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

YENY MARCELA AGUILAR MACIAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SOGAMOSO
2022

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

YENY MARCELA AGUILAR MACIAS

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

DIRECTOR:
MSc. PAULITA FLOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
SOGAMOSO
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

SOGAMOSO, 27 DE NOVIEMBRE DE 2022

AGRADECIMIENTOS

Agradezco a Dios por guiarme siempre en el buen camino, por darme salud y por cada día de vida para realizar mis sueños, a los profesores que fueron mi apoyo en el momento de querer darme por vencido, a mis seres queridos por el apoyo constante y a mis amigos y compañeros que fueron parte de mi experiencia en el largo camino académico.

Contenido

Lista de Tablas

Pág.

Lista de Figuras

GLOSARIO

Ip, Internet Protocolo: dirección asignada en una red que identifica dispositivos Routers, dispositivos de capa dos, switches, host, etc. Y dispositivos finales, una pagina web o un PC pueden tener una dirección IP, hay dos clases de direcciones IP, las direcciones IP Publicas y las direcciones IP privadas.[1]

Router: es un dispositivo de enrutamiento, donde se administran los procesos y configuraciones de la red, estos se comunican con otros Routers, switch, ordenadores, donde se conectan y comparten voz datos, videos, el Routers puede estar conectado a un cableado estructurado, o por red wifi.[2]

Switch: es el dispositivo de capa dos dentro de una red de datos, conecta varios dispositivos a la vez, este conmutador transfiere los datos entre dispositivos cada uno de sus puertos puede tener una puerta de enlace de diferentes vlans ofreciendo una segmentación en la red, mayor seguridad y respaldo en la red.[3]

Redes: una red es un conjunto de dispositivos conectados entre si en un enrutamiento segmentado, es una red LAN, las redes son varias LAN conectadas entre sí, que comparten información de una red a otra.[4]

CCNA: Certified Network Associate, es un grupo de normas, dispositivos de red, tecnologías y certificación de diseño, configuración e implementación de redes de telecomunicaciones de forma acertada, administrar y gestionar los protocolos de enrutamiento certificados por CISCO.[5]

Electrónica: disciplina técnica que hace parte de la física, que estudia los circuitos electrónicos, sus componentes y comportamientos se compone de tubos, condensadores, diodos, resistores, baterías y demás circuitos integrados, indispensables en los dispositivos eléctrico y electrónicos.[6]

Networking: es una red de telecomunicaciones que esta conectada y se comunica entres si, una red LAN esta conectada con los dispositivos vinculados y puede ampliar la red conectando con otras redes LAN o WAN.[7]

---

[1] VV APARICIO-Izurieta - Seguridad con IP seguro en internet (IPSEC) (2022).
[2] JIMENEZ Julio Configuración de un Reuter básico con configuración profesional. (2013)
[3] JD Harris, MJ Moran New molecular switch architectures. (2018).
[4] ROSALES Ronald. Gestión De Proyectos En El Sector De Las Telecomunicaciones (2022)
[5] ACOSTA Jhuly ¿Qué es la Certificación Cisco CCNA y cuáles son sus ventajas?. (2017)
[6] GJ MARCILLO Quimis. Implementación de circuitos electrónicos programables (2022)
[7] RICART Josep. Cisco CCNA Fundamentos de Networking para redes IP. (2022).

RESUMEN

Este informe corresponde a la presentación de la prueba de habilidades practicas del curso de CCNA, del Diplomado de Profundización CISCO, en donde se da solución a dos escenarios propuestos, los dispositivos necesarios para la red son de certificación CISCO, los Routers, switch, y PC, se configuran paso a paso, explicando detalladamente cada uno de ellos, con imágenes claras y comentadas para una mejor interpretación de la red.

El software de simulación seleccionado es Packet Tracer, de tecnología cisco, el cual tiene integrado los dispositivos necesarios y permite realizar el diseño de la red según cada uno de los dos escenarios, la configuración básica de los dispositivos y la implementación de protocolos de red como OSPF, RIP, DHCP, y la configuración de seguridad de los puertos de los switches.

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

ABSTRACT

This report corresponds to the presentation of the practical skills test of the CCNA course, of the CISCO Deepening Diploma, where a solution is given to two proposed scenarios, the necessary devices for the network are CISCO certified, the Routers, switch, and PC, are configured step by step, explaining each of them in detail, with clear and commented images for a better interpretation of the network.

The selected simulation software is Packet Tracer, from Cisco technology, which has the necessary devices integrated and allows the design of the network according to each of the two scenarios, the basic configuration of the devices and the implementation of network protocols such as OSPF, RIP, DHCP, and switch port security settings.

Keywords: CISCO, CCNA, Switching, Routing, Networks, Electronics, Networking

INTRODUCCIÓN

Este informe presenta la prueba de habilidades practicas del diplomado de profundización CCNA esta práctica se realiza con ase a 2 escenarios propuesto en donde se realiza el diseño y la configuración, implementando la red desde cero, aplicando los conocimientos adquiridos durante el curso

Cada uno de los escenarios es un reto para cualquier administrador de redes, como profesional estoy en la capacidad de realizar una red basando solo en las especificaciones técnicas del diseño de esta red, implementando los protocolos necesarios para su funcionamiento garantizando una velocidad alta y alto flujo de trafico de paquetes.

El curso Diplomado de profundización me permitió obtener conocimientos fundamentales que debe tener un ingeniero en base a los diseños de redes actuales que se han expandido usando protocolos de seguridad, vlans, enrutamiento ipv4 e ipv6 y sub redes para garantizar una misma red en varios departamentos.

El simulador Packet Tracer permite realizar un diseño de red complejo y facilitar al gestor de red posibles desperfectos o configuraciones que pongan en peligro una red antes de ser implementada en una red física.

ESCENARIO 1

Escenario: En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un Reuter, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El Reuter y el switch también deben administrarse de forma segura.

Topología de la Red:

Figura 1 Escenario propuesto (Simulador)

Fuente: Documento guía prueba de habilidades practicas

Objetivos

Parte 1: Construir en el simulador la Red

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

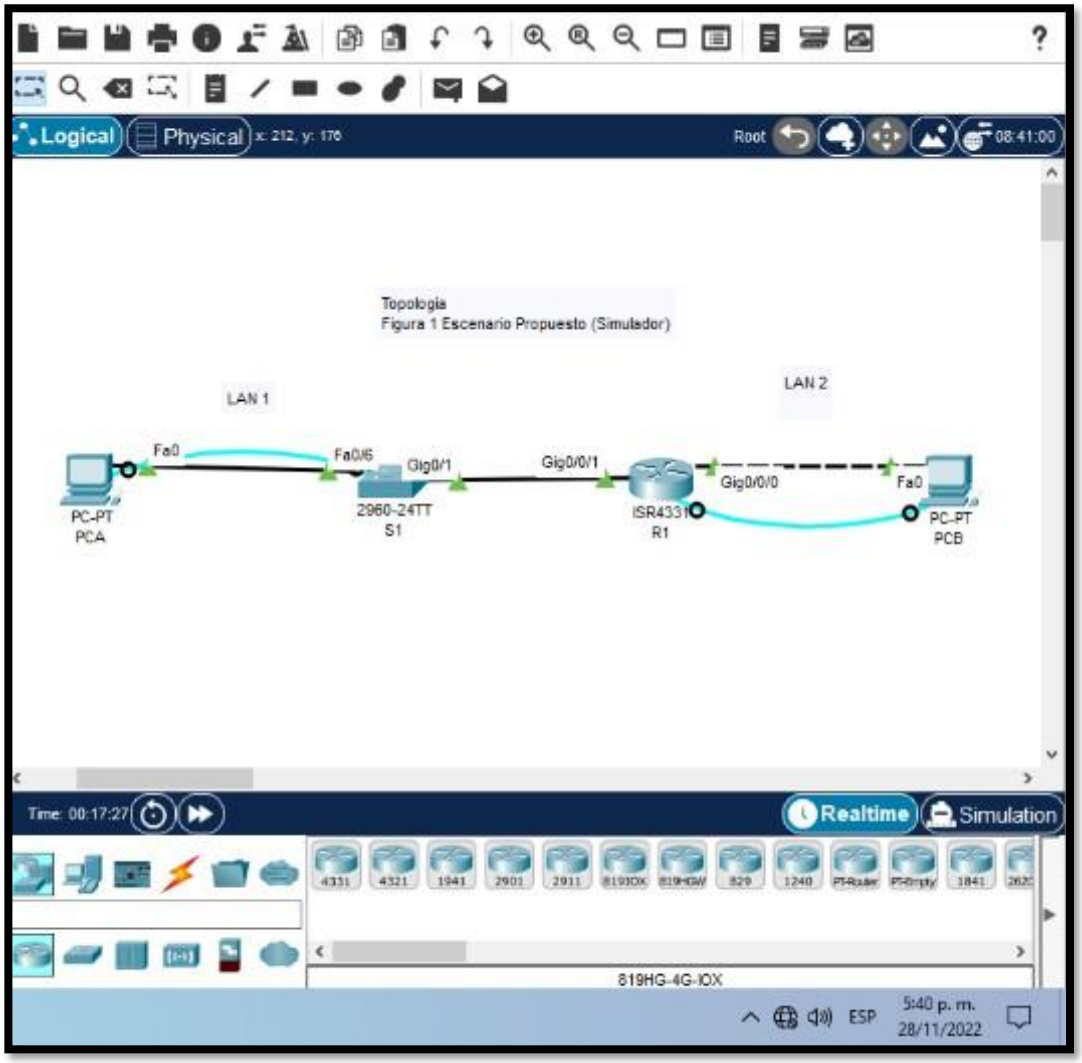
En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Reuter R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1

(60 host) y la LAN2 (20 hosts)

Parte 1: Construya la Red

En el simulador se construye la red de acuerdo con la topología lógica que se plantea en la figura 1, cablee conforme se indica en la topología, y conecte los equipos de cómputo.

Figura 2 escenario con cable de consola



Fuente: autoría propia

Construcción del escenario en el simulador Packet Tracer

Parte 2: Desarrolle el esquema de direccionamiento IP

Se desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredescon la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento.

Tabla 1 de direccionamiento de la red.

Item	**Requerimiento**
Dirección de Red	172.12.3.0 /25
Requerimiento de host SubredLAN1	60
Requerimiento de host SubredLAN2	20
R1 G0/0/1	172.12.3.62 /26
R1 G0/0/0	172.12.3.94/27
S1 SVI	172.12.3.2 /26
PC-A	172.12.3.10 /26
PC-B	172.12.3.106 /27

Fuente: Documento Prueba de Habilidades Practicas CCNA

Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola.

