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

CRISTIAN CAMILO LAVERDE LADINO

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

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

CRISTIAN CAMILO LAVERDE LADINO

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

DIRECTOR: DIEGO EDINSON RAMIREZ

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

Nota de aceptación

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Ibagué, 12 de diciembre de 2020

DEDICATORIA

“Siempre parece imposible hasta que está hecho”
Nelson Mándela.

A Dios por llenarme de sabiduría en la realización de este trabajo, y con mucho cariño a mi familia por su apoyo, comprensión y esfuerzo por llenarme de ánimo cada mañana para afrontar la vida, fundación Generando hacia un futuro por el apoyo recibido en mi proceso formativo.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

DIEGO EDINSON RAMIREZ, Ingeniero Electrónico, tutor asignado al diplomado de profundización cisco (diseño e implementación de soluciones integradas LAN / WAN).

Fundación Generando Hacia un futuro, por el apoyo económico brindado.

CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

AUTOMATIZACIÓN: Una red automatizada es aquella en la cual los dispositivos pueden ser conjurados, aprovisionados, gestionados y probados automáticamente. Esto permite mejorar la ciencia, evitar errores humanos y reducir los gastos operativos.

IPV4: Es un sistema de direccionamiento de 32 bits que se utiliza para identificar un dispositivo en una red. Es el sistema de direccionamiento utilizado en la mayoría de las rede informáticas, incluida Internet.

IPv6: Es un sistema de direccionamiento de 128 bits que se utiliza para identificar un dispositivo en una red. Es el sucesor de IPv4 y la versión más reciente del sistema de direccionamiento utilizado en las redes informáticas.

LAN: Red de Área Local, conecta equipos informáticos ubicados en un área geógrafa reducida, como una edición o una habitación.

ROUTERS: Conectan varias redes. También conectan computadoras en esas redes a Internet. Los routers permiten que todas las computadoras en red compartan una única conexión a Internet, lo que ahorra dinero.

SWITCHES: Son la base de la mayoría de las redes empresariales. Un switch actúa como un controlador, que conecta computadoras, impresoras y servidores a una red en un edificio o campus.

VLAN: Basada en protocolos: los grupos basados en protocolos se pueden definir y vincular a un puerto; por lo tanto, cada paquete que se origina en los grupos de protocolos se asigna a la VLAN configurada en la página.

WAN: Es un conjunto de redes LAN que conecta equipos informáticos que se encuentran en diferentes ubicaciones físicas.

RESUMEN

Simulación y documentación de dos escenarios con características especiales de configuración, necesarias para el funcionamiento y requerimiento para la solución de problemáticas reales en entornos corporativos utilizando tecnología cisco.
Un primer escenario compuesto por una red pequeña la cual es configurada para que los dispositivos que la conforman puedan recibir conectividad IPv4 y IPv6, configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Segundo escenario compuesto por una red pequeña la cual es configurada para que los dispositivos que la conforman puedan recibir conectividad IPv4 y IPv6, siguiendo protocolos de configuración OSPF, DHCP, NTP.
La configuración realizada esta sustentada por medio de imágenes tomadas de la ejecución de comando Ping y show que reflejan la conectividad entre dispositivos y su configuración.

Palabras clave: Cisco, IPv4, IPv6, Networking, Topología, VLAN.

ABSTRACT:

Simulation and documentation of two scenarios with special configuration characteristics, necessary for the operation and requirement for the solution of real problems in corporate environments using Cisco technology.
A first scenario composed of a small network which is configured so that the devices that make it up can receive IPv4 and IPv6 connectivity, routing configuration between VLAN, DHCP, Etherchannel and port-security. Second scenario composed of a small network which is configured so that the devices that make it up can receive IPv4 and IPv6 connectivity, following OSPF, DHCP, NTP configuration protocols.
The configuration carried out is supported by images taken from the execution of the Ping and show command that reflect the connectivity between devices and their configuration.

Keywords: Cisco, IPv4, IPv6, Networking, Topology, VLAN.

INTRODUCCIÓN

El curso diplomado de profundización Cisco, está constituido por dos módulos: Network Fundamentals (CCNA1 R&S) y Routing and Switching Fundamentals (CCNA2 R&S), los cuales forman parte del currículo CCNA R&S adscrito a la Academia CISCO, formado en diez unidades divididas en cinco unidades para el módulo CCNA1 y 5 restantes para el módulo CCNA2.El estudiante utiliza herramientas de Simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de diversos protocolos y métricas de enrutamiento.

Se identifica las herramientas de supervisión y protocolos de administración de red disponibles en el IOS para resolver los problemas de las redes de datos, evaluando el desempeño de routers y switches, mediante el uso de comandos especializados en gestión de redes y compatibles con el protocolo SMNP.

Prueba de habilidades prácticas, es una de las actividades que agrupan el diplomado de profundización CCNA, esta tiene como objetivo poner en práctica las los conceptos aprendidos durante el desarrollo de este diplomado, utilizando la herramienta cisco packet tracer, se desarrollan simulaciones buscando establecer escenario LAN/WAN que permitan analizar comportamientos de diversos protocolos y métricas de enrutamiento.

Dos escenarios propuestos a los cuales se darán solución acorde a los lineamientos establecidos y se documentara todo su desarrollo como evidencia sustentado con imágenes y comandos de ejecución.

Primer escenario configura los dispositivos de una red pequeña, conformada por: un router, dos swich y dos PC, estos configurados con un enrutamiento VLAN, DHCP, Etherchannel y port-security.

Segundo escenario consiste en 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.

DESARROLLO

1 ESCENARIO 1

Figura 1.Topologia escenario 1

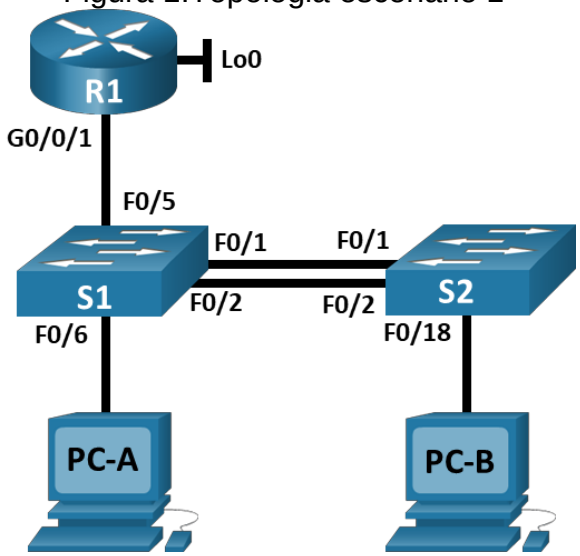
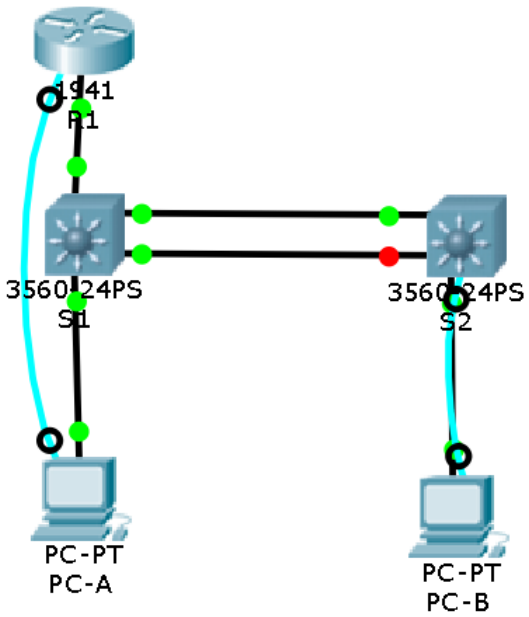


Figura 2. Escenario 1 packet tracer



Fuente: Autor

1.1 TABLA DE VLAN

Tabla 1. Distribución VLAN

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

Esta tabla contiene las VLAN que deberán ser creadas en la red.

1.2 TABLA DE ASIGNACIÓN DE DIRECCIONES

Tabla 2. Direcciones ip

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

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
	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

Esta tabla contiene el direccionamiento IP de la red.

1.3 INICIALIZAR, RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

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

Se procede a borrar la configuración inicial del ROUTER1:
Se utiliza una aserie de comandos para borrar configuración inicial, y que el dispositivo quede libre de configurar a nuestra necesidad.

Tabla 3. Reinicio del Router

Tarea	Comandos
Iniciar modo privilegiado	Router>enable
Eliminar configuración inicial	Router#erase startup-config
Recargar el dispositivo	Router#reload

Se recarga el router, al ejecutar el comando, observamos la información suministrada por la terminal donde encontramos características de fábrica del router.

Tabla 4. Reinicio del switch

Tarea	Comandos
Iniciar modo privilegiado	Switch>en
Eliminar configuración inicial	Switch#erase startup-config
Recargar el dispositivo	Switch#reload

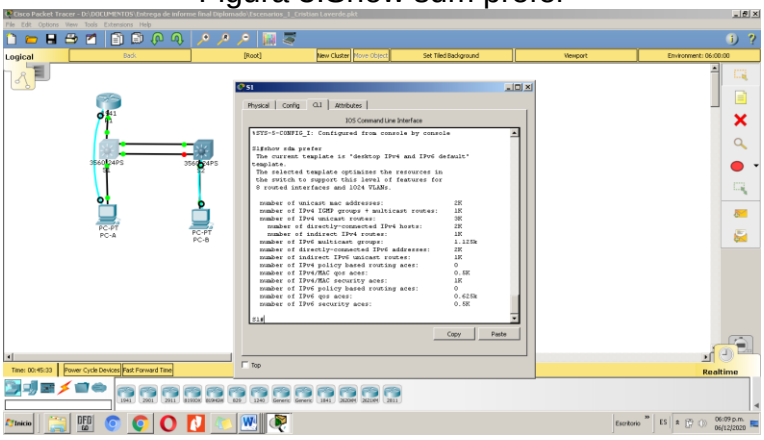
Después de recargar el switch, se configura la plantilla SDM que admita IPv6 según sea necesario y se vuelve a cargar el switch.

Tabla 5. Plantilla SDM

Tarea	Comandos
Ver plantilla SDM	Se ingresa al modo privilegiado observar plantilla predeterminada Switch>enable Switch#show sdm prefer
Configurar plantilla SDM	Se observa que la plantilla SDM no cuenta con características Ipv6, procedemos habilitarlas. Switch#config Switch(config)#sdm prefer ?
Modificar plantilla	Se selecciona dual-ipv4-and-ipv6 Support both IPv4 and IPv6, la cual soporta la configuración requerida. Switch(config)#sdm prefer dual-ipv4-and-ipv6 ? Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Volver a cargar	Este proceso se debe realizar para que se vean reflejados los cambios realizados Switch#reload
Verificar cambios realizados	Se verifica que los cambios realizados ya se vean reflejados en la configuración. Switch>en Switch#show sdm prefer

Se realiza la selección pertinente para que los dispositivos admitan IPv6.

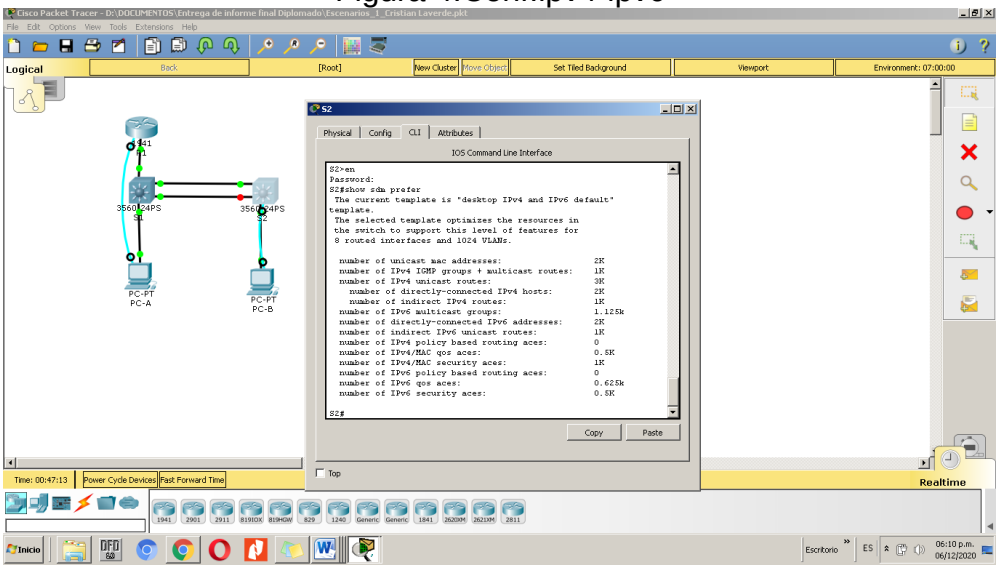
Figura 3.Show sdm prefer



Fuente: Autor

La configuración fue exitosa y los cambios ya se ven reflejados en la configuración del dispositivo

Figura 4.Conf.ipv4-ipv6



Fuente: Autor

Se observa como resultado del comando “show sdm prefer” que ahora la platilla sdm en los dos switche soporta característica ipv4 y ipv6 necesaria para la configuración que debe tener la red.

1.3.2 Configurar R1.

Se deben desactivar la búsqueda DNS y renombrar el router y el dominio, se asigna seguridad de ingreso con mensajes de advertencia, se configuran interfaz y subinterfaces.

