SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DETECNOLOGÍA CISCO

CINDY CAROLINA POVEDA GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA DE SISTEMAS
FUSAGASUGA
2022

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DETECNOLOGÍA CISCO

CINDY CAROLINA POVEDA GONZALEZ

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

DIRECTOR:

PAULITA FLOR SALAZAR
INGENIERA DE TELECOMUNICACIONES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
INGENIERIA DE SISTEMAS
FUSAGASUGA
2022

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Fusagasugá 27 de noviembre de 2022

AGRADECIMIENTOS

Agradezco a Jehová Dios primeramente por permitirme llegar a este punto de estar finalizando esta profesión tan hermosa de la Ingeniería de Sistemas, a mi madre por su apoyo y ayuda total, todo el esfuerzo, dedicación y tenacidad de las dos para poder salir adelante con esta profesión, el crédito es para mi madre quien ha estado para mí siempre, incondicionalmente, y esto es dedicado a ella. A la universidad por recibirme y ser parte de ella haciendo lo mejor y a los tutores quienes dedican su tiempo y paciencia para colaborarnos a hacer mejores personas profesionalmente.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BYOD: brinda un enfoque universal independientemente del tipo de dispositivo que se conecte a la red de una empresa, sea por cable, wifi público, o móvil, ya sea que la conexión sea en un campus principal, sucursal, oficina o desde casa.

DCL: (data control language) lenguaje de control de datos, “controla el acceso de usuario a los objetos de base de datos y su contenido”.[1] (IBM, IBM Documentación, 2021)

EXTRANET: proporciona acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la compañía.

INTRANET: hace relación a una conexión privada de red LAN y WAN que pertenece a una organización que presta el servicio y está diseñada para que accedan o los empleados o personas autorizadas.

MULTIDIFUSION: Transmisión donde el mensaje se entrega a un grupo de hosts

NTP: network time protocol, sincroniza el tiempo y los relojes en las conexiones de red de dispositivos de una misma red.

OSPF: open shortest path first – “el camino más corto primero. Protocolo de direccionamiento de enlace-estado, desarrollado para las redes IP. Protocolo de enrutamiento dinámico”[2].

[1] IBM. Lenguaje de control de datos. Copyright IBM Corporation. 2014.

[2] IBM. Open shortest path First. Copyright Ibm Corporation. 2014

RED CONVERGENTE: o llamadas también multiservicio, se refiere a la integración de los servicios de voz, datos y video en una sola red con IP como protocolo de capa de red.

TCP: protocolo de control de transmisión/protocolo de internet, se utiliza para interconectar dispositivos de red en internet.

UDP: protocolo de datagrama de usuario, transmisión de paquetes no orientado a conexión y no confiable de los paquetes de la capa 4, este protocolo es ligero de transporte de datos que funciona sobre IP.

UNIDIFUSION: forma en la que entrega los mensajes en la que el mensaje se entrega a un solo destinatario.

VTY: línea de terminal virtual, permite definir direcciones IP, que permite acceder remotamente al proceso EXEC del router.

RESUMEN

El diplomado avanzado de CISCO incluye la demostración de habilidades practicas a través de múltiples funciones de aprendizaje, enrutamiento, diagnóstico, configuración y resolución de problemas de red, es una parte integral de los módulos de capacitación que permite la revisión y evaluación. Se desarrollan dos escenarios, cada escenario requirió un enfoque aprendido durante el desarrollo para resolver diferentes prácticas, pero en el primer escenario se desarrolló la relación entre los dos. Los diversos comandos bien utilizados y sus salidas deben, a su vez, codificarse utilizando ciertos parámetros para el segundo escenario, excepto que se repite el procedimiento de puerto propuesto. Todo el contenido anterior está diseñado para profundizar en conceptos básicos de redes como conmutación, enrutamiento, protocolos, IPV4, IPV6, TCP/IP, configuración dinámica de DHCP, direccionamiento, entre otros.

Con esto finaliza la tesis del Diplomado avanzado de CISCO (diseño e implementación de soluciones integradas de redes LAN/WAN).

PALABRAS CLAVE: CONFIGURACIÓN, CISCO, PACKET TRACER, DIRECCIONAMIENTO, ROUTER, SWITCH, HOST, SUBRED.

ABSTRACT

The CISCO advanced diploma includes demonstration of hands-on skills through multiple learning functions, routing, diagnostics, configuration, and network troubleshooting, is an integral part of the training modules allowing for review and evaluation. Two snerarios are developed, each scenario required an approach learned during development to solve different practices, but in the first scenario the relationship between the two was developed. The various well-used commans and their outputs must, in turn, be encoded using certain parameters for the second scenario, except that the proposed port procedure is repeated. All of the above content is designed to deepen basic networking concepts such as switching, routing, protocols, IPV4, IPV6, tcp/ip, Dynamic DHCP configuration, addressing and more. Witch this, the tesis of the CISCO advanced diploma (design and implementation of integrated LAN/WAN network solutions ends).

KEY WORDS: CONFIGURATION, CISCO, PACKET TRACER, ADDRESSING, ROUTER, SWITCH, HOST, SUBNET.

INTRODUCCIÓN

Este documento se elabora para la opción de grado como parte del programa de ingeniería de sistemas cursando el diplomado de profundización en redes. En este documento se presenta dos escenarios desarrollados con la herramienta Packet tracer, poniendo en práctica lo visto en la plataforma Netacad.com de CISCO, en estos escenarios se demuestran las habilidades adquiridas en el aprendizaje de los materiales del curso.

El desarrollo del escenario uno se configura dispositivos de una red pequeña. Se configurará de forma básica un router, switch y 2 equipos. Primeramente, se diseña un esquema de direccionamiento IPv4 para las LAN propuestas, a medida que se avanza con la configuración de cada dispositivo se agregan nuevos comandos, allí se logrará ver la creación de usuarios y contraseñas encriptadas, configuración de líneas virtuales de consola, tanto para router como para switch, que implica la ejecución de un escenario virtual permitiendo simular la conectividad de varios dispositivos utilizados en una red informática.

En cuanto al segundo escenario se desarrolla la configuración básica tanto en la red como en los equipos, router, switches con conexiones ipv4 e ipv6, configurando el enrutamiento por DHCP, VLAN´S y probando y revisando conectividad entre cada uno de los dispositivos, con el propósito de mostrar la capacidad para resolver problemas de redes informáticas pequeñas y a mediana escala que requieren la configuración correcta.

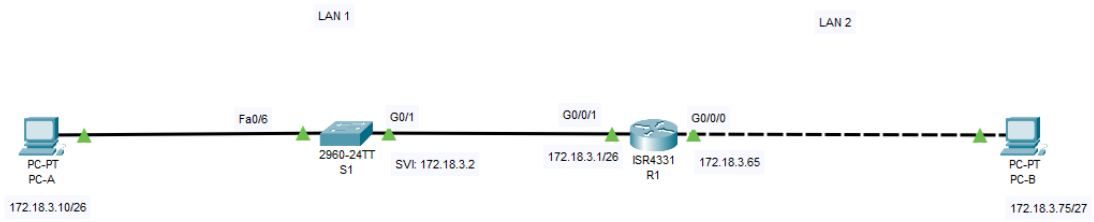
ESCENARIO 1

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

Parte 1: Construya la Red

En el simulador se procede a construir la red de acuerdo a la topología lógica que se plantea en la Guía donde indica que dispositivos y cuantos utilizar, a que puertos va conectado cada uno de ellos. Teniendo en cuenta la red tiene dos LAN, la primera LAN1 debe contar con 60 host y la LAN2 con 20 hosts. (CISCO, 2020)

Figura 1. Topología de red 1



Fuente: prueba habilidades diplomado CCNA

Parte 2: Desarrolle el esquema de direccionamiento IP

Se desarrolla el esquema de direccionamiento IP, teniendo en cuenta que el segundo octeto debe llevar los dos últimos dígitos de la cedula del estudiante.

El primer requerimiento de la LAN 1 debe tener 60 hosts, por tanto, es 2^6, se escogen los 6 primeros octetos, entonces, se tendrá una cantidad de 64 direcciones,

pero como se debe dejar 2 direcciones que son la de broadcast y red, quedan 62 hosts disponibles útiles.

El segundo requerimiento de la LAN 2 debe tener 20 hosts, por tanto, es 2^5, se escogen los 5 primeros octetos, entonces, se tendrá una cantidad de 32 direcciones, pero como se debe dejar 2 direcciones que son la de broadcast y red, quedan 30 hosts disponibles útiles.