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 2 configuración básica en R1

Tarea	Especificación
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del Reuter	R1 Router(config)#hostname R1
Nombre de dominio	ccna-sa.com R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoconpass R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	10 caracteres R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** R1(config)#username admin password admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las	R1(config-line)#transport input SSH R1(config-line)#exit

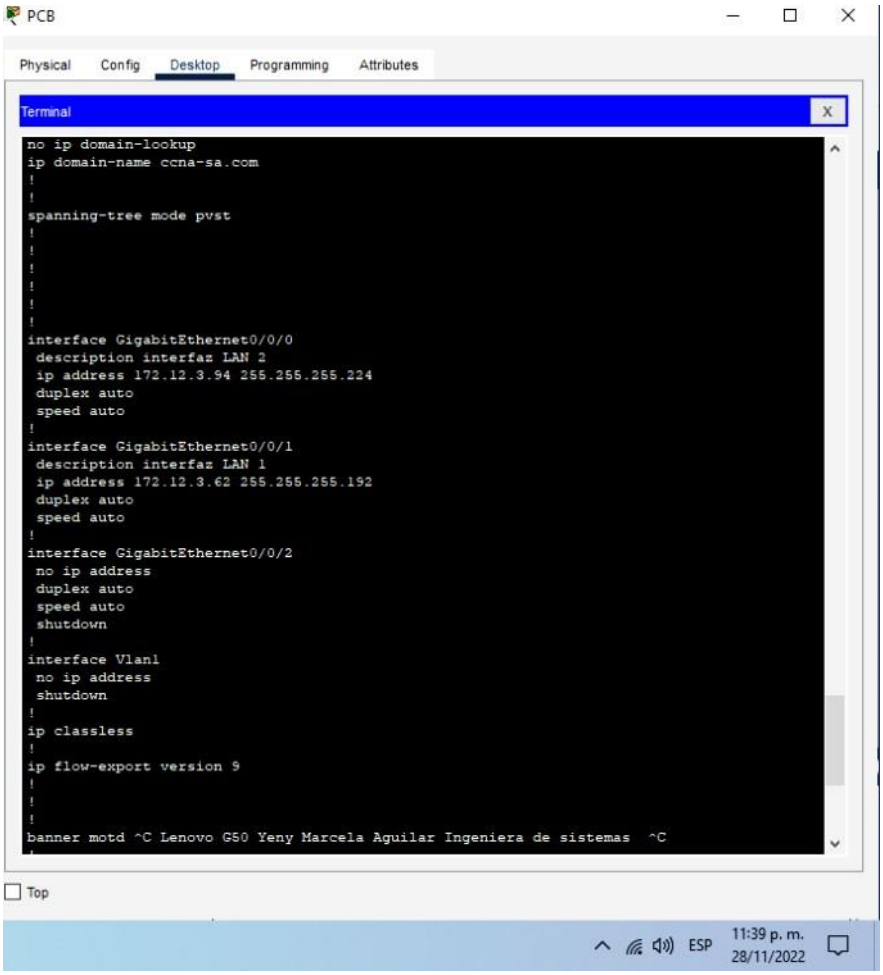
conexionesSSH	
Cifrar las contraseñas de texto nocifrado	R1(config)#service password-encryption
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. R1(config)#banner Motd " Lenovo G50 Yeny Marcela Aguilar Ingeniería de sistemas "
Configuración de interface G0/0/0	Establecer la descripción Establecer la dirección IPv4 Activar la interfaz. R1(config)#interface g 0/0/0 R1(config-if)#ip address 172.12.3.94 255.255.255.224 R1(config-if)#description interfaz LAN2 R1(config-if)#no shutdown R1(config-if)#exit
Configuración de interface G0/0/1	Establecer la descripción Establecer la dirección IPv4 Activar la interfaz. R1(config-if)#interface g 0/0/1 R1(config-if)#ip address 172.12.3.62 255.255.255.192 R1(config-if)#description interfaz LAN1 R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits R1(config)#ip domain-name ccna-sa.com R1(config)#crypto key generate RSA The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of

	360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 R1(config)#exit

Fuente: Documento Prueba de Habilidades Practicas CCNA

Luego de configurar el Router R1 según la tabla de configuración básica se puede verificar la configuración con el comando Show Run según la figura 3 en R1.

Figura 3 ventana show run de R1



Fuente: autoría propia

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3 configuración básica en S1

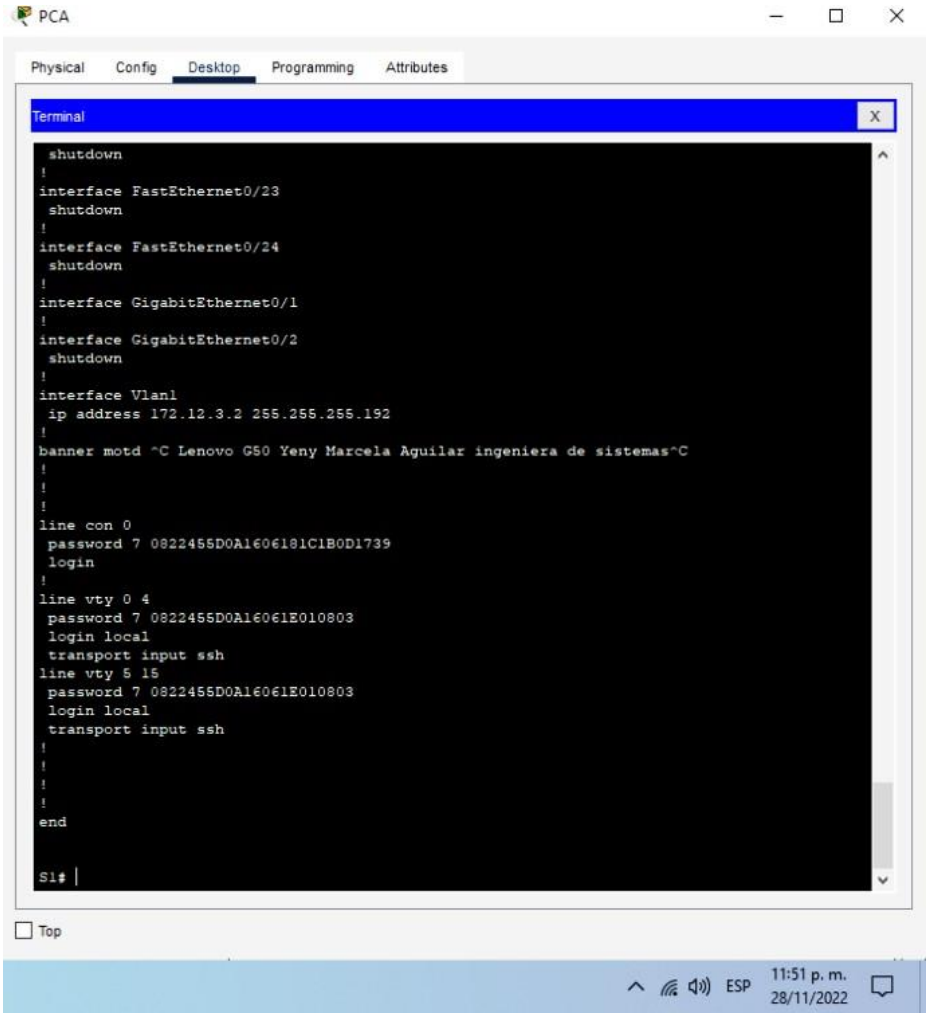
Tarea	Especificación
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup
Nombre del switch	S1 Switch (config)#hostname S1
Nombre de dominio	ccna-sa.com S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	ciscoconpass S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Apagar todos los puertos sin usar	F0/1-4, F0/7-24, G0/1-2 S1(config)#interf range F0/1-4, F0/7-24, G0/2 S1(config-if- range)#shutdown S1(config-if- range)#exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Contraseña: **admin1pass** S1(config)#username admin password admin1pass S1(config)#exit
Configure el inicio de sesión en las líneas	S1(config)#line vty 0 15 R1(config-line)#password ciscocisco R1(config-line)#login local

VTY para que use la base dedatos local	S1(config)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input SSH S1(config-line)#exit
Cifrar las contraseñas de texto nocifrado	S1(config)#service password-encryption
Configurar un banner MOTD	Debe contener el nombre del dispositivo, el nombre completodel estudiante y el programa académico al que pertenece. S1(config)#banner Motd " Lenovo G50 Yeny Marcela Aguilar ingeniería de sistemas"
Generar una clave de cifrado RSA	Módulo de 1024 bits s1(config)#ip domain-name ccna-sa.com s1(config)#crypto key generate RSA The name for the keys will be: s1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 S1(config)#exit
Configure la interfaz de administración (SVI) en VLAN1	Establecer la descripción Establecer la dirección IPv4 S1(config)#interface vlan 1 S1(config-if)#ip address 172.12.3.2 255.255.255.192 S1(config-if)#no shutdown

Fuente: Documento Prueba de Habilidades Practicas CCNA

Ya finalizada la configuración en el Switch S1, por medio de SSH en PCA, en terminal, se utiliza el comando Show Run para visualizar la configuración y verificar que sea correcta, como lo muestra la figura 4 en S1.

Figura 4 show run de S1



Fuente : Autoría propia

Paso 2. Configurar los equipos

Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

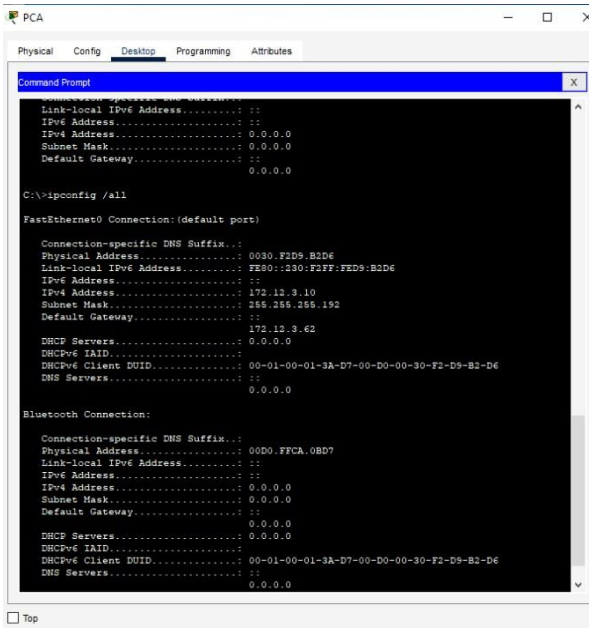
Tabla 4 configuración de red en PC-A

Configuración de red de PC-A	
Descripción	Pertenece LAN1
Dirección física	0030.F2D9.B2D6
Dirección IPv4	172.12.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.12.3.62

Fuente: Documento Prueba de Habilidades Practicas CCNA

Verificación de la configuración en PCA

Figura 5 Comando ipconfig /all en PC A



Fuente: autoría propia

Este comando, ipconfig /all permite verificar la dirección Ipv4 e IPv6 en que esta conectado el dispositivo, también muestra la dirección por defecto, dirección Mac, link-local Ipv6 address entre lo más destacado