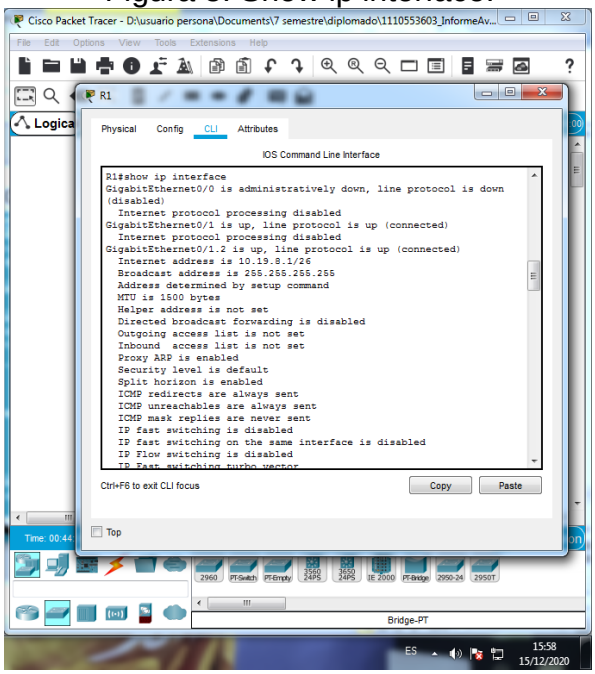
Tarea	**Especificación**
Desactivar la búsqueda DNS	Se utilizan dos líneas de comando para desactivar la búsqueda DNS en el router 1 Router>en Router#conf Router(config)#no ip domain lookup
Nombre del router	Se asigna nombre R1 al router 1 Router(config)#hostname R1
Nombre de dominio	Línea de comando para asignar un nombre de dominio en el router 1 R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Se asigna contraseña para el modo EXEC privilegiado en el router 1. R1(config)#enable secret ciscoenpass

Tarea	Especificación
	R1(config)#line console 0
Contraseña de acceso a la consola	Se asigna una Contraseña de acceso a la consola en el router 1. R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	Establecer la longitud mínima para las contraseñas en el router 1 de 10 caracteres. R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Asignar nombre de usuario admin con contraseña admin1pass. R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Configurar el inicio de sesión en las líneas VTY para que use la base de datos local en el router 1. R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	Configurar VTY solo aceptando SSH en el router 1. R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Cifrar las contraseñas de texto no cifrado en el router 1. R1(config)#service password-encryption
Configure un MOTD Banner	Configure un MOTD Banner en el router 1. R1(config)#banner motd --Prohibido acceso no autorizado --
Habilitar el routing IPv6	Habilitar el routing IPv6 en el router 1 R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Se utiliza serie de comandos para establecer la dirección IPv4,establecer la dirección local de enlace IPv6 como **fe80: :1,** establecer la dirección IPv6 y activar la interfaz. R1(config)#int g0/1.2

Tarea	Especificación
	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 addres 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 addres fe80::1 link-local R1(config-subif)#int g0/1.3 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 addres 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 addres fe80::1 link-local R1(config-subif)#int g0/1.4 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 addres fe80::1 link-local R1(config-subif)#int g0/1.6 R1(config-subif)#encapsulation dot1q 6 Native R1(config-subif)#description Native R1(config-subif)#int g0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	Se configura el Loopback0 interface en el router 1. 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 addres fe80::1 link-local
Generar una clave de cifrado RSA	Genera una clave de cifrado RSA en el R1 con modulo 1024. R1(config)#crypto key generate rsa

Tarea	Especificación
	general-keys modulus 1024

Figura 5. Show ip interface.



Fuente: Autor.

Verificamos las inter faces de red del router por medio del comando show ip interface.

1.3.3 Configure S1 y S2.

S1: Se asigna configuración nombre, dominio, seguridad de acceso con avisos, y configuración de interface.

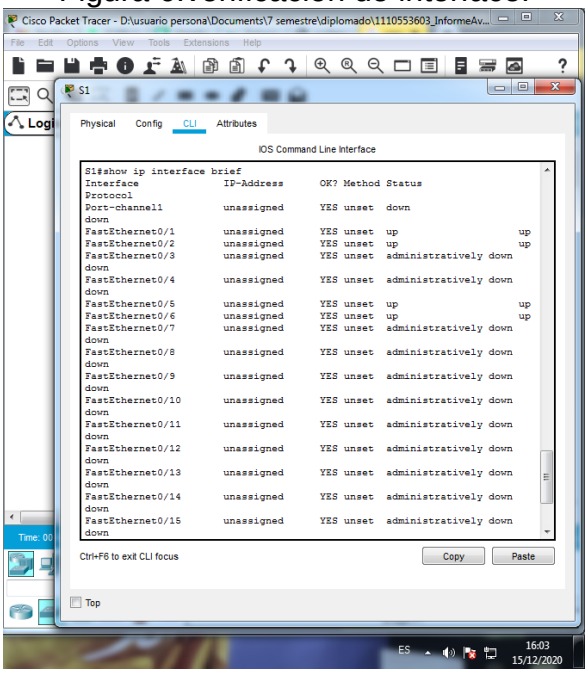
Tabla 6.Configuracion S1

Tarea	Especificación
Desactivar la búsqueda DNS.	comandos para Desactivar la búsqueda DNS en el Switch 1. Switch>en Switch#conf Switch(config)#no ip domain lookup
Nombre del switch	Asignar S1 como nombre a Switch 1 Switch(config)#hostname S1
Nombre de dominio	Asignar Nombre de dominio en el S1

Tarea	Especificación
	S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Asignar contraseña para el modo EXEC privilegiado del S1. S1(config)#enable secret ciscoenpass S1(config)#line console 0
Contraseña de acceso a la consola	Se asigna contraseña para el ingreso a consola del S1. S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	Se asigna nombre de administrador admin con contraseña admin1pass. S1(config-line)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configure el inicio de sección en la línea VTY para usar 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	Se configura las líneas VTY para aceptar únicamente las conexiones SSH. S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Cifrar las contraseñas de texto no cifrado en el S1. S1(config)#service password-encryption
Configurar un MOTD Banner	Se configura aviso de advertencia. S1(config)#banner motd -Prohibido acceso no autorizado-
Generar una clave de cifrado RSA	Generar una clave de cifrado RSA en el S1. S1(config)# crypto key generate rsa generalkeys modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3. S1(config)#int vlan 4 S1(config-if)#description VLAN4 S1(config)#ip address 10.19.8.98

Tarea	Especificación
	255.255.255.248 S1(config)#int vlan 4 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown
Configuración del gateway predeterminado	Configuración del gateway predeterminado en el S1. S1(config)#ip default-gateway 10.19.8.97

Figura 6.verificacion de interface.



Fuente: Autor.

Verificamos que las interfaces configuradas en el switch S1 se encuentren activadas.

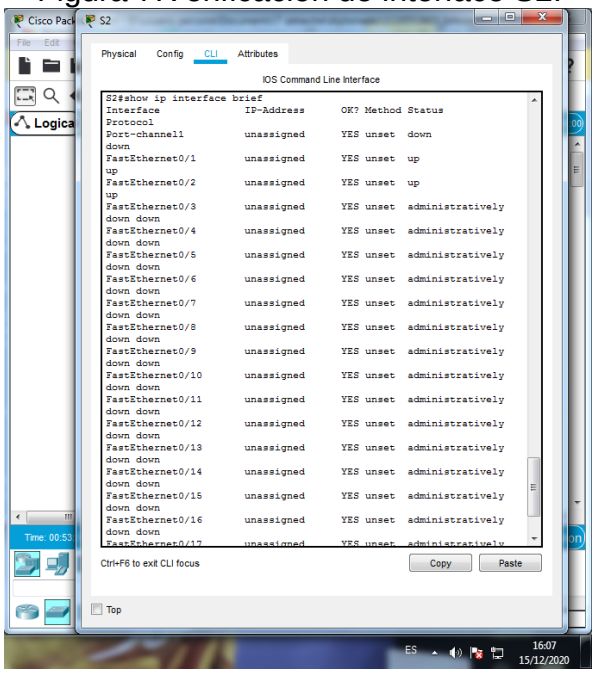
Se asigna configuración S2 nombre, dominio, seguridad de acceso con avisos, y configuración de interface.

Tabla 7.Configuracion S2

Tarea	**Especificación**
Desactivar la búsqueda DNS.	comandos para Desactivar la búsqueda DNS en el Switch 2. Switch>en Switch#conf Switch(config)#no ip domain lookup
Nombre del switch	Asignar S1 como nombre a Switch 1 Switch(config)#hostname S2
Nombre de dominio	Asignar Nombre de dominio en el S2 S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Asignar contraseña para el modo EXEC privilegiado del S2. S2(config)#enable secret ciscoenpass S2(config)#line console 0
Contraseña de acceso a la consola	Se asigna contraseña para el ingreso a consola del S2. S2(config-line)#password ciscoconpass S2(config-line)#login
Crear un usuario administrativo en la base de datos local	Se asigna nombre de administrador admin con contraseña admin1pass. S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configure el inicio de sección en la línea VTY para usar 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	Se configura las líneas VTY para aceptar únicamente las conexiones SSH. S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	Cifrar las contraseñas de texto no cifrado en el S1. S2(config)#service password-encryption
Configurar un MOTD Banner	Se configura aviso de advertencia. S2(config)#banner motd -Prohibido acceso no autorizado-
Generar una clave de cifrado RSA	Generar una clave de cifrado RSA en el S2.

Tarea	Especificación
	S2(config)#crypto key generate rsa
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)#int vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 addres 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Interface S2(config-if)#no shutdown
Configuración del gateway predeterminado	Configuración del gateway predeterminado en el S1. S2(config)#ip default-gateway 10.19.8.97

Figura 7.Verificacion de interface S2.



Fuente: Autor

Verificamos que las interfaces configuradas en el switch S2 se encuentren activadas.

1.4 CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

1.4.1 Configurar S1

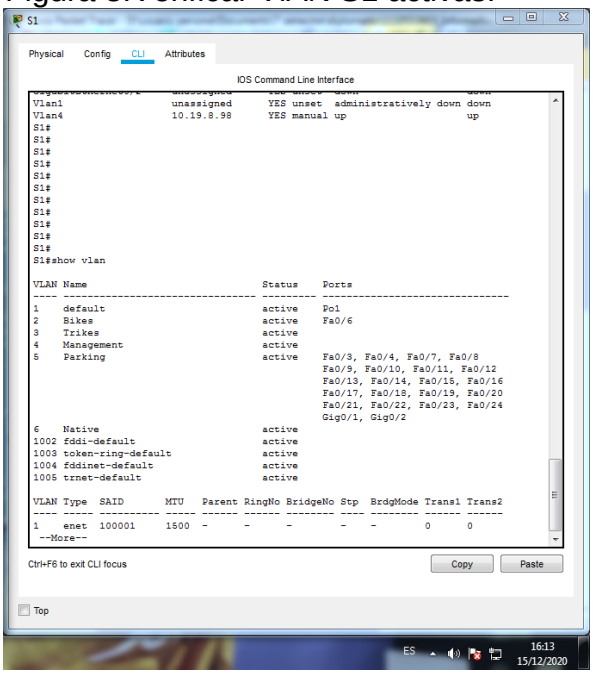
Por medio de los siguientes comandos se procede a configurar el S1, creación de VLAN, troncales, configuración de puertos de acceso de host.

Tabla 8.Creacion de VLANS en S1

Tarea	Especificación
Crear VLAN	Se realiza la creación de VLAN como se especifica en (Tabla 1. Distribución VLAN) S1#confi 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	Crear troncos 802.1Q que utilicen la VLAN 6 nativa. S1(config)#int 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)#int range S1(config)#int 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)#int range f0/1-2 S1(config-if-range)#shutdown
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk

Tarea	Especificación
	S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#int port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	Configurar el puerto de acceso de host para VLAN 2, Interface F0/6. S1(config-if)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	Configurar la seguridad del puerto en los puertos de acceso, Permitir 3 direcciones MAC S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar. S1(config-if)#int range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description no en uso S1(config-if-range)#shutdown S1(config-if-range)#int range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description no en uso S1(config-if-range)#shutdown Proteger todas las interfaces no utilizadas, Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1(config)#int g0/1 S1(config-if)#int range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description *No esta en uso * S1(config-if-range)#shutdown

Figura 8.Verificar VlAN S1 activas.



Fuente:Autor

Se verifica que la creación de las Vlan es tal cual como lo muestra la topología y se encuentran activas y con la asignación de los respectivos puertos.

1.4.2 Configuración de S2.

En la siguiente tabla se presenta la configuración del S1, creación de VLANS como corresponde en la topología.

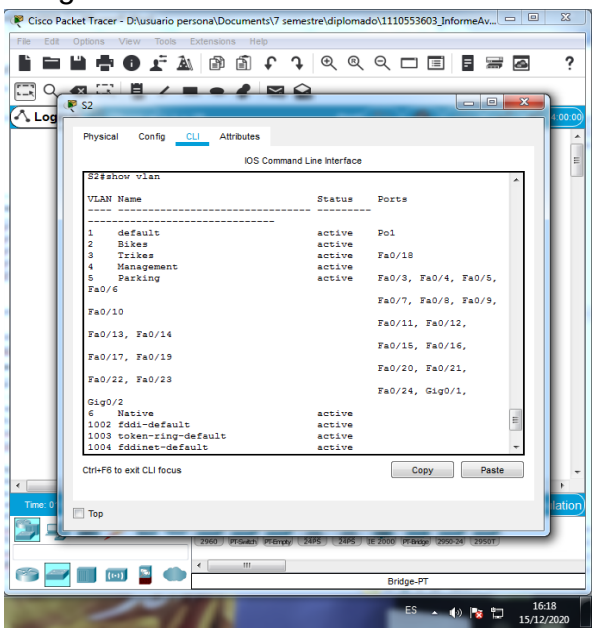
Tabla 9. Creación de VLANS en S2

Tarea	**Especificación**
Crear VLAN	Se realiza la creación de VLAN como se especifica en (Tabla 1. Distribución VLAN) S2>en S2#confi 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)#

Tarea	Especificación
	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.	Crear troncos 802.1Q que utilicen la VLAN 6 nativa S2(config)#int range f0/1-2 S2(config-if-range)#shutdown
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación.Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#
Configurar el puerto de acceso del host para la VLAN 3	Configurar el puerto de acceso de host para VLAN 3, Interface F0/18 S2(config-if-range)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Configure port-security en los access ports	Configurar la seguridad del puerto en los puertos de acceso, Permitir 3 direcciones MAC S2(config-if)#int range f0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description *no esta en uso* S2(config-if-range)#shutdown
Asegure todas las interfaces no utilizadas.	Proteger todas las interfaces no utilizadas, Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S2(config-if-range)#int range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description *no esta en uso* S2(config-if-range)#shutdown

Tarea	Especificación
	S2(config-if-range)#int range g0/1-2 S2(config-if-range)#switchport mode Access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description *no esta en uso* S2(config-if-range)#shutdown

Figura 9.Verificar VLAN activas en S2



Fuente:Autor.

