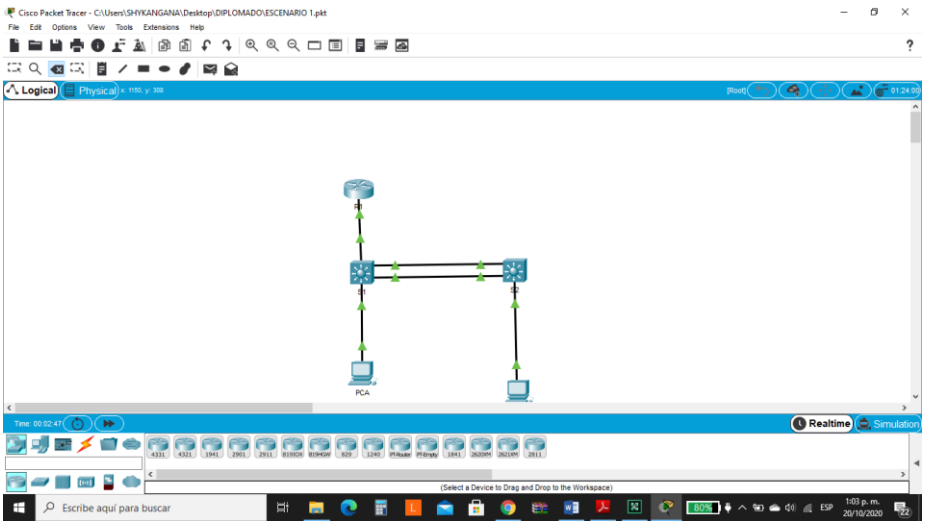
ESCENARIO 1

Figura 1.Escenario 1



Fuente: UNAD

Figura 2. Simulación de escenario 1



Fuente 2: Autor

Se realiza la respectiva conexión de los dispositivos de una red pequeña.

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 de VLAN

Tabla 1. Tabla de VLAN

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

Tabla 2. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
R1 G0/0/1.3	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	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
VLAN S1 4	2001:db8:acad:c: :98 /64	No corresponde
S1 VLAN 4	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	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
PC-A NIC	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Parte 1. Inicializar y Recargar y Configurar aspectos basicos de los dispositivos
Paso 1. Inicializar y volver a cargar el router y el switch.

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

Descripción:

Inicializar y recargar el Router

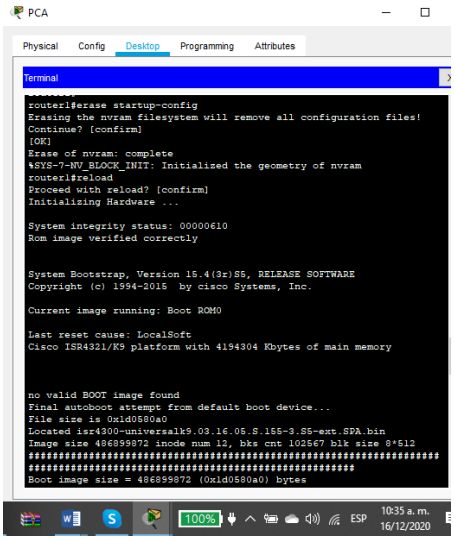
Para realizar la configuración es necesario que los dispositivos esten limpios y que se borren las configuraciones anteriores para que mas adelante no se presenten errores. Por lo anterior se ejecuta el comando erase startup-config para la eliminación de la configuración de inicio y reload para para deshacer los ultimos cambios realizados. En los switchs se eliminan la bases de datos de la Vlan anterior y con el comando Show flash se hace la verificación. Se configura la plantilla SDM para que los switch admitan ipv4 a ipv6 y se recargan de nuevo para que funcionen.

Tabla 3. Inicializar y recargar dispositivos

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router>enable 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>enable 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>enable Switch#show flash
configurar la plantilla SDM para que admita IPv6	Switch#sdm prefer dual-ipv4-and-ipv6 default Switch#exit Switch#reload

En este caso el switch soporta IPv6

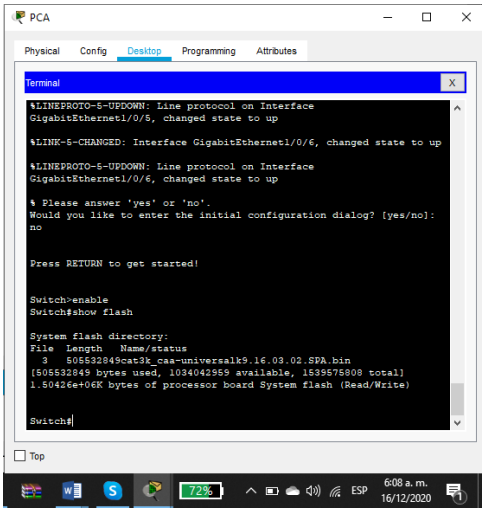
Figura 3. Borrar configuración y reiniciar el Router



Fuente. Autor

Con el comando erase startup-config se borraron las configuraciones anteriores y reload para reiniciarlo.

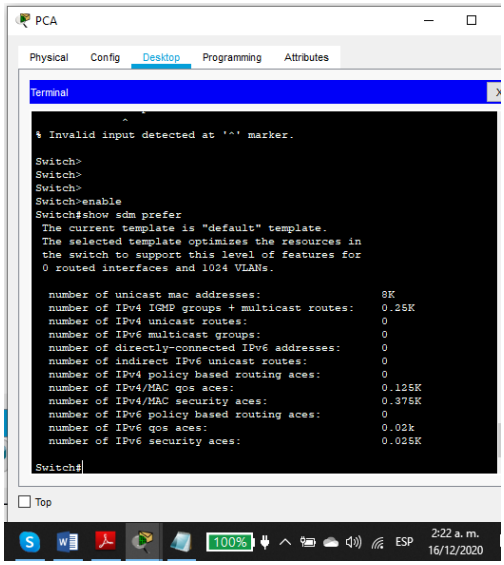
Figura 4. show flash



Fuente: Autor

Con el comando show flash se verificó que la base de datos de VLAN no está en la memoria flash luego de haber reinicializado el switch.

Figura 5. Configuración plantilla SDM



Fuente. Autor

Luego de hacer la configuración de la plantilla SMD con el comando Show sdm prefer se verifica la plantilla actual.

Paso 2 configurar el Router 1

Se requiere la configuración del router que proporcione conectividad a nivel de red en el modelo OSI con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que mas adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y asi proporcionar seguridad , la contraseña de acceso a la consola la longitud minima de 10 caracteres, crear un usuario administrativo en la base de datos local para la autenticación.Tambien se configura el inicio de sesión en las líneas VTY para que use la base de datos local, encriptación del mensaje, se establecen las subinterfaces para Ipv4 e Ipv6 y para finalizar se generar una clave de cifrado RSA para encriptar y descifrar datos.

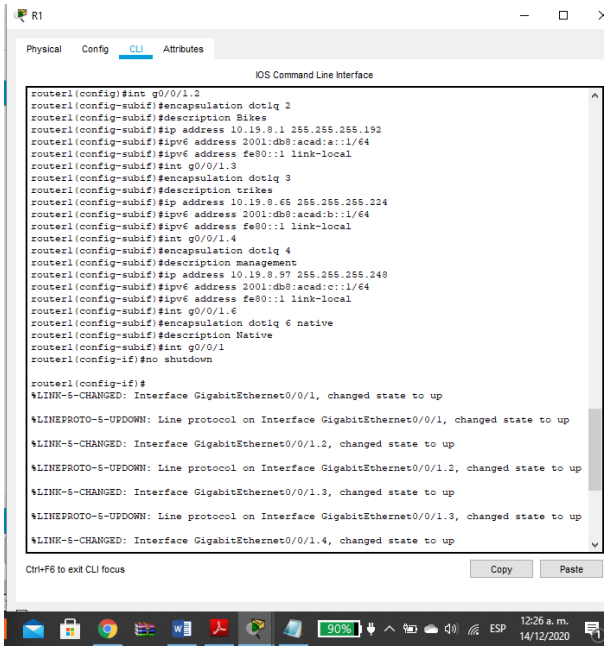
Tabla 4. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del router	Router(config)#hostname R1
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 console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1(config)#username admin 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 R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd $Unauthorized Access is prohibited!$
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
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 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#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 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#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 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#int g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description Native R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown R1(config-if)#
Configure el Loopback0 interface	R1(config-if)#int loopback 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)#description internet R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa R1(config)#

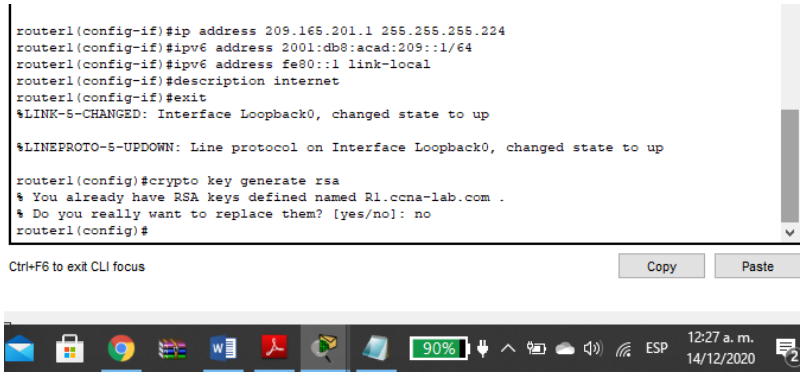
Figura 6. Configuracion R1



Fuente: Autor

Se observa la configuración de las subinterfaces y direcciones ip del R1.

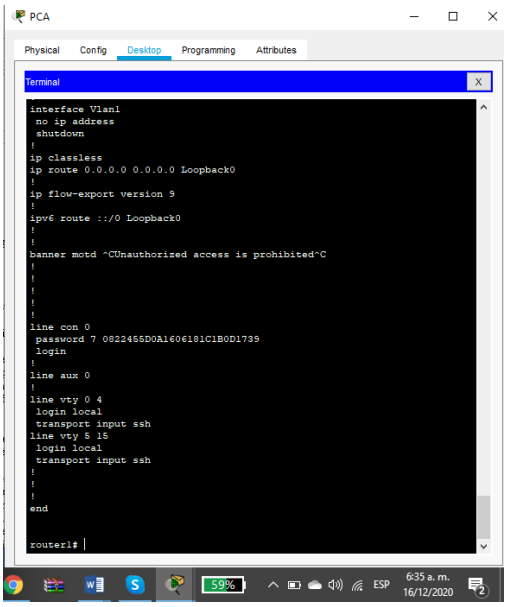
Figura 7. Loopback 0



Fuente: Autor

En esta imagen se observa la configuración de la loopback 0 interface

Figura 8. Show running-config



En la figura 6 muestra el contenido del archivo de configuración activo utlizando el comando show running-config

Paso 3. Configure S1 y S2

El switch se encarga de analizar y evaluar las tramas que ingresan por sus puertos de entrada y los filtra para trabajar únicamente en los puertos correctos. Una adecuada configuración proporciona seguridad, correcta comunicación entre los dispositivos y una red estable.

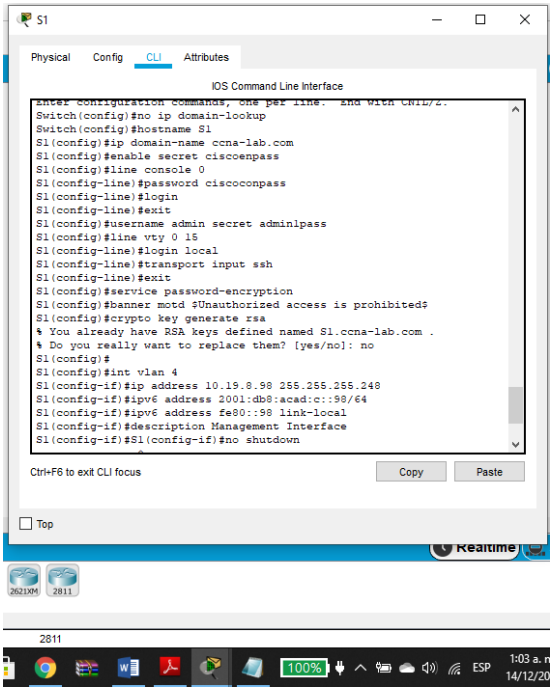
Se realiza laconfiguración básica teniendo en cuenta el nombre, protección por contraseña, encriptación del mensaje, la contraseña para acceso remoto se configura en line vty 0 15, con el comando "password" seguido de un espacio y la contraseña deseada, generar una clave de cifrado RSA, configurar la interfaz de administración (SVI) utilizando el comando S1(config)#int vlan 4 y de esta manera permite crear una SVI asociada a la VLAN cuyo ID se aplica, e ingresar al modo de configuración de esa interfaz, por ultimo la configuración del gateway predeterminado para para precisar el mejor camino hacia un destino remoto.

Tabla 5. Configuración S1

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 S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin 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 S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd $Unauthorized Access is prohibited!$
Generar una claave de cifrado RSA	S1(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S1(config)# S1(config)#int vlan 4 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)#description Management Interface S1(config-if)#no shutdown S1(config-if)#exit

Tarea	Especificación
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 S1(config)#

Figura 9. Configuración S1



Fuente: Autor

Se realiza la configuración del S1 teniendo en cuenta la interfaz de administración y la configuración del gateway predeterminado.

Configuración Switch 2

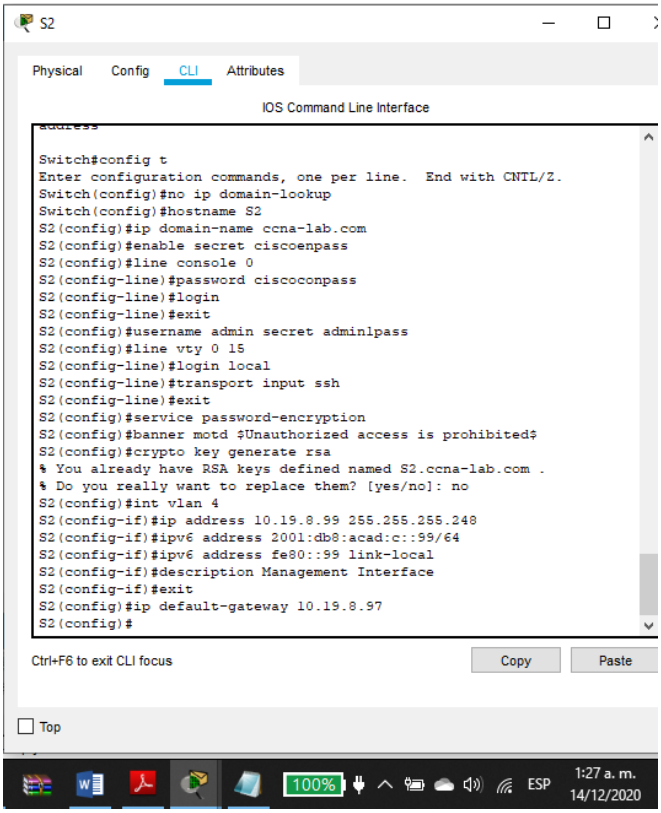
Tabla 6. Configuración S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd $Unauthorized Access is prohibited!$
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)# S2(config)#int vlan 4 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)#description Management Interface S2(config-if)#no shutdown S2(config-if)#exit S2(config)#ip default-gateway 10.19.8.97 S2(config)#

Tarea	Especificación
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97 S2(config)#

Figura 10. Configuracion S2



Fuente: Autor

En el S2 se hace la configuración teniendo en cuenta la interfaz de administración y la configuración del gateway predeterminado.