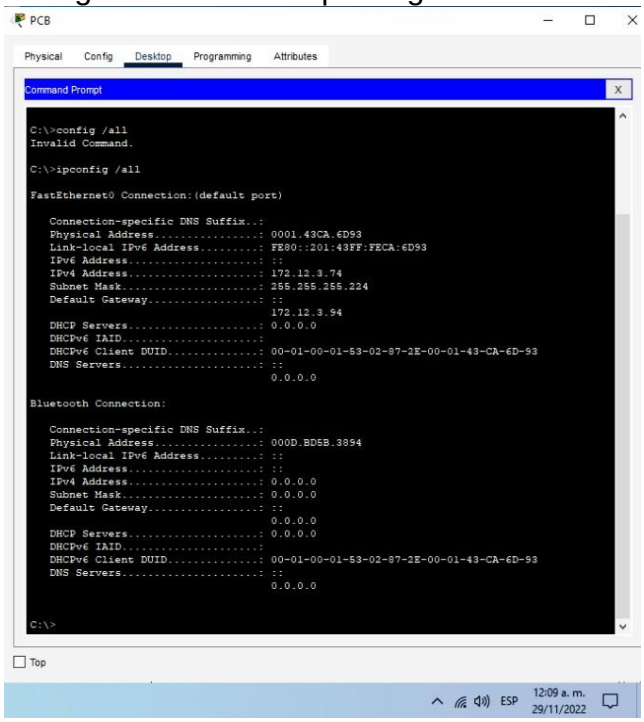
Tabla 5 configuración de red en PC-B

Configuración de red de PC-B	
Descripción	Pertenece LAN2
Dirección física	0001.43CA.6D93
Dirección IPv4	172.12.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.12.3.94

Fuente: Documento Prueba de Habilidades Practicas CCNA

Verificación de red de PC_B

Figura 6 comando ipconfig /all en PC B



Fuente: autoría Propia

Este comando se revisa las direcciones Ipv6 e Ipv4 que están configuradas en el dispositivo, se puede identificar la Mac del equipo y su dirección por defecto.

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

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

Nota: Si los pings a los servidores fallan, deshabilite temporalmente el firewall del equipo yvuelva a realizar la verificación.

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

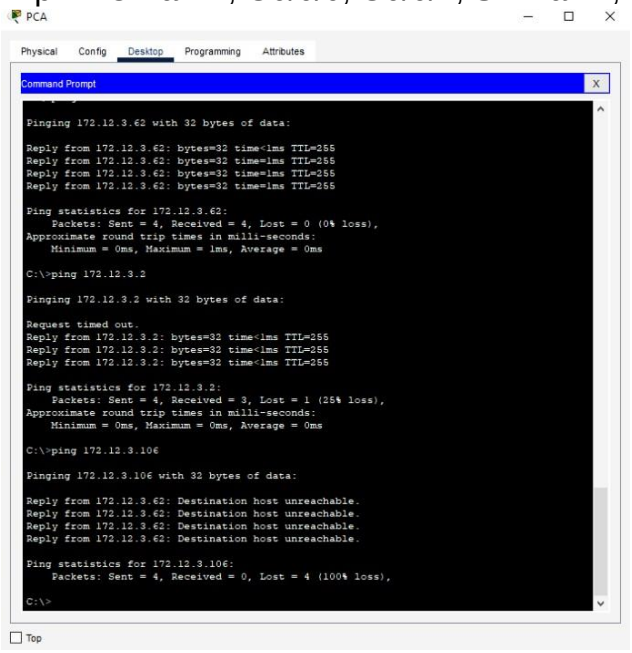
Tabla 6 conectividad entre PC-A, PC-B, S1 Y R1

Desde	**A**	**Dirección IP**	**Resultados de ping**
PC-A	R1 G0/0/0	172.12.3.94	exitoso
	R1 G0/0/1	172.12.3.62	exitoso
	S1 VLAN 1	172.12.3.2	exitoso
	PC-B	172.12.3.106	exitoso
PC-B	R1 G0/0/0	172.12.3.94	exitoso
	R1 G0/0/1	172.12.3.62	exitoso
	S1 VLAN1	172.12.3.106	exitoso

Fuente: Documento Prueba de Habilidades Practicas CCNA

Verificación de conectividad en PCA a R1, G0/0/0, G0/0/1, S1 Vlan 1, PC–B

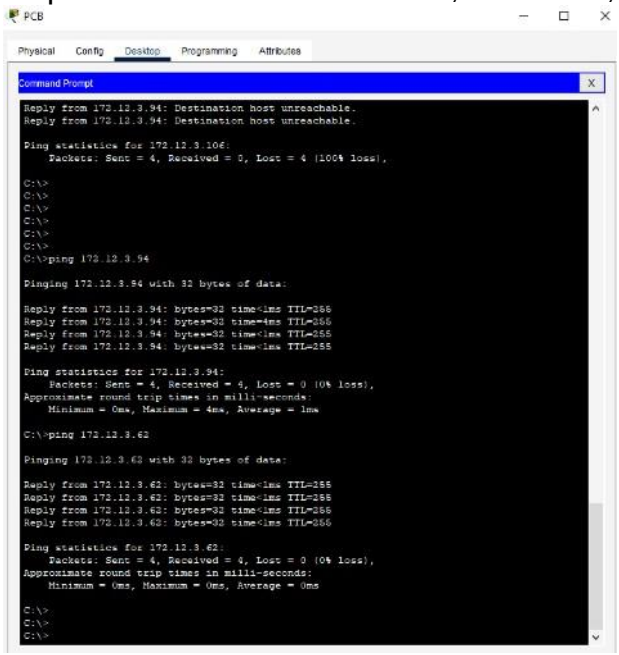
Figura 7 pin PCA a R1, G0/0/0, G0/0/1, S1 Vlan 1, PC – B



Fuente autoría propia

Según la figura 7, en PC-A hay conectividad a R1, G0/0/0, G0/0/1, S1 Vlan 1, PC – B, verificado por medio de Ping a cada uno de los dispositivos de la red.

Figura 8 pin PCB a R1 G0/0/0 G0/0/1, S1 Vlan 1, PC–A



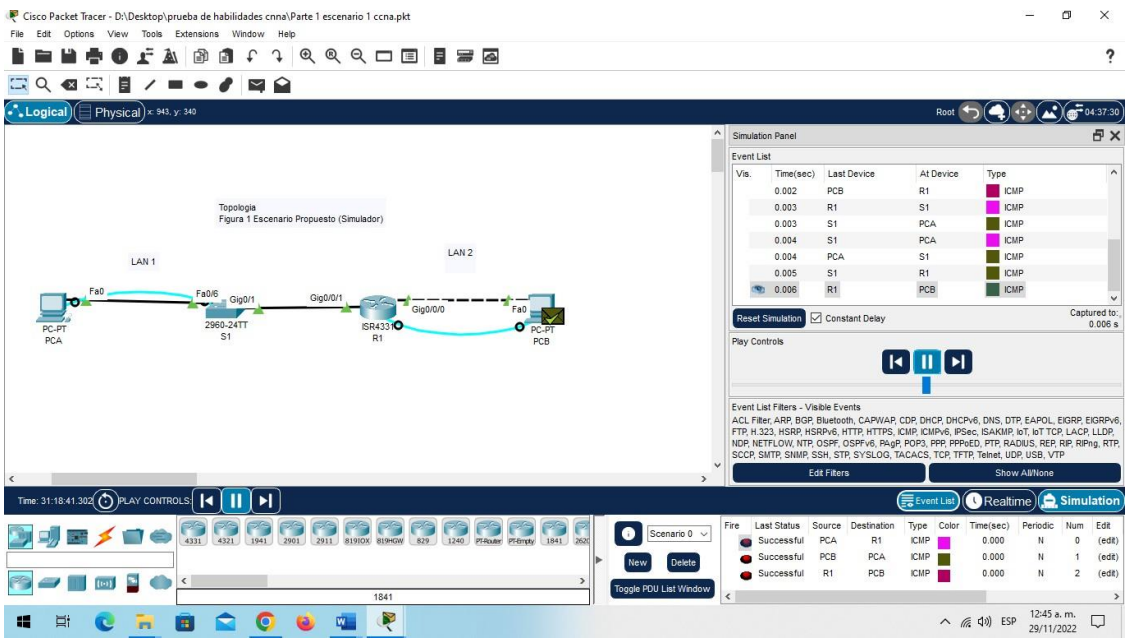
Fuente autoría propia

En la figura 8, en PC-B hay conectividad a R1, G0/0/0, G0/0/1, S1 Vlan 1, PC – B, verificado por medio de Ping a cada uno de los dispositivos de la red.

El comando ping más ip address permite verificar la conectividad en un host remoto, los protocolos de enrutamiento sean en Iv4 e Ipv6 pueden enviar un datagrama para recibir una respuesta de otro dispositivo host conectado en la red, el ICM es un protocolo que revisa y corrige posibles problemas de redes TCP/IP

