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

FREDY ARMANDO ACOSTA HERNANDEZ

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

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

FREDY ARMANDO ACOSTA HERNANDEZ

Diplomado de opción de grado presentado para
Optar el título de Ingeniero de Telecomunicaciones

Asesor:
Diego Edinson Ramírez

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

BOGOTA, 25 de noviembre de 2020

AGRADECIMIENTOS

Le agradezco a Dios por la vida y los sueños cumplidos, las fuerzas para seguir adelante, luego a mi familia especialmente a mi esposa y mi bebe que me han apoyado incondicionalmente en este proceso, que son la motivación de mi vida.

Gracias a la universidad UNAD por guiarme en todo este proceso, con excelentes tutores que influyen en nuestro exitoso futuro profesional.

A mis compañeros de estudio que de alguna u otra manera realizaron este proceso para terminar la carrera.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CISCO: Cisco Systems es una empresa tecnológica multinacional, fundada en 1984, con base en San José (California) en Silicon Valley. Su negocio está basado en la fabricación y venta de dispositivos de red, equipos de telecomunicaciones y algunos otros servicios y productos de Tecnología.

En 1990 Cisco comenzó a cotizar en bolsa, en el NASDAQ, y se comenzó a convertirse en una de las empresas más grandes de su sector. No fue la única compañía que se dedicaba a fabricar y vender dispositivos de red, pero lo que le permitió destacar fue la capacidad de fabricar dispositivos que manejaban varios protocolos en un mismo dispositivo, gracias a Cisco IOS, y a sus múltiples y constantes actualizaciones.

Entre 1992 y 1994, Cisco Systems compró varias empresas que fabricaban dispositivos Ethernet como Kalpana o Crescendo Communications, lo que les permitió crear la unidad de negocio tan exitosa hasta el día de hoy llamada Cisco Catalyst.

Durante sus más de 30 años de historia, los productos que ha comercializado o sigue haciéndolo, es realmente inmensa. Vamos a resumir algunas de las más importantes o interesantes en cada área de tecnología:

- Redes: switches (Catalyst 2960 o serie 9000), routers (ISR 1000 o ISR 4000), dispositivos inalámbricos (Aironet 4800 o Catalyst 9800), gestión de redes (Cisco DNA Server), redes de fibra óptica, …

- Seguridad: Cloud Security (Cloudlock o Umbrella), EndPoint Security (Security Connector o ASA), Firewall (Cisco 3000 o Firepower 9000), Gestión de la Seguridad (Security Manager o Defense Orquestrator), …

- Colaboración: Comunicaciones Unificadas (Webex Teams o Cisco Cloud), Centro de Contacto (Unified Contact Center), Conferencias (Webex o Meeting Server) y Terminales (teléfonos IP o Webex Board)

- DataCenter: Redes (Cisco ONE o redes de almacenamiento), Cómputo y Almacenamiento (almacenamiento por software o servidores unified computing), Análisis (AppDynamics o Análisis de Data Center), Automatización y Nube Híbrida (Cloud Center o Enterprise Cloud Suite)

- Internet Of Things, Software, Vídeo y muchas cosas más… (redesTeleco, s.f.)

ROUTER: Un router recibe y envía datos en redes informáticas. Los routers a veces se confunden con los concentradores de red, los módems o los switch de red. No obstante, los routers pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales.

Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.
Los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino. El router lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión. (htt; CISCO, s.f.)

SWICHT: dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch no proporciona por si solo conectividad con otras redes, y obviamente, TAMPOCO proporciona conectividad con Internet. Para ello es necesario un router. (González, 2013)

VLAN: Una red de área local virtual (Virtual Local Area Network o VLAN) es **un** segmento lógico más pequeño dentro de una gran red física cableada. Las diferentes estaciones se combinan en una solución de red independiente de su ubicación: siempre que estén conectadas entre sí en la misma LAN, es posible combinarlas mediante una VLAN. No supone ningún problema que la LAN abarque varios switches. Lo único importante es que el switch también sea compatible con la VLAN. La única manera de crear VLAN es utilizando switches gestionables (Managed Switches).

Cada VLAN individual recibe su propio dominio de difusión o dominio de broadcast**.** Si un participante envía una difusión dentro de la VLAN, todos los demás participantes de ese segmento (y solo esos participantes) reciben el mensaje. La difusión no se transmite más allá de los límites de la red virtual. La comunicación entre diferentes VLAN se produce a veces utilizando los mismos cables. (IONOS, 2019)

INTERFAZ: En el campo de la informática, el término interfaz se emplea para nombrar a la conexión funcional que existe entre dos programas, sistemas o dispositivos, que brinda una comunicación de diversos niveles, haciendo posible un

intercambio de información. Existen dos tipos de interfaces: las interfaces de usuario y las interfaces físicas. (conceptodefinicion.de, 2019)

RESUMEN

Diplomado CCNA CISCO profundiza los conocimientos en Switch, Router, manipulación y manejo de Packet Tracer. En el presente Trabajo grado se realiza una simulación en la herramienta Packet Tracer que nos permite validar los dos escenarios LAN.

El desarrollo de la guía me permite demostrar conocimientos en conexiones y comandos de los diferentes dispositivos y así ganar destreza en cuanto aprendizaje a configuración de interfaces y VLAN.

Donde se desarrollan dos escenarios con sus elementos como lo son Routers, Switch y PC, donde se realizan las configuraciones de las interfaces de cada elemento. Al final se realizan las pruebas con un ping de cada equipo, y de esta manera confirmar si está bien la configuración realizada.

Palabras Clave: CISCO, CCNA, Enrutamiento, Nat, Ospf, Redes LAN.

ABSTRACT

Diploma CCNA CISCO deepens knowledge in Switch, Router, manipulation and management of Packet Tracer. In this project a simulation is carried out in the Packet Tracer tool that allows us to validate the scenario in LAN.

The development of the guide allows me to demonstrate knowledge in connections and commands of the different devices and thus gain skill in terms of learning to configure interfaces and VLANs.

Where two scenarios are developed with their elements such as Routers, Switch and PC, where the configurations of the interfaces of each element are made. At the end, the tests are carried out with a ping from each computer, and in this way confirm if the configuration is correct.

Keywords: CISCO, CCNA, Routing, Nat, Ospf, Networks LAN.

INTRODUCCIÓN

El presente trabajo se realizó con el fin de afianzar conocimientos en topología de Red LAN, donde se configuran dos tipos de escenarios cada uno con sus dispositivos como Routers y Switch, y equipos, aplicando direccionamientos IPV4 y IPV6 también implementando la seguridad de switch, y routing entre VLAN, se configuro los protocolos de routing dinámico OSPF, y a hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Donde se probará y registrará la red mediante los comandos comunes de CLI.

OBJETIVOS

1.1 Objeto General

Configuración de dos redes el escenario uno y dos aplicando los conocimientos adquiridos en el Diplomado CCNA.

1.2 Objetivos específicos:

Realizar las configuraciones de las redes por medio del software Packet Tracer Router y Switch en el escenario uno y dos.

- Configurar interfaces entre Switch y Router
- Validación de conectividad entre los equipos
- Verificar en cada escenario los resultados obtenidos

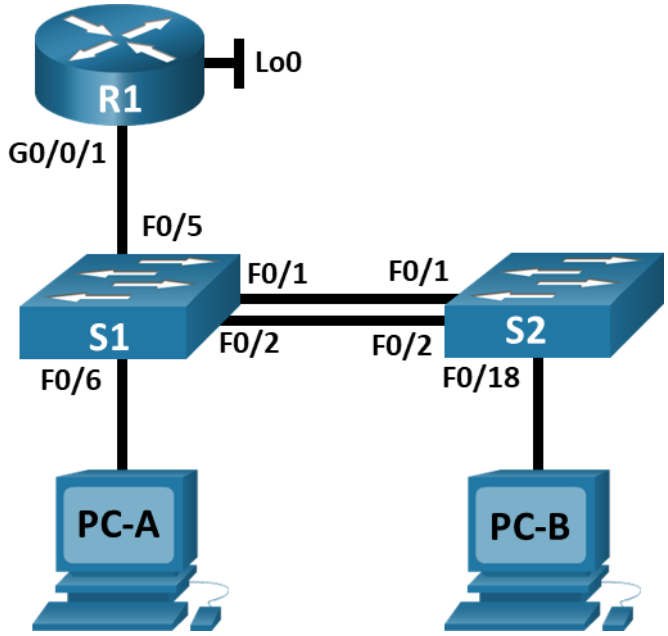
DESARROLLO DE LOS ESCENARIOS PARA LA PRUEBA DE HABILIDADES

1 ESCENARIO 1

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un Reuter, dos switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El Router y el Switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

1.1 TOPOLOGIA

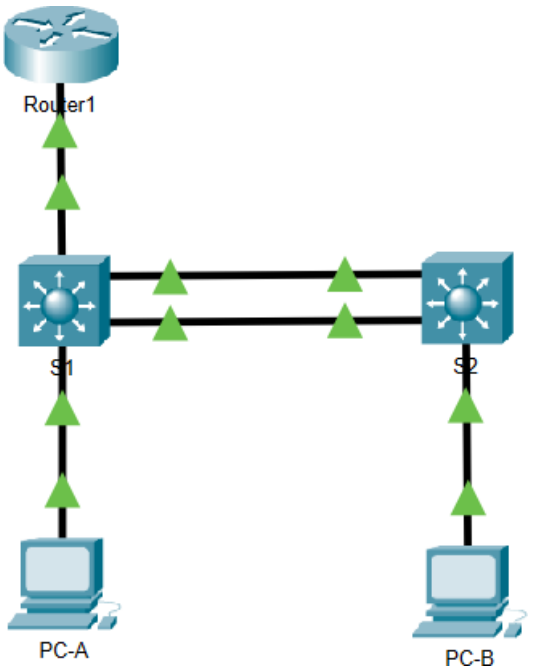
Figura 1: Topología escenario 1



Fuente documento del repositorio

En este primer escenario configuramos los dispositivos de una red pequeña utilizando los elementos como son un Router, dos Switch y dos PC, como lo podemos observar en la siguiente figura.

Figura 2 Montaje escenario 1



Fuente: Autor

Tabla Configuración VLAN
Configuración de Vlan agregándole un nombre a cada una para su identificación

Tabla 1. Configuración VLAN

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

Tabla de asignación de direcciones
Validar la siguiente tabla los dispositivos interfaz y el direccionamiento IP.

En esta tabla observamos la configuración para cada dispositivo realizado en el escenario uno.

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

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

1.2 Instrucciones

1.2.1 Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

1.2.2 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.

Inicializar el Router y volver a cargar

Conectarse al Router
Acceda al Router mediante el puerto de consola e ingrese al modo EXEC privilegiado con el comando enable.

Router>enable
Router#

Eliminar el archivo de configuración de inicio de la NVRAM

Utilizamos el comando erase startup-config para eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM)

A continuación, realizaremos los pasos mencionados anteriormente accediendo al Router para realizar las configuraciones como lo podemos observar en la siguiente tabla.

Escribiendo los siguientes comandos mostrado en las siguientes tareas.

Configuración del Router

Tabla 3. Configuración en R1

Tarea	Comando
Acceda al Router mediante el puerto de consola e ingrese al modo EXEC privilegiado con el comando enable.	Router>enable //Ingreso a modo privilegiado Router#

Borrar el archivo con el siguiente comando startup-config en el router.
 	
//Elimina configuración inicio
	Router>enable //Ingreso a modo privilegiado
	Router#configure terminal //Ingreso a modo de configuración
	Enter configuration commands, one per line. End with CNTL/Z.
	Router(config)#hostname R1 //Asigno nombre al router
	R1(config)#end
	R1#
	R1#erase startup-config //Elimina configuración inicio

Carga el router. Utilizamos el comando reload para eliminar una antigua configuración de la memoria. Cuando reciba el mensaje proceed with reload (continuar con la carga) presionando enter, si se presiona cualquier otra tecla, se anulará la recarga.	Router#reload //Elimina antigua configuración, cuando reciba mensaje

Inicializar el Switch S1 y S2 volver a cargar

Switch S1 y S2
Conectarse al Switch
Accedemos a cada Switch mediante el puerto de consola ingresando al modo EXEC privilegiado. Escribiendo el siguiente comando mostrado en las siguientes tareas.

Tabla 4. Configuración Switch S1 y S2

Tarea	Comando
Switch S1 y S2 Realizamos la configuración	Switch>enable //Ingreso a modo privilegiado Switch# //Ingreso a modo de configuración S1(config)#hostname S1 //Asigno nombre al Switch

	S2(config)#hostname S2 //Asigno nombre al Switch
Determinar si se crearon redes de área local virtuales (VLan, Virtual Local-Área Networks) Utilizamos el siguiente comando **Show flash**	S1#show flash //Determina si hay creación de alguna red de área local virtual Vlan
Verificación comando delete vlan.dat. Como podemos observar no se encontró ningún archivo Vlan.dat para eliminar, si se hubiese encontrado se debe eliminar escribiendo el comando delete vlan.dat dando enter le sale una pregunta si lo quiere eliminarlo realice la prueba escribiéndolo me muestra lo siguiente:	S1#delete vlan.dat //Comando eliminar vlan.dat Delete filename [vlan.dat]? //Donde sale la pregunta si quiere eliminarlo Delete flash:/vlan.dat? [confirm] //le da enter para confirmar //Luego de lo anterior seguimos para el siguiente paso
Borrar el archivo de configuración de inicio en cada Switch. Utilizamos el comando erase startup-config para eliminar la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM)	*S1#erase startup-config* ***//****Elimina configuración inicio* *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] // Confirmamos dando enter*
Recargamos cada Switch Utilizamos el comando reload para eliminar toda información de configuración antigua de la memoria. Cuando reciba el mensaje proceed with reload (continuar con la carga) presionando enter, si se presiona cualquier otra tecla, se anulará la recarga.	S1#reload Proceed with reload? [confirm] //Le damos entrar Se omite el dialogo de configuración inicial, escribimos no y presionamos entrar *% Please answer 'yes' or 'no'.* *Would you like to enter the initial configuration dialog? [yes/no]: no*

Switch S1 y S2
El Switch 3560 tiene una característica llamada Switch Database Management (SDM). SDM ayuda al conmutador a administrar la asignación de recursos de cada característica.

