INFORME PRUEBA DE HABILIDADES PRÁCTICAS

JEISSON DAVID PANTEVIS

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

INFORME PRUEBA DE HABILIDADES PRÁCTICAS

JEISSON DAVID PANTEVIS

Diplomado De Opción De Grado Presentado Para Optar El Título De INGENIERO DE SISTEMAS

DIRECTOR**:**
PAULITA FLOR

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

PITALITO - HUILA, 27 de noviembre de 2022

AGRADECIMIENTOS

Primero a Dios por brindarme la salud y fortaleza para afrontar todos estos retos, a mi familia, mi mamá y mi papá por animarme y siempre apoyarme para salir adelante con esta carrera y en todo lo que emprendo.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

RED: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.[1]

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local que no deberían intercambiar datos usando la red local.[3]

TRONCALES: Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.[5]

SWITCH: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.[2]

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.[2]

PAQUETE DE DATOS: En redes, un paquete es un pequeño segmento de un mensaje más grande. Los datos enviados a través de redes informáticas*, como Internet, se dividen en paquetes. Estos paquetes los vuelve a combinar el ordenador o el dispositivo que los recibe.[4]

COMANDO CLI: La interfaz de línea de comandos o interfaz de línea de órdenes (en inglés, command-line interface, CLI) es un tipo de interfaz de usuario de computadora que permite a los usuarios dar instrucciones a algún programa informático o al sistema operativo por medio de una línea de texto simple.[6]

---

1. LA ENCICLOPEDIA LIBRE, Wikipedia. Red de computadoras. Wikipedia [página web].
2. VELTE, Toby.Manual de cisco. (2008)
3. VELTE, Toby.Manual de cisco. (2008)
4. VELTE, Toby.Manual de cisco. (2008)
5. Wikipedia. Red Troncal [en línea]. Wikipedia, La enciclopedia libre, 2022 [página web].
6. REBOLLEDO, Miguel. Manual de uso Packet Tracer 5 (2011)

RESUMEN

El presente documento corresponde al trabajo final del curso de profundización de la prueba de habilidades prácticas de CISCO Packet Tracer, en este documento podremos encontrar la solución a los 2 escenarios propuestos a través de Packet Tracer y desarrollados en este, en donde se realizan conexiones, configuraciones, programación y pruebas entre los distintos dispositivos que se encuentran en la red.

Palabras clave: Redes, Protocolo, Packet Tracer, Simulación, Conexión configuración, programación pruebas, ping.

ABSTRACT

This document corresponds to the final work of the deepening course of the CISCO Packet Tracer practical skills test, in this document we can find the solution to the 2 scenarios proposed through Packet Tracer and developed in it, where connections are made, configurations, programming and tests between the different devices that are in the network.

Keywords: Networks, Protocol, Packet Tracer, Simulation, Connection configuration, test programming, ping.

INTRODUCCIÓN

Como sabemos hoy en día las redes se han convertido en una herramienta y en una necesidad para el desarrollo tanto personal como de empresas ya que ayudan a interconexión y el trabajo en conjunto. Una de las mejores ayudas de simulación y/o creación de redes es Cisco Packet Tracer porque es una herramienta de simulación de red interactiva. En el desarrollo de las actividades crearemos dos topologías o escenarios de red en la cual configuraremos dispositivos y los programaremos conforme las indicaciones de la guia.

En el escenario 1 configuraremos los dispositivos de una red pequeña en donde por medio de código CLI programaremos un router, un switch y equipos, también diseñaremos un esquema de direccionamiento IPv4 para las LAN propuestas, adicional a esto el router y el switch deben administrase de manera segura.

En el escenario 2 configuraremos los dispositivos de una red pequeña en donde debemos configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados, también configuraremos los switches en modo truncado usando VLAN, DHCP y port-security, adicional a esto el router y el switch deben administrase de manera segura.

DESARROLLO

Escenario 1

Tabla de direccionamiento IP Con CC terminada en 69

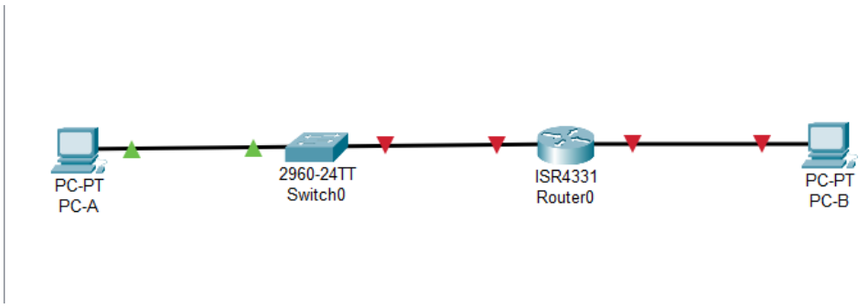
Dirección IP 172.69.3.0

En este primer ejercicio se solicita realizar las respectivas configuraciones de los diferentes dispositivos necesarios, para el diseño de una LAN red pequeña teniendo en cuenta que su direccionamiento debe ser basada en la versión IPv4, se debe realizar las configuraciones necesarias tanto en el router y switch revisando principalmente que nuestra red pueda administrarse de una forma segura y adecuada.

Parte 1: Construya la Red

En el simulador construya 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 1 Esquema de Red Escenario 1



Fuente: Autoría propia

Parte 2: Desarrolle el esquema de direccionamiento IP

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.

Cada estudiante tomará el direccionamiento 172.69.3.0 donde XY corresponde a losúltimos dos dígitos de su cédula. (1077874469)

Tabla de direccionamiento

Tabla 1 Tabla de direccionamiento IP

IP Address:	172.69.3.0	
Network Address:	172.69.3.0	
Usable Host IP Range:	172.69.3.1 - 172.69.3.126	
Broadcast Address:	172.69.3.127	
Total, Number of Hosts:	128	
Number of Usable Hosts:	126	
Subnet Mask:	255.255.255.128	
Wildcard Mask:	0.0.0.127	
Binary Subnet Mask:	11111111.11111111.11111111.10000000	
IP Class:	C	
CIDR Notation:	/25	
IP Type:	Public	
Network Address	Usable Host Range	Broadcast Address:
172.69.3.0	172.69.3.1 - 172.69.3.62	172.69.3.63
172.69.3.128	172.69.3.65 - 172.69.3.126	172.69.3.127

Fuente: Autoría Propia

Tabla 2 Requerimientos de la red

Ítem	Requerimiento
Dirección de Red	172.69.3.0 donde XY corresponde a los últimos dosdígitos de su cédula.
Requerimiento de host SubredLAN1	60 172.69.3.1 – 172.69.3.62 Broadcast 172.69.3.63
Requerimiento de host SubredLAN2	20 172.69.3.65 – 172.69.3.126 Broadcast 172.69.3.127
R1 G0/0/1	Última dirección de host de la subred LAN1 172.69.3.62
R1 G0/0/0	Última dirección de host de la subred LAN2 172.69.3.126
S1 SVI	Segunda dirección de host de la subred LAN1 172.69.3.2
PC-A	Décima dirección de host de la subred LAN1 172.69.3.10
PC-B	Décima dirección de host de la subred LAN2 172.69.3.75

Fuente: Diplomado de profundización cisco

Parte 3: Configure aspectos básicos

Los dispositivos de red (S1 y R1) se configuran mediante conexión de consola. Teniendo en cuanta sobre las temáticas aprendidas con diversos materiales y ayudad de que nos brindan para el desarrollo de la presente actividad se realiza las configuraciones a través del código CLI de consola.