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Se crean las vlans en el S1 para garantizar la calidad del servicio y agrupar los usuarios en en grupos específicos, luego se crean las troncales que utilizan las vlan 6 en las interfaces 1,2 y 5. Es de recordar que las intrefaces 1 y 2 se apagan para

luego configurar EtherChannel. Para crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 se utiliza el comando channel-group 1 mode active de manera que el modo LACP coloca un puerto en un estado de negociación activa, en el que el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP. Se configura el puerto de acceso de host para VLAN 2 para interface 6 de esta manera queda el puerto asignado a la VLAN 2 cambiando al modo permanente. Se configura la seguridad del puerto en los puertos de acceso que hace que haya seguridad y se reestringe la entrada de mas interfaces.

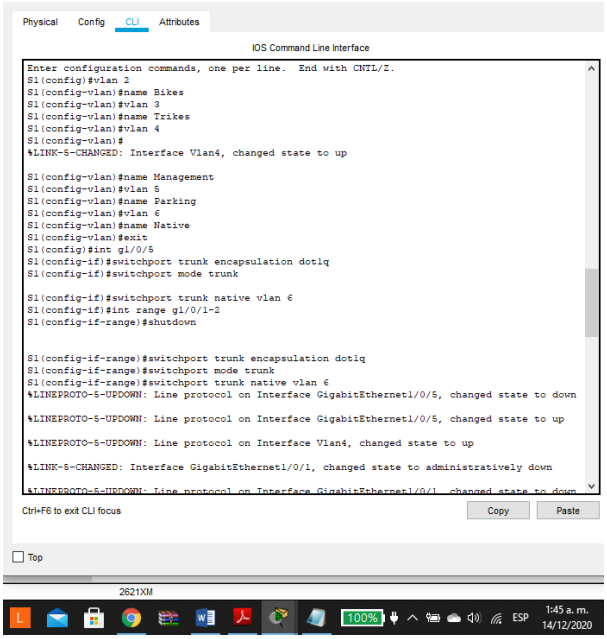
Por ultimo se protegen las interfaces no utilizadas

Tabla 7. Configuración S1 Infraestructura de red VLAN 2

Tarea	**Especificación**
Crear VLAN	S1(config)# 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 S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#int g1/0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#int range g1/0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switch trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In use S1(config-if-range)#shutdown S1(config-if-range)#

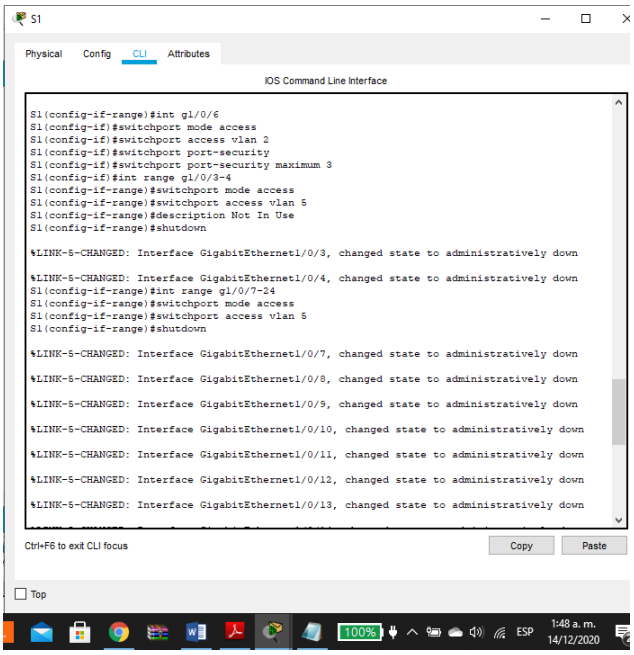
Figura 11. Creación de las vlans y troncales



Fuente: Autor

En el S1 se crean las vlans 2,3,4,5 y 6 y las troncales para la Vlan 6, Nativa.

Figura 12. Configuración puerto host Vlan 2 y seguridad



Fuente: Autor

Se configura el puerto de acceso de host para VLAN 2 y su seguridad para reestringir la entrada de mas interfaz.

Paso 1 Configure el S2.

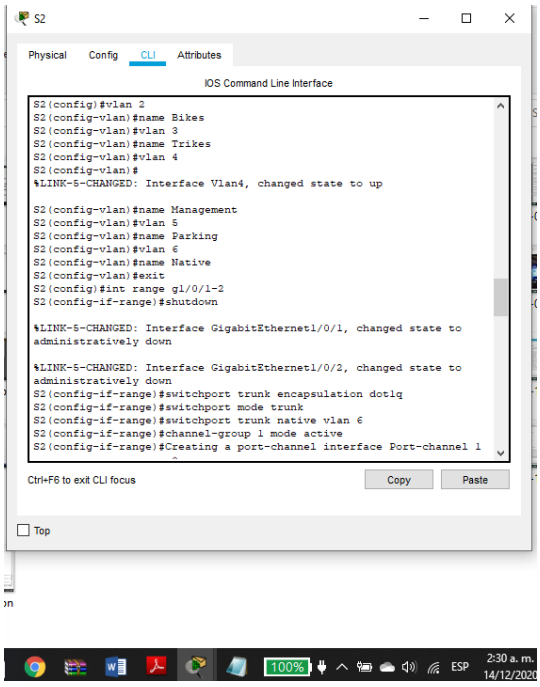
Se siguen los pasos de confguración del S1 teniendo en cuenta que en el paso configurar el puerto de acceso del host es para la VLAN 3

Tabla 8. Configuración S1 Infraestructura de red VLAN 3

Tarea	Específicación
Crear VLAN	S2>enable Password: Password: S2#config term 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 S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(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	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 S2(config-if-range)#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

Configurar el puerto de acceso del host para la VLAN 3	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use S2(config-if-range)#shutdown S2(config)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In use S2(config-if-range)#shutdown

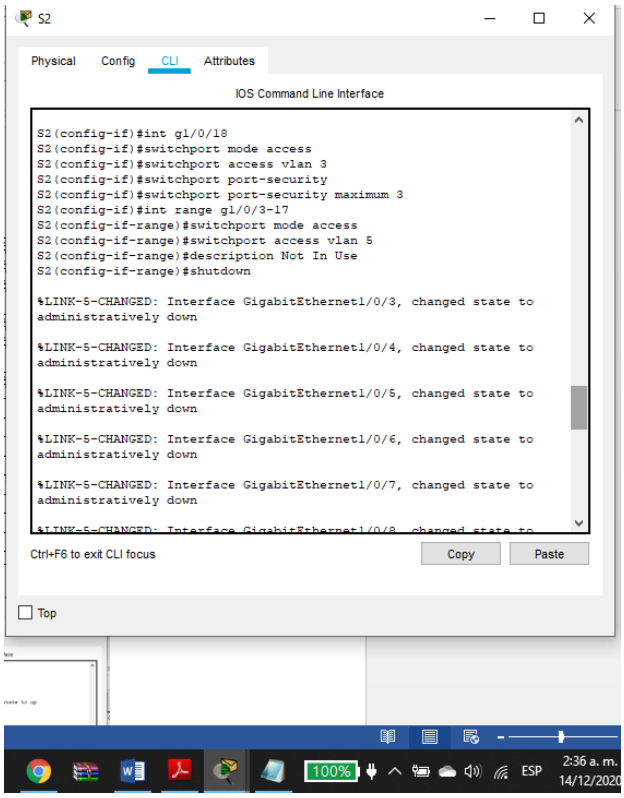
Figura 13. Creación de las vlans y troncales en S2



Fuente: Autor

En el S2 se crean las vlans 2,3,4,5 y 6 y las troncales para la Vlan 6, Nativa.

Figura 14. Configuración puerto host Vlan 3 y seguridad



Fuente: Autor

Se configura el puerto de acceso de host para VLAN 3 y su seguridad para reestringir la entrada de mas interfaces.

Ahora se activan las interface en S1 y S2

Parte 3 Configurar soporte de host

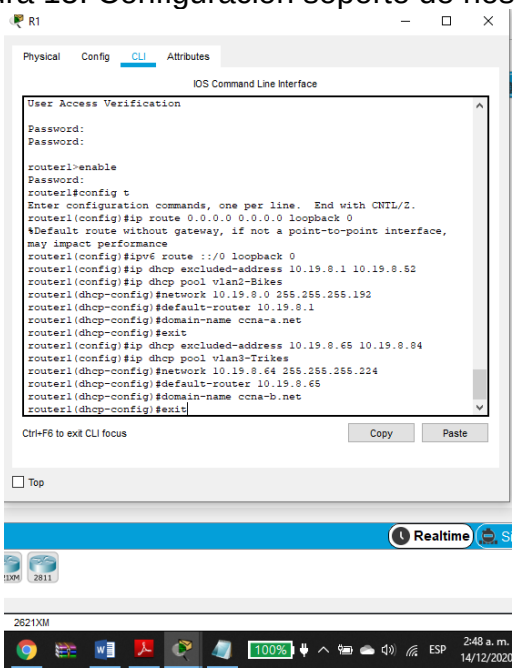
Paso 1. Configure R1

Se inicia la configuración del soporte de host con el almacenamiento de una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing y luego se configurar IPv4 DHCP para VLAN 2 y 3.

Tabla 9. Configurar soporte de host R1

Tarea	Especificación
Configure Default Routing	R1>enable Password: R1#config term 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	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 R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	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 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Figura 15. Configuración soporte de host R1



Fuente: Autor

En esta imagen se evidencian las configuraciones de los host para Ipv4 y los DHCP para las Vlans 2 y 3.

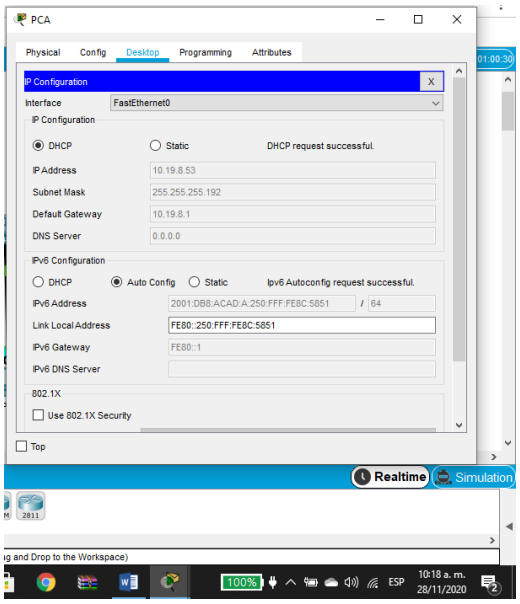
Paso 2. Configurar los servidores

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

Tabla 10. Configuración PC-A

Configuración de red de PC-A	
Descripción	En el PCA se ingresa a la IP configuration y se da clic en DHCP para ipv4 se encuentra la Dirección Ip, a mascara de subred, la puerta de enlace.
Dirección física	0050.0F8C.5851
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::250:FFF:FE8C:5851

Figura 16.Configuración PC-A DHCP



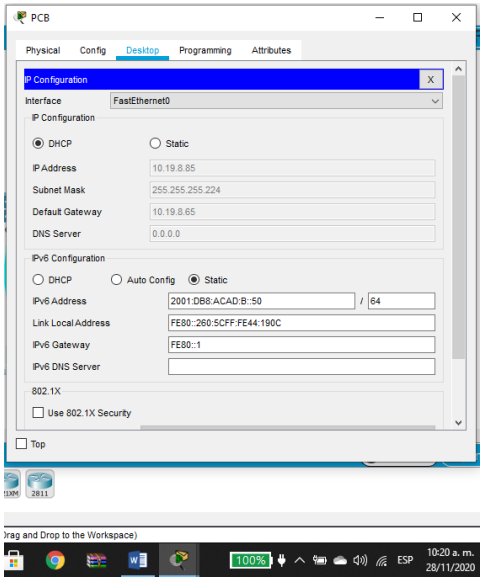
Fuente : Autor

En el PC-A se observa que toma la dirección IP del DHCP Server.

Tabla 11. Configuración PC-B

Configuración de red de PC-B	
Descripción	En el PCB se ingresa a la IP configuration y se da clic en DHCP pa ipv4 se encuentra la Dirección Ip, a mascara de subred, la puerta de enlace.
Dirección física	0050.0F8C.5851
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::260:5CFF:FE44:190C

Figura 17. Configuración PC-B, DHCP



Fuente: Autor

En el PC-B se observa que el DHCP se puede conectar de forma automática.

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

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

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

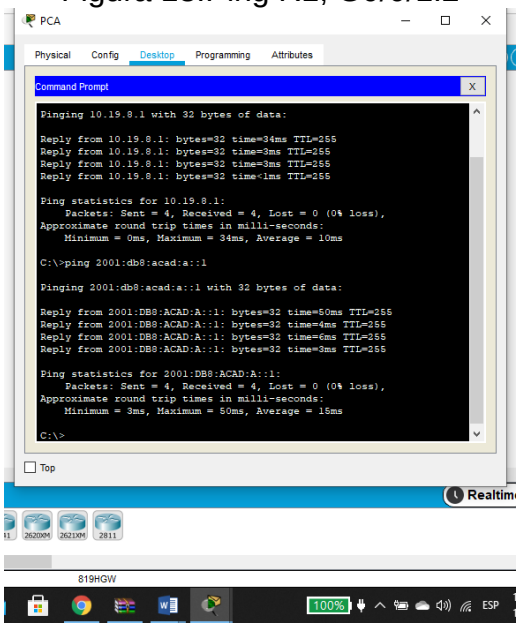
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Tabla concectividad dispositivo de red

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Exitoso*
		IPv6	2001:db8:acad:a: :1	Exitoso
	R1, G0/0/1.3	Dirección	10.19.8.65	Exitoso
		IPv6	2001:db8:acad:b: :1	Exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	Exitoso
		IPv6	2001:db8:acad:c: :1	Exitoso
	S1, VLAN 4	Dirección	10.19.8.98	Exitoso
		IPv6	2001:db8:acad:c: :98	Exitoso
	S2, VLAN 4	Dirección	10.19.8.99.	Exitoso
		IPv6	2001:db8:acad:c: :99	Exitoso
	PC-B	Dirección	IP address will vary.	Exitoso
		IPv6	2001:db8:acad:b: :50	Exitoso
	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209: :1	Exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Exitoso*
		IPv6	2001:db8:acad:209: :1	Exitoso
	R1, G0/0/1.2	Dirección	10.19.8.1	Exitoso
		IPv6	2001:db8:acad:a: :1	Exitoso

Desde	A	de Internet	Dirección IP	Resultados de ping
	R1, G0/0/1.3	Dirección	10.19.8.65	Exitoso
		IPv6	2001:db8:acad:b: :1	Exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	Exitoso
		IPv6	2001:db8:acad:c: :1	Exitoso
	S1, VLAN 4	Dirección	10.19.8.98	Exitoso
		IPv6	2001:db8:acad:c: :98	Exitoso
	S2, VLAN 4	Dirección	10.19.8.99.	Exitoso
		IPv6	2001:db8:acad:c: :99	Exitoso

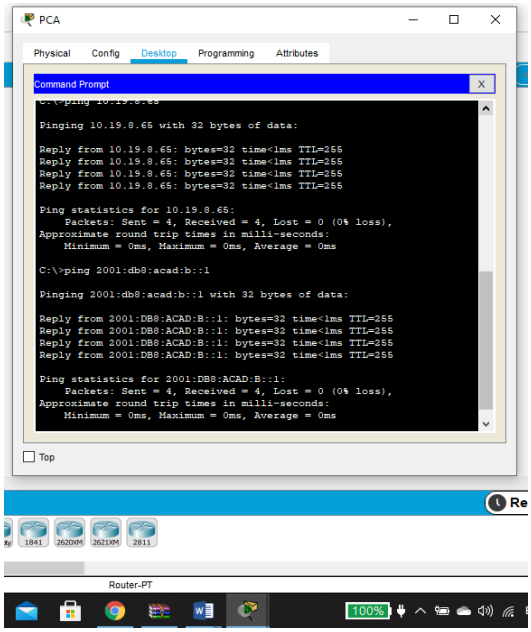
Figura 18.Ping R1, G0/0/1.2



Fuente: Autor

Desde el PC-A se hace ping a la ip 10.19.8.1 siendo exitoso

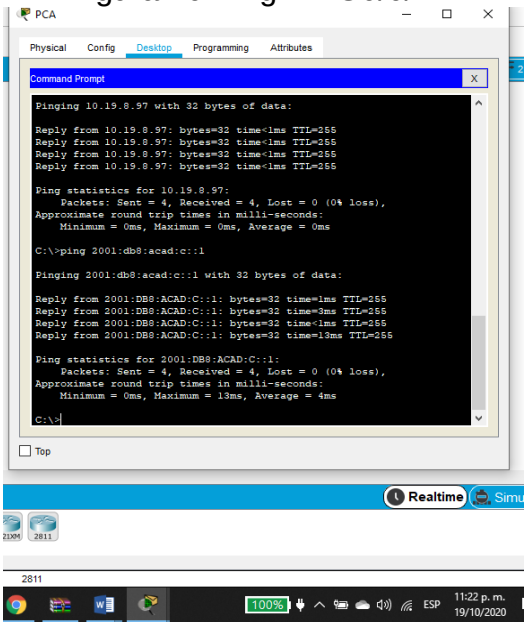
Figura 19.Ping G0/0/1.3



Fuente: Autor

Desde el PC-A se hace ping a la ip 10.19.8.65 siendo éxito.