Con el comando show sdm prefer
La plantilla actual es “desktop default”. La plantilla seleccionada optimiza los recursos en el Switch para soportar.

Tabla 5. Revisión de Plantilla determinada S1 y S2

Tarea	Comando
Verificar la plantilla predeterminada en cada Switch S1 y S2	S1#show sdm prefer //comando revisar la plantilla determinada en el S1 y S2 The current template is "desktop default" template.
Se carga la plantilla del sdm en el Switch para que funcione todo el enrutamiento de IPV6.	Switch#show sdm prefer The current template is "desktop default" template. The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs. number of unicast mac addresses: 6K number of IPv4 IGMP groups + multicast routes: 1K number of IPv4 unicast routes: 8K number of directly-connected IPv4 hosts: 6K number of indirect IPv4 routes: 2K number of IPv4 policy based routing aces: 0 number of IPv4/MAC qos aces: 0.5K number of IPv4/MAC security aces: 1K
Selección de plantilla. Seleccionara para S1 y S2 Plantilla dual-Ipv4-e-IPv6 Así que elegiremos esta plantilla entre varias que muestra el sistema escribimos el siguiente comando sdm prefer dual-ipv4-and-ipv6 default le damos Enter.	S1#config terminal S1(config)#sdm prefer dual-ipv4-and-ipv6 default //Comando seleccionar plantilla S1(config)# S1#copy run start // copiar ejecutar iniciar Destination filename [startup-config]? Building configuration... Building configuration... [OK]
Luego cargamos nuevamente el S1 y S2	Switch#reload //reinicia y carga nuevamente

Escribiendo el comando Reload Utilizamos el comando reload para eliminar toda información de configuración antigua de la memoria. Cuando reciba el mensaje proceed with reload (continuar con la carga) presionando enter, si se presiona cualquier otra tecla, se anulara la recarga.	System configuration has been modified. Save? [yes/no]:no // Escribimos no le damos enter //Se omite el dialogo de configuración inicial, escribimos no y presionamos entrar

1.2.3 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Realizamos en R1 desactivar la búsqueda de los DNS, le configuramos el nombre al Router, le ponemos nombre al dominio, se configuran las contraseñas para modo privilegiado y para la consola, se establece la longitud mínima para las contraseñas de 10 caracteres, Creamos un usuario administrativo en la base de datos local.

Configuramos el inicio de sesión en las líneas VTY, Cifremos las contraseñas de texto no cifrado, Configure un MOTD Banner como un mensaje de advertencia para alguna persona ajena que quiera ingresar, luego habilitamos con un comando la IPv6, se configura la interfaz G0/0/1 y subinterfaces, también configuramos el Loopback0 interface, y por último Generar una clave de cifrado RSA, así terminando la configuración en R1 como lo podemos observar en las siguientes tareas.

Configuración del Router

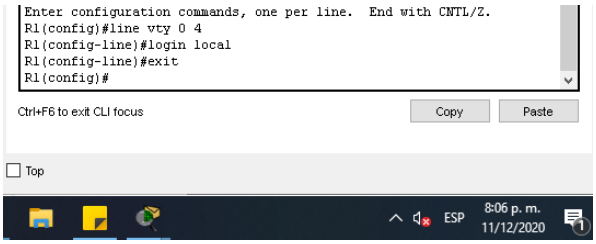
Tabla 6. Configuración en el R1

Tarea	Especificación
Desactivar la búsqueda DNS. Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando exitoso sólo devolverá al indicador "Router (config) #".	Router>enable //Ingreso a modo privilegiado. Router#configure terminal //modo de config Router(config)#no ip domain-lookup //Comando para desactivar la búsqueda DNS Router(config**)#** //Comando exitoso sólo devolverá al indicador "Router (config) #"
Nombre del Router , utilizamos el comando hostname R1	Router›enable Router#configure terminal Router(config)#hostname R1 R1(config)#

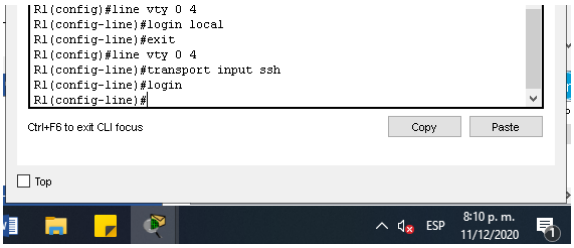
Nombre de dominio.
Los nombres de dominio permiten desvincular a las páginas web de las direcciones IP de los servidores en los que se guardan los archivos de tu web. Configure el nombre de dominio IP de la red mediante el comando ip domain-name nombre-de-dominio comando global configuration mode.
	R1#configure terminal
	R1(config)#ip domain-name ccna-lab.com // poner el nombre del dominio
	R1(config)# //Comando exitoso

Contraseña cifrada para el modo EXEC privilegiado Ciscoenpass Para proteger el acceso a **EXEC privilegiado**, utilice el comando enable password ciscoenpass, y luego lo encriptamos con el comando service password-encryption damos enter y salir.	R1#configure terminal R1(config)#enable password ciscoenpass R1(config)#service password-encryption R1(config)#exit R1#

Tarea	Especificación
Contraseña de acceso a la consola Ciscoconpass. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.	R1#configure terminal R1(config)#line console 0 R1(config-line)#password Ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#
Establecer la longitud mínima para las contraseñas 10 caracteres, utilizamos el siguiente comando, security passwords min-length10 y le damos enter	R1#configure terminal R1(config)#security passwords min-length10 R1(config)#
Crear un usuario administrativo en la base de datos local Nombre de usuario: **admin** Password: **admin1pass**	R1#configure terminal R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local R1(config-line)#exit R1(config)#

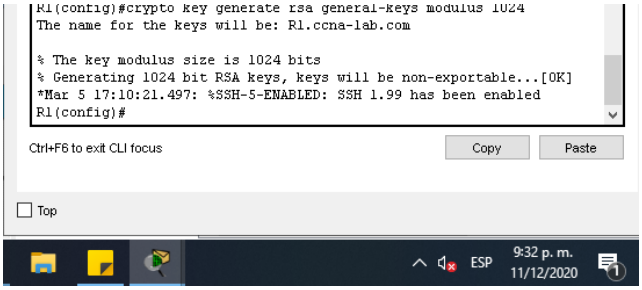
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.
 	
El servidor SSH puede autenticar a los usuarios localmente o con un servidor de autenticación. Para usar el método de autenticación local, cree un par de nombres de usuario y contraseñas con el comando username Nombre de usuario secret Contraseña comando global configuration mode.
	R1(config)#line vty 0 4
	R1(config-line)#login local //Carga la sesión
	R1(config-line)#end
	R1#
	
	Figura 3.configuración línea VTY
	 
	
	Fuente: Autor

Tarea	Especificación

Configurar VTY solo aceptando SSH.
Habilite el protocolo SSH en las líneas vty mediante el comando transport input ssh del modo de configuración de línea. El switch tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al Switch a que acepte solo las conexiones SSH. Use el comando line vty del modo de configuración global y, luego, el comando login local del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.
	R1(config)#line vty 0 4
	R1(config-line)#transport input ssh //se configura el transporte de entrada al ssh
	R1(config-line)#login //Carga la sesión
	R1(config-line)#exit //le damos salir con comando exit y enter
	R1#
	
	Figura 4.Configurar VTY solo aceptando SSH
	 
	
	Fuente: Autor

Cifrar las contraseñas de texto no cifrado. Se utiliza para encriptar las contraseñas configuradas, utilizamos el comando Service password-encryption	Service password-encryption R1#configure terminal R1(config)#Service password-encryption R1(config)#
Configure un MOTD Banner. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	R1(config)#banner motd #Un authorized access prohibited Att: Telecommunications Area. Thank you!# R1(config)#exit R1#
Habilitar el routing IPv6. Utilizamos el comando ipv6 unicast-routing	R1#configure terminal R1(config)#ipv6 unicast-routing R1(config)#

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces. En esta parte configuramos en cada una de las interfaces las direcciones ip y las Vlan con sus respectivos nombres.	R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#description VLAN 2 Bikes R1(config-subif)#ip address 10.19.8.1 255.255.255.192 R1(config-subif)# ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#description VLAN 3 Trikes R1(config-subif)#ip address 10.19.8.65 255.255.255.224 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#description VLAN 4 Management R1(config-subif)#ip address 10.19.8.97 255.255.255.248 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#no shutdown R1(config)#interface gigabitEthernet 0/0/1.6 R1(config-subif)#description VLAN 6 Native R1(config-subif)#no shutdown

Tarea	Especificación
Configure el Loopback0 interface. Una interfaz de bucle invertido es una interfaz virtual que siempre está activa y accesible siempre que al menos una de las interfaces IP del conmutador esté operativa. Como resultado, una interfaz de bucle invertido es útil para tareas de depuración, ya que siempre se puede hacer ping a su dirección IP si hay otra interfaz de conmutador activa.	R1(config)#interface loopback 0 R1(config-if)#description Interface Loopback R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#ipv6 address 2001:db8:acad:209::1/64 R1(config-subif)#no shutdown
Generar una clave de cifrado RSA. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando crypto key genérate rsa del modo de configuración global para habilitar el servidor SSH en el Switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. La configuración se utiliza un tamaño de módulo de 1024 bits. Una longitud de módulo mayor es más segura, pero se tarda más en generarlo y utilizarlo.	Módulo de 1024 bits R1(config)#crypto key generate rsa R1(config)# Figura 5.Generar una clave de cifrado RSA.  Fuente: Autor

1.2.4 Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

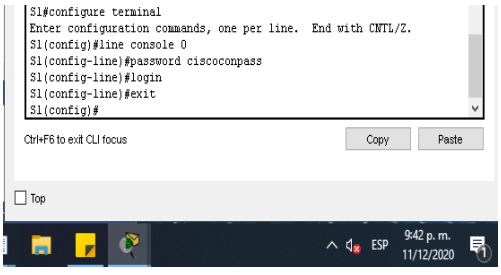
Realizamos las configuraciones en S1 y S2 desactivar la búsqueda de los DNS, le configuramos el nombre a cada Switch , le ponemos nombre al dominio, se configuran las contraseñas para modo privilegiado y para la consola, se establece

la longitud mínima para las contraseñas de 10 caracteres, Creamos un usuario administrativo en la base de datos local, Configuramos el inicio de sesión en las líneas VTY, Ciframos las contraseñas de texto no cifrado, Configure un MOTD Banner como un mensaje de advertencia para alguna persona ajena que quiera ingresar, se configura la clave de cifrado RSA, Configuramos la interfaz de administración (SVI) y por ultimo Configuración del Gateway predeterminado en los dos Switch así terminando la configuración en los Switch como lo podemos observar en la siguientes tareas.

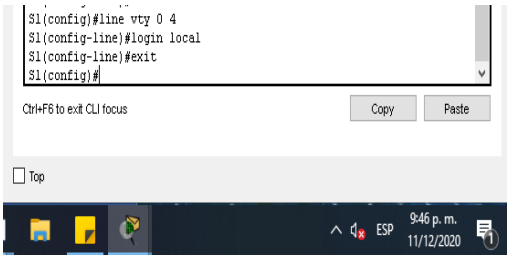
Configuración en el Switch S1 y S2

Tabla 7. Configuración en S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS. Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando exitoso sólo devolverá al indicador "Router (config) #".	Switch >enable Switch #configure terminal Switch(config)#no ip domain-lookup S1(config)#
Nombre del Switch. Para la configuración del nombre del Switch utilizamos el comando hostname S1 y S2 para dar el nombre a cada dispositivo	Switch >enable //Ingreso a modo privilegiado Switch#configure terminal //Ingreso a modo config Switch(config)#hostname S1 **//**Poner el nombre S1(config)# Switch(config)#hostname S2 **//**Poner el nombre S2(config)#
Nombre de dominio. Configure el nombre de dominio IP de la red mediante el comando ip domain-name nombre-de-dominio comando global configuration mode.	S1#configure terminal S1(config)#ip domain name ccna-lab.com S1(config)# S2(config)#ip domain name ccna-lab.com S2(config)#

Tarea	Especificación
Contraseña cifrada para el modo EXEC privilegiado. Para proteger el acceso a EXEC privilegiado, utilice el comando enable password ciscoenpass, y luego lo encriptamos con el comando service password-encryption damos enter y salir.	S1#configure terminal S1(config)#enable password ciscoenpass S1 (config)#service password-encryption S1(config)# S2(config)#enable password ciscoenpass S2 (config)#service password-encryption S2(config)#
Contraseña de acceso a la consola. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.	S1#configure terminal S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit S1(config)# S2#configure terminal S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit S2(config)# Figura 6.Contraseña de acceso a la consola  Fuente: Autor

Tarea	Especificación
Crear un usuario administrativo en la base de datos local. Configuramos un usuario con el nombre admin y asignamos password. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. Comando login local, en la configuración de línea habilita la base de datos local para la autenticación.	S1#configure terminal S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S1(config-line)#exit S1(config)# S2#configure terminal S2(config)#username admin password admin1pass S2(config)#line console 0 S21(config-line)#login local S2(config-line)#exit S2(config)#

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.
 	