En la siguiente tabla se muestra el direccionamiento a utilizar de las 2 LAN como para cada dispositivo de la red.

Tabla 1. Direccionamiento IPV4 1

Ítem	Requerimiento
Dirección de red	172.18.3.0
Requerimiento de host subred LAN1	60 Dirección de red:172.18.3.0 Prefijo: /26 Cantidad direcciones:64 Cantidad direcciones útiles:62 Primera dirección valida:172.18.3.1 Ultima dirección valida:172.18.3.62 Broadcast: 172.18.3.63 Mascara de red: 255.255.255.192
Requerimiento de host subred LAN2	20 Dirección de red:172.18.3.64 Prefijo: /27 Cantidad direcciones:32 Cantidad direcciones útiles:30 Primera dirección valida:172.18.3.65

	Ultima dirección valida:172.18.3.94 Broadcast: 172.18.3.95 Mascara de red: 255.255.255.224
R1 G0/0/1	172.18.3.62/26
R1 G0/0/0	172.18.3.94/27
S1 SVI	172.18.3.2/26
PC-A	172.18.3.10/26
PC-B	172.18.3.75/27

Parte 3: configure aspectos básicos

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

Paso 1: se configuran los ajustes básicos del Router 1, por medio de consola utilizando comandos para poder comunicarse el router con el switch y los computadores, se crean contraseñas y se muestra cómo deben ser encriptadas para que terceras personas o no autorizadas puedan ingresar y ver lo que hay, como tampoco saber ni cual es el usuario utilizado ni las contraseñas, ya que muestran un cifrado encriptado y solo se ve letras y números. También se agrega las 2 interfaces al router, entre otros.

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

Tabla 2. Configuración Router1 1

Tarea	Especificación
Desactivar la búsqueda DNS	El DNS viene activado por defecto. Este comando sirve para cuando se cometa

	un error en el nombre, el enrutador supondrá que debe buscar en el DNS. Pero si se desactiva quiere decir que no está disponible y suspende las búsquedas. Router>enable Router#config terminal Router(config)#no ip domain-lookup Router(config)#exit Router#show run | include domain-lookup No ip domain-lookup Router# copy running-config startup-config
Nombre del router	Se asigna el nombre al router como R1, para identificar de otros dispositivos en el entorno lógico: Router(config)#hostname R1 R1(config)#exit
Nombre de dominio	Se define un nombre de dominio predeterminado que el Cisco IOS utiliza para completar los nombres del host incompetentes. R1#config terminal

	R1(config)#no ip domain-name ccna-sa.com R1(config)#exit
Contraseña cifrada para el modo EXEC privilegiado	Aquí se configura una contraseña para la conexión de consola al modo privilegiado. Se utiliza secret ya que ésta se guarda encriptada en los ficheros de configuración del router. R1#config terminal R1(config)#enable secret ciscoenpass R1(config)#exit R1(config)#disable
Contraseña de acceso a la consola	Se genera una segunda contraseña para la conexión de consola al modo de usuario y se utiliza secret también para que esta sea encriptada en los ficheros del router R1#config terminal R1(config)#line console 0 R1(config-line) #enable secret ciscoconpass R1(config-line) #exit R1(config)#disable

Establecer la longitud mínima para las contraseñas	10 caracteres El definir la longitud de la contraseña de 10 caracteres hace que la contraseña sea más segura para no ser adivinada o que tenga ataques. Password: ciscoenpass Password: ciscoconpass R1>enable Password: ciscoenpass R1#configure terminal R1(config)#security password min-length 10 R1(config)#exit
Crear un usuario administrativo en la base de datos local	Se crea un usuario y contraseña de base local para que con este usuario pueda ingresar a la configuración del router. R1#config terminal R1(config)#username admin secret admin1pass R1(config)#exit R1#
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Estas líneas de terminal virtual del router se utiliza para controlar las conexiones telnet entrantes.

	Se configura esta línea para todos los usuarios con contraseñas específicas a los usuarios para que puedan configurar de manera local el router. Las siguientes líneas no sirvieron ya que no quedan registradas las contraseñas. R1#config terminal R1(config)#line vty 0 4 R1(config-line) #login local R1(config-line) #exit Por tanto, las cree así: R1#config terminal R1(config)#line console 0 R1(config-line) #password admin1pass R1(config-line) #login R1(config-line) #line vty 0 15 R1(config-line) #password admins1pass R1(config-line) #login R1(config)#exit R1#wr El line console 0 se usa para ingresar al modo de configuración de línea de modo consola. Luego se ingresa la

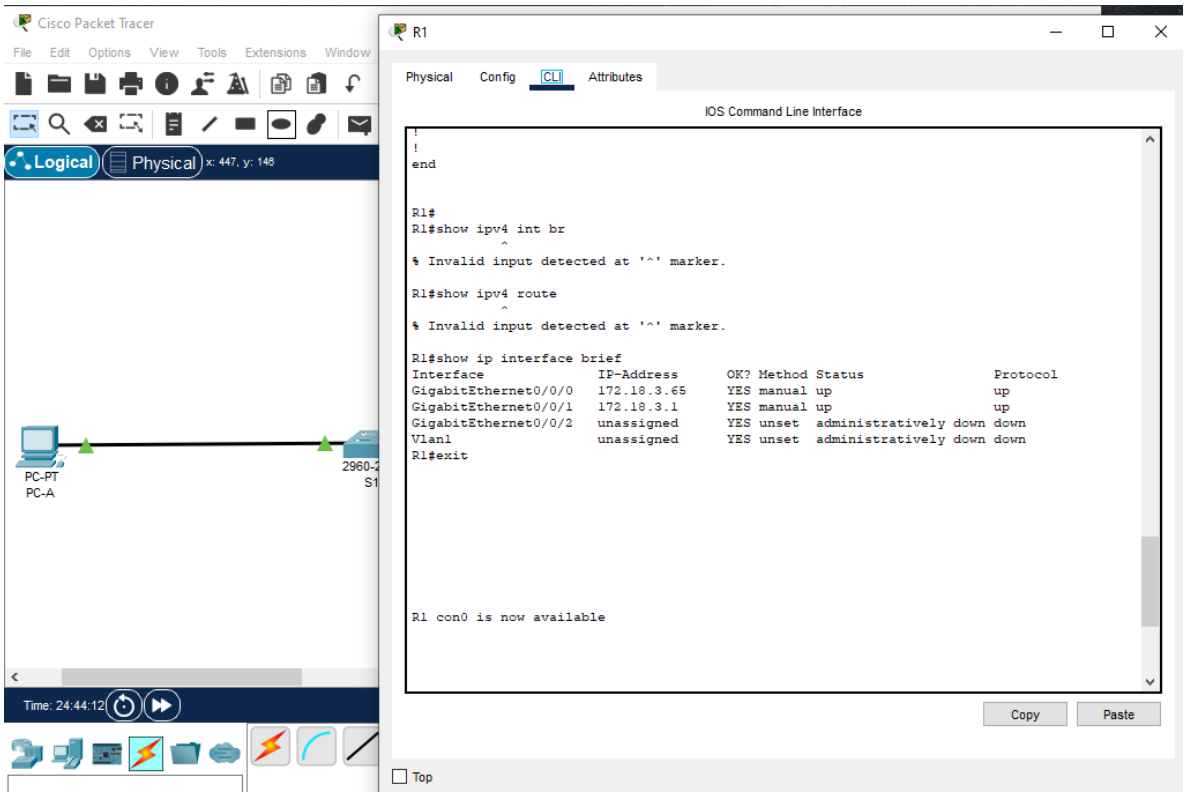
	contraseña y siguiente login para configurar el SW o router para que requiera la autenticación al iniciar sesión. Después se ingresa line vty 0 15 para ingresar a la configuración de vty en las 16 líneas. Para habilitar la contraseña de seguridad de líneas de sesión se utiliza login.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Anteriormente se configura la línea virtual del router con usuario y contraseñas específicas, mientras que con el protocolo SSH lo que hace es encriptar la comunicación entre el cliente, evitando que terceras personas puedan descubrir el usuario y contraseña. R1(config)#crypto key generate rsa R1(config)#1024 R1(config)#ip ssh versión 2 R1(config)#line vty R1(config-line) #login local R1(config-line) #transport input ssh R1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	Este comando service password-encryption utiliza un cifrado débil a las contraseñas que no están cifradas.