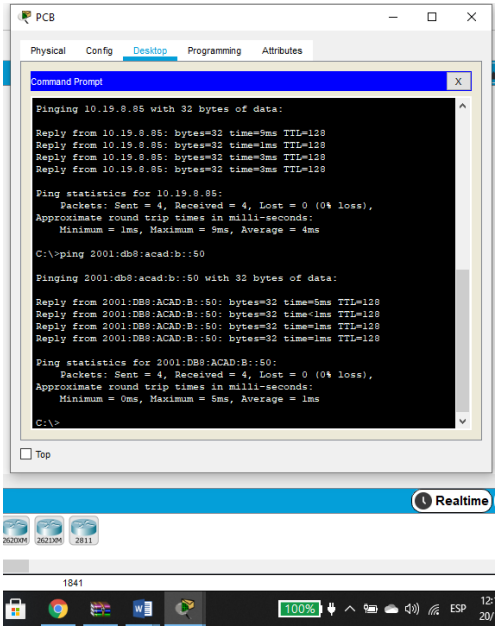
Figura 20.Ping R1 G0/0/1.4



Fuente: Autor

Desde el PC-A se hace ping a R1 ip 10.19.8.97 con paquetes recibidos y enviados

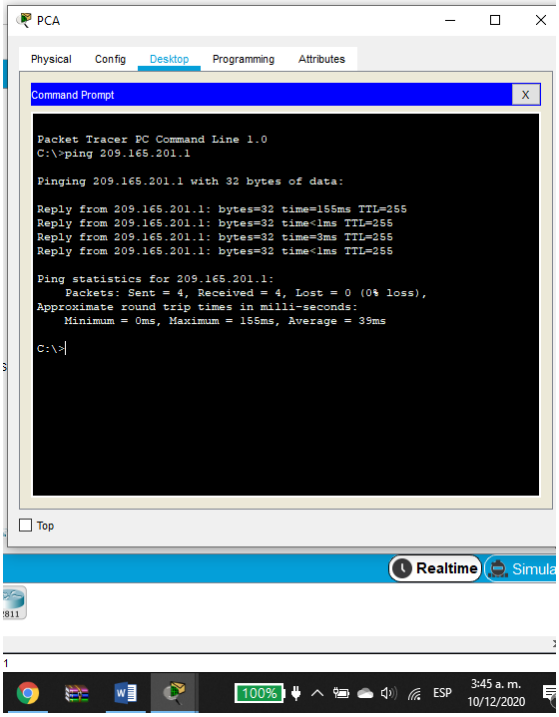
Figura 21.Ping PC-B



Fuente: Autor

Se hace ping al PC-B con ip 10.19.8.85 siendo exitoso.

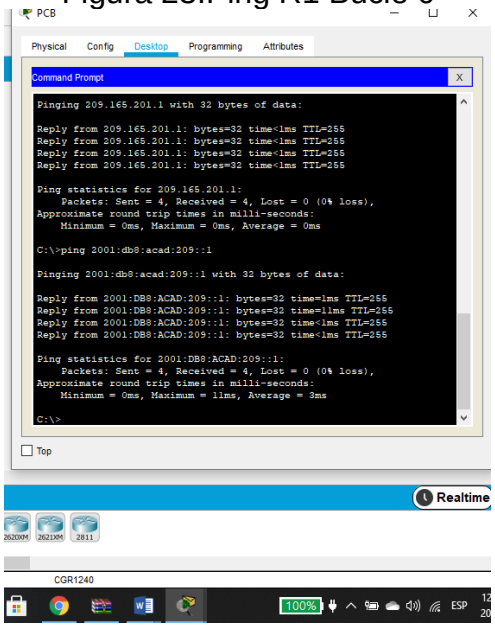
Figura 22.Ping R1 Bucle 0



Fuente: Autor

Desde el PC-A se hace ping al R1 Bucle 0 con ip 209.165.201.1 y hay conectividad.

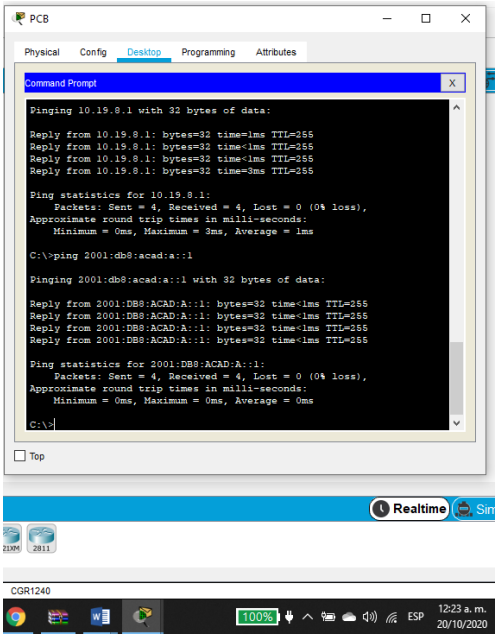
Figura 23.Ping R1 Bucle 0



Fuente: Autor

Desde el PC-B se hace ping al R1 Bucle 0 con ip 209.165.201.1 y hay conectividad

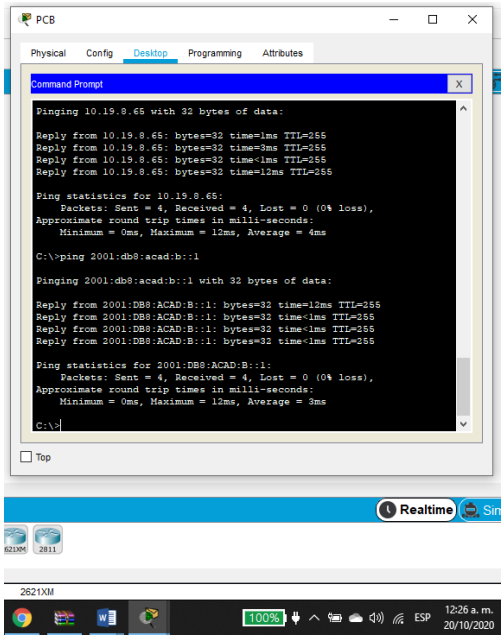
Figura 24.Ping de PC-B a R1 G0/0/1.2



Fuente : Autor

Desde el PC-B se hace ping al R1 G0/0/1.2 con ip 10.19.8.1 y hay conectividad

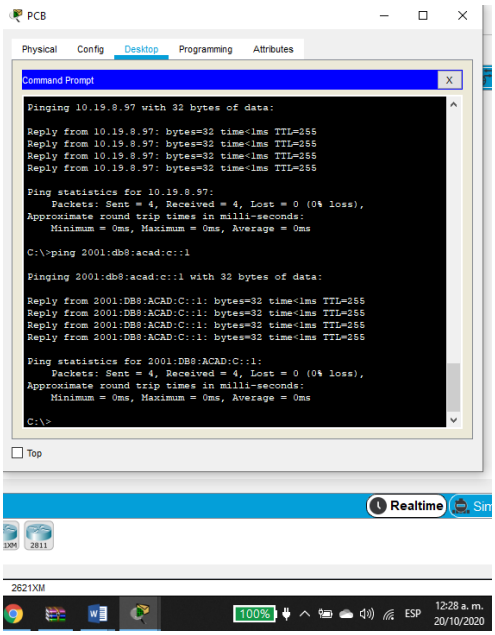
Figura 25. Ping PC-B a R1, G0/0/1.3



Fuente: Autor

Desde el PC-B se hace ping al R1 G0/0)1.3 con ip 10.19.8.65 y hay conectividad

Figura 26.Ping desde PC-B a R1,G0/0/1.4



Fuente:Autor

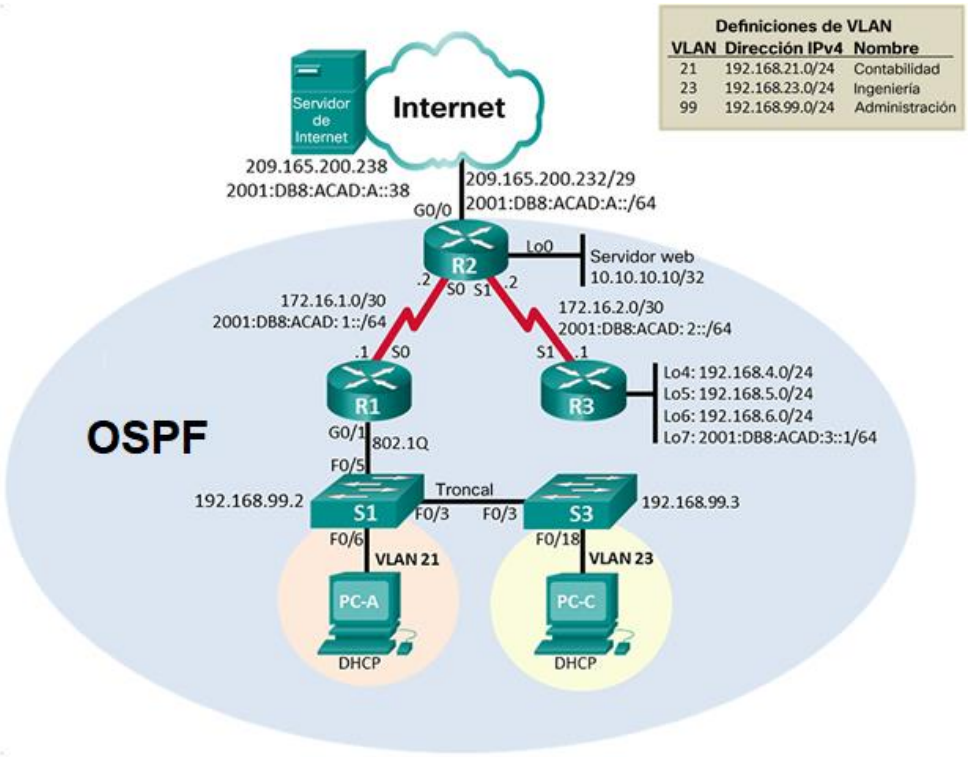
Desde el PC-B se hace ping al R1 G0/0)1.4 con ip 10.19.8.97 y hay conectividad

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.

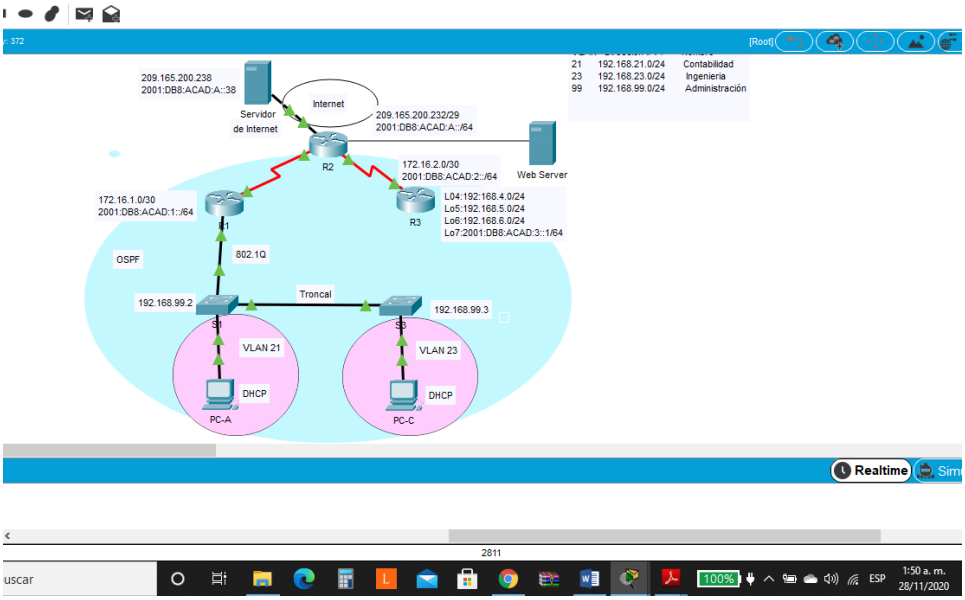
TOPOLOGÍA

Figura 27. Escenario 2



Fuente: UNAD

Figura 28. Simulación Escenario 2



Fuente: Autor

Parte 1. Inicializar dispositivos.

Paso 1.Inicializar y volver a cargar los routers y los switches
Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Para realizar la configuración es necesario que los dispositivos esten limpios y que se borren las configuraciones anteriores para que mas adelante no se presenten errores. Por lo anterior se ejecuta el comando erase startup-config para la eliminación de la configuración de inicio y reload para para deshacer los ultimos cambios realizados. En los switchs se eliminan la bases de datos de la Vlan anterior y con el comando Show flash se hace la verificación.

Tabla 13.Inicializar y recargar dispositivos

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router>enable 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>enable 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>enable Switch#show flash

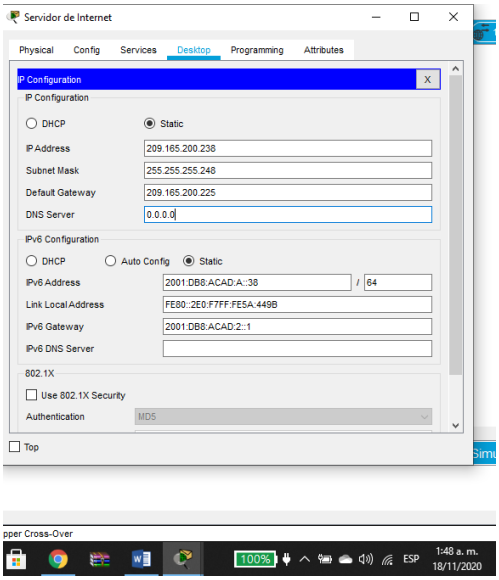
Parte 2:Configurar los parámetros básicos de los dispositivos.

