SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

EDGAR ORLANDO ALFONSO ACOSTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2020

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

EDGAR ORLANDO ALFONSO ACOSTA

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

DIRECTOR

Ing. JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, 24 de Noviembre de 2020

AGRADECIMIENTOS

Mi Trabajo de gradado está ligado a la oportunidad que Dios me ha dado de vivir y ser una persona de bien, adicionalmente a mi padre que ya fallecido y no alcanzo a verme como un profesional titulado, a mi familia que tanto he abandonado por cumplir con mis actividades curriculares, esta carrera ha sido de muchos años de sacrificios familiares y económicos, pero con una satisfacción de haber cumplido a cabalidad los escenarios propuestos, quiero finalmente agradecer al personal de docentes de esta institución, que me han brindado un apoyo importante mediante las asesorías y acompañamiento académico que me han brindado durante el tiempo de aprendizaje para poder lograr los retos de adquirir conocimiento y convertirme en un buen profesional, entendí y comprendí que los retos son la clave para persistir a largo plazo las metas que uno se propone.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Packet Tracer:

Programa de simulación de redes que nos permite como estudiantes experimentar el comportamiento de las redes.

Enrutamiento Estático:

En el enrutamiento estático nos permite dar solución a las redes pequeñas, toda vez que nos brinda seguridad y es bastante económico porque no consume ancho de banda y es fácil de configurar.

Router> enable:

Nos permite hacer un cambio en una configuración a modo privilegiado

show runnin-config:

Comando necesario para permitir observar la configuración activa de routers, switches, access points, firewalls.

no shutdown

Con este comando nos permite activar una interfaz física o lógica.

RESUMEN

En este Diplomado correspondiente a la solución de dos estudios de caso bajo el uso de tecnología CISCO, nos brindara una herramienta de aprendizaje fundamental para adquirir habilidades a nivel profesional, como es la herramienta Packet Tracer, el conocimiento ingresa por medio del aprendizaje y la práctica, con los ejercicios de los escenarios aprendimos a realizar enrutamientos para configurar los equipos de una red local o Lan, a su vez generar una conmutación en ellos, donde podemos hacer entrega de paquetes o mensajes que nos garantice tanto los envíos como las recepciones de los mismos, esto no solo a nivel de comunicaciones sino a nivel de electrónica donde necesitamos que los sistemas binarios trabajen de la mano con la programación asignada a los escenarios propuestos.

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

ABSTRACT

In this Diploma corresponding to the solution of two case studies under the use of CISCO technology, it will provide us with a fundamental learning tool to acquire skills at a professional level, such as the Packet Tracer tool, knowledge enters through learning and practice , with the exercises of the scenarios we learned to carry out routing to configure the equipment of a local or Lan network, in turn generate a switch in them where we can deliver packages or messages that guarantee both the shipments and the receptions of them This not only at the communications level but also at the electronics level where we need binary systems to work hand in hand with the programming assigned to the proposed scenarios.

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

INTRODUCCION

En el presente Diplomado veremos el desarrollo del trabajo individual como opción de grado, donde observaran dos escenarios de prácticas con el objetivo de demostrar los conocimientos adquiridos bajo la modalidad de aprendizaje a distancia en la Universidad Abierta y a Distancia Unad.

En el primer escenario veremos la configuración de los dispositivos de una red que tiene cinco elementos, pero con la complejidad de configurar un router, un switch y dos equipos PC, veremos cómo se aplica la conectividad con IPv4 y la conectividad con IPv6 para los dos PC, posteriormente veremos la configuración del router y el switch los cuales debemos configurar de forma segura. Por último, en esta actividad veremos la configuración del enrutamiento entre VLAN, DHCP, Etherchannel y port-security con las respectivas evidencias de imagen.

En el segundo escenario veremos la configuración de los dispositivos de una red que tiene ocho elementos, con la complejidad de configurar tres router, dos switch, dos equipos PC y un servidor de internet, la finalidad de este escenario es realizar una práctica adecuada para inicializar los dispositivos routers y los switches, todo esto para evitar cualquier configuración adicional que no esté enfocada con la práctica, posteriormente veremos la configuración del servidor de internet y R1 con las tareas necesarias para cumplir la actividad, pasamos a R2 y R3 para aplicar las configuraciones adicionales finales y así ajustar las tareas para la red, importante paso para comenzar con la configuración de los S1 y S3 donde practicaremos la configuración como son búsqueda DNS, crear contraseñas, conectividad de las interfaces, creación de Vlans y finalizaremos con las pruebas de ping a fin de verificar la demostración de conectividad.

DESARROLLO

ESCENARIO 1
TOPOLOGÍA

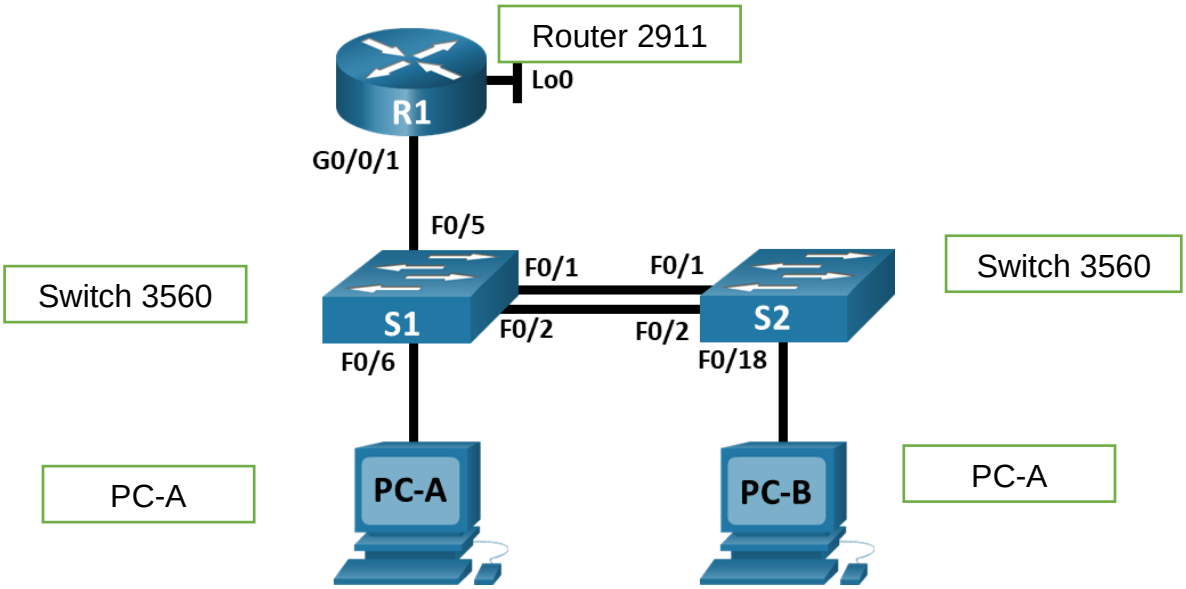
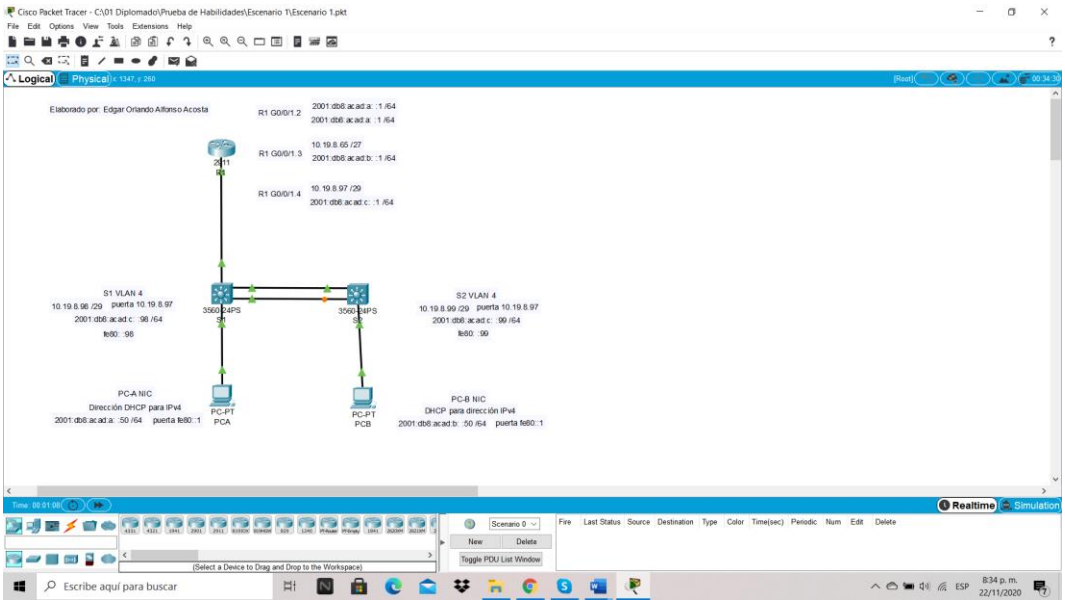


Figura 1. Montaje en Packet Tracer escenario 1



Fuente: Autor.

Iniciamos con el montaje de los equipos en Packet Tracer del escenario 1 con el fin de proseguir con las configuraciones planteadas.

Tabla 1. Vlan para configurar los equipos

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

Tabla 2. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
PC-B NIC	DHCP para dirección IPv4 2001:db8:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

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

PARTE 1. INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BASICOS DE LOS DISPOSITIVOS

PASO 1: INICIALIZAR Y VOLVER A CARGAR EL ROUTER Y EL SWITCH

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

Para este procedimiento entramos al rauter (R1) y los dos switch (S1 y S2) con el fin de hacer el borrado de las configuraciones que puedan tener.
Para este proceso es fundamental hacer borrando de las configuraciones que puedan tener tanto el router y los switch, es un paso recomendable para iniciar cualquier configuración, es posible que al verificar no haya nada configurado, pero la prevención es lo primero y así evitamos cualquier inconveniente para implementar una red.

Estos son los comandos necesarios por utilizar para proseguir e inicializar y volver a cargar los router y los switch.

Tabla 3. Resumen comandos de inicialización y carga R1 S1 y S2.

Descripción	Comando
Entrar al R1 y switch 1 y 2.	enable
En modo privilegiado	erase startup-config
¡Borrar el sistema de archivos nvram eliminará todos los archivos de configuración! ¿Seguir?	Dar clip en enter
Este comando es utilizado para reiniciar el dispositivo	reload

Descripción	Comando
¿Continuar con la recarga?	Dar clip en enter
¿Quieres entrar en el diálogo de configuración inicial? [sí / no]: confirmar	Escribir NO

Fuente: Autor.

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

PASO 2: CONFIGURAR R1
A continuación, daré una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 3 para R1.

Como todo proceso al ingresar a R1 primero nos asigna la actividad desactivar la búsqueda DNS, con el fin de desactivar la traducción de nombres a dirección del dispositivo R1, posteriormente debemos como colocar el nombre R1, tengamos en cuenta que ese por defecto viene el nombre “Router”, luego nos asigna colocar el nombre de dominio para configurar el servidor DNS, por esto, es necesario restringir el ingreso a personal no autorizado y veremos los comandos para colocar la contraseña cifrada para el modo EXEC privilegiado y la contraseña de acceso a la consola. Con todo esto es necesario establecer la longitud mínima para las contraseñas ya que es una opción importante para asegurar las contraseñas complejas con una longitud mínima lo cual ya asegura el R1 de esta actividad. Adicionalmente es importante crear un usuario administrativo en la base de datos local para el modo de configuración de línea de la consola, siempre vemos un número que es cero y este según la investigación se utiliza para representar la primera interfaz de consola, con esto pasamos a configurar el inicio de sesión en las líneas VTY para que use la base de datos local y la configuración de VTY solo aceptando SSH, ya finalizando daremos algunos comandos para cifrar las contraseñas de texto no cifrado, habilitaremos el routing IPv6 y finalmente veremos los comandos para configurar la interfaz G0/0/1 y subinterfaces, el Loopback0 interface y por ultimo vamos a generar una clave de cifrado RSA.

Tabla 4. Configuración R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	R1 R1>enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#hostname R1 R1(config)#
Nombre de dominio	ccna-lab.com R1#enable R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name ccna-lab.com R1(config)#
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass R1(config)#enable secret ciscoenpass R1(config)#do wr R1(config)#do reload
Contraseña cifrada para el modo EXEC privilegiado	Se asigna contraseña cifrada con el comando enable secret ciscoenpass y grabamos con el comando do wr
Contraseña de acceso a la consola	ciscoconpass R1>enable Password: R1# R1#configure terminal R1(config)#line consola 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#exit

Tarea	Especificación
Establecer la longitud mínima para las contraseñas	10 caracteres R1(config)# R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** R1(config)#username admin password admin1pass R1(config)# line console 0 R1(config)# login local R1(config)# exit Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config-line)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd # Router1 Escenario 1#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	**Establezca la descripción** R1(config)#int g0/1 **Establece la dirección IPv4.** R1(config-subif)#description Vlan 2 R1(config-subif)#ip address 10.19.8.1 255.255.255.192 **Establezca la dirección local de enlace IPv6 como fe80: :1** R1(config-subif)#ipv6 address fe80::1 link-local **Establece la dirección IPv6.** R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	**Activar la interfaz.** R1(config-if)#no shutdown Siguiente paso: Repetimos lo mismo para las demás subinterface R1(config-subif)#interface g0/1.3 R1(config-subif)#description Vlan 3 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)#no shutdown R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#no shutdown R1(config-subif)#interface g0/1.4 R1(config-subif)# R1(config)#interface g0/1.4 R1(config-subif)#description Vlan 4 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 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#no shutdown R1(config-subif)#.
Configure el Loopback0 interface	**Establezca la descripción** Se rescribe en siguiente comando R1(config-if)#description loopback 0 **Establece la dirección IPv4.** Se escribe en siguiente comando R1(config-if)#ip address 209.165.201.1 255.255.255.224 **Establece la dirección IPv6.** Se escribe en siguiente comando R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
Configure el Loopback0 interface	**Establezca la dirección local de enlace IPv6 como fe80::1** Se rescribe en siguiente comando R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#no shutdown

PASO 3: CONFIGURE S1 Y S2.
Veremos una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 4 para S1 y S2.

Los pasos son similares al realizado en R1 pues es necesario desactivar la búsqueda DNS en los S1 y S2 con el fin de desactivar la traducción de nombres a dirección de los dispositivos, posteriormente debemos como colocar el nombre ya sea S1 o S2 según el Switch que estemos trabajando y asignar el respectivo dominio, por seguridad es necesario restringir el ingreso a personal no autorizado a los respectivos switch por lo que veremos los comandos para colocar la contraseña cifrada para el modo EXEC privilegiado y la contraseña de acceso a la consola, con todo esto es necesario establecer la longitud mínima para las contraseñas ya que es una opción importante para asegurarlas con una longitud mínima lo cual ya asegura el S1 y S2 en esta actividad, con esto pasamos a configurar el inicio de sesión en las líneas VTY para que use la base de datos local y la configuración de VTY solo aceptando SSH, utilizaremos unos comandos con el fin de cifrar las contraseñas de texto no cifrado, asignaremos un MOTD Banner y como último paso vamos a generar una clave de cifrado RSA con el comando crypto key generate rsa general-keys modulus 1024, ya para terminar esta parte haremos una configuración a la interfaz de administración donde estableceremos la dirección IPv4 de capa 3 y la dirección local de enlace IPv6 tanto para S1 y S2 finalizando con la configuración del gateway predeterminado

Tener en cuenta para permitir IPV6 debemos utilizar los siguientes comandos y hacer lo siguiente en CLI del S1 y S2:

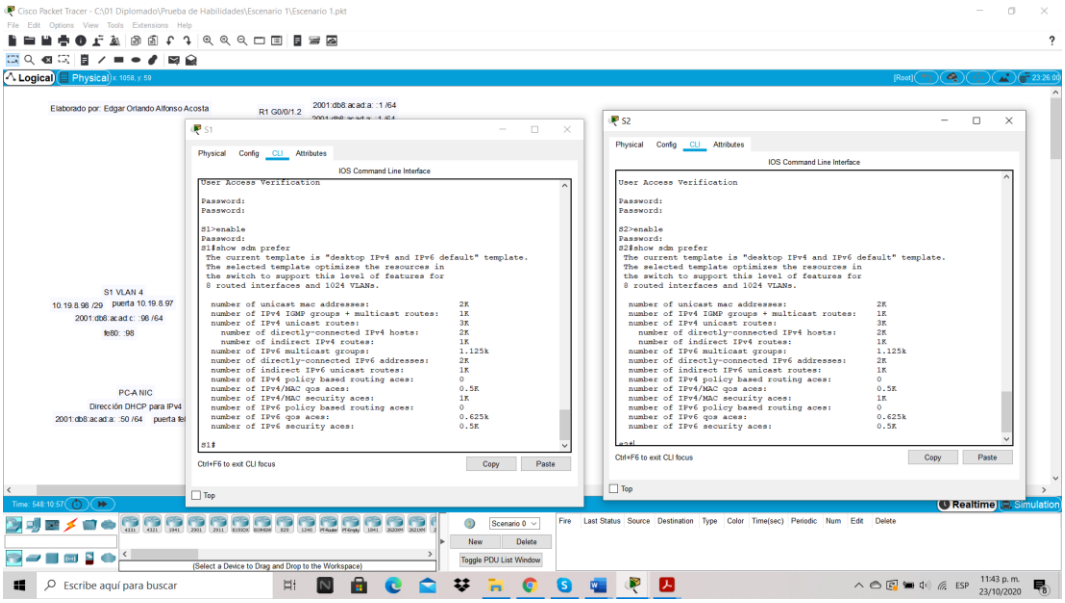
Tabla 5. Configuración plantilla SDM.

Descripción	Comando
Entrar al switch 1 y 2.	
Switch>	enable
Switch#	configure terminal
Switch#	sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#	exit
Switch#	reload
Switch#	show sdm prefe

Fuente: Autor.

Se procede a configurar la plantilla SDM para que admita IPv6 por lo que es necesario volver a cargar los switchs 1 y 2. De lo contrario el comando no funcionara.

Figura 2. Verificación comando show sdm prefer en S1 y S2



Fuente: Autor.