	R1(config)# R1(config)#service password-encryption R1(config)#exit
Configurar un banner MOTD	Se configura este banner para mostrar información a usuarios que de pronto estén ingresando y nos son autorizados, como mensajes de emergencia, o mensajes para que el administrador de red lo pueda ver de forma remota. R1#config terminal R1(config)#banner motd $R1 Cindy carolina poveda González ingeniería de sistemas R1(config)#exit Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.
Configuración de interface G0/0/0	Se ingresa a la configuración del router y como ya se ha creado las contraseñas pide ingresar al modo privilegiado y usuario, luego se configura la interfaz con su respectiva dirección de host diseñada anteriormente con su

	mascara de red, para poder activarla se escribe el comando no shutdown. R1>enable Password: ciscoenpass R1#configure terminal R1(config)# interface gigabitEthernet 0/0/0 R1(config-if) #ip address 172.18.3.65 255.255.255.224 R1(config-if) #no shutdown R1(config-if) #exit R1 con0 is now available
Configuración de interface G0/0/1	R1 Cindy carolina poveda González ingeniería de sistemas User access verification Password: ciscoenpass Password: ciscoconpass R1(config)#interface gigabitEthernet0/0/1 R1(config-if) #ip address 172.18.3.1 255.255.255.192 R1(config-if) #no shutdown R1(config-if) #exit
Generar una clave de cifrado RSA	La clave de cifrado RSA habilita el servidor SSH en el router para poder generar la clave RSA. Y para habilitarla

	se usa el comando crypto key rsa, al crear la clave se solicita que se introduzca una longitud de módulo, en este caso se coloca 1024, ya que una longitud mayor es más segura, se puede tardar más al generarlo y utilizarla. R1#configure terminal R1#(config)#crypto key generate rsa %please define a domain-name first R1(config)crypto key generate rsa How many bits in the modulus [512]: 1024 % generating 1024 bit rsa keys, keys Will be non-exportable…[ok] R1(config)#exit R1# R1 con0 is now available

Figura 2. Mostrar interfaces R1 1



Fuente: autor

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Configuración Switch 1 1

Desactivar la búsqueda DNS	El DNS viene activado por defecto. Este comando sirve para cuando se cometa un error en el nombre, el enrutador supondrá que debe buscar en el DNS. Pero si se desactiva quiere decir que no está disponible y suspende las búsquedas. Switch>enable Switch# configure terminal Switch(config)# no ip domain-lookup

	Switch(config)#exit
Nombre del switch	Se asigna el nombre al router como R1, para identificar de otros dispositivos en el entorno lógico: Switch#configure terminal Switch(config)#hostname S1 S1# exit
Nombre de dominio	Se define un nombre de dominio predeterminado que el Cisco IOS utiliza para completar los nombres del host incompetentes: S1# configure terminal S1(config)#ip domain-name ccna-sa.com S1(config)#exit
Contraseña cifrada para el modo EXEC privilegiado	Aquí se configura una contraseña para la conexión de consola al modo privilegiado. Se utiliza secret ya que ésta se guarda encriptada en los ficheros de configuración del router: S1# configure terminal S1(config)#enable secret ciscoenpass S1(config-line) #exit
Contraseña de acceso a la consola	Se genera una segunda contraseña para la conexión de consola al modo de usuario y se utiliza secret también para que esta sea encriptada en los ficheros del router

	S1# configure terminal S1(config)#line console 0 S1(config)#enable secret ciscoconpass
Apagar todos los puertos sin usar	Como solo se necesitan el puerto de fast Ethernet y el de Gigabit entonces los otros se apagan para evitar robo de información. S1#show interfaces status Muestra todos los puertos que están conectados y ahora se apagan con el siguiente código: S1#configure terminal S1(config)#interface range fastEthernet 0/1-5 Muestra con el siguiente código los puertos que están apagados S1(config-if-range) #shutdown S1(config-if-range) #exit Para deshabilitar los otros puertos se escribe: S1(config)#interface range fastEthernet 0/7-24 Muestra con el siguiente código los puertos que están apagados S1(config-if-range) #shutdown S1(config-if-range) #exit Y para deshabilitar los puertos de gigabit así:

	S1(config)#interface gigabitEthernet 0/2 S1(config-if-range) #shutdown S1(config-if-range) #exit
Crear un usuario administrativo en la base de datos local	Se crea un usuario y contraseña de base local para que con este usuario pueda ingresar a la configuración del switch. Nombre de usuario: admin Contraseña: admin1pass S1#enable S1#configure terminal S1(config)#username admin password admin1pass S1(config)#exit
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	Estas líneas de terminal virtual del switch se utilizan para controlar las conexiones telnet entrantes. Se configura esta línea para todos los usuarios con contraseñas específicas a los usuarios para que puedan configurar de manera local el switch. S1# configure terminal S1(config)#line vty 0 4 S1(config)#login local

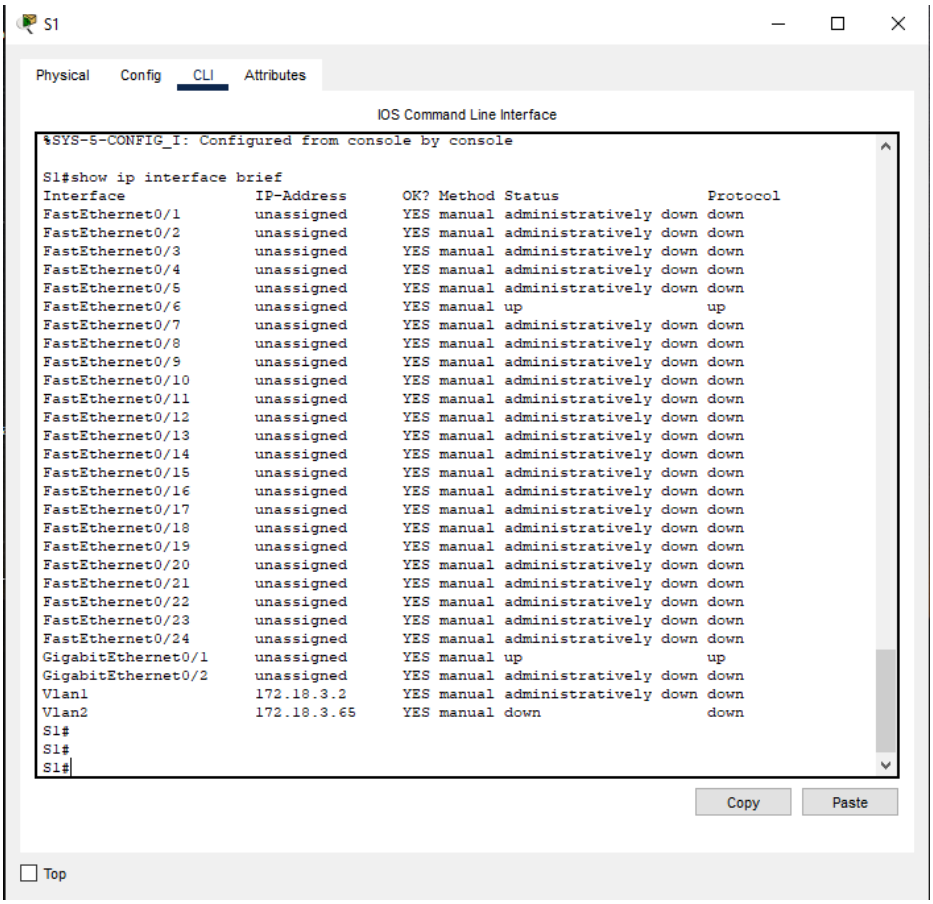
	S1(config)#exit Por tanto, las cree así: S1#config terminal S1(config)#line console 0 S1(config-line) #password admin1pass S1(config-line) #login S1(config-line) #line vty 0 15 S1(config-line) #password admins1pass S1(config-line) #login S1(config)#exit S1#wr El line console 0 se usa para ingresar al modo de configuración de línea de modo consola. Luego se ingresa la contraseña y siguiente login para configurar el SW para que requiera la autenticación al iniciar sesión. Después se ingresa line vty 0 15 para ingresar a la configuración de vty en las 16 líneas. Para habilitar la contraseña de seguridad de líneas de sesión se utiliza login.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Anteriormente se configura la línea virtual del switch con usuario y contraseñas específicas, mientras que con el protocolo SSH lo que hace es encriptar la comunicación entre el cliente, evitando que terceras personas puedan descubrir el usuario y contraseña.