Paso 1: Configurar la computadora de Internet
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 14.Configuración PC internet

Elemento o tarea de configuración	Configuración
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

Figura 29. Configuración PC de Internet



Fuente: Autor

En el servidor de internet se realiza la respectiva configuración teniendo en cuenta las direcciones ip de la topología.

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

Paso 1 Configurar R1

Se requiere la configuración del router que proporcione conectividad a nivel de red en el modelo OSI con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que mas adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y asi proporcionar seguridad, se realiza la configuración de las interfaces del dispositivo

Las tareas de configuración para R1 incluyen las siguientes:

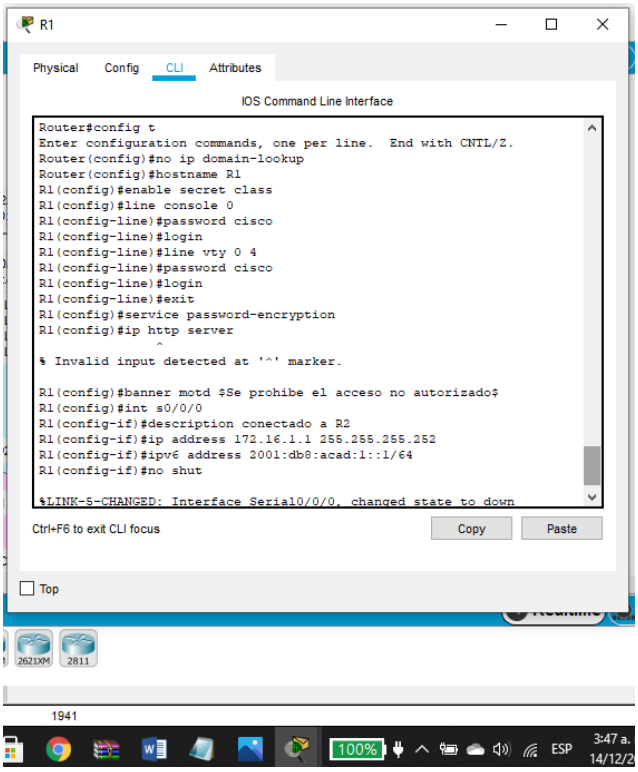
Tabla 15.Configuración R1

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
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login
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)#description connection hacia R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown R1(config-if)#exit
Rutas predeterminadas	R1(config)#int s0/0/0 R1(config-if)#description connection hacia R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#no shutdown

Nota: Todavía no configure G0/1.

Figura 30. Configuración del R1



Fuente: Autor

Se observa la configuración de la interfaz s0/0/0 y las rutas prederminadas.

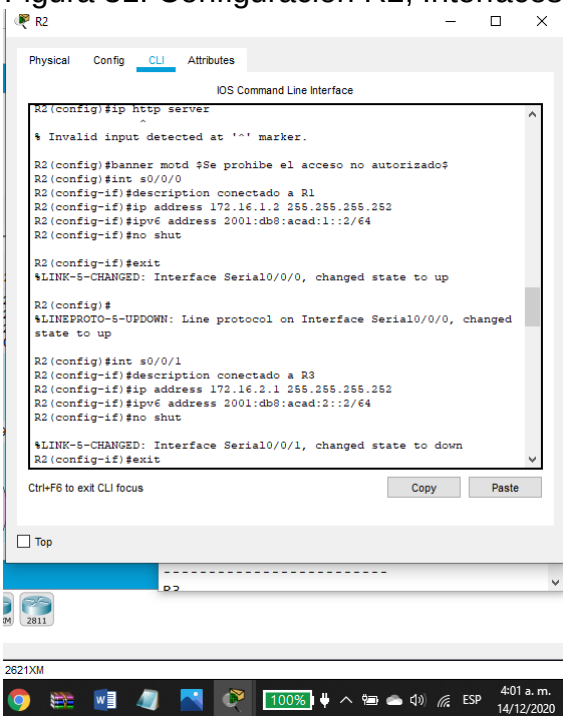
Paso 3: Configurar R2
La configuración del R2 incluye las siguientes tareas:

Tabla 16.Configuración R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
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
Contraseña de acceso Telnet	R2(config-line)#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 (Entrada invalida, este comando no funciona en Packet Tracer)
Mensaje MOTD	R2(config)#banner motd $Se prohibe el acceso no autorizado$
Interfaz S0/0/0	R2(config)#int s0/0/0 R2(config-if)#description conectado a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config)#int s0/0/1 R2(config-if)#description conectado 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)#Clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	R2(config)#int g0/0 R2(config-if)#description conectado a internet R2(config-if)#ip 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 10.10.10.10 255.255.255.252 R2(config-if)#description conectado a servidor web simulado R2(config-if)#exit
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0

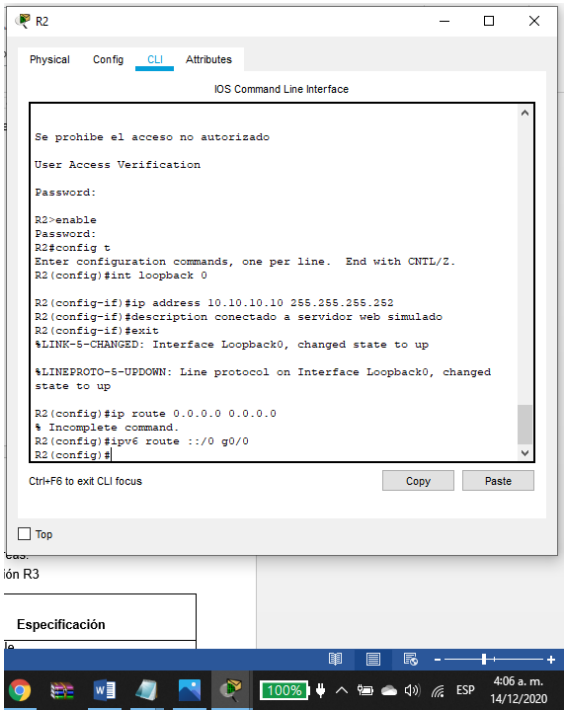
Figura 31. Configuracion R2, Interfaces



Fuente: Autor

En el R2 se hace la configuración de las interfaces con sus direcciones ip

Figura 32. Configuracion R2, Loopback 0 y ruta predeterminada



Fuente: Autor

Se hace la respectiva configuración Interfaz loopback 0 (servidor web simulado) y ruta prederminada.

Paso 4. Configurar R3

Se requiere la configuración del router que proporcione conectividad a nivel de red en el modelo OSI con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que mas adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y asi proporcionar seguridad, se realiza la configuración de las interfaces del dispositivo como la S0/0/1 y la loopback 4,5,6 y 7.

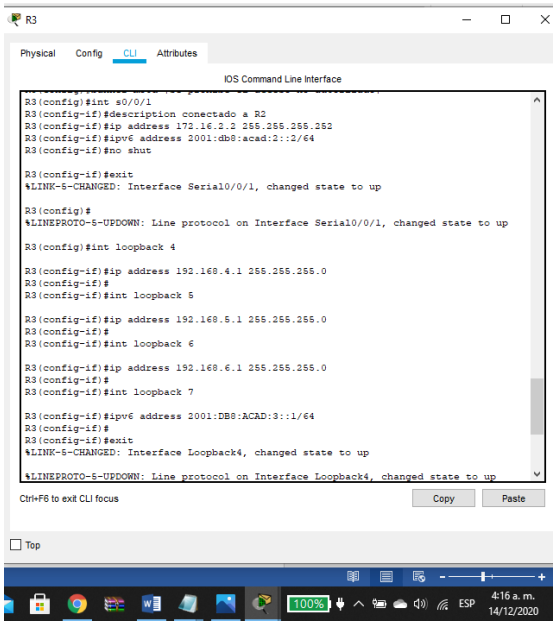
La configuración del R3 incluye las siguientes tareas:

Tabla 17.Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
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
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
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 s0/0/1 R3(config-if)#description conectado a R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252

	R3(config-if)#ipv6 address 2001:db8:acad:2::2/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 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

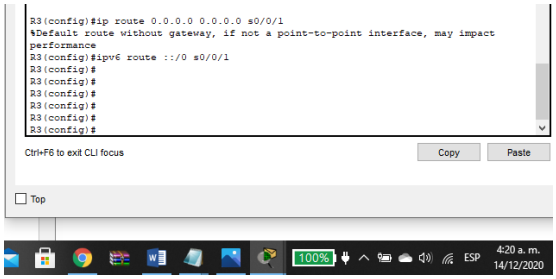
Figura 33.Configuración Interfaces R3



Fuente: Autor

En el R3 se realiza la configuración de las interfaces s0/0/1 y las loopback 4,5,6 y 7

Figura 34. Configuración de la ruta predeterminada



Fuente: Autor

Se colocan los respectivos comandos para la configuración de la ruta predeterminada.

Paso 5. Configurar S1

Se realiza laconfiguración básica teniendo en cuenta el nombre, protección por contraseña, encriptación del mensaje, la contraseña para acceso remoto se configura en line vty 0 4, con el comando "password" seguido de un espacio y la contraseña deseada, por último el mensaje MOTD.

La configuración del S1 incluye las siguientes tareas:

Tabla 18.Configuración S1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#password cisco

	S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	S1(config)#banner motd $Se prohibe el acceso no autorizado$

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 19.Configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config)#service password-encryption
Mensaje MOTD	S3(config)#banner motd $Se prohibe el acceso no autorizado$

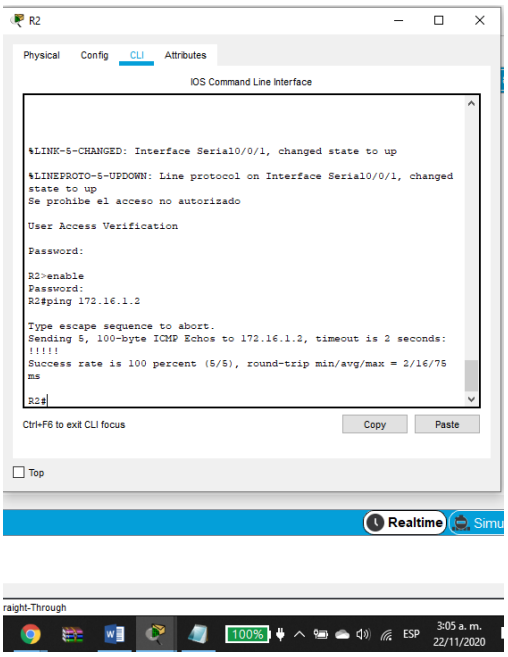
Paso 7: Verificar la conectividad de la red

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 20.Verificar conectividad de red

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

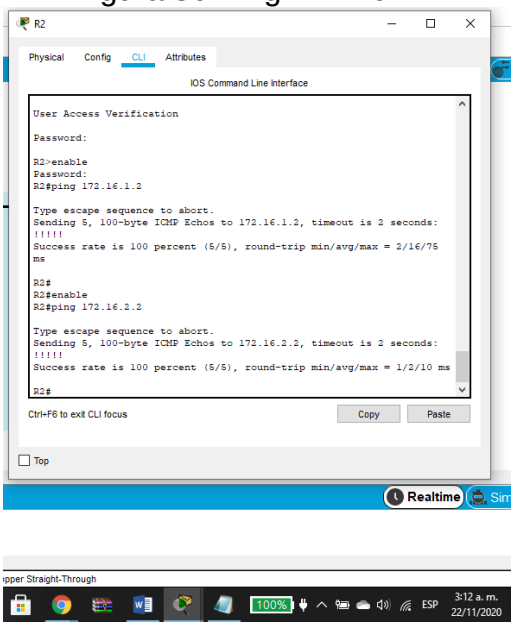
Figura 35. Ping 172.16.1.2



Fuente: Autor

Desde el R1 se hace ping al R2, ip 172.16.1.2 arrojando como resultado la conectividad entre los dos dispositivos.

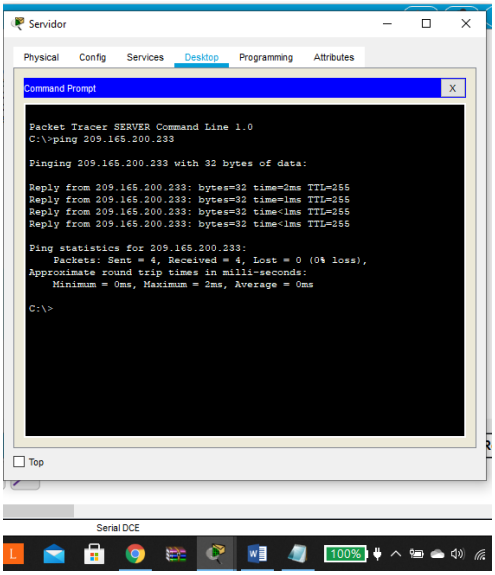
Figura 36.Ping 172.16.2.1



Fuente: Autor

Desde el R2 se hace ping al R3, ip 172.16.2.2 siendo exitoso.

Figura 37.Ping 209.165.200.233



Fuente: Autor

Desde Pc de internet se hace ping al Gateway predeterminado, ip 209.165.200.233 arrojando como resultado la conectividad entre los dos dispositivos.

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

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

Paso 1: Configurar S1

Se crean las bases de datos para VLAN 21,23 y 99, se le asigna una dirección a la ip a la vlan 99 que es la de administración, se asigna el gateway predeterminado y se forzan los enlaces troncales para transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN. Luego se configuran los puertos como puertos de acceso y se asigna F0/6 a la VLAN 21.

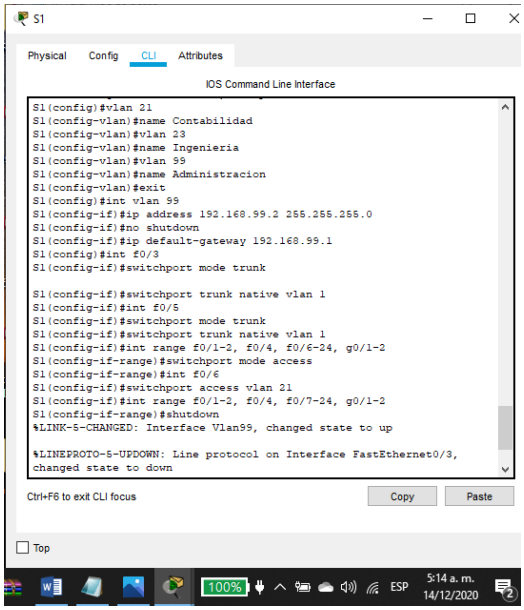
La configuración del S1 incluye las siguientes tareas:

Tabla 21. Configuración de seguridad, Vlans y Routing de vlans del S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1>enable Password: S1#config t 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 S1(config-vlan)#exit
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)#no shutdown
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 trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#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	S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config-if-range)#int f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

Figura 38. Configuración vlans S1



Fuente: Autor

Se realiza la configuración de las vlans en el s1 y se forza la troncal en la interfaz F0/3 y F0/5.

