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

SANTIAGO ELÍAS PALOMINO FRANCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍAS
INGENIERIA ELECTRONICA
VALLEDUPAR
2020

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

SANTIAGO ELÍAS PALOMINO FRANCO

PRUEBA DE HABILIDADES PRÁCTICAS PARA OPTAR EL TITULO DE INGENIERO ELECTRÓNICO.

JUAN CARLOS VESGA
DIRECTOR CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS Y DE INGENIERÍAS
INGENIERÍA ELECTRÓNICA
VALLEDUPAR
2020

Dedico este trabajo a mis padres **Santiago y Oliva**, quienes siempre buscaron la manera de mi superación a través de la educación, a mi esposa **Lina Rada**, quien con su Amor y apoyo incondicional hizo parte fundamental de este proceso que hoy culmina.

AGRADECIMIENTOS

Agradezco a Dios quien siempre está presente en todos los actos de mi vida.

A mis padres y hermanos, quienes con su apoyo incondicional y constante fueron pilares importantes la consecución de esta meta.

A mis hijos María Fernanda, Mateo, Mariana, Mattías y Mayté quienes son una de mi principal motivación para cumplir el sueño de ser Ingeniero Electrónico y a quienes Amo con lo más profundo de mi ser.

Profundo agradecimiento a toda mi familia Unadista, tutores, Directores, compañeros y a todos los que con su paciencia, sapiensa y entrega me dieron los medios y orientación en el desarrollo de este proceso de formación.

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Valledupar, 30 Noviembre de 2020

TABLA DE CONTENIDO

LISTA DE ANEXOS

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACL (Access control list): contiene reglas que otorgan o niegan el **acceso** a ciertos entornos digitales. Hay dos tipos: Sistema de archivos filter el acceso a los archivos y / o directorios. Las ACL del sistema de archivos le dicen a los sistemas operativos qué usuarios pueden acceder al sistema y qué privilegios tienen los usuarios.

CHAP (Challenge Handshake Authentication Protocol): Es un método de autenticación remota o inalámbrica.

ENRUTAMIENTO: es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

IPv4 (Internet Protocol version 4, IPv4): protocolo de interconexión de redes basadas en internet.

LAN: (Local Área Network) es una red que conecta uno o más ordenadores dentro de un ámbito pequeño y limitado. Se puede encontrar a través de cable Ethernet, lo que significa que todos los dispositivos se interconectan mediante un router.

RESUMEN

En el presente trabajo se mostrará de manera simulada en la herramienta Packet Tracer dos escenarios de redes en los cuales se muestra el desarrollo paso a paso el desarrollo de las tareas asignadas en cada uno de los dos escenarios propuestos, documentando la solución los cuales corresponden al registro de la configuración de cada uno de los dispositivos que hacen parte de las redes. La descripción detallada de cada una de las etapas de configuración, verificando conectividad en cada uno de sus pasos.

PALABRAS CLAVE: Protocolo, Redes, topología, Router, Switch, Enrutamiento, Red.

INTRODUCCIÓN

La revolución que ha generado el internet en mucho ámbitos de nuestra cotidianidad, cambiando de manera radical la manera de comunicarnos. Hoy día lo utilizamos para casi todas las actividades. Desde enviar fotos desde una aplicación de mensajería instantánea, leer noticias en la página o una aplicación de un periódico de cualquier parte del mundo o simplemente comprar nuestra cena.

Debido a esto cobra importancia el uso de estas redes de manera eficaz y segura, evitando los riesgos que contienen el estar en la red. Precisamente como ingenieros debemos estar a la vanguardia en el diseño, implementación y administración de redes confiables, seguras y eficientes.

En el presente informe se demostrará de forma práctica los conocimientos adquiridos durante el curso Diplomado de Profundización CCNA de CISCO aplicando las habilidades y competencias adquiridas a lo largo de este.

Se configuraran los dispositivos en cada uno de los escenarios y al final se verificaran si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente.

Aplicando conceptos fundamentales de uso en configuración y administración de redes, tales como: protocolos de enrutamiento RIP, OSPF, listas de control de acceso (ACL), DHCP, VLANs, Servicios NAT y PAT, Redireccionamiento, Tipos de Seguridad, LAN, Autenticación PAP y CHAP, entre otros.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Demostrar el grado de desarrollo de competencias y habilidades adquiridas a lo largo del diplomado de redes CCNA de CISCO.

2.2 OBJETIVOS ESPECÍFICOS

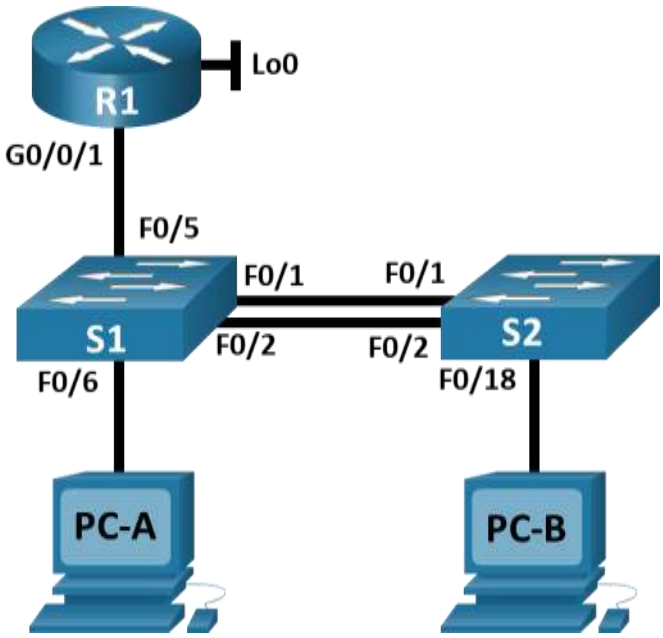
- Implementar en la herramienta de simulación Packet Tracer, la topología de red de los dos escenarios propuestos.
- Realizar la configuración básica a cada uno de los dispositivos de las redes.
- Configurar los dispositivos: router, switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los host soportados.
- Configurar el enrutamiento entre VLAN, DHCP, Etherchannel y portsecurity.
- Configurar los dispositivos con medidas de seguridad para proteger las redes, verificar que estén implementadas apropiadas y con funcionamiento correcto.
- control de accesos ACL y el protocolo de tiempo de red NTP servidor/ cliente.
- Evaluar y probar las redes mediante comandos comunes CLI
- Elaborar Vlans e inter Vlan Routing.
- Determinar la configuración necesaria para la implementación de protocolo de routing OPSFv2.
- Implementar el protocolo dinámico de Routing DHCP.
- la traducción de direcciones de red inalámbrica y estática NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL Verificar conectividad entre los dispositivos de una topología.

Figura 1. Topología Escenario 1

Escenario 1

Topología

Fig. 1 topología de Escenario 1



Fuente: Prueba de Habilidades Cisco 2020 16-04

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

Tabla 1 VLAN

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

Tabla 2. Asignación de direcciones

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

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

Parte 1: Inicializar y Recargar y Configurar aspectos basicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

De acuerdo a lo requerido, se realizará la configuración de cada uno de los dispositivos de la topología planteada iniciando con el borrado de las configuraciones de inicio y las Vlan del router y del switch, eliminando así cualquier configuración previa en los dispositivos.

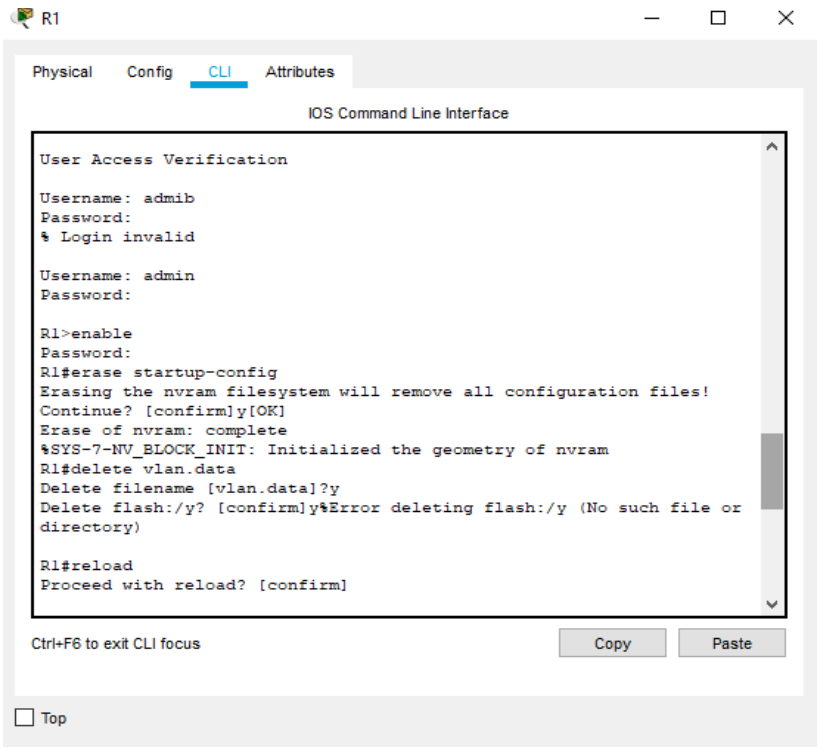
En la tabla 3. Se muestran los comandos necesarios para el borrado de las Vlan, la inicialización del Router y los Switchs

Tabla 3. Comandos para inicializar Router

Comando	Función
R1>enable	Ingresar al modo Exec privilegiado
R1#erase startup-config	Borrar la configuración inicial del dispositivo.
R1#reload	Reiniciar el dispositivo.

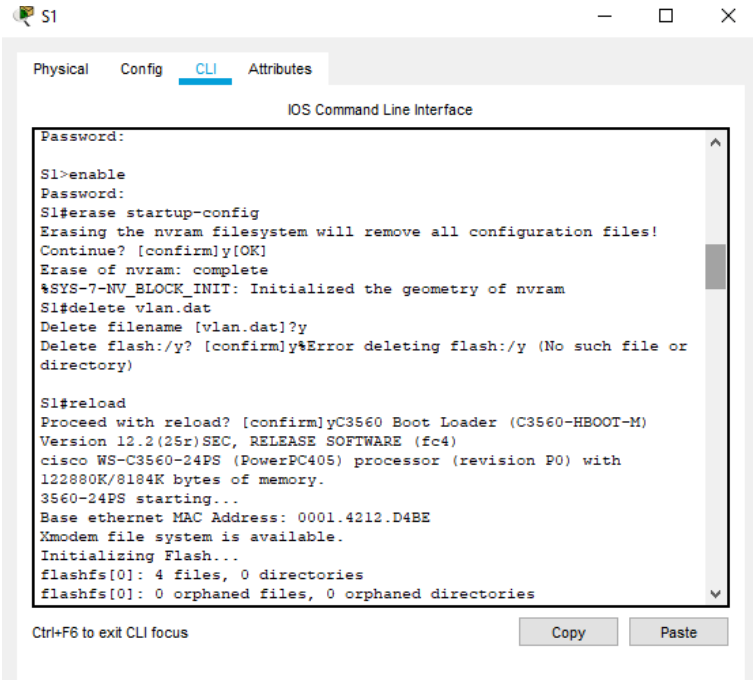
En la Fig 2, 3 y 4, Se muestra el resultado de la configuración del R1 y los Switchs

Fig 2. Inicialización Router



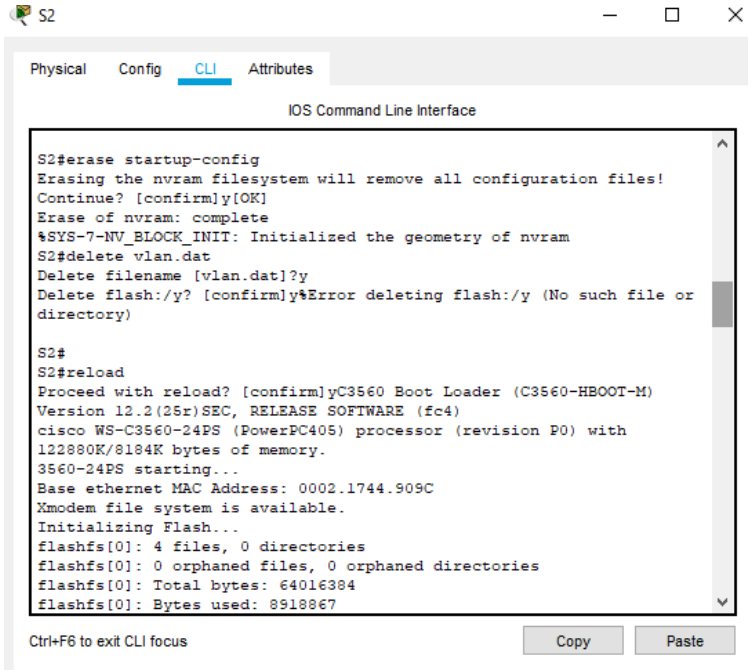
Fuente: Autor

Fig 3. Inicialización de Switch 1



Fuente: Autor

Fig 4. Inicialización de Switch 2



Fuente: Autor

Paso 2: Configurar R1

Con los comandos de la Tabla 4, se configuran los parametros basicos del Router 1 como son:
Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY. Así mismo se establece una longitud minima para las contraseñas. Se habilita el routing Ipv6, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al router. Así kismo se configuran las interfaces,subinterfaces y el Loopback0.

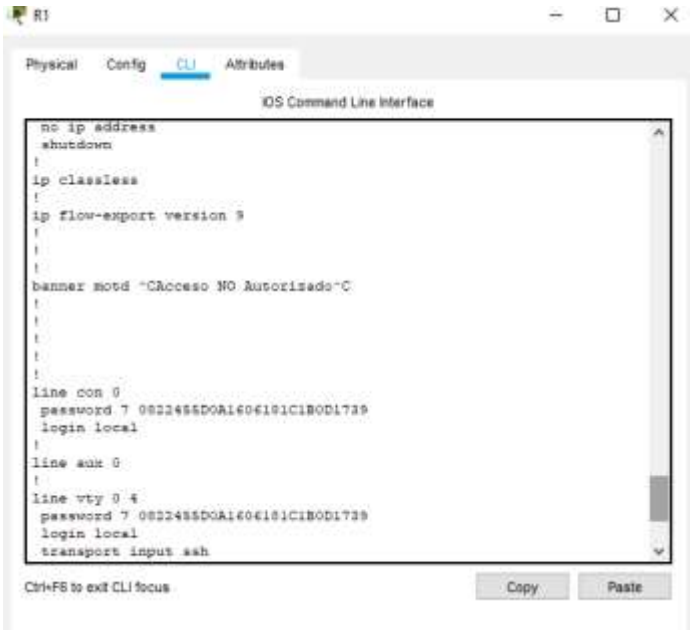
Tabla 4. Comandos de configuración Básica para R1.