Tabla 3 Configuración de Aspectos básicos de la red

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Ingresamos el Comando CLI al Router **Router enable** **Router # configure terminal** **Router(config)#no ip domain-lookup** **Router (config)# exit**
Nombre del router (R1)	Ingresamos el siguiente Código CLI para cambiar el nombre de Router a R1 **Router# configure terminal** **Router(config)#hostname R1** **R1(config)# exit**
Nombre de dominio	Para ingresar el nombre del dominio (ccna-sa.com) debemos ingresar el siguiente comando CLI: **R1#configure terminal** **R1(config)# ip domain-name ccna-sa.com** **R1(config)#exit**
Contraseña cifrada para el modo EXEC privilegiado (Ciscoenpass)	Para asignar la contraseña cifrada para el modo EXEC privilegiado (ciscoenpass) debemos ingresar el siguiente comando CLI en R1: **R1#configure terminal** **R1(config)#enable secret ciscoenpass** **R1(config)#exit**
Contraseña de acceso a la consola (Ciscoconpass)	En este paso para asignar la contraseña para el acceso a la consola debemos ingresar el siguiente comando CLI: **R1#configure terminal** **R1(config)#line console 0** **R1(config-line)#password ciscoconpass** **R1(config-line)#login** **R1(config-line)#exit** **R1(config)#**
Establecer la longitud mínima para las contraseñas de 10 caracteres	Para ingresar una longitud mínima de contraseña de 10 caracteres debemos ingresar el siguiente código CLI: **R1# configure terminal** **R1(config)#security password min-length 10** **R1(config)# exit**

Crear un usuario administrativo en labase de datos local	Para configurar el Nombre de usuario: admin y Contraseña: admin1pass para el ingreso a consola de R1 debemos ingresar el siguiente código CLI: **R1# configure terminal** **R1(config)#username admin password admin1pass** **R1(config)#line console 0** **R1(config-line)#login local** **R1(config-line)#exit** **R1(config)#exit**
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Para configurar el inicio de sesión en las líneas VTY para que se almacene en la base de datos local usamos el siguiente comando CLI: **R1#configure terminal** **R1(config)#line vty 0 4** **R1(config-line)#login local** **R1(config-line)#exit** **R1(config)#exit** **R1#**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Para configurar las líneas VTY y acepten únicamente conexiones SSH, la línea CLI es muy parecida al comando anterior siendo así: **R1#configure terminal** **R1(config)#line vty 0 5** **R1(config-line)#transport input ssh** **R1(config-line)#login local** **R1(config-line)#exit** **R1(config)#exit** **R1#**
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas de texto debemos ingresar el siguiente Código CLI: **R1#configure terminal** **R1(config)#service password-encryption** **R1(config)#exit**
Configurar un banner MOTD	Para crear un Banner MOTD en nuestro router debemos ingresar en la consola el siguiente código CLI: **R1#configure terminal** **R1(config)#banner motd #Jeisson David Pantevis Programa: Diplomado de Profundización Cisco Codigo del Curso: 203092_19#**

	R1(config)#exit **R1#**
Configuración de interface G0/0/0	Ahora vamos empezar a configurar la Interface G0/0/0, en donde configuraremos la dirección IP, para esto usaremos el siguiente código CLI: **R1#configure terminal** **R1(config)# int g0/0/0** **R1(config-if)#ip add 172.69.3.86 255.255.255.128** **R1(config-if)#no shut** **R1(config-if)#exit** **R1(config)#exit**
Configuración de interface G0/0/1	Ahora vamos a empezar a configurar la Interface G0/0/1, en donde configuraremos la dirección IP, para esto usaremos el siguiente código CLI: **R1#configure terminal** **R1(config)# int g0/0/1** **R1(config-if)#ip add 172.69.3.62 255.255.255.128** **R1(config-if)#no shut** **R1(config-if)#exit** **R1(config)#exit**
Generar una clave de cifrado RSA	Para generar una clave de Cifrado RSA en nuestro Router debemos ingresar este comando CLI: **R1#configure terminal** **R1(config)# crypto key generate rsa** **The name for the keys will be: R1.ccna-sa.com** **Chose the size of the key modulus in the range of 360 to 2048 for your** **General Purposr Keys. Choosing a key modulus greater than 512 may take a few minutes.** **How many bits in the modulus [512]: 1024** **% Generating 1024 bit RSA keys, keys will be non-exportable…[OK]** **R1(config)#exit**

Fuente: Diplomado de profundización Cisco

Las tareas de configuración de S1 incluyen lo siguiente

Tabla 4 configuración de R1 y S1 **Tarea**	**Especificación**
Desactivar la búsqueda DNS	Para desactivar la búsqueda DNS en el switch usamos el siguiente código CLI: **Switch# configure terminal** **Switch(config)#no ip domain-lookup** **Switch(config)#exit**
Nombre del switch	Para asignar el nombre al switch debemos ingresar en la consola el siguiente código CLI: **Switch# configure terminal** **Switch(config)#hostname S1** **S1(config)#exit**
Nombre de dominio	Para configurar el nombre del dominio en el switch debemos usar este código en el CLI: **S1#configure terminal** **S1(config)# ip domain-name ccna-sa.com** **S1(config)#exit**
Contraseña cifrada para el modo EXEC privilegiado(ciscoenpass)	Para asignar la contraseña cifrada para el modo EXEC privilegiado (ciscoenpass) debemos ingresar el siguiente comando CLI en S1: **S1#configure terminal** **S1(config)#enable secret ciscoenpass** **S1(config)#exit**
Contraseña de acceso a la consola (ciscoconpass)	En este paso para asignar la contraseña para el acceso a la consola debemos ingresar el siguiente comando CLI: **S1#configure terminal** **S1(config)#line console 0** **S1(config-line)#password ciscoconpass** **S1(config-line)#login** **S1(config-line)#exit** **S1(config)#**
Apagar todos los puertos sin usar	Para desactivar los puertos que van quedar sin usar hay dos maneras de hacerlo por código CLI o por la configuración del switch, por comando CLI seria así: **S1#configure terminal** **S1(config)# int range F0/1-4** **S1(config-if-range) shutdown** **S1(config-if-range) exit** **S1(config)# int range F0/7-24** **S1(config-if-range) shutdown**

	S1(config-if-range) exit **S1(config)# int range G0/1-2** **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**	Para este paso vamos a configurar un usuario administrativo para que tenga acceso al switch para esto usamos el siguiente código CLI: **S1# configure terminal** **S1(config)#username admin password admin1pass** **S1(config)#line console 0** **S1(config-line)#login local** **S1(config-line)#exit** **S1(config)#exit**
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Para configurar el inicio de sesión en las líneas VTY para que se almacene en la base de datos local usamos el siguiente comando CLI: **S1#configure terminal** **S1(config)#line vty 0 4** **S1(config-line)#login local** **S1(config-line)#exit** **S1(config)#exit** **S1#**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Para configurar las líneas VTY y acepten únicamente conexiones SSH, la línea CLI es muy parecida al comando anterior siendo así: **S1#configure terminal** **S1(config)#line vty 0 5** **S1(config-line)#transport input ssh** **S1(config-line)#login local** **S1(config-line)#exit** **S1(config)#exit** **S1#**
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas de texto debemos ingresar el siguiente código CLI: **S1#configure terminal** **S1(config)#service password-encryption** **S1(config)#exit**
Configurar un banner MOTD	Para crear un Banner MOTD en nuestro Switch debemos ingresar en la consola el siguiente código CLI: **S1#configure terminal**

	S1(config)#banner motd #Jeisson David Pantevis Programa: Diplomado de Profundización Cisco Código del Curso: 203092_19# **S1(config)#exit** **S1#**
Generar una clave de cifrado RSA	Para generar una clave de Cifrado RSA en nuestro Switch debemos ingresar este comando CLI: **S1#configure terminal** **S1(config)# crypto key generate rsa** **The name for the keys will be: S1.ccna-sa.com** **Chose the size of the key modulus in the range of 360 to 2048 for your** **General Purposr Keys. Choosing a key modulus greater than 512 may take a few minutes.** **How many bits in the modulus [512]: 1024** **% Generating 1024 bit RSA keys, keys will be non-exportable…[OK]** **S1(config)#exit**
Configure la interfaz de administración (SVI) en VLAN1	Establecer la dirección IPv4 en el SVI en VLAN 1 usando este código CLI: **S1#configure terminal** **S1(config)#int vlan1** **S1(config-if)#ip add 172.69.3.2 255.255.255.128** **S1(config-if)#no shut** **S1(config-if)#exit** **S1(config)#exit** **S1#**

Fuente: Diplomado de profundización Cisco

Configuración de los equipos PC-A y PC-B

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

Tabla 5 configuración de equipos PC-A

Configuración de red de PC-A	
Descripción	PC de escritorio PC-A
Dirección física	0001.97D8.9D7E
Dirección IPv4	172.69.3.10
Máscara de subred	255.255.255.128

Puerta de enlace IPv4 predeterminada	172.69.3.2

Fuente: Diplomado de profundización Cisco

Tabla 6 configuración de equipos PC-B

Configuración de red de PC-B	
Descripción	PC de escritorio ubicado en la segunda Subred PC-B
Dirección física	0060.5CB6.2193
Dirección IPv4	172.69.3.75
Máscara de subred	255.255.255.128
Puerta de enlace IPv4 predeterminada	172.69.3.126