Topología final

Figura 9 topología final escenario 1

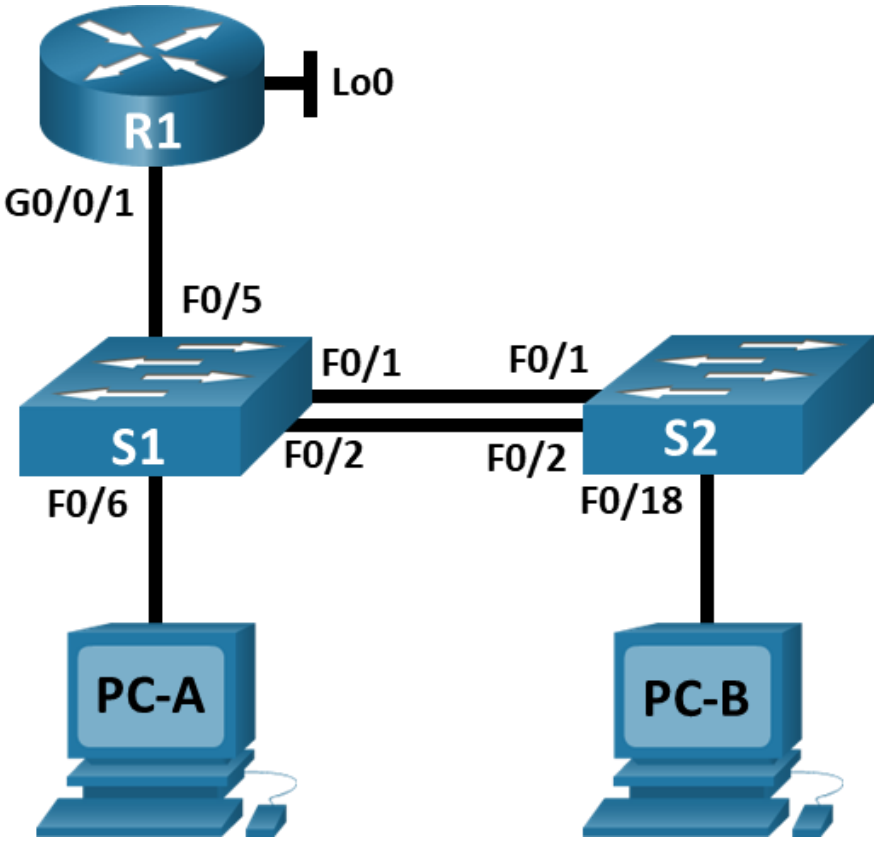


Fuente : autoría propia

ESCENARIO 2

Topología

Figura 10 escenario 2



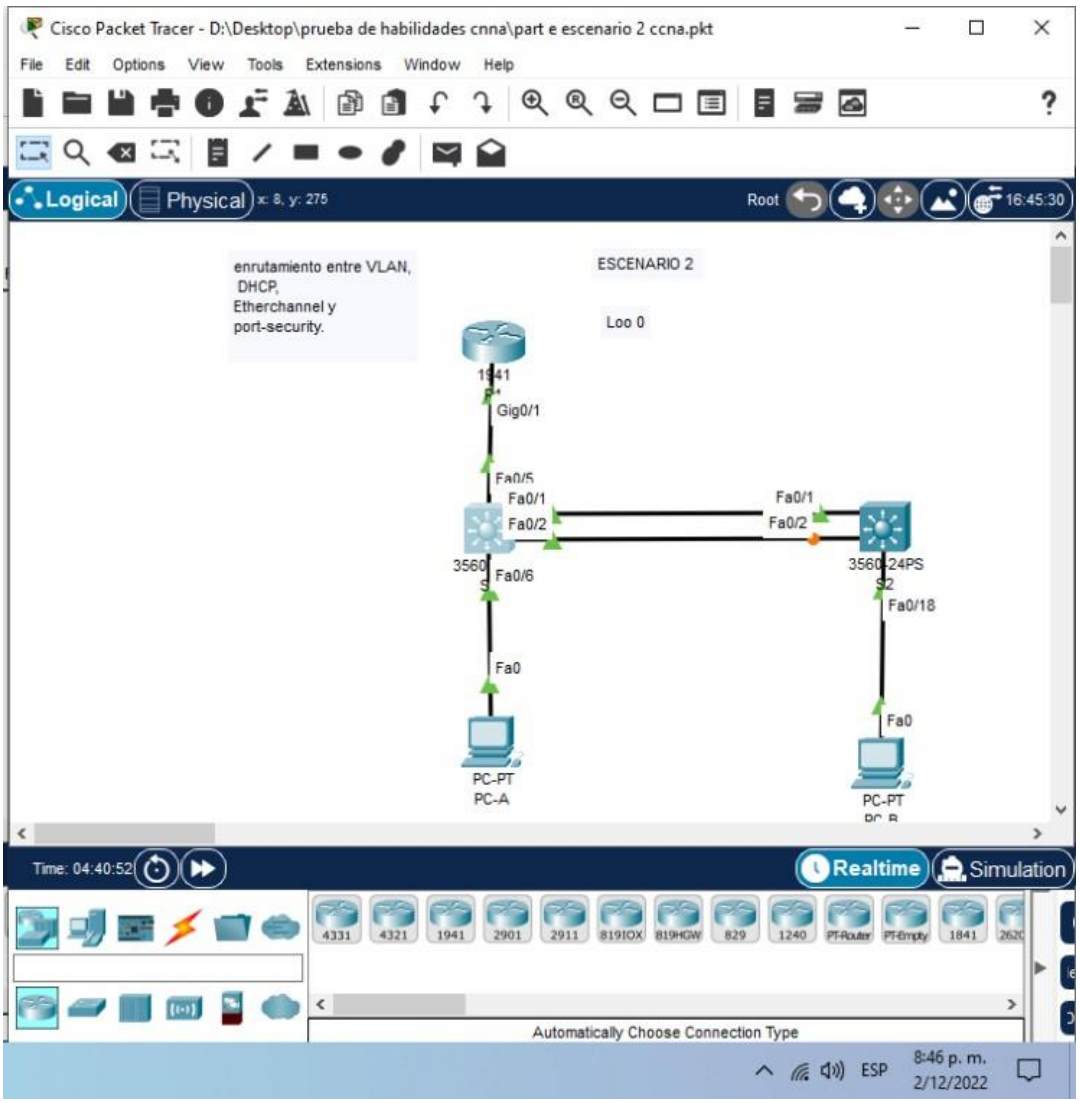
Autoría documento guía prueba de habilidades

En este escenario se configurarán los dispositivos de una red pequeña. Debe configurarun 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.

Topología de la red escenario 2

Según el escenario propuesto, se usan dispositivos cisco para la construcción de la red.

Figura 11 construcción escenario 2



Fuente: Autoría propia

Se construye el escenario 2 en el simulador Packet Tracer, usando dispositivos Router 1941, Switch 3560 y Pcs con tecnología cisco.

Tabla de VLAN

Tabla 8 Tabla de vlans

VLAN	Nombre de la VLAN
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

Fuente: documento prueba de habilidades practicas ccna

Con los datos de la tabla de vlan se asigna esta configuración en cada uno de los switches, S1 y S2.

Tabla de asignación de direcciones

Tabla 9 Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.12.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.12.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.12.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde

R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1/64	No corresponde
S1 VLAN 4	10.12.8.98 /29	10.12.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.12.8.99 /29	10.12.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP paraIPv4	DHCP para puerta de enlace predeterminadaIPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminadaIPv4
	2001:db8:acad:b: :50 /64	fe80::1

Fuente: documento prueba de habilidades practicas ccna

Nota: No hay ninguna interfaz en el router que admita VLAN 50.

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

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

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

Configuracion en Router 1

Enable

Erase startup-config

Delete flash:vlans.dat

Reload.

Configuracion en Switch 1

Enable

Erase startup-config

Delete flash:vlans.dat

Reload.

Configuracion en Switch 2

Enable

Erase startup-config

Delete flash:vlans.dat

Reload.

- Después de recargar el switch, configure la plantilla SDM para que admita IPv6según sea necesario y vuelva a cargar el switch.

Esto acción se realiza en equipos reales hace parte de la configuración de una red simulada, Los comandos son:

En Sw1

Switch>enable

Switch#configure terminal
Switch(config)#sdm prefer dual-ipv4 and ipv6 routing

Switch(config)# do reload

En Sw2

Switch>enable

Switch#configure terminal
Switch(config)#sdm prefer dual-ipv4 and ipv6 routing

Switch(config)# do reload

Paso 2: Configuración en R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 10 Configuración de R1

Tarea	Especificación
Desactivar la búsqueda DNS	*Enable* *Configure terminal* *No ip domain-lookup*
Nombre del Reuter	R1 *Enable* *Configure terminal* *Hostname R1*
Nombre de dominio	ccna-sa.com *Enable* *Configure terminal* *Ip domain name* ccna-sa.com
Contraseña cifrada para el modo EXECprivilegiado	class *Enable* *Configure terminal* *Enable secret class*
Contraseña de acceso a la consola	cisco *Enable* *Configure terminal* *Line console 0* Password cisco login exit
Establecer la longitud mínima para las contraseñas	5 caracteres *Enable* *Configure terminal*

	Security passwords min-length 5 Exit
Crear un usuario administrativo en labase de datos local	Nombre de usuario: **admin** Password: **admin1pass** *Enable* *Configure terminal* *Username admin privilege 15* *Secret admin1pass* *Exit*
Configurar el inicio de sesión en las líneas VTY para que use la base de datoslocal	*line vty 0 4* *login local* *exit*
Configurar VTY solo aceptando SSH	*line vty 0 4* *transport input ssh* *login local* *exit*
Cifrar las contraseñas de texto nocifrado	*service password-encryption* *Enable* *Configure terminal* *service password-encryption* *exit*
Configure un MOTD Banner	*R1(config)#banner Motd " –Lenovo G50 Yeny Marcela Aguilar ingeniería de sistemas-"*
Habilitar el routing IPv6	*Enable* *Configure terminal* *ipv6 unicast routing*

Configurar interfaz G0/0/1 ysubinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6como **fe80: :1** Establece la dirección IPv6.Activar la interfaz. *R1(config)#interface gi0/1.20* *R1(config-subif)#encapsulation dot1q 20* *R1(config-subif)#description LAN to VLAN20* *R1(config-subif)#ip add 10.12.8.1 255.255.255.192* *R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64* *R1(config-subif)#ipv6 add fe80::1 link-local* *R1(config-subif)#no shutdown* *R1(config-subif)#exit* *R1(config)#interface gi0/1.30* *R1(config-subif)#encapsulation dot1q 30* *R1(config-subif)#ip add 10.12.8.65 255.255.255.224* *R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64* *R1(config-subif)#ipv6 add fe80::1 link-local* *R1(config-subif)#description LAN to VLAN30* *R1(config-subif)#no shutdown* *R1(config-subif)#exit* *R1(config)#interface gi0/1.40* *R1(config-subif)#encapsulation dot1q 40* *R1(config-subif)#ip add 10.12.8.97*

	255.255.255.248 *R1(config-subif)#ipv6 add* *2001:db8:acad:c::1/64* *R1(config-subif)#ipv6 add fe80::1 link-local* *R1(config-subif)#description LAN to* *VLAN40* *R1(config-subif)#no shutdown* *R1(config-subif)#exit* *R1(config)#interface gi0/1.56* *R1(config-subif)#encapsulation dot1q 5* *R1(config-subif)#description LAN to* *VLAN56* *R1(config-subif)#exit* *R1(config)#interface gi0/1* *R1(config-subif)#ipv6 add fe80::1 link-local* *R1(config-if)#no shutdown*
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1** *R1(config)#interface lo0* *R1(config-if)#description LAN to* *Loopback0* *R1(config-if)#ip add 209.165.201.1* *255.255.255.224* *R1(config-if)#ipv6 add* *2001:db8:acad:209::1/64* *R1(config-if)#ipv6 add FE80::1 link-local* *R1(config-if)#no shutdown* *R1(config-if)#exit*