Tarea	Especificación
Desactivar la búsqueda DNS	R>enable configure terminal no ip domain-lookup
Nombre del router	hostname R1
Nombre de dominio	ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	enable secret ciscoconpass
Contraseña de acceso a la consola	line console 0 password ciscoconpass login local
Establecer la longitud mínima para las contraseñas	security password min-length 10
Crear un usuario administrativo en la base de datos local	username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 4 password ciscoconpass login local
Configurar VTY solo aceptando SSH	transport input ssh exit
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configure un MOTD Banner	banner motd #Acceso No Autorizado#
Habilitar el routing IPv6	ipV6 unicast-routing

Tarea	Especificación
Configurar interfaz G0/0/1 y subinterfaces	int G0/1 description connection to S1 ip address 10.19.8.0 255.255.255.252 ipv6 address 2001:db8:acad:a: :1 /64 ipv6 address fe80::1 link-local no shutdown exit int G0/1.2 ip address 10.19.8.1 255.255.255.192 ipv6 address 2001:db8:acad:a: :1 /64 ipv6 address fe80::1 link-local no shutdown exit int G0/1.3 ip address 10.19.8.65 255.255.255.224 ipv6 address 2001:db8:acad:b: :1 /64 ipv6 address fe80::1 link-local no shutdown exit int G0/1.4 ip address 10.19.8.97 255.255.255.248 ipv6 address 2001:db8:acad:c: :1 /64 ipv6 address fe80::1 link-local no shutdown exit int G0/1.6 encapsulation dot1q 6 exit int G0/1 no shutdown
Configure el Loopback0 interface	Int Lo 0 description connection to R1 ip address 209.165.201.1 255.255.255.224 ipv6 address 2001:db8:acad:209::1/64 ipv6 address fe80::1 link-local
Generar una clave de cifrado RSA	crypto key generate isa modulus 1024

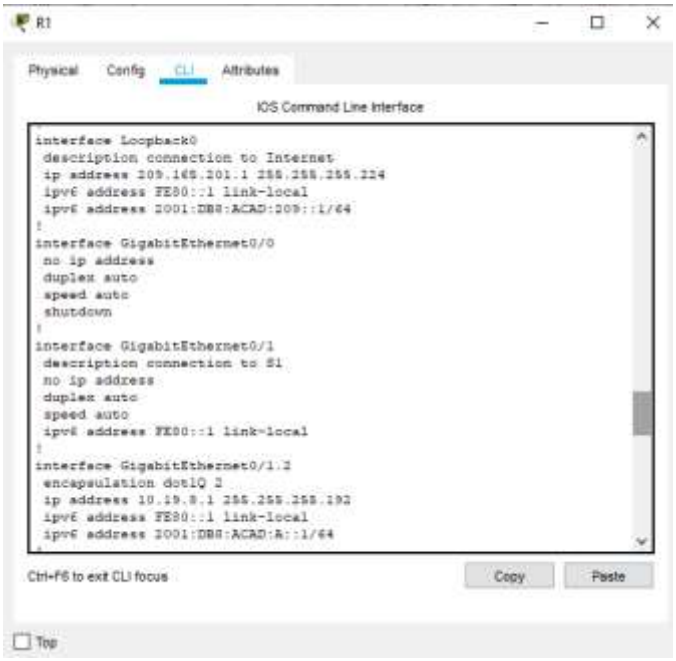
En las figuras 5 y 6 se muestra el resultado de las las configuraciones realizadas al R 1

Fig 5. Configuración básica de R1



Fuente: Autor

Fig 6. Configuración de interfaces y loopback en R1



Fuente: Autor

Paso 3: Configure S1 y S2.

Con los comandos de la tabla 5, se configuran los parametros basicos de los Switch 1 y 2 como son:
Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY. Así mismo se establece una longitud minima para las contraseñas. Se habilita el routing Ipv6, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al router. Se configura la interfaz de admiistración y el gateway predeterminado.

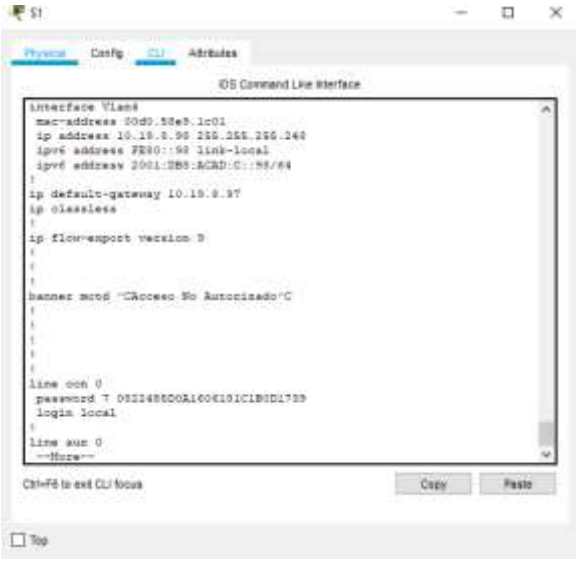
Tabla 5. Comandos configuración Básica de S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	enable switch>configure terminal no ip domain-lookup
Nombre del switch	hostname S1
Nombre de dominio	ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	enable secret ciscoconpass
Contraseña de acceso a la consola	line console 0 password ciscoconpass login local
Crear un usuario administrativo en la base de datos local	username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 4 password ciscoconpass login local exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	service password-encryption
Configurar un MOTD Banner	banner motd #Acceso no Autorizado#
Generar una clave de cifrado RSA	crypto key generate rsa isa modulus 1024
Configurar la interfaz de administración (SVI)	int vlan 4 ip address 10.19.8.98 255.255.255.248 ipv6 address 2001:db8:acad:c::98/64 ipv6 address fe80::98 link-local no shutdown

Tarea	Especificación
Configuración del gateway predeterminado	Ip default-gateway 10.19.8.97

En las figuras 7 y 8 se muestra el resultado de las configuraciones básicas realizadas al S1 y S2

Fig 7. Configuración básica en S1



Fuente: Autor

Fig 8. Configuración básica en S2

Fuente: Autor

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

Paso 1: Configurar S1

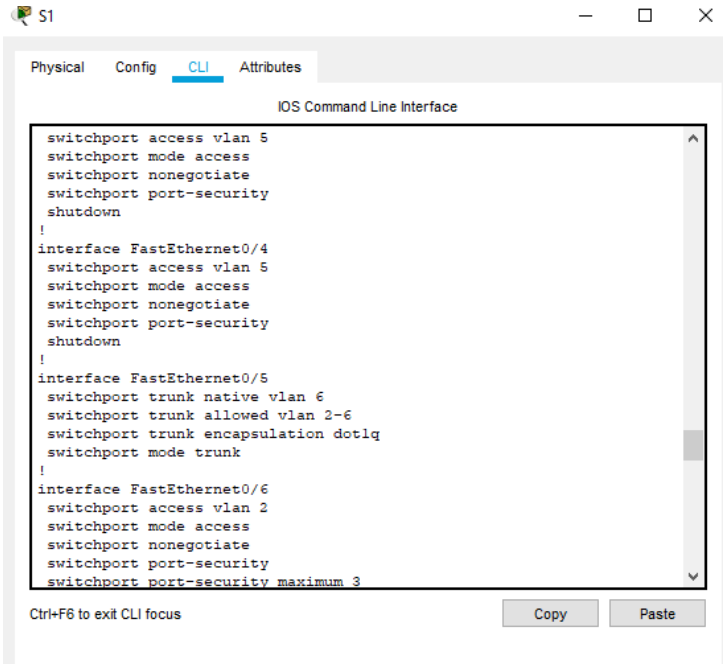
En la tabla 6, se muestran los comandos de configuración de la infraestructura de red. Se crean las Vlan en S1, se crean la troncal, se crea un grupo EtherChannel, se configura el puerto del Host, se configuran los parametros de seguridad de los puertos de acceso y se protegen los puertos que no se están usando.

Tabla 6. La configuración de la infraestructura de red en S1

Tarea	Especificación
Crear VLAN	vlan 2 name Bikes vlan 3 name Trikes vlan 4 name Management vlan 5 name Parking vlan 6 name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	interface f0/1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 switchport trunk allowed vlan 2,3,4,5,6 interface f0/2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 switchport trunk allowed vlan 2,3,4,5,6 Interface f0/5 switchport trunk encapsulation dot1q Switchport mode trunk Switch trunk native Vlan 6 switchport trunk allowed vlan 2,3,4,5,6

Tarea	Especificación
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Interface range FastEthernet0/1-2 Channel-group 1 mode active
Configurar el puerto de acceso de host para VLAN 2	interface f0/6 switchport mode access switchport access vlan 2 no shutdown
Configurar la seguridad del puerto en los puertos de acceso	interface f0/6 switchport mode access switchport port-security switchport port-security maximum 3 no shutdown
Proteja todas las interfaces no utilizadas	interface range Fastethernet 0/3-4 interface range Fastethernet 0/6-24 switchport mode access switchport access vlan 5 switchport port-security switchport port-security maximum 1 switchport port-security violation shutdown

Fig 9. Configuracion de estructura de red en S1



Fuente: Autor

Paso 2: Configure el S2.

En la tablas 7, se muestran los comandos de configuración de la estructura de red en el S2. Se crean las Vlan en S2, se crean la troncal, se crea un grupo EtherChannel, se configura el puerto del Host, se configuran los parametros de seguridad de los puertos de acceso y se protegen los puertos que no se están usando.

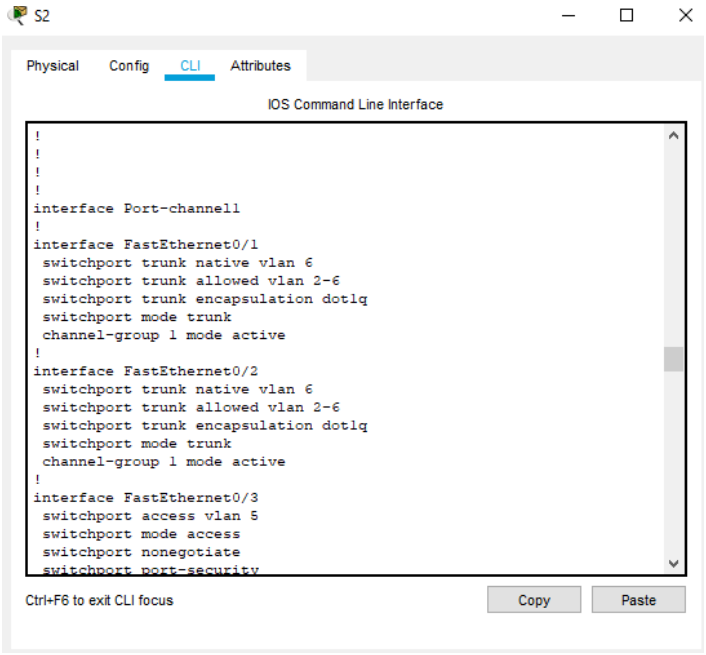
Tabla 7. La configuración de la infraestructura de red en S2

Tarea	Especificación
Crear VLAN	vlan 2 name Bikes vlan 3 name Trikes vlan 4 name Management vlan 5 name Parking vlan 6 name Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	interface f0/1 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 switchport trunk allowed vlan 2,3,4,5,6 interface f0/2 switchport trunk encapsulation dot1q switchport mode trunk switchport trunk native vlan 6 switchport trunk allowed vlan 2,3,4,5,6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Interface range FastEthernet0/1-2 Channel-group 1 mode active
Configurar el puerto de acceso del host para la VLAN 3	interface f0/18 switchport mode access switchport access vlan 3 no shutdown
Configure port-security en los access ports	interface f0/18 switchport mode access switchport port-security switchport port-security maximum 3 no shutdown

Tarea	Especificación
Asegure todas las interfaces no utilizadas.	interface range Fastethernet 0/3-4 interface range Fastethernet 0/6-24 switchport mode access switchport access vlan 5 switchport port-security switchport port-security maximum 1 switchport port-security violation shutdown

La figura 10 nos muestra el resultado de la configuración realizada en el S2

Fig 10. Configuración de estructura de red en S2



Fuente: Autor

Parte 1: Configurar soporte de host

Paso 1: Configure R1

En la tabla 8, se configura el DHCP en la Vlan 2 y la Vlan 3, se configura el Loopback 0 con direción Ipv4 e Ipv6 y el Link Local.

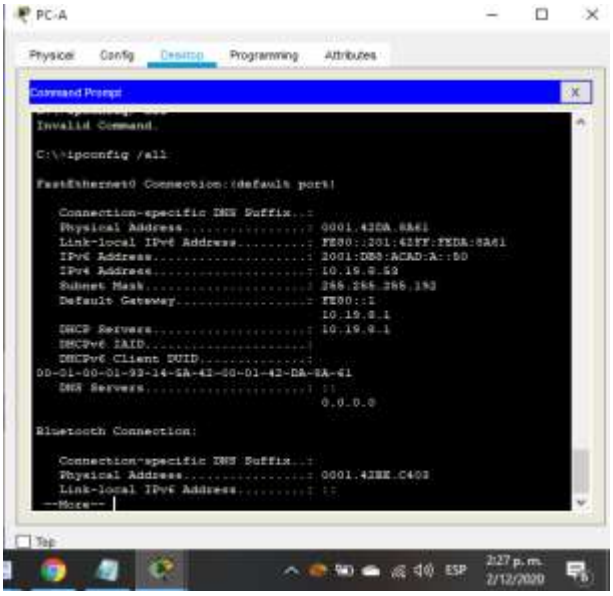
Tabla 8. Configuración soporte de host en R1.

Tarea	Especificación
Configure Default Routing	int Lo 0 description connection to Internet ip address 209.165.201.1 255.255.255.224 ipv6 address 2001:db8:acad:209::1/64 ipv6 address fe80::1 link-local
Configurar IPv4 DHCP para VLAN 2	Ip dhcp pool ccna-a.net network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 exit Ip dhcp excluded-address 10.19.8.1 10.19.8.52
Configurar DHCP IPv4 para VLAN 3	Ip dhcp pool ccna-b.net network 10.19.8.0 255.255.255.192 default-router 10.19.8.1 exit Ip dhcp excluded-address 10.19.8.65 10.19.8.85

Paso 2: Configurar los servidores

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

Fig 11. Configuración por medio del comando ipconfig/all de host-A

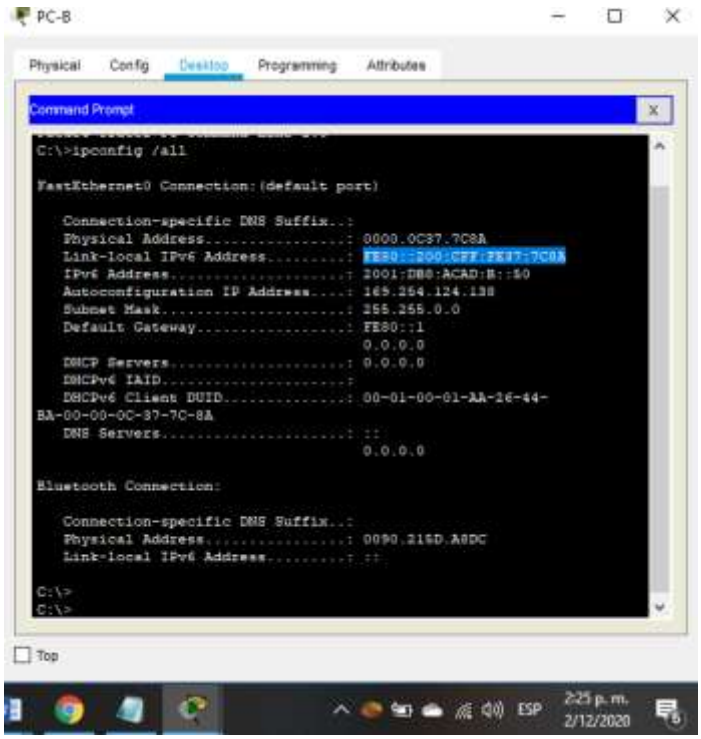


Fuente: Autor

Tabla 9. Configuración de red en PC-A

PC-A Network Configuration	
Descripción	*FastEthernet0 FastEthernet0 Connection:(default port)*
Dirección física	*0001.42DA.8A61*
Dirección IP	*10.19.8.53*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*10.19.8.1*
Gateway predeterminado IPv6	*FE80::1*

Fig 12. Configuración por medio del comando ipconfig/all del host-B



Fuente: Autor

Tabla 10. Configuración de red en PC-B

Configuración de red de PC-B	
Descripción	*FastEthernet0 Connection:(default port)*
Dirección física	0000.0C37.7C8A
Dirección IP	*169.254.124 138*
Máscara de subred	*255.255.0.0*
Gateway predeterminado	*FE80::1*
Gateway predeterminado IPv6	*FE80::200:CFF:FE37:7C8A*

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.