Fuente: Diplomado de profundización Cisco

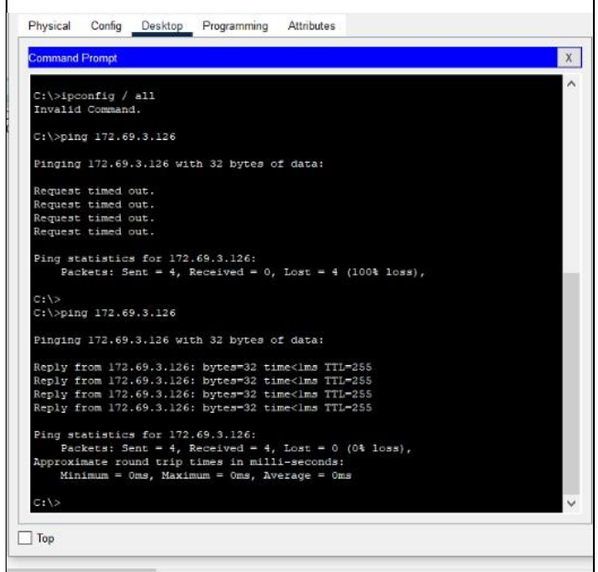
Parte 4: Probar y verificar la conectividad de extremo a extremo

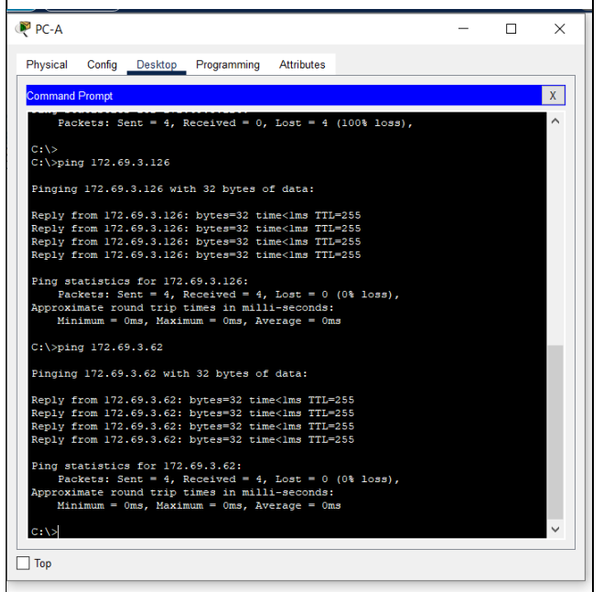
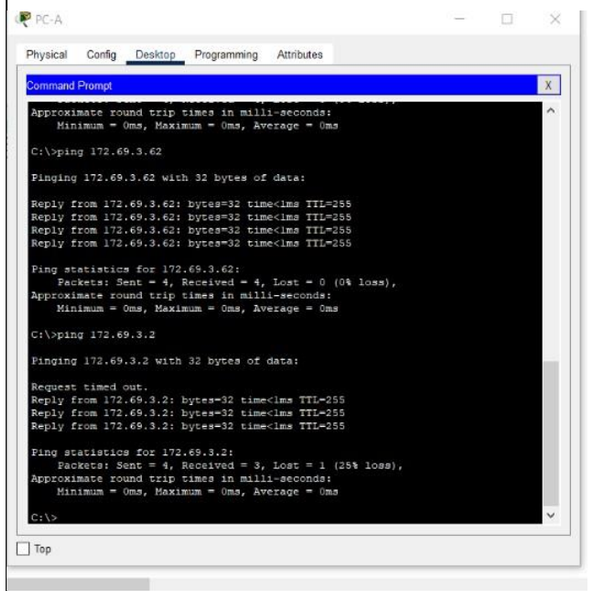
Utilice el comando ping para probar la conectividad entre todos los dispositivos de red.

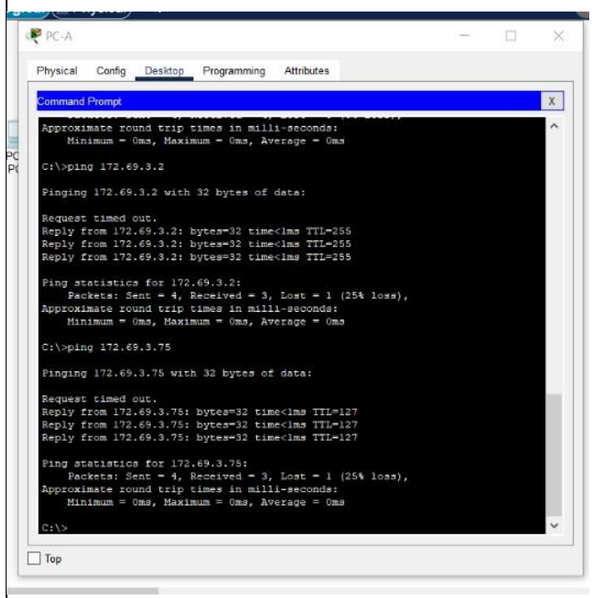
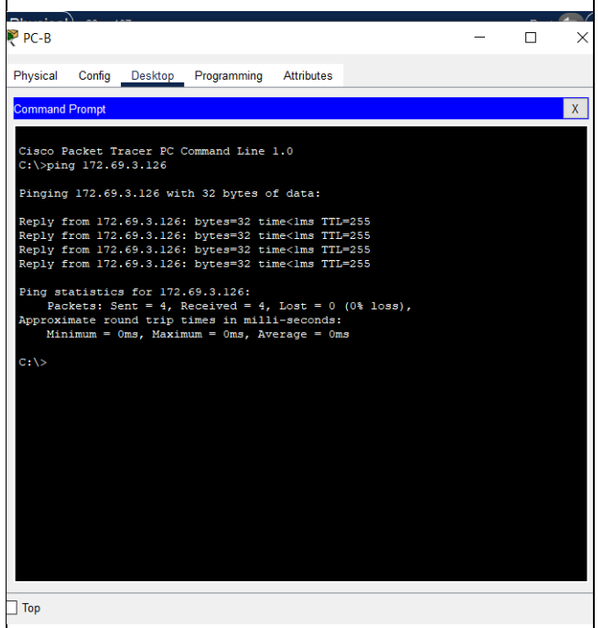
Nota: Si los pings a los servidores fallan, deshabilite temporalmente el firewall del equipo yvuelva a realizar la verificación.

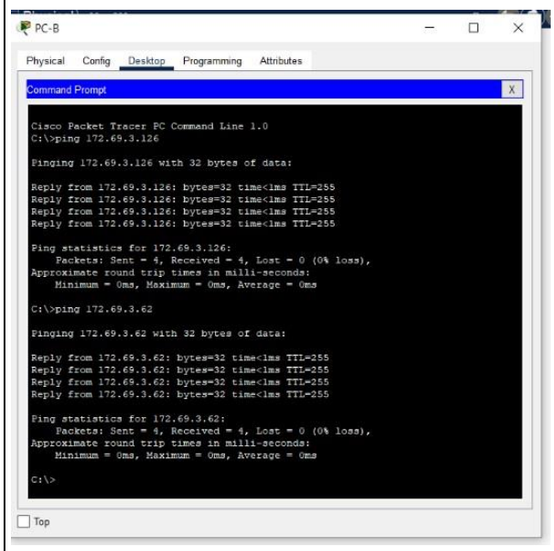
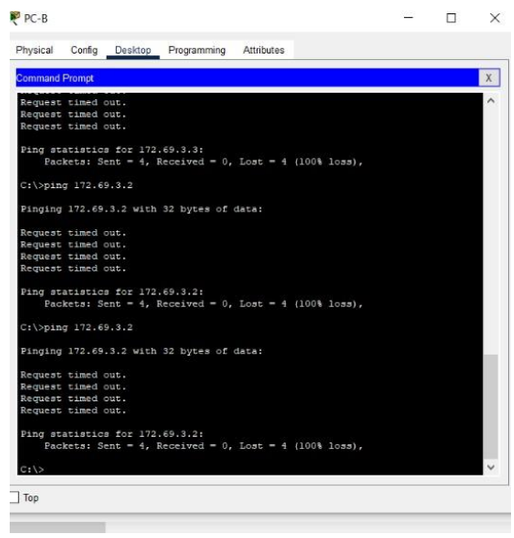
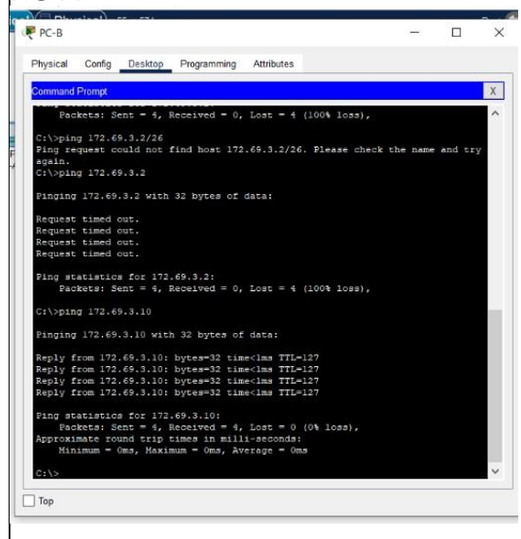
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivode red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 7 Prueba de Ping PC-A y PC-B

