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

LUZ ADRIANA BARAJAS MURCIA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI

INGENIERÍA DE TELECOMUNICACIONES

BOGOTA

2020

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

LUZ ADRIANA BARAJAS MURCIA

Trabajo presentado como requisito para optar el título de
INGENIERA DE TELECOMUNICACIONES

INGENIERO
DIEGO EDINSON RAMIREZ

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI

INGENIERÍA DE TELECOMUNICACIONES

BOGOTA

2020

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, 20 de octubre de 2020

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1 GLOSARIO

DIRECCIÓN: Es el medio por el que la estación de envío o control selecciona la estación a la que envía los datos. Las direcciones identifican ubicaciones de recepción o de almacenamiento. Una dirección física es un código exclusivo asignado a cada dispositivo o estación de trabajo que esté conectado a una red.

PROTOCOLO: Conjunto de normas para el manejo de las comunicaciones a nivel físico o lógico. Definen cómo se entrega la información, cómo se adjunta para que alcance su destino de forma segura y la vía de acceso que sigue. Los protocolos también coordinan el flujo de mensajes y los acuses de recibo.

RED: Es la combinación de dos o más sistemas y los enlaces de conexión de los mismos. Una red física es el hardware que configura la red. El software y el modelo conceptual componen la red lógica.

ROUTER: Es un dispositivo que proporciona conectividad e interconexión entre redes informáticas. Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.

SWITCH: Es un elemento dentro de una red que permite conectar varios dispositivos, como computadoras, impresoras y servidores; en la misma red dentro de una oficina o edificio. Permite a los dispositivos conectados compartir información y comunicarse entre sí.

2 RESUMEN

En esta presentación se realizará el desarrollo de dos escenarios de topologías de red, donde procederemos a configurar los diferentes equipos con el fin de dar solución a los requerimientos solicitados para cada caso empleando direccionamiento y enrutamiento para IPv4 e IPv6. Posteriormente se efectuarán las pruebas respectivas donde se podrá comprobar la configuración exitosa en cada topología.

3 ABSTRACT

In this presentation we will develop two network topology scenarios, where we will proceed to configure the different equipment in order to provide a solution to the requirements requested for each case using IPv4 and IPv6 addressing and routing. Afterwards, the respective tests will be carried out where the successful configuration in each topology can be verified.

4 INTRODUCCIÓN

En este trabajo se muestran los conocimientos adquiridos durante lo visto en el diplomado Cisco CCNA LAN- WAN por medio de la simulación de topologías de red en Packet Tracert, permitiendo la ejecución de configuraciones, ajustes y pruebas para confirmar que todo se efectúo bajo las indicaciones proporcionadas.

Se analizan los dos escenarios planteados, se valida el direccionamiento a asignar, se efectúan las configuraciones necesarias en Packet Tracert, mostrando las habilidades adquiridas en el curso.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Aplicar los conocimientos adquiridos durante el estudio realizado en el diplomado de Cisco CCNA LAN WAN, se efectuará la resolución de dos escenarios en los cuales se deben aplicar configuraciones bajo los lineamientos que se brindan en la guía.

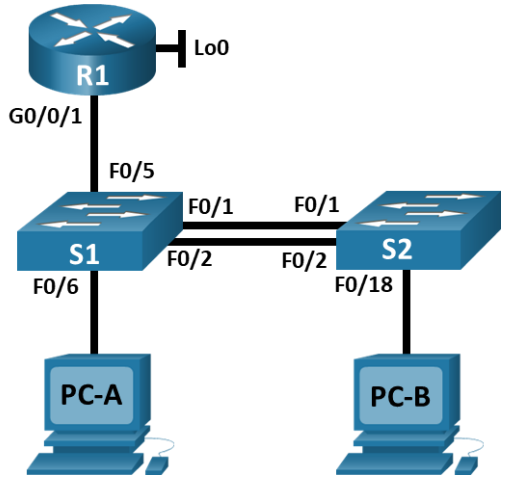
5.2 OBJETIVOS ESPECÍFICOS

Identificar el proceso de configuración a aplicar en cada una de las actividades que componen los escenarios asignados.

Realizar las configuraciones correspondientes en Packet Tracert, efectuar los ajustes que apliquen de acuerdo al análisis con el fin de dar solución a los escenarios planteados.

6 ESCENARIO 1

Figura 1. Topología propuesta escenario 1



En este primer escenario se configurarán los dispositivos de una red pequeña. Se 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.

En la tabla 1 se muestra la información de las VLAN a configurar.

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

Tabla 1. Tabla de VLAN

En la tabla 2 observamos el direccionamiento a configurar para las interfaces de los diferentes equipos.

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
R1 G0/0/1.2	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
R1 G0/0/1.4	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
S2 VLAN 4	2001:db8:acad:c: :99 /64	No corresponde
S2 VLAN 4	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
PC-B NIC	2001:db8:acad:b: :50 /64	fe80::1

Tabla 2. Tabla de asignación direcciones

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

6.1 CONFIGURACIÓN ASPECTOS BÁSICOS DISPOSITIVOS

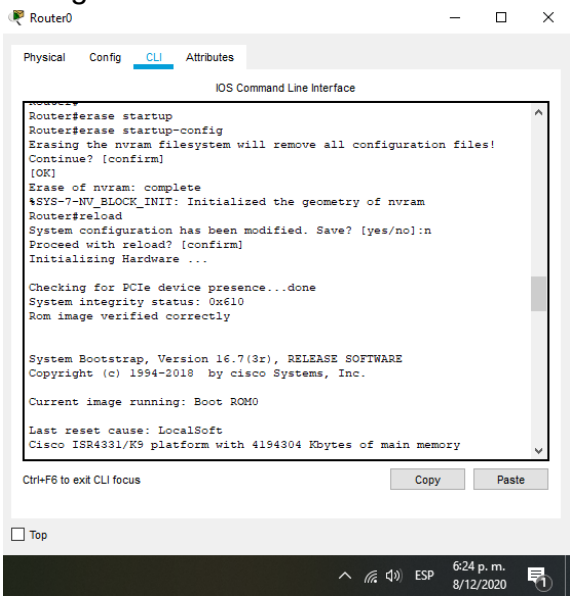
Antes de iniciar la configuración de los dispositivos se deben preparar los equipos para evitar errores, para esto se procede con la eliminación de la configuración que se tenga tanto en Router como en Switches. A continuación se muestran los comandos empleados en cada equipo.

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

Tabla 3. Comando de inicializar dispositivos

En la figura 2 se observa la eliminación de la configuración del router por medio del comando erase startup-config, posterior a confirmar la ejecución se realiza reinicio del equipo.

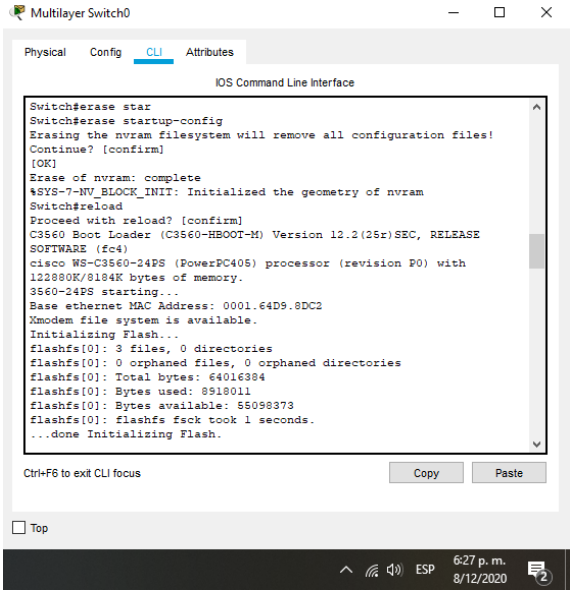
Figura 2. Eliminación configuración Router



Fuente: Autor

En la figura 3 se evidencia la eliminación de la configuración existente el Switch, este comando se ejecuta en S1 y S2, debido a que los equipos son nuevos no se encontraron vlan a eliminar por medio del comando show flash.

Figura 3. Eliminación configuración Switches



Fuente: Autor

Para dar solución a este escenario se procede a realizar la configuración en el Router, Switch 1 y Switch 2 de los nombres de los dispositivos, dominio, contraseñas de seguridad, mensaje de alerta al ingresar a los equipos, direccionamiento de las interfaces y la clave de cifrado. Estas configuraciones se ejecutan en modo configure terminal y configuración de interfaces.

Las tablas siguientes muestran los comandos ejecutados para cumplir con la configuración solicitada en cada equipo.

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router R1	Router#config t Router(config)#hostname R1
Nombre de dominio ccna-lab.com	R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado - ciscoenpass	R1#config t R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola - ciscoconpass	R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas - 10 caracteres	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local Nombre de usuario: **admin** Password: **admin1pass**	R1#config t R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#config t R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd "Este es un sistema seguro. Solo acceso autorizado" R1(config)#exit

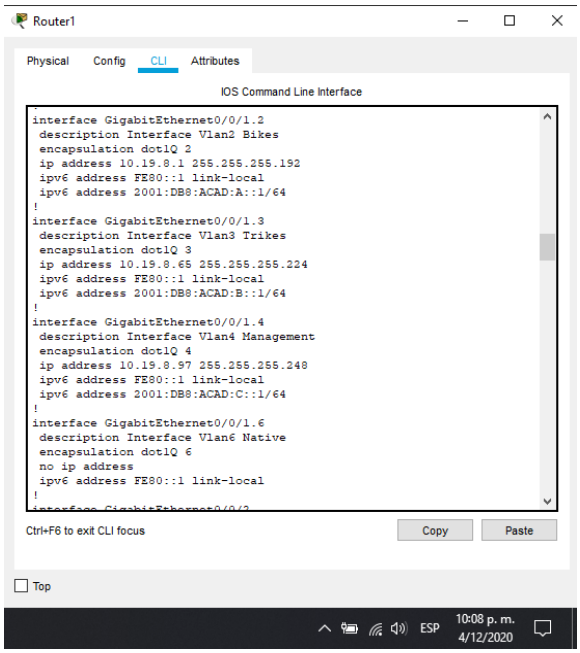
Tarea	Especificación
Habilitar el routing IPv6	R1#config t R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.	R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Interface Vlan2 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)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Interface Vlan3 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)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description Interface Vlan6 Native R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Interface Vlan4 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)#no shutdown

Tarea	Especificación
Configure el Loopback0 interface Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**	R1(config)#interface 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)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA - Módulo de 1024 bits	R1(config)#crypto key generate rsa general-keys modulus 1024

Tabla 4. Tabla de configuración Router

En la tabla 4 se plasmaron los comandos empleados en la configuración del router, con lo ejecutado en el equipo al ingresar muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado, adicionalmente, se configuraron las direcciones ip en las subinterfaces y la interfaz Loopback.

Figura 4. Show run R1



Fuente: Autor

En la figura 4 se observa la configuración de las subinterfaces en el Router 1 por medio del comando show run.

En la tabla 5 se muestran los comandos ejecutados en el switch 1.