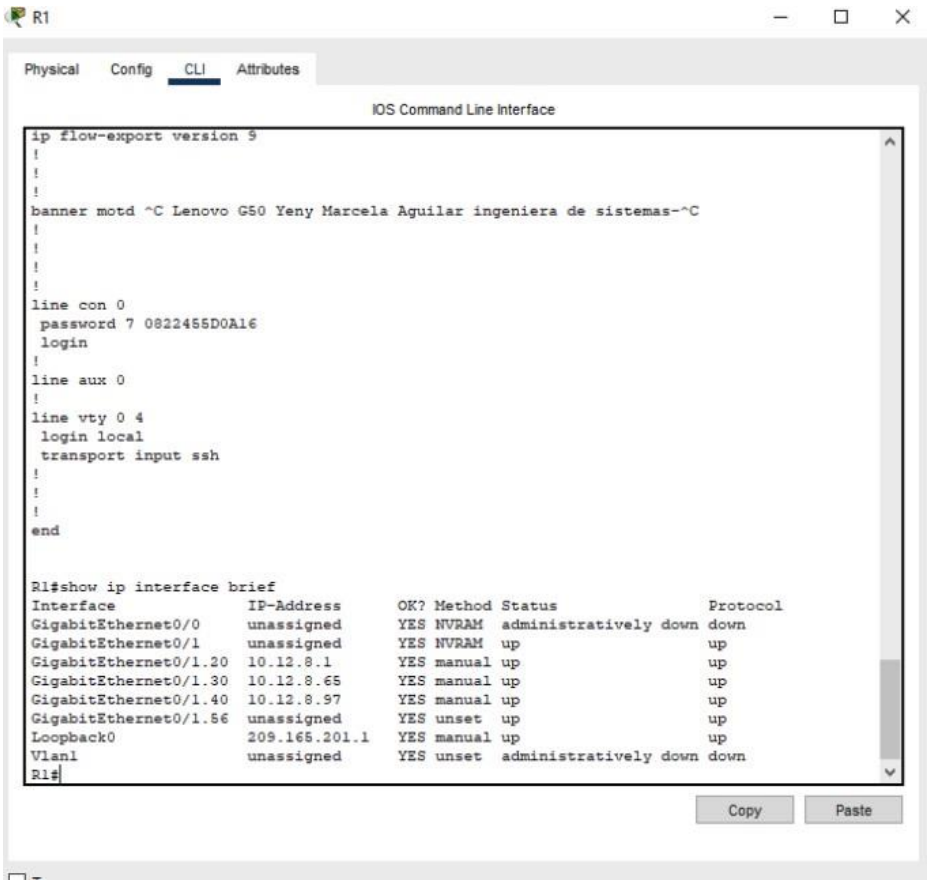
Generar una clave de cifrado RSA	Módulo de 1024 bits *R1(config)#crypto key generate rsa general-key modulus 1024*

Fuente: documento prueba de habilidades practicas ccna

Verificación de la configuración en R1

Utilizamos el comando show ip interface brief

Figura 12 configuración R1



Autoría propia

En la figura 12 se aprecian las subredes creadas para la conectividad con las vlan

que van a estar presentes en el switch, para visualizar estas subinterfaces se ha introducido el comando show ip interface brief, que me permite todas las interfaces del dispositivo, su estado y la dirección ipv4 conectadas.

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 11 Configuración de Switch, S1 y S2

Tarea	Especificación
Desactivar la búsqueda DNS.	*Enable* *Configure terminal* *No Ip domain-lookup*
Nombre del switch	S1 o S2, según proceda *Enable* *Configure terminal* *Hostname S1* *Enable* *Configure terminal* *Hostname S2*
Nombre de dominio	ccna-sa.com *Enable* *Configure terminal* *Ip domain name* ccna-sa.com
Contraseña cifrada para el modo EXECprivilegiado	Class *Enable* *Configure terminal* *Enable secret class*

Contraseña de acceso a la consola	Cisco *Enable* *Configure terminal* *Line console 0* Password cisco login exit
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass** *Enable* *Configure terminal* *Username admin privilege 15* *Secret admin1pass* *Exit*
Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local	*line vty 0 4* *login local* *exit*
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	*line vty 0 4* *transport input ssh* *login local* *exit*
Cifrar las contraseñas de texto no cifrado	*Enable* *Configure terminal* *service password-encryption* *exit*
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo delestudiante y el programa académicoal que pertenece. *Enable* *Configure terminal* *banner Motd " –Lenovo G50*

	Yeny Marcela Aguilar ingeniería de sistemas --"
Generar una clave de cifrado RSA	**Módulo de 1024 bits** *R1(config)#crypto key generate rsa general-key modulus 1024*
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1** **y FE80: :99 para S2** Establecer la dirección IPv6 de capa3 ***S1*** *Enable* *Configure terminal* *Ipv6 unicast-routing* *interface Vlan 40* *ip address 10.12.8.98 255.255.255.248* *ipv6 address 2001:db8:acad:c::98 /64* *ipv6 address fe80::98 link-local* *no shut* *exit* ***S2*** *Enable* *Configure terminal* *Ipv6 unicast-routing* *interface Vlan 40* *ip address 10.12.8.99*

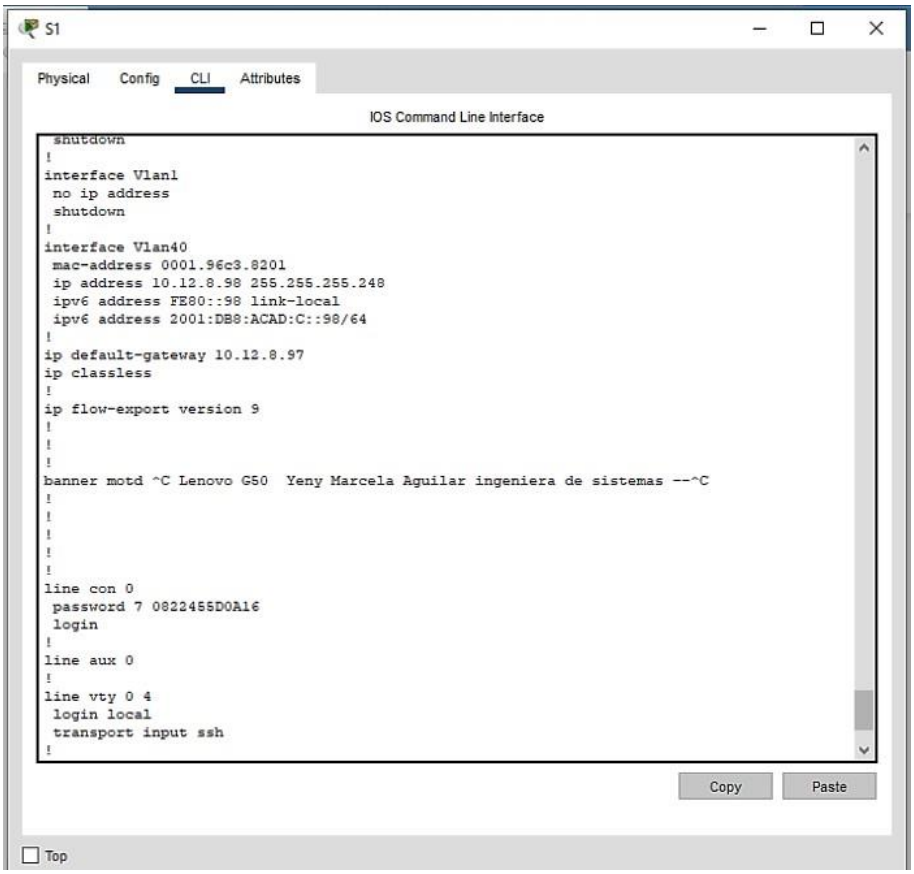
	255.255.255.248 *ipv6 address* *2001:db8:acad:c::99 /64* *ipv6 address fe80::99 link-local* *no shut* *exit*
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada como 10.12.8.97para IPv4 *S1* *Enable* *Configure terminal* *interface Vlan 4* *ip default-gateway 10.12.8.97* S2 *Enable* *Configure terminal* *interface Vlan4* *ip default-gateway 10.12.8.97*

Fuente: documento prueba de habilidades practicas ccna

Verificación de la configuración en switchs S1 y S2

Terminado la configuración en switch S1 y switch S2, se puede revisar si los dispositivos s están configurados correctamente, utilizando el comando Show running-config .

Figura 13 configuración S1

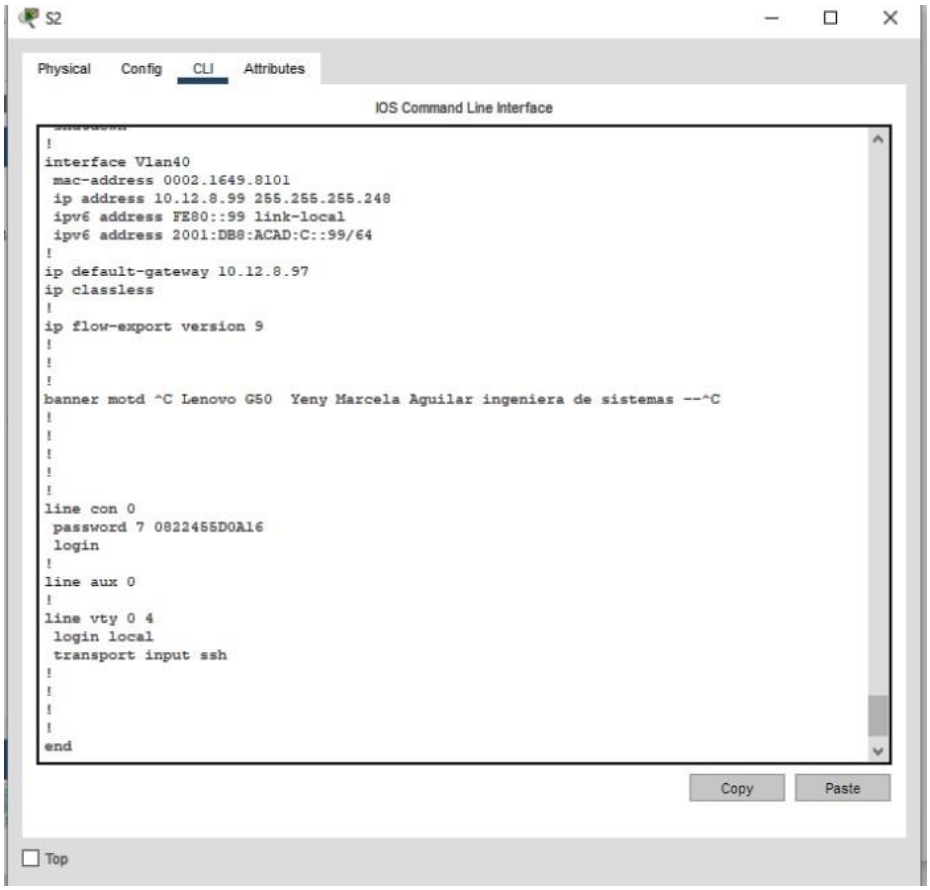


Fuente de autoría propia

En la figura 13 se evidencia la configuración de S1, la vlan 40 con el enrutamiento correcto y el default-Gateway por donde se conectará la red.

Las contraseñas establecidas no se muestran por la configuración de encriptación en el dispositivo, se aprecia números y letras sin lógica.