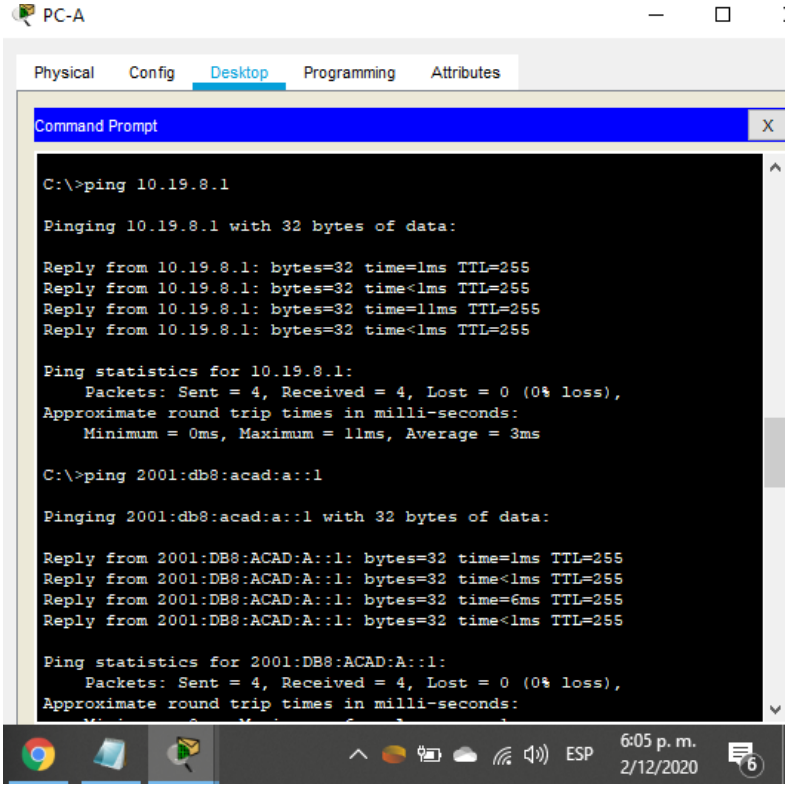
En la tabla 11, se verifica metódicamente la conectividad con cada dispositivo de red.

Tabla 11. Verificación de conectividad en la red.

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

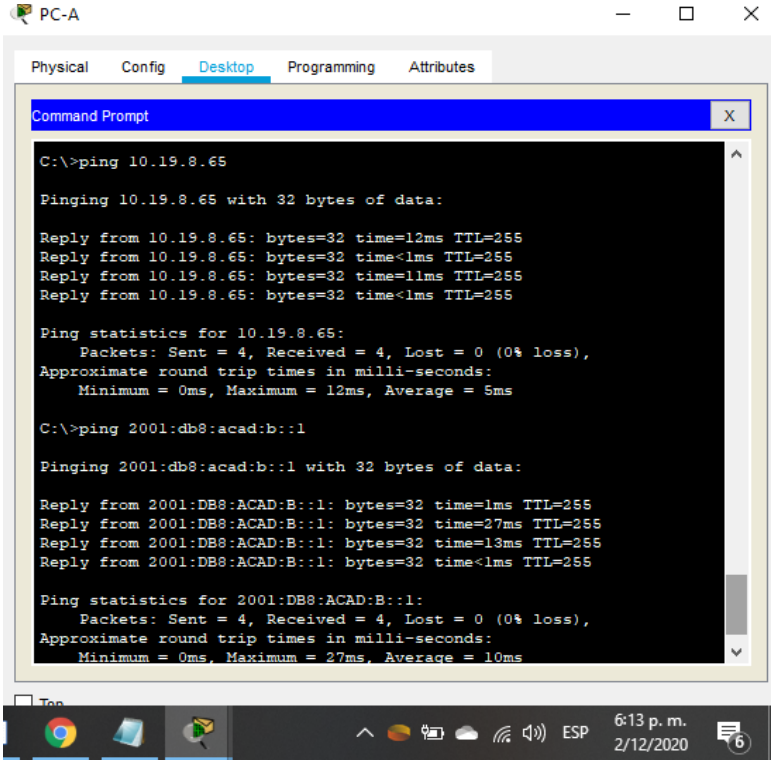
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-B	R1 Bucle 0	Dirección	209.165.201.1	*Efectivo*
		IPv6	2001:db8:acad:209::1	*Efectivo*
	R1, G0/1.2	Dirección	10.19.8.1	*Efectivo*
		IPv6	2001:db8:acad:a::1	*Efectivo*
	R1, G0/1.3	Dirección	10.19.8.65	*Efectivo*
		IPv6	2001:db8:acad:b: :1	*Efectivo*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