Paso 2: Configurar el S3

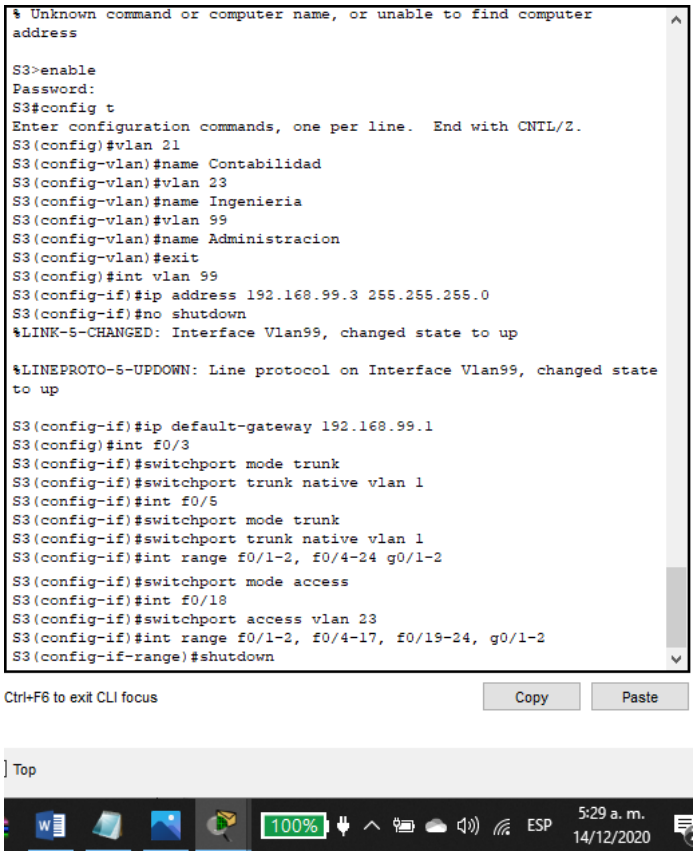
Se crean las bases de datos para VLAN 21,23 y 99, se le asigna una dirección a la ip a la vlan 99 que es la de administración, se asigna el gateway predeterminado y se forzan los enlaces troncales para transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN. Luego se configuran los puertos como puertos de acceso y se asigna F0/18 a la VLAN 23.

La configuración del S3 incluye las siguientes tareas:

Tabla 22.Configuración de seguridad, Vlans y Routing de vlans del S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3>enable Password: S3#config term 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 S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config-vlan)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
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 trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config-if-range)#int f0/18 S3(config-if)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown

Figura 39. Configuración Vlans S3



Fuente: Autor

Se realiza la configuración de las vlans en el s1 y se forza la troncal en la interfaz F0/3 y asignar F0/18 a la VLAN 23.

Paso 3: Configurar R1

En el R1 se configura la subinterface en 802.1Q .21 en G0/1, la 802.1Q .23 en G0/1 y 802.1Q .99 en G0/1 y se activa la interfaz G0/1.

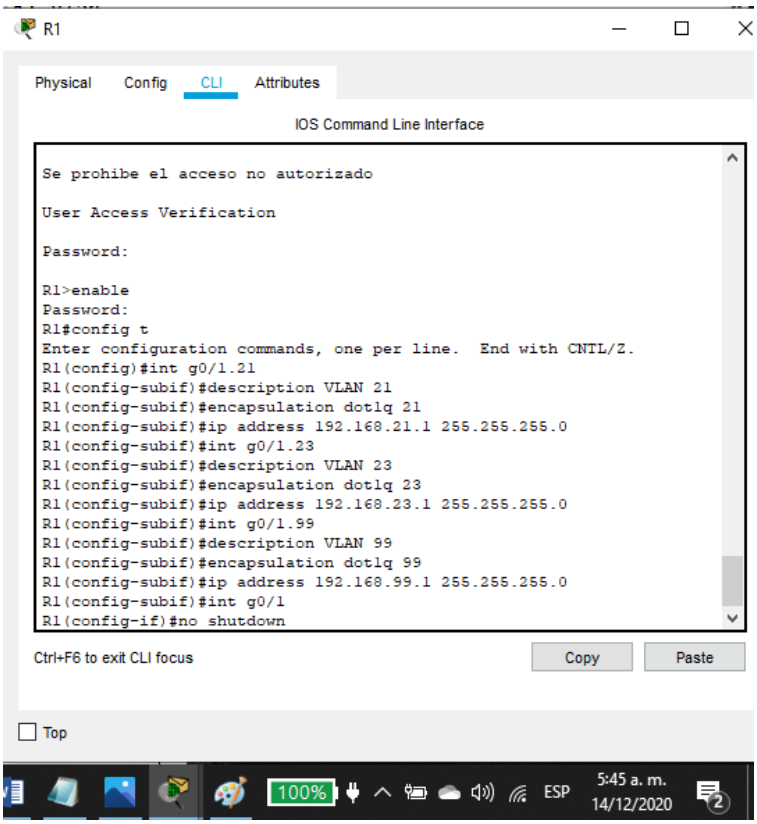
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23.Configuración Vlan R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	R1#config terminal R1(config)#int g0/1.21

	R1(config-subif)#description VLAN 21 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	R1(config-subif)#int g0/1.23 R1(config-subif)#description VLAN 23 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	R1(config-subif)#int g0/1.99 R1(config-subif)#description VLAN 99 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-subif)#int g0/1 R1(config-if)#no shutdown

Figura 40. Configuración Vlan R1



Fuente: Autor

Se hace la configuración de las vlans 21, 23 y 99 en el R1.

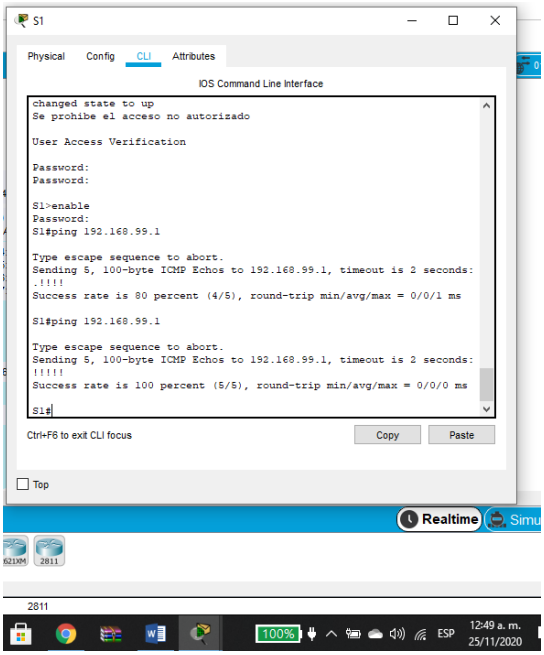
Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 24.Conectividad S1,S3 con R1

Desde	**A**	**Dirección IP**	**Resultados de ping**
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

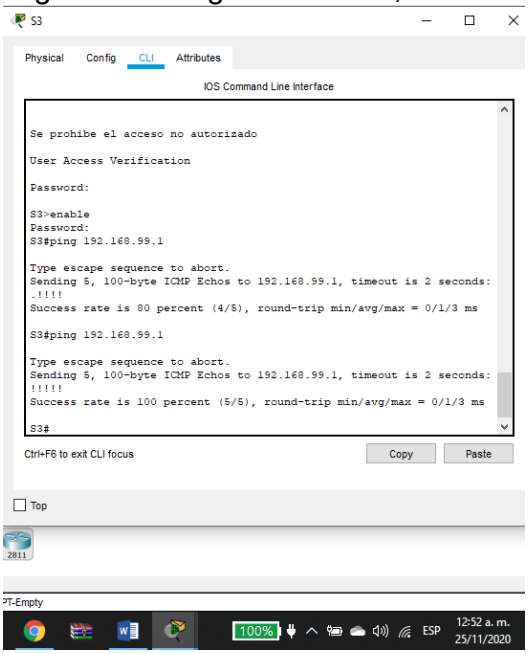
Figura 41.Ping de S1 a R1, Vlan 99



Fuente: Autor

Desde el S1 al R1 dirección Vlan 99 se hace ping, donde la tasa de éxito es 100%.

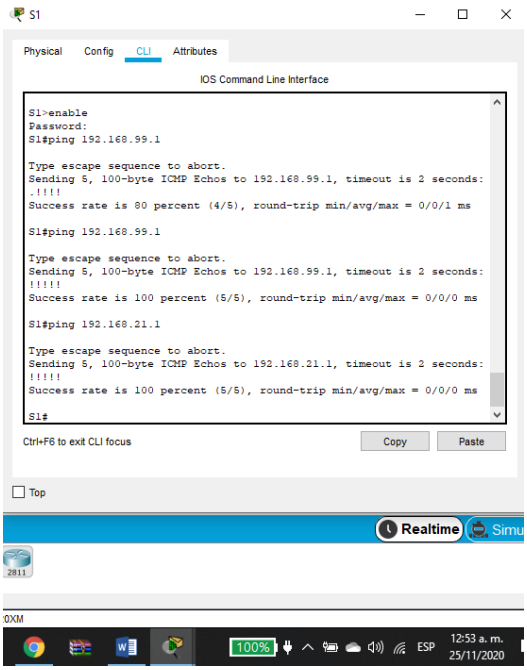
Figura 42. Ping de S3 a R1, Vlan 99



Fuente: Autor

Desde el S3 al R1 dirección Vlan 99 se hace ping, donde la tasa de éxito es 100%.

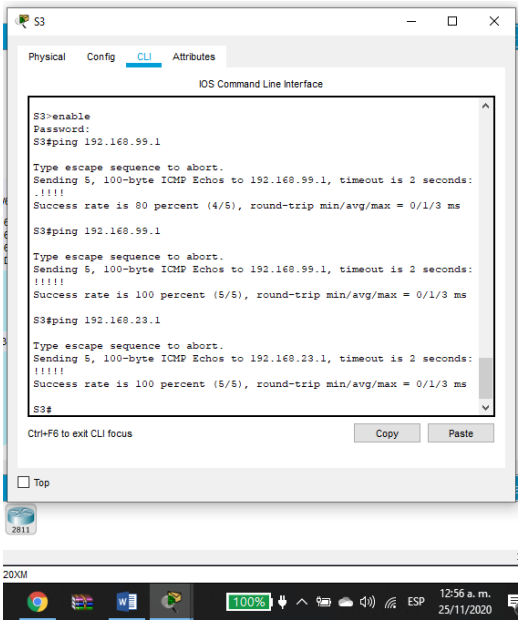
Figura 43. Vlan de S1 a R1, Vlan 21



Fuente: Autor

Desde el S1 al R1 dirección Vlan 21 se hace ping, donde la tasa de éxito es 100%.

Figura 44. Ping S3 a R1, Vlan 23



Fuente: Autor

Desde el S3 al R1 dirección Vlan 23 se hace ping, donde la tasa de éxito es 100%.

Parte 4: Configurar el protocolo de routing dinámico OSPF.

Paso 1: Configurar OSPF en el R1

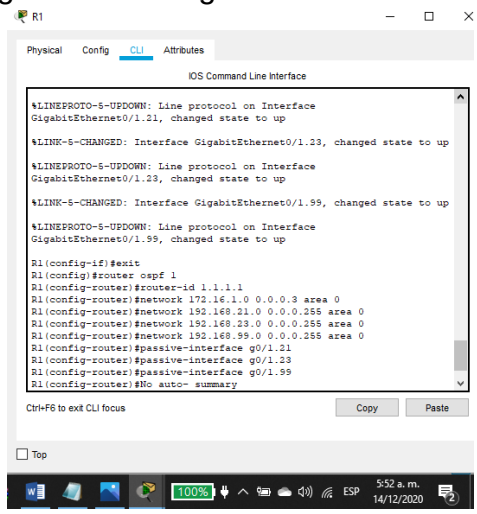
Se configura la OSPF en al area 0 lo que hace que el router dentro de un área mantiene la información completa de la topología del área. Se anuncian las redes conectadas directamente y las interfaces LAN se establecen como pasivas

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 25.Configuración OSPF en el R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1#config terminal 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)#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	R1(config-router)#No auto- summary (Packet Tracer no)

Figura 45. Configuración OSPF en R1



Fuente: Autor

Se realiza la configuración de OSPF en el área 0 del R1 y se establecen todas las interfaces LAN como pasivas.

Con el comando Show ip ospf neighbor en el R1 se visualiza la información de vecino del OSPF relacionado.

Paso 2: Configurar OSPF en el R2

OSPF es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF)

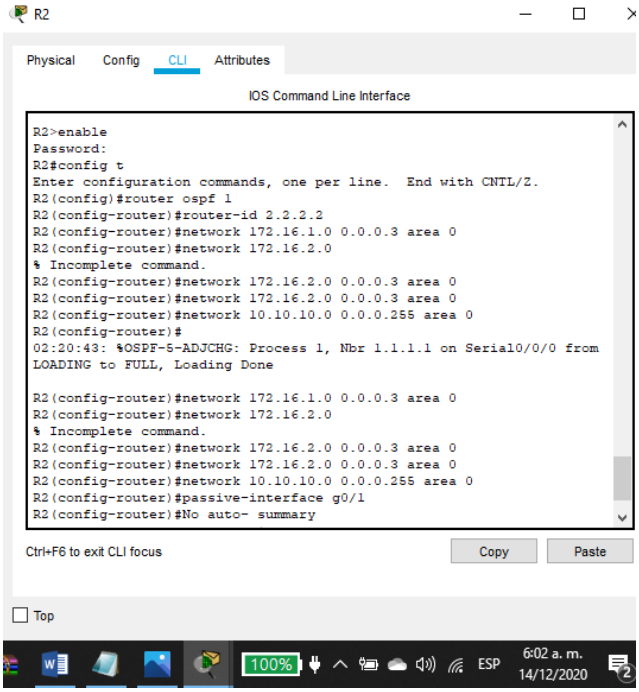
La configuración del R2 incluye las siguientes tareas:

Tabla 26.Configuración 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 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.0 0.0.0.255 area 0

Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface g0/1
Desactive la sumarización automática.	R2(config-router)#No auto- summary

Figura 46. Configuración OSPF en R2



Fuente: Autor

Se realiza la configuración de OSPF en el área 0 del R2 y se establece la interfaz LAN (loopback) como pasiva.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

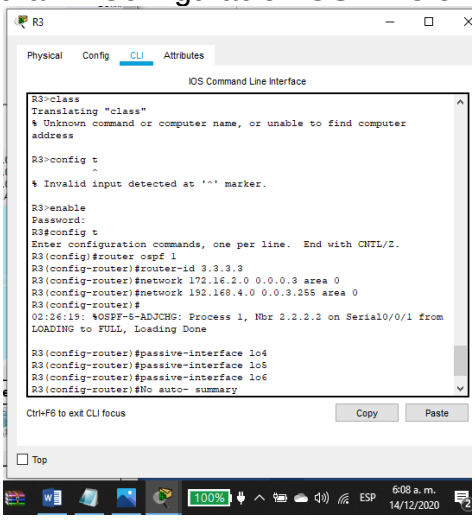
Tabla 27. Configuración OSPFv3 en el R3

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#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 0.0.3.255 area 0
Establecer todas las interfaces de LAN Ipv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6
Desactive la sumarización automática.	R3(config-router)#No auto-summary

Se hace la sumarización y da 192.168.4.0

Figura 47.Configuración OSPFv3 en R3



Fuente: Autor

Se realiza la configuración de OSPF en el área 0 del R3 y se establecen todas las interfaces de LAN Ipv4 (Loopback) como pasivas

Paso 4: Verificar la información de OSPF

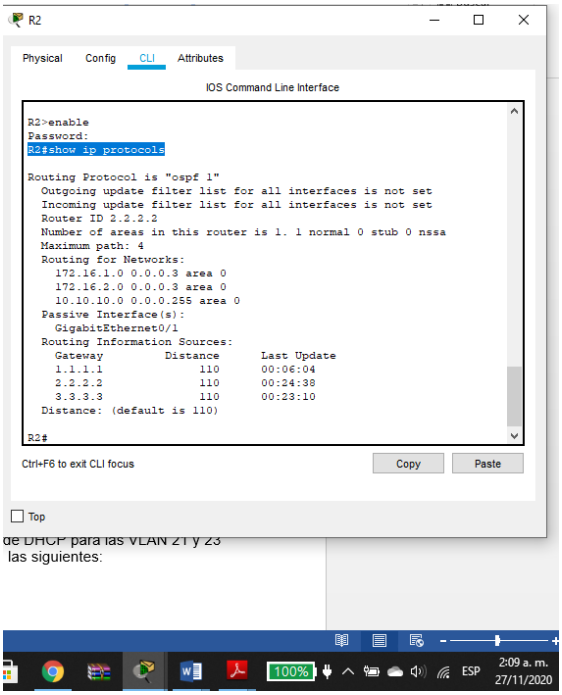
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 28.Verificación funcionamiento de OSPF en R2

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?	R2#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

Emita el comando show ip protocols y verifique que la ID del router sea correcta y que aparezcan las interfaces esperadas en las áreas correspondientes.