Desde	**Destino**	**Dirección IP**	**Resultados de ping**
PC-A	R1 G0/0/0	172.69.3.126	Figura 2 Prueba Ping desde PC-A a R1 G0/0/0  Fuente: Autoría Propia

	R1 G0/0/1	172.69.3.62	Figura 3 Prueba Ping desde PC-A a R1 G0/0/1  Fuente: Autoría Propia
	S1 VLAN 1	172.69.3.2	Figura 4 Prueba Ping desde PC-A a S1 VLAN 1  Fuente: Autoría Propia

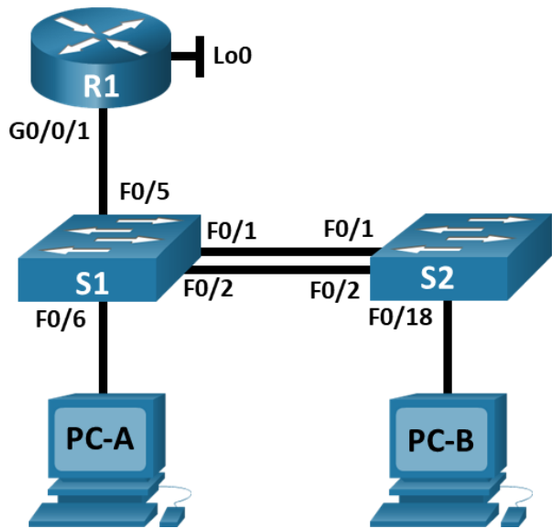
	PC-B	172.69.3.75	Figura 5 Prueba Ping desde PC-A a PC-B  Fuente: Autoría Propia
PC-B	R1 G0/0/0	172.69.3.126	Figura 6 Prueba Ping desde PC-B a R1 G0/0/0  Fuente: Autoría Propia

	R1 G0/0/1	172.69.3.62	Figura 7 Prueba Ping desde PC-B a R1 G0/0/1  Fuente: Autoría Propia
	S1 VLAN1	172.69.3.2	Figura 8 Prueba Ping desde PC-B a S1 VLAN 1  Fuente: Autoría Propia
	PC-A	172.69.3.10	Figura 9 Prueba Ping desde PC-B a PC-A  Fuente: Autoría Propia

Escenario 2

Topología

Figura 10 Topología Escenario 2



Fuente: Diplomado de profundización cisco

Tabla de asignación de direcciones

NOTA: Tenga en cuenta que para el direccionamiento donde aparezca XY deberáreemplazarlos por los últimos dos dígitos de su número de identificación.

Tabla 8 Tabla de direcciones escenario 2

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.69.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.69.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.69.8.97 /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	10.69.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.69.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde

PC-A NIC	Dirección DHCP paraIPv4	DHCP para puerta de enlace 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

Fuente: Diplomado de profundización cisco

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.

Para el Router (R1)

Router>enable

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]

[OK]

Erase of nvram: complete

Router#

Router#reload

Proceed with reload? [confirm]

Para los Switch (S1 y S2)

Switch>enable

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]

[OK]

Erase of nvram: complete

Switch#

Switch#reload

Proceed with reload? [confirm]

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

Con el Código CLI

#sdm prefer dual-ipv4-and-ipv6 default

#exit

#reload

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9 configuración de Router 1 con los parámetros dados y sus respectivas evidencias.

Tarea	Especificación
Desactivar la búsqueda DNS	Para desactivar la búsqueda de DNS en nuestro router debemos ingresar este comando CLI: **Router>enable** **Router#configure terminal** **Router(config)#no ip domain-lookup** **Router(config)#exit**
Nombre del router	Ahora para cambiar el nombre del router debemos usar el siguiente código CLI: **Router>enable** **Router#configure terminal** **Router(config)#hostname R1** **R1(config)#exit**
Nombre de dominio	Para agregar el nombre del dominio general a R1 debemos ingresar el siguiente comando CLI: **R1>enable** **R1#configure terminal** **R1(config)#ip domain-name ccna-sa.com** **R1(config)#exit**
Contraseña cifrada para el modo EXECprivilegiado	Aquí configuraremos la contraseña para modo EXEC privilegiado y el acceso a la consola, lo hacemos con el siguiente comando CLI: **R1>enable** **R1#configure terminal** **R1(config)#enable secret class** **R1(config)#line console 0** **R1(config-line)#password cisco** **R1(config-line)#login** **R1(config-line)#exit** **R1(config)#exit**
Contraseña de acceso a la consola	
Establecer la longitud mínima para las contraseñas	En este punto vamos a configurar la longitud mínima para las contraseñas en este caso 10, para esto usamos el siguiente comando CLI: **R1>enable** **R1#configure terminal** **R1(config)#security passwords min-length 10** **R1(config)#exit**
Crear un usuario administrativo en labase de datos local Nombre de usuario: admin Password: admin1pass	Ahora crearemos un usuario que se alojará en la base de datos del R1, para esto usaremos este código CLI: **R1>enable** **R1#configure terminal** **R1(config)#username admin privilege 15 secret admin1pass** **R1(config)#exit**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local Configurar VTY solo aceptando SSH	Aquí configuraremos en las líneas VTY el inicio de sesión junto con la configuración de SSH, para esto usaremos el siguiente código CLI: **R1>enable** **R1#configure terminal** **R1(config)#line vty 0 4** **R1(config-line)#login local** **R1(config-line)#exit** **R1(config)#line vty 0 15** **R1(config-line)#transport input ssh** **R1(config-line)#login local** **R1(config-line)#exit** **R1(config)#exit**
Cifrar las contraseñas de texto no cifrado	Para cifrar contraseñas de texto no cifrado debemos introducir el siguiente código CLI: **R1>enable** **R1#configure terminal** **R1(config)#service password-encryption** **R1(config)#exit**
Configure un MOTD Banner	Para crear un Banner MOTD en nuestro router debemos ingresar en la consola el siguiente código CLI: **R1#configure terminal** **R1(config)#banner motd #Jeisson David Pantevis Programa: Diplomado de Profundización Cisco Código del Curso: 203092_19#** **R1(config)#exit** **R1#**
Habilitar el routing IPv6	Para habilitar el direccionamiento IPv6 en el router debemos introducir el siguiente código CLI: **R1>enable** **R1#configure terminal** **R1(config)#ipv6 unicast-routing** **R1(config)#exit**
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6como fe80::1 Establece la dirección IPv6.Activar la interfaz. Configuración VLAN 20 Docentes **R1(config)#int g0/0/1.20** **R1(config-subif)#encapsulation dot1q 20** **R1(config-subif)#description LAN to VLAN 20** **R1(config-subif)#ip add 10.69.8.1 255.255.255.192** **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)#int g0/0/1.30** **R1(config-subif)#encapsulation dot1q 30**