Fig 13. Prueba de conectividad mediante comando Ping de PC-A a R1, G0/1.2



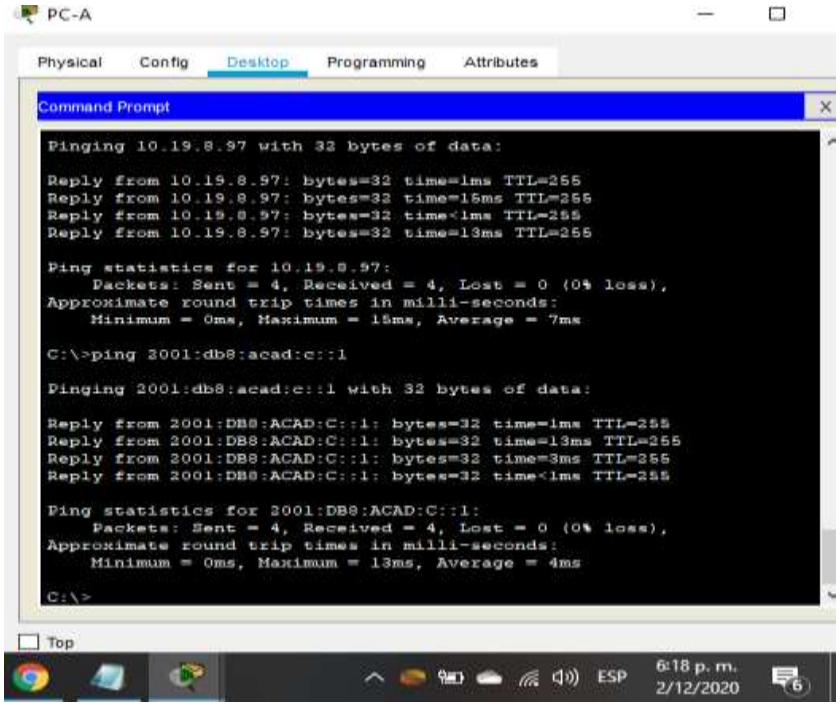
Fuente: Autor

Fig 14. Prueba de conectividad mediante comando Ping de la PC-A a R1



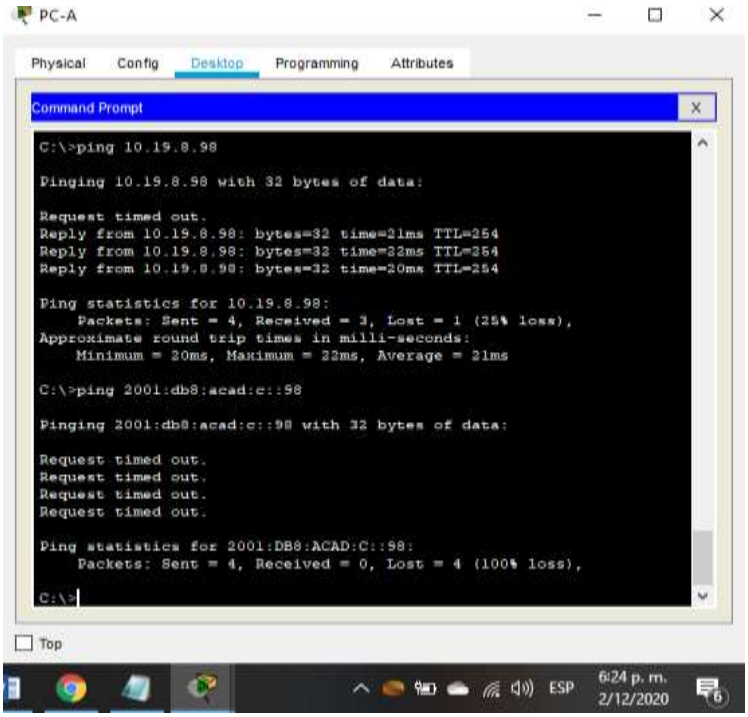
Fuente: Autor

Fig 15.Prueba de conectividad mediante comando Ping de la PC-A a R1, G0/1.4



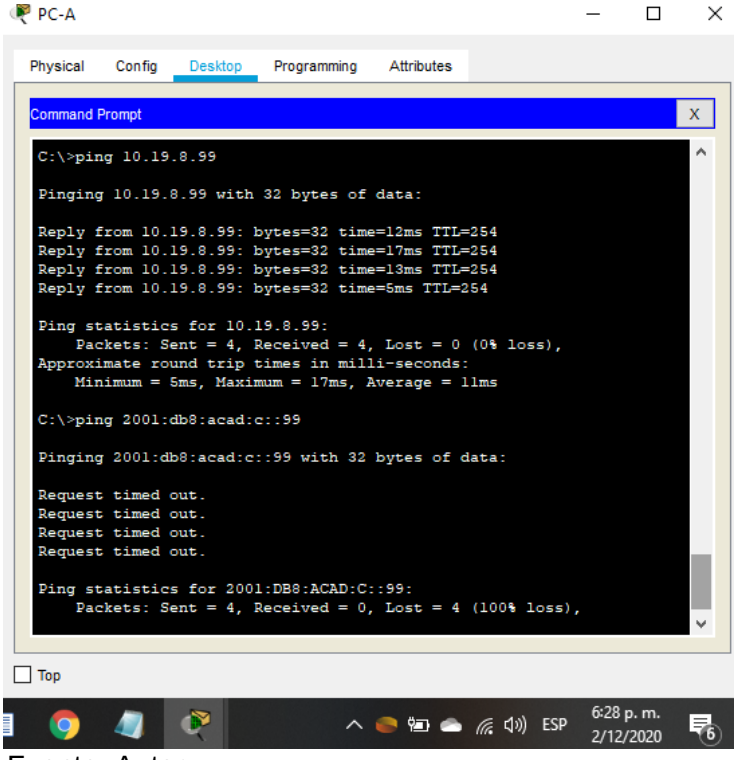
Fuente: Autor

Fig 16.Prueba de conectividad mediante comando Ping de la PC-A a S1, VLAN 4



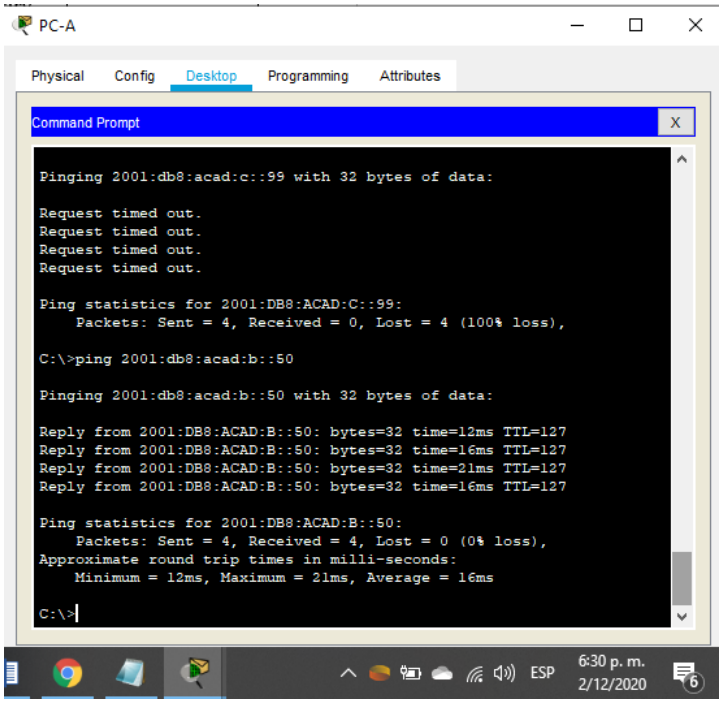
Fuente: Autor

Fig 17. Prueba de conectividad mediante comando Ping de la PC-A a S2, VLAN 4



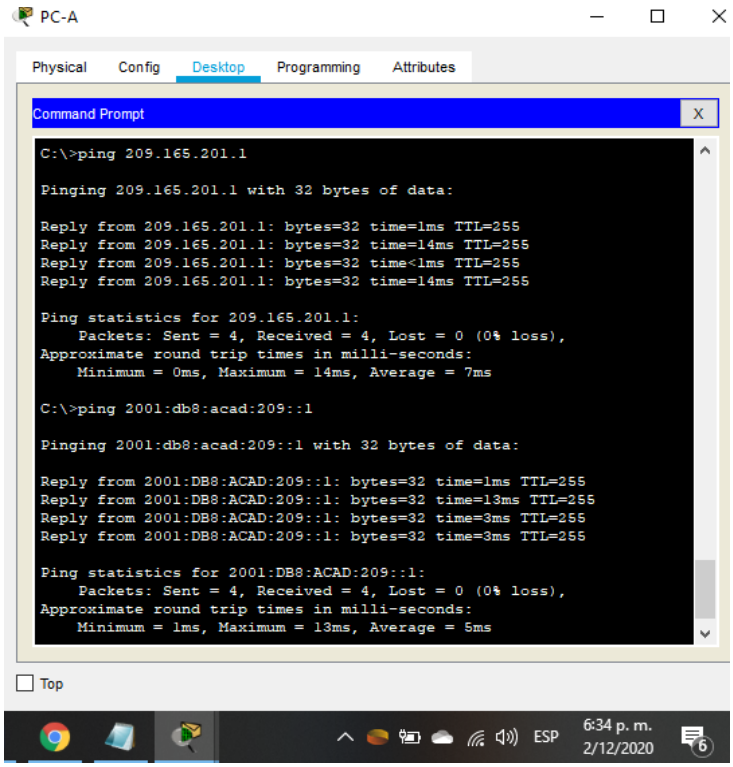
Fuente: Autor

Fig 18. Prueba de conectividad mediante el comando Ping de la PC-A a PC-B



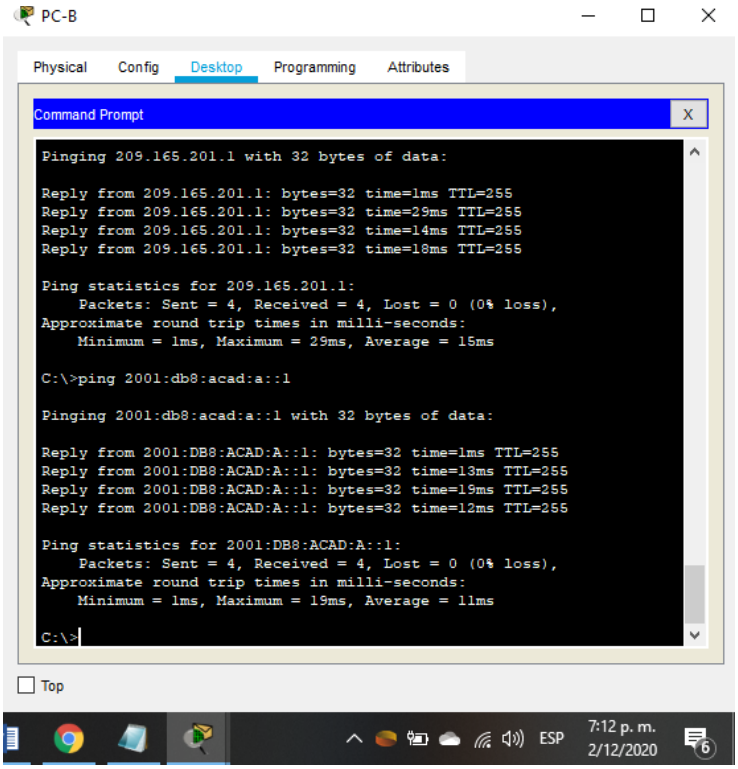
Fuente: Autor

Fig 19. Prueba de conectividad mediante el comando Ping de la PC-A a R1 Bucle 0



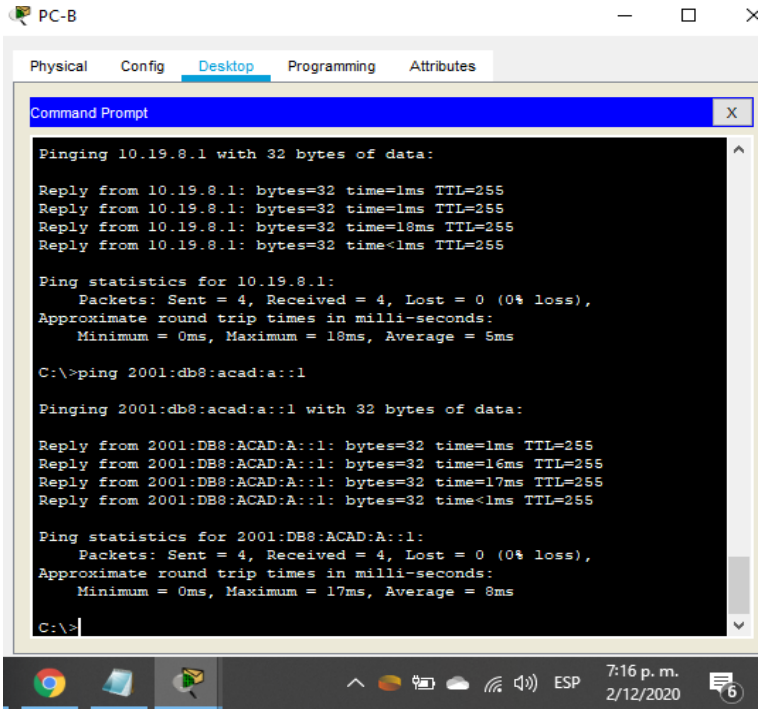
Fuente: Autor

Fig 20. Prueba de conectividad mediante el comando Ping de la PC-B a R1 Bucle 0



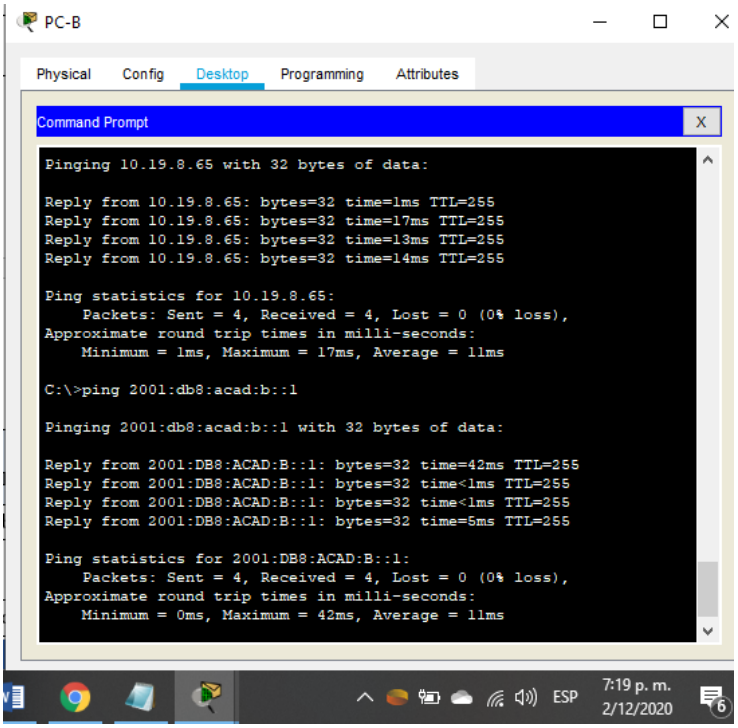
Fuente: Autor

Fig 21. Prueba de conectividad mediante comando Ping de PC-B a R1, G0/1.2



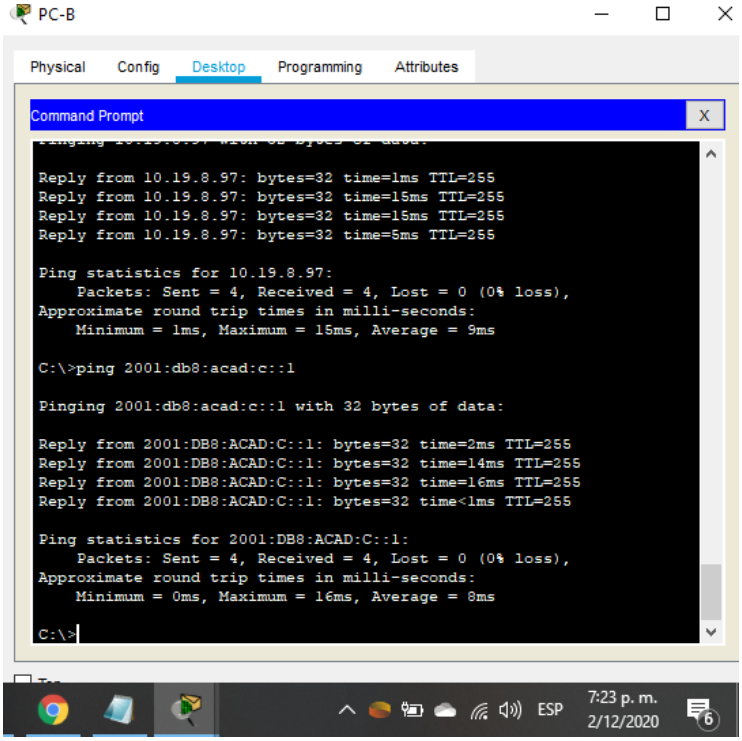
Fuente: Autor

Fig 22. Prueba de conectividad mediante el comando Ping de PC-B a R1, G0/1.3



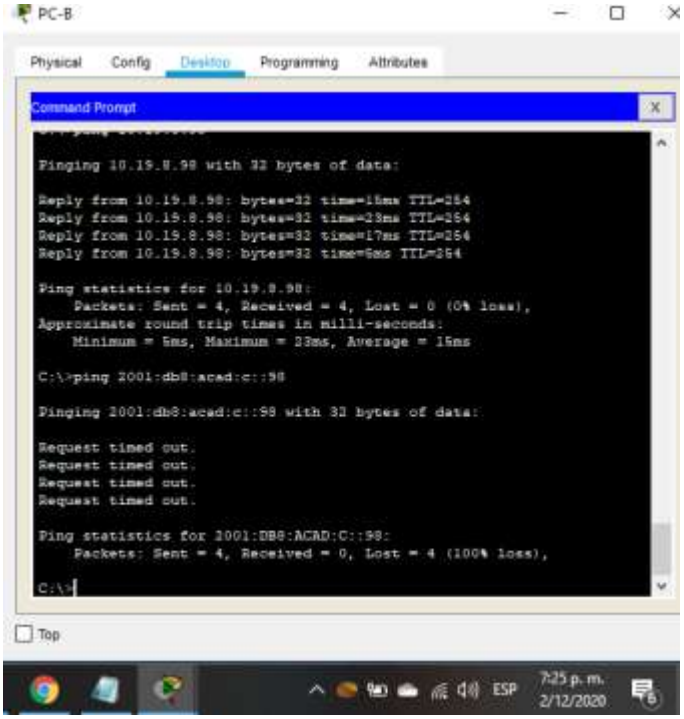
Fuente: Autor

Fig 23. Prueba de conectividad mediante el comando Ping de PC-B a R1, G0/1.4



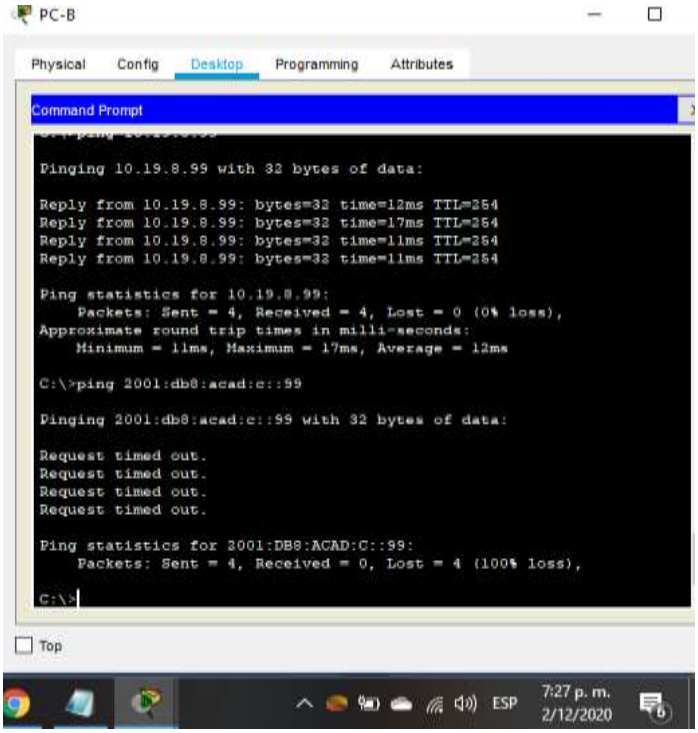
Fuente: Autor

Fig 24.Prueba de conectividad mediante el comando Ping de PC-B a S1, VLAN 4



Fuente: Autor

Fig 25.Prueba de conectividad mediante el comando Ping de PC-B a S2, VLAN 4

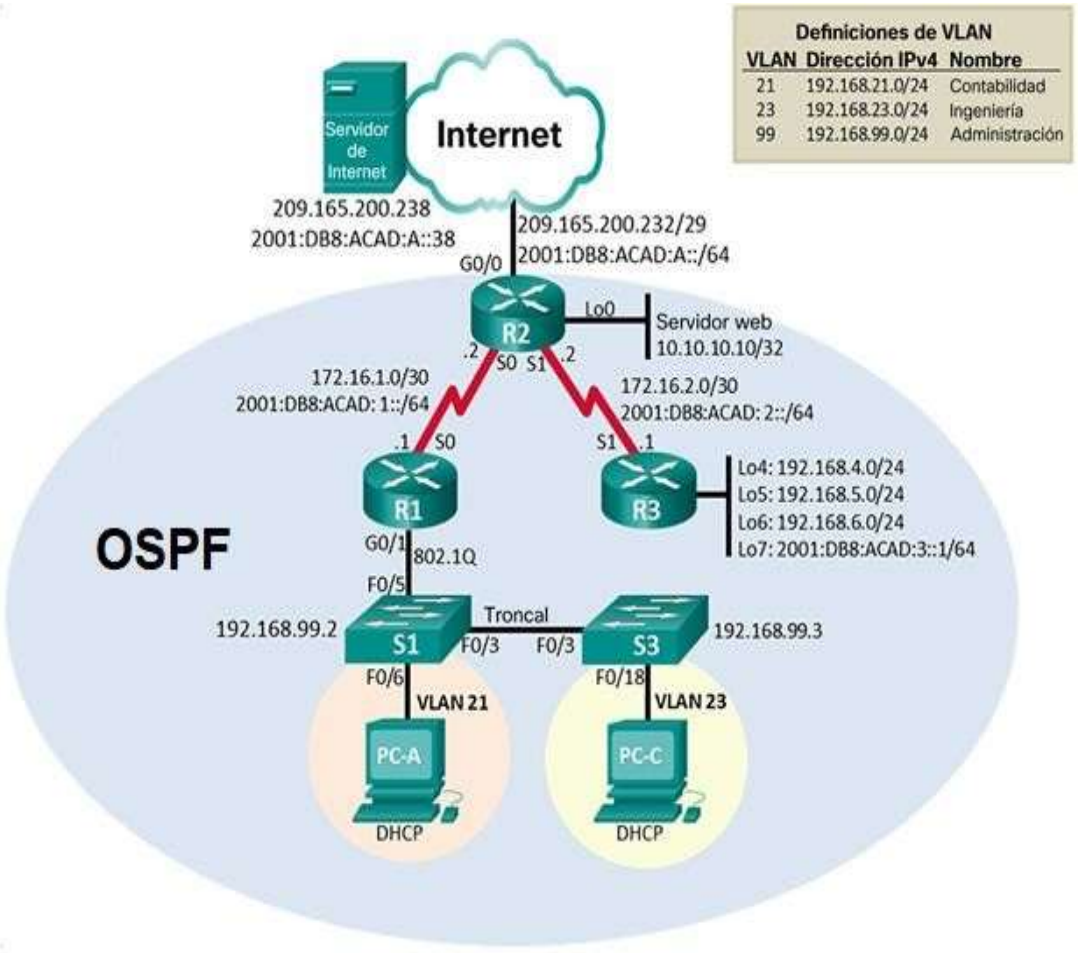


Fuente: Autor

Escenario 2

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

Fig 26. Topología Escenario 2



Fuente: Prueba de Habilidades Cisco 2020 16-04

Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

De acuerdo a lo requerido, se realizará la configuración de cada uno de los dispositivos de la topología planteada iniciando con el borrado de las configuraciones de inicio y las Vlan del router y del switch, eliminando así cualquier configuración previa en los dispositivos.