Figura 48. R2# Show ip protocols



Fuente: Autor

En el R2 se ejecuta el comando show ip protocols donde muestra la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router.

Parte 5: Implementar DHCP y NAT para IPv4

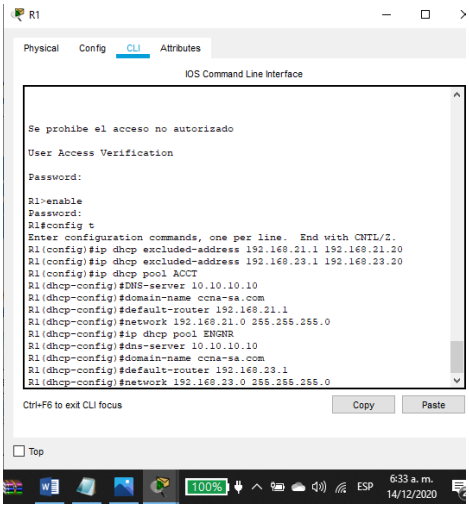
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 29. Configuración de R1 como servidor DHCP

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1#config t R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20.
Crear un pool de DHCP para la VLAN 21.	R1(config)#ip dhcp pool ACCT 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 R1(dhcp-config)#network 192.168.21.0 255.255.255.0
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR 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 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#

Figura 49. Configuración R1 como DHCP



Fuente: Autor

Se hace la configuración del R1 como servidor de DHCP para las VLAN 21 y 23

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

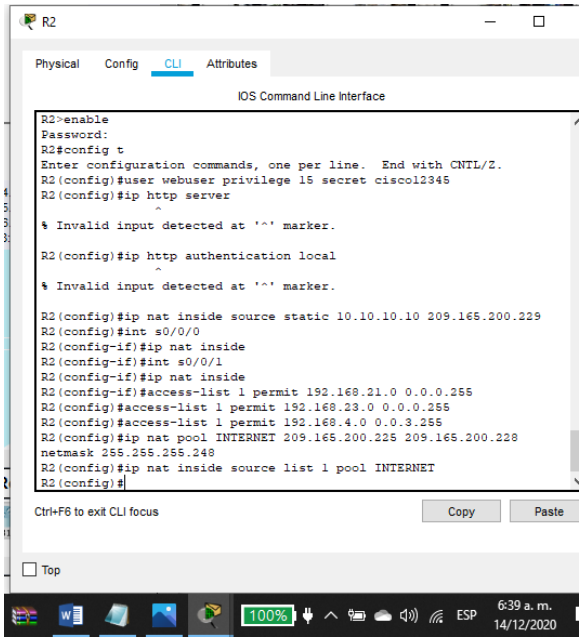
La configuración del R2 incluye las siguientes tareas:

Tabla 30. Configuración NAT, estática y dinámica en R2

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	R2#config t R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (No funciona en Packet Tracer)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local (No funciona en Packet Tracer)
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

Asignar la interfaz interna y externa para la NAT estática	R2(config-if)#int s0/0/0 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	R2#config t 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 R2(config)#
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	R2(config)#ip nat inside source list 1 pool INTERNET

Figura 50.Configuración NAT, estática y dinámica en R2



Fuente: Autor

Se configuro el Servidot HTTP, se creó la Nat estática y se asignó una interfaz interna y externa

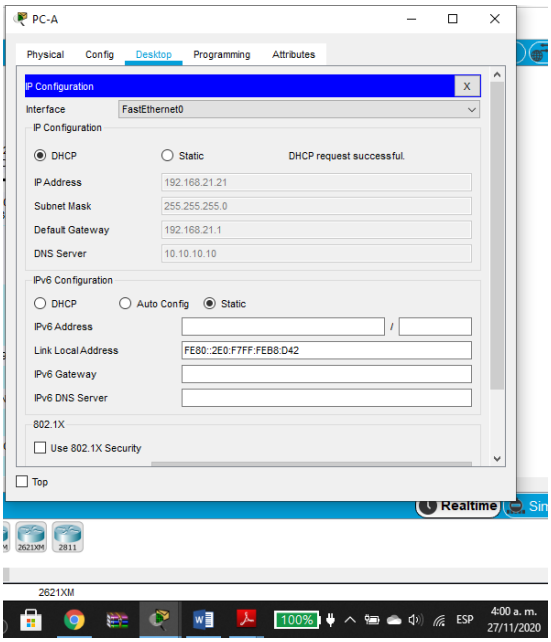
Paso 3: Verificar el protocolo DHCP y la NAT estática

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

Tabla 31. Verificación Protocolo DHCP y Nat estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Estándar
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Ping 192.168.23.21
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**	Falló (ip http server" no funciona en Packet Tracer)

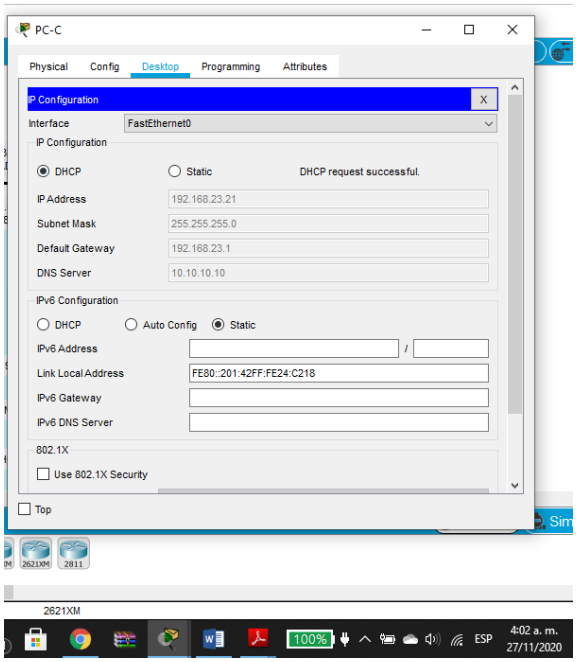
Figura 51. Verificación DHCP en PC-A



Fuente: Autor

En la configuración de la ip del PC-A se da clic en la opción DHCP donde asigna automáticamente una dirección ip.

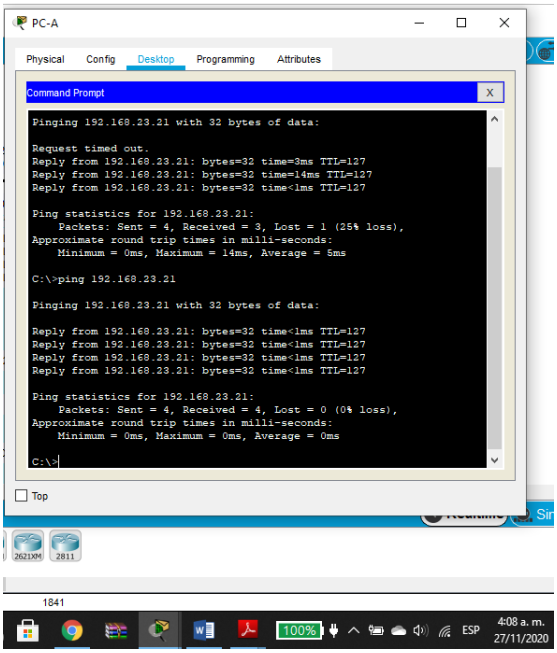
Figura 52.Verificación DHCP en PC-C



Fuente: Autor

En la configuración de la ip del PC-C se da clic en la opción DHCP donde asigna automáticamente una dirección ip.

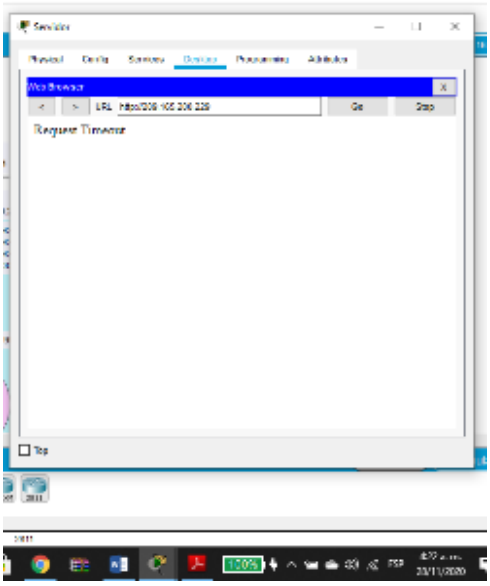
Figura 53.Ping de la PC-A a la PC-C



Fuente: Autor

Desde la PC-A se hace ping a la ip 192.168.23.21 y se comprueba la conexión.

Figura 54.Acceso servidor web 209.165.200.229



Fuente:Autor

Utilizando un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Falló (ip http server" no funciona en Packet Tracer).

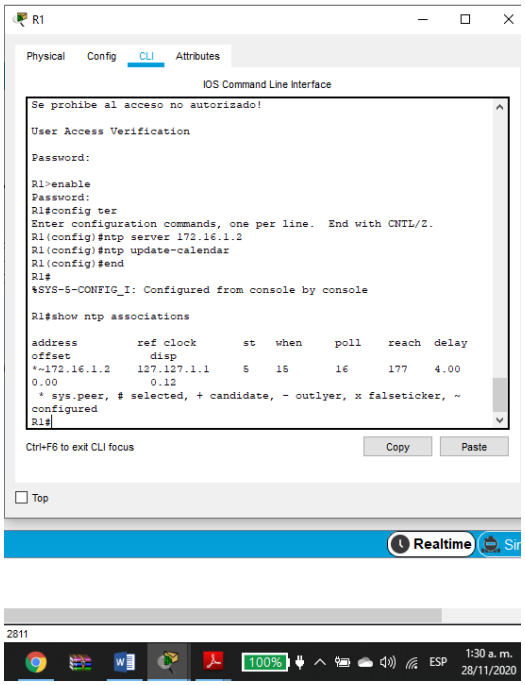
Parte 6: Configurar NTP

El NTP es un protocolo para sincronizar varios relojes de red usando un conjunto de clientes y servidores repartidos. El NTP proporciona los mecanismos de protocolo básicos necesarios para sincronizar los relojes de los diferentes sistemas con una precisión del orden de nanosegundos. Además, contiene indicaciones para especificar la precisión y las posibles fuentes de error del reloj del sistema local. Es así que realiza la configuración de la fecha en el R2, se configura como maestro y luego en el R1 como cliente NTP, las actualizaciones de calendario periodicas con NTP.

Tabla 32. Configuración NTP en R2

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	Password: R2>enable Password: R2#clock set 09:00 05 march 2016
Configure R2 como un maestro NTP.	R2#configure terminal R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1#config terminal R1(config)#ntp server 172.16.1.2 R1(config)#
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar R1(config)#end
Verifique la configuración de NTP en R1.	R1#show ntp associations

Figura 55.R1#show ntp associations



Fuente: Autor

Al ejecutar el comando show ntp associations en el R1 se verifica la configuración de NTP.

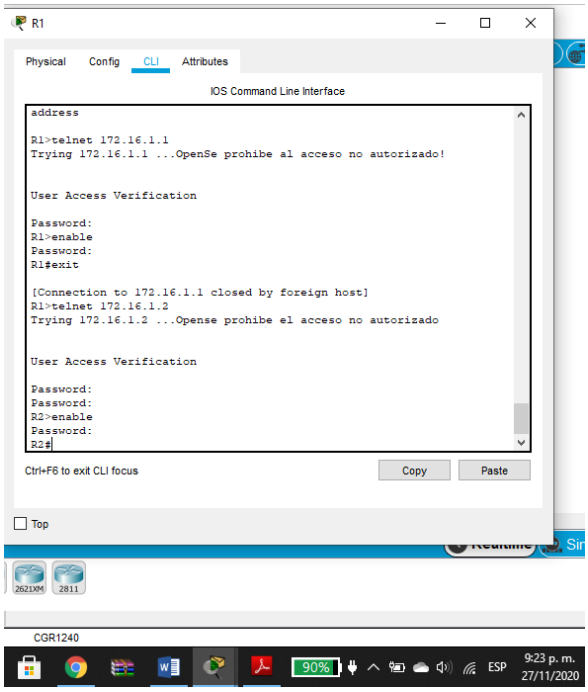
Parte 7: Configurar y verificar las listas de control de acceso (ACL)
Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 33. Configuración ACL

Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que	R2#config terminal R2(config)#ip access-list estándar ADMIN-MGT

solo R1 establezca una conexión Telnet con R2	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 VT	R1(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1>telnet 172.16.1.1

Figura 56.Verificación ACL en R1



Fuente : Autor

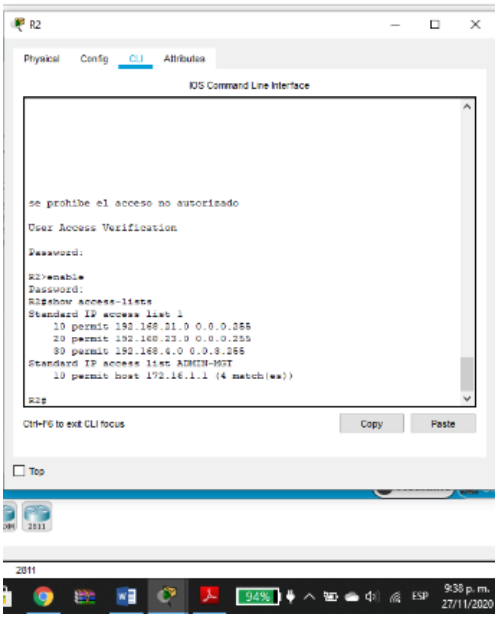
En el R1 se verifica que la ACL funcione.

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

Tabla 34. Verificación de las 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>enable Password: R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 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 ip access-list counters. (Packet Tracer no soporta este comando).
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface
¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation ¿ R2#clear ip nat translation * R2#show ip nat translations

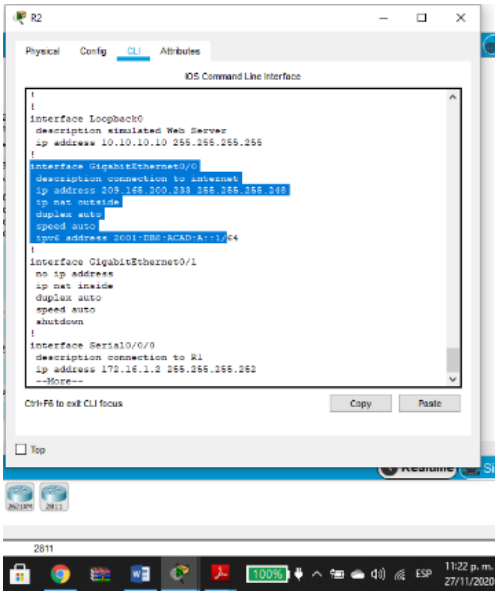
Figura 57.R2#show access-lists



Fuente: Autor

Con el comando show access-lists se muestran las lista de acceso desde la ultima vez que se reestableció.