	S1# configure terminal S1(config)#line vty 0 15 S1(config-line) #transport input ssh
Cifrar las contraseñas de texto no cifrado	Este comando service password-encryption utiliza un cifrado débil a las contraseñas que no están cifradas. S1(config-line) #service password-encryption
Configurar un banner MOTD	Se configura este banner para mostrar información a usuarios que de pronto estén ingresando y nos son autorizados, como mensajes de emergencia, o mensajes para que el administrador de red lo pueda ver de forma remota. S1# configure terminal S1(config)#banner motd $S1 Cindy Carolina Poveda Gonzalez Ingenieria de Sistemas$
Generar una clave de cifrado RSA	La clave de cifrado RSA habilita el servidor SSH en el switch para poder generar la clave RSA. Y para habilitarla se usa el comando crypto key rsa, al crear la clave se solicita que se introduzca una longitud de módulo, en este caso se coloca 1024, ya que una longitud mayor es más segura, se puede tardar más al generarlo y utilizarla. S1(config)#crypto key generate rsa

	%You already have RSA keys defined named S1.ccna-sa.com %do you really want to replace them? [yes/no]: n S1(config)#crypto key generate rsa general-keys modulus 1024 %the key modulus size is 1024 bits %generating 1024 bit RSA keys, keys Will be non-exportable…[ok] *Mar 1 2:41:31.704: %ssh-5-ENABLED: SSH 1.99 has been enabled S1(config)# S1 con0 is now available
Configure la interfaz de administración (SVI) en VLAN1	Se configura la interface vlan1 con su respectiva dirección IP y máscara de subred, esto para que haya conexión en ambas LAN y para activarla para poder hacer ping con el comando no shutdown. También se configura el Gateway para comunicación entre ambas LAN, entre computadoras. S1(config)#interface vlan1 S1(config-if) # ip address 172.18.3.2 255.255.255.192

	S1(config-if) #no shutdown S1#(config-if) #ip default-gateway 172.18.3.63 S1#(config)) exit

Figura 3. Interfaces deshabilitadas 1



Fuente: autor

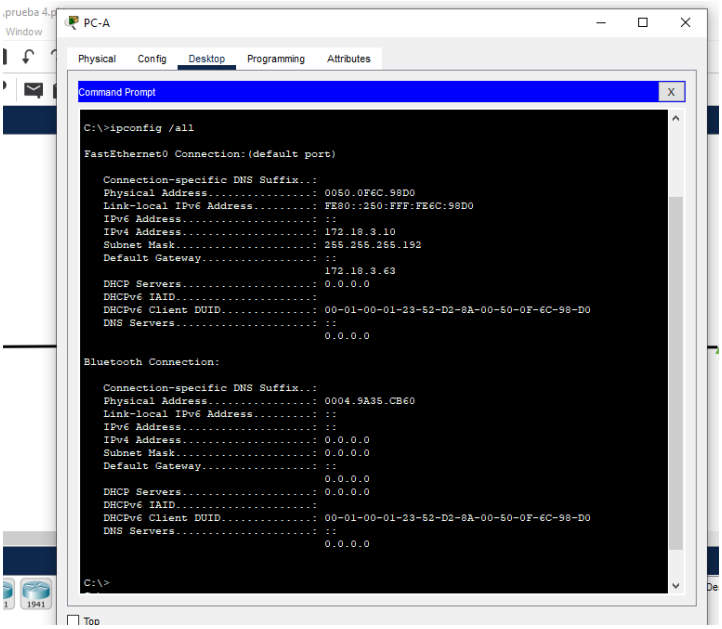
Paso 2. Configurar los equipos

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 PC-A 1

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	En blanco
Dirección IPv4	172.18.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.18.3.63

Figura 4. Ipconfig/all PC-A 1



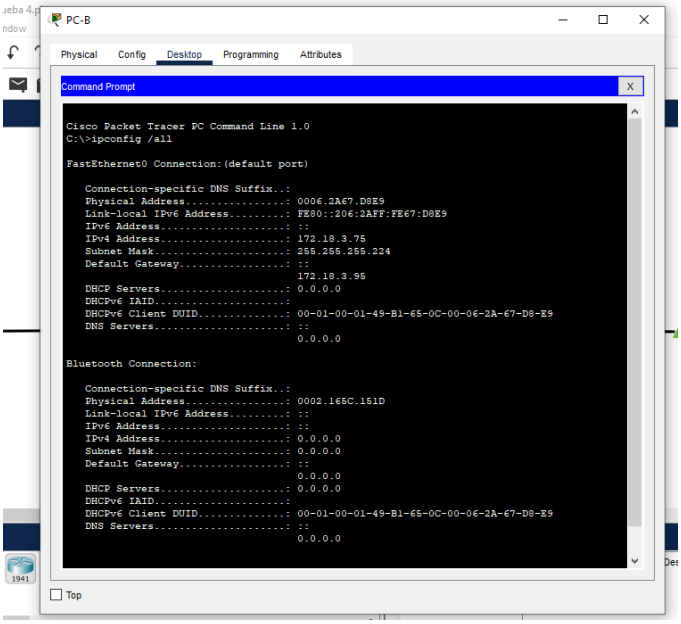
Fuente: autor

Al ejecutar el comando ipconfig /all en el PC-A, muestra la conexión específica, dentro de esta se puede ver la dirección IPv4 de la computadora A la máscara de subred, el Gateway.

Tabla 5. Configuración de Red PC-B 1

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	En blanco
Dirección IPv4	172.18.3.75
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.18.3.95

Figura 5. Ipconfig/all PC-B 1



Fuente: autor

Al ejecutar el comando ipconfig /all en el PC-B, muestra la conexión específica, dentro de esta se puede ver la dirección IPv4 de la computadora A la máscara de subred, el Gateway

Parte 5: probar y verificar la conectividad de extremo a extremo

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

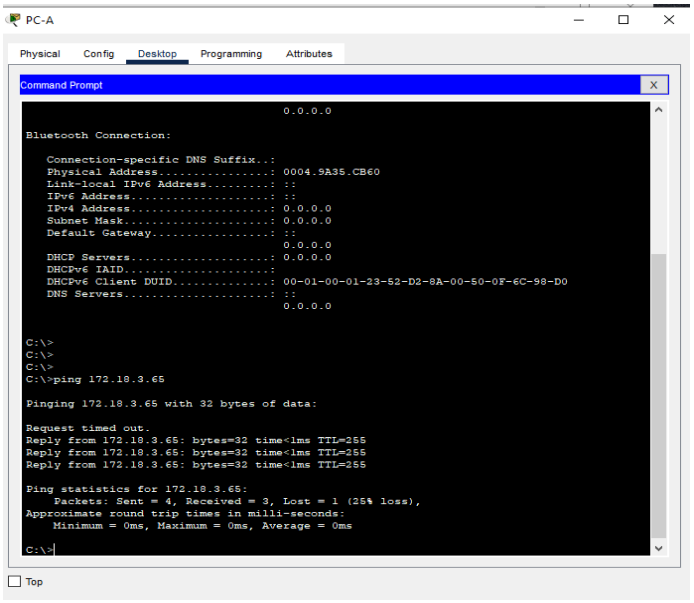
Desde: PC-A

A: R1 G0/0/0

Dirección IP: 172.18.3.65

Resultado ping:

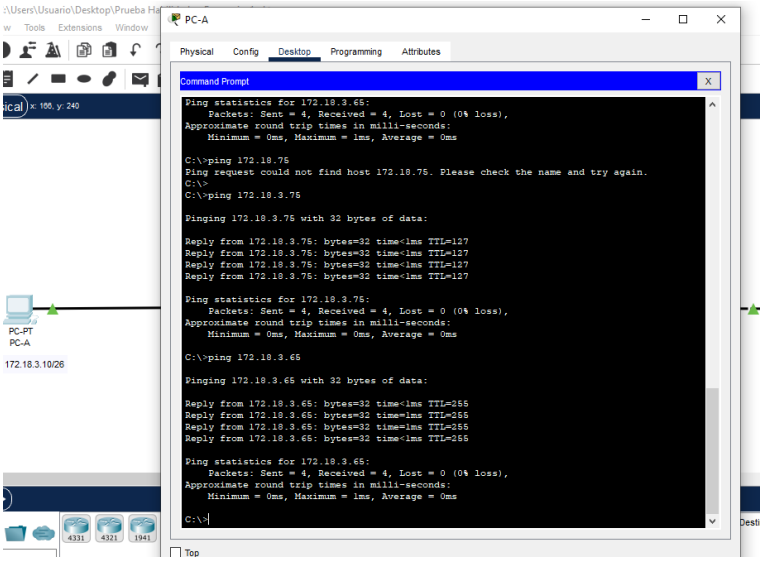
Figura 6. R1 G0/0/0 1



Fuente: autor

Desde la computadora PC-A se hace ping a la dirección 172.18.3.65 que es la interfaz del Router G 0/0/0 y primero dice que el tiempo de espera está agotado, luego logró enviar 4 paquetes de los cuales solo recibió 3 en un tiempo estimado de 1 ms, 1 archivo de perdió. No enviaba todos los paquetes porque la interfaz de vlan1 estaba apagada, por tanto, se perdían paquetes, en la siguiente imagen se muestra el envío correcto a cada una de las interfaces.