En la tabla 12. Se muestran los comandos necesarios para el borrado de las Vlan, la inicialización del Router y los Switchs.

Tabla 12. Códigos para reiniciar los Router y switch

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

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1. Configurar la computadora de Internet

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

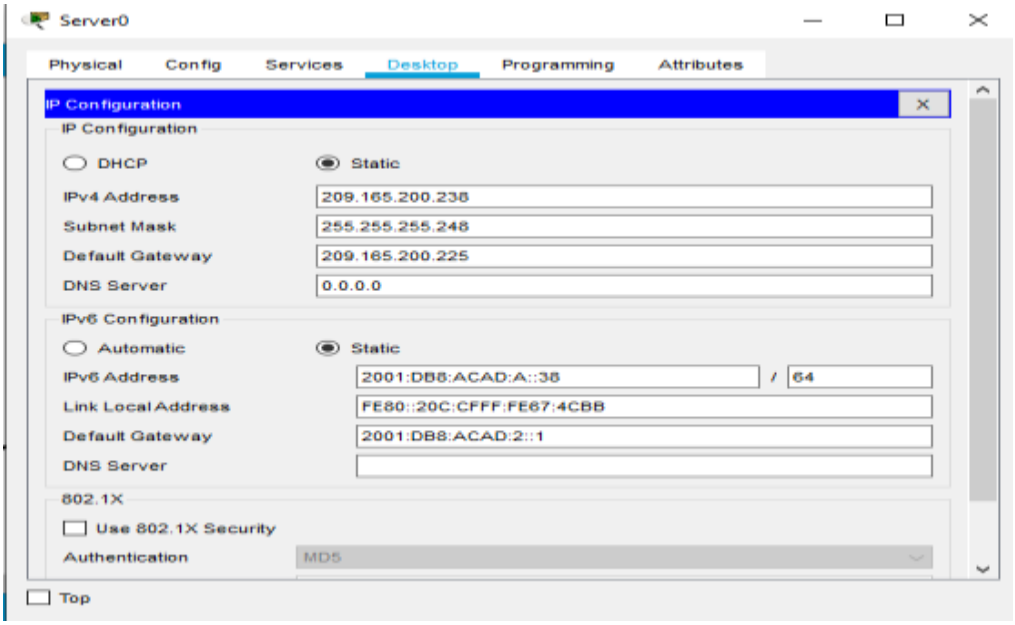
En la Tabla 13, se muestran las direcciones a configurar en la PC de Internet.

Tabla 13. Direccionamiento de PC- de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248

Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fig 27. Configuración de la PC de Internet.



Fuente: Autor

Paso 1: Configurar R1

En la Tabla 14 se muestran los comandos necesarios para la configuración básica del Router 1:

Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al router. Asi mismo se configura la interfaz serial 0/1/0 y la ruta predeterminada.

Tabla 14. Comandos de configuración Básica en R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	enable configure terminal no ip domain-lookup

Nombre del router	hostname R1
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#
Interfaz S0/1/0	int s0/1/0 description connection to R2 ip address 172.16.1.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::1/64 clock rate 128000 no shutdown exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 R2(config-if)#ipv6 route ::/0 g0/0

Nota: Todavía no configure G0/1.

Paso 2: Configurar R2

En la Tabla 15 se muestran los comandos necesarios para la configuración básica del Router 2:

Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al router. Asi mismo se configura las interfaces serial 0/1/0 y 0/1/1, la interfaz G0/1. La interfaz Loopback 0 y la ruta predeterminada.

Tabla 15. Comandos de configuración Básica en R2.

Elemento o Tarea de configuración	Especificación
Desactivar la búsqueda DNS	enable configure terminal no ip domain-lookup
Nombre del router	hostname R2

Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Habilitar el servidor HTTP	ip http server (Este commando no funciona en Packet Tracer)
Mensaje MOTD	banner motd #Acceso No Autorizado#
Interfaz S0/1/0	int s0/1/0 description connection to R1 ip address 172.16.1.2 255.255.255.252 ipv6 address 2001:DB8: ACAD:1::2/64 no shutdown
Interfaz S0/1/1	int s0/1/1 description connection to R3 ip address 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::2/64 clock rate 128000 no shutdown
Interfaz G0/0 (simulación de Internet)	int g0/0 description connection to Internet ip address 209.165.200.233 255.255.255.248 ipv6 address 2001:DB8:ACAD:A::1/64 no shutdown
Interfaz loopback 0 (servidor web simulado)	int l0 ip address 10.10.10.10 255.255.255.255 description simulated web server exit
Ruta predeterminada	R2(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config-if)#ipv6 route ::/0 g0/0

Paso 3: Configurar R3

En la Tabla 16 se muestran los comandos necesarios para la configuración básica del Router 1:

Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY, se encriptan las contraseñas y se

coloca un aviso a personas no autorizadas que intenten acceder al router. Asi mismo se configura la interfaz serial 0/1/1, las infterfaces Lopback 4.5.6.y 7, y la ruta predeterminada.

Tabla 16. Comandos de configuración Básica en R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	enable configure terminal no ip domain-lookup
Nombre del router	hostname R3
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#
Interfaz S0/1/1	int s0/1/1 description connection to R2 ip address 172.16.2.1 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::1/64 clock rate 128000 no shutdown
Interfaz loopback 4	int lo 4 ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	**int lo 5** **ip address 192.168.5.1 255.255.255.0**
Interfaz loopback 6	**int lo 6** **ip address 192.168.6.1 255.255.255.0**
Interfaz loopback 7	**int lo 7** **ipv6 address 2001:DB8:ACAD:3::1/64** **exit**
Rutas predeterminadas	

Paso 4: Configurar S1

En la Tabla 17 se muestran los comandos necesarios para la configuración básica del Switch 1:

Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Switch, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al Switch

Tabla 17. Comandos de configuración Básica en S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	enable configure terminal no ip domain-lookup
Nombre del switch	hostname S1
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	line vty 0 15 password cisco login
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	banner motd #Acceso No Autorizado#

Paso 5: Configurar el S3

En la Tabla 18 se muestran los comandos necesarios para la configuración básica del Switch 3:

Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Switch, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al Switch.

Tabla 18. Comandos de configuración Básica en S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	enable configure terminal no ip domain-lookup
Nombre del switch	hostname S3
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco login
Contraseña de acceso Telnet	**line vty 0 15** **password cisco** **login**
Cifrar las contraseñas de texto no cifrado	**service password-encryption**
Mensaje MOTD	**banner motd #Acceso No Autorizado#**

Paso 6: Verificar la conectividad de la red

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

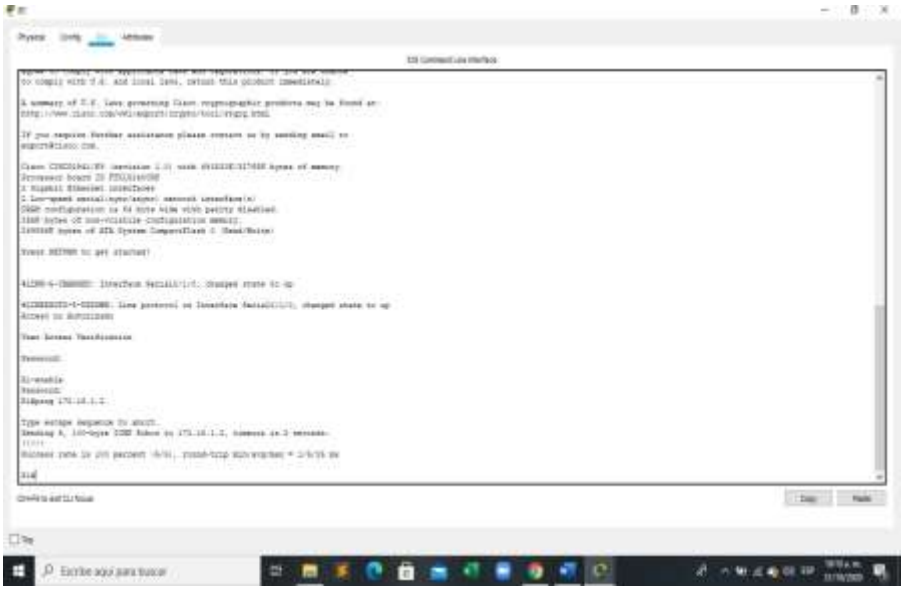
En la tabla 19, se verifica metódicamente la conectividad con cada dispositivo de red.

Tabla 19. Verificación de conectividad en la red y el resultado de la prueba.

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

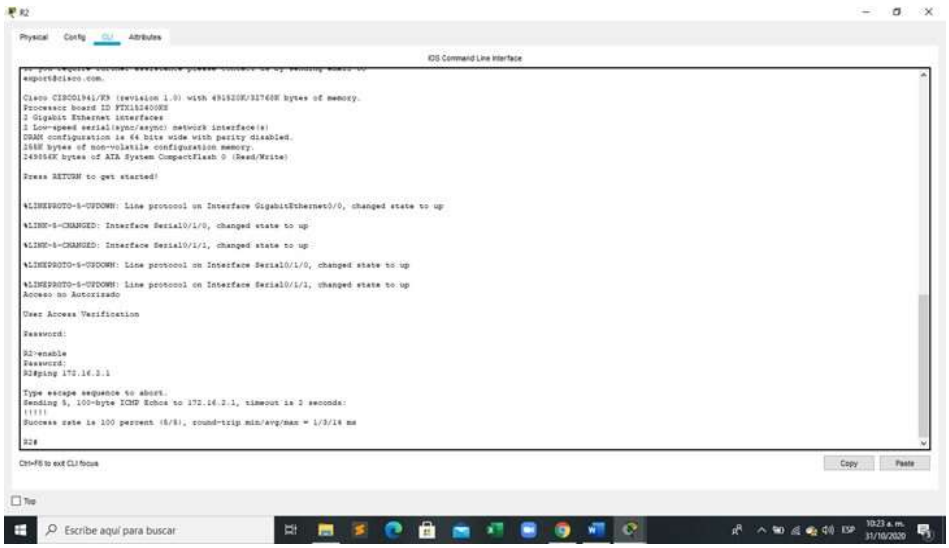
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Fig 28. Prueba de conectividad por medio de Ping entre R1 a R2 a la dirección de la interfaz s0/1/0.



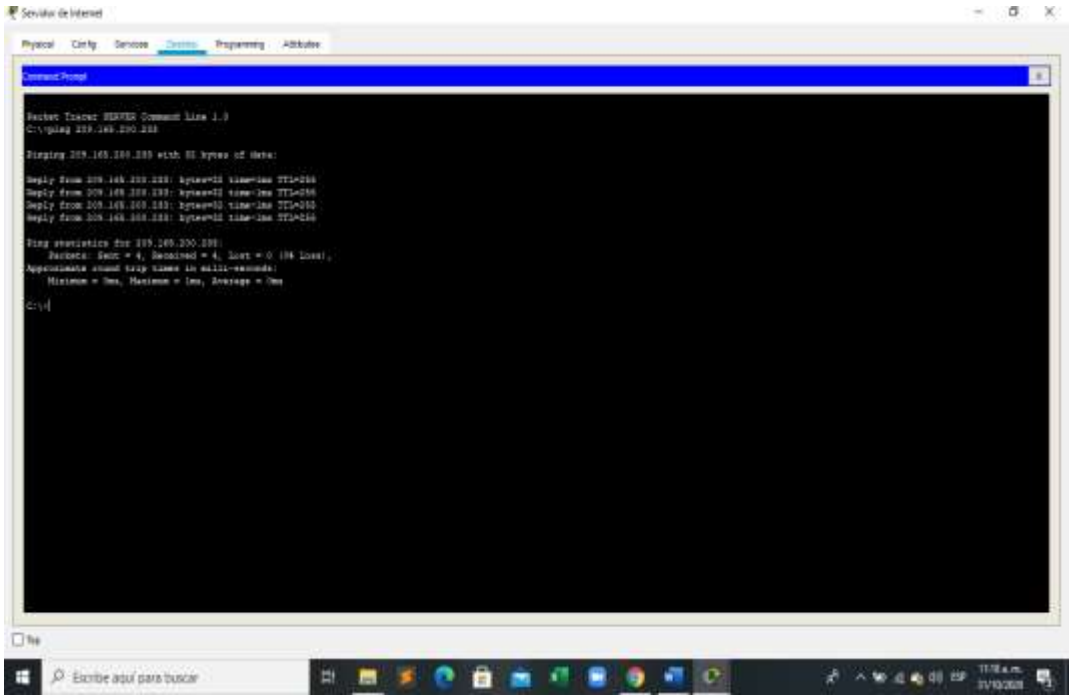
Fuente: Autor

Fig 29. Prueba de conectividad por medio del comando Ping de R1 a R3 a la dirección de la interfaz s0/1/1



Fuente: Autor

Fig 30. Prueba de conectividad por medio del comando Ping de Servidor a Gateway determinado



Fuente: Autor

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

Paso 1: Configurar S1

Se realiza la configuración al switch 1 según la topología propuesta, se crea la base de datos: asignando las Vlan 21, 23 y 99 a los departamentos de Contabilidad, Ingeniería y Administración respectivamente, Se asigna la dirección Ip a la Vlan de administración, se asigna el gateway determinado, se crea enlace troncal al f0/3 y f0/5, se asigna la Vlan 21 al f0/6 y se apagan los puertos que no están en uso.

En la tabla 20 se muestran los comandos de configuración requeridos para cada una de las tareas indicadas.

Tabla 20. Configuración de Seguridad del switch, Vlan y enrutamiento en S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	configure terminal vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion exit
Asignar la dirección IP de administración.	int vlan 99 ip address 192.168.99.2 255.255.255.0 no shutdown exit
Asignar el gateway predeterminado	ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	int f0/3 switchport mode trunk switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	int f0/5 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4, f0/6-24, g0/1-2 switchport mode access
Asignar F0/6 a la VLAN 21	int f0/6 switchport access vlan 21
Apagar todos los puertos sin usar	int range f0/1-2, f0/4, f0/7-24, g0/1-2 shutdown

Paso 2: Configurar el S3

Se realiza la configuración al switch 3 según la topología propuesta, se crea la base de datos: asignando las Vlan 21, 23 y 99 a los departamentos de Contabilidad, Ingeniería y Administración respectivamente, Se asigna la dirección Ip a la Vlan de administración, se asigna el gateway determinado, se crea enlace troncal al f0/3, se asigna la Vlan 21 al f0/18 y se apagan los puertos que no están en uso.