Mediante el comando show sdm prefer en modo privilegiado podemos verificar la plantilla que tengamos en S1 y S2 pero si entramos a modo de configuración global es decir con (config)#sdm prefer command, podemos cambiar la plantilla, aunque esta no aplica para este escenario.

Tabla 6. Configure S1 y S2.
Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	Se procede a desactivar la búsqueda de DNS Con el comando no ip domain-lookup **S1** Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup

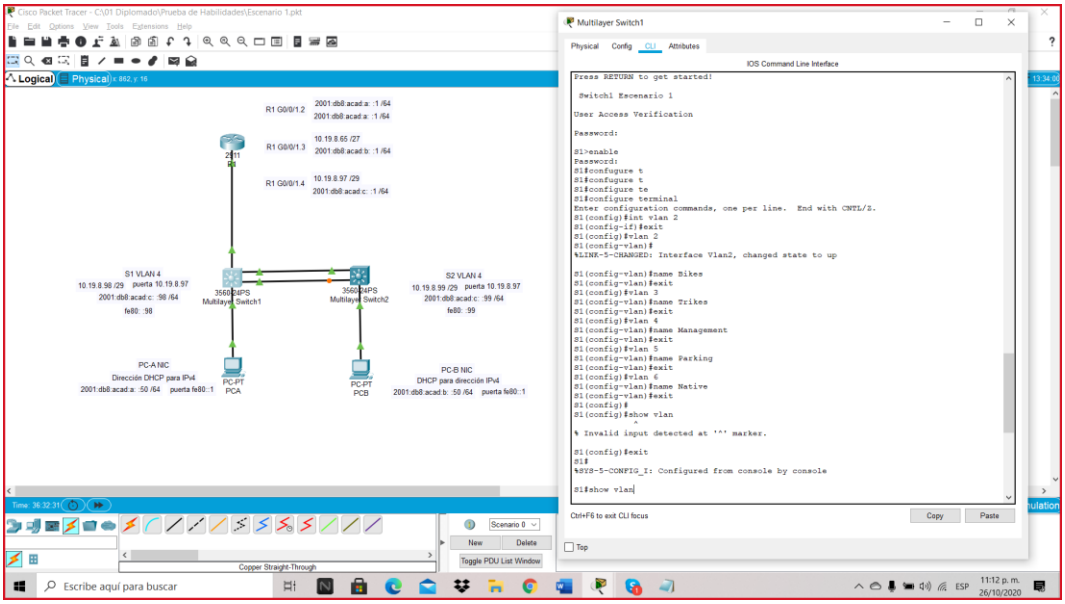
Tarea	Especificación
Desactivar la búsqueda DNS.	**S2** Switch>enable Switch#confi Switch#configure Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda** Se asigna los respectivos nombre con el comando hostname **S1** Switch(config)#hostname S1 S1(config)# **S2** Switch(config)#hostname S2 S2(config)#
Nombre de dominio	**ccna-lab.com** S1(config)#ip domain name ccna-lab.com S2(config)#ip domain name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**Ciscoenpass** S1(config)#enable secret ciscoenpass S2(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 S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** S1(config-line)#username admin password adm S2(config-line)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 S2(config)#line vty 0 4

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#privilege level 5 S1(config-line)#transport input ssh S2(config-line)#privilege level 5 S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption S2(config-line)#service password-encryption
Configurar un MOTD Banner	Se utiliza el siguiente comando para ambos switch banner motd # Switch1 Escenario 1# banner motd # Switch2 Escenario 1#
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1(config)#crypto key generate rsa general-keys modulus 1024 S2(config)#crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	**Establecer la dirección IPv4 de capa 3** S1(config-if)#description vlan4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 **Establezca la dirección local de enlace IPv6 como** **FE80: :98 para S1** S1(config)#int vlan 4 S1(config-if)#description vlan4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#no shutdown S1(config)#

Tarea	Especificación
Configurar la interfaz de administración (SVI)	**FE80: :99 para S2** S2(config)#int vlan 4 S2(config-if)#description vlan4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 **Establecer la dirección IPv6 de capa 3** S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#no shutdown
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4 S1(config-if)#ip default-gateway 10.19.8.97 S2(config-if)#ip default-gateway 10.19.8.97

PARTE 2. CONFIGURACIÓN DE LA INFRAESTRUCTURA DE RED (VLAN, TRUNKING, ETHERCHANNEL)

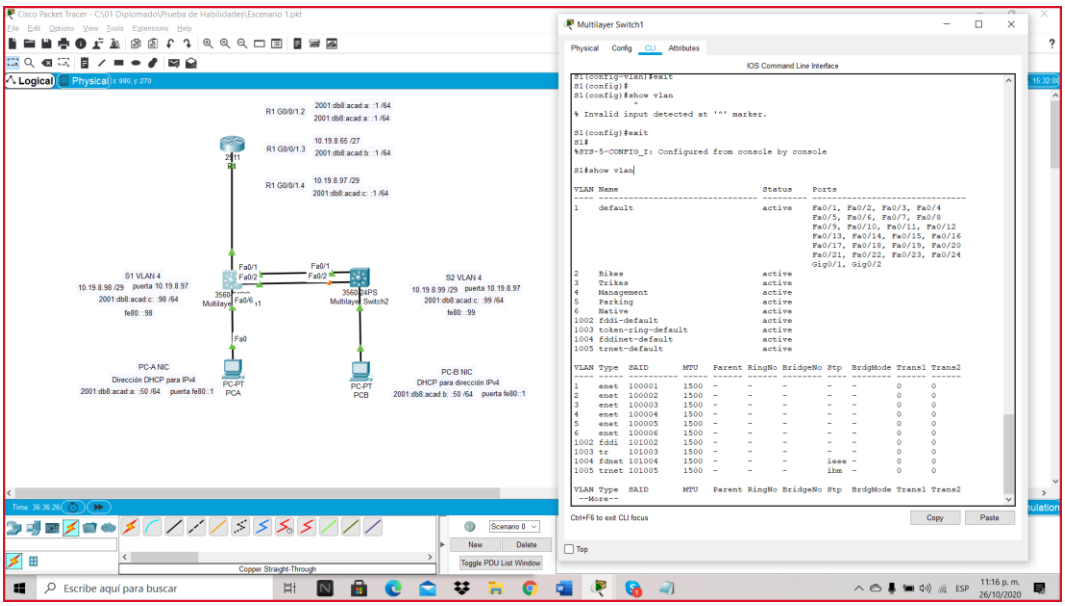
Figura 3. Demostración Configurar la interfaz de administración (SVI)



Fuente: Autor.

Se visualiza a medida de información el paso a paso para la configuración de la interfaz de administración (SVI).

Figura 4. Verificación de creación de las Vlans



Fuente: Autor.

Con el fin de estar seguros en la creación de las Vlans con el comando show Vlan podemos verificar los nombres correctos y si están activas.

PASO 1: CONFIGURAR S1.

Veremos una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 5 para S1.

En esta actividad veremos un paso muy interesante en la creación de las Vlan, las cuales tiene un aspecto importante en el escenario 1, toda vez que con esta practica daremos acceso a redes lógicas independientes dentro de la red para que puedan tener conectividad, recordemos que el S1 es de capa 2 y por ende es necesario utilizar el encabezado de encapsulación 802.1Q. con el fin de incorporar una etiqueta a la trama ya sea la ethernet original y también nos permite aclarar la VLAN a la que pertenece la trama.

Ahora bien antes de crear una vlan debemos ingresar a modo de configuración privilegiado en el respectivo switch 1 e ingresar al comando Vlan, seguido del número que vallamos a crear y de forma automática entramos a modo de configuración global para asignar el nombre correspondiente a la Vlan, es importante seguir con la configuración de troncos 802.1Q y los puertos para poder coordinar los troncales en interfaces Fast Ethernet, para este escenario nos iremos con interfaces F0/1, F0/2 y F0/5 y procedemos a crear troncos 802.1Q que utilicen la VLAN 6 nativa, posterior a esto entramos a configurar el puerto de acceso de host para VLAN 2 para la Interface F0/6.

Cuando realizamos la creación de las Vlan es necesario configurar la seguridad del puerto en los puertos de acceso, ¿cómo se hace esto?, muy sencillo, en configuración Global utilizamos el comando switchport port-security security maximum 3, esto quiere decir que vamos a permitir el uso máximo de tres puertos para la interface F0/6. Finalmente vamos a proteger todas las interfaces que no serán utilizadas, entonces ingresamos en configuración privilegiada, luego digitamos el comando int range fa 0/3-4, fa 0/7-24, G 0/1-2 como pueden observar solo queda la F0/5 activa, luego entramos a configuración global y procedemos a apagarlas.

Tabla 7. Configurar S1

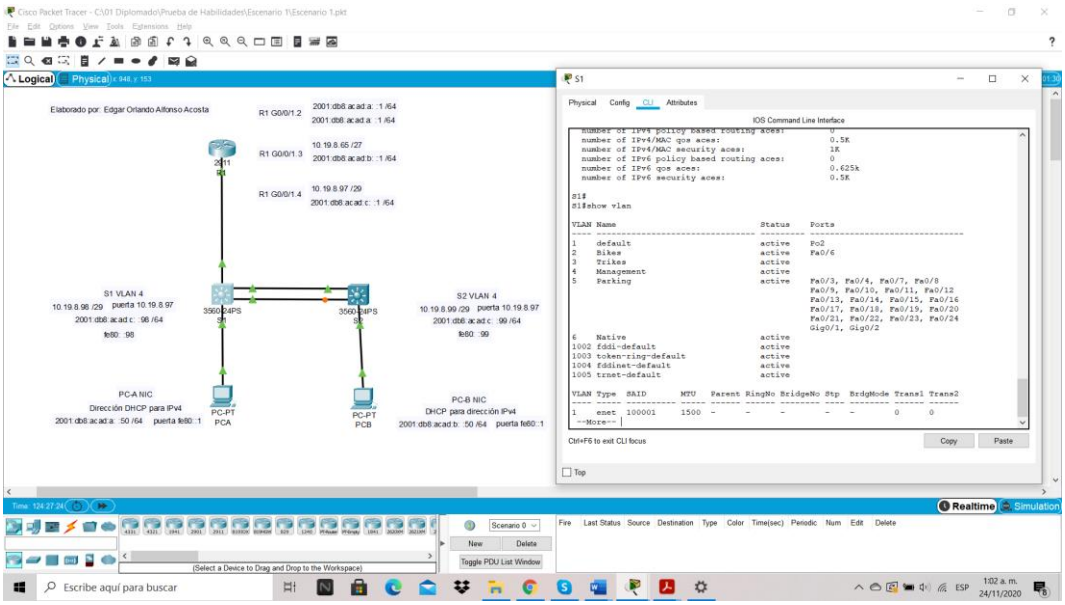
La configuración del S1 incluye las siguientes tareas:

area	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, name Parking VLAN 6, name Native Se asignarn los nombres de las Vlan en S1 S1(config)#Vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit 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)#Vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#

area	Especificación
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**Interfaces F0/1, F0/2 y F0/5** S1(config-if)#interface range fa0/1, fa0/2, fa0/5 S1(config-if-range)#no shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if)#switchport trunk encapsulation dot1q
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-if)#interface range fa0/1,fa0/2, fa0/5
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 S1(config-if-range)# S1(config-if-range)#exit S1(config)#int fa 0/6 S1(config-if)#no shutdown S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 4 S1(config-if)#
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC S1(config)#int fa0/6 S1(config-if)#switchport port-security security maximum 3 S1(config-if)#exit S1(config)#exit S1#show port-security

area	Especificación
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar S1(config-if-range)#exit S1(config)#int range fa 0/3-4, fa 0/7-24, G 0/1-2 S1(config-if-range)#no shutdown S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description puertos sin usa S1(config-if-range)#exit S1(config)#exit

Figura 5. Demostración de las Vlan Creadas en S1



Fuente: Autor.

Con el comando show vlan brief podemos observar el registro o evidencia de la creación de las cinco Vlans con sus respectivos nombres así como la Vlan Nativa y los respectivos puestos asignados a la Vlan 2 y Vlan 5.

PASO 2: CONFIGURE S2.

Veremos una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 6 para S2, que son muy similares a los realizados en la configuración del S1, pero aquí lo que vamos adicionar es la creación de los troncos 802.1Q que utilicen la VLAN 6 nativa pero en las interface F0/1 y F0/2, configuramos

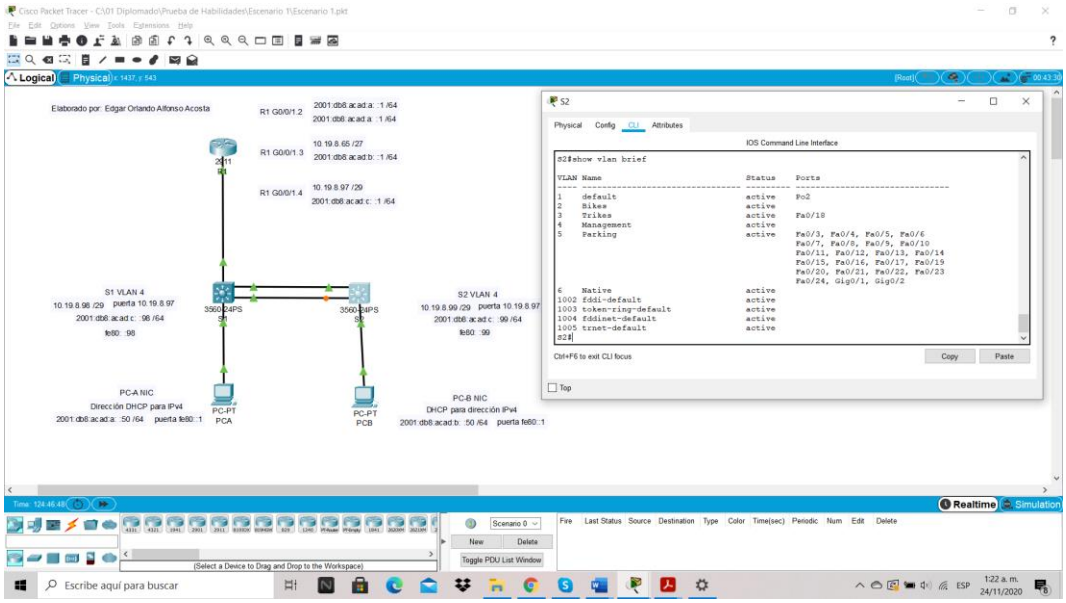
el puerto de acceso del host para la VLAN 3 a la F0/6, y seguidos los mismos pasos de la configuración de S1 y nos aseguramos que todas las interfaces no utilizadas.

Tabla 8. Configure el S2.
Entre las tareas de configuración de S2 se incluyen las siguientes:

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear VLAN	Se practica el mismo escenario realizado con S1 con el fin configurar las Vlan. 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 S2(config-vlan)#exit S2(config)#Vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#Vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2 S2# S2#configure terminal S2(config)#interface range fa0/1, fa0/2, fa0/5 S2(config-if-range)#no shutdown S2(config-if-range)#switchport mode access S2(config-if-range)#switchport mode trunk S2(config-if-range)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#exit S2(config)#exit

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación Se inicia con la creación de un grupo de etherchannel de capa 2 teniendo en cuenta la configuracion del S1 S2(config)#interface range fa0/1, fa0/2 S2(config-if-range)#channel-group 2 mode passive S2(config-if-range)#
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18 Se procede a configurar la el puerto para tener acceso al host en al vlan 3 S2(config)#int fa0/18 S2(config-if)#no shutdown S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports	permite 3 MAC addresses Se procede a configurar el puerto security con los siguientes comandos S2(config)#int fa 0/18 S2(config-if)#switchport port-security 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. Se procede a configurar todas la interfaces no utilizadas S2(config)#int range fa 0/3-17, fa 0/19-24, G 0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description puertos sin usa S2(config-if-range)#exit S2(config)#exit

Figura 6. Demostración de las Vlan Creadas en S2



Fuente: Autor.

Con el comando show vlan brief podemos observar el registro o evidencia de la creación de las cinco Vlans con sus respectivos nombres, así como la Vlan Nativa y los respectivos puertos asignados a la Vlan 3 y Vlan 5.

PARTE 3. CONFIGURAR SOPORTE DE HOST

PASO 1: CONFIGURE R1

A continuación, veremos una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 7 para configurar R1

Para este paso veremos cómo se crean las rutas predeterminadas para IPv4 e IPv6 con el fin de dirigir el tráfico a la interfaz Loopback 0, por lo que tenemos como activad configurar el enrutamiento predeterminado, ¿esto como se hace? Debemos utilizar el comando ip route 0.0.0.0 0.0.0.0 Loopback0 en modo de configuración predeterminado y luego ejecutamos el comando ipv6 route ::/0 Loopback0 para dirigir el tráfico, es recomendable hacer una copia a esta altura, con el fin de evitar errores a futuro, toda vez que si comentemos algún error podemos volver al último escenario para retornar a cargar los comandos correctos. Seguimos con la configuración en R1 para IPv4 DHCP para VLAN 2, ¿qué hacemos en este punto? De forma sencilla creamos un grupo DHCP para VLAN 2, y asignaremos el nombre de dominio ccna-a.net como lo indica la actividad, y ya terminando este párrafo debemos configurar DHCP IPv4 para VLAN 3, al igual que la Vlan 2 asignaremos el nombre de dominio ccna-b.net.