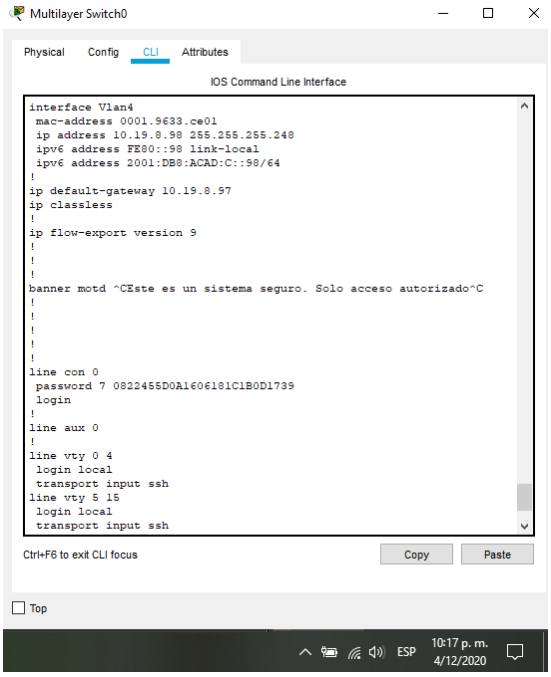
Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch S1	Switch(config)#hostname S1 S1(config)#
Nombre de dominio ccna-lab.com	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola ciscoconpass	S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass	S1#config t S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#config t S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S1(config)#line vty 5 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#line vty 5 15 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 "Este es un sistema seguro. Solo acceso autorizado"
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#crypto key generate rsa general-keys modulus 1024

Tarea	Especificación
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 4 S1(config-if)#no shutdown 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
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config)#ip default-gateway 10.19.8.97 S1(config)#exit

Tabla 5. Tabla configuración S1

Despues de la ejecución realizada en el switch 1, el equipo al ingresar muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado, se configuró la interfaz de administración correspondiente a la interface vlan 4 y el gateway predeterminado.

Figura 5. Show run S1



Fuente: Autor

En la figura 5 se observa la configuración de la interface Vlan4 y el Gateway predeterminado en el Switch 1 por medio del comando show run.

Los comandos ejecutados en el switch 2 se visualizan en la tabla 6.

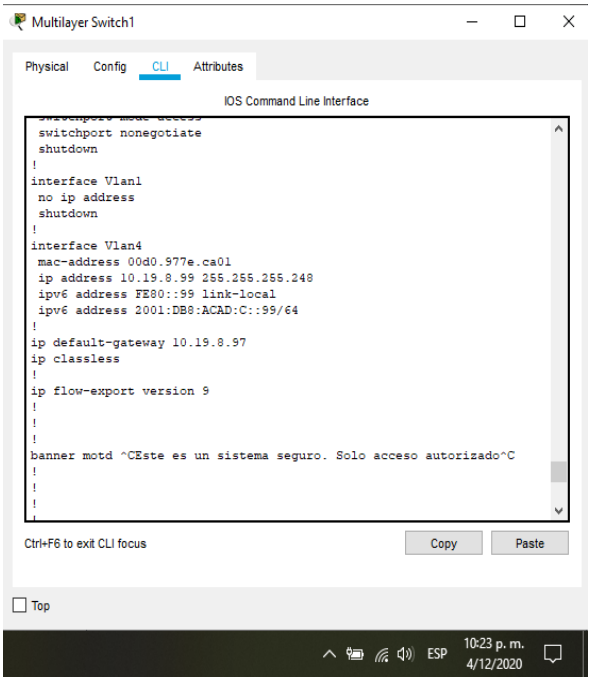
Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch S2	Switch(config)#hostname S2
Nombre de dominio ccna-lab.com	S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado ciscoenpass	S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola ciscoconpass	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 Nombre de usuario: admin Password: admin1pass	S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 4 S2(config-line)#login local S2(config-line)#exit S2(config)#line vty 5 15 S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#line vty 5 15 S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2#config t S2(config)#banner motd "Este es un sistema seguro. Solo acceso autorizado"
Generar una clave de cifrado RSA Módulo de 1024 bits	S2(config)#crypto key generate rsa general-keys modulus 1024

Tarea	Especificación
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S2(config)#interface vlan 4 S2(config-if)#no shutdown 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)#exit
Configuración del gateway predeterminado - Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4	S2#config t S2(config)#ip default-gateway 10.19.8.97 S2(config)#exit

Tabla 6. Tabla configuración S2

En el switch 2 al ejecutar los comandos nombrados se observa que al ingresar muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado, se configuró la interfaz de administración correspondiente a la interface vlan 4 y el gateway predeterminado.

Figura 6. Show run S2



Fuente: Autor

Se observa en la figura 6 la configuración de la interface Vlan4 y el Gateway predeterminado en el Switch 2 por medio del comando show run.

6.2 CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED

En este apartado se realiza la configuración de las VLANs, Troncales y Etherchannel en los dos switches. Adicionalmente, se efectúa la configuración de seguridad en los puertos de acceso y se agrupan las interfaces no utilizadas en una VLAN específica.

En las siguientes tablas se muestran los comandos ejecutados en cada uno de los dispositivos.

Tarea	Especificación
Crear VLAN VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#end S1#config t S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config-if)#config t S1(config)#interface f0/1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#end S1(config-if)#config t S1(config)#interface f0/2 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6

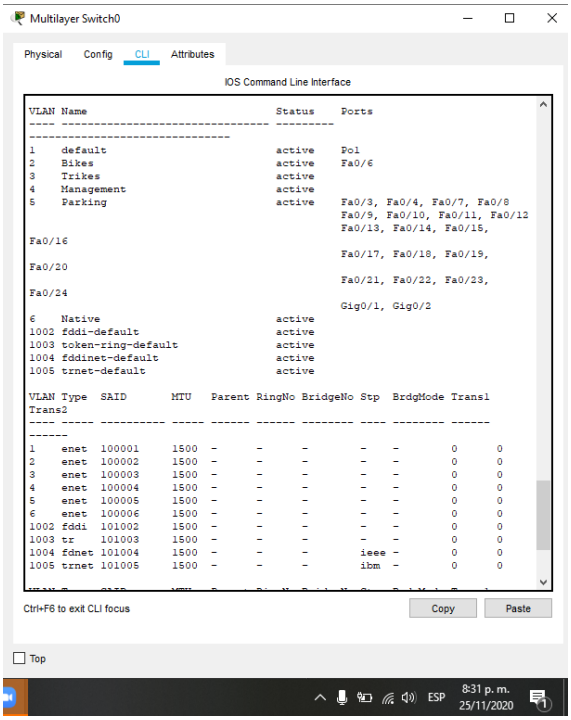
Tarea	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1, F0/2 y F0/5	S1(config)#interface f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#end
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1#config t S1(config)#interface range fa0/1-2 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#no shutdown
Configurar el puerto de acceso de host para VLAN 2 Interface F0/6	S1#config t S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#end
Configurar la seguridad del puerto en los puertos de acceso Permitir 3 direcciones MAC	S1#config t S1(config)#interface f0/6 S1(config-if)#switchport port-security maximum 3 S1(config-if)#
Proteja todas las interfaces no utilizadas Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S1#config t S1(config)#interface range fa0/7-24 S1(config-if-range)#description Interface Vlan5 Parking S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shutdown S1(config)#interface range Gig0/1-2 S1(config-if-range)#description Interface Vlan5 Parking S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shut S1(config-if-range)#exit S1(config)#interface range fa0/3-4 S1(config-if-range)#description Interface Vlan5 Parking S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#shut S1(config-if-range)#exit

Tabla 7. Configuración adicional S1

Despues de realizar la configuración mostrada en la tabla 7, el switch cuenta con 5 vlan que fueron creadas de acuerdo a lo indicado, troncos en las interfaces F0/1, F0/2 y F0/5 cuya Vlan nativa es la vlan 6, las interfaces F0/1 y F0/2 pertenecen a un grupo de puertos EtherChannel con el protocolo LACP para la negociación, se habilitó la interfaz f0/6 como puerto de acceso, adicionalmente, se asignaron los puertos que no se usan a la vlan 5 y se apagaron.

En la figura 7 se evidencian las Vlan creadas en el Switch 1, esto se logra con la ejecución del comando show vlan.

Figura 7. Show Vlan S1



Fuente: Autor

En la tabla 8 se muestran los comandos ejecutados en el switch 2 para cumplir con la configuración solicitada.

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name Management

Tarea	Especificación
Crear VLAN VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native	S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#exit S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa Interfaces F0/1 y F0/2	S2(config)#interface f0/1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#end S2#config t S2(config)#interface f0/2 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#end
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 Usar el protocolo LACP para la negociación	S1#config t S1(config)#interface range fa0/1-2 S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#channel-group 1 mode passive S1(config-if-range)#no shutdown S1(config-if-range)#exit
Configurar el puerto de acceso del host para la VLAN 3 Interfaz F0/18	S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#end
Configure port-security en los access ports permite 3 MAC addresses	S2#config t S2(config)#interface f0/18 S2(config-if)#switchport port-security maximum 3 S2(config-if)#exit
Asegure todas las interfaces no utilizadas. Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#interface range fa0/3-17 S2(config-if-range)#description Interface Vlan5 Parking S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#shutdown S2(config-if-range)#exit S2(config)#interface range fa0/19-24 S2(config-if-range)#description Interface Vlan5 Parking

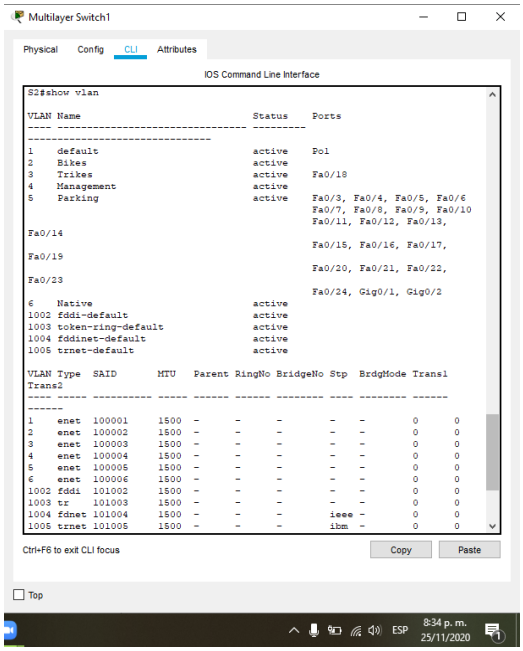
Tarea	Especificación
	S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#shutdown S2(config-if-range)#exit S2(config)#interface range Gig0/1-2 S2(config-if-range)#description Interface Vlan5 Parking S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5

Tabla 8. Configuración adicional S2

Al ejecutar los comandos el switch cuenta con 5 vlan que fueron creadas de acuerdo a lo indicado, troncos en las interfaces F0/1 y F0/2 cuya Vlan nativa es la vlan 6, las interfaces F0/1 y F0/2 pertenecen a un grupo de puertos EtherChannel con el protocolo LACP para la negociación, se habilitó la interfaz f0/18 como puerto de acceso correspondiente a la Vlan 3, adicionalmente, se asignaron los puertos que no se usan a la Vlan 5 y se apagaron.

En la Figura 8 se muestran las vlan configuradas por medio del comando show vlan.

Figura 8. Show Vlan S2



Fuente: Autor

6.3 CONFIGURAR SOPORTE DE HOST

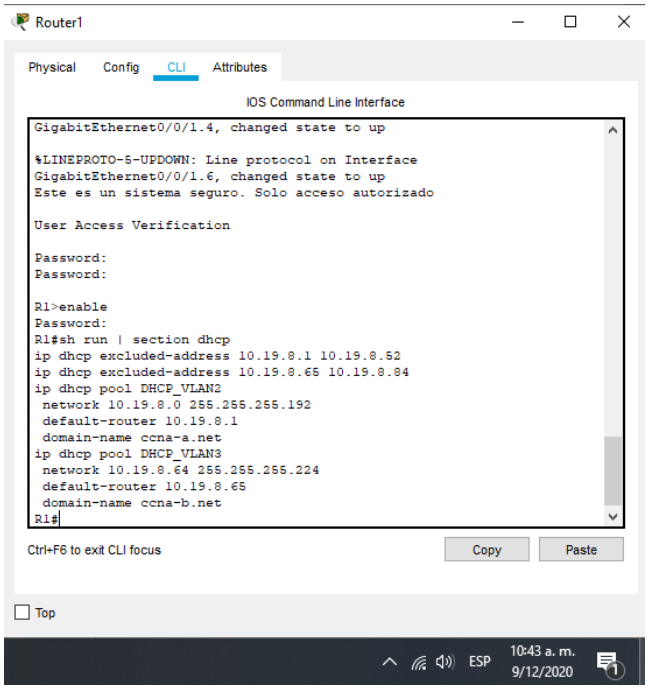
En esta sección se muestran las configuraciones efectuadas en el router con el fin que el tráfico se dirija a la interfaz loopback 0, adicionalmente, se configuran los grupos DHCP para dos de las VLAN.