Se verifica que la creación de las Vlan en el S2 es tal cual como lo muestra la topología y se encuentran activas y con la asignación de los respectivos puertos.

1.4.3 Configurar soporte de host Configure R1

Configure Default Routing, Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0.

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1>en R1#confi R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP	Cree un grupo DHCP para VLAN 2,

Tarea	Especificación
para VLAN 2	compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada. R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#ip dhcp pool VLAN2-Bikes R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#default-name ccna-a.net
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada. R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.89 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)#ip domain-name ccna-b.net

1.4.4 Configurar los servidores.

Configurar 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.PC-A configuración.

PC-A Network Configuration	
Descripción	Connection-specific DNS Suffix..:
Dirección física	FE80::206:2AFF:FE51:7592
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1

PC-A Network Configuration	
Gateway predeterminado IPv6	FE80::1

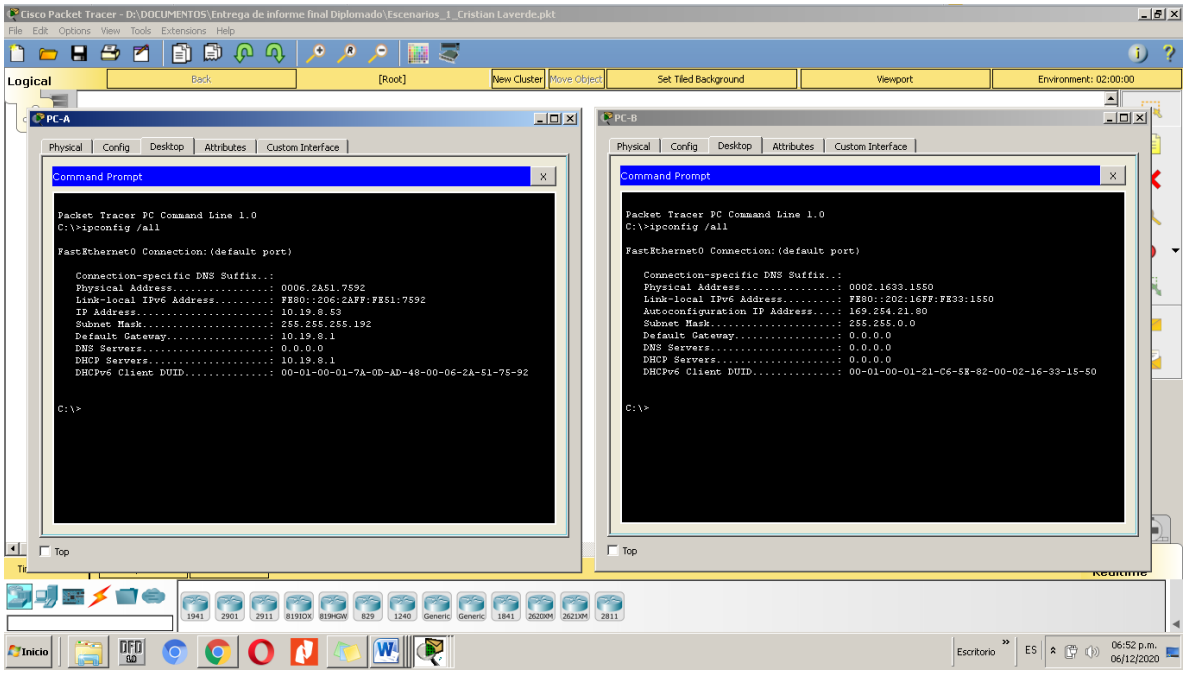
Se observa el direccionamiento que obtiene el PC-A tras recibir la información del servidor DNS.

Tabla 11.PC-B Configuración.

PC-A Network Configuration	
Descripción	Connection-specific DNS Suffix..:
Dirección física	FE80::202:16FF:FE33:1550
Dirección IP	10.19.8.90
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Se observa el direccionamiento que obtiene el PC-B tras recibir la información del servidor DNS

Figura 10.Ipconfig /all en PC-A y PC-B



Fuente: Autor

Por medio del comando ipconfig /all podemos verificar que los PC adquirieron direccionamiento estático IPv6 GUA y DHCP para IPv4.

1.4.5 Probar y verificar la conectividad de extremo a extremo.

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

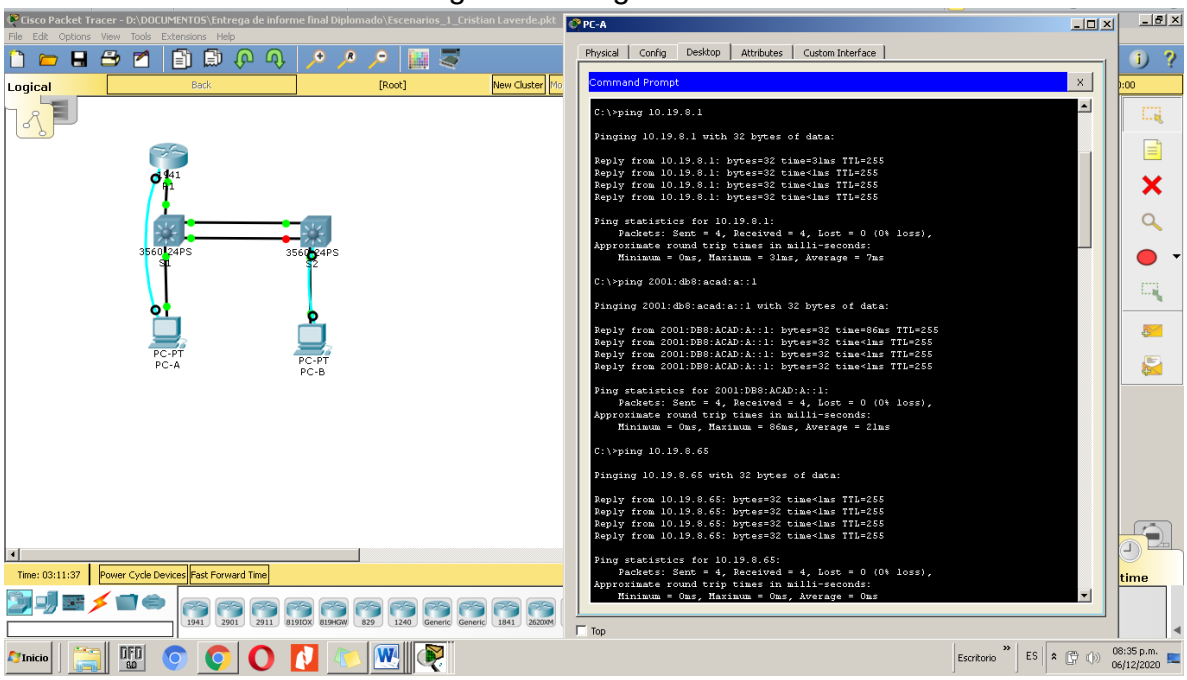
Tabla 12.verificación ping

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

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

Esta tabla hace referencia a las pruebas con el comando ping desde los PC hacia los demás dispositivos las evidencias podrán observarlas en las siguientes imágenes.

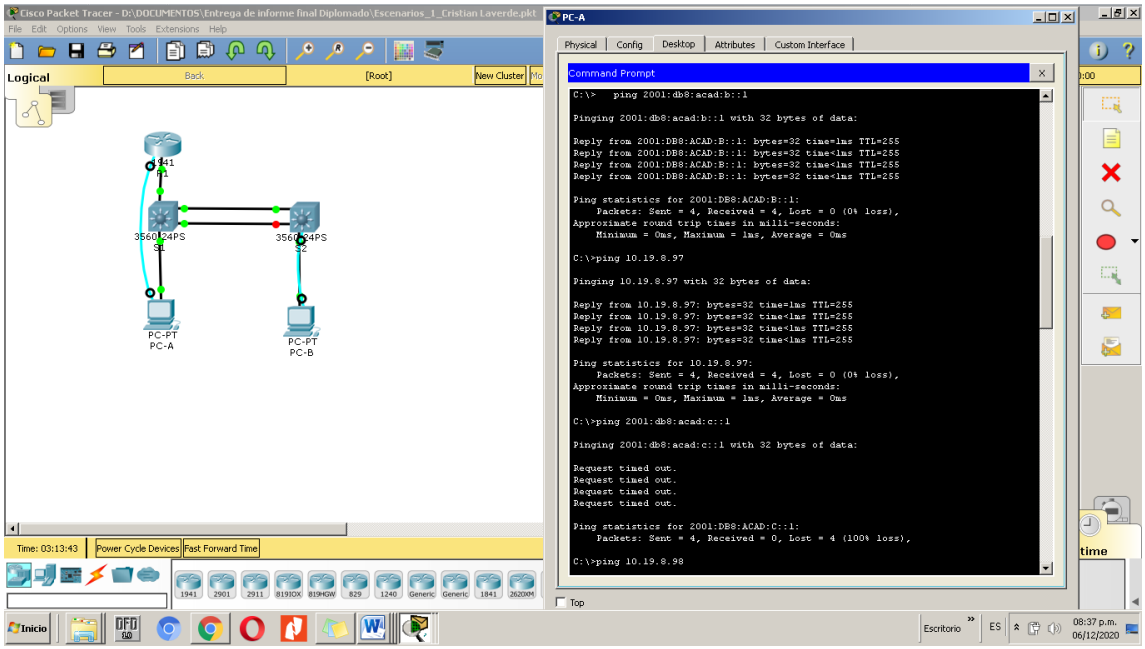
Figura 11.Ping PC-A R1



Fuente: Autor

La ejecución del comando ping entre la PC-A y R1 es satisfactorio, demostrando que hay conectividad entre los dispositivos.

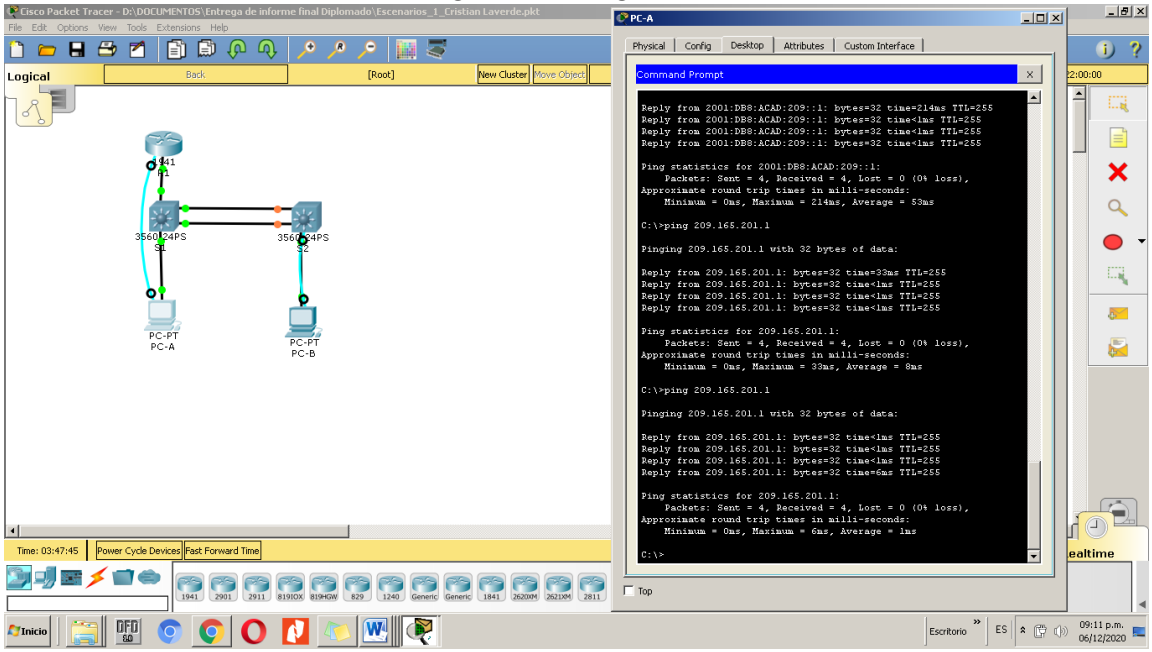
Figura 12.Ping PC-A a R1 interface



Fuente: Autor

La ejecución del comando ping entre la PC-A y R1 es satisfactorio por interface, demostrando que hay conectividad entre los dispositivos.