Tabla 9. Configuración R1
Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 R1(config)#ip route 0.0.0.0 0.0.0.0 Loopback0 R1(config)#ipv6 route ::/0 Loopback0 R1(config)#exit R1#copy running-config startup-config
Configurar IPv4 DHCP para VLAN 2	R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	R1#configure terminal R1(config)#ip dhcp pool vlan2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192
Configurar DHCP IPv4 para VLAN 3	R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#exit R1(config)#ip dhcp pool vlan3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.58 R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84

Datos a tener en cuenta para el siguiente punto

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

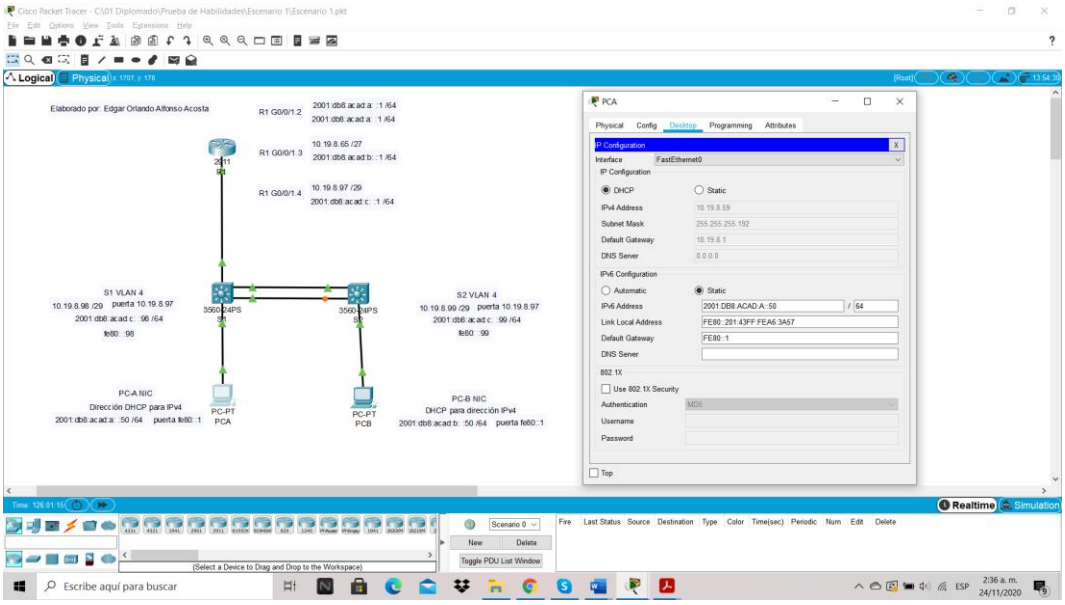
PASO 2: CONFIGURAR LOS SERVIDORES

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

Tabla 10. Configuración de servidores PC-A

PC-A Network Configuration	
Descripción	Datos tomado desde ipconfig /all
Dirección física	0001.43A6.3A57
Dirección IP	10.19.8.59
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

Figura 7. Verificación configuración PC-A



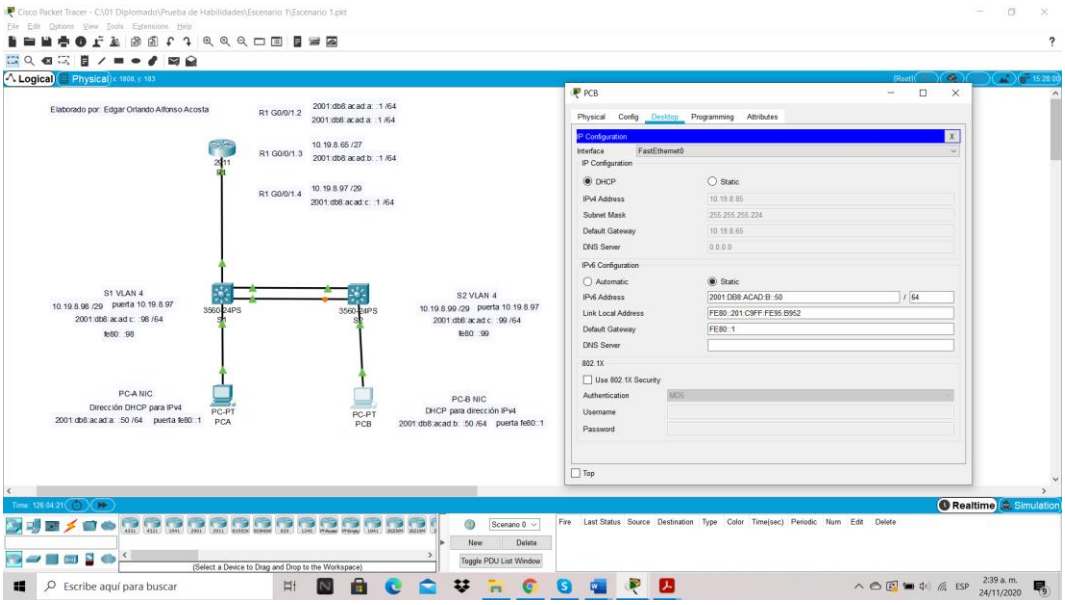
Fuente: Autor.

Se deja evidencia de la configuración de PC-A utilizando DHCP para IPv4 y la asignación de estáticamente a las direcciones IPv6 GUA y Link Local .

Tabla 11. Configuración de servidores PC-B

Configuración de red de PC-B	
Descripción	Datos tomado desde ipconfig /all
Dirección física	0001.C995.B952
Dirección IP	10.19.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	FE80::1

Figura 8. Verificación configuración PC-B



Fuente: Autor.

Se deja evidencia de la configuración de PC-B utilizando DHCP para IPv4 y la asignación de estáticamente a las direcciones IPv6 GUA y Link Local .

PARTE 4. PROBAR Y VERIFICAR LA CONECTIVIDAD DE EXTREMO A EXTREMO

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

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

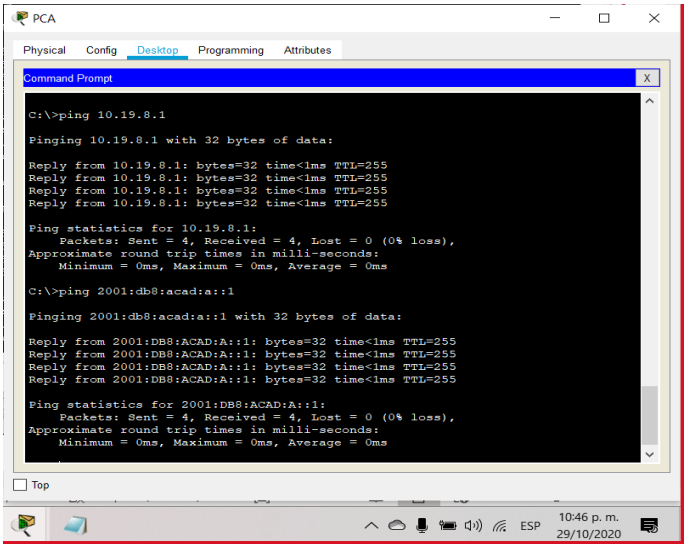
Tabla 12. Probar y Verificar

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	*Conexión ok*
		IPv6	2001:db8:acad:a::1	*Conexión ok*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Conexión ok*
		IPv6	2001:db8:acad:b::1	*Conexión ok*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Conexión ok*
		IPv6	2001:db8:acad:c::1	*Conexión ok*
	S1, VLAN 4	Dirección	10.19.8.98	*Conexión ok*
		IPv6	2001:db8:acad:c::98	*Conexión ok*
	S2, VLAN 4	Dirección	10.19.8.99.	*Conexión ok*
		IPv6	2001:db8:acad:c::99	*Conexión ok*
	PC-B	Dirección	IP address will vary. 10.19.8.85	*Conexión ok*
		IPv6	2001:db8:acad:b::50	*Conexión ok*
	R1 Bucle 0	Dirección	209.165.201.1	*Conexión ok*
		IPv6	2001:db8:acad:209::1	*Conexión ok*
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Conexión ok*
		IPv6	2001:db8:acad:209::1	*Conexión ok*
	R1, G0/0/1.2	Dirección	10.19.8.1	*Conexión ok*
		IPv6	2001:db8:acad:a::1	*Conexión ok*
	R1, G0/0/1.3	Dirección	10.19.8.65	*Conexión ok*
		IPv6	2001:db8:acad:b::1	*Conexión ok*
	R1, G0/0/1.4	Dirección	10.19.8.97	*Conexión ok*

Desde	A	de Internet	Dirección IP	Resultados de ping
		IPv6	2001:db8:acad:c::1	*Conexión ok*
	S1, VLAN 4	Dirección	10.19.8.98	*Conexión ok*
		IPv6	2001:db8:acad:c::98	*Conexión ok*
	S2, VLAN 4	Dirección	10.19.8.99	*Conexión ok*
		IPv6	2001:db8:acad:c::99	*Conexión ok*

Demostración de figuración y comprobación de Ping desde PCA y PCB

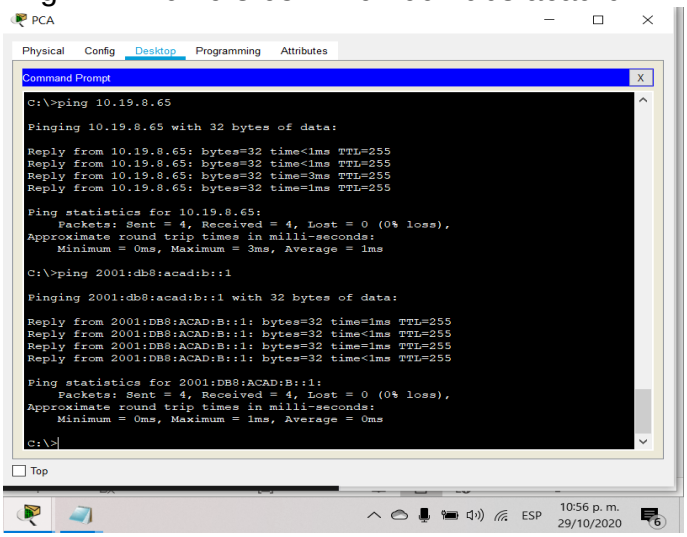
Figura 9. PCA. Ping IPV4 10.19.8.1 IPv6 2001:db8:acad:a::1



Fuente: Autor.

Se evidencia la respuesta de los ping desde PC-A a las direcciones IPV4 10.19.8.1 e IPv6 2001:db8:acad:a::1 y la correcta configuración a R1, G0/0/1.2

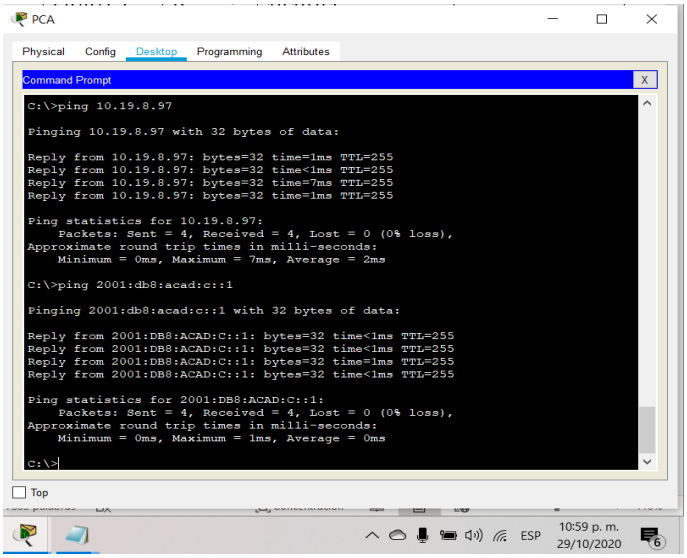
Figura 10. PCA. Ping IPV4 10.19.8.65 IPV6 2001:db8:acad:b::1



Fuente: Autor.

Se comprueba mediante la respuesta de los ping IPV4 10.19.8.65 e IPV6 2001:db8:acad:b::1 la correcta configuración a R1, G0/0/1.3

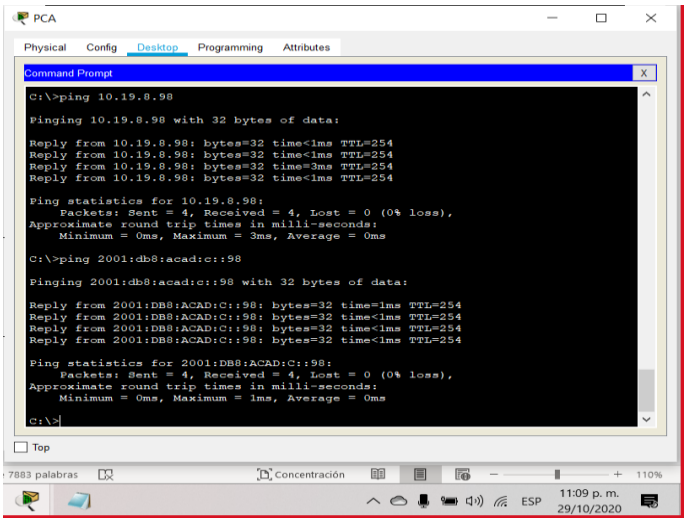
Figura 11. PCA. Ping IPV4 10.19.8.97 IPv6 2001:db8:acad:c::1



Fuente: Autor.

Se comprueba mediante la respuesta de los ping Ping IPV4 10.19.8.97 IPv6 2001:db8:acad:c::1 a R1, G0/0/1.4

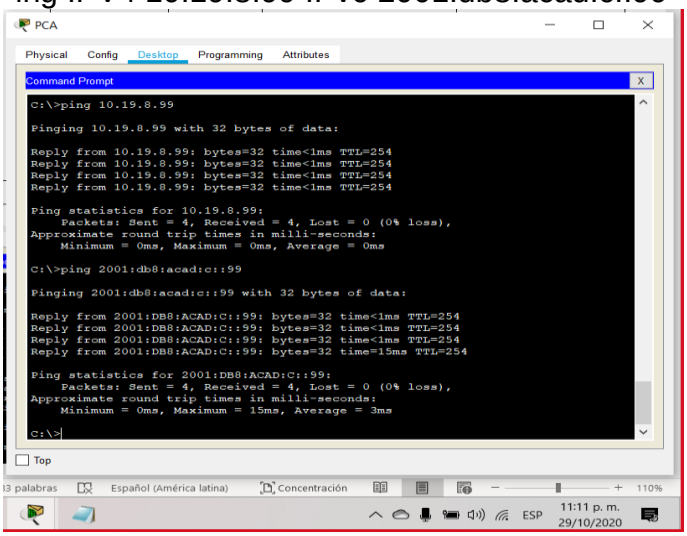
Figura 12. PCA. Ping IPV4 10.19.8.98 IPv6 2001:db8:acad:c::98



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.98 IPv6 2001:db8:acad:c::98 a S1, VLAN 4

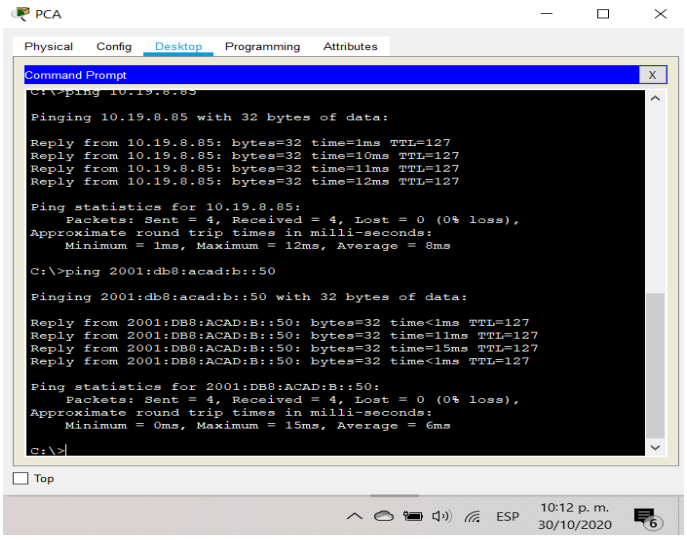
Figura 13. PCA. Ping IPV4 10.19.8.99 IPv6 2001:db8:acad:c::99



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.98 IPv6 2001:db8:acad:c::98 a S2, VLAN 4

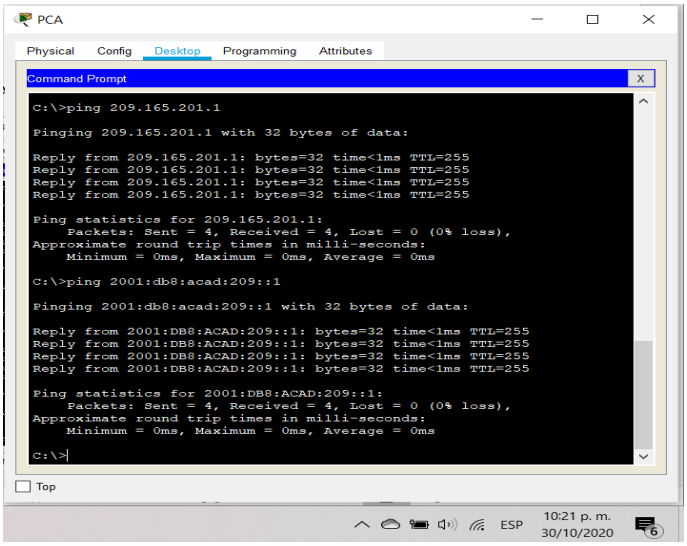
Figura 14. PCA. Ping IPV4 y IPv6



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.85 IPv6 2001:db8:acad:b::50 a PC-B.