	R1(config-subif)#description LAN to VLAN 30 **R1(config-subif)#ip add 10.69.8.65 255.255.255.224** **R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64** **R1(config-subif)#ipv6 add fe80::1 link-local** **R1(config-subif)#no shutdown** **R1(config-subif)#exit** **R1(config)#interface gi0/0/1.40** **R1(config-subif)#encapsulation dot1q 40** **R1(config-subif)#description LAN to VLAN 40** **R1(config-subif)#ip add 10.69.8.97 255.255.255.248** **R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64** **R1(config-subif)#ipv6 add fe80::1 link-local** **R1(config-subif)#no shutdown** **R1(config-subif)#exit** **R1(config)#interface gi0/0/1.56** **R1(config-subif)#encapsulation dot1q 56** **R1(config)#interface gi0/0/1** **R1(config-if)#no shutdown** **R1(config-subif)#exit**
Configure el Loopback0 interface	Aquí configuraremos el loopback0 interface de el R1, para ello usamos el siguiente código CLI: **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)#no shut** **R1(config-if)#ipv6 add 2001:db8:acad:209::1/64** **R1(config-if)#ipv6 add FE80::1 link-local** **R1(config-if)#no shut** **R1(config-if)#exit** **R1(config)#exit**
Generar una clave de cifrado RSA	Para configurar el cifrado RSA de R1 debemos ingresar este código CLI: **R1#configure terminal** **R1(config)# crypto key generate rsa** **The name for the keys will be: R1.ccna-sa.com** **Chose the size of the key modulus in the range of 360 to 2048 for your** **General Purposr Keys. Choosing a key modulus greater than 512 may take a few minutes.** **How many bits in the modulus [512]: 1024** **% Generating 1024 bit RSA keys, keys will be non-exportable…[OK]** **R1(config)#exit**

Fuente: Diplomado de profundización cisco

Paso 3: Configure S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 10 configuración y programación de S1 y S2 según parámetros dados

Tarea	Especificación
Desactivar la búsqueda DNS.	Empezamos configurando los dos switch, empezamos con la desactivación de la búsqueda del DNS, para ello ingresamos el siguiente código CLI en cada uno de lo switch: **Switch>enable** **Switch #configure terminal** **Switch (config)#no ip domain-lookup** **Switch (config)# hostname S1** **S1 (config)#exit** **Switch>enable** **Switch #configure terminal** **Switch (config)#no ip domain-lookup** **Switch (config)# hostname S2** **S2 (config)#exit**
Nombre del switch	
Nombre de dominio	Ahora configuramos el nombre de dominio en los dos switch, para esto usamos el siguiente código CLI: **S1>enable** **S1#configure terminal** **S1(config)#ip domain-name ccna-sa.com** **S1 (config)#exit** **S2>enable** **S2#configure terminal** **S2(config)#ip domain-name ccna-sa.com** **S2 (config)#exit**
Contraseña cifrada para el modo EXEC privilegiado **class**	En esta parte configuraremos tanto la contraseña para el modo EXEC privilegiado y la contraseña de acceso a la consola, para lograr hacer esto vamos a introducir el siguiente código CLI en cada uno de los switch. **S1>enable** **S1#configure terminal** **S1(config)#enable secret class** **S1(config)#line console 0** **S1(config-line)#password cisco** **S1(config-line)#login** **S1(config-line)#exit** **S1(config)#exit** **S2>enable** **S2#configure terminal** **S2(config)#enable secret class** **S2(config)#line console 0** **S2(config-line)#password cisco** **S2(config-line)#login** **S2(config-line)#exit** **S2(config)#exit**
Contraseña de acceso a la consola **cisco**	

Crear un usuario administrativo en la base dedatos local **Nombre de usuario: admin** **Password: admin1pass**	Ahora crearemos un usuario para que pueda acceder a la consola de nuestros switches para esto usaremos el siguiente código CLI: **S1>enable** **S1#configure terminal** **S1(config)#username admin privilege 15 secret admin1pass** **S1(config)#exit** **S2>enable** **S2#configure terminal** **S2(config)#username admin privilege 15 secret admin1pass** **S2(config)#exit**
Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local	Para esta parte debemos configurar el inicio de sesión de las líneas VTY y las conexiones SSH en nuestros switches para ellos usamos el siguiente comando CLI: **S1>enable** **S1#configure terminal** **S1(config)#line vty 0 15** **S1(config-line)#login local** **S1(config)#exit** **S1(config)#line vty 0 15** **S1(config-line)#transport input ssh** **S1(config-line)#login local** **S1(config)#exit** **S2>enable** **S2#configure terminal** **S2(config)#line vty 0 15** **S2(config-line)#login local** **S2(config)#exit** **S2(config)#line vty 0 15** **S2(config-line)#transport input ssh** **S2(config-line)#login local** **S2(config)#exit**
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	Para cifrar las contraseñas de texto en nuestros switches debemos ingresar el siguiente código CLI: **S1>enable** **S1#configure terminal** **S1(config)#service password-encryption** **S1(config)#exit** **S2>enable** **S2#configure terminal** **S2(config)#service password-encryption** **S2(config)#exit**
Configurar un MOTD Banner, Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.	Para crear un Banner MOTD en nuestros switches debemos ingresar en la consola el siguiente código CLI: **S1#configure terminal** **S1(config)#banner motd #Jeisson David Pantevis Programa: Diplomado de Profundización Cisco Código del Curso:**

	203092_19# **S1(config)#exit** **S1#** **S2#configure terminal** **S2(config)#banner motd #Jeisson David Pantevis Programa: Diplomado de Profundización Cisco Código del Curso: 203092_19#** **S2(config)#exit** **S2#**
Generar una clave de cifrado RSA	Para generar una clave de cifrado RSA en nuestros switches debemos ingresar este comando CLI: **S1>enable** **S1#configure terminal** **S1(config)#crypto key generate rsa** **S1(config)#exit** **S2>enable** **S2#configure terminal** **S2(config)#crypto key generate rsa** **S2(config)#exit**
Configurar la interfaz de administración (SVI)	Vamos a configurar el interfaz de administración SVI en los dos switches usando este comando CLI: **S1(config)#int vlan 40** **S1(config-if)#ip add 10.69.8.98 255.255.255.248** **S1(config-if)#ipv6 add 2001:db8:acad:c::98/64** **S1(config-if)#ipv6 add fe80::98 link-local** **S1(config-if)#no shutdown** **SI(config-if)# exit** **S2(config)#int vlan 40** **S2(config-if)#ip add 10.69.8.99 255.255.255.248** **S2(config-if)#ipv6 add 2001:db8:acad:c::99/64** **S2(config-if)#ipv6 add fe80::99 link-local** **S2(config-if)#no shutdown** **S2(config-if)#exit**
Configuración del gateway predeterminado	Aquí configuremos la puerta de enlace predeterminada como 10.69.8.97 para IPv4 en los switches, usando este CLI: **S1(config)#ip default-gateway 10.69.8.97** **S1(config)#do write** **SI(config-if)# exit** **S2(config)#ip default-gateway 10.69.8.97** **S2(config)#do write** **S2(config-if)# exit**

Fuente: Diplomado de profundización cisco

Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Tarea	Especificación
Crear VLAN **VLAN 20, nombre Docentes** **VLAN 30, nombre Estudiantes** **VLAN 40, nombre Invitados** **VLAN 50, nombre Usuarios** **VLAN 56, nombre Native**	En esta parte crearemos las VLAN's correspondientes con sus respectivos nombres y tamaño correspondiente, para crear estas VLAN's debemos realizar este código CLI: **S1>enable** **S1#configure terminal** **S1(config)#vlan 20** **S1(config-vlan)#name Docentes** **S1(config-vlan)#exit** **S1(config)#vlan 30** **S1(config-vlan)#name Estudiantes** **S1(config-vlan)#exit** **S1(config)#vlan 40** **S1(config-vlan)#name Invitados** **S1(config-vlan)#exit** **S1(config)#vlan 50** **S1(config-vlan)#name Usuarios** **S1(config-vlan)#exit** **S1(config)#vlan 56** **S1(config-vlan)#name Native** **S1(config-vlan)#exit**
Crear troncos 802.1Q que utilicen la VLAN 6nativa	Aquí habilitaremos las troncales para las Interfaces F0/1, F0/2 y F0/5, para realizar esto existen 2 métodos por la configuración del switch o por comando CLI; en este caso lo vamos a hacer por comando CLI: **S1#configure terminal** **S1(config)#int f0/1** **S1(config-if)#switchport trunk encapsulation dot1q** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 56** **S1(config-if)#switchport trunk allowed vlan 20,30,40,56** **S1(config-if)#exit** **S1(config)#int f0/2** **S1(config-if)#switchport trunk encapsulation dot1q** **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 56** **S1(config-if-range)#switchport trunk allowed vlan 20,30,40,56** **S1(config-if)#exit** **S1(config)#int f0/5**