Figura 13.Ping PC-A S2

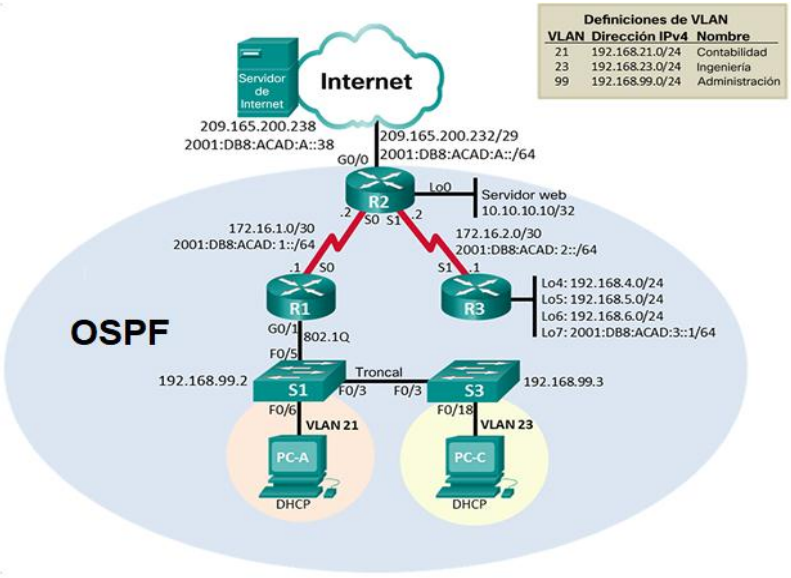


Fuente: Autor

La ejecución del comando ping entre la PC-A y S1 obteniendo satisfactorio por interface, demostrando que hay conectividad entre los dispositivos.

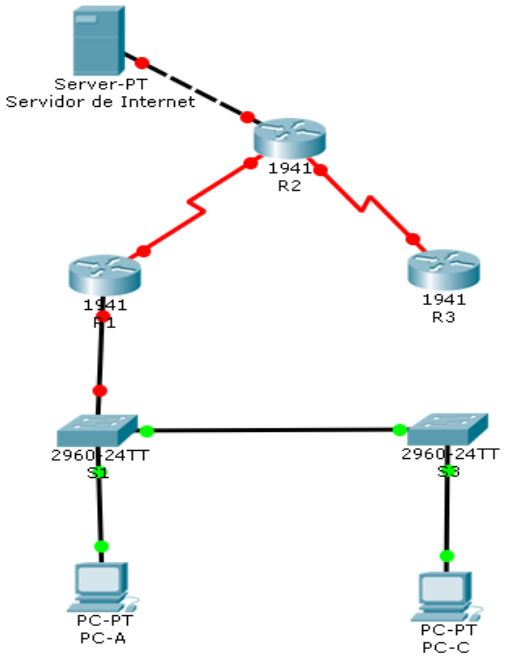
2 ESCENARIO 2

Figura 14.Topología Escenario 2



2.1 MONTAJE DE LA RED EN CISCO PACKET TRACER

Figura 15.Escenario 2 packet tracer.



Fuente: Autor

Se realiza montaje de la red utilizando el programa de simulación Cisco packet tracer.

Tabla 13. Dispositivos

Server-PT	Servidor de internet
Router 1941	R1
Router 1941	R2
Router 1941	R3
Switche 2960-24TT	S1
Switche 2960-24TT	S3
PC-PT	PC-A
PC-PT	PC-C

Tabla de especificación de dispositivos en uso para el montaje de la red.

2.2 INICIALIZAR DISPOSITIVOS

2.2.1 Inicializar y volver a cargar los routers y los switches

Tabla 14. Borrar Configuracion.

Tarea	Comandos
Iniciar modo privilegiado	Router>enable
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Recargar el dispositivo	Router#reload

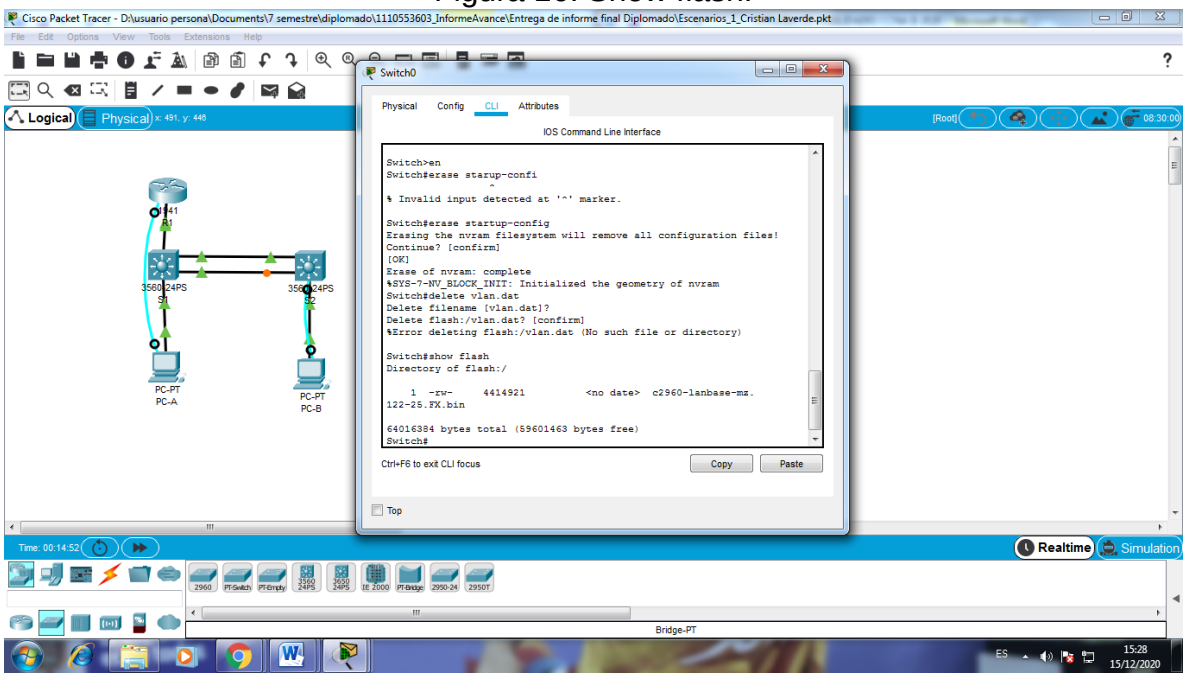
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

Tabla 15.Eliminar base de datos VLAN

Tarea	Comandos
Iniciar modo privilegiado	Switch>en
Eliminar configuración inicial	Switch#erase startup-config
Eliminar la base de datos de VLAN	Switch#delete vlan.dat
Recargar el dispositivo	Switch#reload

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

Figura 16. Show flash.



Fuente: Autor.

Verificamos que el dispositivo ya no cuenta con la base de datos de las VIAN.

2.3 CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

2.3.1 Configurar la computadora de Internet

En la siguiente tabla verá reflejado el direccionamiento asignado para el servidor de internet.

Tabla 16.Configuracion ip

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	201:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:db8:acad:2::1

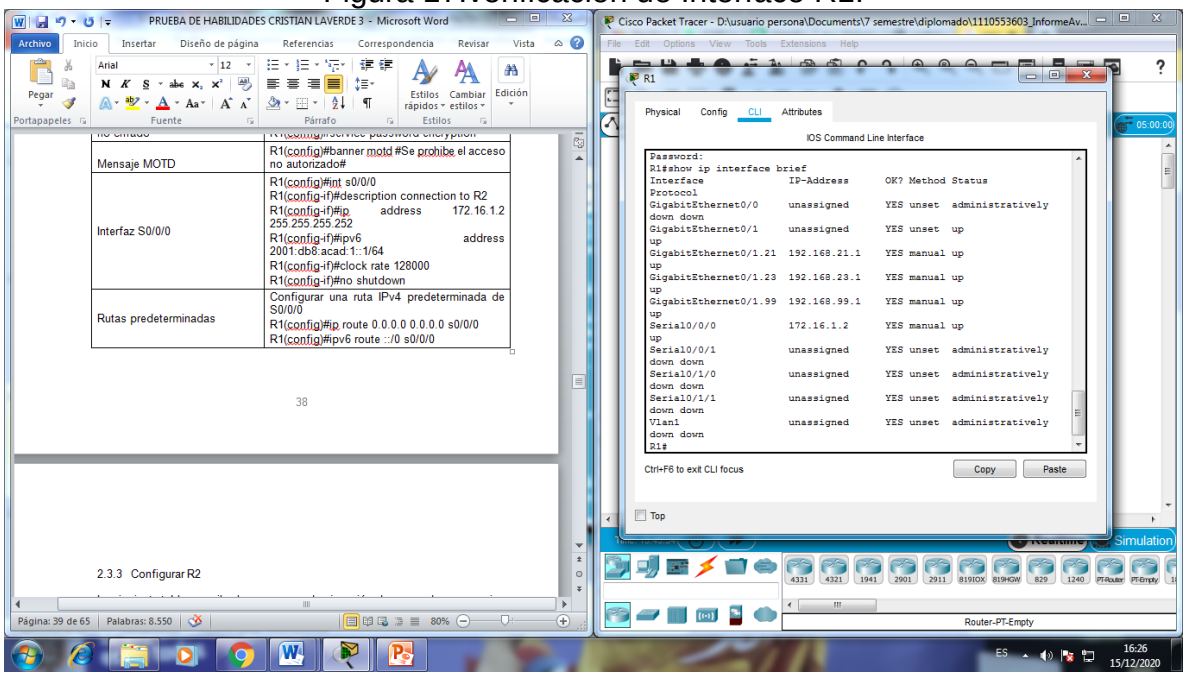
2.3.2 Configurar R1

La siguiente tabla recopila el paso a paso de ejecución de comandos necesarios para la configuración del R1, se podrá observar la tarea realizada y los comandos utilizados.

Tabla 17.Configuracion R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#confi 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 con 0 R1(config-line)#pass cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#pass 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 to R2 R1(config-if)#ip address 172.16.1.2 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0

Figura 17.verificacion de Interface R1.



Fuente:Autor

Se comprueba que las interfaces configuradas en el R1 se encuentran activas.

2.3.3 Configurar R2

La siguiente tabla recopila el paso a paso de ejecución de comandos necesarios para la configuración del R2, se podrá observar la tarea realizada y los comandos utilizados.

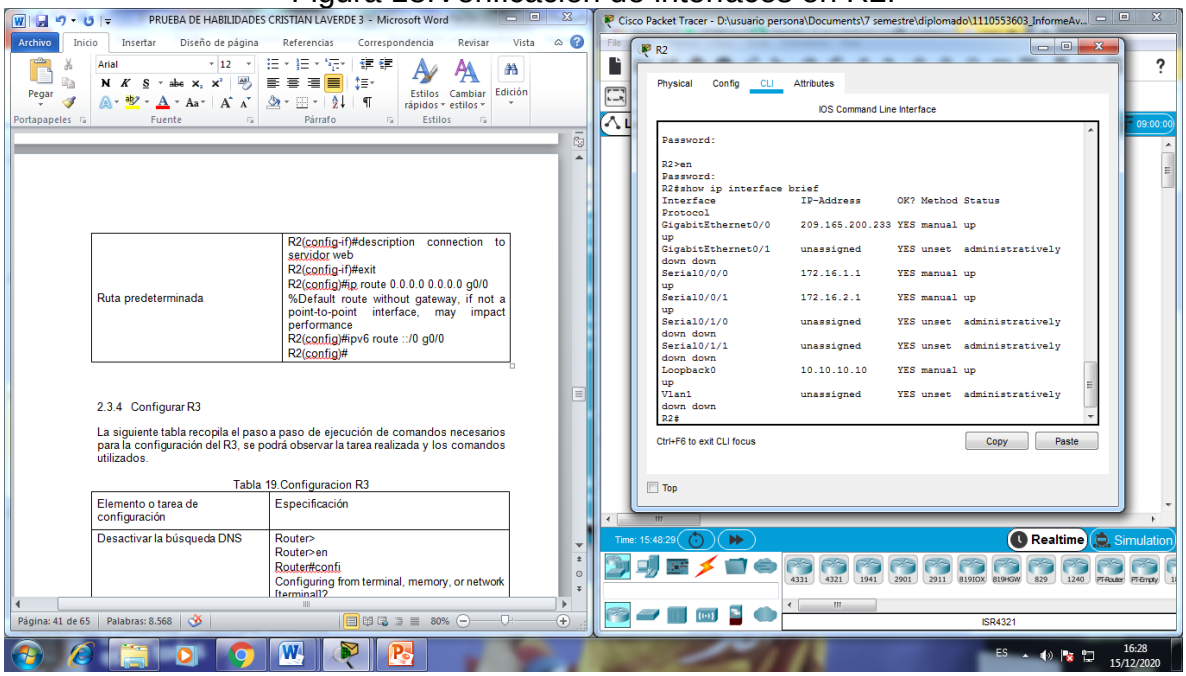
Tabla 18.Configuracion R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#confi 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 con 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
Cifrar las contraseñas de texto no cifrado	R2(config-line)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
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)# ip address 172.16.1.1 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown
Interfaz S0/0/1	R2(config-if)#int s0/0/1 R2(config-if)#description connection 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)	R2(config-if)#int g0/0 R2(config-if)#description connection to Internet R2(config-if)# ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#int loopback 0 R2(config-if)# ip address 10.10.10.10 255.255.255.255

Ruta predeterminada	R2(config-if)#description connection to servidor web R2(config-if)#exit R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Figura 18.Verificacion de interfaces en R2.



Fuente: Autor

Se comprueba que las interfaces configuradas en el R2 se encuentran activas.