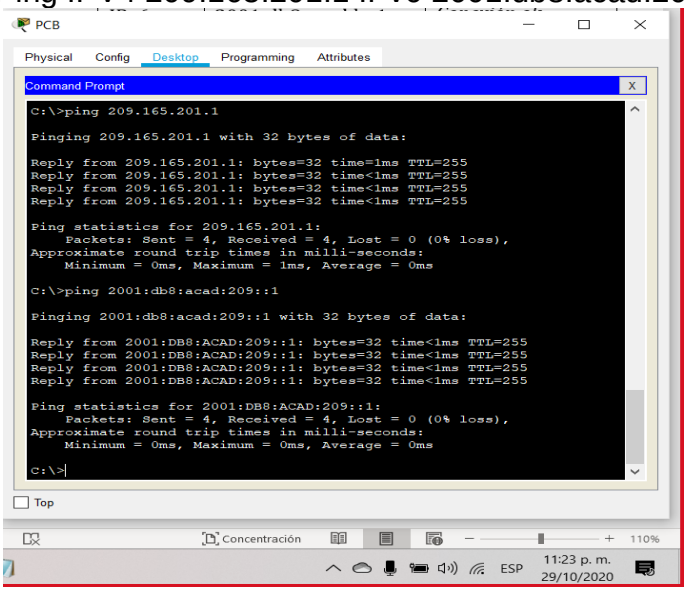
Figura 15. PCA. Ping IPV4 209.165.201.1 IPv6 2001:db8:acad:209::1



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 209.165.201.1 e IPv6 2001:db8:acad:209::1 a R1 Bucle 0

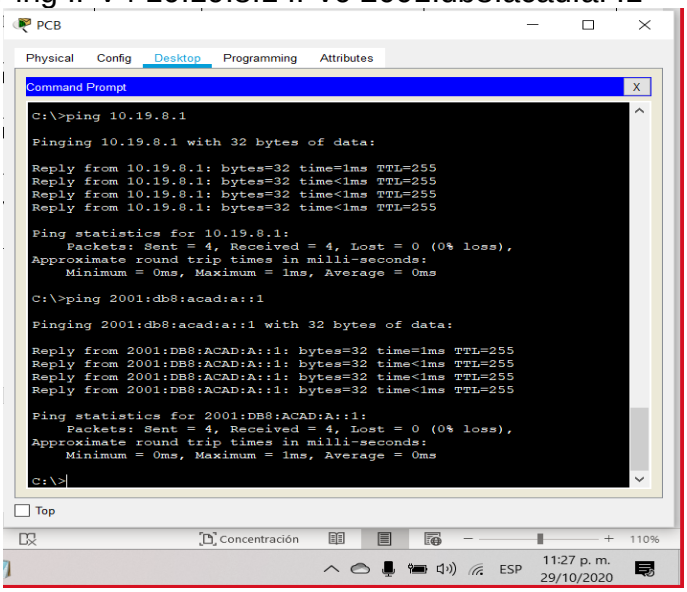
Figura 16. PCB. Ping IPV4 209.165.201.1 IPv6 2001:db8:acad:209: :1



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 209.165.201.1 e IPv6 2001:db8:acad:209: :1 a R1 Bucle 0

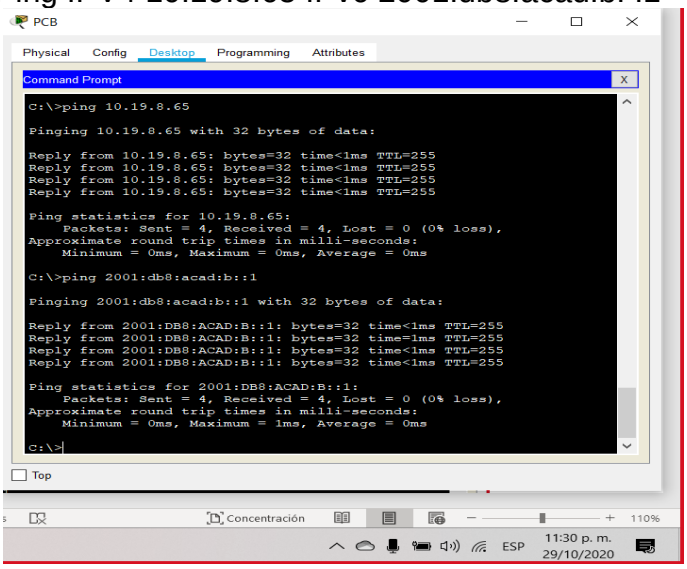
Figura 17. PCB. Ping IPV4 10.19.8.1 IPv6 2001:db8:acad:a: :1



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.1 e IPv6 2001:db8:acad:a: :1 a R1, G0/0/1.2

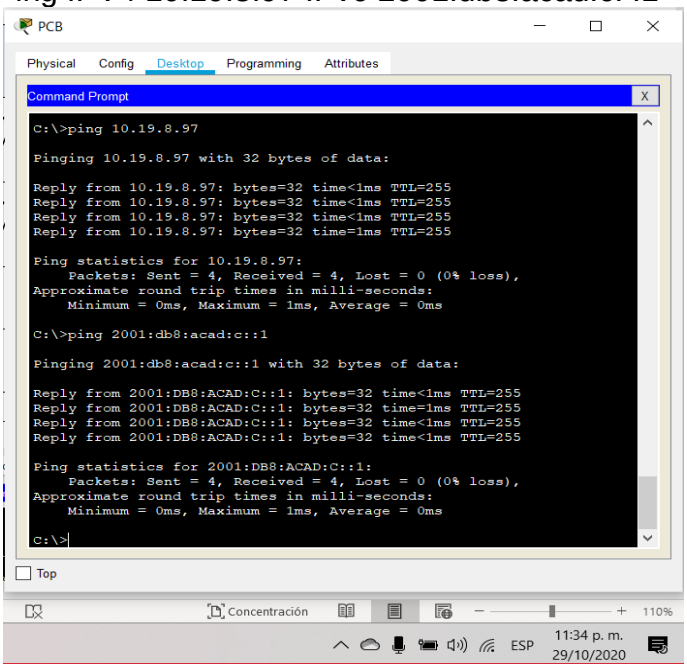
Figura 18. PCB. Ping IPV4 10.19.8.65 IPv6 2001:db8:acad:b: :1



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.65 e IPv6 2001:db8:acad:b: :1 a R1, G0/0/1.3

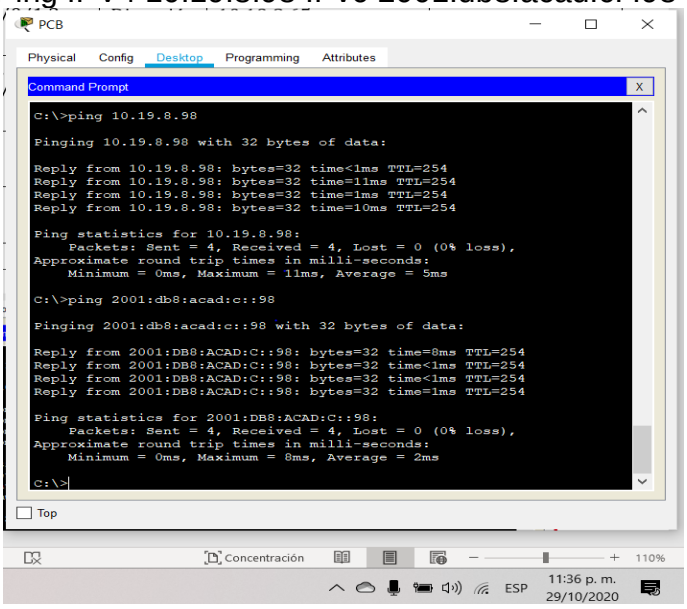
Figura 19. PCB. Ping IPV4 10.19.8.97 IPv6 2001:db8:acad:c: :1



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.97 e IPv6 2001:db8:acad:c: :1 a R1, G0/0/1.4

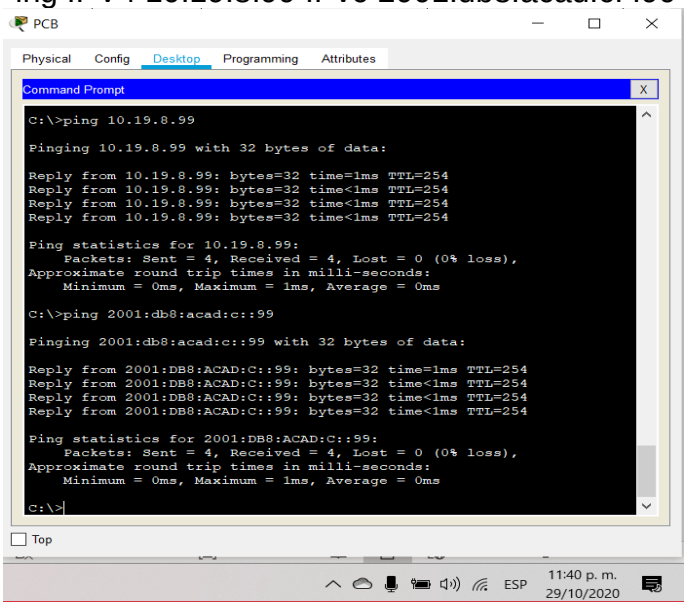
Figura 20. PCB. Ping IPV4 10.19.8.98 IPv6 2001:db8:acad:c: :98



Fuente: Autor.

Se comprueba mediante la respuesta de los Ping 10.19.8.98 e IPv6 2001:db8:acad:c: :98 a S1, VLAN 4

Figura 21. PCB. Ping IPV4 10.19.8.99 IPv6 2001:db8:acad:c: :99



Fuente: Autor.

Descripción: Se comprueba mediante la respuesta de los Ping 10.19.8.99 e IPv6 2001:db8:acad:c: :99 a S2, VLAN 4.

ESCENARIO 2

TOPOLOGÍA

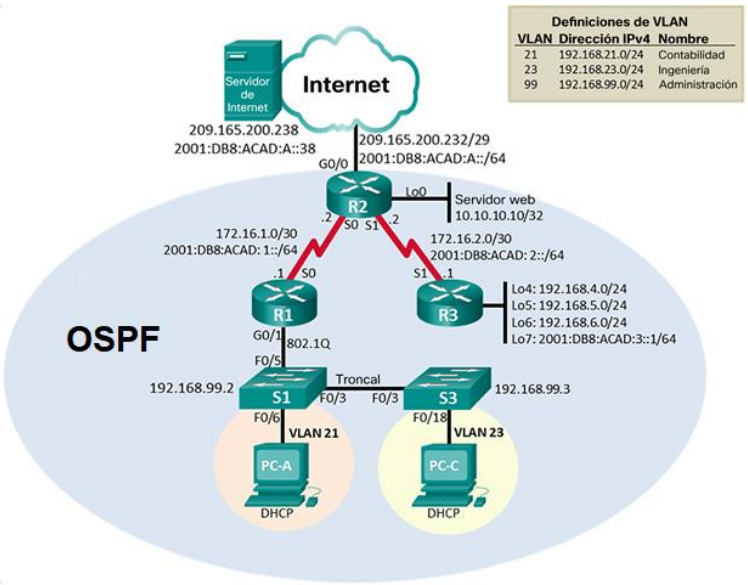
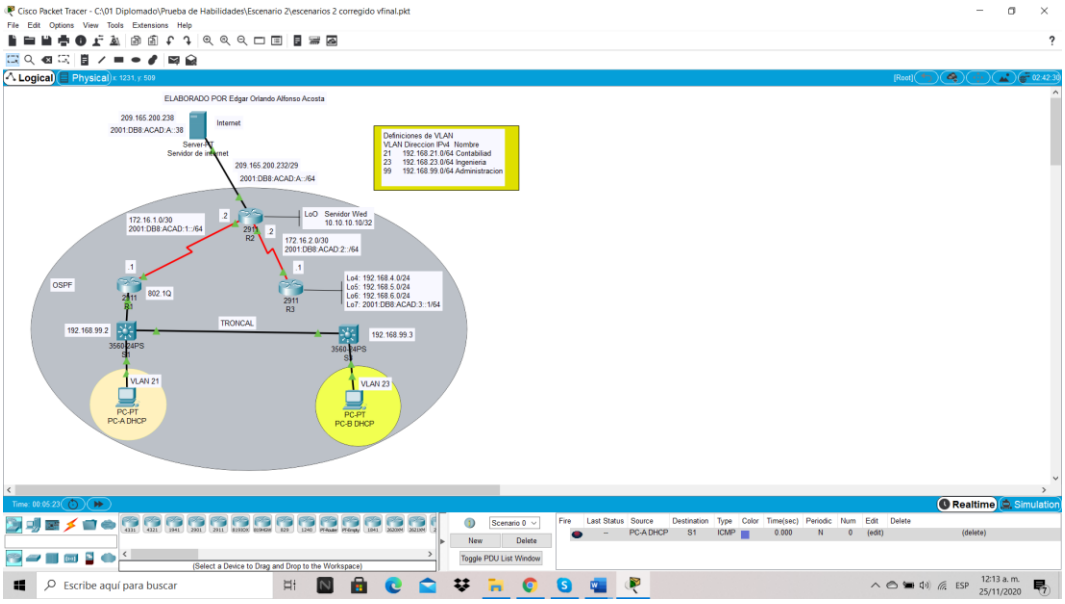


Figura 22. Montaje en Packet Tracer escenario 2



Fuente: Autor.

Descripción: Evidencia del montaje de acuerdo con el caso del escenario 2 donde se observa la autenticidad de mi sustentación

PARTE 1. INICIALIZAR DISPOSITIVOS

Veremos una pequeña explicación a este paso, para iniciar debemos eliminar las respectivas configuraciones que puedan tener los router y los switch del escenario número 2, es importante realizar este paso en todos los procesos de configuraciones y en cualquier proyecto, toda vez que es posible que al verificar no haya nada configurado, pero la prevención es fundamental, nunca lo dudemos en hacerlo y así evitamos cualquier inconveniente para implementar la red.

Estos son los comandos necesarios para utilizar y para proseguir e inicializar y volver a cargar los router y los switch del escenario 2.

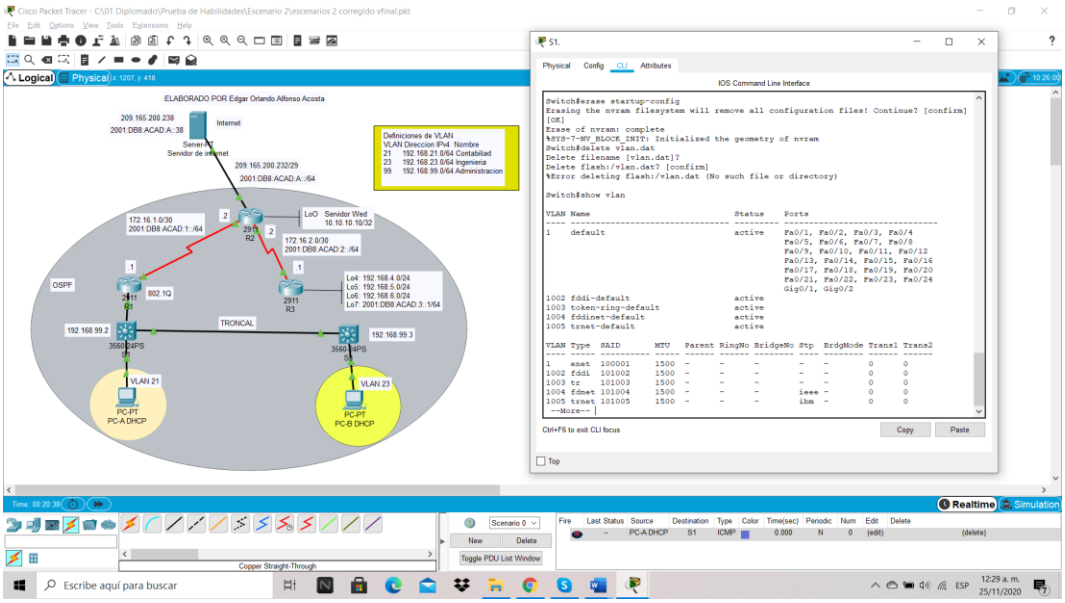
Nota: Este proceso lo realizaremos en todos los Router y Switch del escenario 2

PASO 1: INICIALIZAR Y VOLVER A CARGAR LOS ROUTERS Y LOS SWITCHES

Tabla 13. Inicialización y carga de los router y los switch escenario 2

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

Figura 23. Verificación de borrado de las Vlan en un Switch



Fuente: Autor.

Se evidencia que no hay Vlans creadas en uno de los Switch.

PARTE 2. CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

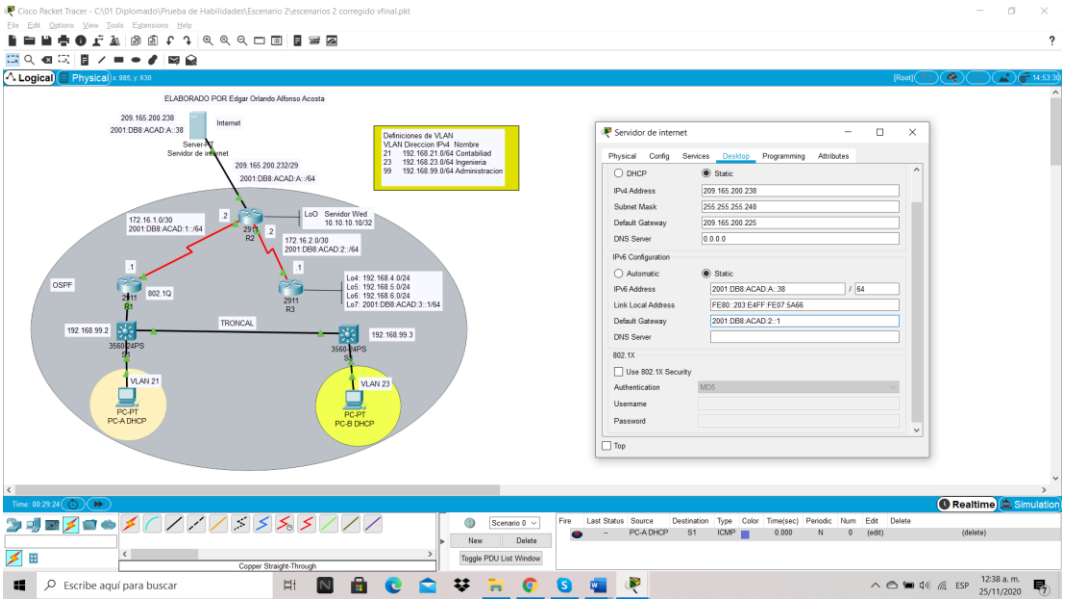
En la parte 2 de este escenario procedemos a configurar el servidor de internet con la dirección IPV4, mascara, puerta de enlace, dirección IPv6 y puerta de enlace de IPv6, con esto datos inicio de forma básica para proseguir con la configuración del R1.

PASO 1: CONFIGURAR LA COMPUTADORA DE INTERNET

Tabla 14. Datos de configuración de servidor de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:D88:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Figura 24. Configuración del servidor internet



Fuente: Autor.

Descripción: Iniciamos con la configuración del servidor de Internet con los datos suministrados en la tabla

PASO 2: CONFIGURAR R1

En este paso vamos a realizar la configuración de R1 en las mismas condiciones del escenario 1, volvemos hacer la práctica de una forma ágil, iniciamos con la desactivación de búsqueda DNS, le asignamos el nombre correspondiente que será R1, asignamos las contraseñas de exec privilegiado cifrada, así como la contraseña de acceso a la consola y la contraseña de acceso a telnet, como medida de seguridad para cualquier dispositivo de red le asignaremos una contraseña de texto no cifrado con el mensaje MOTD, y finalizando este paso entraremos a la interfaz S0/0/0 ya que es necesario para que al router se pueda acceder, es decir se debe configurar la interface específica, ingresando al modo de configuración de interfaz con el comando del modo de configuración global, ya dentro de la interfaz ingresamos las direcciones IPv4 e IPv6 relacionadas en la topología, finalizamos con el comando clock rate 128000 y la prendemos con el comando no shutdown, para terminar creamos las rutas predeterminadas.