Figura 14 configuración S2



Fuente de autoría propia

En la figura 14 se evidencia la configuración de S2, la vlan 40 con el enrutamiento correcto y el default-Gateway que es el mismo de S1 y por donde se conectara también a la red

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12 Configuración de Switch S1

Tarea	**Especificación**
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native S1 *enable* *configure terminal* *VLAN 20* *name Docentes* *VLAN 30* *name Estudiantes* *VLAN 40* *name Invitados* *VLAN 50* *name Usuarios* *VLAN 56* *name Native*
Crear troncos 802.1Q que utilicen la VLAN 6nativa	Interfaces F0/1, F0/2 y F0/5 *S1* *Enable* *Configure terminal* *interface FastEthernet 0/1* *switchport trunk encapsulation dot1q* *switchport trunk native vlan 56* *switchport mode trunk* *interface FastEthernet0/2* *switchport trunk encapsulation dot1q*

	switchport trunk native vlan 56 *switchport mode trunk* *interface FastEthernet0/5* *switchport trunk encapsulation dot1q* *switchport trunk native vlan 56* *switchport mode trunk*
Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para lanegociación *S1* *Enable* *Configure terminal* *interface Port-channel1* *switchport trunk encapsulation dot1q* *switchport mode trunk* *exit* *interface FastEthernet0/1* *switchport trunk native vlan 56* *switchport trunk encapsulation dot1q* *switchport mode trunk* *channel-protocol lacp* *channel-group 1 mode active* *exit* *interface FastEthernet0/2* *switchport trunk encapsulation dot1q* *switchport trunk native vlan 56* *switchport mode trunk*

	channel-protocol lacp *channel-group 1 mode active* exit interface range FastEthernet0/1-2 switchport trunk allowed vlan20,30,40,50,56 exit
Configurar el puerto de acceso de host paraVLAN 20	Interface F0/6 *Enable* *Configure terminal* *Interface F0/6* *switchport access vlan 20* *switchport mode access* *no shut* *exit*
Configurar la seguridad del puerto en los puertos de acceso	Permitir 4 direcciones MAC *Enable* *Configure terminal* *interface range FastEthernet 0/3 -4* *switchport port-security* *switchport port-security maximum 4* *interface range FastEthernet 0/6 -24* *switchport port-security* *switchport port-security maximum 4*
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar

	interface FastEthernet0/3 *description DOWN THE SECURITY PORT* *switchport access vlan 50* *switchport mode access* *switchport port-security* *switchport port-security maximum 4* *shutdown* *interface FastEthernet0/4* *description DOWN-SECURITY* *switchport access vlan 50* *switchport mode access* *switchport port-security* *switchport port-security maximum 4* *shutdown* *interface FastEthernet0/7* *description DOWN-SECURITY* *switchport access vlan 50* *switchport mode access* *switchport port-security* *switchport port-security maximum 4* *shutdown* *interface FastEthernet0/8* *description DOWN-SECURITY* *switchport access vlan 50* *switchport mode access* *switchport port-security*

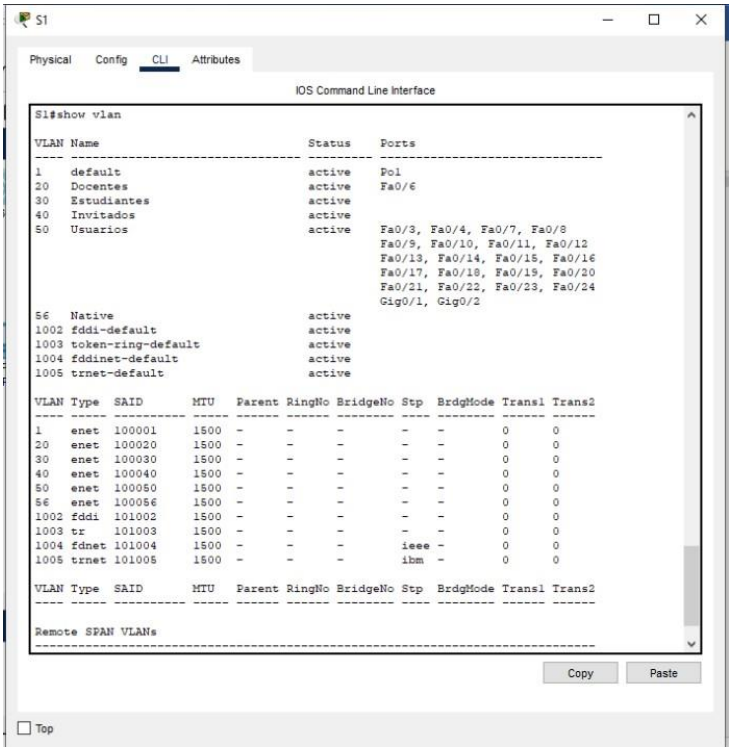
	switchport port-security maximum 4 *shutdown* *interface FastEthernet0/9* *description DOWN-SECURITY* *switchport access vlan 50* *switchport mode access* *switchport port-security* *switchport port-security maximum 4* *shutdown* *interface FastEthernet0/10* *description DOWN-SECURITY* *switchport access vlan 50* *switchport mode access* *switchport port-security*

Fuente: Documento Prueba de Habilidades Practicas CCNA

Al verificar las vlan existentes en el switch S1, se utiliza el comando Show Vlan, que expone las vlan con su nombre, estado y los puertos activos.

En este momento de la configuración es indispensable que las vlan creadas estén correctamente nombradas

Figura 15 vlans existentes en S1



Fuente de autoría propia

En la figura 15, expone un listado de las vlans creadas , el estado de las vlans, los puertos asignados a cada vlan, por medio del comando show vlan.

Al presentarse algún error en la creación de las vlans nombradas, se puede corregir borrando la vlan y volver a crearla con los parámetros establecidos asegurando la correcta configuración del switch S1.

Paso 5: Configure el S2.

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

Tabla 13 Configuración de Switch S2

Tarea	Especificación
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native S2 *enable* *configure terminal* *VLAN 20* *name Docentes* *VLAN 30* *name Estudiantes* *VLAN 40* *name Invitados* *VLAN 50* *name Usuarios* *VLAN 56* *name Native*
Crear troncos 802.1Q que utilicen la VLAN 56 nativa	Interfaces F0/1 y F0/2 *S2* *Enable* *Configure terminal*

	interface FastEthernet 0/1 *switchport trunk native vlan 56* *switchport trunk encapsulation dot1q* *switchport mode trunk* *exit* *interface FastEthernet0/2* *switchport trunk native vlan 56* *switchport trunk encapsulation dot1q* *switchport mode trunk* *exit*
Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para lanegociación *S2* *Enable* *Configure terminal* *interface Port-channel1* *switchport trunk encapsulation dot1q* *switchport mode trunk* *interface FastEthernet0/1* *switchport trunk encapsulation dot1q* *switchport mode trunk* *channel-protocol lacp* *channel-group 1 mode active* *switchport trunk allowed vlan20,30,40,50,56* *exit* *interface FastEthernet0/2* *switchport trunk encapsulation*

	dot1q *switchport mode trunk* *channel-protocol lacp* *channel-group 1 mode active* *switchport trunk allowed vlan20,30,40,50,56* *exit*
Configurar el puerto de acceso del host para laVLAN 30	Interfaz F0/18 *Enable* *Configure terminal* *interface FastEthernet0/18* *switchport access vlan 30* *switchport mode access* *switchport port-security* *switchport port-security maximum 4* *exit*
Configure port-security en los access ports	permite 4 MAC address Enable Configure terminal interface range FastEthernet 0/3 -24 switchport port-security switchport port-security maximum 4 interface range GigabitEthernet 0/1 -2 switchport port-security switchport port-security maximum 4

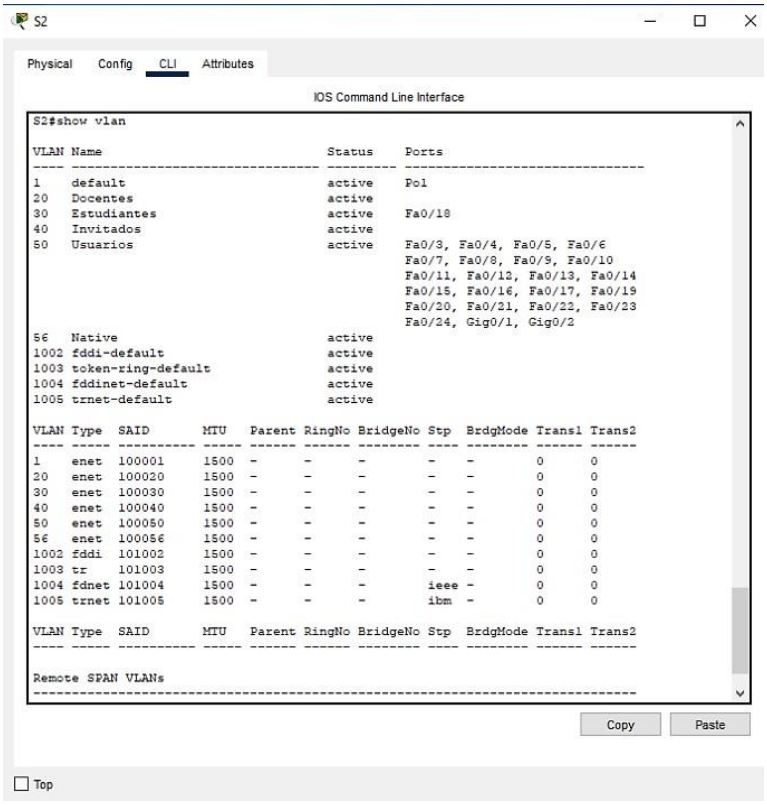
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar *Enable* *Configure terminal* *interface range FastEthernet 0/3 - 17* *description DOWN THE SECURITY PORT* *switchport mode access* *switchport access vlan 50* *shutdown* *interface range FastEthernet 0/19 - 24* *description DOWN THE SECURITY PORT* *switchport mode access* *switchport access vlan 50* *shutdown* *interface range GigabitEthernet 0/1 -2* *description DOWN THE SECURITY PORT* *shutdown*
Configure port-security en los access ports	permite 4 MAC address Enable Configure terminal interface range FastEthernet 0/3 -24 switchport port-security

	switchport port-security maximum 4 interface range GigabitEthernet 0/1 - 2 switchport port-security switchport port-security maximum 4 exit
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar *Enable* *Configure terminal* *interface range FastEthernet 0/3 - 17* *description DOWN-SECURITY* *shutdown* *interface range FastEthernet 0/19 - 24* *description DOWN-SECURITY* *shutdown* *interface range GigabitEthernet 0/1 -2* *description DOWN-SECURITY* *shutdown*

Fuente: Documento Prueba de Habilidades Practicas CCNA

Ya finalizada la configuración en S2, se utilizan comandos que permiten verificar la creación de las vlan , nombre, estado, el comando show vlan expone la información de las vlan del switch S2.