	S1(config-if)#switchport trunk encapsulation dot1q **S1(config-if)#switchport mode trunk** **S1(config-if)#switchport trunk native vlan 56** **S1(config-if)#exit**
Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	Aquí vamos a usar el protocolo LACP para la negociación, para ello ingresaremos el siguiente código CLI: **S1(config)#int range f0/1-2** **S1(config-if-range)#channel-group 1 mode active** **S1(config-if-range)#channel-protocol lacp** **S1(config-if-range)#exit** **S1(config)#interface port-channel 1** **S1(config-if)#switchport trunk encapsulation dot1q** **S1(config-if)#switchport mode trunk** **S1(config-if)#exit** **S1(config)#switchport trunk native vlan 56**
Configurar el puerto de acceso de host paraVLAN 20	Ahora vamos a configurar la Interface F0/6 con VLAN 20, para configurarla de manera correcta debemos ingresar el siguiente código CLI: **S1(config)#int f0/6** **S1(config-if)#switchport mode access** **S1(config-if)#switchport access vlan 20** **S1(config-if)#no shutdown** **S1(config-if)#exit**
Configurar la seguridad del puerto en lospuertos de acceso permitir 4 direcciones MAC	Para configurar esta opción vamos a agregar una seguridad para solo permitir 4 direcciones MAC en nuestro puerto. **S1(config)#interface fa0/6** **S1(config-if)#switchport port-security** **S1(config-if)#switchport port-security maximum 3** **S1(config-if)#exit**
Proteja todas las interfaces no utilizadas	Vamos a asignar a VLAN 50, establecer en modode acceso, agregar una descripción y apagar **S1(config)#int range f0/3-4, f0/7-24, g0/1-2** **S1(config-if-range)#switchport mode access** **S1(config-if-range)#switchport access vlan 50** **S1(config-if-range)#description puertos sin utilizar** **S1(config-if-range)#shutdown**

Fuente: Diplomado de profundización cisco

Paso 5: Configure el S2.

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

Tabla 12 configuración de S2 según parámetros Dados

Tarea	Especificación
Crear VLAN **VLAN 20, nombre Docentes** **VLAN 30, nombre Estudiantes** **VLAN 40, nombre Invitados** **VLAN 50, nombre Usuarios** **VLAN 56, nombre Native**	En esta parte crearemos las VLAN's correspondientes con sus respectivos nombres y tamaño correspondiente, para crear estas VLAN's debemos realizar este código CLI: **S2>enable** **S2#configure terminal** **S2(config)#vlan 20** **S2(config-vlan)#name Docentes** **S2(config-vlan)#exit** **S2(config)#vlan 30** **S2(config-vlan)#name Estudiantes** **S2(config-vlan)#exit** **S2(config)#vlan 40** **S2(config-vlan)#name Invitados** **S2(config-vlan)#exit** **S2(config)#vlan 50** **S2(config-vlan)#name Usuarios** **S2(config-vlan)#exit** **S2(config)#vlan 56** **S2(config-vlan)#name Native** **S2(config-vlan)#exit**
Crear troncos 802.1Q que utilicen la VLAN 6nativa	Aquí habilitaremos las troncales para las Interfaces F0/1, F0/2 para realizar esto existen 2 métodos por la configuración del switch o por comando CLI; en este caso lo vamos a hacer por comando CLI: **S2(config)#int range f0/1-2** **S2(config-if-range)#switchport trunk encapsulation dot1q** **S2(config-if-range)#switchport mode trunk native vlan 56** **S2(config-if-range)#switchport trunk allowed vlan 20,30,40,56** **S2(config-if-range)# exit** **S2(config)#**
Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2	Aquí vamos a usar el protocolo LACP para la negociación en los puertos F0/1-2, para esto ingresaremos el siguiente comando CLI: **S2(config)#interface port-channel 2** **S2(config-if)#switchport trunk encapsulation dot1q** **S2(config-if)#switchport mode**

	trunk **S2(config-if)#switchport trunk native vlan 56** **S2(config-if)#exit** **S2(config)#interface range fa0/1-2** **channel-group 2 mode passive** **S2(config-if-range)#no shutdown** **S2(config-if-range)#channel-protocol lacp** **S2(config-if-range)#exit** **S2(config)#interface port-channel 2** **S2(config-if)#switchport trunk encapsulation dot1q** **S2(config-if)#switchport mode trunk** **S2(config-if)#switchport trunk native vlan 56** **S2(config-if)#exit** **S2(config)#interface range fa0/1-2** **channel-group 2 mode passive** **S2(config-if-range)#no shutdown** **S2(config-if-range)#exit**
Configurar el puerto de acceso del host para la VLAN30	Vamos a configurar la Interfaz F0/18 con acceso al host VLAN 30 para esto ingresaremos este comando CLI: **S2(config)#int f0/18** **S2(config-if)#switchport mode access** **S2(config-if)#switchport access vlan 30** **S2(config-if)#exit**
Configure port-security en los access ports	Esta configuración solo se permite 4 MAC address en el puerto, ahora vamos a configurarlo usando el siguiente código CLI: **S2(config)#int f0/18** **S2(config-if)#switchport port-security** **S2(config-if)#switchport port-security maximum 4**
Asegure todas las interfaces no utilizadas.	En esta parte apagaremos todos los puertos que están sin usar, para ello ingresaremos el siguiente código CLI: **S2(config)#int range f0/3-17, f0/19-24, g0/1-2** **S2(config-if-range)#switchport mode access** **S2(config-if-range)#switchport access vlan 50** **S2(config-if-range)#description Puertos no utilizados** **S2(config-if-range)#shutdown**

Fuente: Diplomado de profundización cisco

Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 configuración del Soporte de Host en R1

Tarea	Especificación
Configure Default Routing	Para configurar el router y dejarlo en default debemos ingresar el siguiente código CLI: **R1>enable** **R1#configure terminal** **R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0** **R1(config)# ipv6 route ::/0 loopback 0** **R1(config)#exit**
Configurar IPv4 DHCP paraVLAN 20	Aquí vamos a crear un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net yespecifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada **R1>enable** **R1#configure terminal** **R1(config)#service dhcp** **R1(config)#ip dhcp pool DHCP_vlan2** **R1(dhcp-config)#ip dhcp excluded-address 10.69.8.2 10.69.8.52** **R1(dhcp-config)# network 10.69.8.0 255.255.255.192** **R1(dhcp-config)#default-router 10.69.8.1** **R1(dhcp-config)#domain-name unad-ccna-sa.net** **R1(dhcp-config)# exit**
Configurar DHCP IPv4 paraVLAN 30	Ahora crearemos un grupo DHCP para VLAN 3, compuesto por lasúltimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net yespecifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada **R1(config)#service dhcp** **R1(config)#ip dhcp pool DHCP_vlan3** **R1(dhcp-config)#ip dhcp excluded-address 10.69.8.65 10.69.8.84** **R1(dhcp-config)# network 10.69.8.64 255.255.255.224** **R1(dhcp-config)#default-router 10.69.8.65** **R1(dhcp-config)#domain-name unad-ccna-sa.net** **R1(dhcp-config)# exit**

Fuente: Diplomado de profundización cisco

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 14 configuración de Servidores para PCA Y PCB

Configuración de red de PC-A	
Descripción	ccna-sa.com
Dirección física	0060.3EA7.B1CC
Configuración de red de PC-A	
Dirección IP	IPV4:10.69.8.53 IPV6: 2001:db8:acad:a: :50 /64
Máscara de subred	255.255.255.192
Gateway predeterminado	10.69.8.1
Gateway predeterminado IPv6	fe80::1

Fuente: Diplomado de profundización cisco

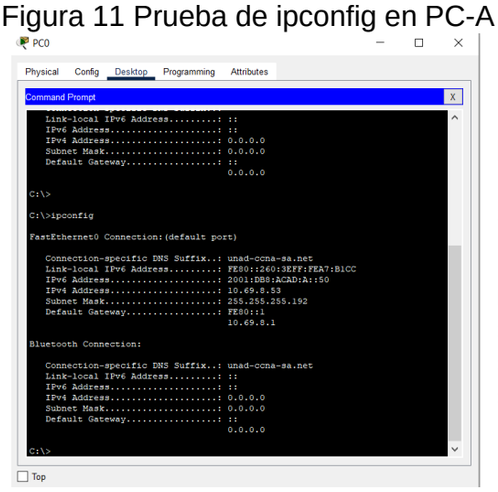
Tabla 15 configuración de Servidores para PCA Y PCB