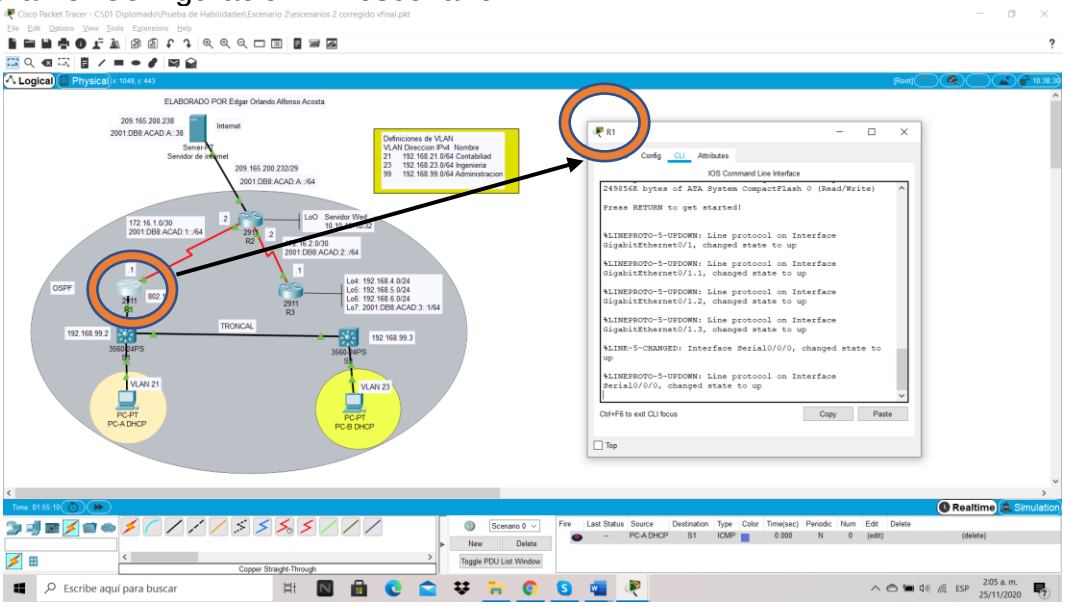
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Configuración R1 escenario 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure t Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R1 Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	Class R1(config)#enable secret class
Contraseña de acceso a la consola	Cisco R1(config)#line console 0 R1(config-line)#password cisco
Contraseña de acceso Telnet	Cisco R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit R1(config)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1#configure t R1#configure terminal R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd # Se prohíbe el acceso no autorizado#

Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Interfaz S0/0/0	R1#configure terminal R1(config)# R1(config)#int s0/0/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#

Figura 25. Configuración R1 escenario 2



Fuente: Autor.

Las actividades de configuración se realizaron el R1 en la opción CLI con el fin de ir programando el direccionamiento acuerdo con el escenario 2.

Nota: Todavía no configure G0/1.

PASO 3: CONFIGURAR R2

La configuración para R2 es muy similar a la de R1, iniciamos con la desactivación de búsqueda DNS, le asignamos el nombre correspondiente que será R2, asignamos las contraseñas de exec privilegiado cifrada, así como la contraseña de acceso a la consola y la contraseña de acceso a telnet, como medida de seguridad para cualquier dispositivo de red le asignaremos una contraseña de texto no cifrado, tendremos una pequeña diferencia con R1, toda vez que este paso indica habilitar el servidor HTTP, según confirmación de nuestro tutor el comando ip http server no funciona en Packet Tracer, por lo tanto no se realiza, procedemos a colocar el mensaje MOTD y finalizando entrando a las interfaces S0/0/0 y S0/0/1 ya que es necesario para acceder al router, también ingresamos a Interfaz G0/0 (simulación de Internet) para establecer la dirección IPv4 y la dirección IPv6, le asignamos a la Interfaz loopback 0 (servidor web simulado) su respectivo direccionamiento y creamos las rutas predeterminadas.

La configuración del R2 incluye las siguientes tareas:

Tabla 16. Configuración R2 escenario 2

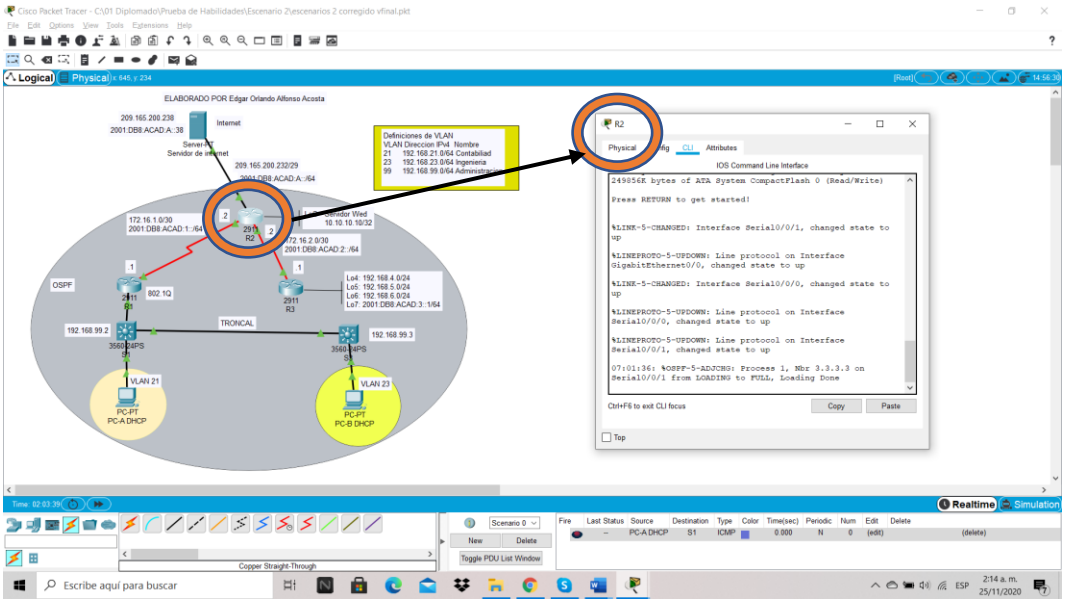
Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	R2 Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	Class 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)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	Se prohíbe el acceso no autorizado. banner motd # Se prohíbe el acceso no autorizado#

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. R2(config)#int s0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 Activar la interfaz R2 (config-if)#no shutdown
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R2(config)#int s0/0/1 R2(config-if)#description Connection to R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#ipv6 address 2001:db8:acad:2::2/64
Interfaz S0/0/1	Establecer la frecuencia de reloj en 128000. R2(config-if)#clock rate 128000 Activar la interfaz R2 (config-if)#no shutdown

Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz R2(config)# R2(config)#int g0/0 R2(config-if)#description Salida Internet R2(config-if)#ip addess 209.165.200.233 255.255.255.248 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 sh R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulated Web Server R2(config-if)#exit

Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Figura 26. Configuración R2 escenario 2



Fuente: Autor.

Las actividades de configuración se realizaron el R2 en la opción CLI con el fin de ir programando el direccionamiento acuerdo con el escenario 2

PASO 4: CONFIGURAR R3

Para la configuración de R3 tendremos similitudes con la configuración de R2, iniciamos con la desactivación de búsqueda DNS, le asignamos el nombre correspondiente que será R3, asignamos las contraseñas de exec privilegiado cifrada, así como la contraseña de acceso a la consola y la contraseña de acceso a telnet; como medida de seguridad para cualquier dispositivo de red le

asignaremos una contraseña de texto no cifrado y el mensaje MOTD, seguidamente entramos a la interfaces S0/0/1 ya que es necesario para acceder al router, establecemos la dirección IPv4 y la dirección IPv6. Asignaremos las direcciones IP de acuerdo con la topología a las Interfaz loopback 4 a la Interfaz loopback 7 y aquí finalizamos con la creación de las rutas predeterminadas.

La configuración del R3 incluye las siguientes tareas:

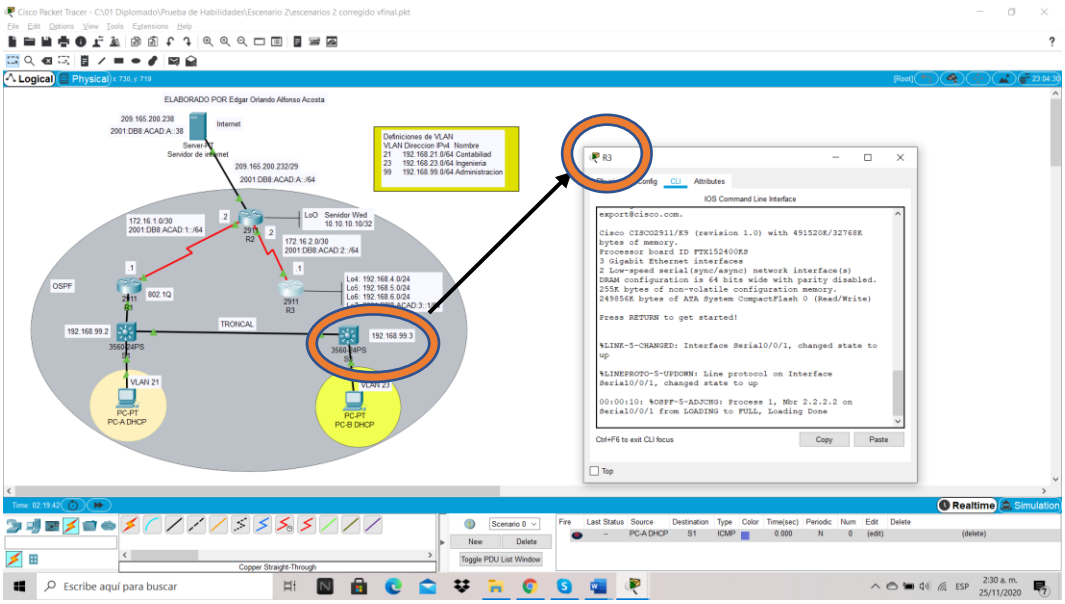
Tabla 17. Configuracion R3 escenario 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router#configure Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	R3 Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	Class R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R3(config)#banner motd # Se prohibe el acceso no autorizado#

Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R3(config)#int s0/0/1 R3(config-if)#description Connection R3 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	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#int loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit

Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#int loopback 7 R3(config-if)#ipv6 addres 2001:DB8:ACAD:3::1/64 R3(config-if)#no shutdown R3(config-if)#exit
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1

Figura 27. Configuracion R3 escenario 2



Fuente: Autor.

Las actividades de configuración se realizaron el R3 en la opción CLI con el fin de ir programando el direccionamiento acuerdo con el escenario 2.

PASO 5: CONFIGURAR S1

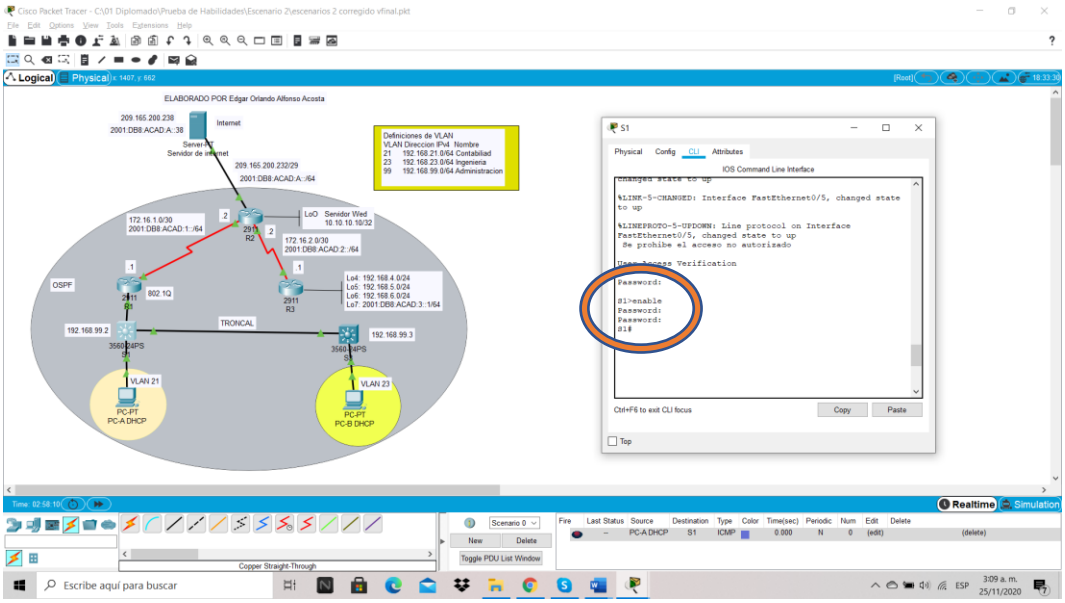
Para el siguiente paso 5 correspondiente a la configuración de S1 tendremos que realizar las actividades de desactivación de búsqueda DNS, le asignamos el nombre correspondiente que será S1, asignamos las contraseñas de exec privilegiado cifrada, así como la contraseña de acceso a la consola y la contraseña de acceso a telnet; como medida de seguridad, le asignaremos una contraseña de texto no cifrado y el mensaje MOTD con el siguiente mensaje, #Se prohibe el acceso no autorizado#. En el mensaje aprendimos que no se admiten tildes en la frase.

La configuración del S1 incluye las siguientes tareas:

Tabla 18. Configuración de S1 escenario 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. S1(config)#banner motd # Se prohibe el acceso no autorizado# S1(config)#

Figura 28. Configuración de S1 escenario 2



Fuente: Autor.

Se asignan las claves de acceso en S1 para evitar que usuarios no autorizados accedan al switch y puedan modificar o adulterar las configuraciones.

PASO 6: CONFIGURAR EL S3

Para el siguiente paso 6 haremos 7 pasos ya conocidos en S1

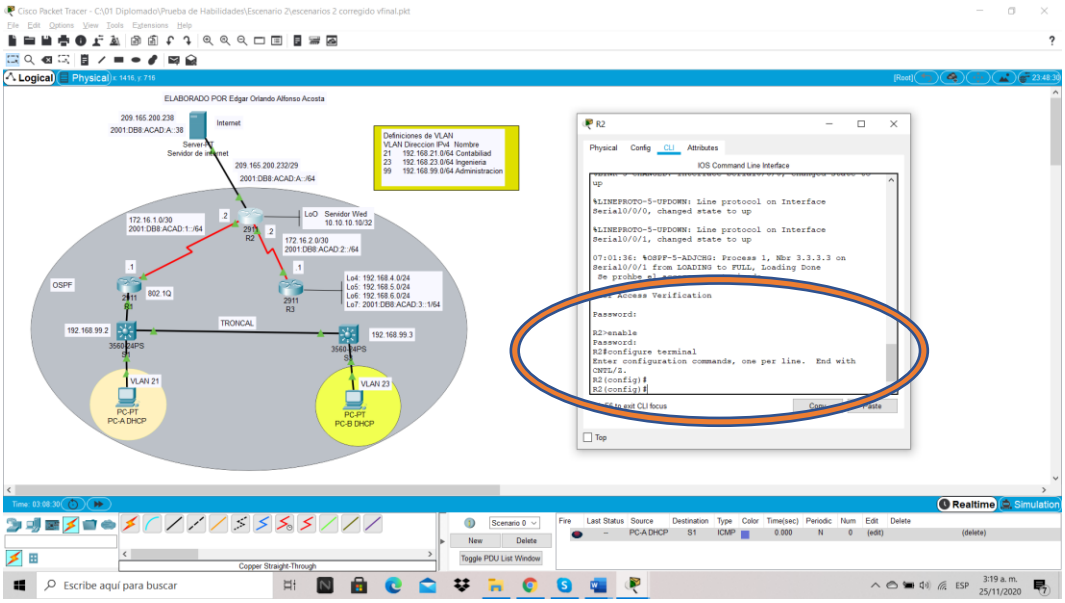
a la configuración de S1 tendremos que realizar las actividades de desactivación de búsqueda DNS, le asignamos el nombre correspondiente que será S3, asignamos las contraseñas de exec privilegiado cifrada, así como la contraseña de acceso a la consola y la contraseña de acceso a telnet; como medida de seguridad le asignaremos una contraseña de texto no cifrado y el mensaje MOTD con el siguiente mensaje, #Se prohibe el acceso no autorizado#.

La configuración del S3 incluye las siguientes tareas:

Tabla 19. Configuracion S3 escenario 2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
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	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#
Contraseña de acceso Telnet	S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#exit S3(config)#
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 # S3(config)#

Figura 29. Configuracion S3 escenario 2



Fuente: Autor.

Descripción: Se asignan las claves de acceso en S3 para evitar que usuarios no autorizados accedan al switch y puedan modificar o adulterar las configuraciones.

PASO 7: VERIFICAR LA CONECTIVIDAD DE LA RED

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

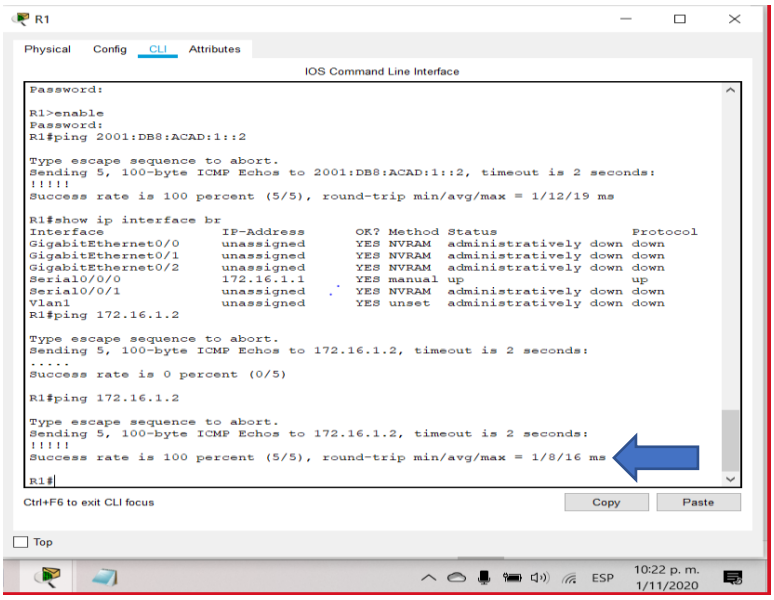
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 20. Cuadro detalle la conectividad de la red

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

Con los siguientes pantallazos dejo como evidencia el paso 7 con los respectivo ping y respuesta satisfactoria.