Figura 7. Desde PC-A a LAN 2 1



Fuente: autor

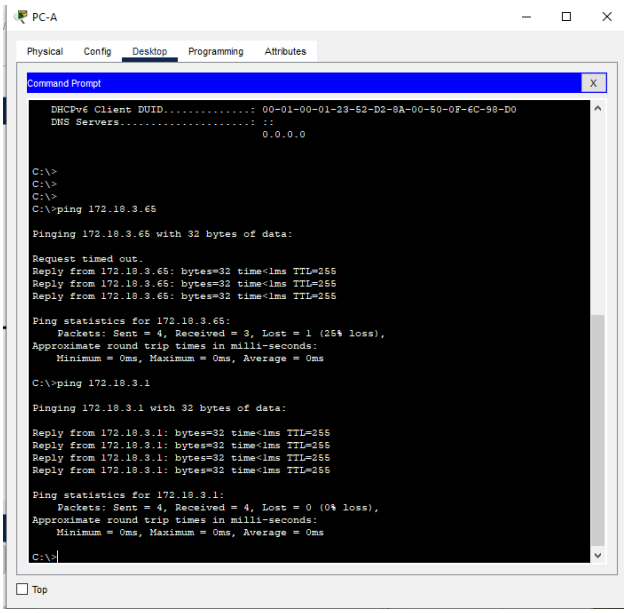
Desde: PC-A

A: R1 G0/0/1

Dirección IP: 172.18.3.1

Resultado ping:

Figura 8. R1 G0/0/1 1



Fuente: autor

Desde la computadora PC-A se hace ping a la dirección 172.18.3.1 que es la interfaz del Router G 0/0/1, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 1 ms.

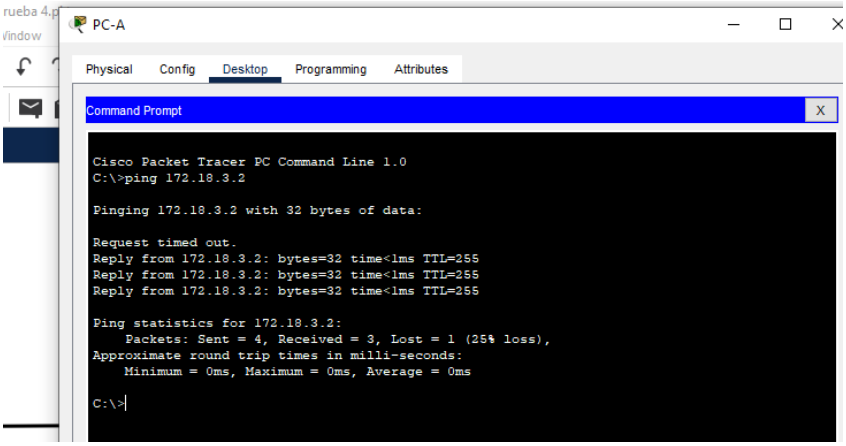
Desde: PC-A

A: S1 VLAN 1

Dirección IP: 172.18.3.2

Resultado ping:

Figura 9. S1 VLAN1 1



Fuente: autor

Desde la computadora PC-A se hace ping a la dirección 172.18.3.2 que es la interfaz del switch SVLAN1, logra enviar 4 paquetes de los cuales solo recibe 3 en un tiempo estimado de 1 ms, con 1 archivo perdido.

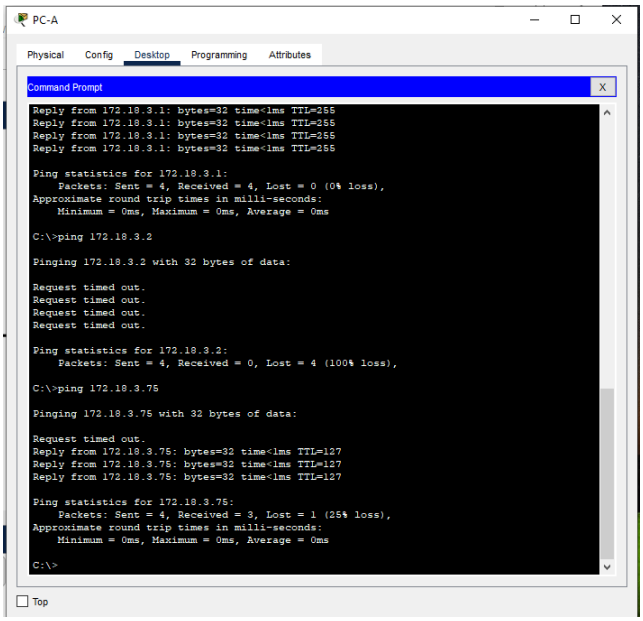
Desde: PC-A

A: PC-B

Dirección IP: 172.18.3.75

Resultado ping:

Figura 10. PC-B 1



Fuente: autor

Desde la computadora PC-B se hace ping a la dirección 172.18.3.75 que es la interfaz de la computadora, primero dice que el tiempo de espera agotado, luego logra enviar 4 paquetes de los cuales solo recibe 3 en un tiempo estimado de 1 ms, con 1 archivo perdido.

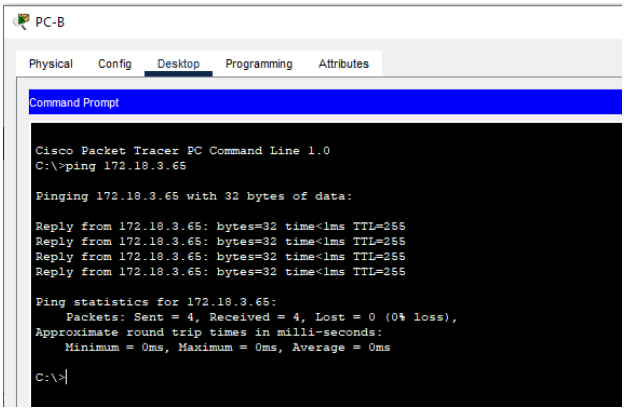
Desde: PC-B

B: R1 G0/0/0

Dirección IP: 172.18.3.65

Resultado ping:

Figura 11. Desde PC-B a R1 G0/0/0 1



Fuente: autor

Desde la computadora PC-B se hace ping a la dirección 172.18.3.65 que es la interfaz del router G0/0/0, primero dice que el tiempo de espera agotado, luego logra enviar 4 paquetes y recibe 4 en un tiempo estimado de 1 ms.

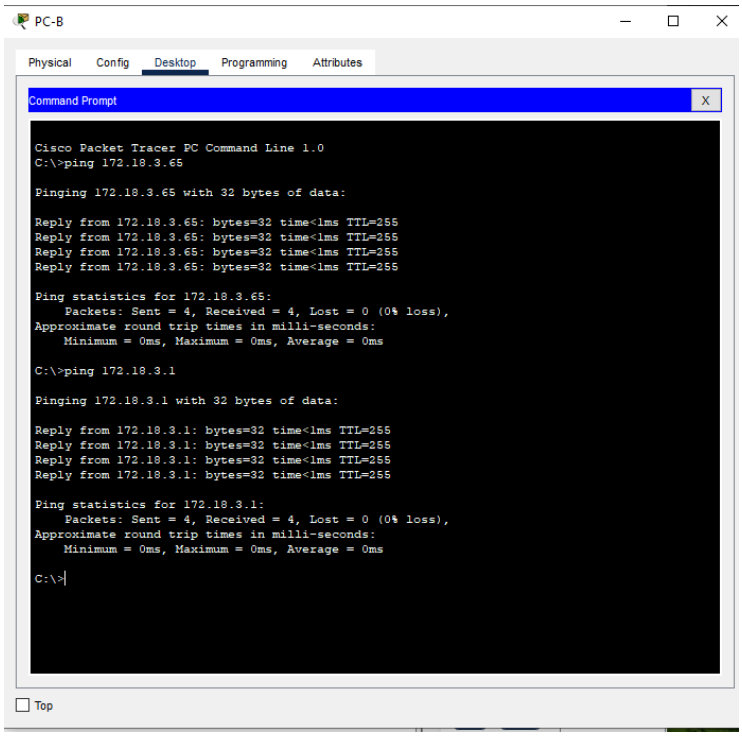
Desde: PC-B

B: R1 G0/0/1

Dirección IP: 172.18.3.1

Resultado ping:

Figura 12. Desde PC-B a R1 G0/0/1 1



Fuente: autor

Desde la computadora PC-B se hace ping a la dirección 172.18.3.1 que es la interfaz del router G0/0/1, envía 4 paquetes y recibe 4 en un tiempo estimado de 1 ms.