2.3.4 Configurar R3

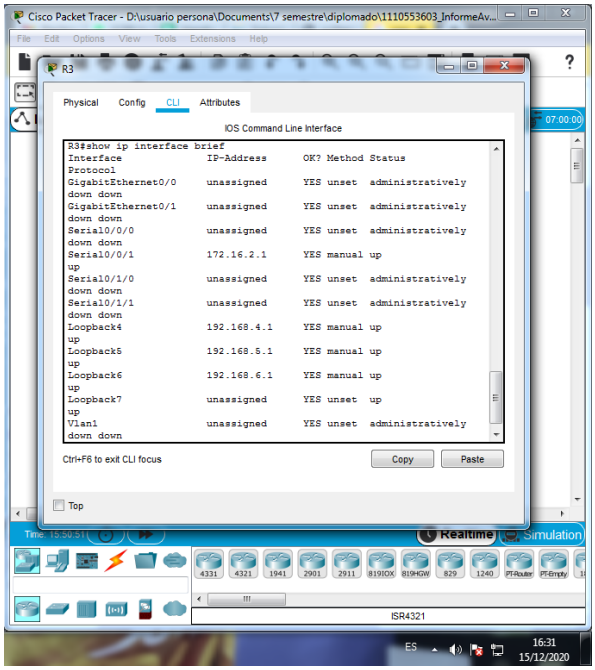
La siguiente tabla recopila el paso a paso de ejecución de comandos necesarios para la configuración del R3, se podrá observar la tarea realizada y los comandos utilizados.

Tabla 19.Configuracion R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router> Router>en Router#confi Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/Z. 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-line)#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 connection to R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:db8:acad:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config-if)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.

Interfaz loopback 5	R3(config-if)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#no shutdown Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	R3(config-if)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#no shutdown Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	R3(config-if)#int loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 S0/0/1

Figura 19. verificacion de interface en R3



Fuente: Autor.

Se comprueba que las interfaces configuradas en el R3 se encuentran activas.

2.3.5 Configurar S1

Se procede a ejecutar una serie de comandos pertinentes para la configuración del Switch nombrado S1.

Tabla 20. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#line console 0
Contraseña de acceso a la consola	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-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #se prohibe el acceso no autorizado#

2.3.6 Configurar el S3

Se procede a ejecutar una serie de comandos pertinentes para la configuración del Switch nombrado S3 el cual requiere de una configuración básica con asignación de contraseñas para ingreso.

Tabla 21.Configuración S3

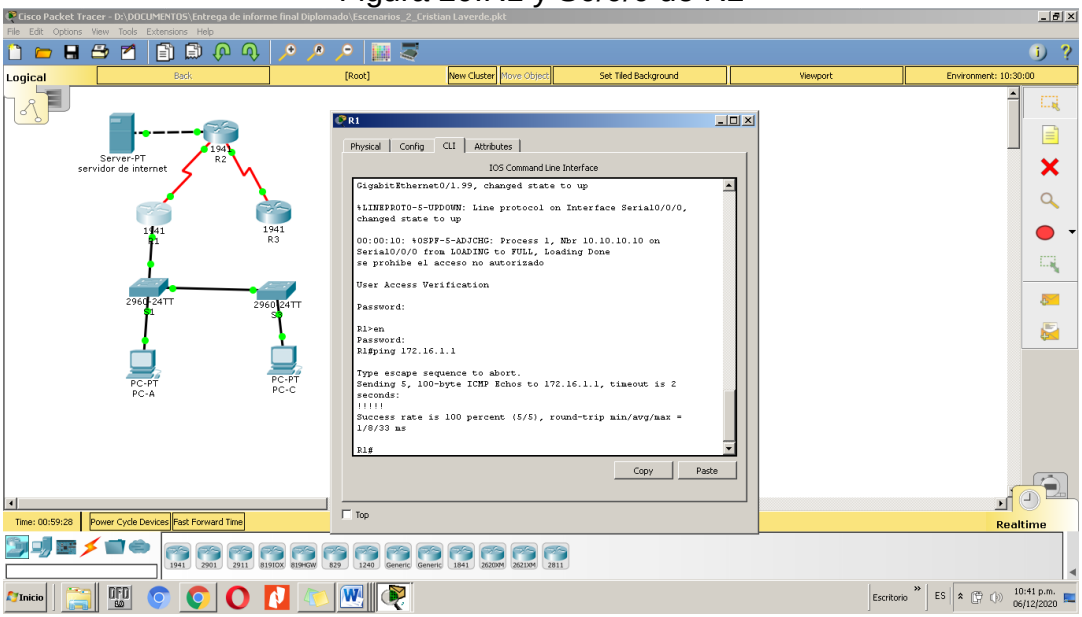
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class S3(config)#line console 0
Contraseña de acceso a la consola	S3(config-line)#password 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-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #se prohibe el acceso no autorizado#

2.3.7 Verificar la conectividad de la red

Se han venido realizando varios procesos de configuración en los dispositivos, es importante verificar que la conectividad de la red se encuentre como es requerido, para esto se verifica la conectividad por medio del comando de consola ping.

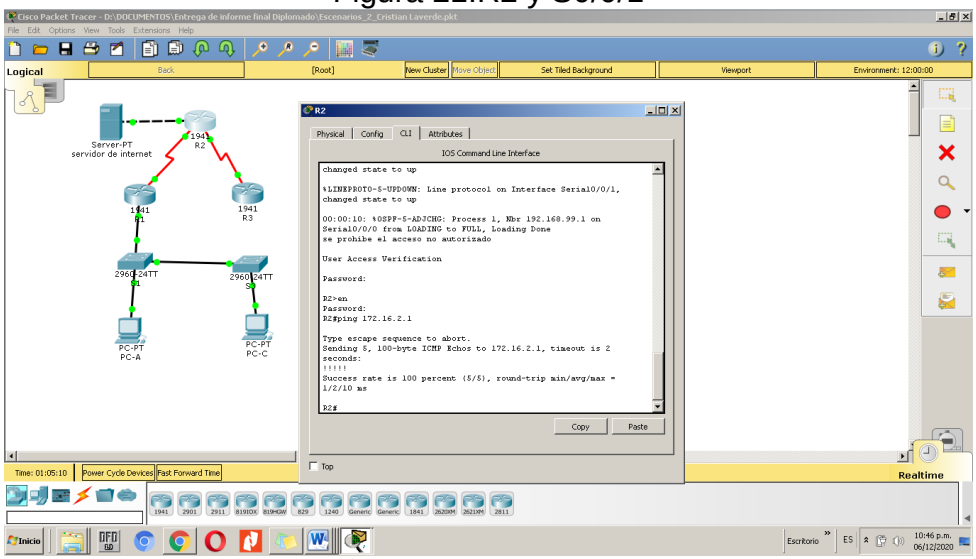
Figura 20.R1 y S0/0/0 de R2



Fuente: Autor

La conectividad de red entre R1 y S0/0/0 de R2 es satisfactoria.

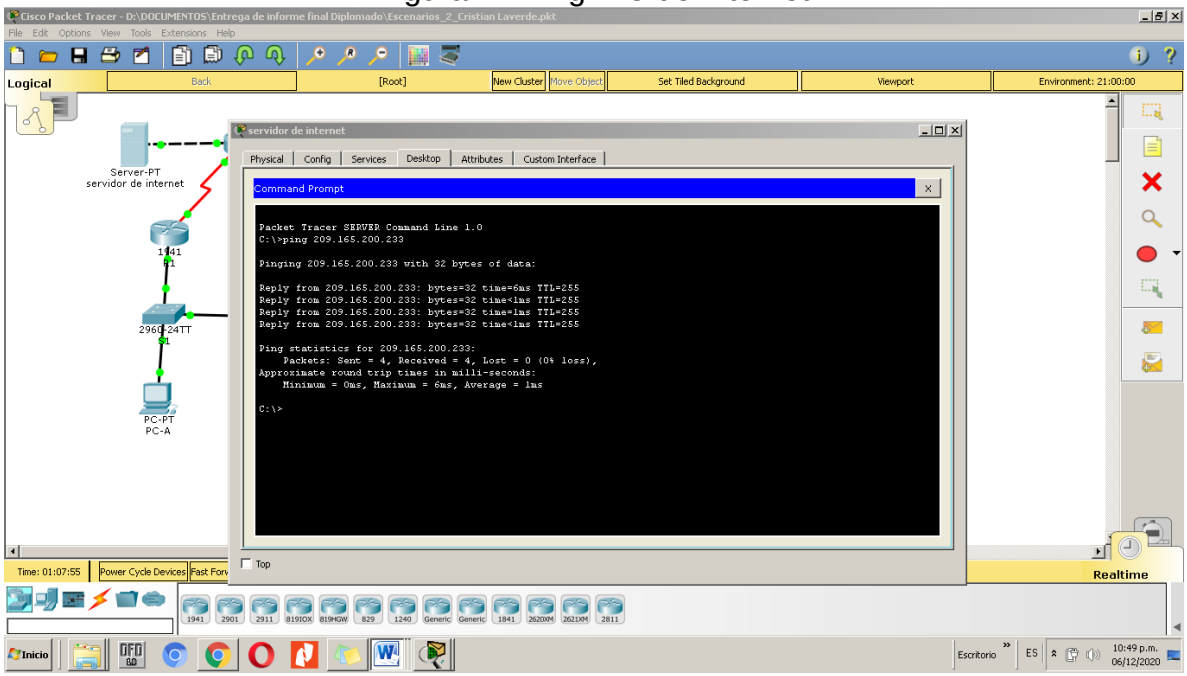
Figura 21.R2 y S0/0/1



Fuente: Autor

La conectividad de red entre R2 y S0/0/1 de R3 es satisfactoria.

Figura 22.Ping PC de Internet



Fuente: Autor

La conectividad de red entre PC de Internet y Gateway predeterminado con dirección ip 209.165.200.233 es satisfactoria.

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

2.4.1 Configurar S1

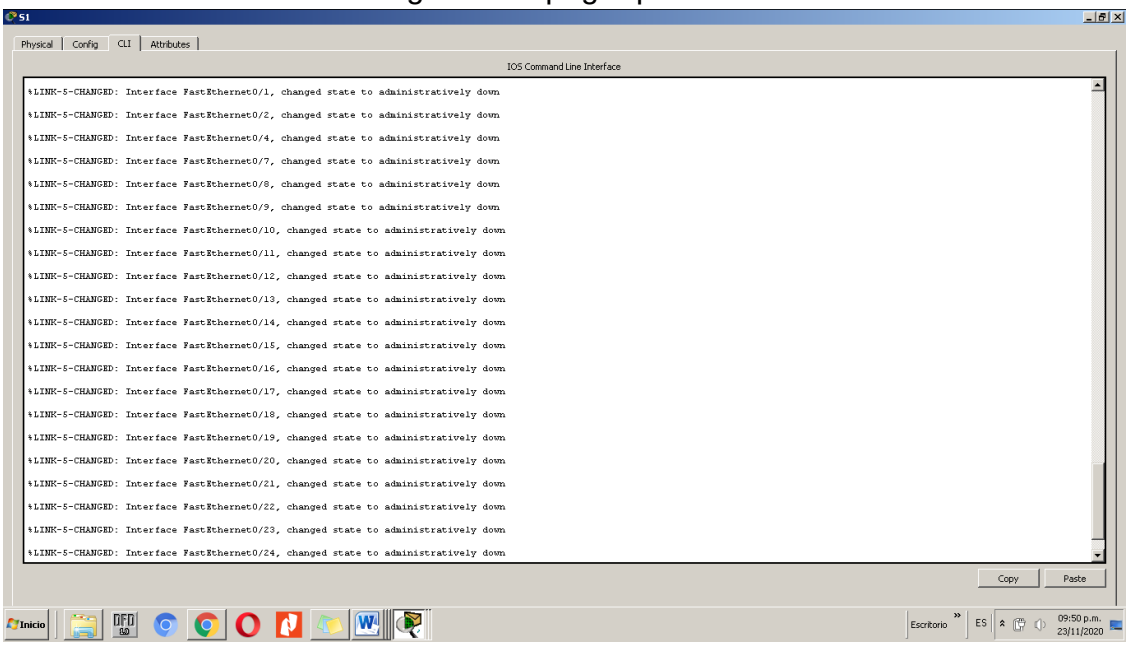
La presente tabla corresponde a la configuración que se realizó en el switch 1 nombrado S1, el cual tiene una configuración básica con seguridad de ingreso y la creación de las VLAN 21,223 y 99.

Tabla 22.Configuracion de seguridad S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1>en S1#config 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
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología. S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
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
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa S1(config)#int f0/3 S1(config-if)#switchport mode trunk

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range. S1(config)#int vlan1 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 23.Apagar puertos.



Fuente: Autor

Se utiliza el comando S1(config-if)#int range f0/1-2,f0/4,f0/7-24,g0/1-2 para a pagar los puertos que no están en uso.

2.4.2 Configurar el S3

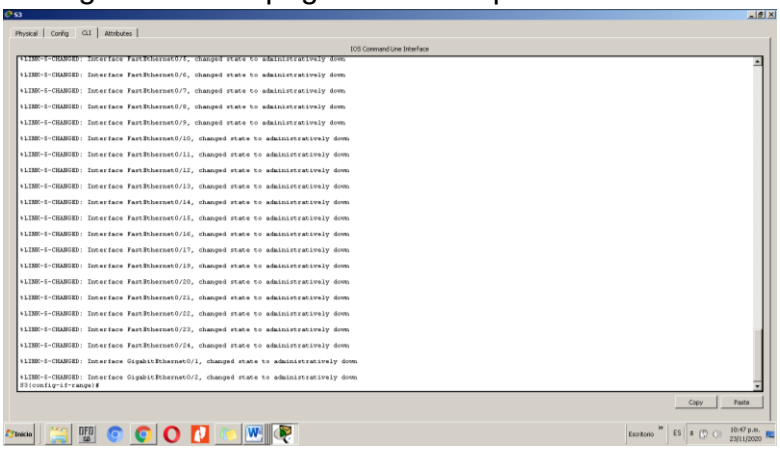
Se configura el switch S3, creando las VLAN correspondientes con las características requeridas para la red

Tabla 23.Configurar VLAN para S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	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)#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	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología. S3(config)#int vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa. S3(config)#int fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range. S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#int range fa0/1-2, fa0/4-24, g0/1-2
Asignar F0/18 a la VLAN 21	S3(config-if-range)#int f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar	S3(config-if)#int range fa0/1-2,fa0/4-17,fa0/19-24,g0/1-2 S3(config-if-range)#shutdown

Figura 24.S3 Apagar todos los puertos sin usar.