En la siguiente tabla se muestran los comandos ejecutados en el router y los grupos DHCP creados.

Tarea	Especificación
Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0 R1(config)#ipv6 route ::/0 loopback0
Configurar IPv4 DHCP para VLAN 2 Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#service dhcp R1(config)#ip dhcp pool DHCP_VLAN2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool DHCP_VLAN2 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit R1(config)#exit
Configurar DHCP IPv4 para VLAN 3 Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1#config t R1(config)#service dhcp R1(config)#ip dhcp pool DHCP_VLAN3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#ip dhcp pool DHCP_VLAN3 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

Tabla 9. Configuración adicional R1

Figura 9. Configuración DHCP R1



Fuente: Autor

En la figura 9 se puede observa la configuración del pool DHCP realizada en el Router 1, esto se visualiza por medio del comando sh run | section dhcp

6.4 CONFIGURAR LOS SERVIDORES

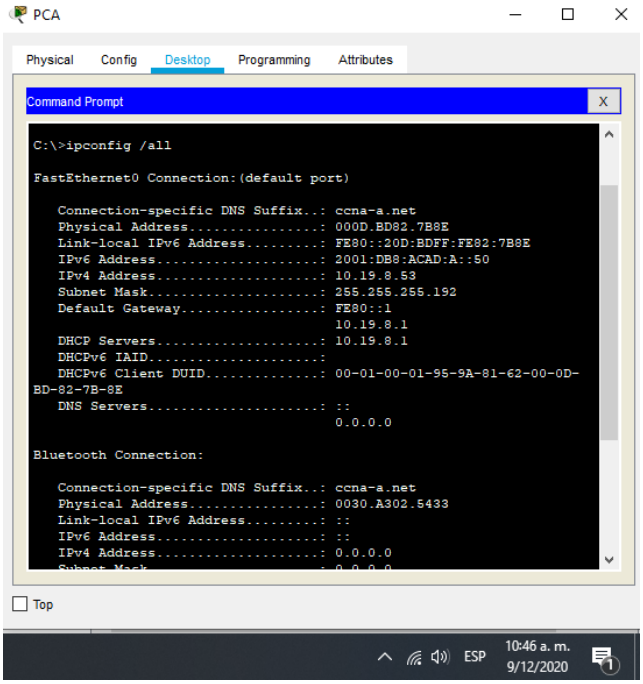
Se proceden a configurar los equipos PC-A y PC-B con el fin de validar que las diferentes configuraciones ejecutadas anteriormente quedaron adecuadas y permiten la conexión entre los dispositivos.

En las tablas se muestra la configuración realizada para IPv6 y la dirección proporcionada por DHCP para IPv4.

Configuración de red de PC-A	
Descripción	ccna-a.net
Dirección física	000D.BD82.7B8E
Dirección IP	IPv6 Address: 2001:DB8:ACAD:A::50 IPv4 Address:10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 10. Configuración red PC-A

Figura 10. Configuración de red PC-A



Fuente: Autor

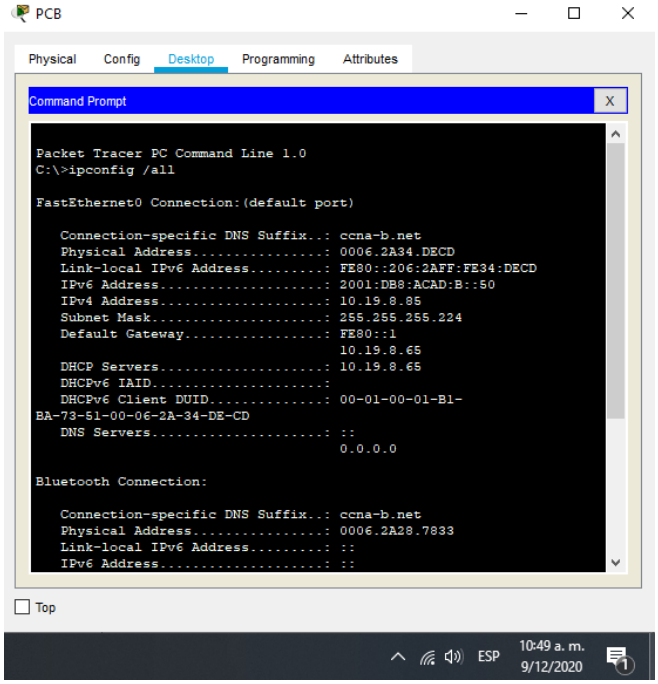
En la figura 10 se evidencia la respuesta del comando ipconfig/all que muestra la configuración tomada por el PC-A y que fue registrada en la tabla 10.

Configuración de red de PC-B	
Descripción	ccna-b.net
Dirección física	0006.2A34.DECD
Dirección IP	IPv6 Address: 2001:DB8:ACAD:B::50 IPv4 Address: 10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Tabla 11. Configuración red PC-B

En la figura 11 se evidencia la respuesta del comando ipconfig/all que muestra la configuración tomada por el PC-B y que fue registrada en la tabla anterior.

Figura 11. Configuración de red PC-B



Fuente: Autor

Después de efectuar las configuraciones, se procede con la ejecución de pruebas de conectividad por medio de ping a diferentes direcciones. En la tabla siguiente se muestra el resultado de cada ping efectuado a la dirección respectiva, posterior a esta se pueden observar las imágenes de los diferentes pings ejecutados.

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

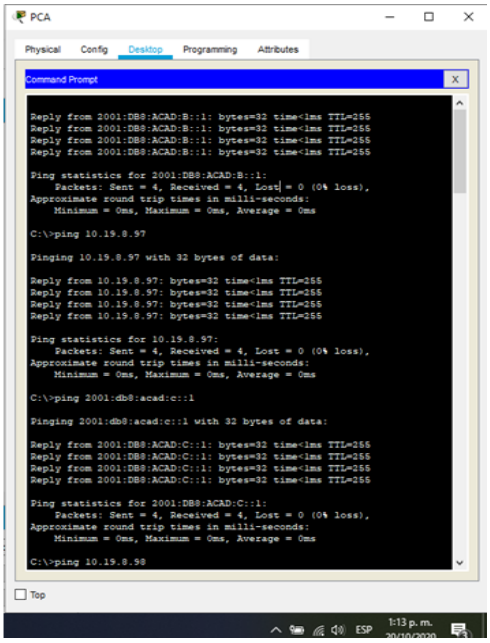
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	PC-B	Dirección	IP address will vary.	Exitoso
PC-A	PC-B	IPv6	2001:db8:acad:b: :50	Exitoso
PC-A	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
PC-A	R1 Bucle 0	IPv6	2001:db8:acad:209: :1	Exitoso
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Exitoso
PC-B	R1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

Tabla 12. Ejecución de pruebas ping

En las siguientes figuras se podrán ver las pruebas de ping ejecutadas desde el PC-A a los diferentes equipos de la red, allí podremos observar que sus resultados fueron exitosos, excepto a la IPv6 de los dos switch

En la figura 12 se puede ver el ping desde el PC-A a las direcciones IP 2001:db8:acad:b: :1, 10.19.8.97, 2001:db8:acad:c: :1 los cuales fueros exitosos.

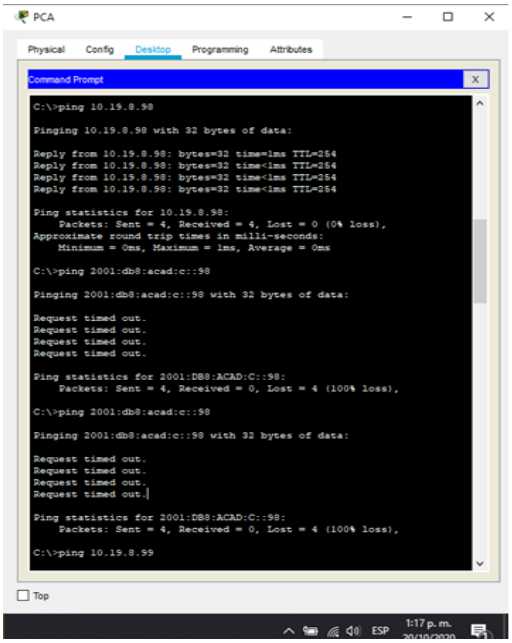
Figura 12. Ping PC-A Parte 1



Fuente: Autor

En la figura 13 se evidencia ping desde el PC-A a las IP 10.19.8.98 y 2001:db8:acad:c: :98, en esta ocasión el ping a la IPv6 no fue exitoso

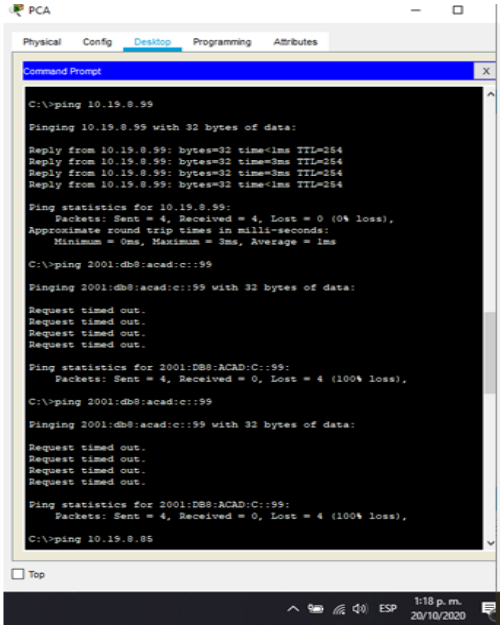
Figura 13. Ping PC-A Parte 2



Fuente: Autor

En la figura 14 se evidencia ping desde el PC-A a las IP 10.19.8.99 y 2001:db8:acad:c: :99, en esta ocasión el ping a la IPv6 no fue exitoso.

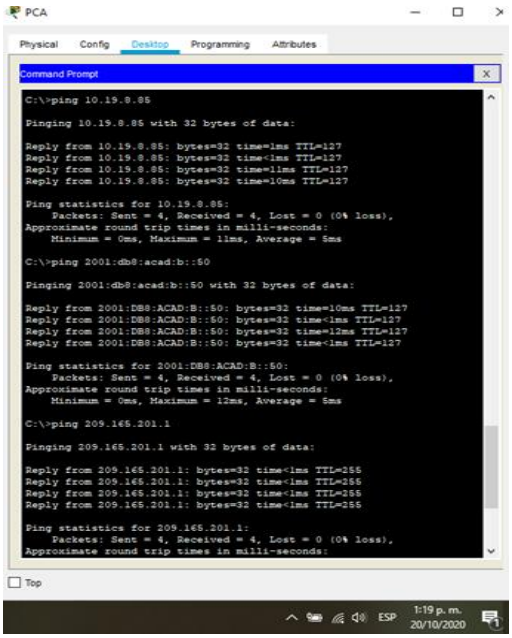
Figura 14. Ping PC-A Parte 3



Fuente: Autor

En la figura 15 se evidencia ping desde el PC-A a las IP 10 10.19.8.85 y 2001:db8:acad:b: :50, los cuales fueron exitosos.