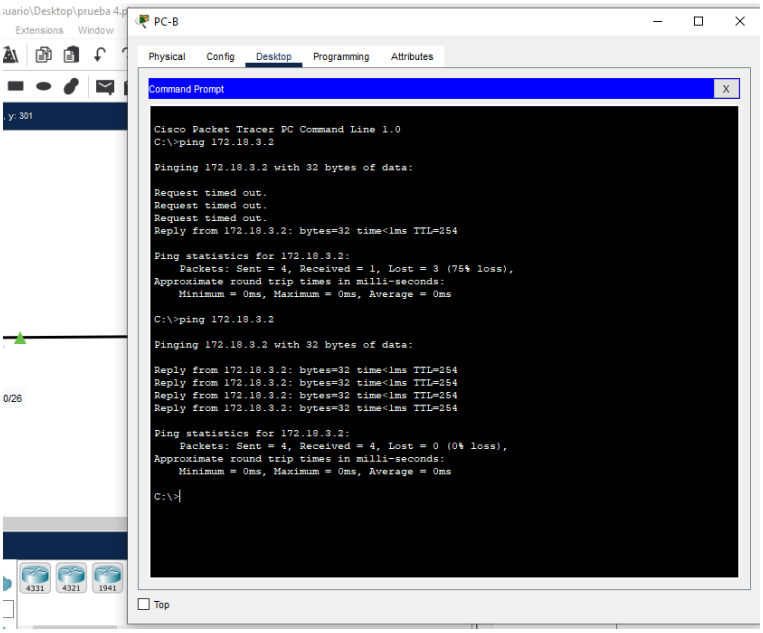
Desde: PC-B

B: S1 VLAN1

Dirección IP: 172.18.3.2

Resultado ping:

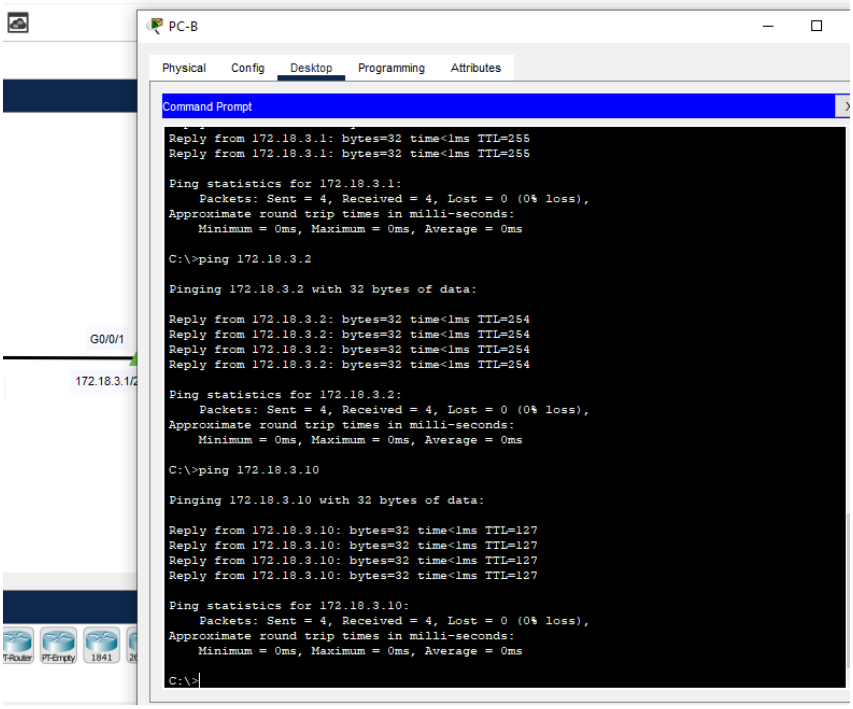
Figura 13. Desde PC-B a S1 VLAN1 1



Fuente: autor

Desde la computadora PC-B se hace ping a la dirección 172.18.3.2 que es la interfaz del switch S1 VLAN1, envía 4 paquetes y recibe 4 en un tiempo estimado de 1 ms. No enviaba los paquetes ya que la interfaz de vlan1 estaba apagada por tanto se perdían los paquetes desde el pc-B al switch y a otras interfaces. En la siguiente imagen se muestra la conectividad y el envío de paquetes a todos los dispositivos. Desde el PC-B, que es la LAN2 a la LAN1.

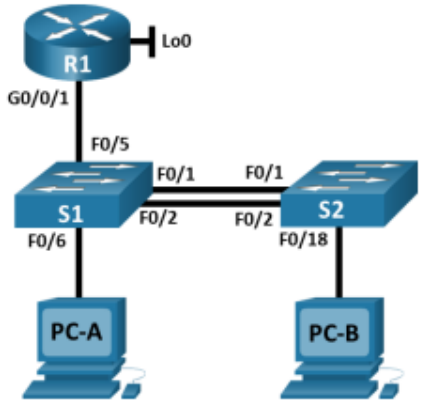
Figura 14. Desde PC-B a LAN 1 1



Fuente: autor

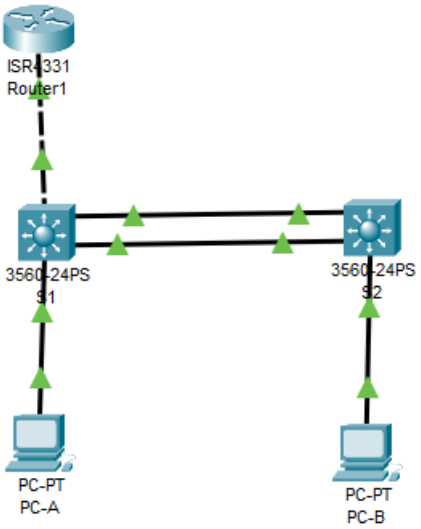
ESCENARIO 2

Figura 15. Topología 1



Fuente: prueba de habilidades diplomado CCNA

Figura 16. Topología final 1



Fuente: autor

En este escenario se configurarán los dispositivos de una red pequeña. Se realiza la configuración básica de los dispositivos intermedios y finales donde admitan IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura, se configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

En la siguiente tabla se muestra el número y el nombre de las VLAN a utilizar más adelante:

Tabla 6. VLAN´s 1

VLAN	NOMBRE DE LA VLAN
20	Docentes
30	Estudiantes
40	Invitados
50	Usuarios
56	Native

A continuación, la tabla donde muestra las asignaciones de direcciones, lo que corresponde a cada dispositivo.

Tabla 7. Asignación de direcciones 1

Dispositivo	**Interfaz**	**Dirección IPv4**	**Máscara de subred**	**Gateway predeterminado**
R1	G0/01.20	10.18.8.1/26 2001:db8: acad: a:1/64	255.255.255.0	N/D

	G0/0/1.30	10.18.8.65/27	255.255.255.252	N/D
	G0/0/1.40	10.18.8.97/29 2001:db8: acad: c:1/64	255.255.255.252	
	G0/0/1.56	NO corresponde	No corresponde	N/D
R1	Loopback 0	209.165.201.1/27 2001:db8: acad:209::1/64		
S1	VLAN 4	10.18.8.98/29 2001:db8: acad: c:98/64 FR80::98		10.18.8.97 N/D N/D
S2	VLAN 4	10.18.8.99/29 2001:db8: acad: c:99/64 FE80::99		10.18.8.97 N/D N/D
PC-A	NIC	Dirección DHCP para IPv4 2001:db8: acad: a:50/64	DHCP asignado	DHCP para puerta de enlace predeterminada IPv4 Fe80/:1
PC_B	NIC	DHCP para dirección IPv4	DHCP asignado	DHCP para puerta de

		2001:db8: acad: b:50/64		enlace predeterminada IPv4 Fe80::1

Parte 1: Inicializar y Recargar y Configurar aspectos básicos

Paso 1: primero se inicializa y se vuelve a cargar el router y los switches

En los siguientes comandos se borra la configuración de inicio y las VLAN del router y de los switches, para luego volver a cargar los dispositivos.