Configuración de red de PC-B	
Descripción	ccna-sa.com
Dirección física	0001.64C3.A456
Dirección IP	IPV4:10.69.8.85 IPV6: 2001:db8:acad:b: :50 /64
Máscara de subred	255.255.255.224
Gateway predeterminado	10.69.8.65
Gateway predeterminado IPv6	fe80::1

Fuente: Diplomado de profundización cisco

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

Figura 11 Prueba de ipconfig en PC-A

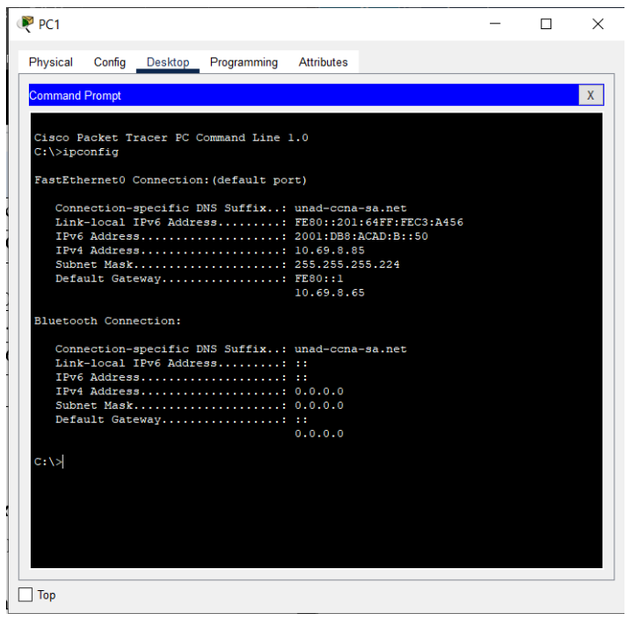


Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

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

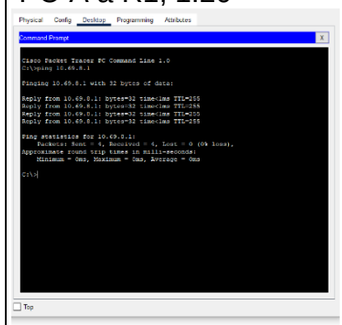
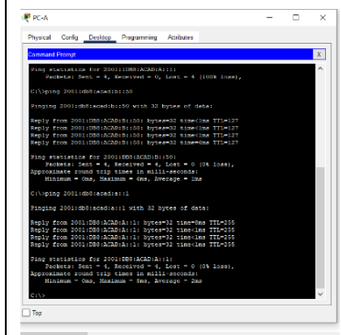
Fuente: Autoría Propia

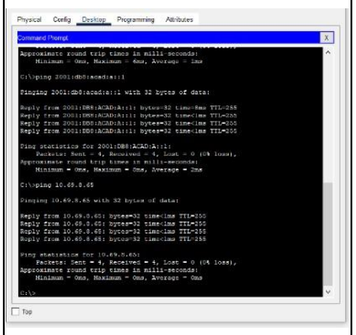
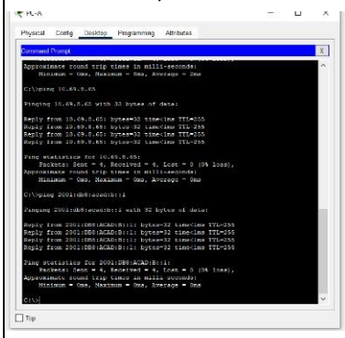
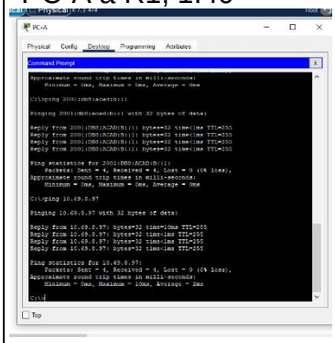
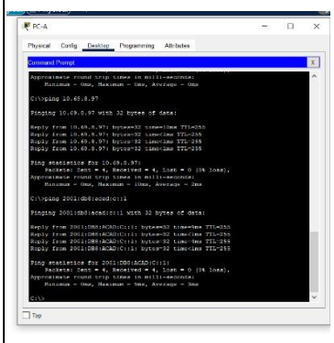
Figura 12 Prueba de ipconfig en PC-B

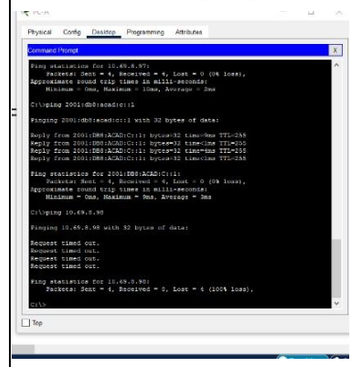
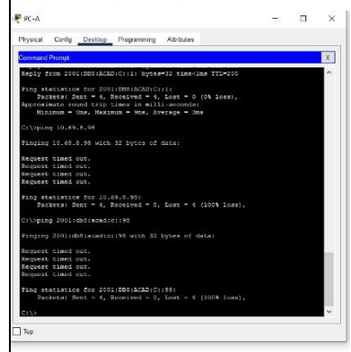
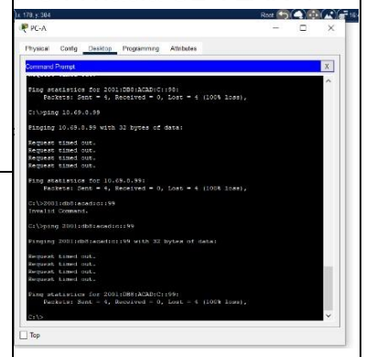
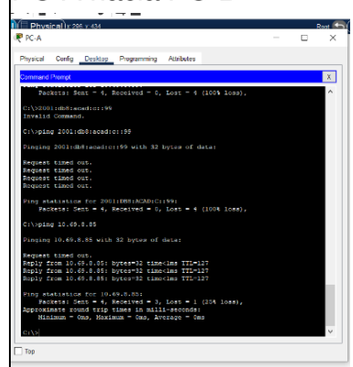


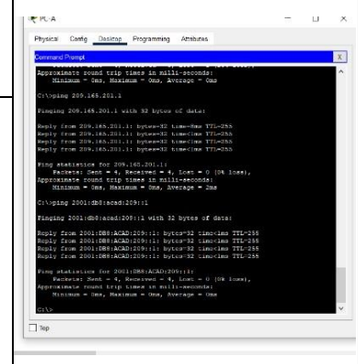
Fuente: Autoría Propia

Tabla 16 Pruebas Realizadas desde PC-A y PC-B a los otros dispositivos de la red

Desde	A		Dirección IP	**Resultados de ping**
PC-A	R1, G0/0/1.20	IPv4	10.69.8.1/26	Figura 13 Prueba Ping PC-A a R1, 1.20  Fuente: Autoría Propia
		IPv6	2001:db8:acad:a::1/64	Figura 14 Prueba Ping PC-A R1, 1.20  Fuente: Autoría Propia

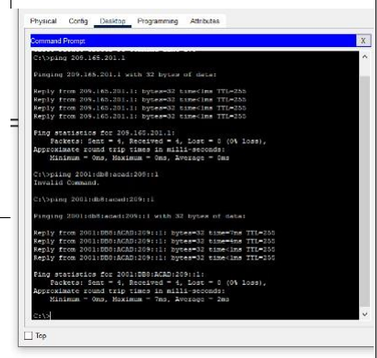
	R1, G0/0/1.30	IPv4	10.69.8.65/27	Figura 15 Prueba Ping PC-A a R1, 1.30  Fuente: Autoría Propia
		IPv6	2001:db8:acad:b::1/64	Figura 16 Prueba Ping PC-A a R1, 1.30  Fuente: Autoría Propia
	R1, G0/0/1.40	IPv4	10.69.8.97/29	Figura 17 Prueba Ping PC-A a R1, 1.40  Fuente: Autoría Propia
		IPv6	2001:db8:acad:c::1/64	Figura 18 Prueba Ping PC-A a R1, 1.40  Fuente: Autoría Propia