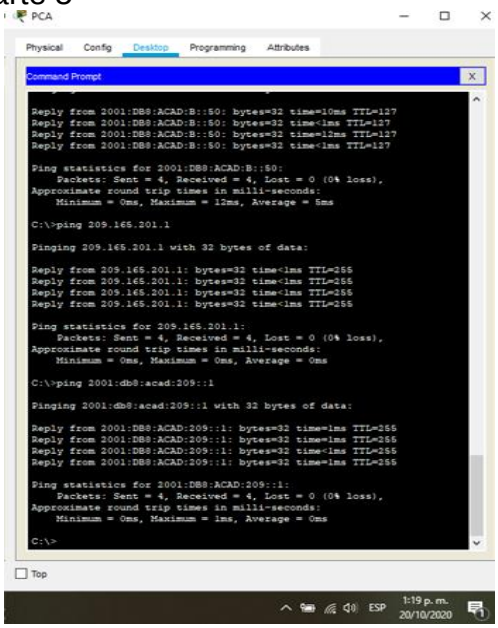
Figura 15. Ping PC-A Parte 4



Fuente: Autor

En la figura 16 se evidencia ping desde el PC-A a las IP 209.165.201.1 y 2001:db8:acad:209: :1, los cuales fueron exitosos.

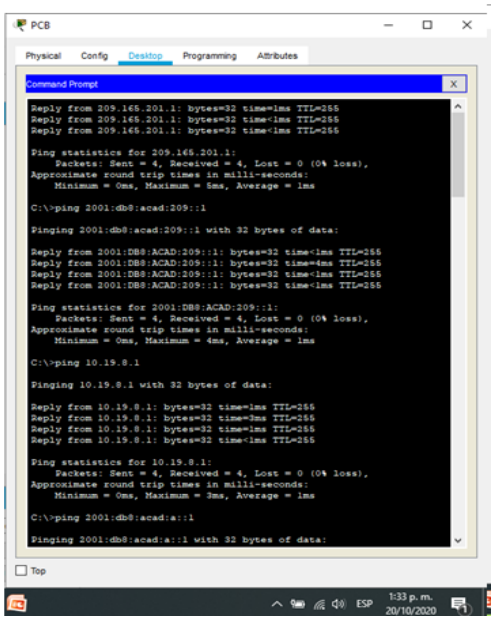
Figura 16. Ping PC-A Parte 5



Fuente: Autor

En la figura 17 se evidencia ping desde el PC-B a las IP 209.165.201.1, 2001:db8:acad:209: :1 y 10.19.8.1, los cuales fueron exitosos.

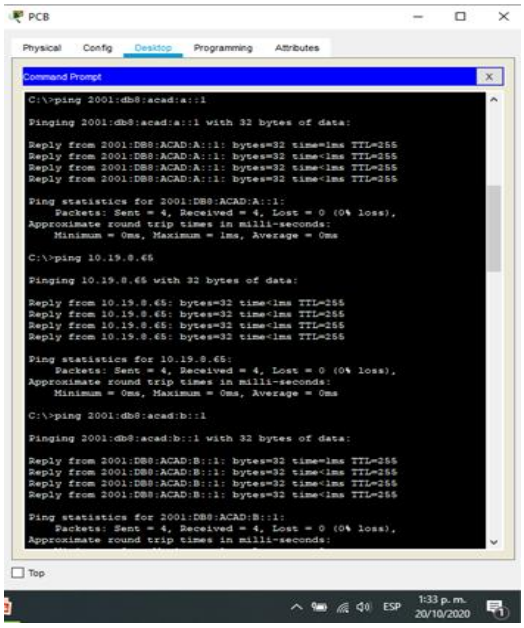
Figura 17. Ping PC-B Parte 1



Fuente: Autor

En la figura 18 se evidencia ping desde el PC-B a las IP 2001:db8:acad:a: :1, 10.19.8.65 y 2001:db8:acad:b: :1, los cuales fueron exitosos.

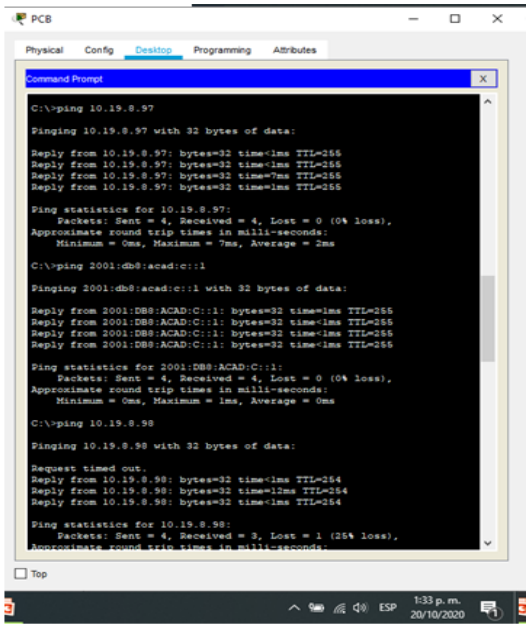
Figura 18. Ping PC-B Parte 2



Fuente: Autor

En la figura 19 se evidencia ping desde el PC-B a las IP 10.19.8.97 y 2001:db8:acad:c: :1, los cuales fueron exitosos.

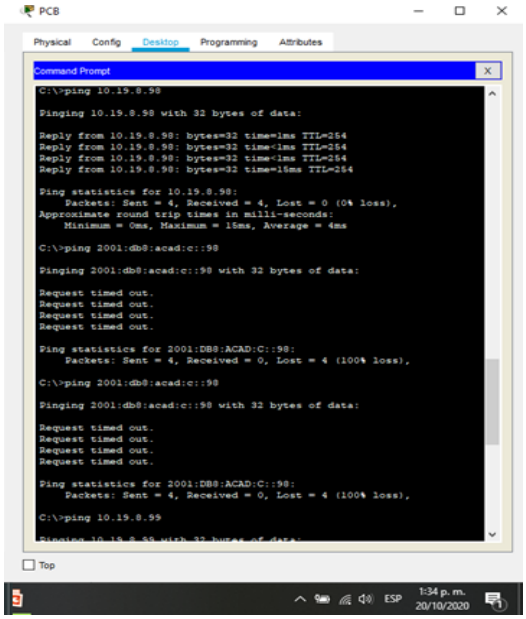
Figura 19. Ping PC-B Parte 3



Fuente: Autor

En la figura 20 se evidencia ping desde el PC-B a las IP 10.19.8.98 y 2001:db8:acad:c: :98, en esta ocasión el ping a la IPv6 no fue exitoso.

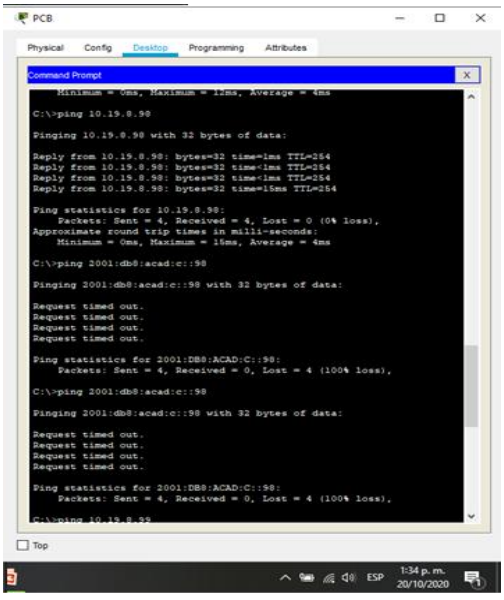
Figura 20. Ping PC-B Parte 4



Fuente: Autor

En la figura 21 se evidencia ping desde el PC-B a las IP 10.19.8.99 y 2001:db8:acad:c: :99, en esta ocasión el ping a la IPv6 no fue exitoso.

Figura 21. Ping PC-B Parte 5

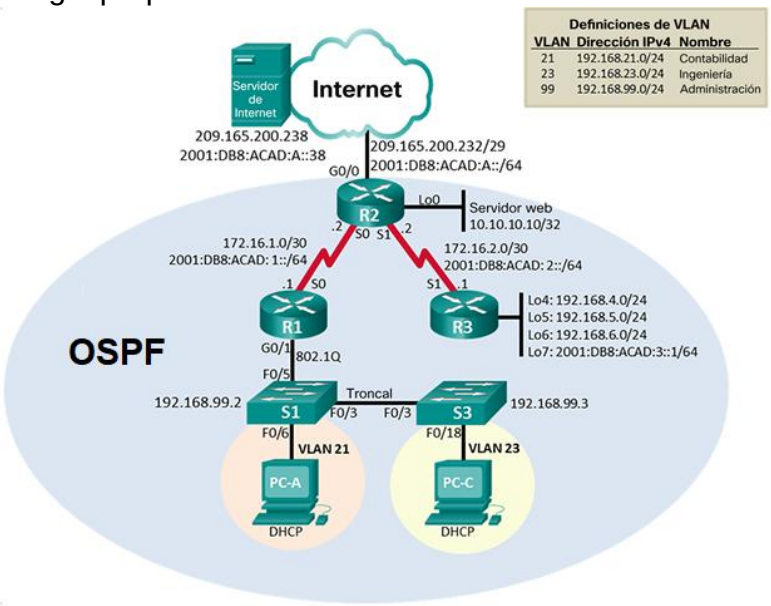


Fuente: Autor

7 ESCENARIO 2

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.

Figura 22. Topologia propuesta escenario 2



7.1 INICIALIZAR LOS DISPOSITIVOS

En este apartado se preparan los dispositivos para la configuración a realizar, se borran las configuraciones previas con el fin de evitar errores. A continuación se muestran los comandos empleados para los switches y routers

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#delete vlan.dat Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Tabla 13. Comando de inicializar dispositivos

Despues de ejecutar los comandos en los equipos quedan listos para realizar la configuración que se requiera.

7.2 CONFIGURACIÓN ASPECTOS BÁSICOS DISPOSITIVOS

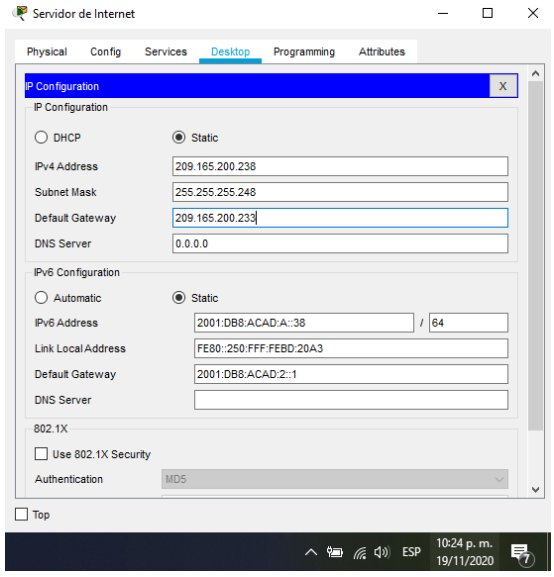
7.2.1 CONFIGURAR LA COMPUTADORA DE INTERNET

Se procede a realizar la configuración en el servidor de Internet de las direcciones IP, se asigna el Gateway predeterminado de acuerdo a la topología de red, en la tabla siguiente se evidencia el direccionamiento configurado:

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 14. Direccionamiento PC internet

Figura 23. Configuración IP PC



Fuente: Autor

En la figura 23 se observa la configuración efectuada en el servidor de internet de direcciones IP y Gateway indicados en la tabla de direccionamiento.