Se accede al router mediante el puerto de consola ingrese al modo EXEC privilegiado con el comando enable.

Router>enable

Con el comando erase startup-config se elimina la configuración de inicio de la memoria de acceso aleatorio no volátil (NVRAM).

Router#erase startup-config

El comando reload es para eliminar la antigua configuración de la memoria. Cuando se reciba el mensaje de continuar con la recarga (proceed with reload). Y volver a cargar el router para eliminar la información.

Router #reload

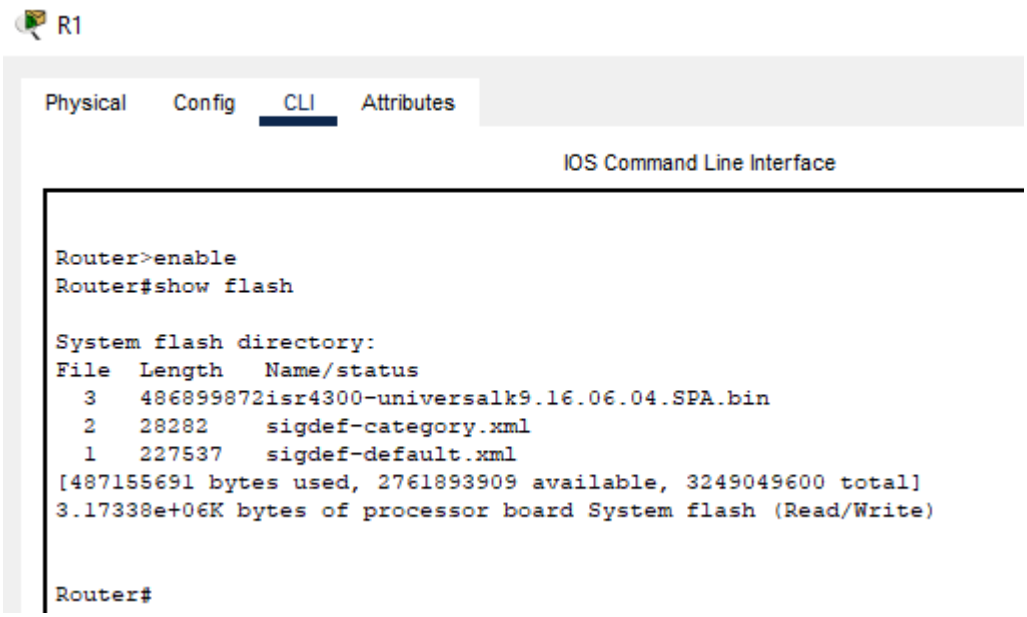
se presiona enter para confirmar la recarga. Si se presiona cualquier otra tecla se anulará la recarga.

Proceed with reload? [confirm]

Una vez que se vuelva a cargar el router, solicita introducir el diálogo de configuración inicial. Se escribe no y presiona Enter.
Would you like to enter the initial configuration dialog? [yes/no]: no

Mostrar si se encontró VLAN.dat y si se crearon VLAN en el router.
En la siguiente figura se muestra con el comando show flash en el router que no aparece la VLAN, por tanto, no se elimina. Sin embargo, se realiza la eliminación para demostración de lo que sucede.

Figura 17. Show flash R1 1



Fuente: autor

Switch 1

Switch> enable
Switch#configure terminal
Se realiza el mismo procedimiento para el switch 1

Se elimina toda configuración

Switch#erase startup-config

Se elimina la vlan

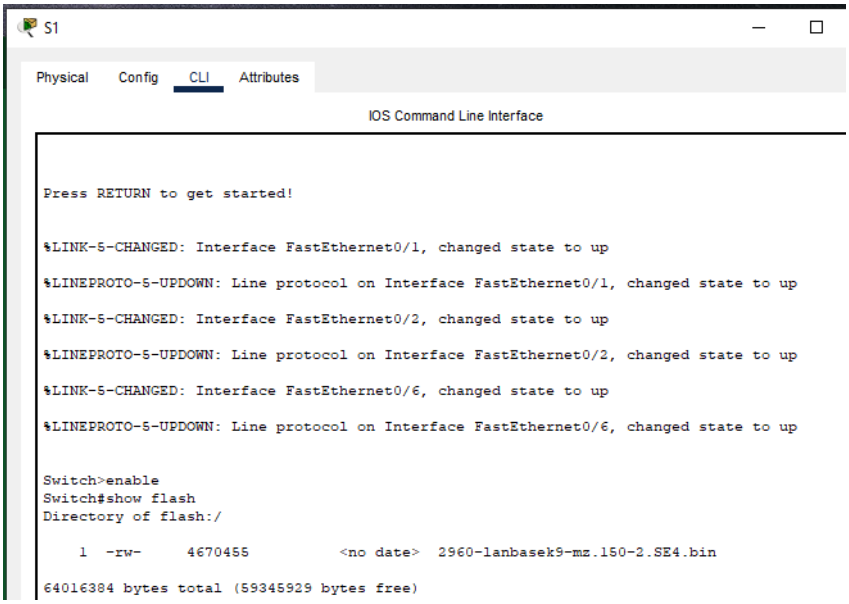
Switch#delete vlan.dat

Switch#reload

Switch> show flash

En la siguiente figura no muestra ninguna vlan

Figura 18. Show flash S1 1



Fuente: autor

No se creó ninguna vlan entonces se puede continuar con la configuración, si apareciera una, se debería eliminar la memoria flash. Borrar el archivo de configuración de inicio y luego recargar el switch.

Después de recargar el switch, se configura la plantilla SDM para que admita IPv6 según sea necesario y se vuelve a cargar el switch

Switch > enable
Activar plantilla predeterminada:

Switch#configure terminal

Habilitar plantilla SDM para IPv4 e IPv6:
Switch(config)#sdm prefer dual-ipv4-andipv6 default

Switch(config) # exit

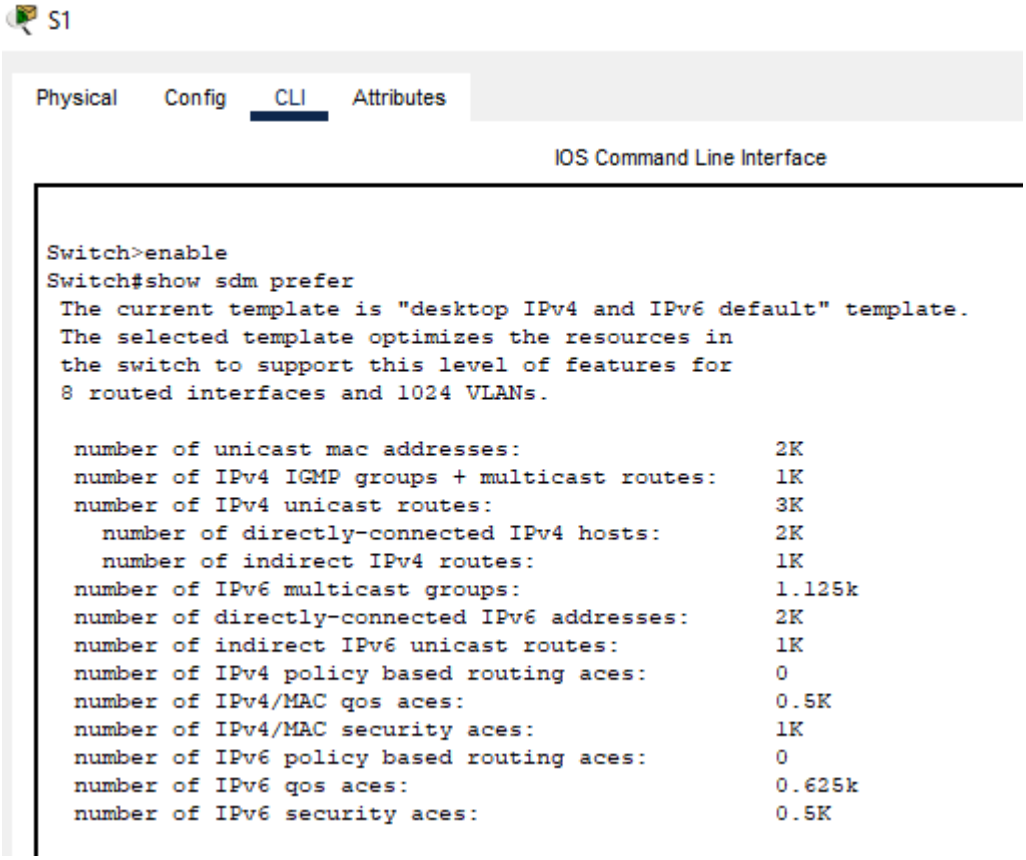
Reiniciar el switch:
Switch # reload
System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]
Se confirma si se quiere cargar nuevamente el switch, muestra la referencia, la versión del switch

Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r) SEC, RELEASE SOFTWARE (fc4) cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/8184K bytes of memory.