Se realiza la configuración de las líneas VTY con el comando line vty 0 4 y luego con el comando login local, en la configuración de línea habilita la base de datos local para la autenticación.
	S1#configure terminal
	S1(config)#line vty 0 4
	S1(config-line)#login local // habilita la base de datos **local**
	S1(config-line)#exit
	S1(config)#
	
	S2#configure terminal
	S2(config)#line vty 0 4
	S2(config-line)#login local
	S2(config-line)#exit
	S2(config)#
	
	Figura 7.Configurar el inicio de sesión en las líneas VTY
	 
	
	Fuente: Autor

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH. Habilite el protocolo SSH en las líneas vty mediante el comando transport input ssh del modo de configuración de línea. El Switch tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al Switch a que acepte solo las conexiones SSH. Use el comando line vty del modo de configuración global y, luego, el comando login local del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.	S1#configure terminal S1(config)#crypto key generate rsa S1(config)#ip ssh version 2 S1(config)#line vty 0 4 S1(config-line)#transport input ssh S1(config-line)#login S1(config-line)#exit S1(config)# S2#configure terminal S2(config)#crypto key generate rsa S2(config)#ip ssh version 2 S2(config)#line vty 0 4 S2(config-line)#transport input ssh S2(config-line)#login S2(config-line)#exit S2(config)#
Cifrar las contraseñas de texto no cifrado. Se utiliza para encriptar las contraseñas configuradas, utilizamos el comando Service password-encryption	S1#configure terminal S1(config)#service password-encryption S1(config)# S2#configure terminal S2(config)#service password-encryption S2(config)#
Configurar un MOTD Banner. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	S1#configure terminal S1(config)# banner motd #Unauthorized access prohibited!# S1(config)#exit S1# S2#configure terminal S2(config)# banner motd #Unauthorized access prohibited!# S2(config)#exit S2#

Tarea	Especificación
Generar una clave de cifrado RSA. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando crypto key genérate rsa del modo de configuración global para habilitar el servidor SSH en el Switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. La configuración se utiliza un tamaño de módulo de 1024 bits. Una longitud de módulo mayor es más segura, pero se tarda más en generarlo y utilizarlo.	S1#configure terminal S1(config)#crypto key generate rsa S1(config)# S2#configure terminal S2(config)#crypto key generate rsa S2(config)#
Configurar la interfaz de administración (SVI). Se configura la interface Vlan 4 se configura la ip y la máscara de red en IPV4 y IPV 6	S1#configure terminal S1(config)#interface vlan 4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#no shutdown S1(config)# S2#configure terminal S2(config)#interface vlan 4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#no shutdown S2(config)#
Configuración del Gateway predeterminado en los dos Switch	S1#configure terminal S1(config)#ip default-gateway 10.19.8.97 S2#configure terminal S2(config)#ip default-gateway 10.19.8.97

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

1.3.1 Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En este paso se procede a configurar S1 creando las Vlan, Creando la troncal 802.1Q para que utilicen la VLAN 6 nativa, luego creamos un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, Se Configura el puerto de acceso de host para VLAN 2, Configurar la seguridad del puerto en los puertos de acceso, seguimos la configuración para Proteger todas las interfaces no utilizadas, Terminando la configuración en los Switch como lo podemos observar en las siguientes tareas.

Tabla 8. Configuración S1

Tarea	Especificación
Crear VLAN, En el Switch S1 procedemos a configurar cada una de las Vlan con sus respectivos nombres. Total Vlan creadas 6	S1#configure terminal S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit S1(config)# S1#configure terminal S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)# S1#configure terminal S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)# S1#configure terminal S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)# S1#configure terminal S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#

Tarea	Especificación
Crear troncal 802.1Q que utilicen la VLAN 6 nativa Switchport trunk encapsulation dot1q establece el modo de encapsulación de la interfaz troncal en el estándar de la industria 802.1Q. Switchport trunk encapsulation establece el modo de encapsulación de la interfaz troncal en ISL propietario. Troncal en modo switchport: pone la interfaz en modo troncal permanente y negocia para convertir el enlace vecino en un enlace troncal.	S1#configure terminal S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#switchport trunk encapsulation dot1Q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config)#exit S1#configure terminal S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2. Un canal de puerto es un enlace de comunicación entre dos conmutadores compatible con interfaces de grupo de canales coincidentes en cada conmutador. ... Los canales de puerto combinan el ancho de banda de varios puertos Ethernet en un solo enlace lógico.	S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1Q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk allowed vlan all S1(config-if)#channel-protocol lacp S1(config-if)#exit
Configurar el puerto de acceso de host para VLAN 2. Switchport acceder al modo comando fuerzas del puerto sea un acceso puerto de tiempo y cualquier dispositivo conectado a este puerto sólo será capaz de comunicarse con otros dispositivos que se encuentran en la misma VLAN	S1#configure terminal S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#exit S1(config)#

Tarea	Especificación
Configurar la seguridad del puerto en los puertos de acceso. La función de seguridad del puerto de conmutación (seguridad del puerto) es una pieza importante del rompecabezas de seguridad del conmutador de red; proporciona la capacidad de limitar qué direcciones se permitirán enviar tráfico en puertos de conmutación individuales dentro de la red conmutada.	S1#configure terminal S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3 S1(config-if)#exit S1(config)#
Proteja todas las interfaces no utilizadas. Switchport acceder al modo comando fuerzas del puerto sea un acceso puerto de tiempo y cualquier dispositivo conectado a este puerto sólo será capaz de comunicarse con otros dispositivos que se encuentran en la misma VLAN Accedemos a la Vlan 5 y le damos shutdown	S1#configure terminal S1(config)#interface range fastEthernet 0/3-4 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit S1(config)# S1#configure terminal S1(config)#interface range fastEthernet 0/7-24 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit S1(config)# S1#configure terminal S1(config)#interface range G0/1-2 S1(config-if)#switchport mode access S1(config-if)#description No Utilizada S1(config-if)#switchport access vlan 5 S1(config-if)#shutdown S1(config-if)#exit S1(config)#

1.3.2 Paso 5 Configure el S2.

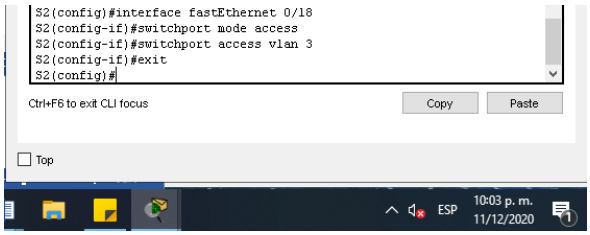
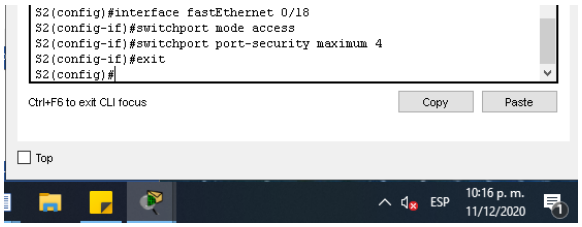
Entre las tareas de configuración de S2 se incluyen las siguientes:

En este paso se procede a configurar S2 he igualmente que el anterior Switch creando las VLan , Creando la troncal 802.1Q para que utilicen la VLAN 6 nativa, luego creamos un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, Se Configura el puerto de acceso de host para VLAN 2, Configurar la seguridad del puerto en los puertos de acceso, seguimos la configuración para Proteger todas las interfaces no utilizadas, terminando la configuración en los Switch como lo podemos observar en la siguiente tareas:

Tabla 9. Configuración S2

Tarea	Especificación
Crear VLAN En el Switch S2 procedemos a configurar cada una de las Vlan con sus respectivos nombres. Total Vlan creadas 6	S2#configure terminal S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#exit S2(config)# S2#configure terminal S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#exit S2(config)# S2#configure terminal S2(config)#vlan 4 S2(config-vlan)#name Management S2(config-vlan)#exit S2(config)# S2#configure terminal S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#exit S2(config)# S2#configure terminal S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#

Tarea	Especificación
Crear troncal 802.1Q que utilicen la VLAN 6 nativa. Switchport trunk encapsulation dot1q establece el modo de encapsulación de la interfaz troncal en el estándar de la industria 802.1Q. Switchport trunk encapsulation establece el modo de encapsulación de la interfaz troncal en ISL propietario. Troncal en modo switchport: pone la interfaz en modo troncal permanente y negocia para convertir el enlace vecino en un enlace troncal.	S2#configure terminal S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2. Un canal de puerto es un enlace de comunicación entre dos conmutadores compatible con interfaces de grupo de canales coincidentes en cada conmutador. ... Los canales de puerto combinan el ancho de banda de varios puertos Ethernet en un solo enlace lógico.	S2#configure terminal S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#interface port-channel 1 S2(config-if)#switchport trunk encapsulation dot1Q S2(config-if)#switchport mode trunk S2(config-if)#channel-group 1 mode active S2(config-if)#switchport trunk allowed vlan all S2(config-if)#channel-protocol lacp S2(config-if)#exit

Tarea	Especificación
Configurar el puerto de acceso del host para la VLAN 3. Switchport acceder al modo comando fuerzas del puerto sea un acceso puerto de tiempo y cualquier dispositivo conectado a este puerto sólo será capaz de comunicarse con otros dispositivos que se encuentran en la misma VLAN	S2#configure terminal S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 Figura 8.configuración puerto Vlan 3  Fuente: Autor
Configure port-security en los access ports. La función de seguridad del puerto de conmutación (seguridad del puerto) es una pieza importante del rompecabezas de seguridad del conmutador de red; proporciona la capacidad de limitar qué direcciones se permitirán enviar tráfico en puertos de conmutación individuales dentro de la red conmutada.	S2#configure terminal S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport port-security maximum 4 S2(config-if)#exit *Figura 9.Configure port-security en los access ports.*  Fuente: Autor

Tarea	Especificación
Asegure todas las interfaces no utilizadas. Switchport acceder al modo comando fuerzas del puerto sea un acceso puerto de tiempo y cualquier dispositivo conectado a este puerto sólo será capaz de comunicarse con otros dispositivos que se encuentran en la misma VLAN Accedemos a la Vlan 5 y le damos shutdown	S2(config)#interface range F0/3-17 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit S2(config)#interface range F0/19-24 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit S2(config)#interface range G0/1-2 S2(config-if)#switchport mode access S2(config-if)#description No Utilizada S2(config-if)#switchport access vlan 5 S2(config-if)#shutdown S2(config-if)#exit

1.4 Parte 3: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:
En Este paso procedemos a configurar el Router R1, donde configuramos DHCP IPv4 para VLAN 2 y Vlan 3 lo podemos observar en las siguientes tareas.

Tabla 10. Configuración R1

Tarea	Especificación
Configure Default Routing	R1(config)#ip route 0.0.0.0 0.0.0.0 loopbach0
Configurar DHCP IPv4 para VLAN 2. Se configura en el router la ip dhcp excluyendo las direcciones.	R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.51 R1(config)#ip dhcp pool VLAN2 R1(config)#network 10.19.8.0 255.255.255.192 R1(config)#default-router 10.19.8.1 R1(config)#dns-server 10.19.8.51 R1(config)#domain-name ccna-a.net R1(config)#

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3 Protocolo de red que permite que un servidor asigne automáticamente una dirección IP a un dispositivo habilitado para IP desde un rango definido de números configurados para una red determinada.	R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.83 R1(config)#ip dhcp pool VLAN3 R1(dhcp-config)#network 10.19.8.64 255.255.255.224 R1(config)#default-router 10.19.8.65 R1(config)#dns-server 10.19.8.83 R1(config)#domain-name ccna-b.net R1(config)#

1.4.1 Paso 6: 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 11. Configuración Red PC-A

Configuración de red de PC-A	
Descripción	ccna-a.net
Dirección física	000c.852A9A47
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

En esta parte se realiza la configuración en el equipo PC-A

Tabla 12. Configuración Red PC-B

Configuración de red de PC-B	
Descripción	*ccna-b.net*
Dirección física	*00D0.BABA.934E*
Dirección IP	*10.19.8.64*
Máscara de subred	*255.255.255.224*
Gateway predeterminado	*10.19.8.65*
Gateway predeterminado IPv6	*FE80::1*

En esta parte se realiza la configuración en el equipo PC-B

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

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

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

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla, se realizan las pruebas indicadas en la topología del escenario 1, dando como resultados correctos en la simulación, como podemos ver en la siguiente tabla las pruebas realizadas.