7.2.2 CONFIGURAR R1

De acuerdo a lo solicitado en la siguiente tabla se realiza la configuración en el Router 1 de nombre, contraseña, interfaz serial, etc. para esto se emplean comandos como hostname, password, ip address, entre otros.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router R1	Router#config t Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada - class	R1#config t R1(config)#enable secret class
Contraseña de acceso a la consola cisco	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet cisco	R1#config t R1(config)#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 Se prohíbe el acceso no autorizado.	R1(config)#banner motd "Se prohibe el acceso no autorizado." R1(config)#exit
Interfaz S0/0/0 Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6	R1#config t R1(config)#interface s0/0/0 R1(config-if)#description Interface Conexion_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
Interfaz S0/0/0 Establecer la frecuencia de reloj en 128000 Activar la interfaz	R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#

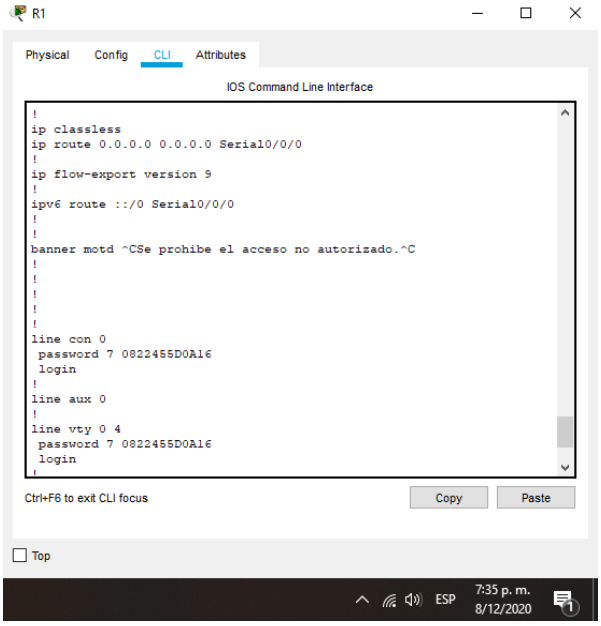
Rutas predeterminadas Configurar una ruta IPv4 predetermina de S0/0/0 - Configurar una ruta IPv6 predeterminada de S0/0/0	R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Tabla 15. Configuración R1

Nota: Todavía no configure G0/1.

En la tabla 15 se plasmaron los comandos empleados en la configuración del router, con lo ejecutado en el equipo al ingresar muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado, adicionalmente, se configuró la interfaz s0/0/0 que tiene conexión al Router 2 y las rutas predeterminadas IPv4 y Ipv6.

Figura 24. Show run R1



Fuente: Autor

En la figura 24 se observa una parte de la configuración del equipo mostrada por medio del comando show run, en esta parte se evidencia la ruta predeterminada y las contraseñas establecidas.

7.2.3 CONFIGURAR R2

Se configura el Router 2 con los aspectos básicos, así como las interfaces seriales, G0/0, Loopback 0, etc. En la siguiente tabla se muestran los comandos empleados para lograr lo requerido.

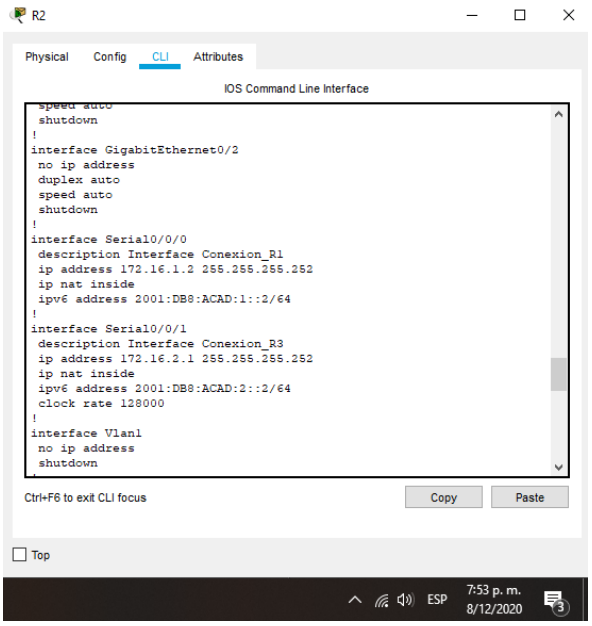
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router R2	Router#config t Router(config)#hostname R2
Contraseña de exec privilegiado cifrada (class)	R2#config t R2(config)#enable secret class
Contraseña de acceso a la consola cisco	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet cisco	R2#config t R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD Se prohíbe el acceso no autorizado.	R2(config)#banner motd "Se prohibe el acceso no autorizado."
Interfaz S0/0/0 Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R2#config t R2(config)#interface s0/0/0 R2(config-if)#description Interface Conexion_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 R2(config-if)#exit
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz	R2#config t R2(config)#interface s0/0/1 R2(config-if)#description Interface Conexion_R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet) Establecer la descripción.	R2#config t R2(config)#interface g0/0

Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R2(config-if)#description Interface Conexion_Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248
Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz	R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado) Establecer la descripción. Establezca la dirección IPv4.	R2#config t R2(config)# interface loopback 0 R2(config-if)#description Interface Loopback0 R2(config-if)# ip address 10.10.10.10 255.255.255.255
Ruta predeterminada - Configure una ruta predeterminada IPv4 e IPv6 de G0/0.	R1(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R1(config)#ipv6 route ::/0 g0/0

Tabla 16. Configuración R2

Los comandos de la tabla 16 fueron ejecutados en el router y después de esto al ingresar al equipo se muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado, adicionalmente, se observan habilitadas las interfaces s0/0/0 y s0/0/1 que tienen conexión a los Router 1 y 3 respectivamente, la interfaz loopback0 y las rutas predeterminadas IPv4 y Ipv6.

Figura 25. Show run R2



Fuente: Autor

En la figura 25 se observa una parte de la configuración del equipo mostrada por medio del comando show run, en esta parte se evidencian las interfaces seriales.

7.2.4 CONFIGURAR R3

En este apartado se configura de forma básica el Router 3, se realiza configuración de las diferentes loopback y de la interfaz serial en este equipo.

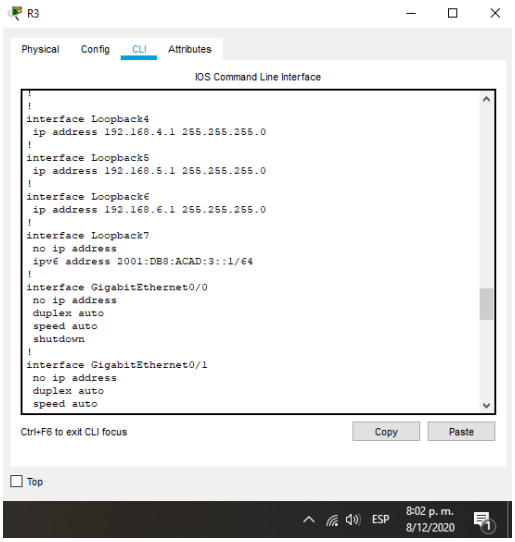
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config t Router(config)#no ip domain-lookup
Nombre del router R3	Router#config t Router(config)#hostname R3
Contraseña de exec privilegiado cifrada (class)	R3#config t R3(config)#enable secret class
Contraseña de acceso a la consola cisco	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet cisco	R3#config t R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD Se prohíbe el acceso no autorizado.	R3(config)#banner motd "Se prohibe el acceso no autorizado." R3(config)#exit
Interfaz S0/0/1 Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz	R3#config t R3(config)#interface s0/0/1 R3(config-if)#description Interface Conexion_R2 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown

Interfaz loopback 4 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3#config t R3(config)# interface loopback 4 R3(config-if)# ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3#config t R3(config)# interface loopback 5 R3(config-if)# ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.	R3#config t R3(config)# interface loopback 6 R3(config-if)# ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7 - Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.	R3#config t R3(config)# interface loopback 7 R3(config-if)# ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Tabla 17. Configuración R3

En la tabla 17 se encuentran los comandos empleados en la configuración del router, con lo ejecutado al ingresar se muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado, adicionalmente, se configuró la interfaz s0/0/1 que tiene conexión al Router 2, las rutas predeterminadas IPv4 y Ipv6 y las interfaces Loopback 4,5, 6 y 7.

Figura 26. Show run R3



Fuente: Autor

En la figura 26 se observa una parte de la configuración del equipo mostrada por medio del comando show run, en esta parte se evidencian las interfaces loopback.

7.2.5 CONFIGURAR S1

Se efectúa la configuración básica en el Switch 1, de manera inicial se configuran las contraseñas de acceso, mensaje de bienvenida al equipo.

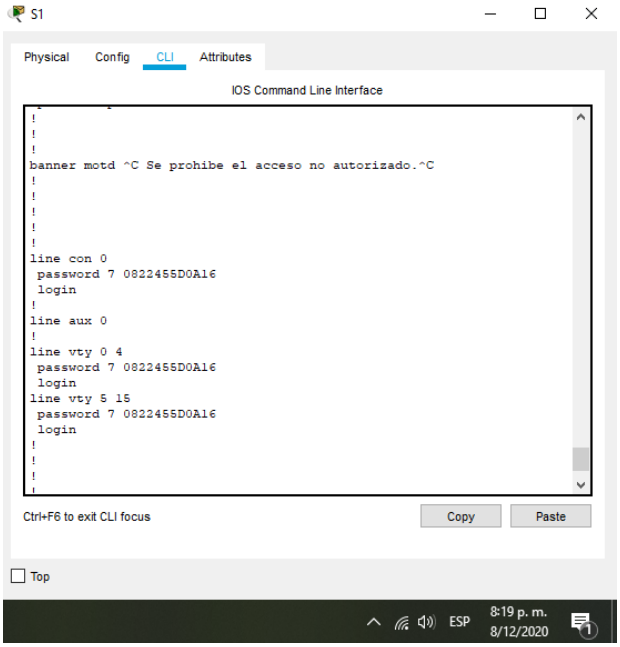
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch (S1)	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada (class)	S1(config)#enable secret class
Contraseña de acceso a la consola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

Tabla 18. Configuración S1

Despues de la ejecución realizada en el switch 1, el equipo al ingresar muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado.

En la figura 27 se observa una parte de la configuración que muestra el comando show run, en esta parte se evidencia el saludo de bienvenida y las contraseñas establecidas.

Figura 27. Show run S1



Fuente: Autor

7.2.6 CONFIGURAR EL S3

Se efectúa la configuración básica en el Switch 3, de manera inicial se configuran las contraseñas de acceso, mensaje de bienvenida al equipo.

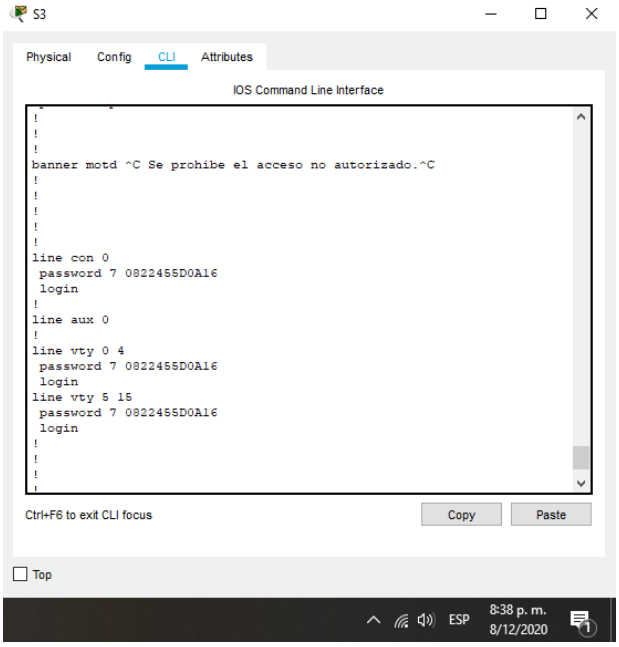
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t Switch(config)#no ip domain-lookup
Nombre del switch (S3)	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada (class)	S3(config)#enable secret class
Contraseña de acceso a la consola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

Mensaje MOTD Se prohíbe el acceso no autorizado.	S3(config)#banner motd " Se prohibe el acceso no autorizado."

Tabla 19. Configuración S3

Despues de la ejecución realizada en el switch 3, el equipo al ingresar muestra un mensaje de advertencia, solicita contraseña de acceso a la consola y al modo EXEC privilegiado.