En la tabla 21 se muestran los comandos de configuración requeridos para cada una de las tareas indicadas.

Tabla 21. Configuración de Seguridad del switch, Vlan y enrutamiento en S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	configure terminal vlan 21 name Contabilidad vlan 23 name Ingenieria vlan 99 name Administracion exit
Asignar la dirección IP de administración	int vlan 99 ip address 192.168.99.3 255.255.255.0 no shutdown exit
Asignar el gateway predeterminado.	ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	int f0/3 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	int range f0/1-2, f0/4-24, g0/1-2 switchport mode access
Asignar F0/18 a la VLAN 21	switchport access vlan 21
Apagar todos los puertos sin usar	int range f0/1-2, f0/4-17, f0/19-24, g0/1-2 shutdown

Paso 3: Configurar R1

Realizamos la configuración del Router 1 según la topología propuesta, asignando la subinterfaz de cada una de las vlan (21, 23 y 99) y se activa la interfaz G0/1.

En la tabla 22 se muestran los comandos requeridos para cada una de las tareas indicadas:

Tabla 22. Configuración de protocolo 802.1Q en R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	configure terminal int g0/1.21 description VLAN 21 encapsulation dot1q 21 ip address 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1	int g0/1.23 description VLAN 23 encapsulation dot1q 23 ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	int g0/1.99 description VLAN 99 encapsulation dot1q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	int g0/1 no shutdown

Paso 4: Verificar la conectividad de la red

Utilizando el comando **ping** se realiza prueba de conectividad entre los switches y el R1.

En la tabla 23, se muestra la conectividad de cada switch con el router.

Tabla 23. Verificación de conectividad en los Switch´s

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

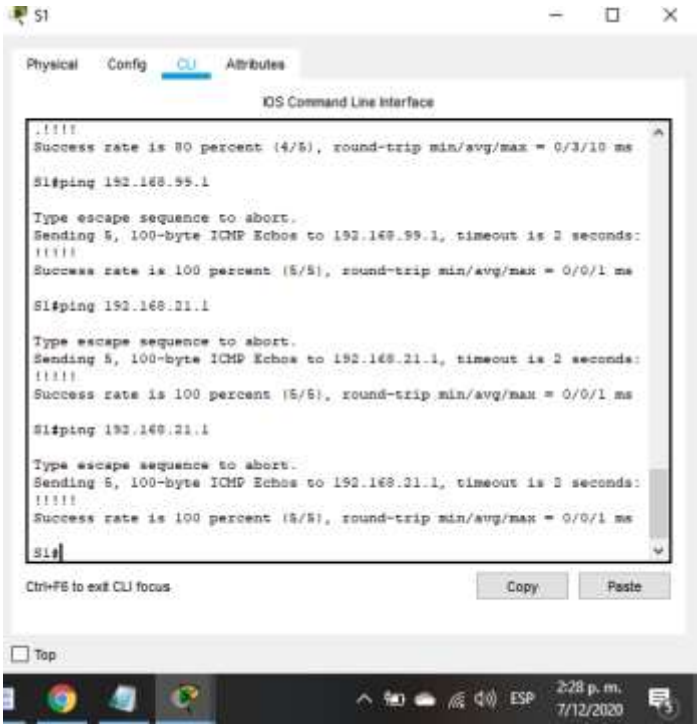
Fig 31. Prueba de conectividad por medio del comando Ping de S1 a R1a la Vlan 99

Fuente: Autor

Fig 32. Prueba de conectividad por medio del comando Ping de S3 a R1 a la Vlan 99.

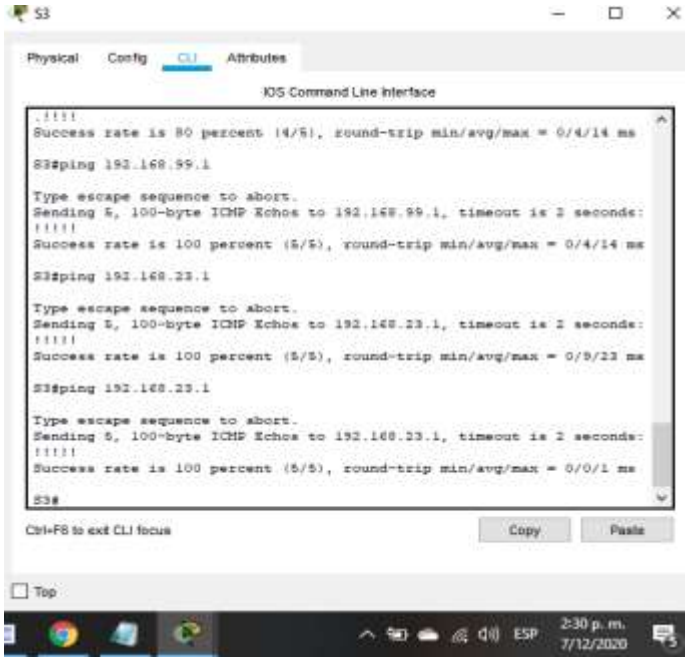
Fuente: Autor

Fig 33. Prueba de conectividad por medio del comando Ping de S1 a R1 a la Vlan 21.



Fuente: Autor

Fig 34. Prueba de conectividad mediante del comando Ping de S3 a R1a la Vlan 23.



Fuente: Autor

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

Tabla 24. Configuración Protocolo OSPF en R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	configure terminal router ospf 1 area 0
Anunciar las redes conectadas directamente	network 172.16.1.0 255.255.255.252 network 192.168.21.0 255.255.255.0 network 192.168.23.0 255.255.255.0 network 192.168.99.0 255.255.255.0
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary (este comando no lo soporta Packet tracer)

Paso 2: Configurar OSPF en el R2

Se realiza la configuración del protocolo Ospf en Router 1, se anuncian las redes que pueden conectarse directamente a él, especificando la ruta de cada una de las conexiones, se establecen las interfaces LAN como pasivas y se desactiva la sumarización automática.

En la tabla 25, se muestran los comandos de configuración necesarios para realizar la tarea.

Tabla 25. Configuración Protocolo OSPF en R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 area 0
Anunciar las redes conectadas directamente	(Se omitirá la red G0/0). network 10.10.10.10 255.255.255.255 network 172.16.1.0 255.255.255.252 network 172.16.2.0 255.255.255.252
Establecer la interfaz LAN (loopback) como pasiva	passive-interface loopback 0
Desactive la sumarización automática.	no auto-summary

Paso 3: Configurar OSPFv3 en el R3

Se realiza la configuración del protocolo Ospf en Router 3, se anuncian las redes que pueden conectarse directamente a él, especificando la ruta de cada una de las conexiones, se establecen las interfaces LAN como pasivas y se desactiva la sumarización automática.

En la tabla 26, se muestran los comandos de configuración necesarios para realizar la tarea.

Tabla 26. Configuración Protocolo OSPF en R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	router ospf 1 router-id 1.1.1.1
Anunciar redes IPv4 conectadas directamente	int s0/1/0 ipv6 ospf 1 area 0 int s0/1/1 ipv6 ospf 1 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface loopback 4 passive-interface loopback 5 passive-interface loopback 6
Desactive la sumarización automática.	no auto-summary

Paso 4: Verificar la información de OSPF

Mediante unos comandos CLI se hace la verificación de que el protocolo OSPF esté funcionando como se espera.

En la tabla 27, se muestran los comandos necesarios para observar la configuración.

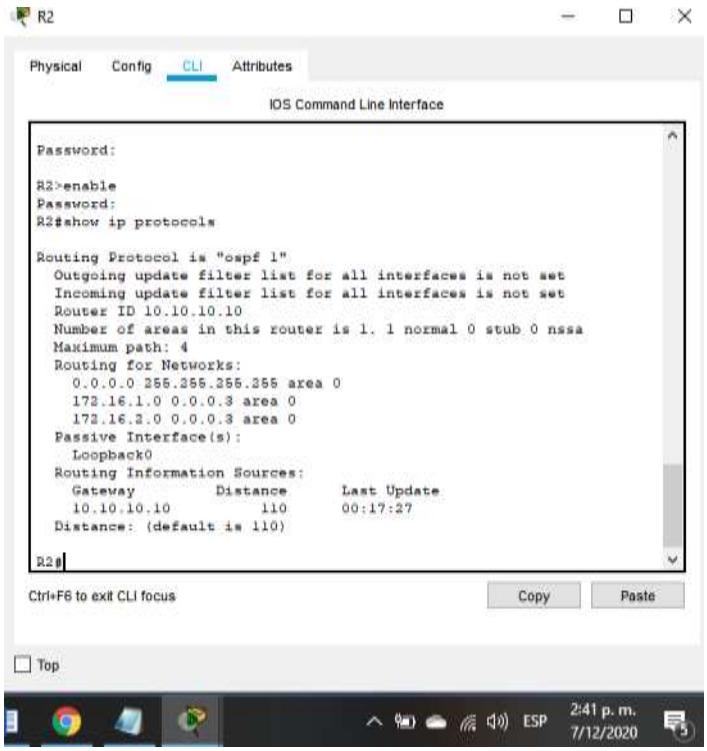
Tabla 27. Verificación de funcionamiento OSPF

Pregunta	Respuesta
¿Con qué commando 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 ip OSPF interface

Fig 35. Configuración OSPF en R1

Fuente: Autor

Fig 36. Configuración de OSPF en R2



Fuente: Autor

Fig 37. Configuración OSPF en R3

Fuente: Autor

Implementar DHCP y NAT para IPv4

Realizamos la configuración del R1 como servidor de DHCP para las VLAN 21 y 23, reservando las primeras 20 direcciones IP para las respectivas vlan (21 y 23) y configurando el servicio DHCP posteriormente.

En la tabla 28, se muestran los comandos de configuración necesarios para configurar el DHCP y NAT.

Paso 5: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Tabla 28. Configuración de R1 como servidor DHCP.

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

Crear un pool de DHCP para la VLAN 21.	ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.1 dns-server 10.10.10.10 domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.1 dns-server 10.10.10.10 domain-name ccna-sa.com

Paso 6: Configurar la NAT estática y dinámica en el R2

Se Realiza la configuración de R2 para establecer las NAT estática y dinámica, creando una base de datos local para garantizar el acceso de usuario con contraseña, se asigna la interfaz interna y externa para la NAT estática, se configura la NAT dentro de una lista de acceso privada y se define el pool de direcciones públicas, se habilita el servicio HTTP.

En la tabla 29, se muestran los comandos necesarios para realizar la tarea de configuración.

Tabla 29. Configuración de NAT en R2

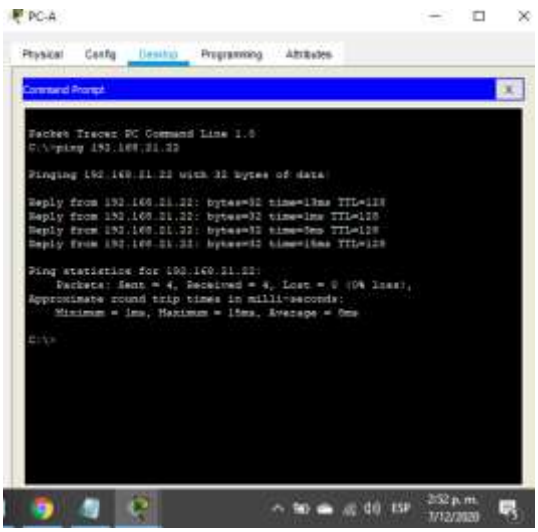
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	configure terminal username webuser privilege 15 secret cisco12345
Habilitar el servicio del servidor HTTP	ip http server (Este commando no funciona en Packet Tracer)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local (Este commando no funciona en Packet Tracer)
Crear una NAT estática al servidor web.	ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	int g0/0 ip nat outside int s0/1/0 ip nat inside int s0/1/1 ip nat inside
Configurar la NAT dinámica dentro de una ACL privada	access-list 1 permit 192.168.21.0 0.0.0.255 access-list 1 permit 192.168.23.0 0.0.0.255 access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Paso 7: Verificar el protocolo DHCP y la NAT estática

Mediante el comando ping realizamos la comprobación de conectividad entre los dispositivos luego de las configuraciones anteriores.

Tabla 30. Verificación de Configuración DHCP y Nat estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Fig 38.Configuración DHCP en PC-A  Fuente: Autor
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Fig 39. Configuración DHCP en PC-C  Fuente: Autor

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Fig. 40. Ping de PC-A a PC-C  Fuente: Autor
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	(No se pudo acceder dado que el comando “ip http server” no funciona en Packet Tracer)

Parte 5: Configurar NTP

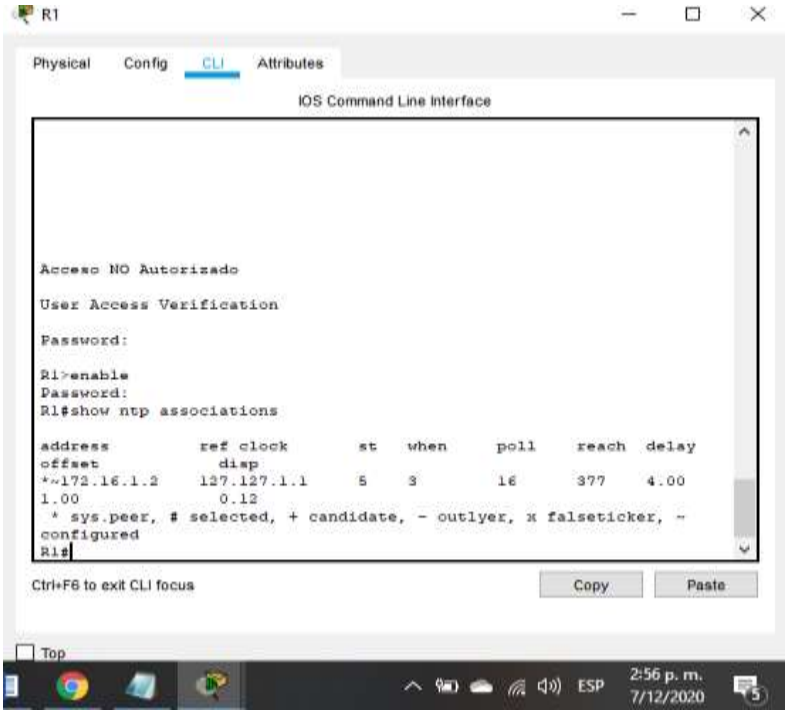
Se configura la hora en R2, se establece R1 como cliente y R2 como servidor NTP, Se configura R1 para que haga actualizaciones de calendario periódicamente con hora NTP y finalmente, realizamos la verificación de la configuración en R1.

En la tabla 31 se muestran los comandos necesarios para la configuración NTP

Tabla 31. Configuración NTP.

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

Fig 40. Configuración NTP en R1



Fuente: Autor

Parte 6: Configurar y verificar las listas de control de acceso (ACL)

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

Se configuran una lista de acceso, definiendo que solo R1 establezca una conexión Telnet con R2, se aplica ACL con nombre a las líneas VTY, se permite el acceso por Telnet a las líneas VTY.