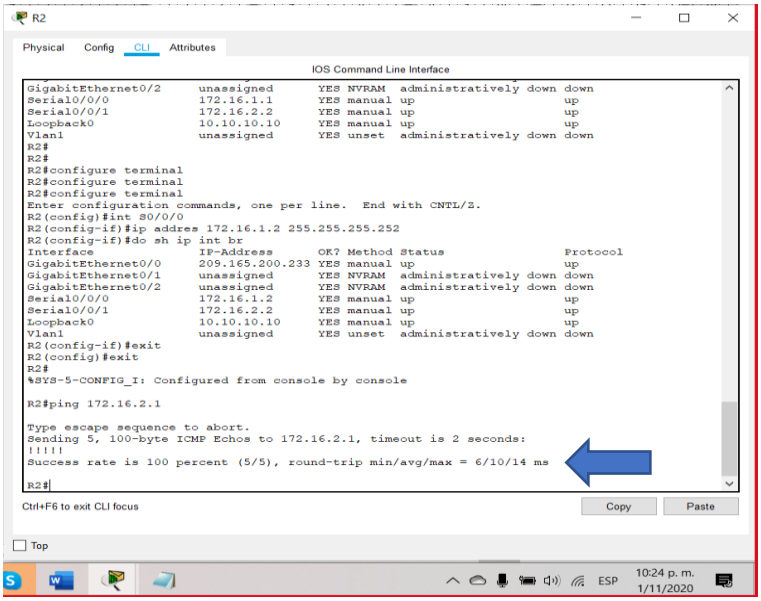
Figura 30. Ping des R1 a la dirección IP 172.16.1.2



Fuente: Autor.

Se establece respuesta satisfactoria desde R1 a la dirección IP 172.16.1.2 con successs rate is 100 percent.

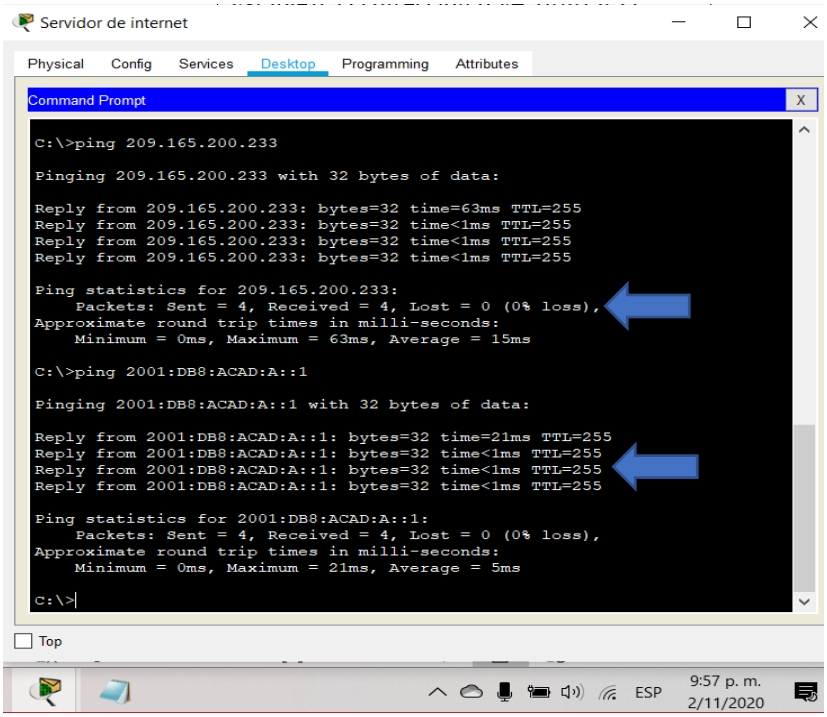
Figura 31. Ping des R2 a la dirección IP 172.16.1.2



Fuente: Autor.

Se establece respuesta satisfactoria desde R2 a la dirección IP 172.16.2.1 con successs rate is 100 percent.

Figura 32. Ping desde PC de Internet a la dirección IP 209.165.200.233



Fuente: Autor.

Se establece respuesta satisfactoria desde PC de Internet a la dirección IP 209.165.200.233 con successs rate is 100 percent.

PARTE 3. CONFIGURAR LA SEGURIDAD DEL SWITCH, LAS VLAN Y EL ROUTING ENTRE VLAN

PASO 1: CONFIGURAR S1

Procedo a dar una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 19 para S1, aquí configuraremos las tres Vlan correspondientes a la 21, 23 y 99 con sus respectivos nombres, asignaremos la dirección IPv4 a la VLAN llamada administración previamente, asignaremos la dirección ip addres 192.168.99.2 y su respectiva puerta de enlace 192.168.99.1, posteriormente debemos forzar el enlace troncal en la interfaz F0/3 y el enlace troncal en la interfaz F0/5 como VLAN nativa y procedemos a enceder las interface, debemos configurar el resto de los puertos como puertos de acceso y asignamos a la interface F0/6 la VLAN 21, pero fundamental apagar todos los puertos que no vallamos a utilizar.

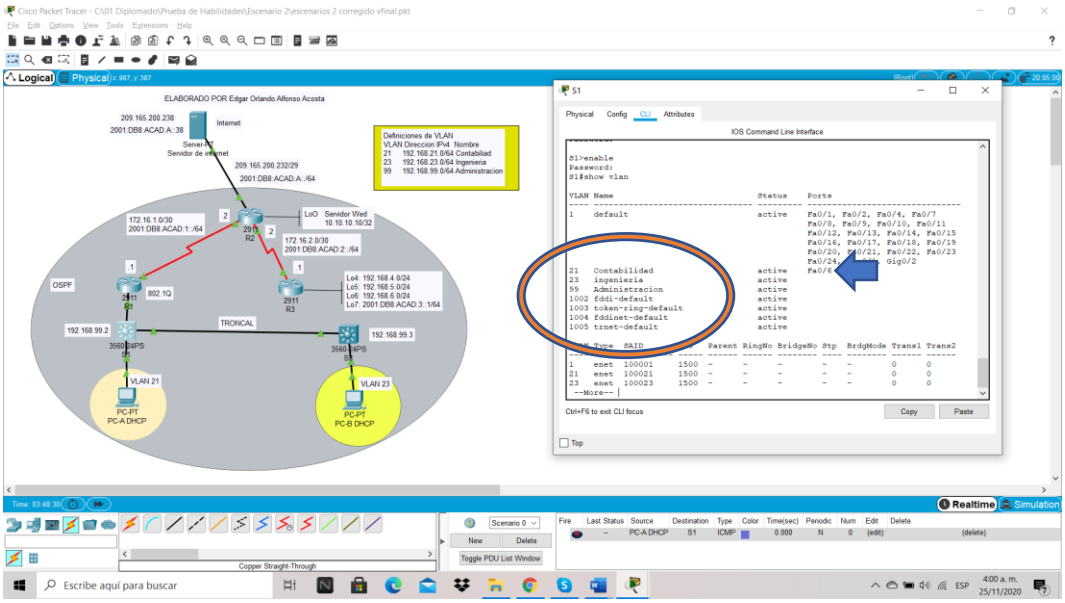
La configuración del S1 incluye las siguientes tareas:

Tabla 21. Configuración S1 escenario 2

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>enable Password: S1#configure terminal 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)#exit S1(config)#
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)#ip addres 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown S1(config-if)#
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config-if)#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#configure terminal S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#exit
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 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#no shutdown S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switch mode Access S1(config-if-range)#exit S1(config)#
Asignar F0/6 a la VLAN 21	S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switch mode Access S1(config-if-range)#exit S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit
Apagar todos los puertos sin usar	S1(config)#int range fa0/1-2, fa0/4, fa0/7-24, g0/1-2 S1(config-if-range)#shutdown

Figura 33. Configuración S1 escenario 2



Fuente: Autor.

Confirmación de Vlan creadas y asignación a la Int fa0/6 la Vlan 21

PASO 2: CONFIGURAR EL S3

De acuerdo al paso 1 procedo a dar una breve explicación del paso a paso de los comandos que se relacionaran en la tabla 20 para S3, aquí configuraremos las tres Vlan correspondientes a la 21, 23 y 99 con sus respectivos nombres, asignaremos la dirección IPv4 a la VLAN llamada administración previamente, asignaremos la dirección ip addres 192.168.99.3 y su respectiva puerta de enlace 192.168.99.1, posteriormente debemos forzar el enlace troncal en la interfaz F0/3 y el enlace troncal en la interfaz F0/5 como VLAN nativa y procedemos a en ceder las interface, debemos configurar el resto de los puertos como puertos de acceso y asignamos a la interface F0/18 a la VLAN 21, pero fundamental apagar todos los puertos que no vallamos a utilizar.

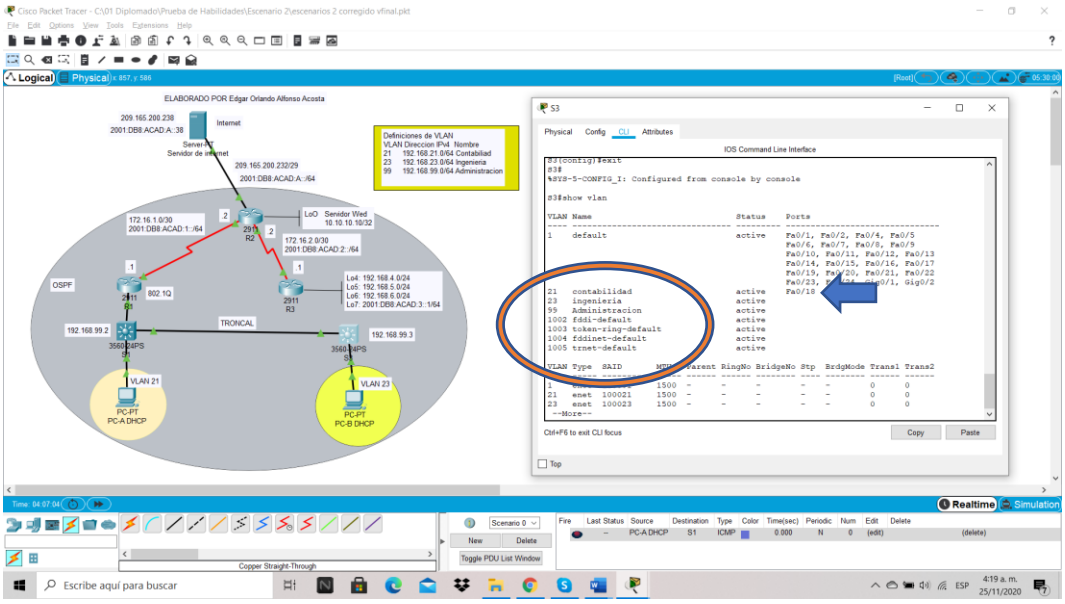
La configuración del S3 incluye las siguientes tareas:

Tabla 22. Configuración S3 escenario

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>enable Password: S3#configure terminal 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)#exit S3 (config)#
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 S1(config-if)# S3(config-if)#ip addres 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown S3(config-if)#
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config-if)#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#configure terminal S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#exit S3(config)#
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#int range fa0/1-2, fa0/4-24, g0/1-2 S3(config-if-range)#switch mode Access S3(config-if-range)#exit S3(config)#
Asignar F0/18 a la VLAN 21	S3(config-if)#interface f0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit S3(config)#exit

Figura 34. Configuración S3 escenario



Fuente: Autor.

Confirmación de Vlan creadas y asignación a la Int fa0/18 a la Vlan 21

PASO 3: CONFIGURAR R1

Entramos a los pasos de mucho cuidado para que los enlaces en piensen a tener comunicación, procedo a realizar una breve explicación del paso a paso; debemos ingresar a la configuración de la subinterfaz 802.1Q .21 en la G0/1 y asignamos una descripción correspondiente a la LAN de Contabilidad, donde vamos asignar a la VLAN 21 el encapsulamiento de dot1q, este protocolo dot1Q lo que hace, es básicamente, es modificar el paquete de información que estamos enviando, o en palabras técnicos la trama, así lo haremos para encapsular las Vlan 23 y 99, finalmente lo que haremos es Activar la interfaz G0/1.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 23. Configuración R1 escenario 2

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#configure terminal R1(config)#int g0/1.1 R1(config-subif)#description Contabilidad LAN R1(config-subif)#encapsulation dot1q 21 R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit

Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.2 R1(config-subif)#description Ingeniería LAN R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 R1(config)#int g0/1.3 R1(config-subif)#description Administración LAN R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int g0/1 R1(config-if)#no shutdown R1(config-subif)#exit R1(config)#exit

PASO 4: VERIFICAR LA CONECTIVIDAD DE LA RED

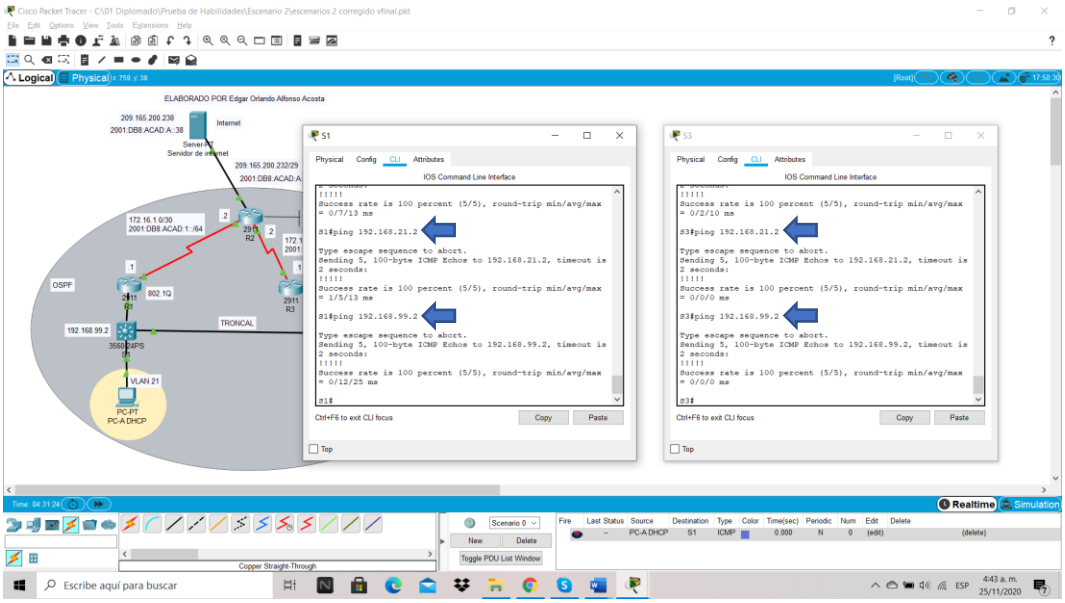
Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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

Tabla 24. Datos para verificar la conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	Satisfactorio
S3	R1, dirección VLAN 99	192.168.99.2	Satisfactorio
S1	R1, dirección VLAN 21	192.168.21.2	Satisfactorio
S3	R1, dirección VLAN 23	192.168.23.2	Satisfactorio

Figura 35. Verificar la conectividad de la red



Fuente: Autor.

Se Valida los direccionamientos mediante la opción de Ping a las direcciones R1, dirección VLAN 99,

PARTE 4. CONFIGURAR EL PROTOCOLO DE ROUTING DINÁMICO OSPF

En el siguiente paso 4 trabajaremos en el mismo R1 con el fin de configurar el protocolo de rounting dinámico OSDF.

PASO 1: CONFIGURAR OSPF EN EL R1

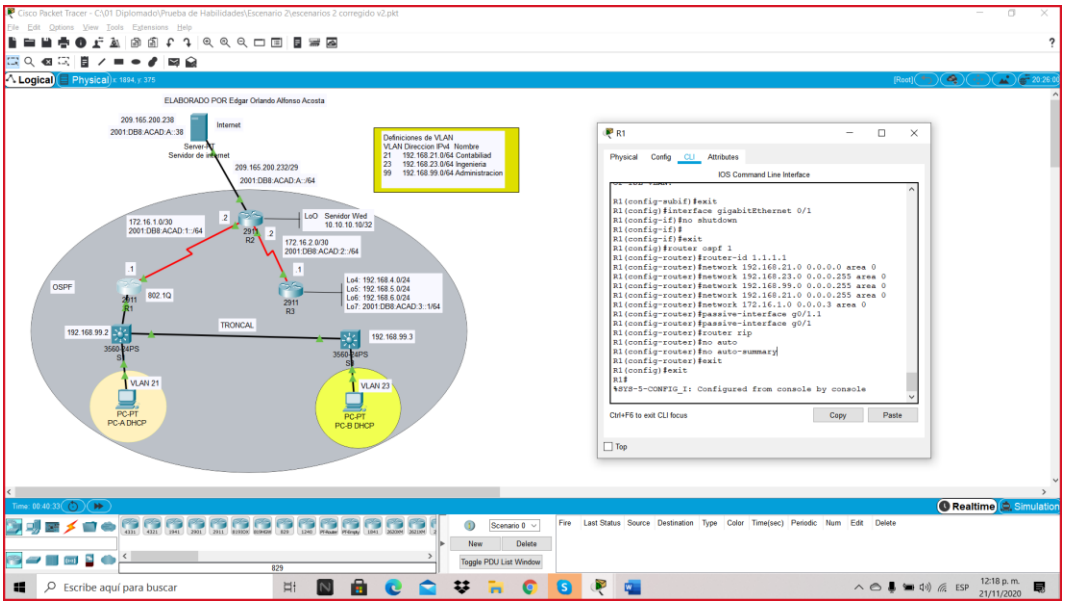
Para este paso vamos a explicar brevemente la configuración de R1 donde utilizaremos la configuración OSPF área 0, recordemos lo aprendido en cisco donde hay distintos tipos de routers OSPF y estos controlan el tráfico que entra a las áreas y sale de estas. Adicionalmente nos indica que los routers OSPF se categorizan según la función que cumplen en el dominio de routing, ahora bien con esta definición vamos anunciar las redes conectadas directamente, ingresando a configuración global de router asignándole a R1 el comando router-id 1.1.1.1 y posteriormente digitamos network con las cuatro dirección IP que la topología nos indica e identificando el área 0, proseguimos con establecer todas las interfaces LAN como pasivas tanto para interface g0/1.1como la interface g0/1 y finalmente desactivamos la sumarización automática. Ver los comando en la tabla 23.