Figura 28. Show run S3



Fuente: Autor

En la figura 28 se observa una parte de la configuración que muestra el comando show run, en esta parte se evidencia el saludo de bienvenida y las contraseñas establecidas.

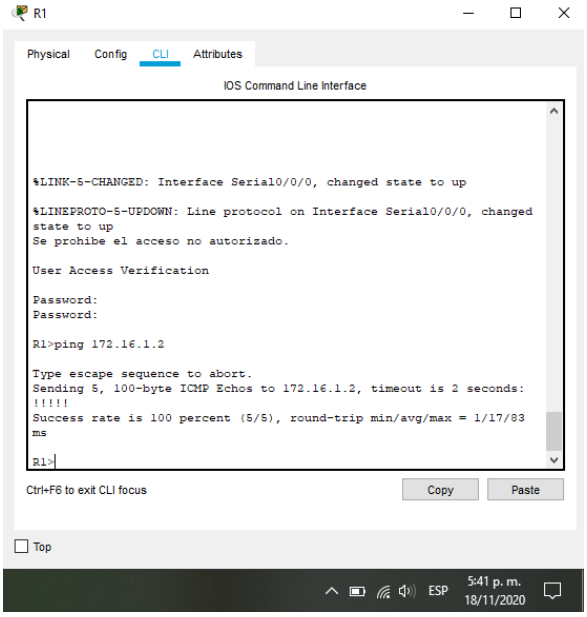
7.2.7 VERIFICAR LA CONECTIVIDAD DE LA RED

Se realizan pruebas de conectividad por medio de ping entre los Routers y entre el servidor de internet y el Gateway predeterminado

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	exitoso
R2	R3, S0/0/1	172.16.2.2	exitoso
PC de Internet	Gateway predetermi	209.165.200.233	exitoso

En la figura 29 se muestra el resultado de ping del Router 1 a la IP 172.16.1.2 del Router 2 el cual fue exitoso.

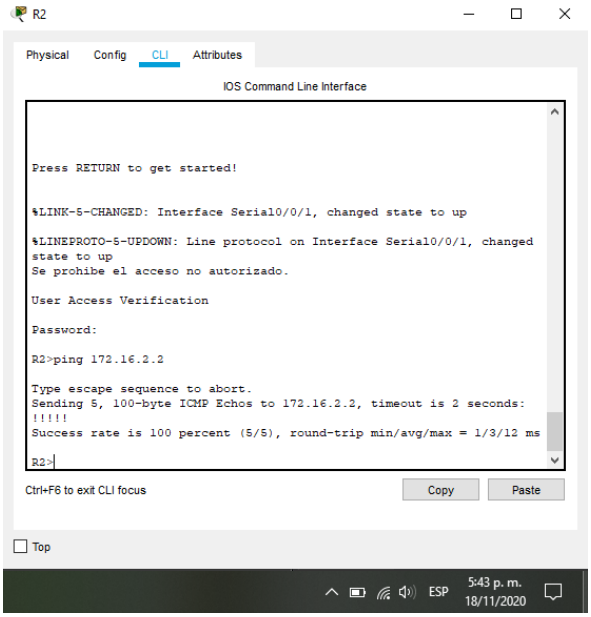
Figura 29. Ping desde R1



Fuente: Autor

En la figura 30 se muestra el resultado de ping del Router 2 a la IP 172.16.2.2 del Router 3, el cual fue exitoso.

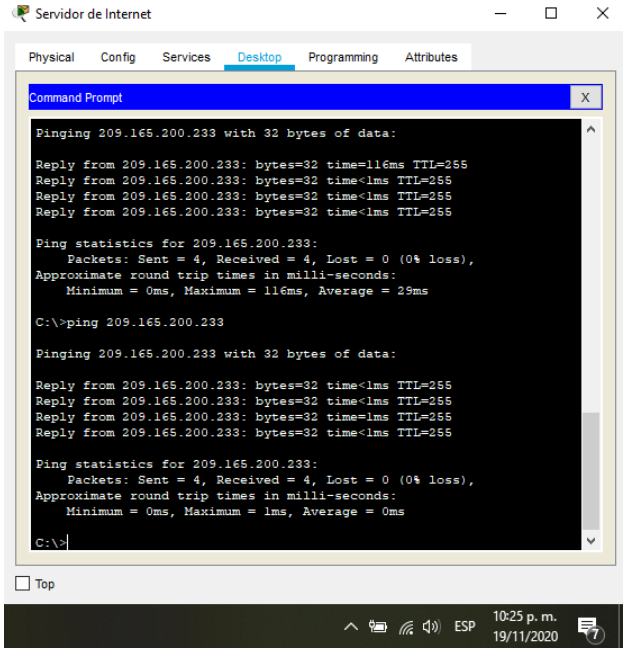
Figura 30. Ping desde R2



Fuente: Autor

En la figura 31 se muestra el resultado de ping desde el servidor de internet a la IP 209.165.200.233 del Gateway predeterminado el cual fue exitoso.

Figura 31. Ping desde servidor internet



Fuente: Autor

7.3 CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

7.3.1 CONFIGURAR S1

En este apartado se configurarán las Vlan en el Switch 1, los puertos troncales, puertos de acceso y Gateway predeterminado.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Vlan 21 Contabilidad Vlan 23 Ingenieria Vlan 99 Administracion Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#exit S1(config)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#exit S1(config)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#end

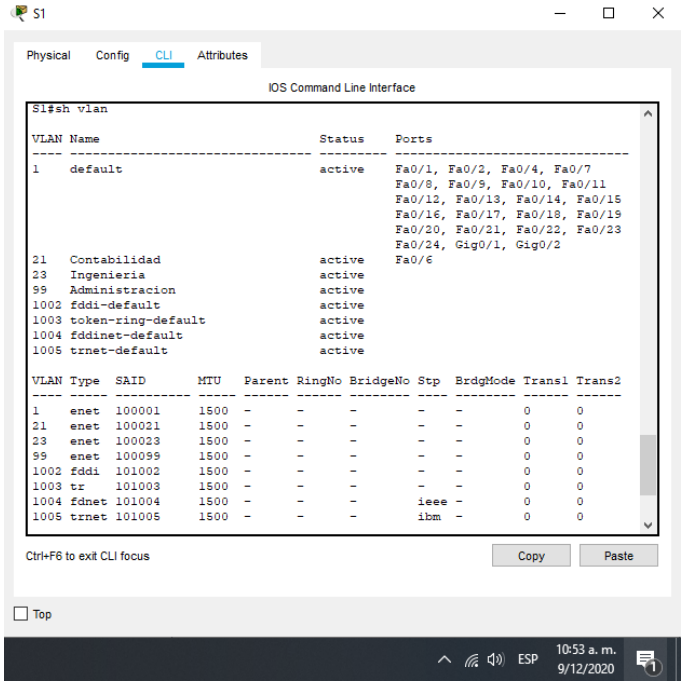
Asignar la dirección IP de administración. Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología	S1(config)#interface vlan 99 S1(config-if)#no shutdown S1(config-if)#ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.	S1(config)#ip default-gateway 192.168.99.1 S1(config)#exit
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN native	S1(config-if)#config t S1(config)#interface f0/3 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Forzar el enlace troncal en la interfaz F0/5 Utilizar la red VLAN 1 como VLAN native	S1(config-if)#config t S1(config)#interface f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S1#config t S1(config)# interface range fa0/1-2 S1(config-if)#switchport mode access S1(config-if)#exit S1(config)# interface fa0/4 S1(config-if)#switchport mode access S1(config-if)#exit S1(config)# interface range fa0/7-24 S1(config-if)#switchport mode access S1(config-if)#exit S1(config)# interface range g0/1-2 S1(config-if)#switchport mode access S1(config-if)#end
Asignar F0/6 a la VLAN 21	S1(config)#interface fa0/6 S1(config-if-range)#switchport access vlan 21 S1(config-if-range)#no shutdown S1(config-if-range)#exit

Apagar todos los puertos sin usar	S1#config t S1(config)# interface range fa0/1-2 S1(config-if)#shutdown S1(config)# interface fa0/4 S1(config-if)# shutdown S1(config)# interface range fa0/7-24 S1(config-if)# shutdown S1(config)# interface range g0/1-2 S1(config-if)# shutdown S1(config-if)#end

Tabla 20. Configuración Vlan S1

Despues de realizar la configuración mostrada en la tabla 20, el switch cuenta con 3 vlan, interface vlan 99, Gateway predeterminado, enlace troncal en las interfaces f0/3 y f0/5 cuya Vlan nativa es 1, adicionalmente, los puertos que no se usan se apagaron y se cambiaron a modo acceso.

Figura 32. Show vlan S1



Fuente: Autor

En la figura 32 se puede comprobar las Vlan configuradas en el switch de acuerdo a los comandos ejecutados, para obtener dicha información se empleó el comando show vlan.

7.3.2 CONFIGURAR EL S3

En este apartado se configurarán las Vlan en el Switch 3, los puertos troncales, puertos de acceso y Gateway predeterminado.

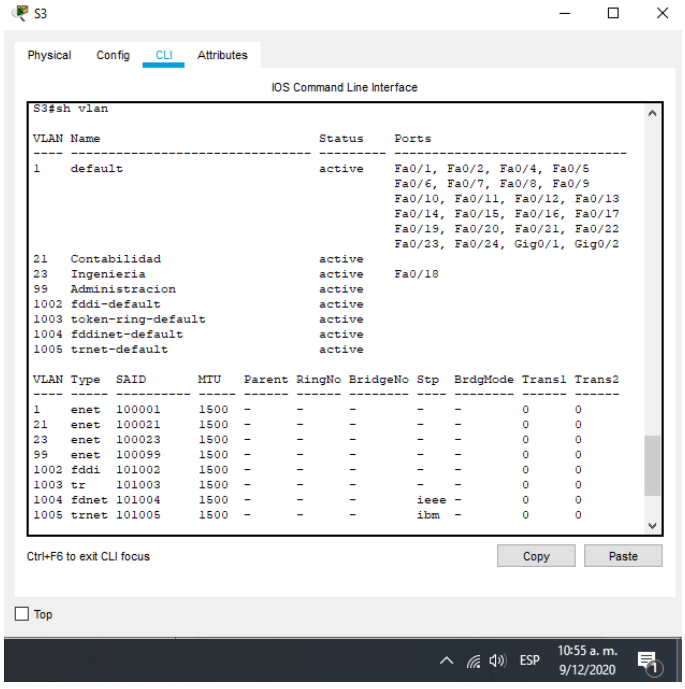
Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN Vlan 21 Contabilidad Vlan 23 Ingenieria Vlan 99 Administracion Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#exit S3(config)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#exit S3(config)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#end
Asignar la dirección IP de administración Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología	S3(config)#interface vlan 99 S3(config-if)#no shutdown S3(config-if)#ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado. Asignar la primera dirección IP en la subred como gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1 S3(config)#exit
Forzar el enlace troncal en la interfaz F0/3 Utilizar la red VLAN 1 como VLAN native	S3(config-if)#config t S3(config)#interface f0/3 S3(config-if)#switchport trunk encapsulation dot1q S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#end
Configurar el resto de los puertos como puertos de acceso Utilizar el comando interface range	S3#config t S3(config)# interface range fa0/1-2 S3(config-if)#switchport mode access S3(config)# interface range fa0/4-17 S3(config-if)#switchport mode access S3(config)# interface range fa0/19-24 S3(config-if)#switchport mode access S3(config)# interface range g0/1-2 S3(config-if)#switchport mode access S3(config-if)#end

Asignar F0/18 a la VLAN 23	S3(config)#interface fa0/18 S3(config)#switchport access vlan 23 S3(config)#no shutdown S3(config-if-range)#exit
Apagar todos los puertos sin usar	S3#config t S3(config)# interface range fa0/1-2 S3(config-if)#shutdown S3(config)# interface range fa0/4-17 S3(config-if)# shutdown S3(config)# interface range fa0/19-24 S3(config-if)# shutdown S3(config)# interface range g0/1-2 S3(config-if)# shutdown S3(config-if)#end

Tabla 21. Configuración Vlan S3

Despues de realizar la configuración mostrada en la tabla 21, el switch cuenta con 3 vlan, interface vlan 99, Gateway predeterminado, enlace troncal en la interfaz f0/3 cuya Vlan nativa es 1, adicionalmente, los puertos que no se usan se apagaron y se cambiaron a modo acceso.