Figura 16 vlans existentes en S2



Fuente de autoría propia

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14 Configuración de soporte de host en R1

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 *Enable* *Configure terminal*

	ip route 0.0.0.0 0.0.0.0 10.12.8.0 *ipv6 route ::/0 2001:db8:acad:209::1*
Configurar IPv4 DHCP paraVLAN 20	Cree un grupo DHCP para VLAN 20, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada *Enable* *Configure terminal* *ip dhcp pool VLAN20* *network 10.12.8.0 255.255.255.192* *default-router 10.12.8.1* *domain-name unad-ccna-sa.net* *ip dhcp excluded-address 10.12.8.52 10.12.8.62* *exit*
Configurar DHCP IPv4 paraVLAN 30	Cree un grupo DHCP para VLAN 30, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada *Enable* *Configure terminal* *ip dhcp pool VLAN30* *network 10.12.8.64 255.255.255.224* *default-router 10.12.8.65* *domain-name* unad-ccna-sb.net *ip dhcp excluded-address 10.12.8.84 10.12.8.94*

Fuente: Documento Prueba de Habilidades Practicas CCNA

Paso 2: Configurar los servidores

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

Tabla 15 Configuración de red en PC-A

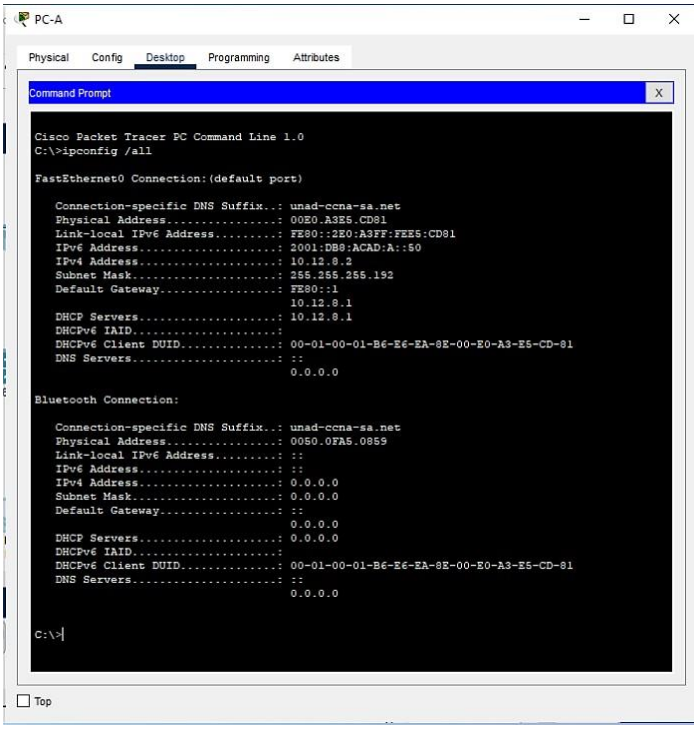
Configuración de red de PC-A	
Descripción	FastEthernet 0 Connection (default port)
Dirección física	OOEO.A3E5.CD81
Dirección IP	10.12.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.12.8.1
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Documento Prueba de Habilidades Practicas CCNA

Para configurar la tabla 15 es necesario ingresar al PC-A y seleccionar la opción Destok y luego command prompt, estando en la ventana se le ingresa el comando ipconfig /all, con la información requerida para llenar la tabla.

El comando, ipconfig, proporciona la información de red, un poco menos detallada el enrutamiento corresponde a la tabla de direccionamiento, y a la puerta de enlace de la red.

Figura 17 ipconfig /all en PC-A



Fuente de autoría propia

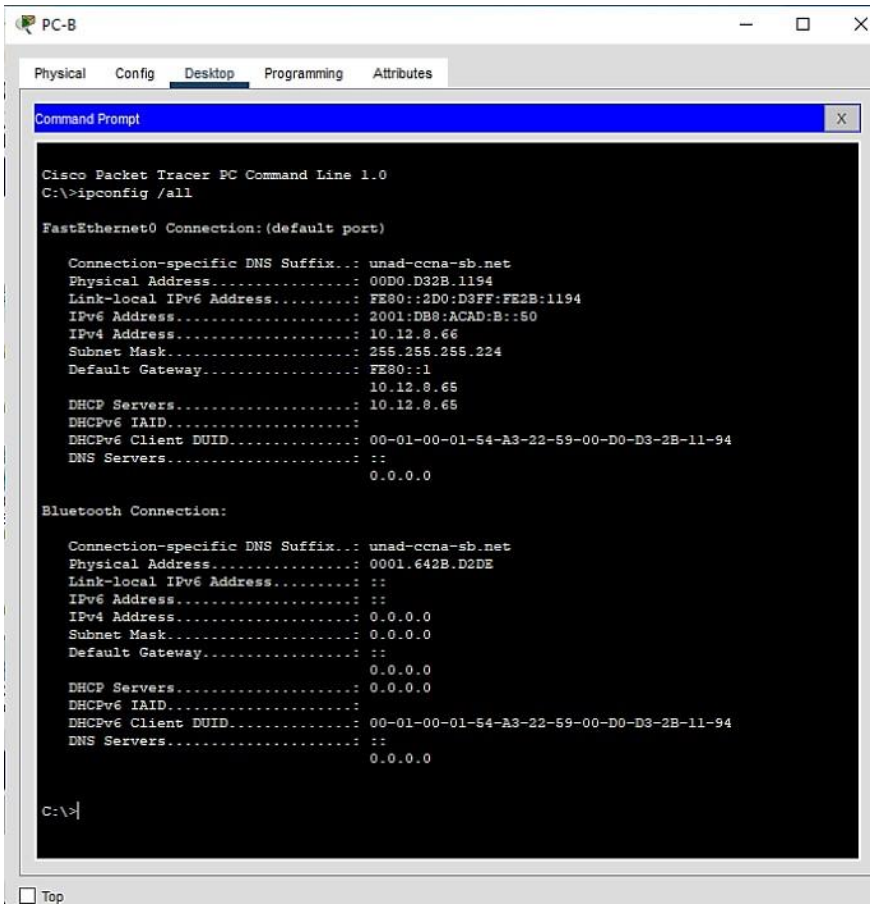
En la figura 17 se aplica el comando ipconfig /all y se muestra la información de red de PC-A con el puerto Fastethernet 0

Tabla 16 Configuración de red en PC-B

Configuración de red de PC-B	
Descripción	FastEthernet 0 Connection (default port)
Dirección física	
Dirección IP	10.12.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.12.8.65
Gateway predeterminado IPv6	2001:DB8:ACAD:B::1

Fuente: Documento Prueba de Habilidades Practicas CCNA

Figura 18 ipconfig /all en PC-B



Fuente de autoría propia

Parte 3: Probar y verificar la conectividad de extremo a extremo

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

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

Tabla 17 conectividad de extremo a extremo

Desde	A		Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.20	IPv4	10.12.8.1	exito
		IPv6	2001:DB8:ACAD:A::1	exito
	R1, G0/0/1.30	IPv4	10.12.8.65	exito
		IPv6	2001:DB8:ACAD:B::1	exito
	R1, G0/0/1.40	IPv4	10.12.8.97	exito
		IPv6	2001:DB8:ACAD:C::1	exito
	S1, VLAN 40	IPv4	10.12.8.98	exito
		IPv6	2001:DB8:ACAD:C::98	Fallo
	S2, VLAN 40	IPv4	10.12.8.99	exitoso
		IPv6	2001:DB8:ACAD:C::99	exitoso
	PC-B	IPv4	DHCP	exitoso
		IPv6	2001:DB8:ACAD:B::50	fallo
	R1 Bucle 0	IPv4	209.165.201.1	exitoso
		IPv6	2001:DB8:ACAD:209::1	exitoso
PC-B	R1 Bucle 0	IPv4	209.165.201.1	exitoso
		IPv6	2001:DB8:ACAD:209::1	exitoso
	R1, G0/0/1.20	IPv4	10.12.8.1	exitoso
		IPv6	2001:DB8:ACAD:A::1	exitoso

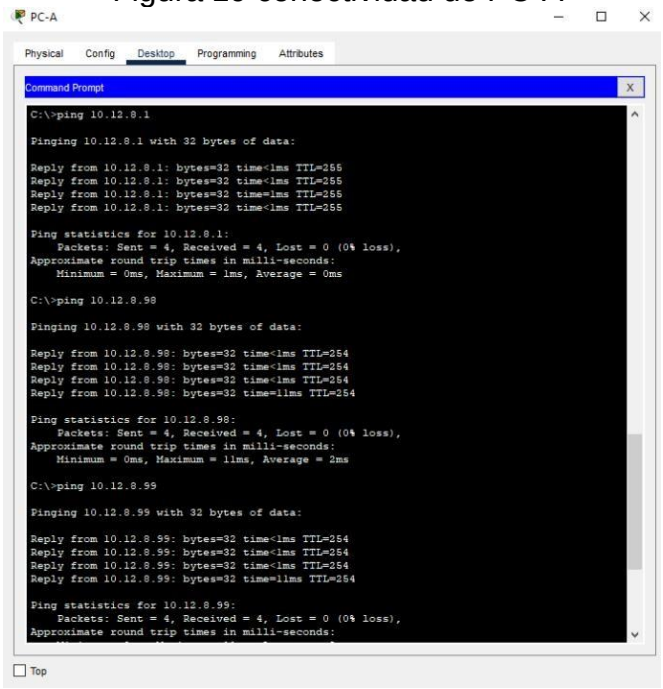
	R1, G0/0/1.30	IPv4	10.12.8.65	exitoso
		IPv6	2001:DB8:ACAD:B::1	exitoso
	R1, G0/0/1.40	IPv4	10.12.8.97	exitoso
		IPv6	2001:DB8:ACAD:C::1	exitoso
	S1, VLAN 40	IPv4	10.12.8.98	exitoso
		IPv6	2001:DB8:ACAD:C::98	fallo
	S2, VLAN 40	IPv4	10.12.8.99	exitoso
		IPv6	2001:DB8:ACAD:C::99	fallo

Fuente: Documento Prueba de Habilidades Practicas CCNA

Verificación de conectividad de externo a extremo

Ping de PCA a R1, G0/0/1.20, , S1 VLAN 40, S2 VLAN 40

Figura 19 conectividad de PC-A



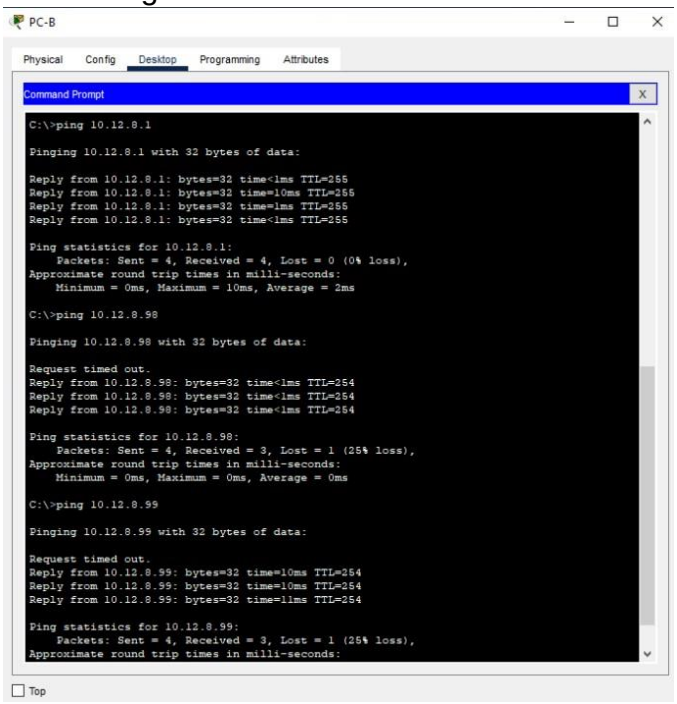
Fuente de autoría propia

En la figura 19 Por medio del comando ping y el direccionamiento de la red, se puede verificar si hay conectividad entre los dispositivos de la red en PC-A

Se verifica la conectividad en PCA a Router R1, G0/1.20 ip 10.12.8.1 con éxito, conectividad de PCA a Switch S1, Vlan 40, ip 10.12.8.97, y conectividad de PCA a Switch, S2 Vlan 40, ip 10.12.8.98 con éxito.