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 25. Configuración OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#router-id 1.1.1.1 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 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 g0/1.1 R1(config-router)#passive-interface g0/1
Desactive la sumarización automática	R1(config-router)#router rip R1(config-router)#no auto R1(config-router)#no auto-summary

Figura 36. Configuración OSPF en el R1



Fuente: Autor.

Se da ingreso al R1 ingresamos a la interface 0/1 la prendemos y podemos observar el cargue del nombre ID del router con el fin de cargar en network las direcciones IP de área 0, dejamos la interface g0/1.1 y g0/1 como pasivas.

PASO 2: CONFIGURAR OSPF EN EL R2

Con la experiencia del paso anterior ingresamos a configuración global de router asignándole a R2 el comando router-id 2.2.2.2 y posteriormente digitamos network con las cuatro dirección IP que la topología nos indica e identificando el área 0, proseguimos con establecer todas las interfaces LAN como pasivas para la interface g0/1 y finalmente desactivamos la sumarización automática. Ver los comandos en la tabla 24.

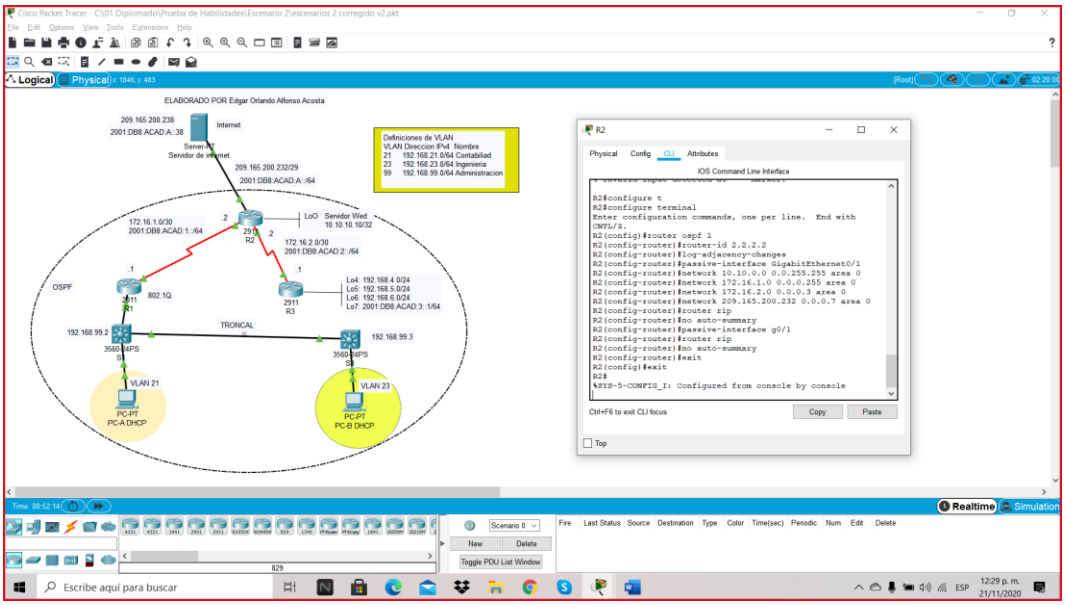
La configuración del R2 incluye las siguientes tareas:

Tabla 26. Configuración OSPF en el R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. Password: R2>enable Password: R2#configure terminal R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2 R2(config-router)#log-adjacency-changes R2(config-router)#passive-interface GigabitEthernet0/1 R2(config-router)#network 10.10.0.0 0.0.255.255 area 0 R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 209.165.200.232 0.0.0.7 area 0 R2(config-router)#router rip R2(config-router)#no auto-summary R2(config-router)#

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

Figura 37. Configuración OSPF en el R2



Fuente: Autor.

Se da ingreso al R2, ingresamos a la interfaz GigabitEthernet 0/1, observamos el cargue del nombre ID del router con el fin de cargar en network las direcciones IP de área 0, finalizamos dejando la interface g0/1 como pasiva y desactivando la sumarización automática.

PASO 3: CONFIGURAR OSPFV3 EN EL R2

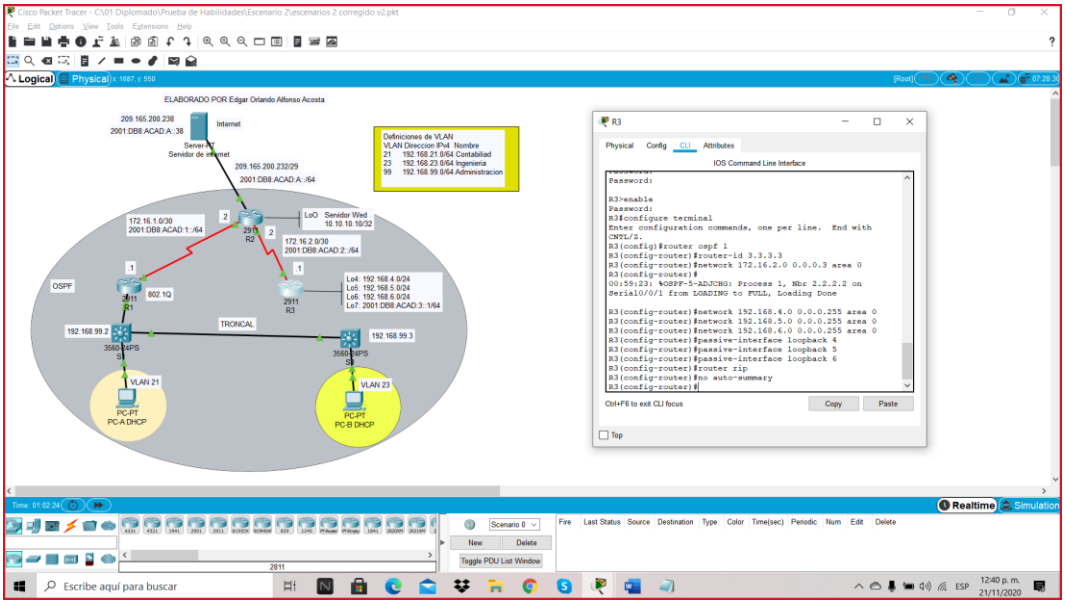
La configuración del R3 incluye las siguientes tareas:

Ya finalizando debemos seguir con algunos pasos similares realizado en R1 y R2 por lo que en R3 ingresamos a configuración global de router asignándole a R3 el comando router-id 3.3.3.3, recordemos que esta topología indica que los router se comunicaran por cable serial, en este caso será por el Serial0/0/1asignado las tres network con las dirección IP que la topología nos indica y el área 0, proseguimos a establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas, es decir desde loopback 4 a loopback 7 y finalizamos desactivando la sumarización automática. Ver los comandos en la tabla 25.

Tabla 27. Configuración OSPFv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)# 06:11:05: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1 from LOADING to FULL, Loading Done R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7
Desactive la sumarización automática.	R3(config-router)#router rip R3(config-router)#no auto-summary R3(config-router)#

Figura 38. Configuración OSPFv3 en el R2



Fuente: Autor.

Podemos dar por finalizado observando la figura 38 donde en R3, ingresamos con el comando router-id 3.3.3.3 asignamos el network 172.16.2.0 0.0.0.3 área 0, para poder anunciar redes IPv4 conectadas directamente.

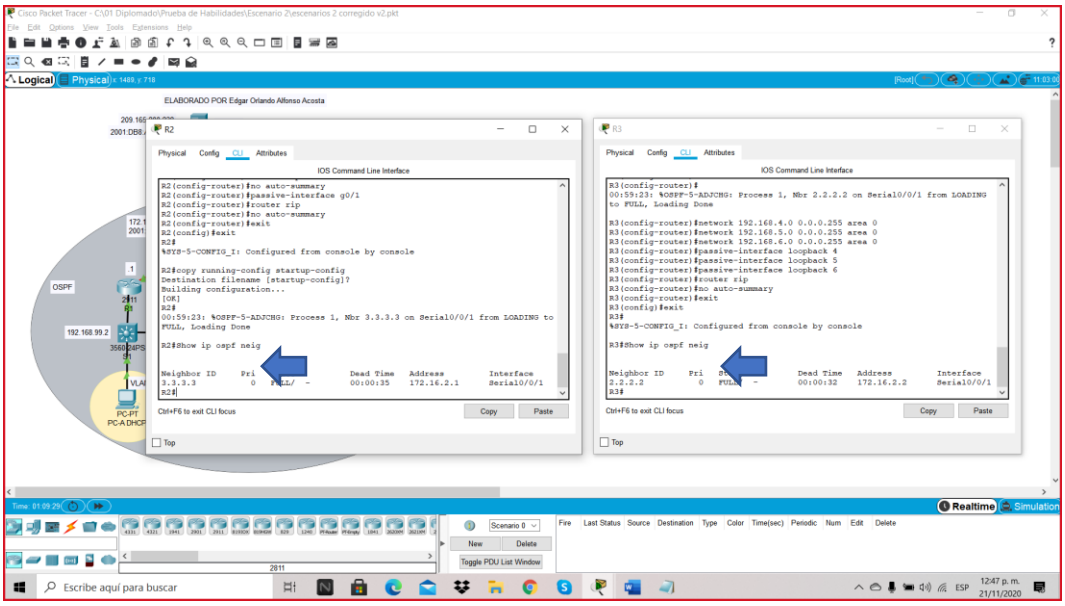
PASO 4: VERIFICAR LA INFORMACIÓN DE OSPF

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

Tabla 28. Verificación información de 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?	Show ip ospf neig
¿Qué comando muestra solo las rutas OSPF?	Show ip ospf interface
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip protocols

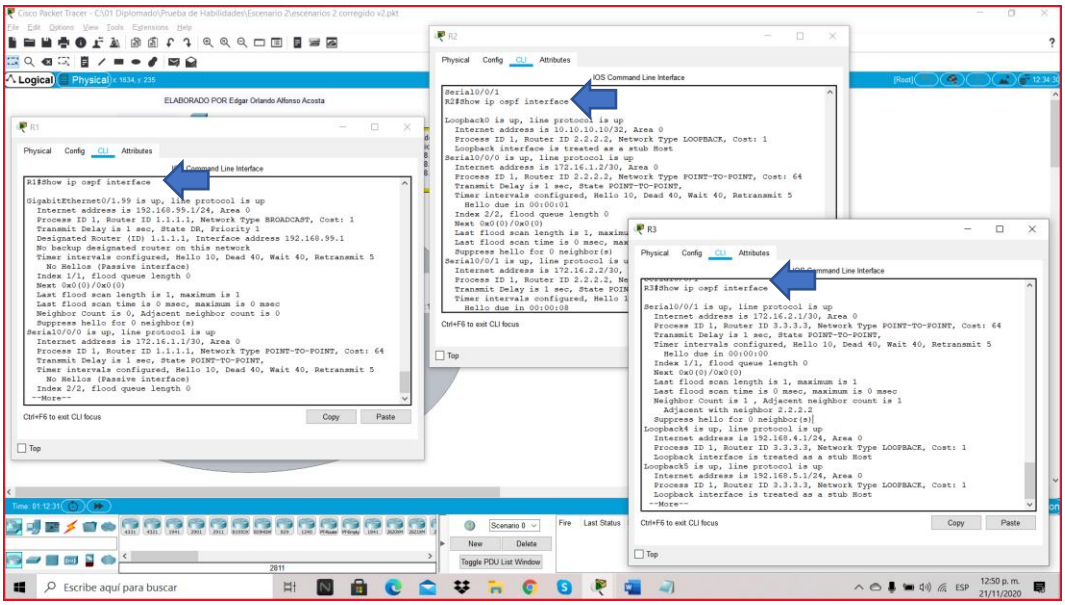
Figura 39. Verificación información de OSPF comando Show ip ospf neig



Fuente: Autor.

Podemos observar el comando **Show ip ospf neig** en R2 y R3 para mostrar la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router.

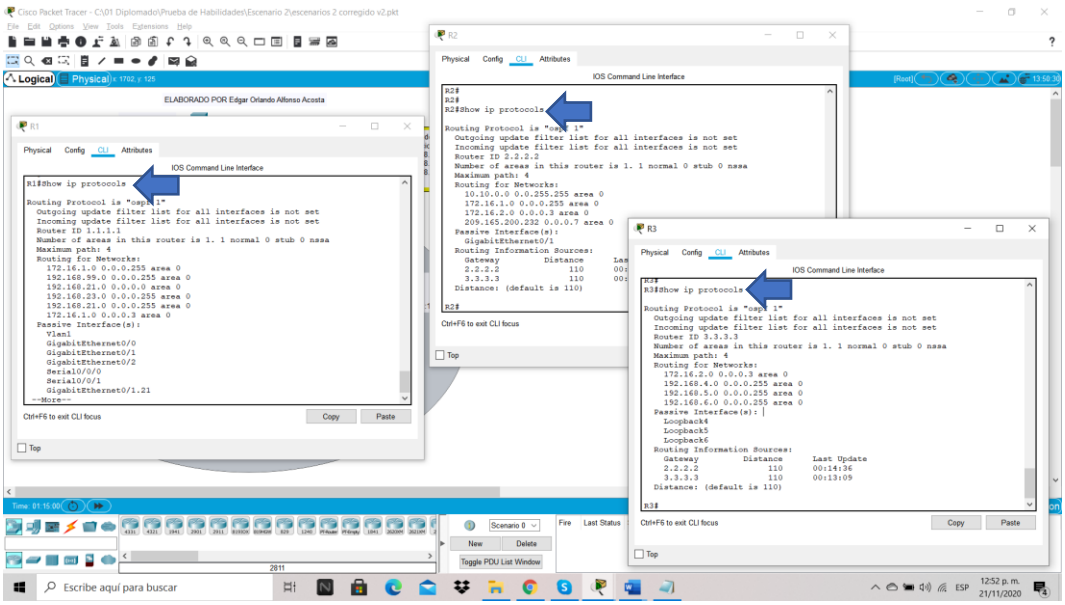
Figura 40. Verificación información de OSPF comando Show ip ospf interface



Fuente: Autor.

Podemos observar el comando **Show ip ospf interface** en R1, R2 y R3 para mostrar solo las rutas OSPF.

Figura 41. Verificación información de OSPF comando Show ip protocols



Fuente: Autor.

Podemos observar el comando **Show ip protocols** en R1, R2 y R3 para mostrar la sección de OSPF de la configuración en ejecución.

PARTE 5. IMPLEMENTAR DHCP Y NAT PARA IPV4

PASO 1: CONFIGURAR EL R1 COMO SERVIDOR DE DHCP PARA LAS VLAN 21 Y 23

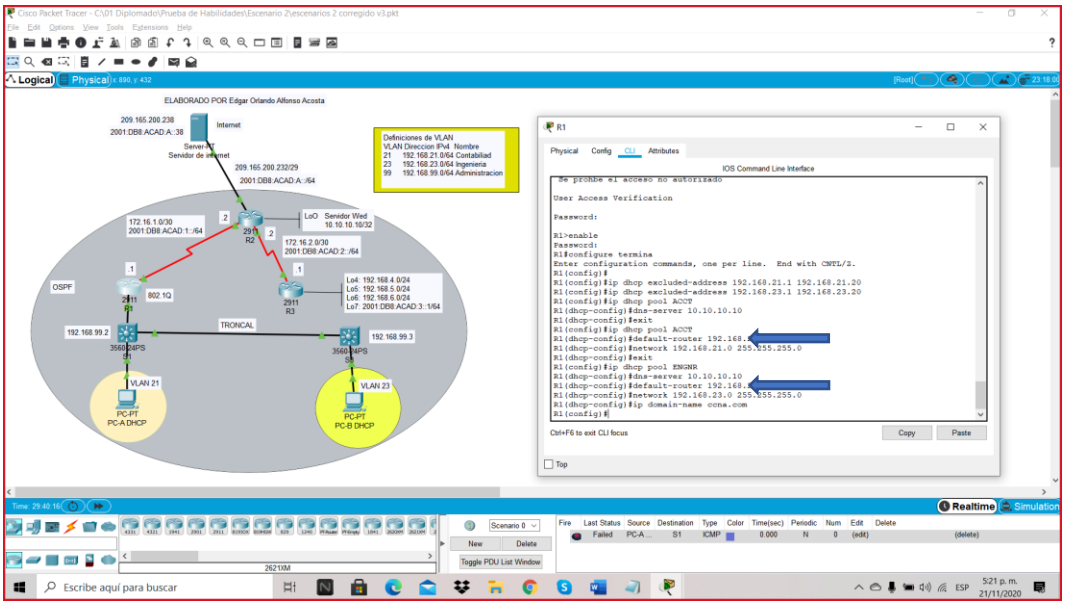
Las tareas de configuración para R1 incluyen las siguientes:

Daré una breve descripción del paso 1 de la parte 5 donde implementaremos DHCP y NAT para IPv4, en R1 entramos a configuración privilegiado vamos a reservar las primeras 20 direcciones IP en la Vlan 21 pero estáticas, esto será viable con el comando)#ip dhcp excluded-address 192.168.21.1 192.168.21.20, también vamos a reservar las primeras 20 direcciones IP en la Vlan 23 con el comando)#ip dhcp excluded-address 192.168.23.1 192.168.23.20, es preciso configurar un pool de DHCP para la VLAN 21 y esta tarea la haremos en R1 dando el nombre de ACCT, asignando al servidor DNS: la dirección 10.10.10.10, nombrando el dominio como ccna-sa.com y establecer el gateway predeterminado.