Figura 33. Show vlan S3



Fuente: Autor

En la figura 33 se puede comprobar las Vlan configuradas en el S3 de acuerdo a los comandos ejecutados, para obtener dicha información se empleó el comando show vlan.

7.3.3 CONFIGURAR R1

Se configuran las interfaces para las Vlan en el router 1 empleando los comandos indicados en la tabla

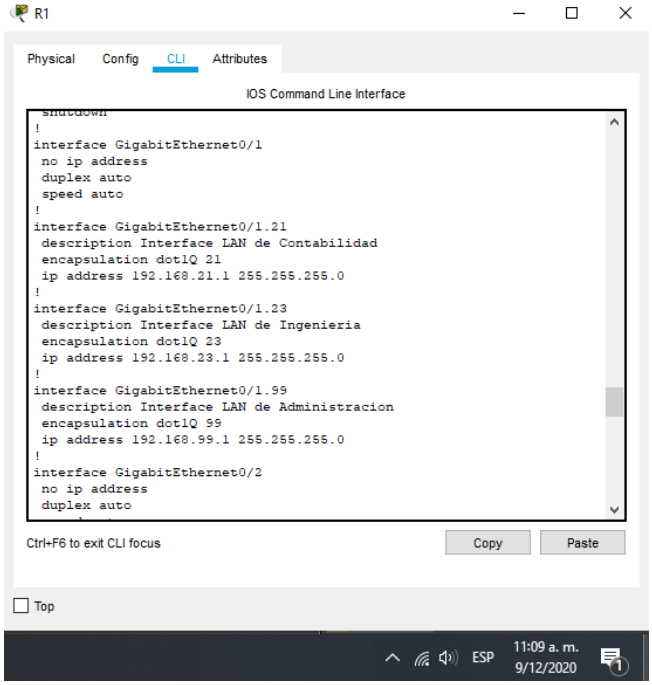
Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1 Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz	R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#description Interface LAN de Contabilidad R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#no shutdown
Configurar la subinterfaz 802.1Q .23 en G0/1 Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz	R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#description Interface LAN de Ingenieria R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#no shutdown
Configurar la subinterfaz 802.1Q .99 en G0/1 Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz	R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#description Interface LAN de Administracion R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#no shutdown
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-subif)#no shutdown

Tabla 22. Configuración Vlan R1

Al realizar las configuraciones mostradas en la tabla 22, el router cuenta con la configuración de las subinterfaces correspondiente a las vlan de la red, con el fin que todas las subinterfaces quedaran activas, se activó la interfaz G0/1.

En la figura 34 se muestra una sección del comando Show Run en donde se evidencia la configuración de las subinterfaces que se realizó con los comandos mostrados en la tabla anterior.

Figura 34. Verificación subinterfaces R1



Fuente: Autor

7.3.4 VERIFICAR LA CONECTIVIDAD DE LA RED

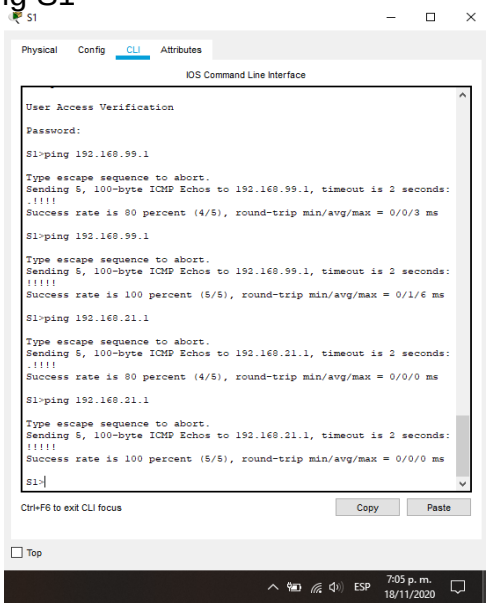
Después de las configuraciones realizadas de las Vlan en los Switches y Routers se procede a confirmar la conectividad entre los equipos por medio de ping.

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

Tabla 23. Prueba de conectividad S1 y S3

En la figura 35 se ve el ping realizado desde el S1 a las IP 192.168.99.1 y 192.168.21.1 de las Vlan 99 y 21 del Router 1 respectivamente, los cuales fueron exitosos.

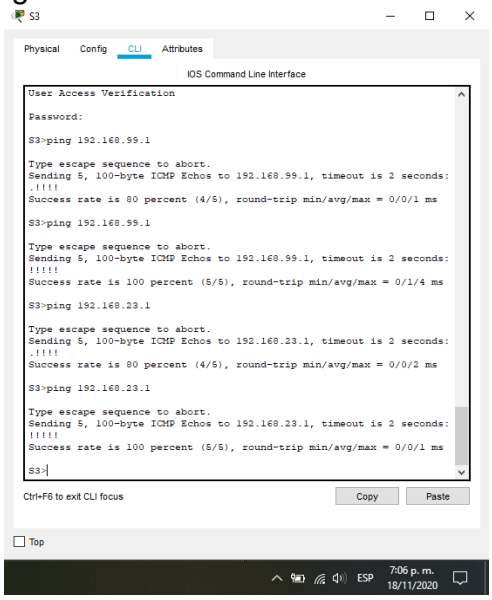
Figura 35. Prueba de Ping S1



Fuente: Autor

En la figura 36 se ve el ping realizado desde el S3 a las IP 192.168.99.1 y 192.168.23.1 de las Vlan 99 y 23 del Router 1 respectivamente, los cuales fueron exitosos.

Figura 36. Prueba de Ping S3



Fuente: Autor

7.4 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

7.4.1 CONFIGURAR OSPF EN EL R1

Para configurar el protocolo de enrutamiento dinámico OSPF en el Router 1 se proceden a ejecutar los comandos indicados en la tabla que se encuentra a continuación. Se indica el comando para desactivar la sumarización automática, sin embargo, para el protocolo OSPF no es necesario realizarlo.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Anunciar las redes conectadas directamente Asigne todas las redes conectadas directamente.	R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/1 R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática	R1(config-router)#no auto-summary

Tabla 24. Configuración OSPF R1

7.4.2 CONFIGURAR OSPF EN EL R2

Para configurar el protocolo de enrutamiento dinámico OSPF en el Router 2 se proceden a ejecutar los comandos indicados en la tabla que se encuentra a continuación. Se indica el comando para desactivar la sumarización automática, sin embargo, para el protocolo OSPF no es necesario realizarlo.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0

Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface Loopback0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Tabla 25. Configuración OSPF R2

7.4.3 CONFIGURAR OSPFV3 EN EL R3

Para configurar el protocolo de enrutamiento dinámico OSPF en el Router 3 se proceden a ejecutar los comandos indicados en la tabla que se encuentra a continuación. Se indica el comando para desactivar la sumarización automática, sin embargo, para el protocolo OSPF no es necesario realizarlo.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface Loopback4 R3(config-router)#passive-interface Loopback5 R3(config-router)#passive-interface Loopback6 R3(config-router)#passive-interface Loopback7
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Tabla 26. Configuración OSPF R3

7.4.4 VERIFICAR LA INFORMACIÓN DE OSPF

Con el fin de confirmar las configuraciones de enrutamiento realizadas en los routers se ejecutan los siguientes comandos:

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?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show running-config | section ospf

Tabla 27. Comandos para mostrar OSPF

En la figura 37 podemos ver el resultado de la ruta OSPF configurada en el router 2.

Figura 37. Show ip route ospf

Fuente: Autor

7.5 IMPLEMENTAR DHCP Y NAT PARA IPV4

7.5.1 CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

Con el fin de tener pool de DHCP para cada Vlan se procede a realizar la configuración en el Router 1 de los pools ACCT y ENGNR

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(dhcp-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(dhcp-config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#service dhcp R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#service dhcp R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit

TABLA 28. CONFIGURACIÓN DHCP R1

Al realizar la configuración del DHCP que se muestra en la tabla 28, se exceptuaron para asignar dos rango de ip, posterior a esto se configura el pool de DHCP para las vlan 21 y 23 sobre el que se requiere se inicie la asignación de IP dinámica a los host que se conecten.

7.5.2 CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

Se requiere configurar NAT estático y dinámico en el Router 2, en la tabla se muestran los comandos ejecutados para realizar la configuración. Adicionalmente, se configura el pool de direcciones públicas utilizables, en esta sección se configura el NAT y el pool de acuerdo a las indicaciones de la guía, Dirección global interna: 209.165.200.229, Conjunto de direcciones utilizables: 209.165.200.225 – 209.165.200.228

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15	R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authentication local
Crear una NAT estática al servidor web. Dirección global interna: 209.165.200.229	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#Interface s0/0/0 R2(config-if)#Ip nat inside R2(config)#Interface s0/0/1 R2(config-if)#Ip nat inside R2(config)#Interface g0/0 R2(config-if)#Ip nat outside
Configurar la NAT dinámica dentro de una ACL privada Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3	R2(config)# Access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)# Access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)# Access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2(config)# ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)# ip nat inside source list 1 pool INTERNET

Tabla 29. Configuración NAT R2

7.5.3 VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

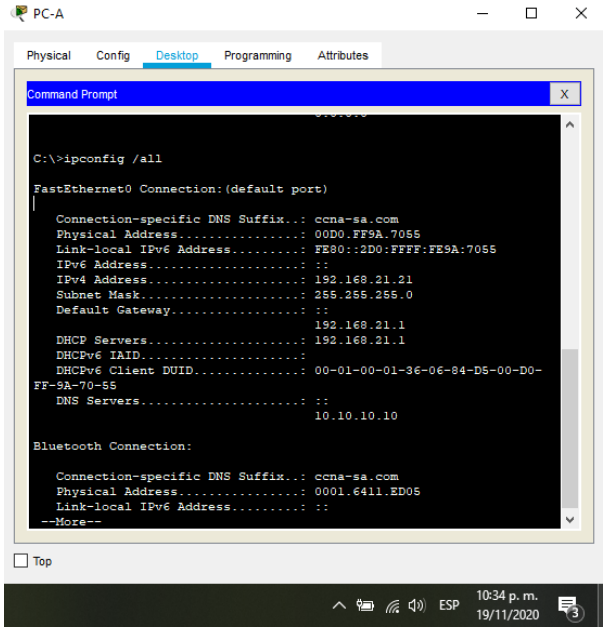
Despues de las configuraciones de DHCP y NAT estática se procede a revisar que los equipos tomen las IPs de manera dinámica.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso, toma ip 192.168.21.21
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso, toma ip 192.168.23.22
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Exitoso
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	PT no soporta el comando para habilitar el servidor http, por lo cual no se pudo realizar en R2, en un ambiente real debería funcionar y solicitar los datos de autenticación

Tabla 30. Pruebas DHCP

En la figura 38 se observa que el PC-A toma dirección IP por DHCP, en esta ocasión se le asignó la ip 192.168.21.21