Tabla 13. Configuración Red PC-A Y PC-B

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

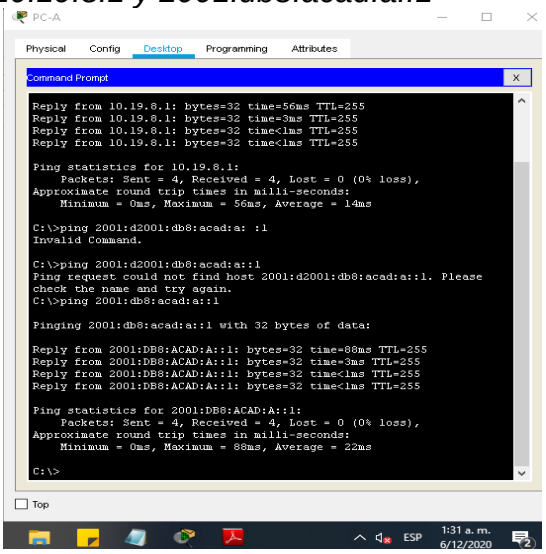
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	*R1, G0/0/1.4*	IPv6	2001:db8:acad:c: :1	***ok***
PC-B	S1, VLAN 4	Dirección	10.19.8.98	***ok***
PC-B	*S1, VLAN 4*	IPv6	2001:db8:acad:c: :98	***ok***
PC-B	S2, VLAN 4	Dirección	10.19.8.99.	***ok***
PC-B	*S2, VLAN 4*	IPv6	2001:db8:acad:c: :99	***ok***

A continuación, se muestran las pruebas realizadas desde PC-A y PC-B

Resultados PC-A ping

Como podemos observar en las siguientes figuras se realiza ping a los dos tipos de direcciones IP dando como resultado las respuestas correctas indicadas en la tabla superior.

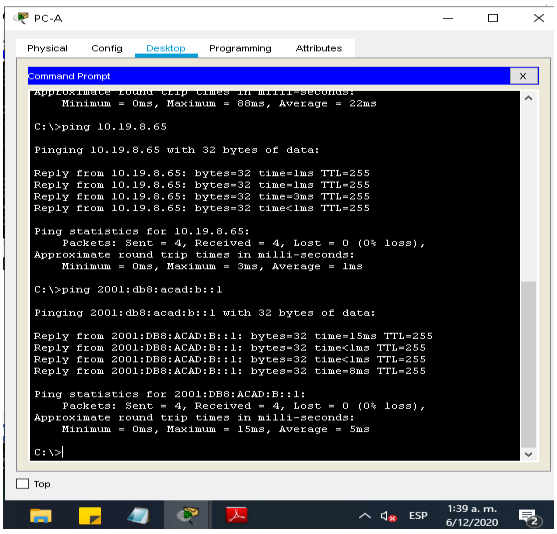
Figura 10. PC-A ping 10.19.8.1 y 2001:db8:acad:a::1



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

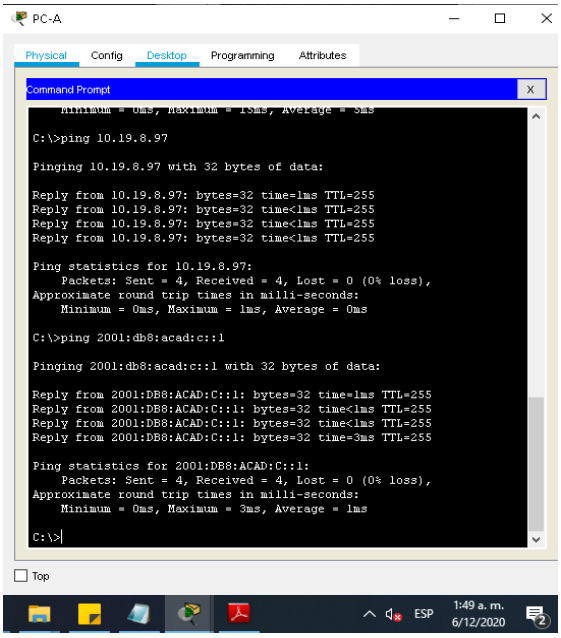
Figura 11. PC-A Ping 10.19.8.65 y 2001:db8:acad:b::1



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

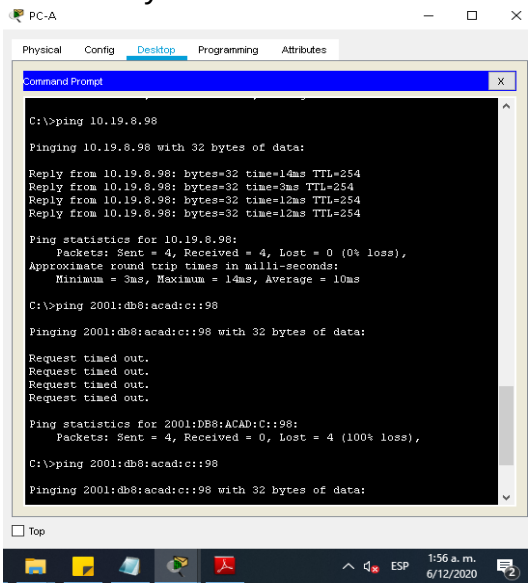
Figura 12. PC-A ping 10.19.8.97 y 2001:db8:acad:c::1



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

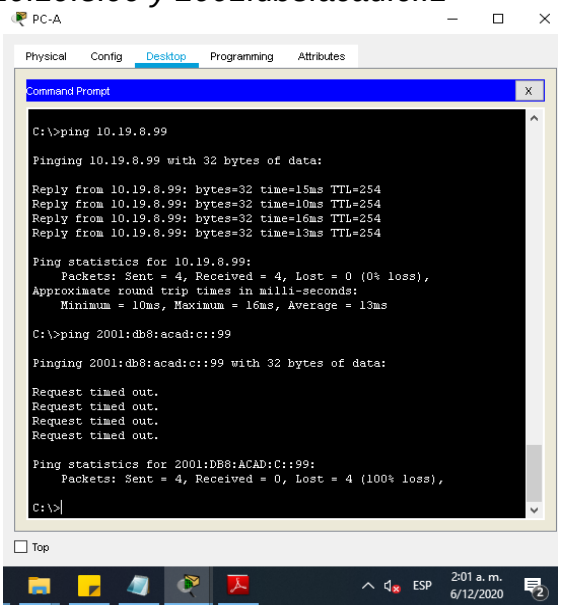
Figura 13. PC-A ping 10.19.8.98 y 2001:db8:acad:c::98



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

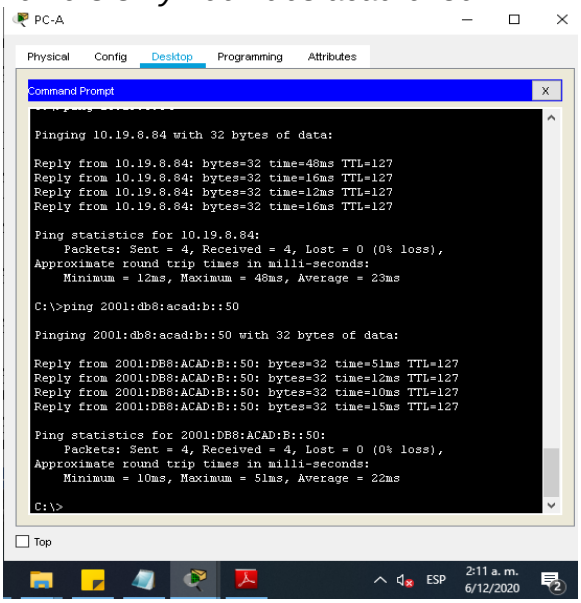
Figura 14.PC-A ping 10.19.8.99 y 2001:db8:acad:c::1



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

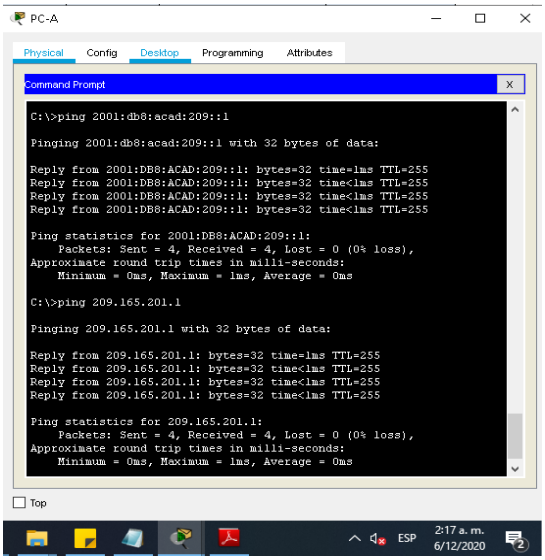
Figura 15.PC-A ping 10.19.8.84 y 2001:db8:acad:b::50



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

Figura 16. PC-A ping 2001:db8:acad:209::1 y 209.165.201.1



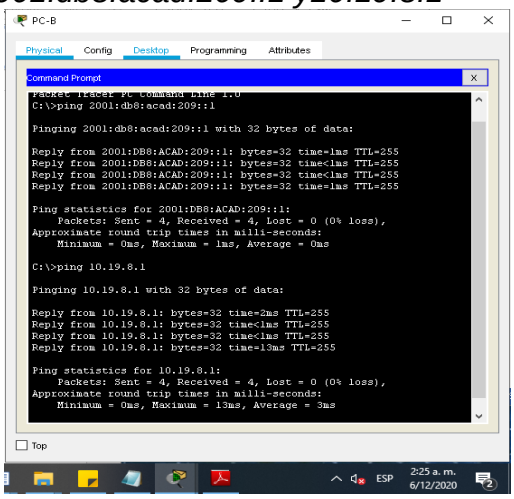
Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

Resultados PC-B ping

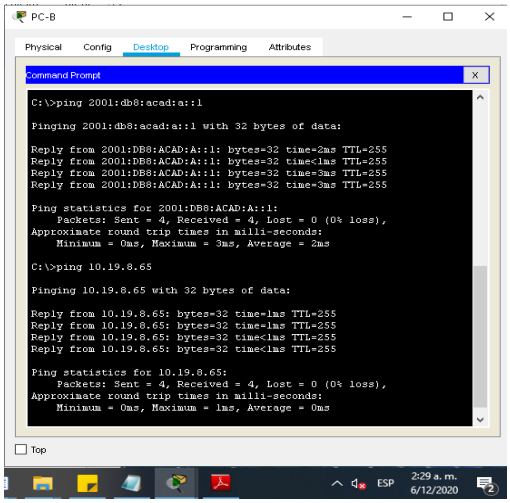
Como podemos observar se realiza ping a los dos tipos de direcciones IP dando como resultado respuesta correcta.

Figura 17. PC-B ping 2001:db8:acad:209::1 y10.19.8.1



Fuente: Autor

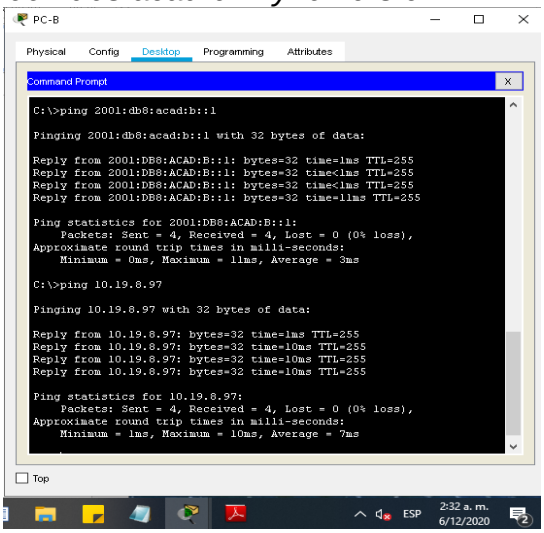
Figura 18. PC-B ping 2001:db8:acad:a::1 y10.19.8.65



Fuente: Autor

Desde PC-B se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

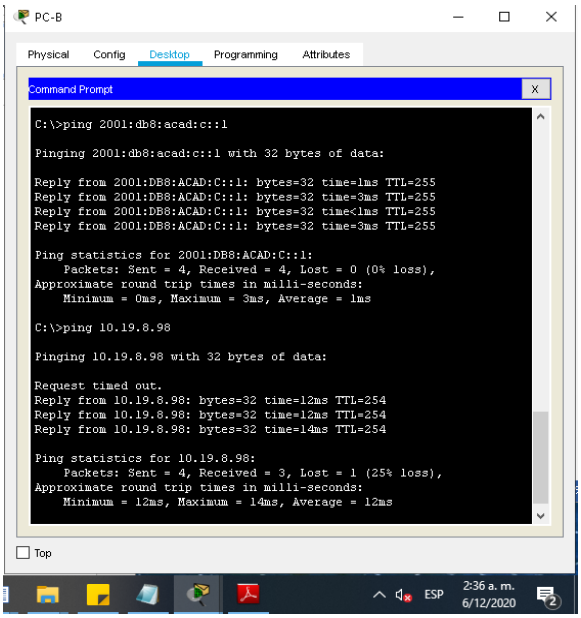
Figura 19. PC-B ping 2001:db8:acad:b::1 y10.19.8.97



Fuente: Autor

Desde PC-B se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

Figura 20. PC-B ping 2001:db8:acad:c::1 y10.19.8.98



Fuente: Autor

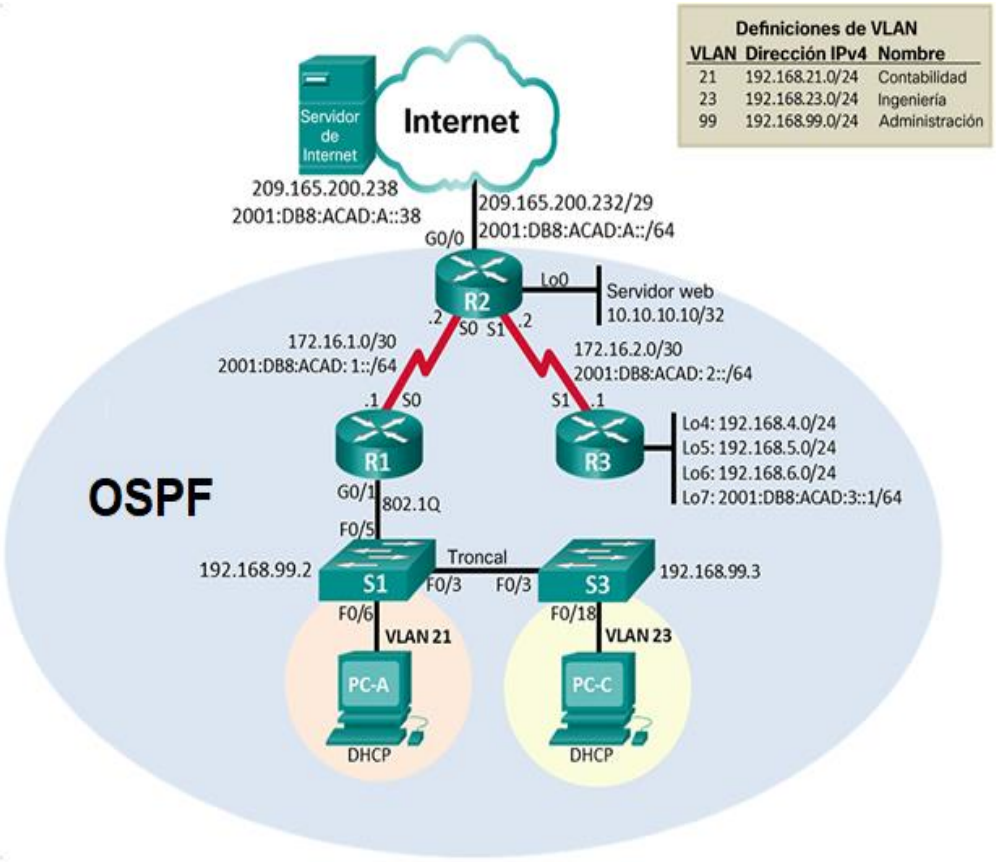
Desde PC-B se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta.