Tabla 29. Configuración R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(config)#ip dhcp pool ACCT R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#ip domain-name ccna.com
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#ip domain-name ccna.com

Figura 42. Configuración R1 como servidor de DHCP para las VLAN 21 y 23



Fuente: Autor.

Proceso de DHCP y NAT para IPv4, en R1 y para las VLAN 21 y 23

PASO 2: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Veremos en esta descripción el paso 2 donde implementaremos NAT estática y dinámica en el para R2, por lo que crearemos una base de datos local con una cuenta de usuario, con nombre, contraseña y nivel de privilegio 15, no podemos en este caso habilitar el servicio del servidor HTTP porque el router que estamos trabajando no aplica para simulaciones en packet tracer, de todas maneras vamos a Configurar el servidor HTTP para utilizar la base de datos local para la autenticación, seguidamente creamos una NAT estática al servidor web con la dirección global interna: 209.165.200.229, por lo que es fundamental asignar la interfaz interna y externa para la NAT estática con el comando)#ip nat inside source static 10.10.10.10 209.165.200.229, luego procedemos a configurar la NAT dinámica dentro de una ACL privada y definimos la traducción de NAT dinámica que es Show ip nat statistics.

Tabla 30. Configuración NAT estática y dinámica en el R2

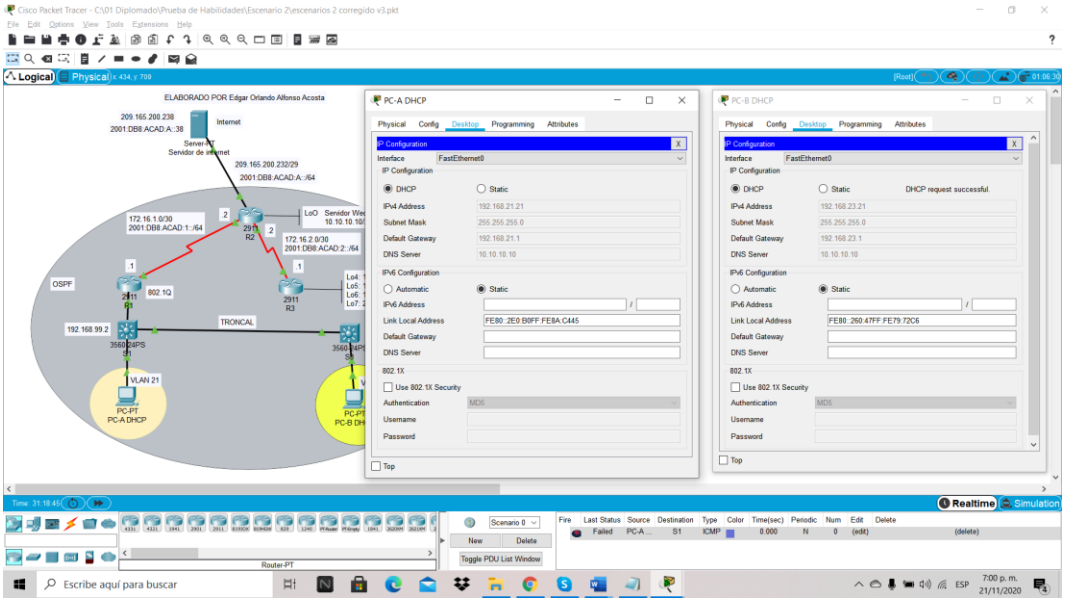
Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#user webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	No Aplica equipos de simulación
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.99.0 0.0.0.255
Crear una NAT estática al servidor web.	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 R2(config)#access-list 100 permit tcp any host 209.165.200.229 eq www R2(config)#access-list 100 permit icmp any any
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	Show ip nat statistics

PASO 3: VERIFICAR EL PROTOCOLO DHCP Y LA NAT ESTÁTICA

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

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Se carga la información de forma automática ver resultados en la figura 43.
Verificar que la PC-B haya adquirido información de IP del servidor de DHCP	Se carga la información de forma automática ver resultados en la figura 43.
Verificar que la PC-A pueda hacer ping a la PC-B **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Pinging 192.168.21.22 Exitoso Ver figura 44
Verificar que la PC-A pueda hacer ping a la PC-B **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Pinging 192.168.21.21. Exitoso Ver figura 44
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**	Se puede ingresar al navegador Web pero dentro de la configuración del usuario y contraseña no la pide. Ver figura 45

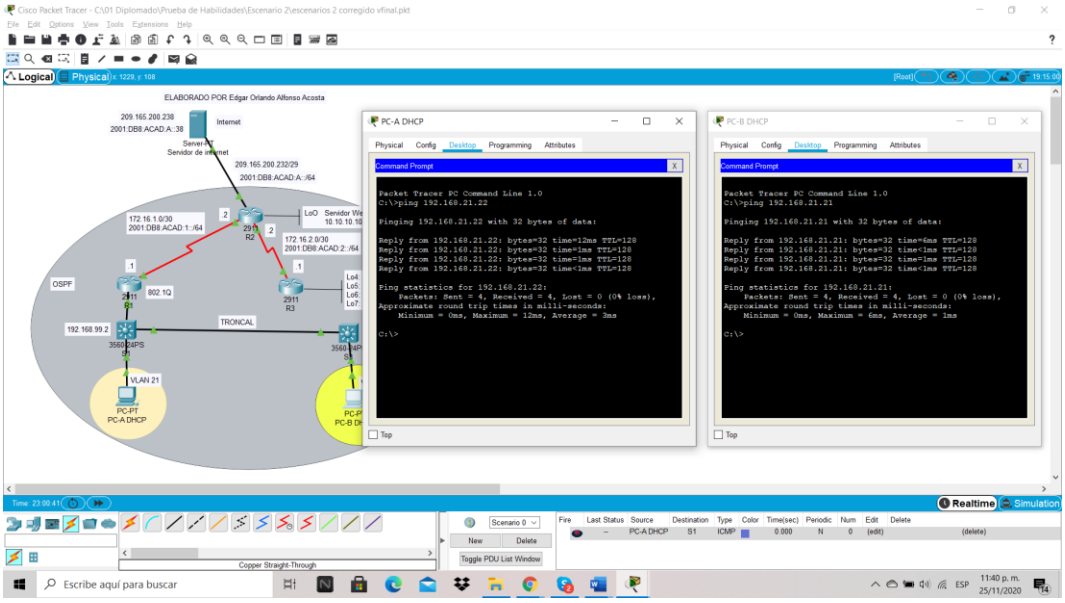
Figura 43. Verificación PC-A con información de IP del servidor de DHCP



Fuente: Autor.

Evidencia que la PC-A y PC-B adquirido información de IP del servidor de DHCP.

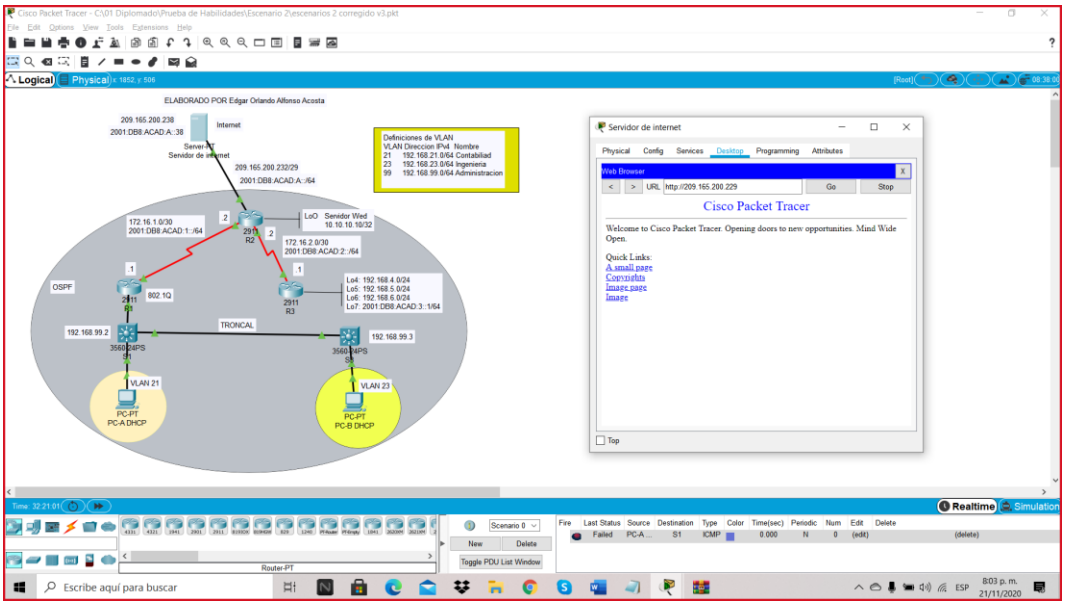
Figura 44. Verificación que la PC-A pueda hacer ping a la PC-B



Fuente: Autor.

Confirmación que el ping desde PC-A a PC-B responde los cuatro paquetes y desde PC-B a PC-A responde satisfactoriamente los cuatro paquetes.

Figura 45. Navegador web accede al servidor web (209.165.200.229)



Fuente: Autor.

Se muestra en la figura 45 que mediante el servidor web de Internet tenemos acceso a cisco packet tracer, para esta prueba se cambia en el servidor web la dirección IP original 209.165.200.238 a 209.165.200.229 y así Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345.

PARTE 6. CONFIGURAR NTP

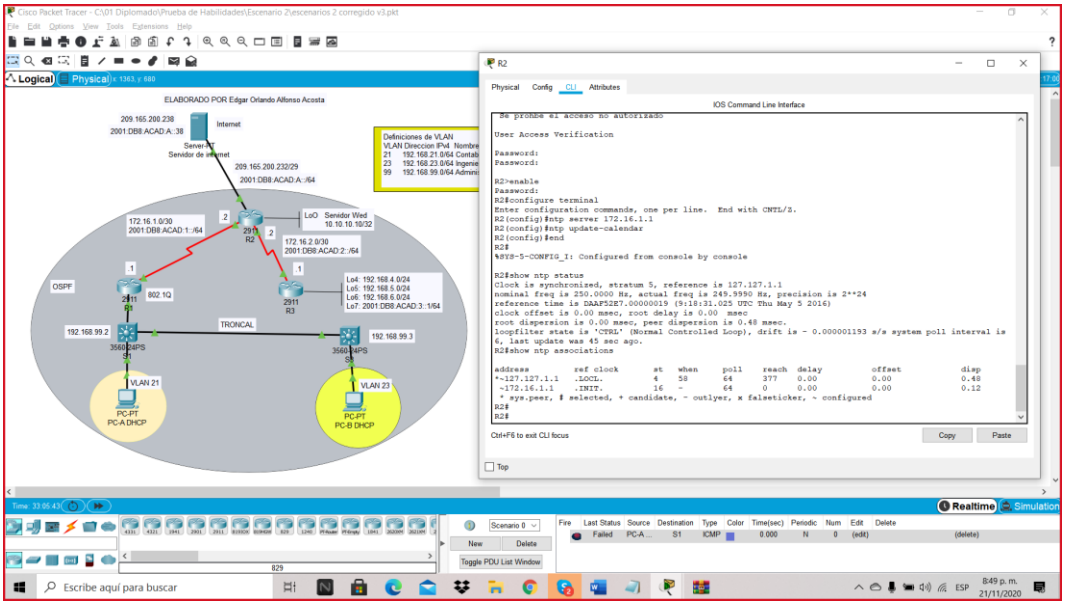
En la parte 6 en R2 ingresamos de modo privilegiado, ajustamos la fecha, hora, maestro NTP, cliente NTP y actualizamos el calendario con la hora NTP.

Tabla 31. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#clock set 09:00:00 may 05 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R2(config)#ntp server 172.16.1.1
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R2(config)#ntp update-calendar R2(config)#end

Verifique la configuración de NTP en R1	R2#show ntp status R2#show ntp associations

Figura 46. Configuración NTP



Fuente: Autor.

En la figura se muestra el modo privilegiado de acceso en R2, con el ajuste de la fecha, hora, maestro NTP, cliente NTP y actualizamos el calendario con la hora NTP.

PARTE 7. CONFIGURAR Y VERIFICAR LAS LISTAS DE CONTROL DE ACCESO (ACL)

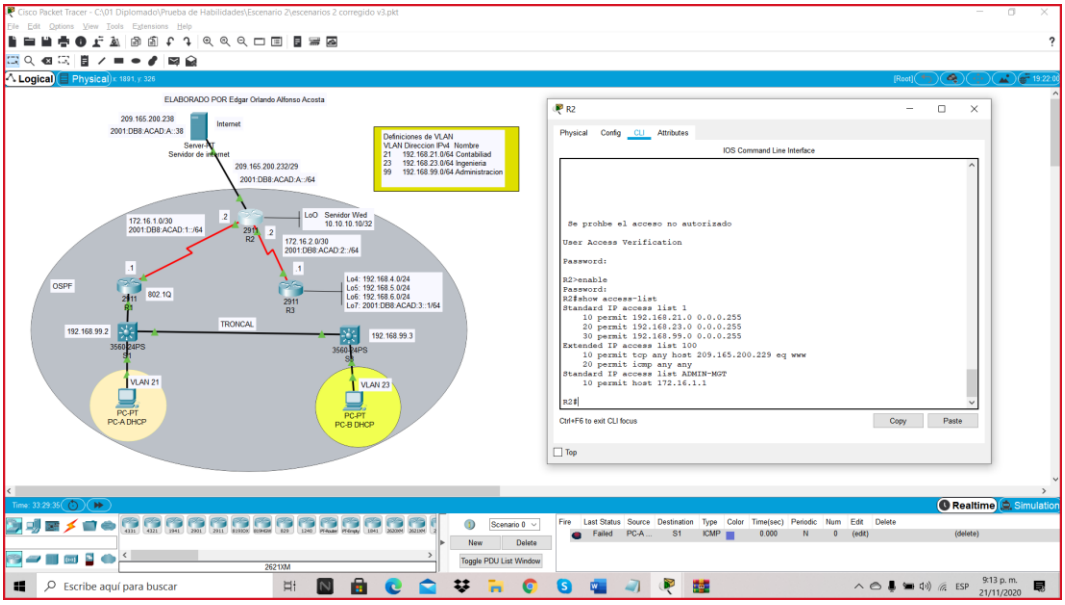
PASO 1: RESTRINGIR EL ACCESO A LAS LÍNEAS VTY EN EL R2

Veremos una pequeña descripción del paso a paso de la tabla 47, para restringir el acceso a las líneas VTY en el Router número dos, primero tenemos configurar la lista de acceso con un nombre y así permitir que solo el router numero uno establezca una conexión Telnet con router número dos, esto se hace con el comando de acceso privilegiado **ip access-list** y luego con el comando en acceso global demos **permit host** apuntándole a la dirección 172.16.1.1, ahora debemos aplicar la ACL con nombre a las líneas VTY el cual corresponde a **access-class ADMIN-MGT in,** seguidamente permitimos el acceso por Telnet a las líneas de VTY.

Figura 47. Restricción el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line VTY 0 15 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line VTY 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#end
Verificar que la ACL funcione como se espera	Ver figura 48 Función esperada satistactoria.

Figura 48. Restricción acceso a las líneas VTY en el R2



Fuente: Autor.

Con el comando show access-list se muestran las listas de acceso

PASO 2: INTRODUCIR EL COMANDO DE CLI ADECUADO QUE SE NECESITA PARA MOSTRAR LO SIGUIENTE.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Router#show access-lists
Restablecer los contadores de una lista de acceso	(config)#ip access-list standard 2 (config-std-nacl)#18 permit 172.22.1.1 (config-std-nacl)#exit
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Router#show ip nat translations
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-B 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-B, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. Router# show ip nat statistics
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Router#clear ip nat translation *

CONCLUSIONES

En el primer escenario de trabajo de habilidades podemos concluir que con la práctica interiorizamos temas de configuraciones de los dispositivos como si estuviéramos creando una red pequeña en la vida real. Estos pasos nos dan destreza en la configuración básica de un router, un switch y host, a su vez tuvimos la oportunidad de conocer el proceso y diferencia entre direccionamientos IPv4 e IPv6. Es importante reconocer que hoy no tenemos la practica suficiente para realizar los pasos con suficiente agilidad, pero debemos continuar repasando hasta que nuestro cerebro interiorice los temas y los conceptos propuestos. Finalmente, en este escenario identificamos y solucionamos el problema propio de enrutamiento mediante el uso adecuado de estrategias basadas en comandos IOS y de tráfico en las interfaces.

En el Segundo escenario de trabajo de habilidades, más complejo que el primer escenario, se concluye que el ejercicio está encaminado a entender pasos importantes en la solución de problemas relacionados con diversos aspectos de Networking, entre ellos es claro entender la forma esquemática de una red, las definiciones de Vlan se implementaron para comprender la vlan nativa que es usada para todo el tráfico sin etiqueta del enlace troncal y puede ser recibida en un puerto configurado con el 802.1Q.

Se comprende las capas de red la cual nos proporciona conectividad y selección de ruta entre dos sistemas de hosts, comprendí la creación de contraseñas para accesos no autorizados, la configuración de puertos, la activación de interfaz, la configuración de OSPF y muchos pasos de suma importancia que al momento de configurar una red, extienden valor y en principio cada paso está asociado en forma de cadena para proteger aspectos de Networking.

Como aspecto general de conclusión, los comandos que se requieren para poder configurar una red y conocidos en Packet Tracer, son de fácil aprendizaje para poder ejecutarlos en el paso a paso de las configuraciones ya sean de usuario, privilegiado o global, aunque se utilizan palabras en ingles son bastante comunes a nivel de aprendizaje.

BIBLIOGRAFIA

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

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

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

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

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

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

CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

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

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

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

CISCO. (2019). Redes Conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

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

UNAD (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

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

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167

ANEXOS

Anexo 1 Link Descarga Escenario 1

https://drive.google.com/file/d/1_RL9PYciQHfYYsl5qY8SoR5Tr4cNfoZK/view?usp=sharing

Anexo 2 Link Descarga Escenario 2

https://drive.google.com/file/d/1auiRTN9ODMk33R0236DtGfoL0U0nB5V5/view?usp=sharing

Anexo 3 Link Articulo Científico

https://drive.google.com/file/d/17ECCN0UUn81Yx7Vl_ksXJ-QaB1FZpf8l/view?usp=sharing