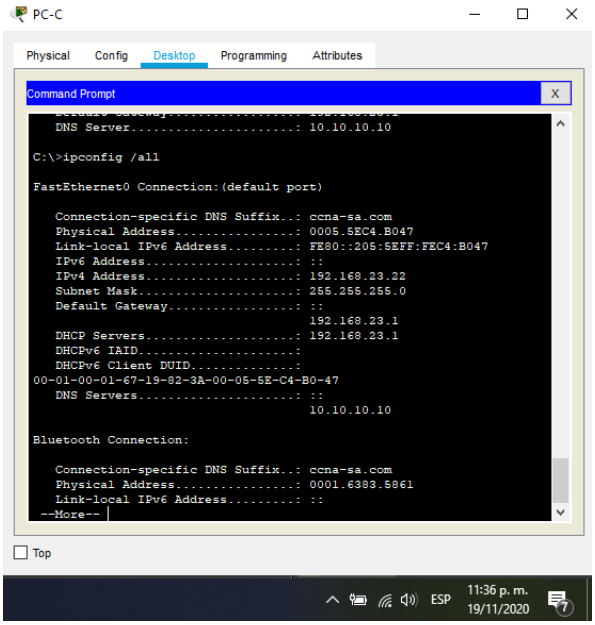
Figura 38. DHCP PC-A



Fuente: Autor

En la figura 39 se observa que el PC-C toma dirección IP por DHCP, en esta ocasión se le asignó la ip 192.168.23.22

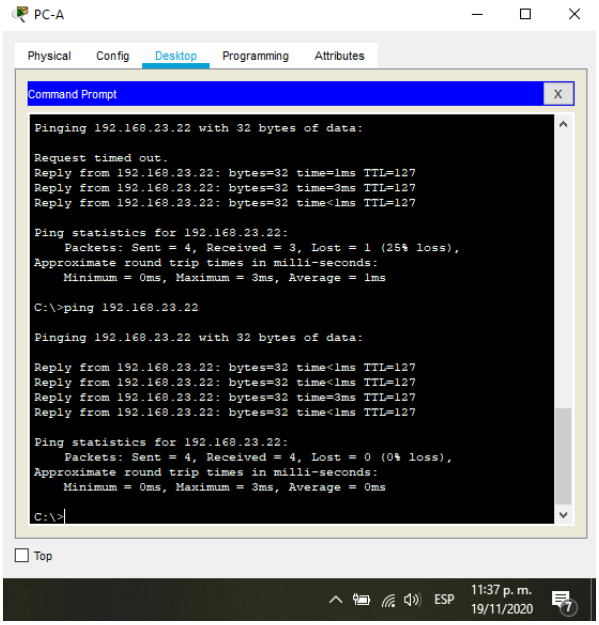
Figura 39. DHCP PC-C



Fuente: Autor

En la figura 40 se ejecutó ping del PC-A 192.168.21.21 al PC-C 192.168.23.22 el cual fue exitoso.

Figura 40. Ping PC-A A PC-C



Fuente: Autor

7.6 CONFIGURAR NTP

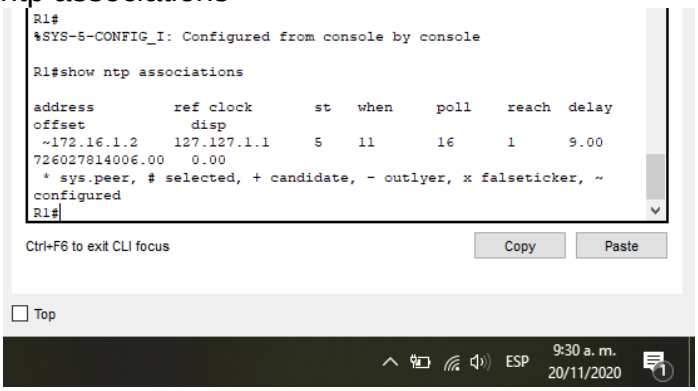
Se procede a configurar el protocolo para sincronización de relojes en los routers 2 y 1, en la tabla se indican los comandos empleados para tal fin

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2. 5 de marzo de 2016, 9 a. m.	R2#Clock set 09:00:00 05 march 2016
Configure R2 como un maestro NTP. Nivel de estrato: 5	R2(config)#ntp master 5
Configurar R1 como un cliente NTP. Servidor: R2	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Tabla 31. Configuración NTP

Con la configuración realizada en la tabla 31, el router 1 que es cliente NTP toma la hora establecida en el router 2. En la imagen 41 se puede ver en R1 el resultado de Show ntp associations.

Figura 41. Show ntp associations



Fuente: Autor

7.7 CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

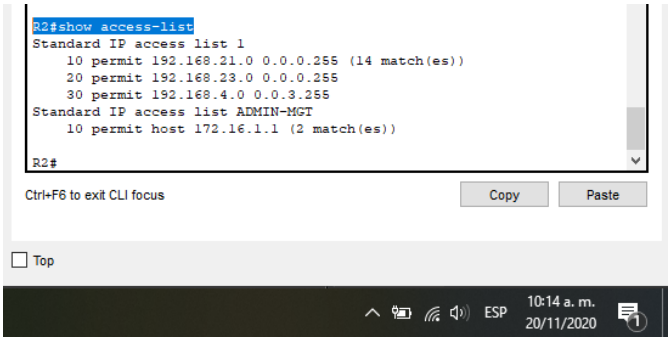
7.7.1 RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

Se configura la lista de acceso en el router 2 para restringir el acceso a las líneas vty, adicionalmente, se indica el comando a emplear para verificar la lista de acceso.

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

En la figura 42 se muestra la aplicación de las listas de acceso creadas, esto se muestra con el comando show Access-list

Figura 42. Show access-list



Fuente: Autor

7.7.2 INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE

Se indican los comandos correspondientes para obtener la información solicitada en la tabla

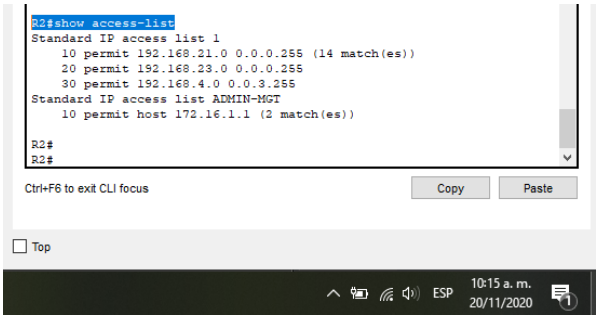
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list
Restablecer los contadores de una lista de acceso	clear ip access-list counters R2#clear ip access-list counters 1 PT no soporta el 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? Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.	R2#show ip nat translation
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

Tabla 32. Comandos comprobación R2

En la figura 43 se ve el resultado del comando show Access-list en el R2, se muestra la lista de acceso estándar y la lista ADMIN-MGT

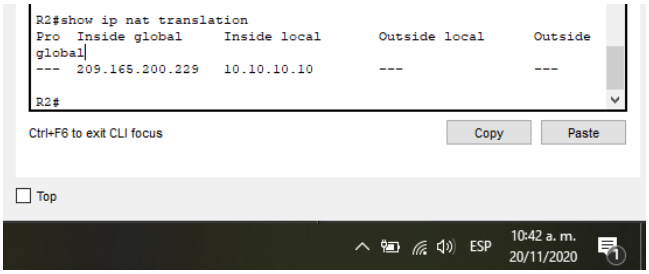
Figura 43. Show access-list R2



Fuente: Autor

En la figura 44 se muestra las traducciones NAT realizadas en el router 2 por medio del comando show ip nat translation, en este caso no se tenia traducciones realizadas

Figura 44. Show ip nat translation R2



Fuente: Autor

8 CONCLUSIONES

En el desarrollo del escenario se puede concluir que para efectuar una actividad exitosa es necesario tener clara la topología de red y los equipos que interactuaran en ella, asi como el direccionamiento que se va a emplear, esto para permitir un correcto funcionamiento de la misma y evitar enrutamientos erróneos.

Al realizar el diseño y configuración del escenario en Packet Tracert se fortalecen los conocimientos adquiridos en el curso y se brindan herramientas de análisis para brindar solución a los requerimientos reales que se presentan en la cotidianidad.

Al momento de configurar las Vlan es necesario validar cuales son las que deben crearse y habilitarse en cada equipo, ya que al no configurar una puede que los equipos pertenecientes a dicha vlan no tomen los enrutamientos o asignaciones en la red que se requiere.

La asignación por DHCP de las direcciones IP en la red permite la optimización de recursos, ya que este asigna automáticamente direcciones de red reutilizables y configuraciones adicionales a los diferentes host que se conectan.

El protocolo de enrutamiento OSPF proporciona balanceo de carga entre rutas de igual peso. Cuando un administrador especifica múltiples rutas hacia un destino con el mismo costo, el protocolo OSPF distribuye el tráfico entre todas las rutas de la misma manera.

Usar NAT aumenta el nivel de seguridad de la red ya que pemite ocultar el esquema de direccionamiento y la topología interna de la red, adicionalmente, ayuda a mitigar el agotamiento del espacio de direcciones IP públicas globales.

9 BIBLIOGRAFIA

B. (2018, 5 abril). Configurar DHCP en router CISCO. Bitacora Byte. https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

¿Cómo funciona un switch? (2020, 15 abril). Cisco. Recuperado 17 de Octubre de 2020, de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html

Configuración de los interfaces serial - Redes locales y globales. (s. f.). 1. Configuración de los interfaces serial - Redes locales y globales. Recuperado 17 de noviembre de 2020, de https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/3-configuracion-del-router/dddd-3/1-configuracion-de-los-interfaces-serial

Configuración del protocolo OSPF - Redes locales y globales. (s. f.). 6. Configuración del protocolo OSPF - Redes locales y globales. Recuperado 18 de noviembre de 2020, de https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/6-configuracion-del-encaminamiento/2-encaminamiento-dinamico/6-protocolo-ospf/6-configuracion-del-protocolo-ospf

En.wikiversity.org. 2020. Cisco Networking/CCENT/Access Control Lists - Wikiversity. Recuperado 20 de Noviembre de 2020, de: https://en.wikiversity.org/wiki/Cisco_Networking/CCENT/Access_Control_Lists#:~:text=Access%20lists%20filter%20either%20inbound,ip%20access%2Dlist%20EXEC%20command

Ferreiro, A. C. (2020, 20 octubre). Reforzando la seguridad en los router Cisco. Backtrack Academy. Recuperado 16 de octubre de 2020, de https://backtrackacademy.com/articulo/reforzando-la-seguridad-en-los-router-cisco#:%7E:text=A%20partir%20del%20release%2012.3,de%200%20a%2016%20caracteres.&text=Este%20comando%20se%20aplica%20sobre,exec%20privilegiado%20y%20lineas%20virtuales.

IBM Knowledge Center. (s. f.). IBM. Recuperado 17 de octubre de 2020, de https://www.ibm.com/support/knowledgecenter/es/ssw_aix_72/navigation/welcome.html

Interfaces y subinterfaces - Cursos CISCO CCNA. (s. f.). Interfaces y subinterfaces - Cursos CISCO CCNA. Recuperado 16 de octubre de 2020, de https://sites.google.com/site/cursosciscoccna/cisco-3/6-enrutamiento-entre-las-vlan/1-2-interfaces-y-subinterfaces

¿Qué es NAT? (s. f.). ¿Qué es NAT? Recuperado 21 de noviembre de 2020, de https://www.speedcheck.org/es/wiki/nat/

¿Qué es un router? - Definición y usos. (2020, 17 abril). Cisco. Recuperado 17 de Octubre de 2020, de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html#%7Ehow-does-a-router-work

Servidor de Nombres IP (2015, 17 marzo). Cisco. Recuperado 16 de octubre de 2020, de https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity_exp/rel3_1/command/reference/i_cmds.html

10 ANEXOS

Escenario 1

https://drive.google.com/file/d/11931PI56uJUy6b-h277rCdKzJdeuDwpr/view?usp=sharing

Escenario 2

https://drive.google.com/file/d/1MfMFrYSCo2oTVol7zZhZ15hn6k1rL1CB/view?usp=sharing

Articulo

https://drive.google.com/file/d/1bcRPoFXWBntsMQbDXZc3wKgZGVH4OVP3/view?usp=sharing