En la tabla 32, se muestran los comandos de configuración para la tarea.

Tabla 32. Configuración ACL 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	configure terminal ip access-list standard ADMIN-MGT permit host 172.16.1.1 exit
Aplicar la ACL con nombre a las líneas VTY	line vty 0 15 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	Exitoso

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

Tabla 33. Comandos de verificación de configuraciones.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-list
Restablecer los contadores de una lista de acceso	clear access-list counters clear ip? bgp Clear BGP connections dhcp Delete items from the DHCP database nat Clear NAT ospf OSPF clear commands route Delete route table entries
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface
¿Con qué comando se muestran las traducciones NAT?	show ip nat translations 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.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations

CONCLUSIONES

- En el desarrollo de este proyecto se logró implementar mediante el simulador como Packet Tracer, las topologías propuestas en los dos escenarios, afianzando así los conocimientos adquiridos a lo largo del seminario.

- Se realizaron las configuraciones básicas a cada uno de los dispositivos de la red, así como también la conectividad en los distintos protocolos Ipv4 e Ipv6.

- Implementar las medidas necesarias mediante protocolos PAP Y CHAP nos permite el acceso utilizando contraseñas y así garantizar la seguridad en los dispositivos de red, utilizando también el control de acceso con lista ACL, protocolos de autenticación, etc.

- Estos escenarios han permitido aplicar los conceptos aprendidos en el Diplomado, como por ejemplo elaborar Vlans e inter Vlans routing, implementar los protocolo DHCVP, los protocolos de routing dinámico y estático, OPSF V2 y otros tipos de enrutamiento.

- La importancia de Garantizar eficacia en la red utilizando direccionamiento PAT y PPP los cuales nos permiten la optimización el direccionamiento Ip de los dispositivos pertenecientes a la red.

- Los conocimientos sobre redes LAN/WLAN ofrecido por CCNA(Cisco Certified Network Associate), nos permite de manera práctica aprender a diseñar, implementar y mantener estructuras de redes y así prepararnos profesionalmente en este campo tan necesario y tan utilizado en estos tiempos.

- Mediante la configuración de EtherChannel Se permiten agrupar hasta 16 enlaces troncales diferentes, permite la agrupación lógica de varios enlaces físicos Ethernet, la cual es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico usado y así se obtiene un enlace troncal de alta velocidad.

.

BIBLIOGRAFÍA

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

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

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

Capa de Aplicación CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1. (s.f.).

NAT (Network Address Translation. (2020, 9 junio). Tomado de Wikipedia. https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

ANEXOS

- Links de archivos ejecutables de los 2 escenarios en Packet Tracer

  https://1drv.ms/u/s!AnR_eqwO-qnEiCpm2MNGdw27DSsV?e=a56TO2

  https://1drv.ms/u/s!AnR_eqwO-qnEiC7U8jB11oqi2moc?e=Kyv033

- Link del Artículo Científico.

  https://1drv.ms/b/s!AnR_eqwO-qnEiC3R706nsU1DW419?e=L3hULx

- Artículo Científico

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

Palomino Franco. Santiago Elías. Estudiante de Ingeniería Electrónica de la Universidad Nacional Abierta y a Distancia, sapafra@hotmail.es

I. Resumen

En este primer escenario se configurarán los dispositivos de una red pequeña. Se configura un router, un switch y equipos que admiten 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.

Aplicando conceptos fundamentales de uso en configuración y administración de redes, tales como: protocolos de enrutamiento RIP, OSPF, listas de control de acceso (ACL), DHCP, VLANs, Servicios NAT y PAT, Redireccionamiento, Tipos de Seguridad, LAN, Autenticación PAP y CHAP, entre otros.

Índice de Términos - ACL (Access control list), Enrutamiento, Protocolo, topología.

Summary

In this first scenario, the devices of a small network will be configured. A router, a switch, and computers that support both IPv4 and IPv6 connectivity are configured for the supported hosts. The router and switch must also be managed securely. You will configure routing between VLAN, DHCP, Etherchannel, and port-security. Applying fundamental concepts of use in network configuration and administration, such as: RIP routing protocols, OSPF, access control lists (ACL), DHCP, VLANs, NAT and PAT services, Redirection, Security Types, LAN, PAP Authentication and CHAP, among others. Terms Index - ACL (Access Control List), Routing, Protocol, topology.

I. INTRODUCCION

La revolución que ha generado el internet en muchos ámbitos de nuestra cotidianidad, cambiando de manera radical la manera de comunicarnos. Hoy día lo utilizamos para casi todas las actividades. Desde enviar fotos desde una aplicación de mensajería instantánea, leer noticias en la página o una aplicación de un periódico de cualquier parte del mundo o simplemente comprar nuestra cena.

Debido a esto cobra importancia el uso de estas redes de manera eficaz y segura, evitando los riesgos que contienen el estar en la red. Precisamente como ingenieros debemos estar a la vanguardia en el diseño, implementación y administración de redes confiables, seguras y eficientes.

En el presente informe se demostrará de forma práctica los conocimientos adquiridos durante el curso Diplomado de Profundización CCNA de CISCO aplicando las habilidades y competencias adquiridas a lo largo de este.

Se configuraran los dispositivos en el escenario y al final se verificaran si fueron aplicadas apropiadamente las configuraciones implementadas y que las redes funcionen correctamente.

II. ESCENARIO PROPUESTO.

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

Fig. 1. Topología del caso

A. Escenario simulado.

En la Fig. 2. Se muestra la topología propuesta montada en el software de simulación Packet Tracer

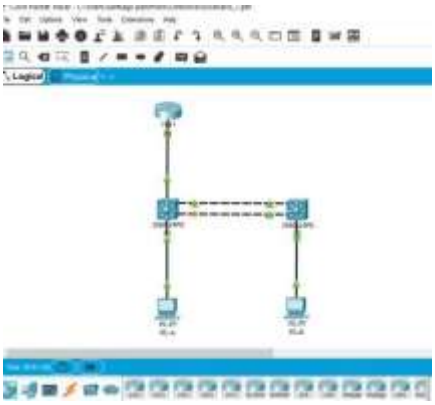


Fig. 2. Simulación de Escenario en Packet Tracer

B. Inicializar y volver a cargar el Router

De acuerdo a lo requerido, se realizará la configuración de cada uno de los dispositivos de la topología planteada iniciando con el borrado de las configuraciones de inicio y las Vlan del router y del switch, eliminando así cualquier configuración previa en los dispositivos.

En la tabla 3. Se muestran los comandos necesarios para el borrado de las Vlan, la inicialización del Router y los Switchs

.

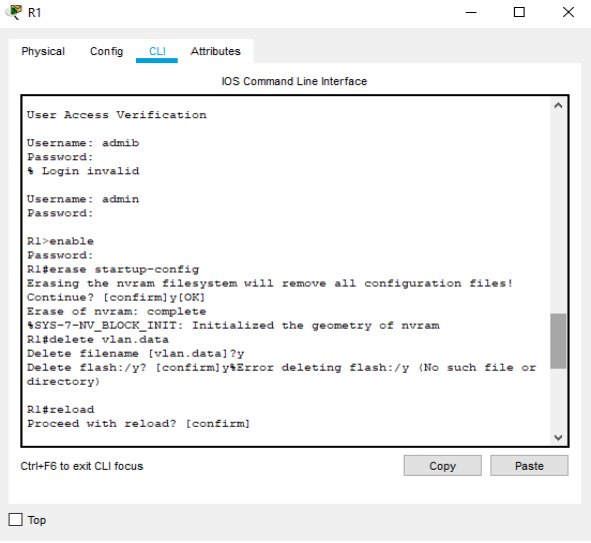
Tabla I. Comandos para inicializar Router

Comando	Función
Router>enable	**Ingresar al modo Exec privilegiado**
R1#erase startup-config	**Borrar la configuración inicial del dispositivo.**
R1#reload	**Reiniciar el dispositivo.**

Tabla II. Comandos para inicializar Switch's

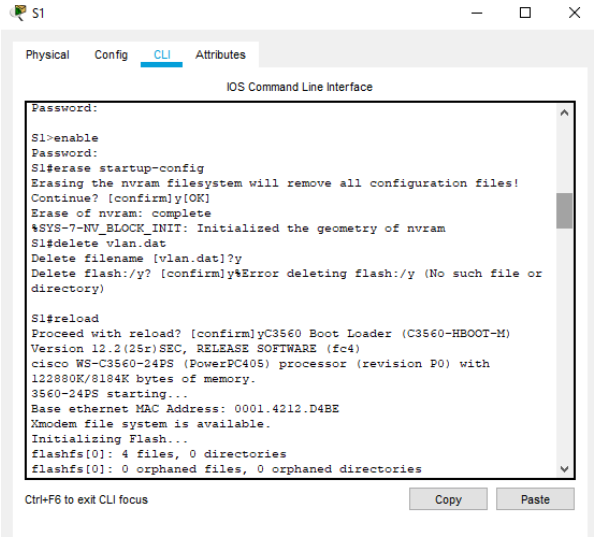
Comando	Función
Switch>enable	**Ingresar al modo Exec privilegiado**
S1#erase startup-config	**Borrar la configuración inicial del dispositivo.**
S1#delete vla.dat	**Borrar la BD de Vlan existentes en el dispositivo.**
S1#reload	**Reiniciar el dispositivo.**

Fig 3. Borrado de configuraciones preconfiguradas e Inicialización del Router 1.



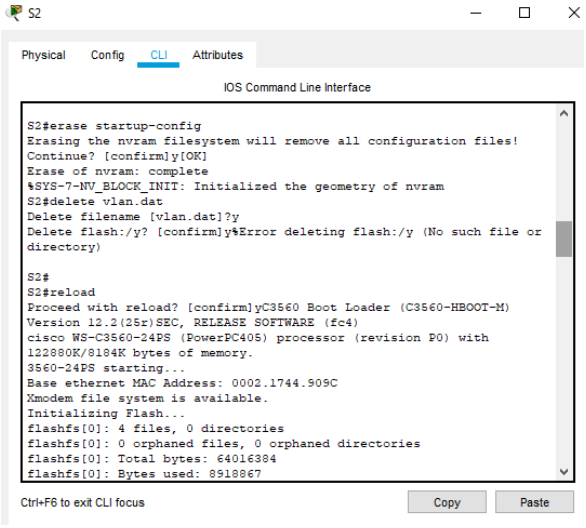
Fuente: Autor

Fig 4. Borrado de configuraciones preconfiguradas e Inicialización del Switch 1.



Fuente: Autor

Fig 5.Borrado de configuraciones preconfiguradas e Inicialización del Switch 2



Fuente: Autor

C. Direccionamiento de los dispositivos

En la Tabla III se muestra el direccionamiento de cada una de las interfaces y de los dispositivos utilizados en el escenario.

Tabla III. Direcciones de Interfaces y dispositivos.

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**

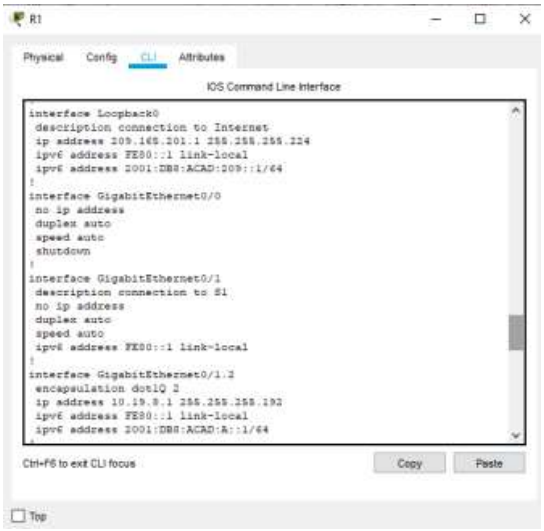
R1 G0/0/1.3 R1 G0/0/1.3	10.19.8.65 /27	**No corresponde**
	2001:db8:acad:b: :1 /64	**No corresponde**
R1 G0/0/1.4 R1 G0/0/1.4	10.19.8.97 /29	**No corresponde**
	2001:db8:acad:c: :1 /64	**No corresponde**
R1 G0/0/1.6	No corresponde	**No corresponde**
R1 Loopback0 R1 Loopback0	209.165.201.1 /27	**No corresponde**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

En la tabla IV se muestra la lista de direccionamiento Vlan en el Router 1 del escenario.

Tabla. IV. Direccionamiento Vlan

Dispositivo / interfaz	Dirección IP / Prefijo
R1 G0/0/1.2	**10.19.8.1 /26**
R1 G0/0/1.2	**2001:db8:acad:a: :1 /64**
R1 G0/0/1.3	**10.19.8.65 /27**
R1 G0/0/1.3	**2001:db8:acad:b: :1 /64**
R1 G0/0/1.4	**10.19.8.97 /29**

Fig 6 Configuración de las interfaces y sub interfaces en R1



Fuente: Autor

Para que los Switchs puedan permitir el direccionamiento con Protocolo Ipv6, se hace necesario cambiar la plantilla SDM la cual de manera predeterminada no permite el direccionamiento Ipv6 en sus interfaces.

En la Tabla V, se muestran los comandos necesarios para cambiar la plantilla SDM.

Tabla V. Configuración Cambio de Plantilla SDM.

Comando	Función
Switch>enable	**Ingresar al mod Exec Privilegiado**
Switch#configure terminal	**Ingresar al modo Exec de configuración global.**
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing	**Habilitar el direccionamiento Ipv4 e Ipv6 en el dispositivo.**
Switch(config)#reload	**Reiniciar el dispositivo.**

D. Configuración de Router 1

Con los comandos de la Tabla VI, se configuran los parametros basicos del Router 1 como son:
Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY. Así mismo se establece una longitud minima para las contraseñas. Se habilita el routing Ipv6, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al router. Así kismo se configuran las interfaces,subinterfaces y el Loopback0.
.

Tabla VI. Comandos configuración Router 1

Tarea	Especificación
Desactivar la búsqueda DNS	**Router>enable**
Router#configure terminal	**Router(config)#no ip domain-lookup**
Nombre del router	**Router(config)#hostname R1**
Nombre de dominio	**R1 (config)#ip domain-name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**R1(config)#enable secret ciscoconpass**
Contraseña de acceso a la consola	**R1(config)#line console 0** **R1(config-line)#password ciscoconpass** **R1(config-line)#login**
Establecer la longitud mínima para las contraseñas	**R1(config)#security password min-length 10**
Crear un usuario administrativo en la base de datos local	**R1(config)#user name admin privilege 1 secret admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	**R1(config-line)#line vty 0 15** **R1(config-line)#password ciscoconpass** **R1(config-line)#login**
Configurar VTY solo aceptando SSH	**R1(config-line)#transport input ssh** **R1(config-line)#exit**
Cifrar las contraseñas de texto no cifrado	**R1(config-line)#service password-encryption**
Configure un MOTD Banner	**R1(config)#banner motd #Acceso No Autorizado#**
Habilitar el routing IPv6	**R1(config)#ipv6 unicast-routing**
Configurar interfaz G0/0/1 y subinterfaces	**R1(config)#int G0/0/0** **R1(config-if)#description connection to S1** **R1(config-if)#ip address 10.19.8.0 255.255.255.252** **R1(config-if)#ipv6 address 2001:db8:acad:a: :1 /64** **R1(config-if)# ipv6 address fe80::1 link-local** **R1(config-if)#clock rate 128000**
Activar la interfaz.	**R1(config-if)#no shutdown** **R1(config-if)#exit**
	R1(config-if)#description connection to R1
Configure el Loopback0 interface	**R1(config-if)#ip route 0.0.0.0 0.0.0.0 g0/0209.165.201.1 /27** **R1(config-if)#ipv6 route 2001:db8:acad:209: :1 /64** **R1(config-if)# ipv6 address fe80::1 link-local**
Generar una clave de cifrado RSA	**R1 (config)#crypto key generate isa modulus 1024**

En la Figura 7 y la Figura 8 a continuación mediante el comando show running-config, se muestra la configuración realizada en el Router 1.