Figura 58.Show ip access list



Fuente : Autor

Con el comando show ip access-list se muestra solo las listas de acceso IP configuradas en el enrutador.

CONCLUSIONES

Con la solución del escenario uno se logró comprender conceptos y desarrollar habilidades para hacer la configuración básica de una red como si fuera en tiempo real, se logró hacer la diferencia entre la IPv4 y la IPv6 y captar cada uno de los comandos para hacer con mas agilidad y concentración cada paso, el enrutamiento se hizo y se determinó el camino que deben seguir los paquetes de datos con el protocolo ip.

Con la solución del escenario dos se trabajaron mas configuraciones funadamentales asignando protocolos de seguridad y la identificación de otros protocolos de enrutamiento como el OSPF que es muy importante porque facilita el intercambio de comunicación de routing y cuando se gurdan se mantienen en la RAM, ademas aprendí que los cambios que se hacen en la red son mas rápidos.

Al desarrollar los dos escenarios me familiarice con cada instrucción y cada comando, cuando no había solución se buscaba el error y volvía a inciar para lograr la configuración, de nuevo leía y poco a poco comprendi la dedicación y concentración que hay que tener para entregar un buen trabajo que funcione y quedar satisfecho con el deber cumplido.

BIBLIOGRAFÍA

Graziani, R. y Johnson, A. (2008). Conceptos y protocolos de enrutamiento. Guía de estudio de CCNA Exploration. España: Pearson.

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

CISCO. (2019). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

ANEXOS

Anexo 1 link de descarga escenario 1.

https://drive.google.com/file/d/1oPwnQNZ2wChMhEMFAIU6cHBm2iahVaoX/view?usp=sharing

Anexo 2 link de descarga escenario 2.

https://drive.google.com/file/d/1feDUlNt66ld8UqhCWGjO478CRwRfzlVh/view?usp=sharing

Configuración de una red pequeña, Escenario 1

Andrea del Pilar Vargas Cometa

Universidad Nacional Abierta y a Distancia, avargasco@unadvirtual.edu.co

Resumen

Este Artículo hace parte de la presentación y sustentación final del diplomado. En él podrá encontrar la configuración de una red pequeña en Cisco Packet Tracer; es preciso contar con los dispositivos necesarios como un router, dos switches y dos equipos que admitan la conectividad IPv4 e IPv6 para el host soportado. Esta configuración ayuda a asignar una dirección IP vía el protocolo de configuración dinámica de host (DHCP) o manualmente de la IP Address estático. Se configurará el enrutamiento entre Vlan, DHCP, Etherchannel y port-security. Se encuentra también la descripción paso a paso de la configuración de los aspectos básicos de los dispositivos, la infraestructura de red, el soporte de host y por último la verificación de la conectividad de extremo a extremo con imágenes que soportan cada una de las pruebas, las tablas de direccionamiento y los comandos respectivos.

Palabras claves: enrutamiento, host, red, ROUTER SWITCH, DHCP.

Abstract - This Article is part of the presentation and final support of the diploma. In it you will find the configuration of a small network in Cisco Packet Tracer; you need to have the necessary devices such as a router, two switches, and two computers that support IPv4 and IPv6 connectivity for the supported host. This setting helps to assign an IP address via Dynamic Host Configuration Protocol (DHCP) or manually from the static IP address. The routing between Vlan, DHCP, Etherchannel and port-security will be configured. There is also the step-by-step description of the configuration of the basic aspects of the devices, the network infrastructure, the host support and finally the verification of the end-to-end connectivity with images that support each of the tests, addressing tables and respective commands.

Keywords: routing, host, network, ROUTER SWITCH, DHCP.

I. INTRODUCCIÓN

Hoy en dia las empresas necesitan de una buena red que sea segura y rápida donde puedan compartir información o archivos que trabajan en sus computadoras buscando una transmisión de datos mas ágil y eficaz, también buscan economia en el hadware, software y ahorro de espacio; es asi que al estar conectado a una red todos podrán usar el software de red y disponer de menos dispositivos.

En el siguiente artículo se encuentra la solución al escenario 1 que corresponde a la configuración de una red pequeña con los respectivos dispositivos, las direcciones Ip, los comandos que son muy importantes para dar una orden capaz de ser interpretada por el lenguaje informático y asi configurar cada uno de los dispositivos, compartir la información, asegurar la confiabilidad y aumentar la velocidad de transimisión de datos.

II METODOLOGÍA

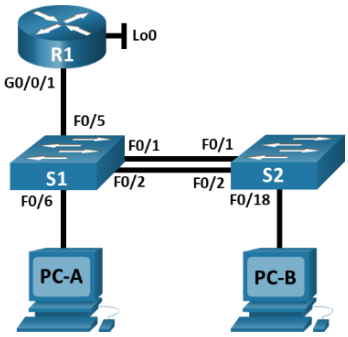
La metodología empleada es la metodología activa ya que es un proceso interactivo basado en la counicación tutor-estudiante y el metodo es teorico- práctico donde a través de enlaces con contenidos teoricos se obtuvo un aprendizaje significativo, se captaron conceptos que luego se llevaron a la práctica, en este caso para dar solución a un escenario.

Antes de dar solución al escenario fue preciso leer y argumentarse de cada tema y luego aplicarlo a través de un programa de simulación. Es importante que primero se obtenga el conocimiento para no llegar a cometer errores y caer en facilidad de no realizar una buena configuración y solucionar el problema.

II. DESARROLLO

Escenario 1

Figura 59.Escenario 1



En la figura 1 se muestra la configuración de los dipositivos.

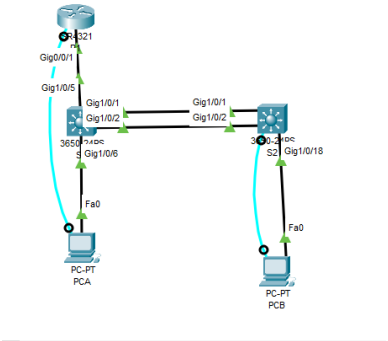
Se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel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

1. IMPLEMENTACIÓN

A. Inicio

[1]Los dispositivos a utilizar consta de un router 4321, 2 switchs 3650 , 2 pc, cable directo y cable de consola, se realiza la respectiva conexión.

Figura 60. Simulación Escenario 1



Fuente: Autor

En la figura 1 se presenta la topología del escenario1 realizada en packet tracer.

2. CONFIGURACIÓN INICIAL

A. Configuración Router y Switchs

- Inicializar y recargar el Router y los switchs

[4] Para realizar la configuración es necesario que los dispositivos esten limpios y que se borren las configuraciones anteriores para que mas adelante no se presenten errores. Por lo anterior se ejecuta el comando erase startup-config para la eliminación de la configuración de inicio y reload para para deshacer los ultimos cambios realizados. En los switchs se eliminan la bases de datos de la Vlan anterior y con el comando Show flash se hace la verificación. Se configura la plantilla SDM para que los switch admitan ipv4 a ipv6 y se recargan de nuevo para que funcionen.

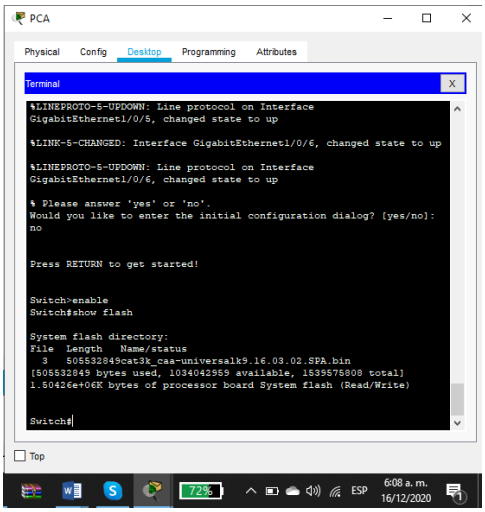
En la tabla 1 se muestran los comandos para inicializar y recargar los dispositivos.

Tabla 35. Inicializar y recargar los dispositvos

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router>enable 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>enable 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>enable Switch#show flash

configurar la plantilla SDM para que admita IPv6	Switch#sdm prefer dual-ipv4-and-ipv6 default Switch#exit Switch#reload

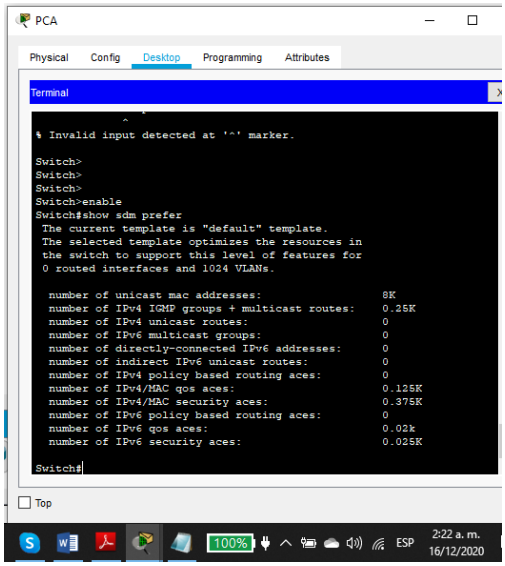
Tabla 36. Show flash



Fuente: Autor

Con el comando show flash se verificó que la base de datos de VLAN no está en la memoria flash luego de haber reinicializado el switch.

Tabla 37. Configuración plantilla smd



Fuente: Autor

Luego de hacer la configuración de la plantilla SMD con el comando Show sdm prefer se verifica la plantilla actual.

- Configurar el Router

[6]Se requiere la configuración del router que proporcione conectividad a nivel de red en el modelo OSI con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que mas adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y asi proporcionar seguridad , la contraseña de acceso a la consola la longitud minima de 10 caracteres, crear un usuario administrativo en la base de datos local para la autenticación.Tambien se configura el inicio de sesión en las líneas VTY para que use la base de datos local, encriptación del mensaje, se establecen las subinterfaces para Ipv4 e Ipv6 y para finalizar se generar una clave de cifrado RSA para encriptar y descifrar datos.

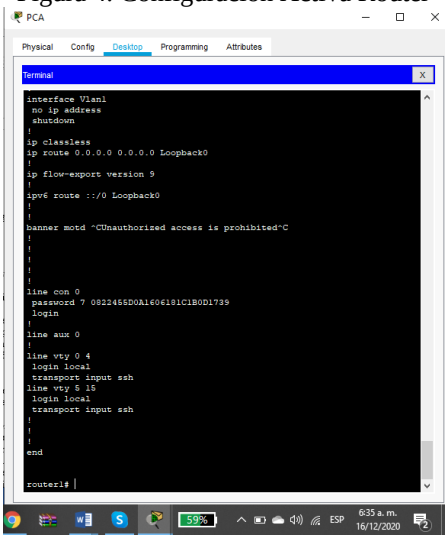
En la tabla 4 se fijan los comandos para la respectiva configuración.

Tabla 38. Configuracion del Router

Tarea	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain lookup
Nombre del router	Router(config)#hostname R1
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 console 0 R1(config-line)#password ciscoconpass R1(config-line)#login
Establecer la longitud mínima para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario administrativo	R1(config)#username admin secret admin1pass

en la base de datos local	
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 R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd $Unauthorized Access is prohibited!$
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
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 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#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 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#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 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#int g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 native R1(config-subif)#description Native R1(config-subif)#int g0/0/1 R1(config-if)#no shutdown R1(config-if)#
Configure el Loopback0 interface	R1(config-if)#int loopback 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)#description internet R1(config-if)#exit
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa R1(config)#

Figura 4. Configuración Activa Router



Fuente: Autor

En la figura 3 con el comando show running-config muestra el contenido del archivo de configuración activo

- Configuración S1 y S2

[1] El switch se encarga de analizar y evaluar las tramas que ingresan por sus puertos de entrada y los filtra para trabajar únicamente en los puertos correctos. [8]Una adecuada configuración proporciona seguridad, correcta comunicación entre los dispositivos y una red estable.

[2] Conectarse al Switch por consola S1>, ir al modo EXEC privilegiado S1>enable S1#, ir al modo de configuración global S1#Config term y realizar laconfiguración básica teniendo en cuenta el nombre, protección por contraseña, encriptación del mensaje, la contraseña para acceso remoto se configura en line vty 0 15, con el comando "password" seguido de un espacio y la contraseña deseada, generar una clave de cifrado RSA, configurar la interfaz de administración (SVI) utilizando el comando S1(config)#int vlan 4 y de esta manera permite crear una SVI asociada a la VLAN cuyo ID se aplica, e ingresar al modo de configuración de esa interfaz, por ultimo la configuración del gateway predeterminado para para precisar el mejor camino hacia un destino remoto.

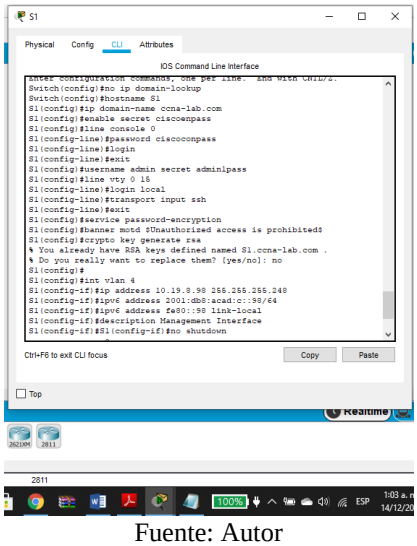
En la tabla 5 se encuentran los comandos para la respectiva configuración del S1.

Tabla 39 configuración S1.

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 S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin 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 S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd $Unauthorized Access is prohibited!$
Generar una claave de cifrado RSA	S1(config)#crypto key generate rsa

Tarea	Especificación
Configurar la interfaz de administración (SVI)	S1(config)# S1(config)#int vlan 4 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)#description Management Interface S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	S1(config)#ip default-gateway 10.19.8.97 S1(config)#

Tabla 5. Configuración S1



Fuente: Autor

Se realiza la configuración del S1 teniendo en cuenta la interfaz de administración y la configuración del gateway predeterminado.

Configuración del S2

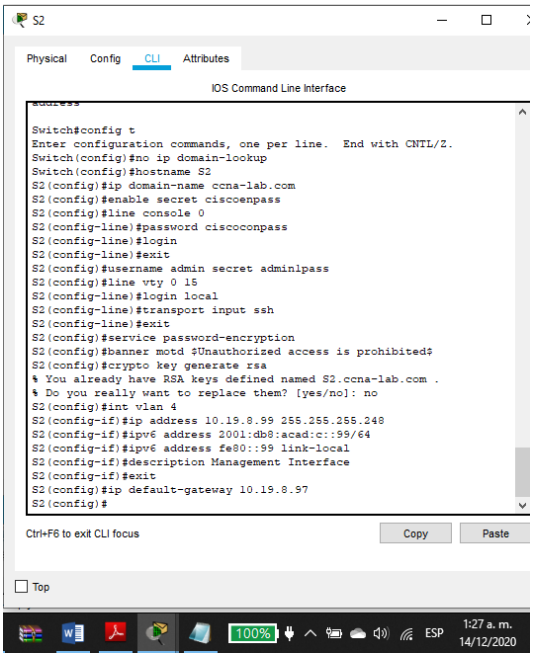
Como se hizo con el switch 1 se hace la configuración respectiva. En la tabla 7 se encuentran los comandos.