2 ESCENARIO 2

Escenario: Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

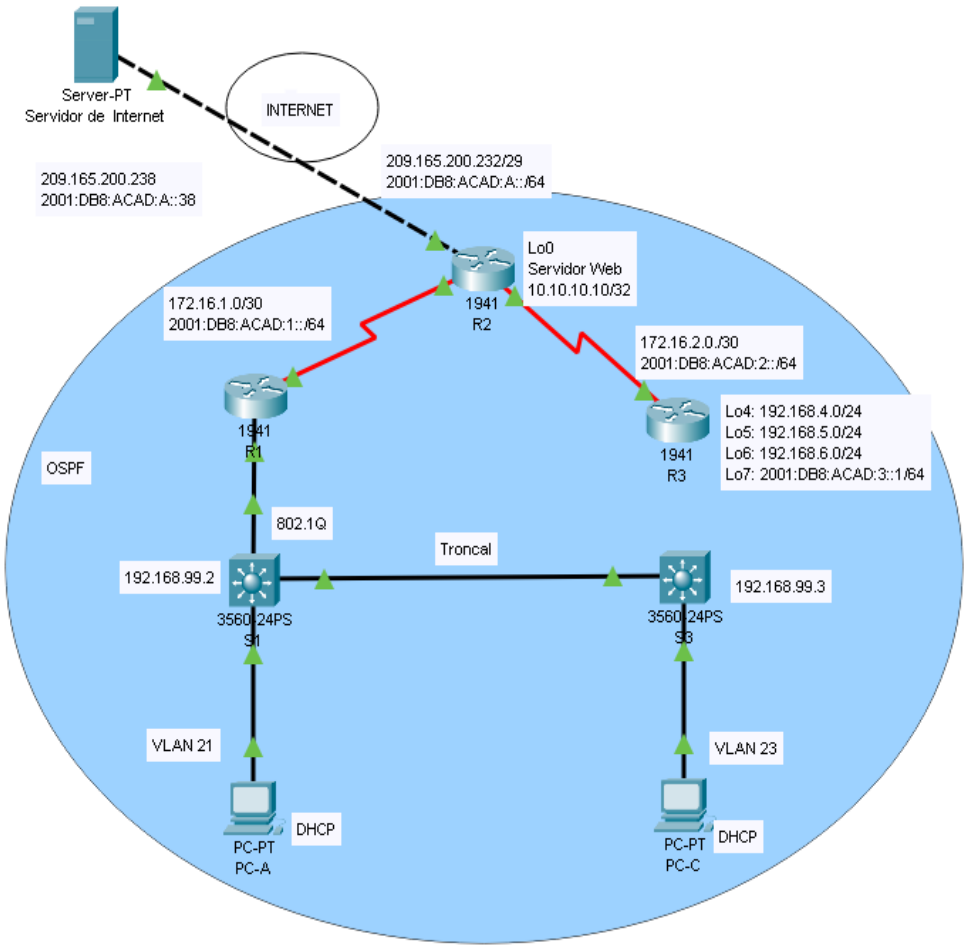
2.1 Topología

Figura 21. Simulación del escenario 2



Fuente documento del repositorio

Figura 22. Topología simulación del escenario 2 Packet Tracer



Fuente: Autor

2.2 Parte 1: inicializar dispositivos.

2.2.1 Paso 1: Inicializar y volver a cargar los Routers y los switch

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Se realiza la eliminación mediante el comando delete y reinicios de los equipos con el comando reload.

En este paso se realizan las configuraciones en cada dispositivo para iniciar las configuraciones dadas con los comandos en la siguiente tabla.
Configuración de los dispositivos

Tabla 14. Configuración Comandos IOS

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los Routers. Borrar el archivo con el siguiente comando startup-config	Router›enable Router# erase startup-config
Volver a cargar todos los Routers. Escribiendo el comando Reload Utilizamos el comando reload para eliminar toda información de configuración antigua de la Memoria. Cuando reciba el mensaje proceed with reload (continuar con la carga) presionando enter, si se presiona cualquier otra tecla, se anulara la recarga	Router›enable 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 flash:vlan.dat
Volver a cargar ambos switches	Switch ›enable Switch# reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches. //Muestra la información Guardada en la memoria flash con el comando Show vlan	Switch# show vlan

2.3 Parte 2: Configurar los parámetros básicos de los dispositivos

2.3.1 Paso 1: Configurar la computadora de Internet

Se configurarán los dispositivos de acuerdo con las direcciones IP que nos brinda la Topología del escenario 2.

Tabla 15. Configuración de la computadora 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	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

2.3.2 Paso 2: Configurar R1

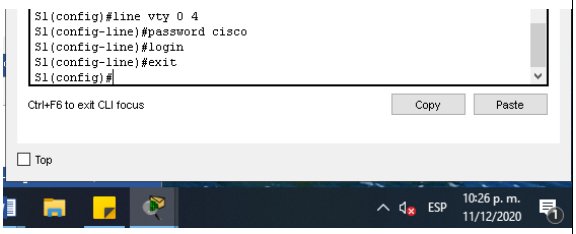
Las tareas de configuración para R1 incluyen las siguientes tareas:

En este paso realizamos la configuración en R1 Configuramos los DNS, el nombre, las contraseñas exec privilegiado, acceso a la consola, acceso a Telnet

Ciframos las contraseñas, Mensaje MOTD escribimos el mensaje de advertencia si alguien va a ingresar sin autorización, luego se configuran las interfaces, y las rutas predeterminadas las podemos observar en la siguiente tabla.

Tabla 16. Configuración R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS. Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando exitoso sólo devolverá al indicador "Router (config) #".	Router›enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router. utilizamos el comando hostname R1	Router›enable Router#config terminal Router(config)#hostname R1
Contraseña de exec privilegiado cifrada. Para proteger el acceso a EXEC privilegiado, utilice el comando enable secret class damos enter y salir.	R1›enable R1# config terminal R1(config)#enable secret class R1(config)#exit

Contraseña de acceso a la consola. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet. -Utiliza el comando line vty 0 15para ingresar al modo de configuración de vty en las 16 vty lines (Enumerado del 0 al 15). -Utiliza el subcomando login para habilitar la contraseña de seguridad de las sesiones vty utilizando una Contraseña simple.	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit Figura 23.Contraseña de acceso Telnet.  Fuente: Autor
Cifrar las contraseñas de texto no cifrado. Para proteger el acceso, utilice el comando enable password cisco, y luego lo encriptamos con el comando service password-encryption damos enter y salir.	R1(config)#service password-encryption R1(config)#exit
Mensaje MOTD. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	R1#config terminal R1(config)# banner motd # Se prohíbe el acceso no autorizado ATT Área Telecomunicaciones# R1(config)# exit
Interfaz S0/0/0 Se configura la interfaz serial con la descripción conexión y luego se configura la ip y mascara y luego la	R1#config terminal R1(config)#Interface s0/0/0 R1(config-if)#Description Conexion R1 y R2 R1(config-if)#ip address 172.16.1.1

activamos.	255.255.255.252 R1(config-if)#no shutdown R1(config)#exit R1(config)#interface s0/0/0 R1(config-if)#ipv6 enable R1(config)#ip address 2001:db8:acad:1::1/64 R1(config)#no shutdown
Rutas predeterminadas. Una ruta predeterminada es una ruta estática que coincide con todos los paquetes. En lugar de almacenar todas las rutas para todas las redes en la tabla de routing, un router puede almacenar una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing.	R1(config)#interface serial 0/0/0 R1(config-if)#ip address 0.0.0.0 0.0.0.0 R1(config-if)#exit Configuración ruta Ipv6 predeterminada S0/0/0 R1(config)#interface Serial0/0/0 R1(config-if)#ipv6 address ::/0 R1(config-if)#exit

Nota: Todavía no configure G0/1.

2.3.3 Paso 3: Configurar R2

En este paso se realiza la misma configuración que en paso anterior
La configuración del R2 incluye las siguientes tareas:

En este paso realizamos la configuración en R2 Configuramos los DNS, el nombre Router, las contraseñas exec privilegiado, acceso a la consola, acceso a Telnet Ciframos las contraseñas, Mensaje MOTD escribimos el mensaje de advertencia si alguien va ingresar sin autorización, luego se configuran las interfaces, y las rutas predeterminadas las podemos observar en la siguiente tabla.

Tabla 17. Configuración R2

Elemento o tarea configuración	Especificación
Desactivar la búsqueda DNS. Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando exitoso sólo devolverá al indicador "Router (config) #".	Router(config)#no ip domain-lookup

Nombre del router. Utilizamos el comando hostname R1	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada. Las contraseñas también se usan para controlar el acceso al modo EXEC... y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado.	R2(config)#e nable secret class R2(config)#e xit
Contraseña de acceso a la consola. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet. -Utiliza el comando line vty 0 15 para ingresar al modo de configuración de vty en las 16 vty lines (Enumerado del 0 al 15). -Utiliza el subcomando login para habilitar la contraseña de seguridad de las sesiones vty utilizando una Contraseña simple.	R2(config)#li ne vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config- line)#exit
Cifrar las contraseñas de texto no cifrado. Para proteger el acceso luego lo encriptamos con el comando service password-encryption damos enter y salir.	R2#config terminal R2(config)#service password-encryption R2(config)#exit
Habilitar el servidor HTTP La simulación no permite su configuracion.	No se puede configurar para habilitarlo
Mensaje MOTD. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	R2#config terminal R2(config)#banner motd # Se prohíbe el acceso no autorizado # R2(config)#exit

Interfaz S0/0/0 Se configura la interfaz serial con la ip y mascara y luego la activamos.	R2(config)#Interface s0/0/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#interface s0/0/0 R2(config-if)#ipv6 enable R2(config-if)#ip address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz S0/0/1 Se configura la interfaz serial con la ip y mascara y luego la activamos.	R2(config)#interface s0/0/1 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#no shutdown R2(config)#interface s0/0/1 R2(config-if)#ipv6 enable R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz G0/0 (simulación de Internet) Se configura la interfaz con la ip y mascara le agregamos bad mask para la dirección pública y luego la activamos. Y seguimos la configuración IPV6	R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 Bad mask /29 for address 209.165.200.232 R2(config-if)#no shutdown R2(config-if)#exit R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado). La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, ... Configuración de la interfaz Loopback0	R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit

Ruta predeterminada. Una ruta predeterminada es una ruta estática que coincide con todos los paquetes. En lugar de almacenar todas las rutas para todas las redes en la tabla de routing, un router puede almacenar una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing.	R2(config)# interface G0/0 R2(config-if)# ip route 0.0.0.0 0.0.0.0 G0/0 R2(config-if)# exit R2(config)# interface G0/0 R2(config)# ipv6 route ::/0 G 0/0 R2(config)# exit

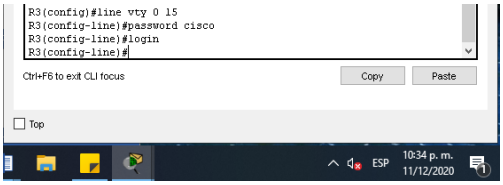
2.3.4 Paso 4: Configurar R3

En este paso se realiza la misma configuración que en paso anterior
La configuración del R3 incluye las siguientes tareas:

En este paso realizamos la configuración en R3 Configuramos los DNS, el nombre Router, las contraseñas exec privilegiado, acceso a la consola, acceso a Telnet Ciframos las contraseñas, Mensaje MOTD escribimos el mensaje de advertencia si alguien va ingresar sin autorización, luego se configuran las interfaces, y la Interfaz loopback, las podemos observar en la siguiente tabla.