Fuente: Autor

Se utiliza el comando S3(config-if)#int range fa0/1-2,fa0/4-17,fa0/19-24,g0/1-2 para a pagar los puertos que no están en uso.

2.4.3 Configurar R1

A continuación verá reflejada la configuración de subinterfaz realizada para el Router1, según se especifica en la topología para este escenario.

Tabla 24.subinterfaz R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad, asignar la VLAN 21, asignar la primera dirección disponible a esta interfaz. R1(config)#int g0/1.21 R1(config-subif)#description 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	Descripción: LAN de Ingeniería Asignar la VLAN 23, asignar la primera dirección disponible a esta interfaz 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 Descripción: LAN de Ingeniería
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-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 R1(config-subif)#int g0/1 Descripción: LAN de Administración
Activar la interfaz G0/1	R1(config-if)#no shutdown

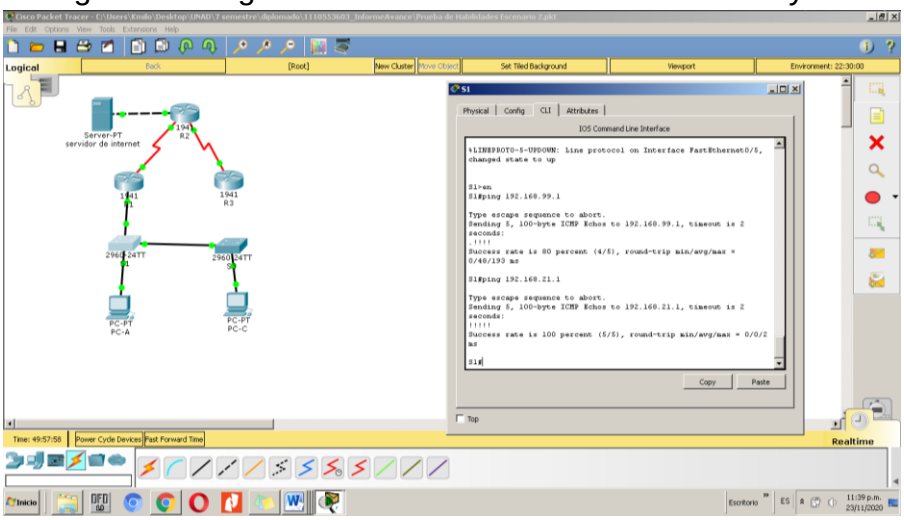
2.4.4 Verificar la conectividad de la red

La presente tabla resume las pruebas de conectividad entre las VLAN, desde los Switche S1 y S3.

Tabla 25.Conectividad de Red S1, S3.

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

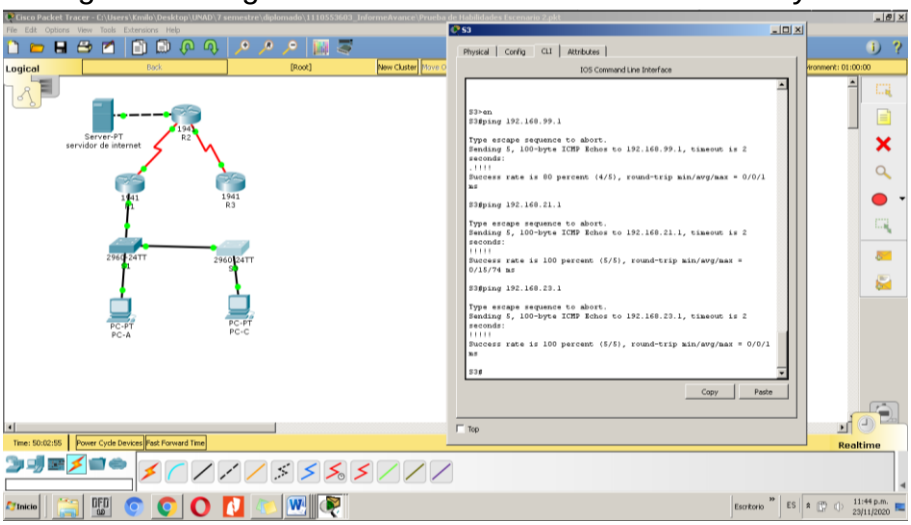
Figura 25.Ping desde S1 a R1 A dirección VLAN 99 y 21.



Fuente: Autor

Se verifica Conexión dando positiva para el Ping desde S1 a R1 A dirección VLAN 99 y 21.

Figura 26.Ping desde S3 a R1 A dirección VLAN 99 y 23.



Fuente: Autor

Se verifica Conexión dando positiva para el Ping desde S3 a R1 A dirección VLAN 99 y 23.

2.5 CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

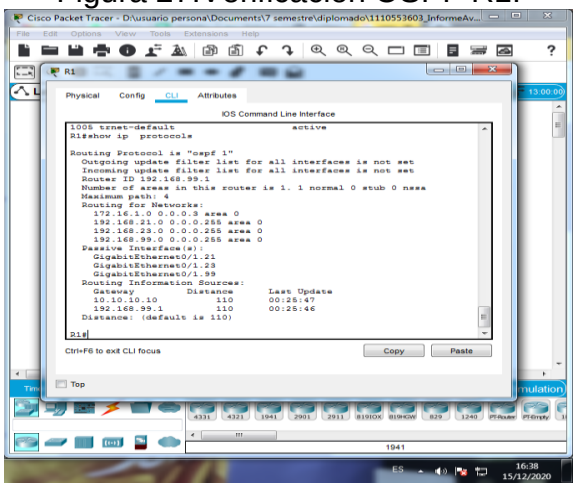
2.5.1 Configurar OSPF en el R1.

La siguiente tabla contiene la configuración para el R1 con el protocolo routing dinámico OSPF.

Tabla 26.Configuraciòn OSPF en el R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#router ospf 1 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 192.168.21.0 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

Figura 27.Verificacion OSPF R1.



Fuente : Autor.

Se verifica por medio del comando show ip protocols que el router R1 ya cuenta con la configuración OSPF.

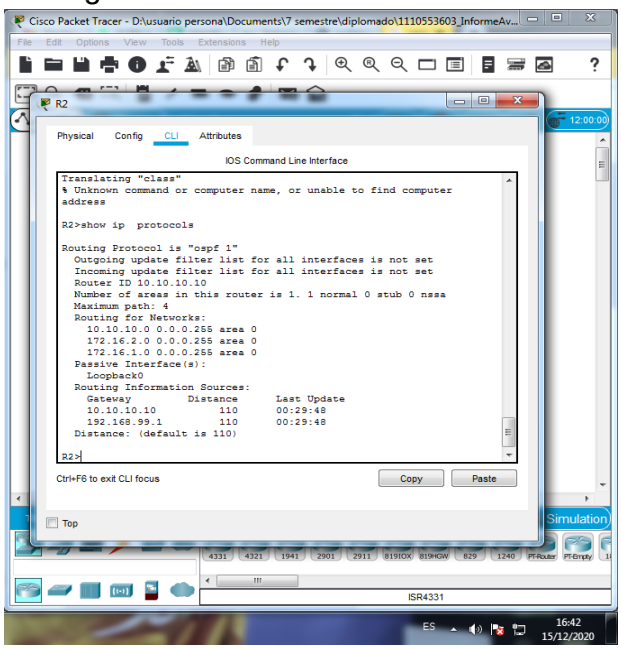
2.5.2 Configurar OSPF en el R2.

La siguiente tabla contiene la configuración para el R2 con el protocolo routing dinámico OSPF.

Tabla 27.Configuraciòn OSPF en el R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	Configurar OSPF área 0 R2(config)#router ospf 1 R2(config-router)#network 10.10.10.10 0.0.0.3 area 0
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config-router)#network 172.16.2.0 0.0.0.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Figura 28.Verificacion OSPF en R2.



Fuente: Autor

Se verifica por medio del comando show ip protocols que el router R2 ya cuenta con la configuración OSPF.

2.5.3 Configurar OSPFv3 en el R3.

La siguiente tabla contiene la configuración para el R3 con el protocolo routing dinámico OSPF.

Tabla 28.Configuraciòn OSPFv3 en el R3.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#ipv6 unicast-routing R3(config)#ipv6 router ospf 1 R3(config-rtr)#router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente	R3(config)#int s0/0/1 R3(config-if)#ipv6 ospf 1 area 0 R3(config-if)#int Loopback7 R3(config-if)#ipv6 ospf 1 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

2.5.4 Verificar la información de OSPF.

Unos comandos de consolas permiten observar la configuración que tenemos en los dispositivos, esto facilita su revisión en la siguiente tabla se relacionan esos comandos.

Tabla 29.Verificar OSPF.

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#show ip ospf interface 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 running-config

2.6 IMPLEMENTAR DHCP Y NAT PARA IPV4

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

Se procede a configurar el R1 para que cumpla las funciones de servidor DHCP para las VLAN 21 y 23.

Tabla 30.R1 Como servidor de DHCP

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-addres 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-addres 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)#ip dhcp pool ACCT Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#network 192.168.21.0 255.255.255.0
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(dhcp-config)#ip dhcp pool ENGNR Servidor DNS: 10.10.10.10 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1

2.6.2 Configurar la NAT estática y dinámica en el R2

Se procede a configurar el Router nombrado R2 con una serie de comandos ordenados en la siguiente tabla,necesarios para configurar NAT estática y dinámica.

Tabla 31.Configuraciòn NAT

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>en R2#conf R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server Este comando no es soportado por packet tracer Este comando no es soportado por packet tracer pero este sería el comando a utilizar en un router físico.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authetication local 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
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229

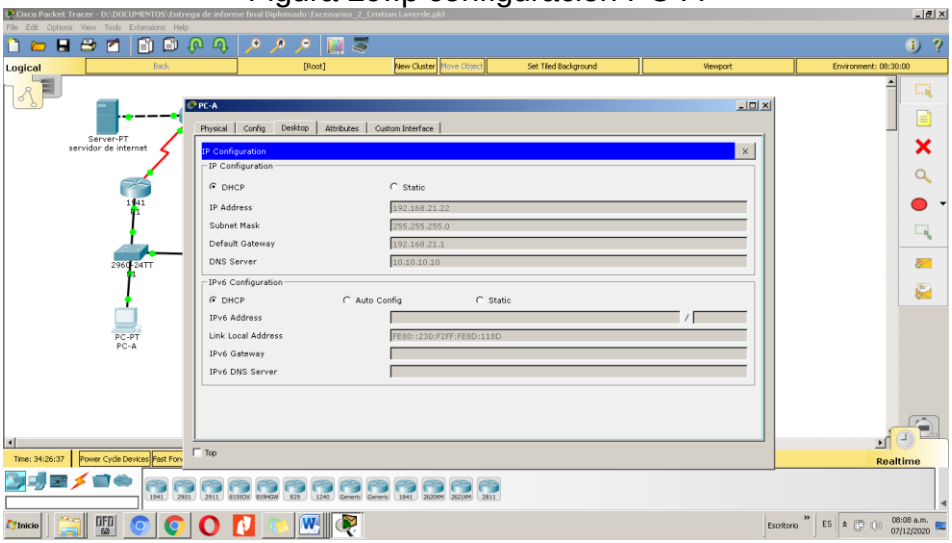
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 Asignar la interfaz interna y externa para la NAT estática R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/1 R2(config-if)#ip nat outside
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

2.6.3 Verificar el protocolo DHCP y la NAT estática

Se procede a verificar que las configuraciones previas del servidor DHCP y la NAT se hayan aplicado de manera correcta.

Verificar que la PC-A haya adquirido información de IP del servidor de DHCP.

Figura 29.Ip configuración PC-A

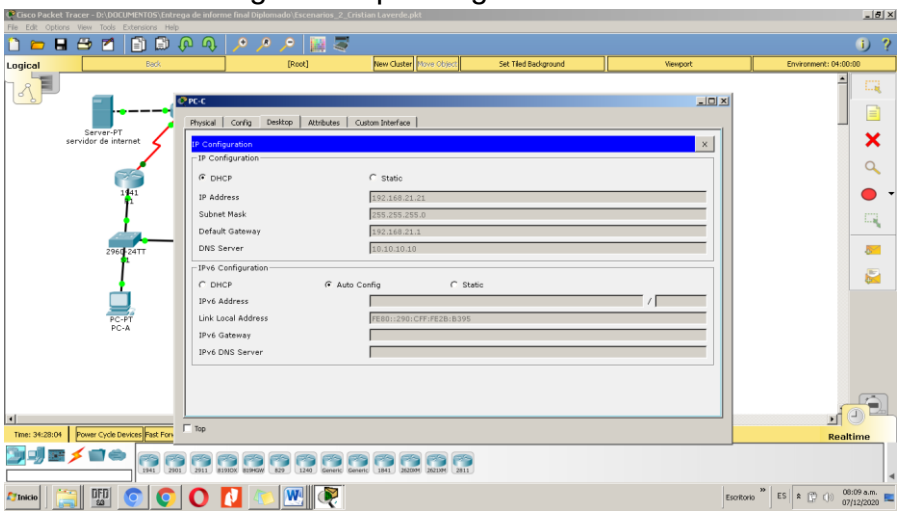


Fuente: Autor

Como se observa la PC-A cuenta con el direccionamiento DHCP.

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP.