Tabla 40. Configuración S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch(config)#no ip domain lookup
Nombre del switch	Switch(config)#hostname S2
Nombre de dominio	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption

Tarea	Especificación
Configurar un MOTD Banner	S2(config)#banner motd $Unauthorized Access is prohibited!$
Generar una clave de cifrado RSA	S2(config)#crypto key generate rsa
Configurar la interfaz de administración (SVI)	S2(config)# S2(config)#int vlan 4 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)#description Management Interface S2(config-if)#no shutdown S2(config-if)#exit S2(config)#ip default-gateway 10.19.8.97 S2(config)#
Configuración del gateway predeterminado	S2(config)#ip default-gateway 10.19.8.97 S2(config)#

Figura 6. Configuración switch 2



Fuente: Autor

En la figura 4 se muestra que en el S2 se hace la configuración teniendo en cuenta la interfaz de administración y la configuración del gateway predeterminado

B. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

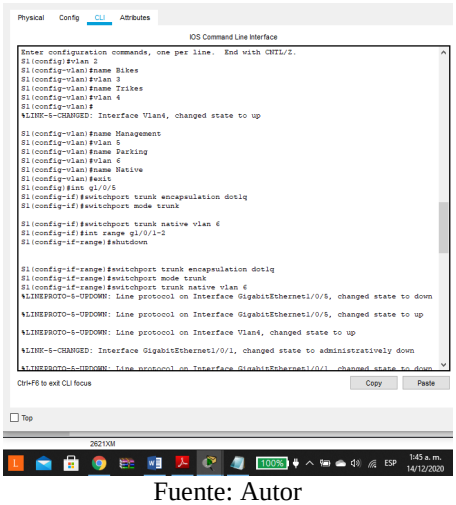
[9]Se crean las vlans en el S1 para garantizar la calidad del servicio y agrupar los usuarios en en grupos específicos, luego se crean las troncales que utilizan las vlan 6 en las interfaces 1,2 y 5. Es de recordar que las intrefaces 1 y 2 se apagan para luego configurar EtherChannel. Para crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 se utiliza el comando channel-group 1 mode active de manera que el modo LACP coloca un puerto en un estado de negociación activa, en el que el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP. Se configura el puerto de acceso de host para VLAN 2 para interface 6 de esta manera queda el puerto asignado a la VLAN 2 cambiando al modo permanente. Se configura la seguridad del puerto en los puertos de acceso que hace que haya seguridad y se reestringe la entrada de mas interfaces.

En la tabla 7 se encuentran los comandos para la configuración.

Tabla 7. Configuración S1 Vlan 2

Tarea	Especificación
Crear VLAN	S1(config)# 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)# 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 S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1(config)#int g1/0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)# S1(config-if)#switchport trunk native vlan 6 S1(config-if)#int range g1/0/1-2 S1(config-if-range)#shutdown S1(config-if-range)# S1(config-if-range)#switchport trunk encapsulation dot1q 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-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switch trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	S1(config-if)#int g1/0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	S1(config-if)#int range g1/0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In Use S1(config-if-range)#shutdown S1(config-if-range)# S1(config-if-range)#int range g1/0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown S1(config-if-range)#int range g1/1/1-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description Not In use S1(config-if-range)#shutdown S1(config-if-range)#

Figura 7. Creación de las Vlans en el S1



Fuente: Autor

En la figura 5, en el S1 se crean las vlans 2,3,4,5 y 6 y las troncales para la Vlan 6, Nativa

Configurar Switch 2

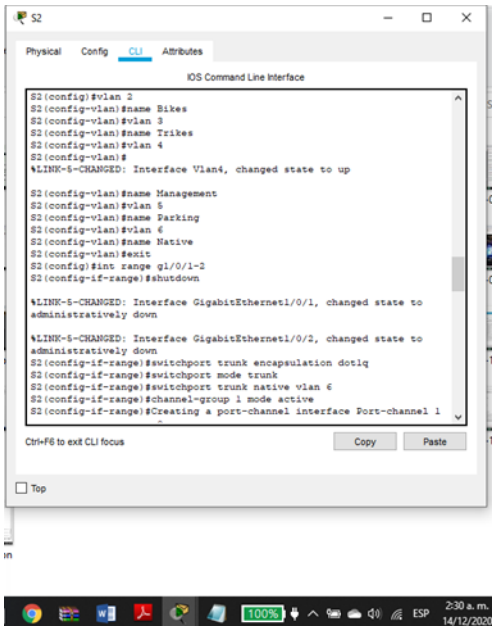
[10]Se siguen los pasos de confguración del S1 teniendo en cuenta que en el paso configurar el puerto de acceso del host es para la VLAN 3. En la tabla se encuentran los comandos para realizar la configuración.

Tabla 2. Configuración S2 Vlan 3

Tarea	Específicación
Crear VLAN	S2>enable Password: Password: S2#config term 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)# 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 S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#int range g1/0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q
	S2(config-if-range)#switchport mode trunk S2(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	S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 S2(config-if-range)#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
Configurar el puerto de acceso del host para la VLAN 3	S2(config-if)#int g1/0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	S2(config-if)#int range g1/0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In Use

	S2(config-if-range)#shutdown S2(config-if-range)#int range g1/1/19-24 interface range not validated - command rejected S2(config)#int range g1/0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description Not In use S2(config-if-range)#shutdown S2(config-if-range)#

Figura 8. Creación de las vlans y troncales en S2



Fuente: Autor

En estta figura se muestra que el el S2 se crean las vlans 2,3,4,5 y 6 y las troncales para la Vlan 6, Nativa.

C. Configurar soporte de host

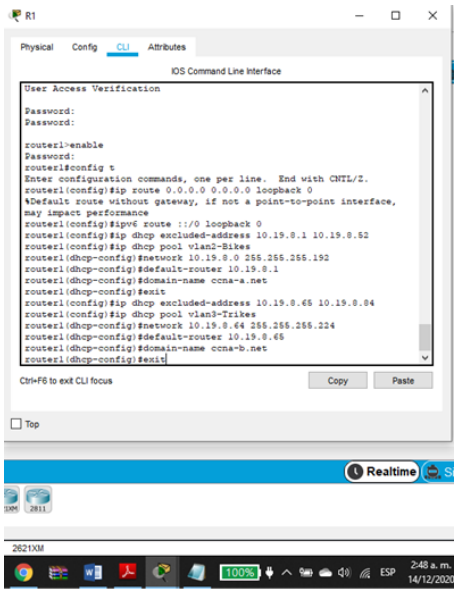
Se inicia la configuración del soporte de host con el almacenamiento de una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing y luego se [3]configurar IPv4 DHCP para VLAN 2 y 3.

En la tabla 8 se encuentran los comandos para realizar la respectiva configuración.

Tabla 41. Configuración soporte host

Tarea	Especificación
Configure Default Routing	R1>enable Password: R1#config term 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	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 R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	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 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Figura 961. Configuración soporte de host R1



Fuente: Autor

En la figura 7 se evidencia la configuración del soporte host y se verifica la creación de los DHCP para vlan 2 y 3

D. Configuración de los servidores

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

Tabla 42. Configuración de red de PC-A

Configuración de red de PC-A	
Descripción	En el PCA se ingresa a la IP configuration y se da clic en DHCP para ipv4 se encuentra la Dirección Ip, a mascara de subred, la puerta de enlace.
Dirección física	0050.0F8C.5851
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::250:FFF:FE8C:5851

Tabla 43. Configuración de red de la PC-B

Configuración de red de PC-B	
Descripción	En el PCB se ingresa a la IP configuration y se da clic en DHCP pa ipv4 se encuentra la Dirección Ip, a mascara de subred, la puerta de enlace.
Dirección física	0050.0F8C.5851
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::260:5CFF:FE44:190C

3. VERIFICAR LA CONECTIVIDAD DE RED

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

Tabla 44. Tabla conectividad dispositivo de red

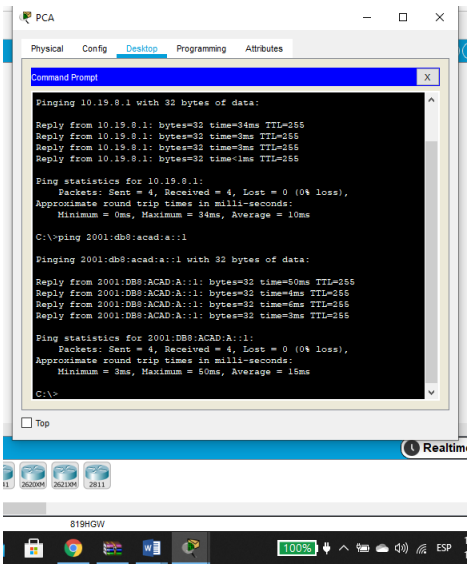
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Exitoso*
		IPv6	2001:db8:acad:a: :1	Exitoso
	R1, G0/0/1.3	Dirección	10.19.8.65	Exitoso
		IPv6	2001:db8:acad:b: :1	Exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	Exitoso
		IPv6	2001:db8:acad:c: :1	Exitoso
	S1, VLAN 4	Dirección	10.19.8.98	Exitoso
		IPv6	2001:db8:acad:c: :98	Exitoso
	S2, VLAN 4	Dirección	10.19.8.99.	Exitoso
		IPv6	2001:db8:acad:c: :99	Exitoso
	PC-B	Dirección	IP address will vary.	Exitoso
		IPv6	2001:db8:acad:b: :50	Exitoso
	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
		IPv6	2001:db8:acad:209: :1	Exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Exitoso*
		IPv6	2001:db8:acad:209: :1	Exitoso
	R1, G0/0/1.2	Dirección	10.19.8.1	Exitoso
		IPv6	2001:db8:acad:a: :1	Exitoso
	R1, G0/0/1.3	Dirección	10.19.8.65	Exitoso
		IPv6	2001:db8:acad:b: :1	Exitoso
	R1, G0/0/1.4	Dirección	10.19.8.97	Exitoso
		IPv6	2001:db8:acad:c: :1	Exitoso
	S1, VLAN 4	Dirección	10.19.8.98	Exitoso

De sde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c: :98	Exitoso
	S2, VLAN 4	Dirección	10.19.8.99.	Exitoso
		IPv6	2001:db8:acad:c: :99	Exitoso

Ahora se hace ping para probar los dispositivos de red

En las siguientes figuras se detalla que si hay conectividad con lo solicitado en la tabla 11.

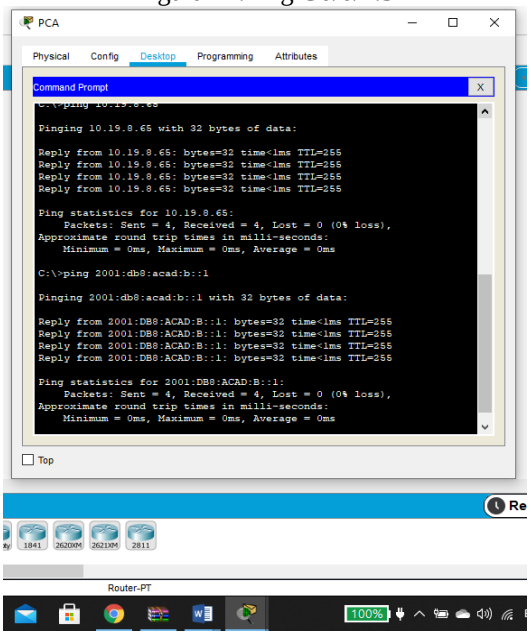
Figura 10. Ping de PC-A al R1



Fuente: Autor

En la figura 4 se muestra el ejemplo del ping que se realizó para comprobar la conectividad del PC-A al R1

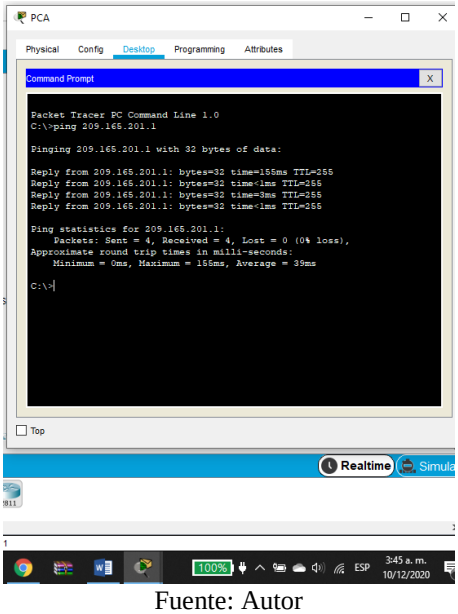
Figura 11.Ping G0/0/1.3



Fuente: Autor

Desde el PC-A se hace ping a la ip 10.19.8.65 siendo éxito

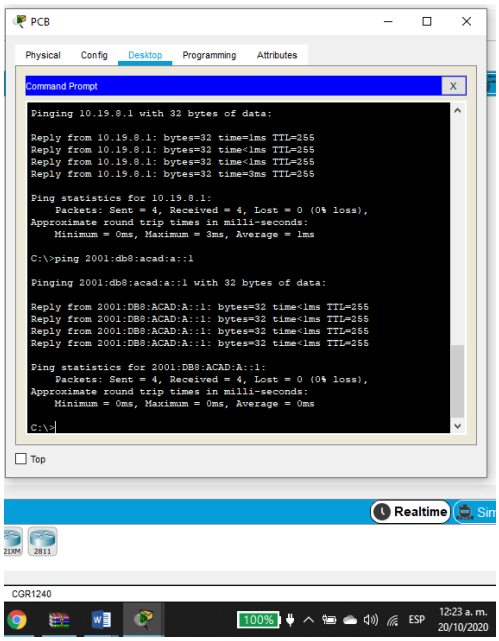
Figura 12. Ping R1 Bucle 0



Fuente: Autor

Desde el PC-A se hace ping al R1 Bucle 0 con ip 209.165.201.1 y hay conectividad.

Figura 13. Ping de PC-B a R1 G0/0/1.2



Fuente: Autor

Desde el PC-B se hace ping al R1 G0/0/1.2 con ip 10.19.8.1 y hay conectividad

IV CONCLUSIONES

Las redes pequeñas se convierten en una herramienta para compartir recursos, asegurar la confiabilidad y disponibilidad de la información, reducir costos de las acciones. Por otra parte, la facilidad para acceder a documentos alojados en cualquier nodo de la red, es muy útil a la hora de realizar un trabajo en conjunto. Todo esto mejora el trabajo en equipo y la participación de todas los integrantes en determinada empresa.

Se necesitan responsables del manejo de la red en caso de fallas y sobre todo para el mantenimiento de los dispositivos, esto requiere un mejor conocimiento y la responsabilidad estaría en las personas con más capacidades para cada una las necesidades que requiera el manejo de redes pequeña.

IV. REFERENCIAS

[1] CISCO. (2019). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#1

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

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

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

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

[6] CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

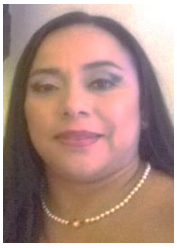
[7] A. S. Tanenbaum, Redes de Computadoras, Editorial Prentice Hall, tercera edición, 1997. Recuperado de : https://www.academia.edu/25306593/Redes_de_Computadoras_3ra_Edici%C3%B3n_Andrew_S_Tanenbaum_FREELIBROS_ORG

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

[9]CISCO. (2019). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1

[10] CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

Biografía



Andrea del Pilar Vargas Cometa, nace el 26 de Septiembre de 1980 en Belalcázar Páez Cauca, realizó sus estudios primarios y secuendarios en la Institución Educativa Normal Superior Enrique Vallejo de Tierradentro, donde obtiene el Titulo de Bachiller Académico con Énfasis en Pedagogía y continua en la misma Institución obteniendo el titulo de Normalista Superior. En la actualidad adelanta estudios en Ingeniría de sistemas en la Universidad Abierta y a Distancia UNAD y cursa el Diplomado en Profundización

Cisco. Trabaja en la Dirección de Núcleo Educativo de Rosas Cauca de la Secretaría Educación del Cauca.