Tabla 18. Configuración R3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando exitoso sólo devolverá al indicador "Router (config) #".	Router(config)#no ip domain-lookup
Nombre del router. Utilizamos el comando hostname R1 asignarle el nombre.	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada. Las contraseñas también se usan para	R3(config)#enable secret class

controlar el acceso al modo EXEC... y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado.	
Contraseña de acceso a la consola. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet. -Utiliza el comando line vty 0 15 para ingresar al modo de configuración de vty en las 16 vty lines (Enumerado del 0 al 15). -Utiliza el subcomando login para habilitar la contraseña de seguridad de las sesiones vty utilizando una Contraseña simple.	R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login Figura 24.Contraseña de acceso Telnet  Fuente: Autor
Cifrar las contraseñas de texto no cifrado. Para proteger el acceso encriptamos con el comando service password-encryption damos enter y salir.	R3(config-line)#service password-Encryption R3(config)#exit
Mensaje MOTD. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	R3#config terminal R3(config)#banner motd # Se prohíbe el acceso no autorizado # R3(config)#exit
Interfaz S0/0/1 Se configura cada una de las interfaces seriales con la ip y mascara y luego la activamos.	R3(config)#interface s0/0/1 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface s0/0/1 R3(config-if)# ipv6 enable

	R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)#exit R3(config)#interface s0/0/1 R3(config-if)# ipv6 enable R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown R3(config-if)#exit
Interfaz loopback 4. Una interfaz de bucle invertido es una interfaz virtual que siempre está activa y accesible siempre que al menos una de las interfaces IP del conmutador esté operativa. Como resultado, una interfaz de bucle invertido es útil para tareas de depuración, ya que siempre se puede hacer ping a su dirección IP si hay otra interfaz de conmutador activa.	R3(config)#interface looback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5. Una interfaz de bucle invertido es una interfaz virtual que siempre está activa y accesible siempre que al menos una de las interfaces IP del conmutador esté operativa.	R3(config)#interface looback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6. Una interfaz de bucle invertido es una interfaz virtual que siempre está activa y accesible siempre que al menos una de las interfaces IP del conmutador esté operativa.	R3(config)#interface looback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7 Una interfaz de bucle invertido es una interfaz virtual que siempre está activa y accesible siempre que al menos una de las interfaces IP del conmutador esté operativa.	R3(config)#interface looback 7 R3(config-if)#ipv6 addres 2001:DB8:ACAD:3::1/64 R3(config-if)#exit

2.3.5 Paso 5: Configurar S1

En este paso se realiza la configuración del Switch la configuración del S1 incluye las siguientes tareas:

En este paso realizamos la configuración en S1 Configuramos los DNS, el nombre, las contraseñas exec privilegiado, acceso a la consola, acceso a Telnet
Ciframos las contraseñas, Mensaje MOTD escribimos el mensaje de advertencia si alguien va a ingresar sin autorización, las podemos observar en a la siguiente tabla.

Tabla 19. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS. Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando exitoso sólo devolverá al indicador "Router (config) #".	Switch(config)#no ip domain-lookup
Nombre del switch. Utilizamos el comando hostname S1	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada. Las contraseñas también se usan para controlar el acceso al modo EXEC... y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado.	S1(config)#enable secret class
Contraseña de acceso a la consola. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola. Luego asignamos el password y lo activamos.	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login

Contraseña de acceso Telnet -Utiliza el comando line vty 0 15 para ingresar al modo de configuración de vty en las 16 vty lines (Enumerado del 0 al 15).Asignamos Password -Utiliza el subcomando login para habilitar la contraseña de seguridad de las sesiones vty utilizando una Contraseña simple.	S1(config-line)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado. Para Proteger la contraseña luego lo encriptamos con el comando service password-encryption damos enter y salir.	S1(config-line)#service password-encryption
Mensaje MOTD. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	S1(config)#banner motd # Se prohíbe el acceso no autorizado Att Área Telecomunicaciones# S1(config)#exit

2.3.6 Paso 6: Configurar S3

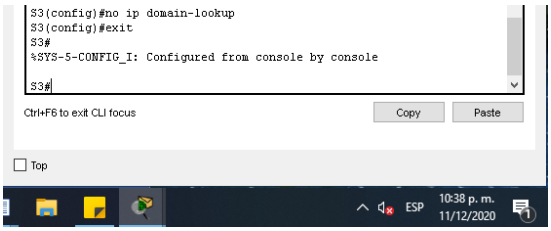
En este paso se realiza la misma configuración en el S3 que al anterior, la configuración del S3 incluye las siguientes tareas:

En este paso realizamos la configuración en S1 Configuramos los DNS, el nombre, las contraseñas exec privilegiado, acceso a la consola, acceso a Telnet.

Ciframos las contraseñas, Mensaje MOTD escribimos el mensaje de advertencia si alguien va a ingresar sin autorización, las podemos observar en a la siguiente tabla.

Tabla 20. Configuración S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS. Introduce el comando "no ip domain-lookup" y presiona la tecla "Enter". No habrá ningún mensaje de salida si la operación es exitosa. Un comando	Switch(config)#no ip domain-lookup Figura 25.Desactivar la búsqueda DNS

exitoso sólo devolverá al indicador "Router (config) #".	 Fuente: Autor
Nombre del Switch. Utilizamos el comando hostname S3	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada. Las contraseñas también se usan para controlar el acceso al modo EXEC... y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado.	S3(config)#enable secret class
Contraseña de acceso a la consola. En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola. Luego asignamos el password y lo activamos.	S3(config)#line console 0 S3(config- line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet -Utiliza el comando line vty 0 15 para ingresar al modo de configuración de vty en las 16 vty lines (Enumerado del 0 al 15).Asignamos Password -Utiliza el subcomando login para habilitar la contraseña de seguridad de las sesiones vty utilizando una Contraseña simple.	S3(config-line)#line vty 0 15 S3(config -line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado. Para Proteger la contraseña luego lo encriptamos con el comando service password-encryption damos enter y	S3(config-line)#service password-encryption

salir.	
Mensaje MOTD. Se configura un mensaje al momento que quieran acceder para advertir a los posibles intrusos que no son bienvenidos en su red.	S3(config)#banner motd # Se prohíbe el acceso no autorizado # S3(config)#exit

2.3.7 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:

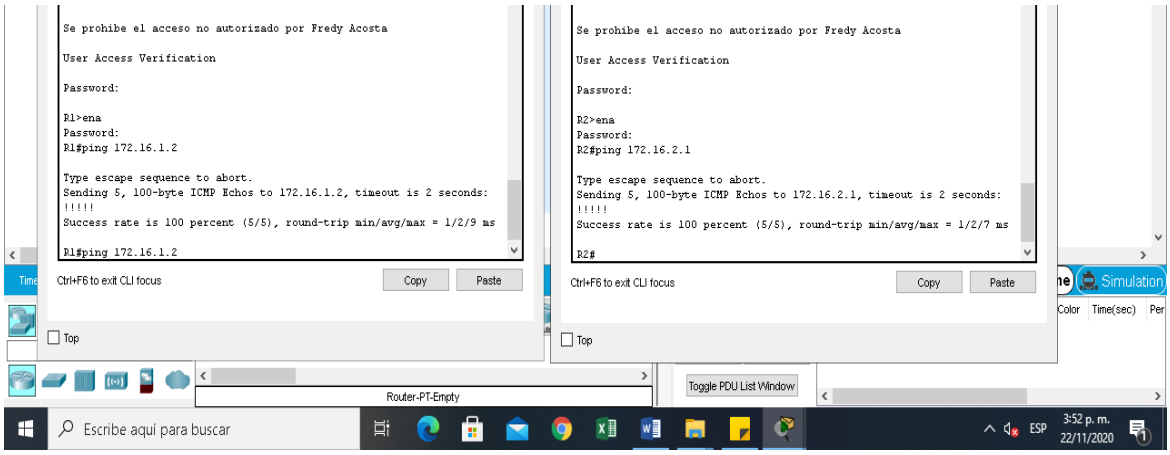
Tabla 21. Verificación conectividad de la Red

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.2	R1#ping 172.16.1.2
R2	R3, S0/0/1	172.16.2.1	R2#ping 172.16.2.1
PC de Internet	Gateway predeterminado	209.165.200.233	SERVER Command Line 1.0 C:\>ping 209.165.200.233

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

Resultados del ping en R1 y R2 y el PC de internet como lo podemos ver en la siguiente figura.

Figura 26.Resultados de ping en R1 y R2

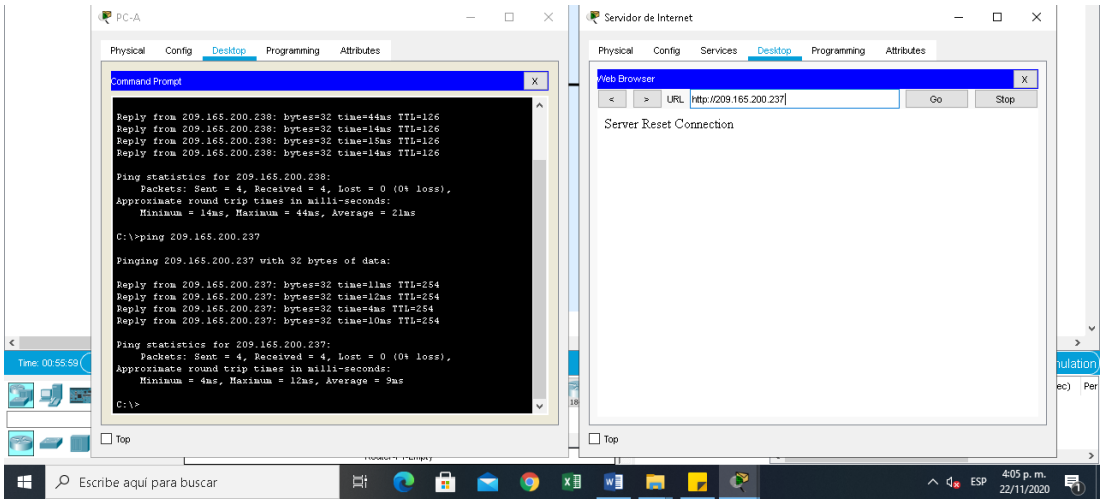


Fuente: Autor

Como podemos observar desde cada Router se realiza ping donde muestra que hay conexión de forma correcta obteniendo los resultados esperados.

Se realiza ping donde verificamos el servidor, lo podemos ver en la siguiente figura.

Figura 27: Verificación desde el PC-A al servidor Internet



Fuente: Autor

Como podemos observar en la figura se realiza ping donde verificamos la conexión hacia el servidor indicando que da respuesta correcta.

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

2.4.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

En este paso se configura S1 donde se crea la base de datos de VLAN, se Asigna la dirección IP de administración, configuramos el gateway predeterminado, Forzamos el enlace troncal en la interfaz F0/3 y F0/5, Configuramos el resto de los puertos como puertos de acceso, Asignamos a las interfaces F0/6 la VLAN 21, por ultimo configuramos Apagar todos los puertos sin usar, como lo podemos ver en la siguiente tabla.

Tabla 22. Configurar S1

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	S1(config)#VLAN 21 S1(config-vlan)#name contabilidad S1(config-vlan)#VLAN 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#VLAN 99 S1(config-vlan)#name administracion
Asignar la dirección IP de administración.	S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no shutdown
Asignar el Gateway predeterminado. Se realiza la configuración con el comando ip default-gateway y la ip.	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3 Se configura troncal en modo switchport: pone la interfaz en modo troncal permanente y negocia para convertir el enlace vecino en un enlace troncal. La VLAN nativa predeterminada es la VLAN 1. Es decir, si no configura una VLAN nativa explícitamente,	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

cualquier tráfico no etiquetado recibido en un puerto troncal se coloca automáticamente en la VLAN 1. El puerto troncal es el "opuesto" (más o menos) de lo que se conoce como un puerto de acceso.	
Forzar el enlace troncal en la interfaz F0/5. Se configura troncal en modo switchport: pone la interfaz en modo troncal permanente y negocia para convertir el enlace vecino en un enlace troncal. La VLAN nativa predeterminada es la VLAN 1. Es decir, si no configura una VLAN nativa explícitamente, cualquier tráfico no etiquetado recibido en un puerto troncal se coloca automáticamente en la VLAN 1. El puerto troncal es el "opuesto" (más o menos) de lo que se conoce como un puerto de acceso.	Utilizar la red VLAN 1 como VLAN nativa S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#
Asignar F0/6 a la VLAN 21 Se configura la interface Switchport acceder al modo de ” comando fuerzas del puerto sea un acceso puerto de tiempo y cualquier dispositivo conectado a este puerto sólo será capaz de comunicarse con otros dispositivos que se encuentran en la misma VLAN	S1(config-if-range)#interface f0/6 S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar. Se configura el puerto range donde se mencionan los demás puertos y con el comando shutdown los deshabilitamos	S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2 S1(config-if-range)#shutdown

2.4.2 Paso 2: Configurar S3

En este paso se hará lo mismo que en el paso anterior
La configuración del S3 incluye las siguientes tareas:

En este paso se configura S3 donde se crea la base de datos de VLAN, se Asigna la dirección IP de administración, configuramos el Gateway predeterminado, Forzamos el enlace troncal en la interfaz F0/3, Configuramos el resto de los puertos como puertos de acceso, Asignamos a las interfaces F0/18 a la VLAN 21, por último, configuramos Apagar todos los puertos sin usar, como lo podemos ver en la siguiente tabla.