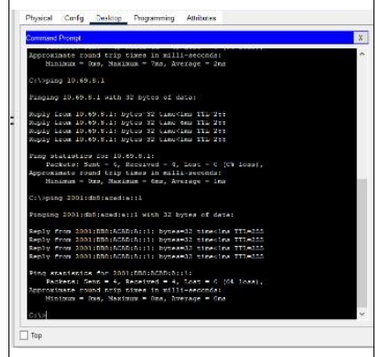
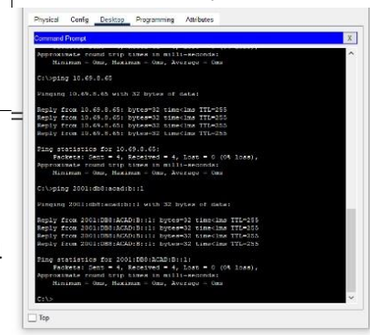
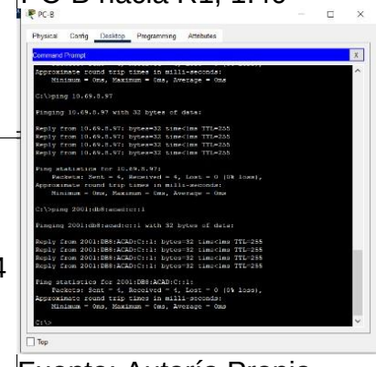
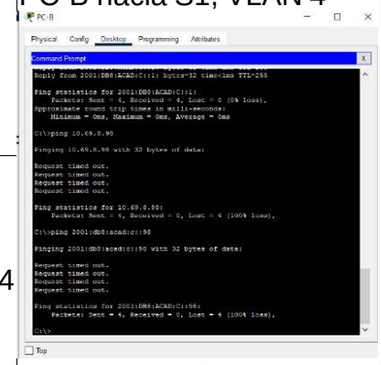
<table>
<tr><td rowspan="4"></td><td rowspan="2">S1, VLAN 4</td><td>IPv4</td><td>10.69.8.98/29</td><td>Figura 19 Prueba PING PC-A hacia S1 VLAN 4
 
Fuente: Autoría Propia</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::98/64</td><td>Figura 20 Prueba PING PC-A hacia S1 VLAN 4
 
Fuente: Autoría Propia</td></tr>
<tr><td rowspan="2">S2, VLAN 4</td><td>IPv4</td><td>10.69.8.99/29</td><td>Figura 21 Prueba PING PC-A hacia S2 VLAN 4
 
Fuente: Autoría Propia</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c::99/64</td></tr>
<tr><td>PC-B</td><td>IPv4</td><td>10.69.8.85</td><td>Figura 22 Prueba PING PC-A hacia PC-B
 
Fuente: Autoría Propia</td></tr>
</table>

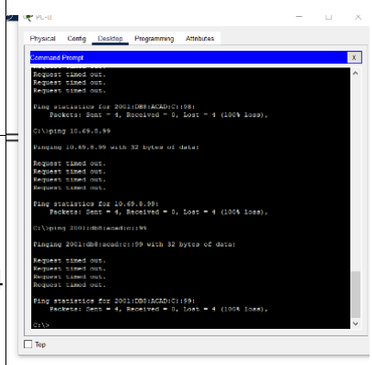
		IPv6	2001:db8:acad:b: :50 /64	Figura 24 Prueba PING PC-A hacia PC-B  Fuente: Autoría Propia
	R1 Bucle 0	IPv4	209.165.201.1/27	Figura 23 Prueba PING PC-A hacia R1 Bucle 0
		IPv6	2001:db8:acad:209::1 /64	 Fuente: Autoría Propia

Fuente: Diplomado de profundización cisco

Tabla 17 Prueba de Ping desde PC-B a los dispositivos de la RED

Desde	B		Dirección IP	Resultados de ping
PC-B	R1 Bucle 0	IPv4	209.165.201.1/27	Figura 25 Prueba PING PC-B hacia R1 Bucle 0
		IPv6	2001:db8:acad:209::1 /64	 Fuente: Autoría Propia
	R1, G0/0/1.2	IPv4	10.69.8.1/26	

		IPv6	2001:db8:acad:a::1/64	Figura 26 Prueba PING PC-B hacia R1, 1.20  Fuente: Autoría Propia
	R1, G0/0/1.3	IPv4	10.69.8.65/27	Figura 27 Prueba PING PC-B hacia R1, 1.30 
		IPv6	2001:db8:acad:b::1/64	Fuente: Autoría Propia
	R1, G0/0/1.4	IPv4	10.69.8.97/29	Figura 28 Prueba PING PC-B hacia R1, 1.40 
		IPv6	2001:db8:acad:c::1/64	Fuente: Autoría Propia
	S1, VLAN 4	IPv4	10.69.8.98/29	Figura 29 Prueba PING PC-B hacia S1, VLAN 4 
		IPv6	2001:db8:acad:c::98/64	Fuente: Autoría Propia

		IPv4	10.69.8.99/29	Figura 30 Prueba PING PC-B hacia S2, VLAN 4  Fuente: Autoría Propia
	S2, VLAN 4	IPv6	2001:db8:acad:c::99/64	

Fuente: Diplomado de profundización cisco

CONCLUSIONES

Se desarrollaron con éxito las temáticas plantadas por el diplomado Cisco por medio de la prueba de habilidades prácticas llevándonos a un entorno amplio en el conocimiento de las redes tanto de una forma práctica como teórica aportando así al desarrollo de nuestro aprendizaje en el área de las telecomunicación e ingeniería.

En el escenario 1, mediante la construcción de la red básica, se logró dar direccionamiento IP y configurar los dispositivos, usando enrutamientos y mecanismos de seguridad, lo cual nos ayuda a mejorar el funcionamiento y la configuración de switches y routers, dando confiabilidad tanto a redes empresariales como a redes pequeñas.

En el escenario 2 se construyó y se estructuró la red mediante uso de mecanismos de seguridad, enrutamientos, protocolo STP y configuración de VLANs, logrando generar redundancia, confiabilidad en la red, y a dar resolución a problemas en entornos como redes corporativas LAN y WLAN.

Finalmente podemos decir que mediante las herramientas facilitadas por el diplomado cisco, hemos complementado nuestros conocimientos para así desarrollar las habilidades necesarias para construir e implementar redes con diferentes aplicaciones.

BIBLIOGRAFÍA

Colaboradores de Wikipedia. Conmutador (dispositivo de red) [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 5 de diciembre del 2022]. Disponible en https://es.wikipedia.org/w/index.php?title=Conmutador_(dispositivo_de_red)&oldid=147365380.

Colaboradores de Wikipedia. Interfaz de línea de comandos [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 5 de diciembre del 2022]. Disponible en https://es.wikipedia.org/w/index.php?title=Interfaz_de_l%C3%ADnea_de_comandos&oldid=146541768.

Colaboradores de Wikipedia. Red Troncal [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 5 de diciembre del 2022]. Disponible en https://es.wikipedia.org/w/index.php?title=Red_Troncal&oldid=146657388.

Colaboradores de Wikipedia. Router [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 5 de diciembre del 2022]. Disponible en https://es.wikipedia.org/w/index.php?title=Router&oldid=147600358.

Colaboradores de Wikipedia. VLAN [en línea]. Wikipedia, La enciclopedia libre, 2022 [fecha de consulta: 5 de diciembre del 2022]. Disponible en https://es.wikipedia.org/w/index.php?title=VLAN&oldid=147337360.

LA ENCICLOPEDIA LIBRE, Wikipedia. Red de computadoras. Wikipedia [página web]. (9, noviembre, 2022). [Consultado el 5, diciembre, 2022]. Disponible en Internet: https://es.wikipedia.org/wiki/Red_de_computadoras.

P. Flor Modelo TCP/IP. [online]. Disponible en: https://repository.unad.edu.co/handle/10596/43437 .

R. J. Castaño Ribes, Redes locales. Madrid: Macmillan Iberia, S.A. 2013. [En Línea] Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/43257

R. J. Castaño Ribes, Redes locales. Madrid: Macmillan Iberia, S.A. 2013. [En Línea] Disponible en: https://elibro net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/43257?pag=233

VELTE, Toby. Guía del usuario de Cisco Router and Security Device Manager {En línea} (2007) {5 de Diciembre del 2022} Disponible en. https://www.cisco.com/c/dam/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/spanish/24ln_es.pdf

ANEXOS

ANEXO A:

https://drive.google.com/file/d/1pk20TI92-rUyqvF_ePSg5UI0TihZhV50/view?usp=sharing

ANEXO B:

https://drive.google.com/file/d/1DLHnm3XWMAiD9LLsH94iIBnJC2tf9Y6h/view?usp=sharing