Fig. 7. Configuración R1

Fuente: Autor

Fig. 8. Configuración R1

Fuente: Autor

E. Configuración de S1 y S2

Con los comandos de la tabla VII, se configuran los parametros basicos de los Switch 1 y 2 como son:
Desativar la busqueda de DNS, se coloca contraseña al acceso EXEC privilegiado, se le coloca el nombre al Router, se configuran los parametros de seguridad, colocando contraseñas en consola y en VTY. Así mismo se establece una longitud minima para las contraseñas. Se habilita el routing Ipv6, se encriptan las contraseñas y se coloca un aviso a personas no autorizadas que intenten acceder al router. Se configura la interfaz de admiistración y el gateway predeterminado.

Tabla VII. Comandos de configuración de los S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	**Enable** **switch>configure terminal** **no ip domain-lookup**
Nombre del switch	**hostname S1**
Nombre de dominio	**ip domain-name ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**enable** **secret ciscoconpass**
Contraseña de acceso a la consola	**line console 0** **password ciscoconpass** **login local**
Crear un usuario administrativo en la base de datos local	**username admin password admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	**line vty 0 4** **password ciscoconpass** **login local** **exit**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	**input ssh**
Cifrar las contraseñas de texto no cifrado	**service password-encryption**
Configurar un MOTD Banner	**banner motd #Acceso no Autorizado#**
Configurar la interfaz de administración (SVI)	**ipv6 address fe80::98 link-local** **no shutdown**
Configuración del gateway predeterminado	**Ip default-gateway 10.19.8.97**

En las figuras 9 y 10 a continuación, vemos las configuraciones realizadas en los Switchs S1 Y S2

Fig 9. Configuración básica del S1

Fuente: Autor

Fig. 10. Configuración básica de S2

Fuente: Autor

F. Configuración de Vlans, Trunking, EtherChannel para S1.

En la Tabla VIII a continuación se muestran los comandos necesarios para la configuración de estructura de red.

Tabla VIII. Configuración de estructura de red

Tarea	Especificación
Crear VLAN	**vlan 2** **name Bikes** **vlan 3** **name Trikes** **vlan 4**

	name Management **vlan 5** **name Parking** **vlan 6** **name Native**
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**interface f0/1** **switchport trunk encapsulation dot1q** **switchport mode trunk** **switchport trunk native vlan 6** **switchport trunk allowed vlan 2,3,4,5,6** **interface f0/2** **switchport trunk encapsulation dot1q** **switchport mode trunk** **switchport trunk native vlan 6** **switchport trunk allowed vlan 2,3,4,5,6** **Interface f0/5** **switchport trunk encapsulation dot1q** **Switchport mode trunk** **Switch trunk native Vlan 6** **switchport trunk allowed vlan 2,3,4,5,6**
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Interface range FastEthernet0/1-2** **Channel-group 1 mode active**
Configurar el puerto de acceso de host para VLAN 2	**interface f0/6** **switchport mode Access** **switchport access vlan 2** **no shutdown**
Configurar la seguridad del puerto en los puertos de acceso	**interface f0/6** **switchport mode Access** **switchport port-security** **switchport port-security maximum 3** **no shutdown**
Proteja todas las interfaces no utilizadas	**interface range Fastethernet 0/3-4** **interface range Fastethernet 0/6-24** **switchport mode Access** **switchport access vlan 5** **switchport port-security** **switchport port-security maximum 1** **switchport port-security violation shutdown**

A continuación en las Figuras 6 y Figura 7 mediante el comando show running-config se muestran las configuraciones en S1

Fig. 11 Configuración de estructura de red en S1

Fuente: Autor

Fig. 12. Configuración de estructura de red en S1

Fuente: Autor

G. Configuración de Vlans, Trunking, EtherChannel para S2.

En la Tabla VIII a continuación se muestran los comandos necesarios para la configuración de estructura de red.

Tarea	Especificación
Crear VLAN	vlan 2 name Bikes vlan 3 name Trikes vlan 4 name Management vlan 5 name Parking vlan 6 name Native
	interface f0/1

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**switchport trunk encapsulation dot1q** **switchport mode trunk** **switchport trunk native vlan 6** **switchport trunk allowed vlan 2,3,4,5,6** **interface f0/2** **switchport trunk encapsulation dot1q** **switchport mode trunk** **switchport trunk native vlan 6** **switchport trunk allowed vlan 2,3,4,5,6**
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Interface range FastEthernet0/1-2** **Channel-group 1 mode active**
Configurar el puerto de acceso del host para la VLAN 3	**interface f0/18** **switchport mode access** **switchport access vlan 3** **no shutdown**
Configure port-security en los Puertos de acceso	**interface f0/18** **switchport mode access** **switchport port-security** **switchport port-security maximum 3** **no shutdown**
Asegure todas las interfaces no utilizadas.	**interface range Fastethernet 0/3-4** **interface range Fastethernet 0/6-24** **switchport mode access** **switchport access vlan 5** **switchport port-security** **switchport port-security maximum 1** **switchport port-security violation** **shutdown**

A continuación en las Figuras 8 mediante el comando show running-config se muestran las configuraciones en S2

Fig. 13. Configuración de estructura de red en S2.

Fuente:Autor

Fig. 14. Configuración de estructura de red en S2

Fuente: Autor

H. Configuración de enrutamiento y dispersión DHCP para Vlan 2 y 3.

En la Tabla X, se muestran los comandos necesarios para configurar rutas estáticas y DHCP automáticas para los host PC-A y PC-C del escenario propuesto.

Tarea	Especificación
Configure Default Routing	**int Lo 0** **description connection to Internet** **ip address 209.165.201.1 255.255.255.224** **ipv6 address 2001:db8:acad:209::1/64** **ipv6 address fe80::1 link-local**
Configurar IPv4 DHCP para VLAN 2	**network 10.19.8.0 255.255.255.192Ip dhcp pool ccna-a.net** **default-router 10.19.8.1** **exit** **Ip dhcp excluded-address 10.19.8.1 10.19.8.52**
Configurar DHCP IPv4 para VLAN 3	**Ip dhcp pool ccna-b.net** **network 10.19.8.0 255.255.255.192** **default-router 10.19.8.1** **exit** **Ip dhcp excluded-address 10.19.8.65 10.19.8.85**

A continuación en la figura 10 y figura 11 mediante el comando show running-config, se muestra la configuración realizad a R1

Fig. 15. Configuración de enrutamiento y dispersión en R1

Fuente: Autor

Fig. 16. Configuración de enrutamiento y dispersión en R1

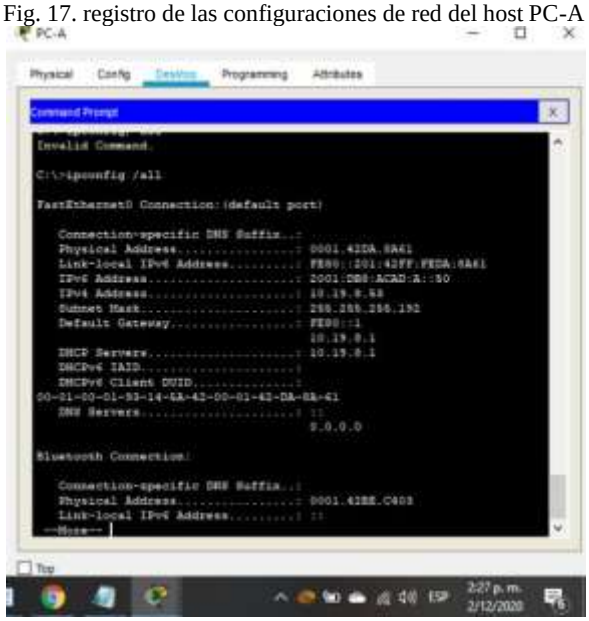
Fuente: Autor

I. Configuración de enrutamiento de Host.

Se hace la configuración de los equipos host de la red, para que utilicen DHCP para Ipv4 y asigne estáticamente las direcciones Ipv6 GUA y Link local.

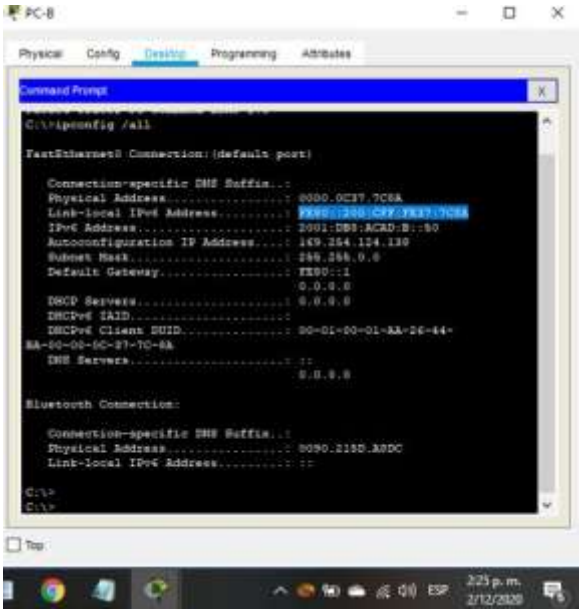
En la Fig. 17 y Fig. 18. Mediante el comando ipconfig/all, se muestra el registro de las configuraciones de red del host.

Fig. 17. registro de las configuraciones de red del host PC-A



Fuente: Autor

Fig. 18. registro de las configuraciones de red del host PC-B



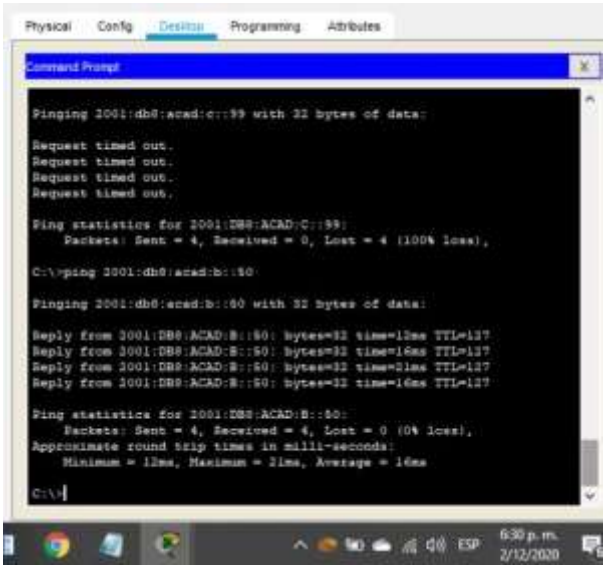
Fuente: Autor

J. Prueba de conectividad.

Mediante comando Ping, se hace prueba de conectividad entre los host PC-A y PC-B. Utilizando las direcciones Ip tomadas por estos durante DHCP.

En la Fig.19 se muestra el resultado del PING.

Fig. 19 Prueba de conectividad mediante comando Ping de PC-A a PC-B



Fuente: Propia.

III. CONCLUSIÓN

Utilizando la configuración EtherChannel, se pueden agrupar varios enlaces físicos Ethernet y tratarlos como un enlace único el cual suma la velocidad nominal de cada puerto físico usado y de esta forma obtener un puerto troncal de alta velocidad.

Mediante la utilización del protocolo DHCP, los dispositivos conectados al servidor de red obtienen de forma automática una asignación de dirección Ip, así como otros parámetros que necesite el cliente.

Haciendo uso del protocolo de encapsulamiento 802.1Q el cual permite que las tramas Ethernet viajen a través de la red con una etiqueta que contiene la identificación de la Vlan creada. Es decir, se pueden crear subinterfaces y asociarlas a una Ip. Lo cual es importante debido a la disminución de costos en la implementación y/o mejoramiento de la red al no tener que comprar más dispositivos.

La forma más eficiente de segmentar la red es sin duda el uso de la VLAN´s, pues utilizando un enlace troncal se pueden pasar varias de ellas simultáneamente a Ethernet sin necesidad de usar un enlace físico para cada una. Aumentando con ello el buen desempeño y la eficacia de la red.

IV REFERENCIAS

1. CISCO, “Protocolos y comunicaciones de red. Fundamentos de Networking”, Recuperado de: https://static-courseassets.s3.amazonaws.com

2. CISCO, “Configuración de EtherChannel y enlace troncal 802.1Q entre switches de configuración fija Catalyst L2 y un enrutador (enrutamiento InterVLAN). {En línea}”, {30 noviembre de 2020} Disponible en https://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html

3. CISCO, “Redes Conmutadas. Principios de Enrutamiento y Conmutación. {En línea}”, {Consultado noviembre 2020}. Disponible en https://static- courseassets.s3.amazonaws.com courseassets.s3.amazonaws.com/RSE6/es/index.html#4

4. CISCO, “EtherChannel {En línea}”, {Consultado diciembre 2020} Disponible en https://www.cisco.com/c/en/us/tech/lanswitching/etherchannel/index.html

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

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

7. UNAD, “Principios de Enrutamiento”, [OVA]. {En línea}. {Consultado diciembre 2020}. Disponible en https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

8. CISCO, “Routing Estático. Principios de Enrutamiento y Conmutación”, {En línea}. {Consultado noviembre 2020}. Disponible en https://static-courseassets.s3.amazonaws.com/RSE6/es/index.html#2

V. BIOGRAFÍA

Santiago Elías Palomino Franco (1975) Nació en Astrea Cesar, el 22 de Julio de 1975. Se graduó como bachiller del Instituto Técnico Industrial ***Pedro Castro Monsalvo*** de la ciudad de Valledupar.
Técnico Profesional en Mantenimiento Electrónico del Servicio Nacional de Aprendizaje **“SENA”** en la ciudad de Valledupar.
Estudiante de Ingeniería Electrónica de la Universidad Nacional Abierta y a Distancia **“UNAD”** en la ciudad de Valledupar, Cesar.

Él se desempeña actualmente como **Técnico Electricista Automotriz** en la Alianza Multimodal de Transporte “AMTUR”
El sr Palomino está convencido que solo a través de la educación se puede lograr la transformación del mundo. Sus áreas de interés, está en lograr la conectividad en áreas rurales de Valledupar.