Tabla 23. Configurar S3

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN Configuramos la Vlan le asignamos un nombre para identificarla	S3(config)# S3(config)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#exit S3(config-if)#
Asignar la dirección IP de administración Asignamos la ip y mascara de red y realizamos la activación.	S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(config-if)#no shutdown
Asignar el Gateway Predeterminado. Gateway, puerta de enlace o pasarela, es un dispositivo dentro de una red de comunicaciones, que permite a través de sí mismo, acceder a otra red	S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3. Se configura la interfaz troncal en modo switchport: pone la interfaz en modo troncal permanente y negocia para convertir el enlace vecino en un enlace troncal.	Utilizar la red VLAN 1 como VLAN nativa S3(config)#interface f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso. Utilizando el comando interface range	S3(config-if)#interface range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21. Se configura la interface Switchport acceder al modo de" comando fuerzas del puerto sea un acceso puerto de tiempo y cualquier dispositivo conectado a este puerto sólo será capaz de comunicarse con otros dispositivos que se encuentran en la misma VLAN.	S3(config-if-range)#interface f0/18 S3(config-if)#switchport access VLan 21
Apagar todos los puertos sin usar Se configura el puerto range donde se mencionan los demás puertos y con el comando shutdown los apagamos.	S3(config-if)#interface range f0/1-2, f0/4-17, f0/19- 24, g0/1-2 S3(config-if-range)#shutdown

2.4.3 Paso 3: Configurar R1

La configuración del R1 incluye las siguientes tareas:

En este paso realizamos la configuración R1 donde configuramos la subinterfaz 802.1Q .21 en G0/1, Configurar la subinterfaz 802.1Q .23 en G0/1, Configurar la subinterfaz 802.1Q .99 en G0/1 y por lo último activamos la interfaz G0/1.
Configurar R1

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad R1(config)#interface g0/1.21 Asignar la VLAN 21 R1(config-subif)#description vlan 21 R1(config-subif)#encapsulation dot1q 21

	Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería R1(config-subif)#int g0/1.23 Asignar la VLAN 23 R1(config-subif)#description VLAN 23 R1(config-subif)#encapsulation dot1q 23 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración R1(config-subif)#int g0/1.99 Asignar la VLAN 99 R1(config-subif)#description VLAN 99 R1(config-subif)#encapsulation dot1q 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)#interface g0/1 R1(config-if)#no shutdown

Tabla 24. Configurar R1

2.4.4 Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switch, 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, como podemos observar en a la siguiente tabla.

Tabla 25: Verificación conectividad Red

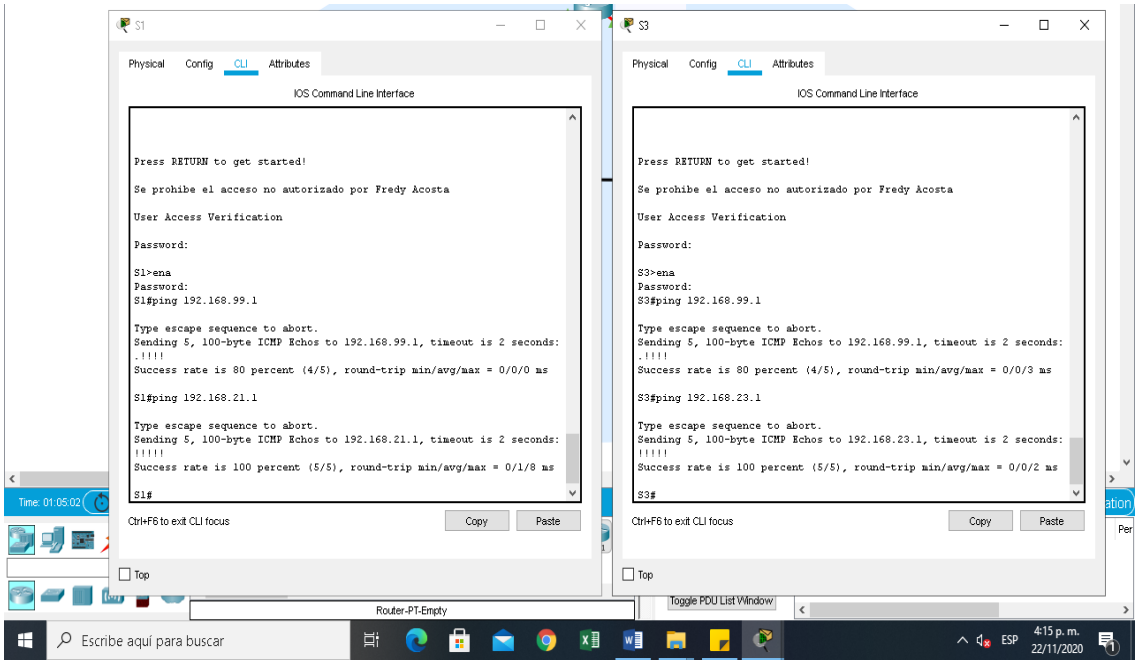
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#Ping 192.168.99.1
S3	R1, dirección VLAN 99	192.168.99.1	S3#Ping 192.168.99.1

S1	R1, dirección VLAN 21	192.168.21.1	S1#Ping 192.168.21.1
S3	R1, dirección VLAN 23	192.168.23.1	S3#Ping 192.168.23.1

Verificamos la conectividad por medio de un ping de S1 a S3 y viceversa dando los resultados correctos, lo podemos observar en al siguiente Figura.

Verificación de conectividad

Figura 28. Verificación de conectividad S1 y S3



Fuente: Autor

2.5 Parte 4: Configurar el protocolo de routing dinámico OSPF

2.5.1 Paso 1: Configurar OSPF en el R1

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

En este paso se procede a configurar este protocolo Ospf área 0 en R1 en las interfaces gigabitethernet, luego enunciamos las redes conectadas directamente, se establece la interfaz Lan (loopback) como pasiva, en la sumarización automática no

se configura para este tipo de protocolo no realiza un resumen automático, por lo que no es un comando necesario, como podemos observar en a la siguiente tabla.

Tabla 26. Configuración del OSPF en R1

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R1(config)#int g0/1 R1(config-if)# bandwidth 1000000 R1(config)#exit R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1 R1(config-router)#auto-cost reference-bandwidth 1000
Anunciar las redes conectadas directamente	R1(config-router)#network 172.16.1.0 0.0.0.255 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R1(config-router)#passive-interface g0/1
Desactive la sumarización automática.	R1(config-router)#no auto-summary OSPF, no realiza un resumen automático, por lo que no es un comando necesario

2.5.2 Paso 2: Configurar OSPF en R2

La configuración del R2 incluye las siguientes tareas:
En la configuración de R2 en este paso se realiza las mismas configuraciones que en el paso anterior del protocolo OSPF.

En este paso se procede a configurar el protocolo Ospf área 0 en R2 en las interfaces gigabitethernet, luego enunciamos las redes conectadas directamente, se establece la interfaz LAN (loopback) como pasiva, en la sumarización automática no se configura para este tipo de protocolo no realiza un resumen automático, por lo que no es un comando necesario, como podemos observar en a la siguiente tabla.

Tabla 27. Configuración OSPF R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0 Se configura la interface La cantidad máxima de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado	R2(config)#int s0/0/0 R2(config-if)# bandwidth 1000000 R2(config)#exit R2(config)#router ospf 1 R2(config-router)#router-id 2.2.2.2 R2(config-router)#auto-cost reference-bandwidth 1000
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva. Se utiliza en todos los protocolos de enrutamiento para desactivar las actualizaciones enviando desde una determinada interfaz.	R2(config-router)#passive-interface s0/0/0 R2(config-router)#passive-interface s0/0/1
Desactive la sumarización automática.	R2(config-router)#no auto-summary OSPF, no realiza un resumen automático, por lo que no es un comando necesario

2.5.3 Paso 3: Configurar OSPF en el R3

La configuración del R3 incluye las siguientes tareas:

En este paso se procede a configurar el protocolo Ospf área 0 en R3 en las interfaces gigabitethernet, luego enunciamos las redes IPv4 conectadas directamente, se establece la interfaz Lan (loopback) como pasiva, en la sumarización automática no se configura para este tipo de protocolo no realiza un resumen automático, por lo que no es un comando necesario, como podemos observar en a la siguiente tabla.

Tabla 28. Configuración OSPF R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#int s0/0/1 R3(config-if)# bandwidth 1000000

Se configura la interface La cantidad máxima de datos transmitidos a través de una conexión a Internet en un período de tiempo determinado	R3(config)#exit R3(config)#router ospf 1 R3(config-router)#router-id 3.3.3.3 R3(config-router)#auto-cost reference-bandwidth 1000
Anunciar redes IPv4 conectadas directamente Se utiliza el comando Network la ip y el área.	R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#network 192.16.4.0 0.0.0.255 area 0 R3(config-router)#network 192.16.5.0 0.0.0.255 area 0 R3(config-router)#network 192.16.6.0 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
Desactive la sumarización automática. OSPF, no realiza un resumen automático, por lo que no es un comando necesario	R3(config-router)#no auto summary

2.5.4 Paso 4: Verificar la información de OSPF

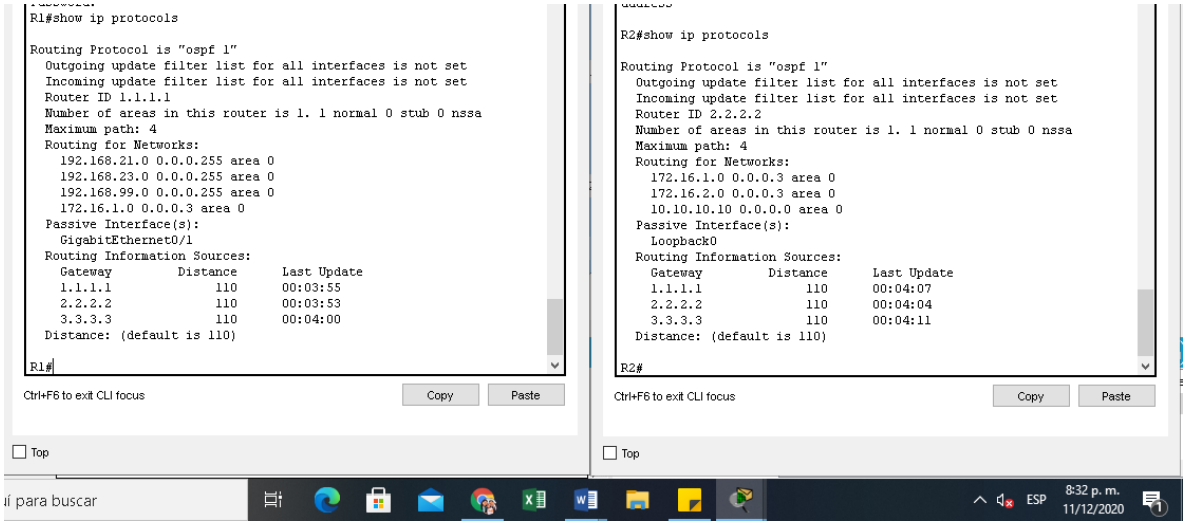
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información.
En este paso se Verifico el protocolo OSPF esté funcionando como se espera, se realizan las siguientes preguntas las podemos observar en la siguiente tabla.

Tabla 29. Verificación de la información 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 protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run

En este paso se Verifico el protocolo OSPF esté funcionando como se espera, se realizan las pruebas con los comandos como podemos observar en las siguiente figura con el Comando show ip protocols en los tres Router R1, R2 y R3

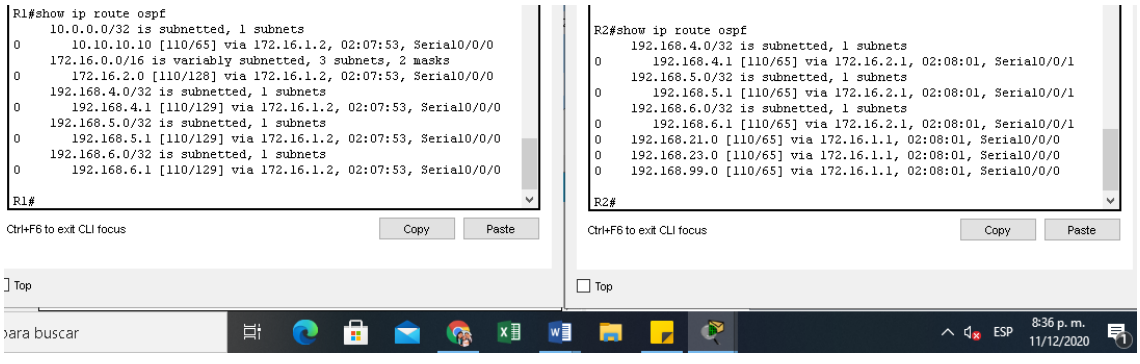
Figura 29. Comando show ip protocols *en R1, R2*



Fuente: Autor

Se emplea el siguiente Comando show ip Router Ospf en R1, R2 y R3, obteniendo los siguientes resultados, lo podemos observar en la siguiente figura implementando el Comando show ip route ospf en los tres Router en R1, R2 y R3

Figura 30. Comando show ip route ospf en R1, R2



Fuente: Autor

2.6 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

En este paso se realizó la configuración en R1 como servidor de DHCP para las VLAN 21 y 23, las tareas de configuración para R1 implementando un pool DHCP para las VLan 21 y 23.