Ping de PCB a R1, G0/0/1.20 , S1 VLAN 40, S2 VLAN 40

Figura 20 conectividad de PC-B



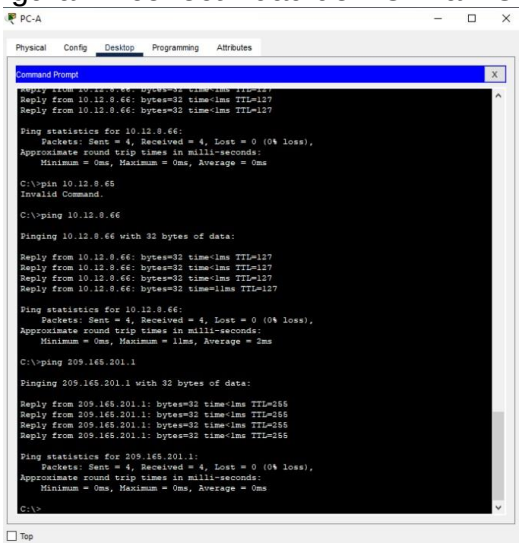
Fuente de autoría propia

En la figura 20. Se verifica la conectividad en PCB a Router R1, G0/1.20 ip 10.12.8.1 con éxito, conectividad de PCA a Switch S1, Vlan 40, ip 10.12.8.98, y conectividad de PCA a Switch, S2 Vlan 40, ip 10.12.8.99 con éxito.

Al presentar algún fallo es recomendable revisar las configuraciones anteriores, a este paso la configuración es de extremo a extremo.

Ping de PCA a PCB, R1 bucle 0

Figura 21 conectividad de PC-A a PC-B

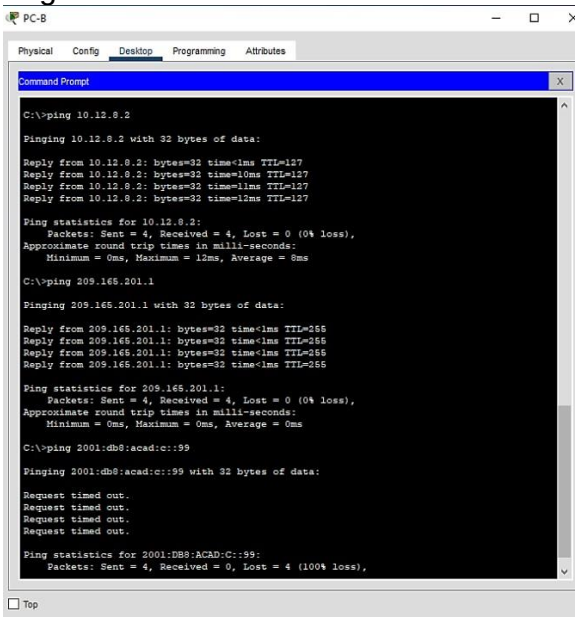


Fuente de autoría propia

En la figura 21. Se verifica la conectividad en de PCA a PCB, ip 10.12.8.66 con éxito, conectividad de PCA a Bucle 0, ip 209.165.201.1con éxito.

Ping de PCB a PCA, R1 bucle 0 Y S1 VLAN 40 2001:DB8:ACAD

Figura 22 conectividad de PC-B a PC-A

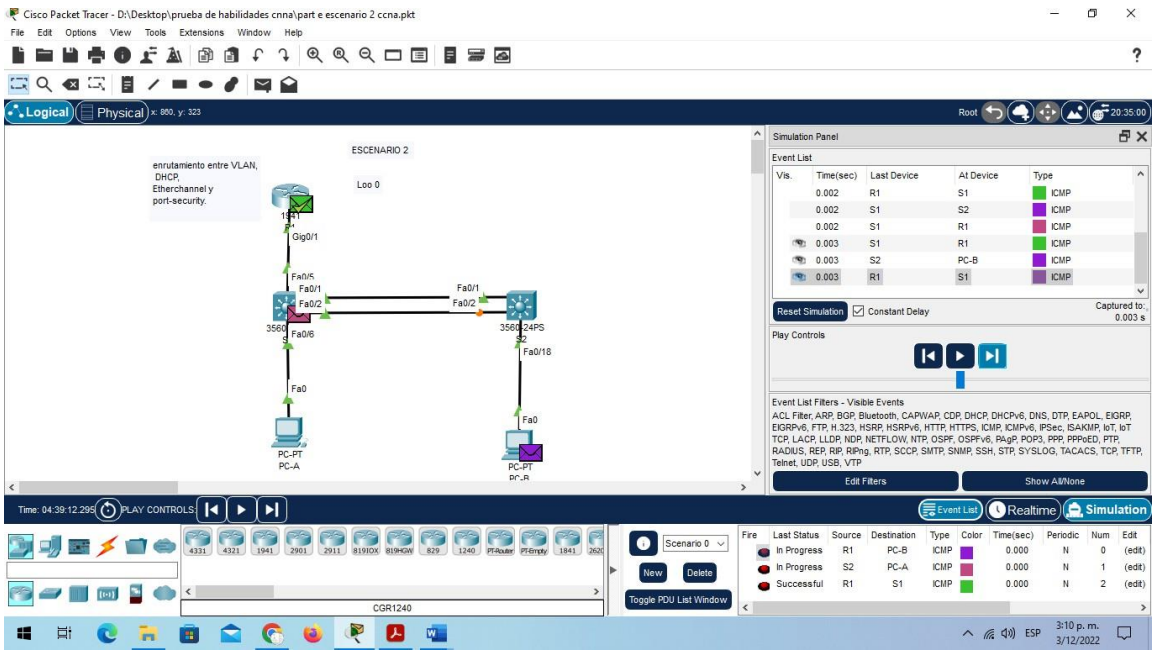


Fuente de autoría propia

En la figura 22, Se verifica la conectividad en de PCB a PCA, ip 10.12.8.2 con éxito, conectividad de PCA a Bucle 0, ip 209.165.201.1con éxito y la conectividad con switch S2, vlan 40, ipv6 2001:db8:acad:c::99 ha fallado,

Topología Final Funcionando

Figura 23 topología final de escenario 2



Fuente de autoría propia

CONCLUSIONES

En el escenario 1 la dirección de red es segmentada en dos sub redes, LAN 1 y LAN 2 con numero de host de 60 y 20 host respectivamente, el direccionamiento IPv4 en una red esta limitada por la mascara de sub red al usar solo una parte de la disposición de los host finales hace de este escenario una red escalable de buen rendimiento, siendo administrada de forma segura, con mayor velocidad de transmisión y menor itinerancia en el trafico de la red permitiendo el flujo de la información en todos os dispositivos que componen la red.

En el escenario 2 se presenta una problemática en una red que esta compuesta por Routers, Switchs y PC, en la configuración se crean subinterfaces, conectadas a las vlans, el enrutamiento IPv4 e IPv6 se obtiene una red mas estable y escalable, los dispositivos de la red se comunican según el protocolo Dual Stack.

El protocolo DHCP establece una configuración de red dinámica al reconocer un host y genera una dirección Ipv4 conectando a la red con mascara de subred y la puerta de enlace predeterminada, esto facilita la conexión a la red y es controlada por el Routers, separando una exclusión de direcciones con el propósito de asignarlas a puertos conectados por cableado estructurado.

La red de datos escenario 2 esta segmentada y permite un mayor control del direccionamiento de la red aprovechando la distribución de los hosts a la necesidad de cada una de las subinterfaces, cada vlan es independiente y el administrador de la red puede trasladar cada una de las estaciones de trabajo dentro de la LAN.

Para el desarrollo de la prueba de habilidades se aplicaron los conocimientos obtenidos en el curso de Diplomado de Profundización de CCNA al diseñar implementar y configurar los escenarios propuestos adquiriendo las habilidades y destrezas para la implementación de redes.

BIBLIOGRÁFIA

CISCO. 2022. Ocho pasos para configurar su switch de red. {En línea}. {12 de octubre de 2022} Disponible en https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/how-to-setup-network-switch.html

Diaz García, Brayan Styben; Ramos L. 2020. Rediseño de red local empresa Servicol Ltda. {En línea}. {11 de noviembre de 2022} Disponible en https://repository.ucc.edu.co/handle/20.500.12494/28255 pages=51-63

JIMENEZ Julio; DURAN D. Configuración de un Reuter básico con configuración profesional. Cisco TAC Engineer. {En línea}. {20 de octubre de 2022} Disponible en https://www.cisco.com/c/es_mx/support/docs/cloud-systems-management/configuration-professional/111999-basic-router-config-ccp-00.html

Muñoz Araque Robert Steven. 2020. Rediseño lógico de una red LAN a partir de la implementación de vlan, inter-vlan routing, dhcp, acl y portsecurity en un modelo jerárquico de red de tres capas cisco. {En línea}. {15 de octubre de 2020} Disponible en https://repository.ucc.edu.co/handle/20.500.12494/20575

Upna. Practica 2. Configuración de VLAN en conmutadores CISCO. {En línea}. {19 de octubre de 2020} Disponible en https://www.tlm.unavarra.es/~daniel/docencia/ftpr/ftpr19_20/practicas/practica2.pdf

ANEXOS

Anexos A

Enlace de descarga de los archivos de simulación de los escenarios

https://drive.google.com/drive/folders/10ybNM7oip8MLeeewRw2BdyzfcLDebtG1