Figura 30.Ip configuración PC-C

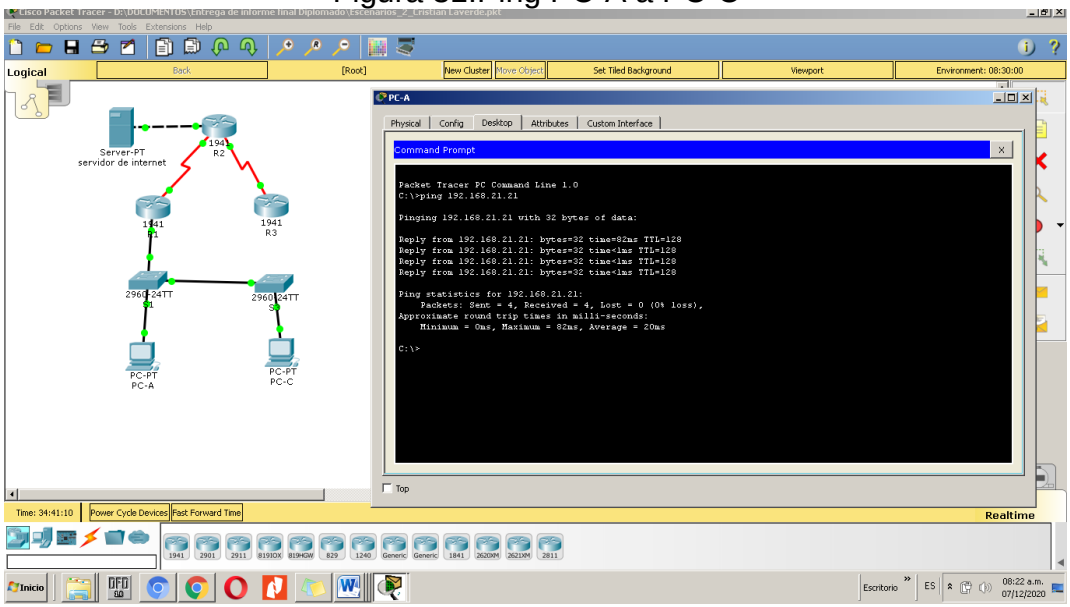


Fuente: Autor

La PC-C también adquirió el direccionamiento DHCP.

Verificar que la PC-A pueda hacer ping a la PC-C obteniendo un resultado positivo.

Figura 31.Ping PC-A a PC-C



Fuente: Autor

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

2.7 Configurar NTP

Se procede a configurar NTP para el router 2 con los comando que se mostraran en la Tabla 26.

Tabla 32. Configuración NTP en R2

Elemento o tarea de configuración	**Especificación**
Ajuste la fecha y hora en R2.	se ajusta el siguiente horario 5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 05 march 2016 5 de marzo de 2016, 9 a. m.
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5 Nivel de estrato: 5Tabla 12.Configurar NTP.
Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp server 209.165.200.229

Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R2#show ntp associations

2.8 Configurar y verificar las listas de control de acceso (ACL)

2.8.1 Restringir el acceso a las líneas VTY en el R2

Se procede a configurar la lista de acceso esto permitirá que solo el router 1 pueda establecer conexión Telnet con las líneas de VTY, todo el proceso realizado se puede ver en la Tabla 27.

Tabla 33. Restricción VTY en el R2

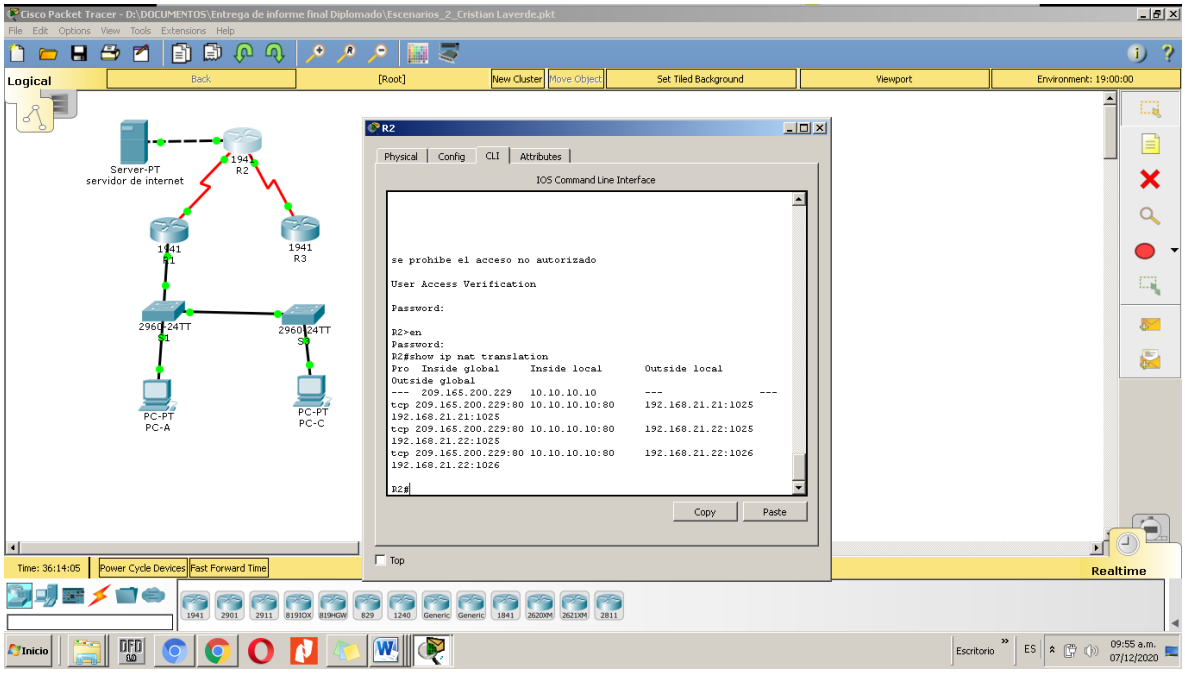
Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2
Aplicar la ACL con nombre a las líneas VTY	R2(config-line)#access-class ADMN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-clas ADMN-MGT in
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2

2.8.2 Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente.

Tabla 34.Comandos CLI.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2>en R2#show access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#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 statistics
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#show ip nat translation

Figura 32.R2#show ip nat translation



Fuente: Autor

Se observa las traducciones NAT que se encuentran activas en este momento.

CONCLUSIONES

Se concluye resaltando que la herramienta de simulación Cisco packet tracer facilito el montaje y configuración de los escenarios trabajados en este documento. Las dos redes requerían de la aplicación de protocolos específico y el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Fue importante conocer las especificaciones de los dispositivos para seleccionar los más indicados para la funcionalidad requerida por la red, Recordando que cada dispositivo fue diseñado para soportar características específicas y de esto depende su funcionalidad.

En ambos escenarios se realiza un enrutamiento entre VLAN que permitió la conexión entre las diferentes subredes y como característica de este tipo de enrutamiento mejora la seguridad y permite una configuración centralizada pero con diferentes dependencias como es requerido en entornos corporativos. La administración de direcciones ip se facilita con la activación de servidor DHCP, este realiza el proceso de asignación de direccionamiento IP de manera automático evitando la configuración manual. Es pertinente que se estén verificando constantemente la conectividad entre dispositivos con el fin de garantizar un buen funcionamiento de la red.

El escenario 2 requirió de una configuración más compleja por los requisitos de esta como lo es la traducción de direcciones de red dinámicas y estáticas (NAT) que permitió que los host internos compartieran una única dirección IPv4 pública para todas las comunicaciones externas. Creación de ACL que resulta ser muy beneficiosa por limitar el tráfico y mejorar el rendimiento de la red.

BIBLIOGRAFIA

Guía de Referencia de Comandos de Cisco Unity Express. (2020, 18 agosto). Cisco. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity_exp/command/reference/guide/CUECmdReference/e_cmds.html

HTTPS--HTTP Server and Client with SSL 3.0. (2020, 30 septiembre). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/xe-17/https-xe-17-book/HTTPS--HTTP_Server_and_Client_with_SSL_3-0.html?dtid=osscdc000283

CCNA: Introduction to Networks. (2020, 1 julio). Networking Academy. https://www.netacad.com/es/courses/networking/ccna-introduction-networks

Cisco Packet Tracer. (2020, 8 mayo). Networking Academy. https://www.netacad.com/es/courses/packet-tracer

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

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

CISCO. (2019). División de redesIP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

Configuring the Cisco IOS DHCP Server. (2015, 8 diciembre). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3se/3850/dhcp-xe-3se-3850-book/config-dhcp-server.html?dtid=osscdc000283

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei- NT1IlnWR0hoMxgBNv1CJ

IPv6 Routing: OSPFv3. (2017, 12 julio). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-1sg/ip6-route-ospfv3.html?dtid=osscdc000283

Network Address Translation (NAT) FAQ. (2020, 18 noviembre). Cisco. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html?dtid=osscdc000283#gen-nat

Open Shortest Path First (OSPF). (2020, 23 octubre). Cisco. https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-ospf.html?dtid=osscdc000283

SunilKhanna. (2020, 17 agosto). 802.1q. Cisco Community. https://community.cisco.com/t5/networking-documents/802-1q/ta-p/3113232?dtid=osscdc000283

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches. (2020, 15 mayo). Cisco. https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html?dtid=osscdc000283

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

Virtual LANs/VLAN Trunking Protocol (VLANs/VTP). (2017, 1 marzo). Cisco. https://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html

ANEXOS

ANEXO 1

Enlaces de descargar archivo Packet tracer de simulación del escenario 1.
https://drive.google.com/file/d/1AGXKbBd9WgCsnyOdjwdwMGY7sZD0SS8j/view?usp=sharing

ANEXO 2

Enlaces de descargar archivo Packet tracer de simulación del escenario 2.
https://drive.google.com/file/d/1HnV2C3g5TqflXmBZgMRfZpJ-krvI-4wM/view?usp=sharing

ANEXO 3

Enlaces de descargar Artículo Científico IEEE
https://drive.google.com/file/d/1Dl4YWQcLBF4idDXLfGlZxI6OlO7KctyT/view?usp=sharing

Solución de dos estudios de caso bajo el uso de tecnología CISCO

Cristian Camilo Laverde Ladino
Universidad Nacional Abierta y a Distancia UNAD, cclaverdel@unadvirtual.edu.co

Resumen

Simulación y documentación de dos escenarios con características especiales de configuración, necesarias para el funcionamiento y requerimiento para la solución de problemáticas reales en entornos corporativos utilizando tecnología cisco.
Un primer escenario compuesto por una red pequeña la cual es configurada para que los dispositivos que la conforman puedan recibir conectividad IPv4 y IPv6, configuración de enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Segundo escenario compuesto por una red pequeña la cual es configurada para que los dispositivos que la conforman puedan recibir conectividad IPv4 y IPv6, siguiendo protocolos de configuración OSPF, DHCP, NTP.
La configuración realizada esta sustentada por medio de imágenes tomadas de la ejecución de comando Ping y show que reflejan la conectividad entre dispositivos y su configuración.

Palabras clave: Cisco, IPv4, IPv6, Networking, Topología, VLAN.

Abstract:

Simulation and documentation of two scenarios with special configuration characteristics, necessary for the operation and requirement for the solution of real problems in corporate environments using Cisco technology.
A first scenario composed of a small network which is configured so that the devices that make it up can receive IPv4 and IPv6 connectivity, routing configuration between VLAN, DHCP, Etherchannel and port-security. Second scenario composed of a small network which is configured so that the devices that make it up can receive IPv4 and IPv6 connectivity, following OSPF, DHCP, NTP configuration protocols.
The configuration carried out is supported by images taken from the execution of the Ping and show command that reflect the connectivity between devices and their configuration.

Keywords: Cisco, IPv4, IPv6, Networking, Topology, VLAN.

I. INTRODUCCIÓN

Solución de dos estudios de caso bajo el uso de tecnología CISCO como Prueba de habilidades prácticas, es una de las actividades que agrupan el diplomado de profundización [1] CCNA, esta tiene como objetivo poner en práctica los conceptos aprendidos durante el desarrollo de este diplomado, utilizando la herramienta [2] cisco packet tracer, se desarrollan simulaciones buscando establecer escenario LAN/WAN que permitan analizar comportamientos de diversos protocolos y métricas de enrutamiento para brindar soluciones a problemáticas presentes en entornos corporativos.

Dos escenarios propuestos a los cuales se darán solución acorde a los lineamientos establecidos y se documentara todo su desarrollo como evidencia sustentado con imágenes y comandos de ejecución.

Primer escenario configura los dispositivos de una red pequeña, conformada por: un router, dos swich y dos PC, estos configurados con un enrutamiento [3] VLAN, DHCP, Etherchannel y port-security.

Segundo escenario consiste en 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 [4] (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.

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

Simulación y documentación de dos escenarios con características especiales de configuración, necesarias para el funcionamiento y requerimiento para la solución de problemáticas reales en entornos corporativos utilizando tecnología cisco.

III. ESCENARIO 2

Imagen1.Topología Escenario 2

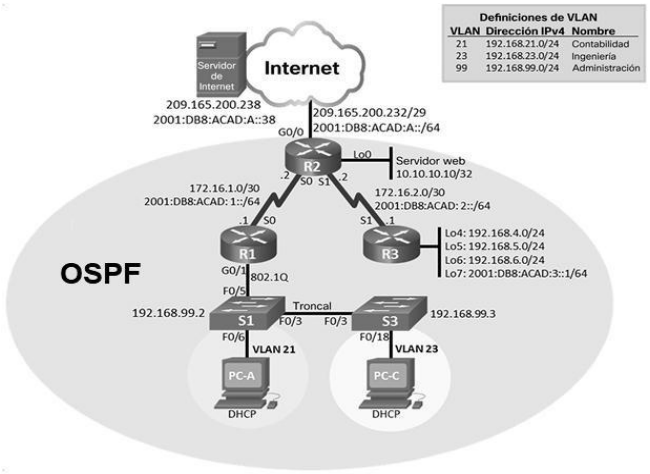


Tabla 1. Dispositivos

Server-PT	Servidor de internet
Router 1941	R1
Router 1941	R2
Router 1941	R3
Switche 2960-24TT	S1
Switche 2960-24TT	S3
PC-PT	PC-A
PC-PT	PC-C

A. Inicializar dispositivos

Es necesario antes de iniciar la configuración de un dispositivo borrar las configuración anterior esto para evitar posibles configuraciones innecesarias o que puedan interferir en las nuevo servicio que va realizar, para eso se utiliza el comando [5] erase startup-config en el modo EXEC y luego se procede a reiniciar el dispositivo.