Tabla 30. Configuración DHCP y NAT en R1

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.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccnasa.com R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit

2.6.2 Paso 1: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

En este paso se creó una base de datos local con una cuenta de usuario, se requería en la topología habilitar el servicio del servidor HTTP, en el software de simulación no lo permite configurarlo por esta razón no se configura, se crea la Nat estática al servidor Web y asignamos la interfaz interna y externa para esta Nat estática, se configura la NAT dinámica dentro de una ACL privada, continuamos los pasos de configuración donde definimos el pool de direcciones IP publicas utilizables y por lo último definimos la traducción de Nat dinámica, lo podemos observar en la siguiente tabla:

Tabla 31. R2 Configuración NAT y Estática dinámica

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** Comandos R2(config)#username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	En el programa simulación no se puede configurar este comando
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 R2(config)#exit
Crear una NAT estática al Servidor web.	Dirección global interna: **209.165.200.229** Comandos R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
Asignar la interfaz interna y externa para la NAT estática	R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside R2(config-if)#exit
Configurar la NAT dinámica dentro de una ACL privada	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225 – 209.165.200.228** R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248

Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

2.6.3 Paso: 3 Verificar el protocolo DHCP y la NAT estática

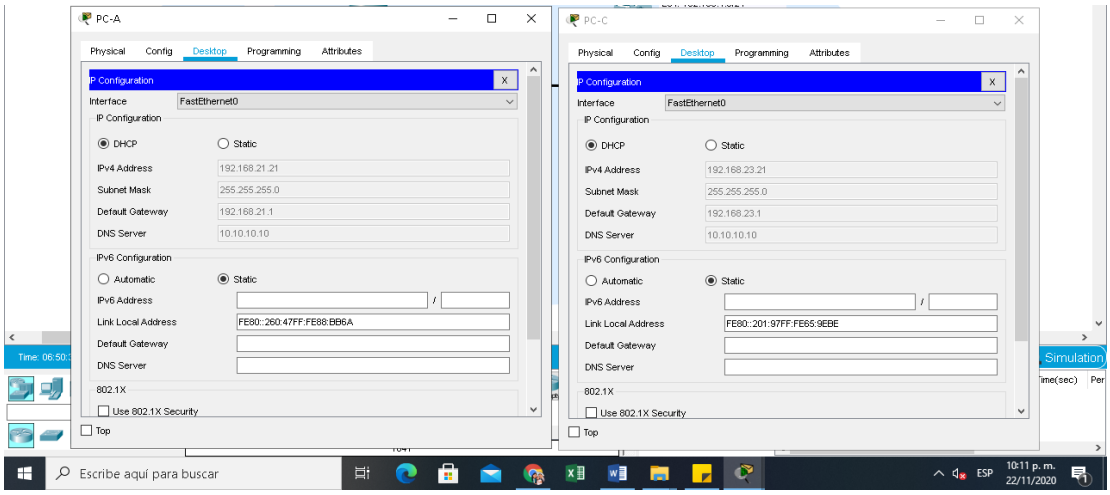
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente, como se observa en la siguiente tabla.

Tabla 32. Verificación DHCP y la NAT Estática

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	PC-A, Desktop, DHCP. IP Address 192.168.21.21 Subnet Mask 255.255.255.0 Default Gateway 192.168.21.1 DNS Server 10.10.10.10 Link local Address FE80::260:47FF:FF88:BB6A
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	PC-A, Desktop, DHCP. IP Address 192.168.23.21 Subnet Mask 255.255.255.0 Default Gateway 192.168.23.1 DNS Server 10.10.10.10 Link local Address FE80::201:97FF:FF65:9EBE
Verificar que la PC-A pueda hacer ping a la PC- C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Ping 192.168.23.21
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Servidor internet, Desktop, Web Browser, WRL: http://209.165.200.237

Utilice las anteriores tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta, como lo podemos observar en la siguiente figura.

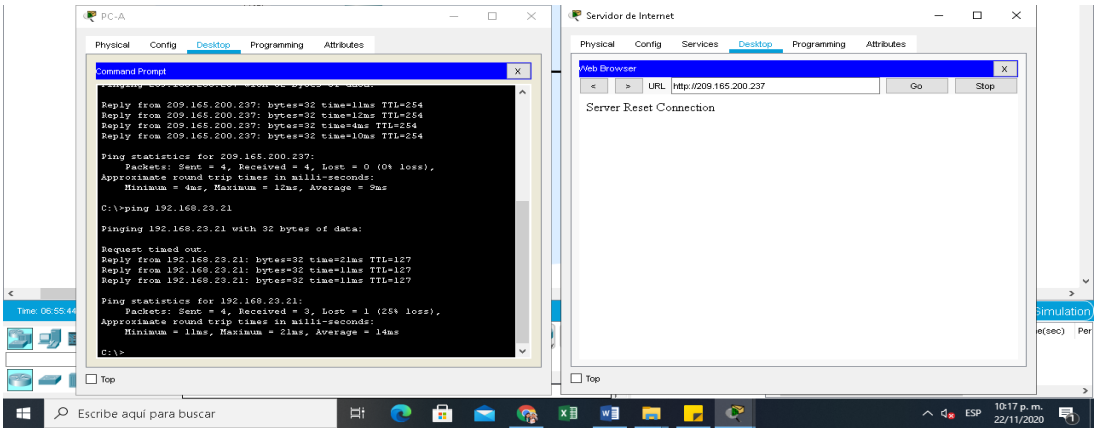
Figura 31. Verificación protocolo DHCP en PC-A y PC-B



Fuente: Autor

Como podemos observar en la imagen la configuración IP que tienen los dos equipos.

Figura 32. Verificación PC-A ping al servidor internet



Fuente: Autor

Desde PC-A se realiza la prueba de conectividad por medio del comando Ping. Dando respuesta correcta hacia el servidor.

2.7 Parte 6: Configurar NTP

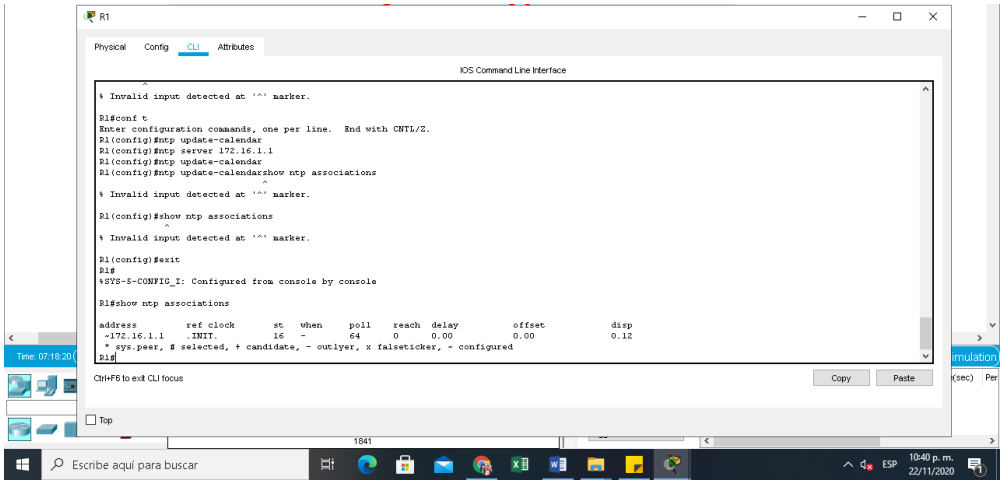
En este paso se realizó la configuración de la fecha y hora en los Routers R1 y R2 observamos en la siguiente tabla:

Tabla 33. Se configura en R2 la fecha y hora

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 9:00:00 05 March 2016
Configure R2 como un Maestro NTP.	Nivel de estrato: **5** R2(config)#NTP master 5
Configurar R1 como un cliente NTP.	Servidor: **R2** R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario Periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	Configure terminal Ntp server 172.16.1.1 Ntp update-calendar End Show ntp associations

Comando show ntp associations la configuración de R1

Figura 33. Verificación NTP en R1



Fuente: Autor

En este paso Verificamos con el comando show ntp associations la configuración de R1 de la fecha y hora.

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

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

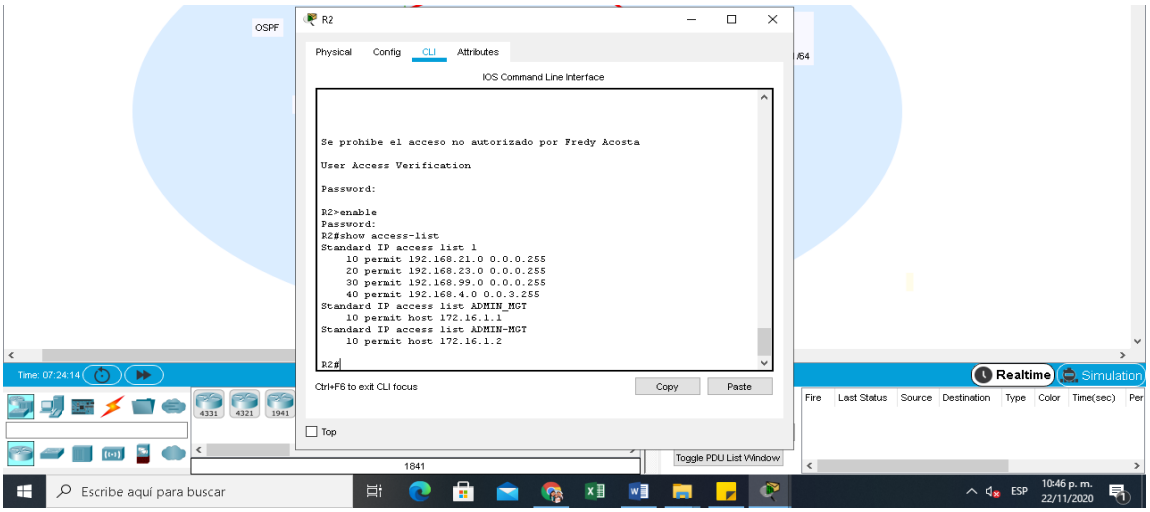
En este paso se realiza la configuración en restringir el acceso a las líneas VTY en el R2 y configurar las listas de control de acceso al (ACL), como lo podemos observar en la siguiente tabla.

Tabla 34. Restringir el acceso a las líneas VTY en 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**
Aplicar la ACL con nombre a las líneas VTY	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.2 R2(config-std-nacl)#exit R2(config)#
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT R2(config-line)#transport input telnet R2(config-line)#exit R2(config) #
Verificar que la ACL funcione como se espera	Show access-list

Como observamos se realizan las configuraciones en el Router R2 aplicando los comandos para configurar líneas VTY

Figura 34. Configuración y verificación listas control



Fuente: Autor

Como observamos en la figura la configuración y verificación de las listas de control realizando los pasos anteriores de la tabla y luego con el comando Show access-list nos muestra las listas de control.

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

Tabla 35. Comando Adecuado de CLI

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Comando R2#show access-list
Restablecer los contadores de una lista de acceso	Comando R2(config)#clear ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Comando R2#show ip interface

¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC- C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. R2#show ip nat translation
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Comando R2#clear ip nat translation

CONCLUSIONES

Finalmente podemos Concluir el desarrollo de dos escenarios de red LAN nos permitió comprender y conocer la importancia en su implementación, aplicando las configuraciones de distintos dispositivos como Router, switch y PCS configurando una red de comunicación implementando los protocolos.

En el primer escenario se configuro los dispositivos de una red pequeña. Comprendida por los elementos Router, dos switch y dos equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados, se realizaron pruebas de conectividad dando los resultados esperados.

En el segundo escenario se configuro también una red pequeña para que admita conectividad entre direccionamiento IPv4 e IPv6, seguridad de switch, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante su desarrollo, se probó y registro la red mediante los comandos comunes de CLI, dando los resultados correctos.

Se utilizó la herramienta de simulación Cisco Packet Tracer aplicando los conocimientos adquiridos en CCNA Cisco para dar solución de estos dos escenarios.

Comprensión y destreza de los comandos para una óptima configuración y así mismo su comprobación de cada escenario.

BIBLIOGRAFIA

(s.f.). Obtenido de https://www.cisco.com/c/es_mx/solutio

ns/small-business/resource-center/networking/what-is-a-router.html

CISCO. (s.f.). *CISCO*. Obtenido de CISCO: https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html

conceptodefinicion.de. (26 de 07 de 2019). *conceptodefinicion.de*. Obtenido de conceptodefinicion.de: https://conceptodefinicion.de/interfaz/

González, M. S. (08 de 11 de 2013). *Redes telematicas*. Obtenido de Redes telematicas: http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

IONOS. (26 de 03 de 2019). *Digital Guide IONOS*. Obtenido de IONOS: https://www.ionos.es/digitalguide/servidores/know-how/vlan/

redesTeleco. (s.f.). *redesteleco.com*. Obtenido de redesteleco.com Redes, Cloud y Tecnología en general : https://redesteleco.com/cisco/

Temática: Ethernet

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

Temática: Capa de red

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

Temática: Direccionamiento IP

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

Temática: División de redes IP en subredes

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

Temática: Capa de transporte

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

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

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

Temática: Configuración de un sistema operativo de red
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

ANEXOS

ANEXO 1

Enlace de descarga de archivos de simulación 1 y 2

https://drive.google.com/drive/folders/1HTsipbVMvj-mRsbplfZrmW6H0E52z_GP?usp=sharing

ANEXO 2

Artículo Científico IEEE

https://drive.google.com/drive/folders/1HTsipbVMvj-mRsbplfZrmW6H0E52z_GP?usp=sharing