Tabla 2. Borrar configuración

Tarea	Comandos
Iniciar modo privilegiado	Router>enable
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config
Recargar el dispositivo	Router#reload

B. Configurar los parámetros básicos de los dispositivos

Se procede asignar el correspondiente direccionamiento a los dispositivos y se configura de tal manera que sea segura su administración con asignación de contraseñas para su configuración, algunos dispositivos requieren que sea habilitado el servidor [6]HTTP con el fin que los datos enviados y recibidos de un servidor HTTP se cifren antes de enviarse a través de Internet.

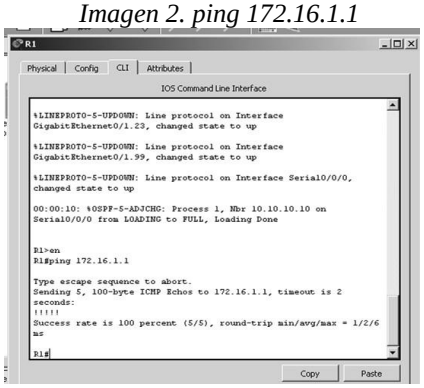
Tabla 3 1.Configuración R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router#confi 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 con 0 R1(config-line)#pass cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#pass 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#

C. Verificar la conectividad de la red.

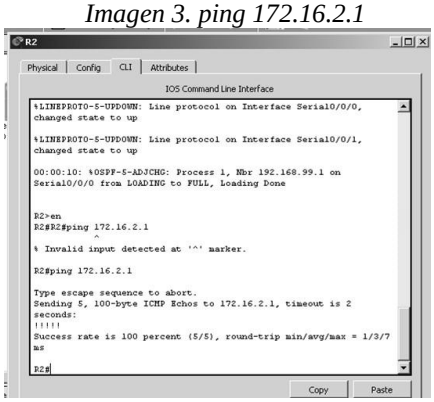
Previo a la configuración de cada dispositivo incluyendo la asignación de direccionamiento y conectividad entre ellas, procedemos a verificar que sea posible la comunicación de la red para esto se utiliza el comando ping.

Imagen 2. ping 172.16.1.1



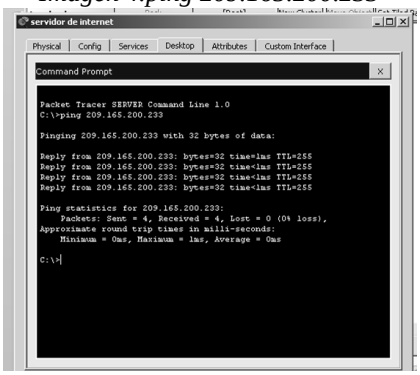
Se observa positiva conexión entre R1 y R2, S0/0/0.

Imagen 3. ping 172.16.2.1



Se observa positiva la conexión entre el R2 y R3, S0/0/1.

Imagen 4.ping 209.165.200.233



Se confirma conexión entre el servidor web y Gateway predeterminado.

D. Configurar la seguridad del switch, las VLAN y el routing entre VLAN.

Esta etapa es muy importante de ella se basa la comunicación de toda la red y su distribución interna, se debe hacer la creación de las VLAN y el direccionamiento y puntos de acceso, este proceso se realiza en el S1 y S3.

Tabla 4.Creacion de VLAN

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1>en S1#config 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

E. Configurar R1

Este router recibe una configuración de protocolo [7]802.1q el cual define el funcionamiento de los puentes VLAN que permiten la definición, operación y administración de topologías de LAN virtuales dentro de una infraestructura de LAN puenteada.

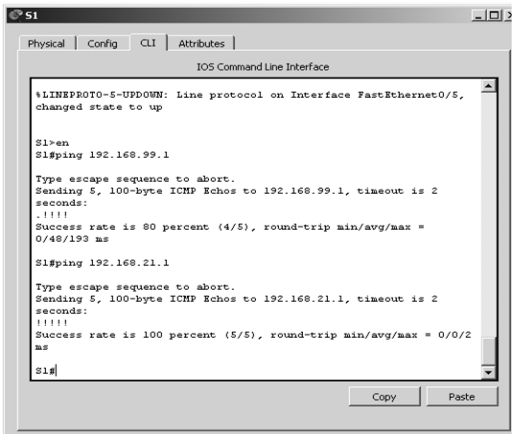
Tabla 5.subinterfaz R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad, asignar la VLAN 21, asignar la primera dirección disponible a esta interfaz. R1(config)#int g0/1.21 R1(config-subif)#description 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	Descripción: LAN de Ingeniería Asignar la VLAN 23, asignar la primera dirección disponible a esta interfaz 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 Descripción: LAN de Ingeniería

F. Verificar la conectividad de la red

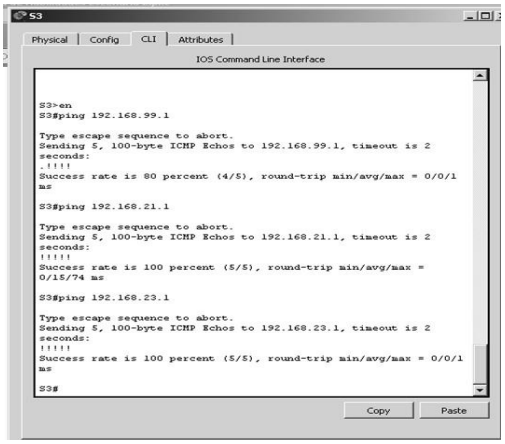
Es necesario comprobar que la conectividad de red entre R! y los switch sea exitosa, para garantizar esto se procede hacer a utilizar el comando ping.

Imagen5.Ping desde S1 a R1 A dirección VLAN 99 y 21.



Se verifica Conexión dando positiva para el Ping desde S1 a R1 A dirección VLAN 99 y 21.

Imagen 6.Ping desde S3 a R1 A dirección VLAN 99 y 23



Se verifica Conexión dando positiva para el Ping desde S3 a R1 A dirección VLAN 99 y 23.

G. Configurar OSPF en el R1 y R2.

Para la configuración del Router 1 y 2, se procede asignar el protocolo [8]OSPF, los enrutadores OSPF envían información sobre el estado del enlace a los enrutadores vecinos para que todos los enrutadores en un área tengan una vista completa de la topología de la red.

Tabla 5.Configuraciòn OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 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 192.168.21.0 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

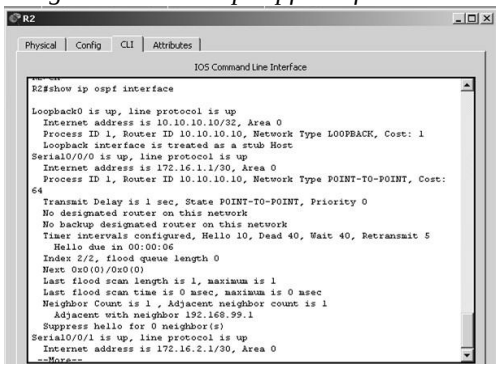
H. Configurar OSPFv3 en el R3.

El Router 3 deberá ser configurado bajo el protocolo [9]OSPFv3 enrutamiento de estado de enlace IPv4 e IPv6 que admite familias de direcciones de unidifusión (AF) IPv6 e IPv4.

I. Verificar la información de OSPF.

Se procede a verificar que la configuración anterior del protocolo OSPF esté funcionando como es requerido para eso se observa por medio de comandos de consola SHOW.

Imagen 7. R2#show ip ospf interface



Se puede observar la id del proceso OSPF y las interface pasivas configuradas en el roter.

J. Implementar DHCP y NAT para IPv4

El R1 se debe configurar como servidor de DHCP para las VLAN 1 y 23, con un reservado de direcciones ip y se crea el pool DHCP para las VLAN.

K. Configurar la NAT estática y dinámica en el R2.

[4] NAT solo requiere una única dirección IP para representar un grupo completo de computadoras a cualquier cosa fuera de su red. Para esto es debido crear una base de datos local, habilitar el servicio del servidor HTTP.

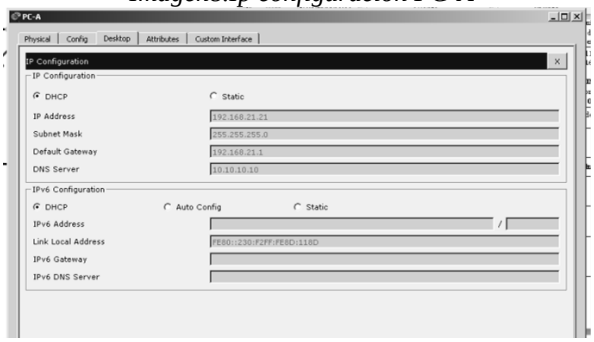
Tabla 6.Configuraciòn NAT

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>en R2#conf R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	R2(config)#ip http server Este comando no es soportado por packet tracer Este comando no es soportado por packet tracer pero este sería el comando a utilizar en un router físico.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#ip http authetication local 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

L. Verificar el protocolo DHCP y la NAT estática

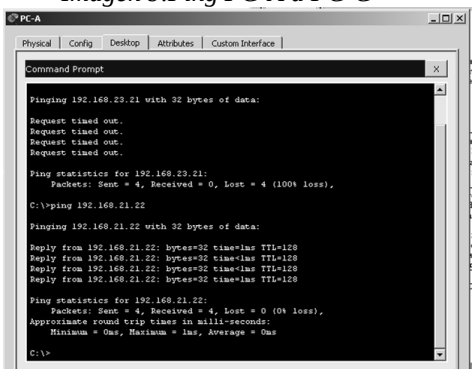
Se comprueba que los pc cuenten con la información ip del servidor DHCP y que entre ellas puedan hacer ping.

Imagen8.Ip configuración PC-A



Podemos observar que los PC ya cuentan con el direccionamiento DHCP.

Imagen 9.Ping PC-A a PC-C



De manera satisfactoria podemos observar el ping en tre las PC, grantizando la buena conectividad en la red.

IV. Conclusiones

Se concluye resaltando que la herramienta de simulación Cisco packet tracer facilito el montaje y configuración de los escenarios trabajados en este documento. Las dos redes requerían de la aplicación de protocolos específico y el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Fue importante conocer las especificaciones de los dispositivos para seleccionar los más indicados para la funcionalidad requerida por la red, Recordando que cada dispositivo fue diseñado para soportar características específicas y de esto depende su funcionalidad.

En ambos escenarios se realiza un enrutamiento entre VLAN que permitió la conexión entre las diferentes subredes y como característica de este tipo de enrutamiento mejora la seguridad y permite una configuración centralizada pero con diferentes dependencias como es requerido en entornos corporativos. La administración de direcciones ip se facilita con la activación de servidor DHCP, este realiza el proceso de asignación de direccionamiento IP de manera automático evitando la configuración manual. Es pertinente que se estén verificando constantemente la conectividad entre dispositivos con el fin de garantizar un buen funcionamiento de la red.

El escenario 2 requirió de una configuración más compleja por los requisitos de esta como lo es la traducción de direcciones de red dinámicas y estáticas (NAT) que permitió que los host internos compartieran una única dirección IPv4 pública para todas las comunicaciones externas. Creación de ACL que resulta ser muy beneficiosa por limitar el tráfico y mejorar el rendimiento de la red.

V. Referencias

[1] CCNA: Introduction to Networks. (2020, 1 julio). Networking Academy. https://www.netacad.com/es/courses/networking/ccna-introduction-networks

[2] Cisco Packet Tracer. (2020, 8 mayo). Networking Academy. https://www.netacad.com/es/courses/packet-tracer

[3] Virtual LANs/VLAN Trunking Protocol (VLANs/VTP). (2017, 1 marzo). Cisco. https://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html

[4] Network Address Translation (NAT) FAQ. (2020, 18 noviembre). Cisco. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html?dtid=osscdc000283#gen-nat

[5] Guía de Referencia de Comandos de Cisco Unity Express. (2020, 18 agosto). Cisco. https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/unity_exp/command/reference/guide/CUECmdReference/e_cmds.html

[6] HTTPS--HTTP Server and Client with SSL 3.0. (2020, 30 septiembre). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/xe-17/https-xe-17-book/HTTPS--HTTP_Server_and_Client_with_SSL_3-0.html?dtid=osscdc000283

[7] SunilKhanna. (2020, 17 agosto). 802.1q. Cisco Community. https://community.cisco.com/t5/networking-documents/802-1q/ta-p/3113232?dtid=osscdc000283

[8] Open Shortest Path First (OSPF). (2020, 23 octubre). Cisco. https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-ospf.html?dtid=osscdc000283

[9] IPv6 Routing: OSPFv3. (2017, 12 julio). Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-1sg/ip6-route-ospfv3.html?dtid=osscdc000283

Biografía

Cristian C. Laverde Ladino Nació en Ibagué – Tolima en la República de Colombia, el 29 de Noviembre de 1994. Se graduó de Tecnólogo de Análisis y Desarrollo de Sistemas de Información del Servicio Nacional de Aprendizaje (SENA), y estudia Ingeniería de sistemas en la Universidad Nacional Abierta y a Distancia. Su experiencia profesional incluye la Universidad de Ibagué como programador de plataforma Moodle, La Gobernación del Tolima como capacitador TIC, Entrenador de la selección Tolima de tenis de mesa para personas en condición de discapacidad. Sus áreas de interés incluyen, entre otras, la biomecánica.