Switch # show sdm prefer

En la siguiente figura muestra que soporta ipv6 y ipv4

Figura 19. Show sdm prefer S1 1



Fuente: autor

Switch 2

Switch#enable

Switch#erase startup-config

Switch#delete vlan.dat

Switch#reload

Después de recargar el switch, se configura la plantilla SDM para que admita IPv6 según sea necesario y se vuelve a cargar el switch:

Switch#configure terminal

Habilitar plantilla SDM para IPv4 e IPv6:
Switch(config)#sdm prefer dual-ipv4-andipv6 default

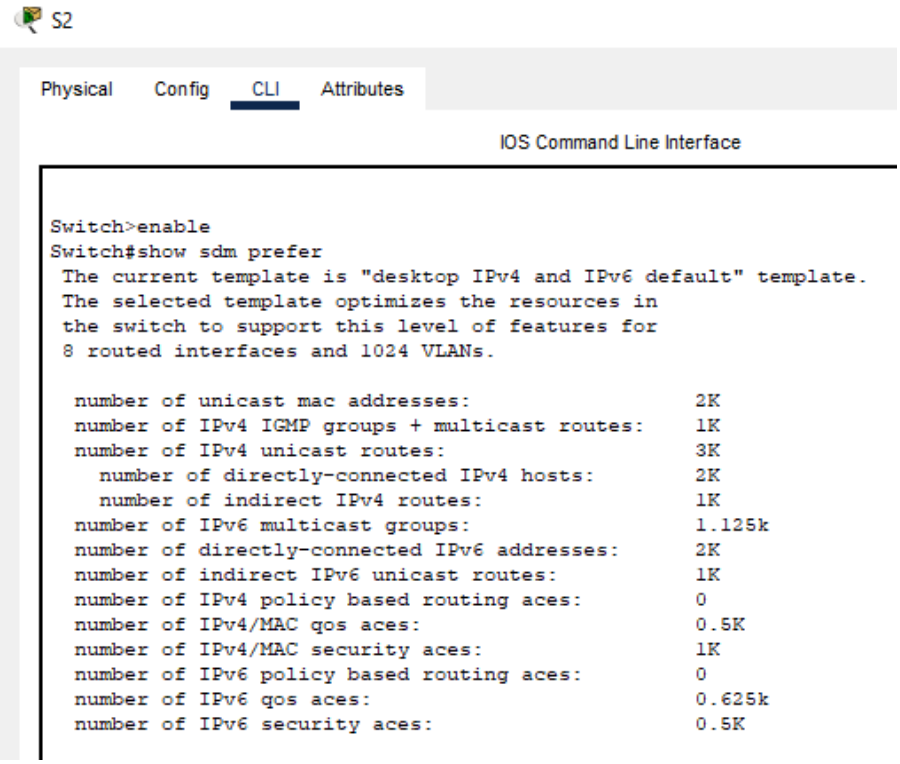
Switch(config) # exit

Reiniciar el switch:
Switch # reload
System configuration has been modified. Save? [yes/no]: y
Building configuration...
[OK]

Se confirma si se quiere cargar nuevamente el switch, muestra la referencia, la versión del switch
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r) SEC, RELEASE SOFTWARE (fc4) cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with 122880K/8184K bytes of memory.

Switch > enable
Activar plantilla predeterminada:
Switch # show sdm prefer

En la siguiente figura muestra que soporta ipv6 y ipv4
Figura 20. Show sdm prefer S2 1



Fuente: autor

Paso 2: configuración R1

En la siguiente tabla se mostrará cada uno de las configuraciones básicas que contiene un router, desde el nombre del router hasta la configuración de la RSA.

Tabla 8. Configuración R1 1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS Nombre del router	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	El DNS viene activado por defecto. Este comando sirve para cuando se cometa un error en el nombre, el enrutador supondrá que debe buscar en el DNS. Pero si se desactiva quiere decir que no está disponible y suspende las búsquedas. Router(config)#no ip domain lookup
Nombre del router	R1 Se asigna el nombre al router como R1, para identificar de otros dispositivos en el entorno lógico: Router(config)#hostname R1
Nombre de dominio	ccna-sa.com Se define un nombre de dominio predeterminado que el Cisco IOS utiliza para completar los nombres del host incompetentes. R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Class Aquí se configura una contraseña para la conexión de consola al modo privilegiado. Se utiliza secret ya que ésta se guarda encriptada en los ficheros de configuración del router. R1(config)#enable secret class

Contraseña de acceso a la consola	Cisco Se genera una segunda contraseña para la conexión de consola al modo de usuario y se utiliza secret también para que esta sea encriptada en los ficheros del router R1(config)#line console 0 R1(config-line) #password cisco R1(config-line) #login R1(config-line) #exit
Establecer la longitud mínima para las contraseñas	5 caracteres El definir la longitud de la contraseña de 5 caracteres hace que la contraseña sea más segura para no ser adivinada o que tenga ataques R1(config)#security password min-length 10
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass Se crea un usuario y contraseña de base local para que con este usuario pueda ingresar a la configuración del router R1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Estas líneas de terminal virtual del router se utiliza para controlar las conexiones telnet entrantes.

	R1(config)#line vty 0 15 R1(config-line) #login local
Configurar VTY solo aceptando SSH	Anteriormente se configura la línea virtual del router con usuario y contraseñas específicas, mientras que con el protocolo SSH lo que hace es encriptar la comunicación entre el cliente, evitando que terceras personas puedan descubrir el usuario y contraseña. R1(config-line) #transport input ssh R1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	Este comando service password-encryption utiliza un cifrado débil a las contraseñas que no están cifradas. R1(config)#service password-encryption
Configure un MOTD Banner	Se configura este banner para mostrar información a usuarios que de pronto estén ingresando y nos son autorizados, como mensajes de emergencia, o mensajes para que el administrador de red lo pueda ver de forma remota. R1(config)#banner motd "R1 Cindy Carolina Poveda Gonzalez Ingenieria de Sistemas"
Habilitar el routing IPv6	Este comando se utiliza para poder configurar cualquier protocolo IPV6, habilitar el router como IPV6

	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Se establece la descripción de ipv4 y ipv6, también se establece la dirección local, R1(config)#interface g0/0/1.20 El siguiente comando sirve para agregar una etiqueta a la trama Ethernet R1(config-subif) #encapsulation dot1q 20 Se coloca el nombre de la vlan R1(config-subif) #description vlan Docentes R1(config-subif) #ip address 10.18.8.1 255.255.255.192 R1(config-subif) #ipv6 address 2001:db8:acad:a::1/64 R1(config-subif) #ipv6 address fe80::1 link-local R1(config-subif) #interface g0/0/1.30 R1(config-subif) #encapsulation dot1q 30 R1(config-subif) #description vlan Estudiantes R1(config-subif) #ip address 10.18.8.65 255.255.255.224 R1(config-subif) #ipv6 address 2001:db8: acad:b::1/64 Se coloca el siguiente link-local de la ipv6 R1(config-subif) #ipv6 address fe80::1 link-local

	R1(config-subif) #interface g0/0/1.40 R1(config-subif) #encapsulation dot1q 40 R1(config-subif) #description vlan Invitados R1(config-subif) #ip address 10.18.8.97 255.255.255.248 R1(config-subif) #ipv6 address 2001:db8:acad:c::1/64 R1(config-subif) #ipv6 address fe80::1 link-local R1(config-subif) #interface g0/0/1.56 R1(config-subif) #encapsulation dot1q 56 Native R1(config-subif) #description vlan Native R1(config-subif) #interface g0/0/1 Y se activa cada una de las interfaces R1(config-if) #no shutdown
Configure el Loopback0 interface	Se establece la interfaz loopback 0 esta sirce para administrar un dispositivo en Cisco IOS, asegura que como mínimo haya una interfaz siempre disponible. R1(config-if) #interface loopback 0 R1(config-if) # %LINK-5-CHANGED: Interface Loopback0, changed state to up

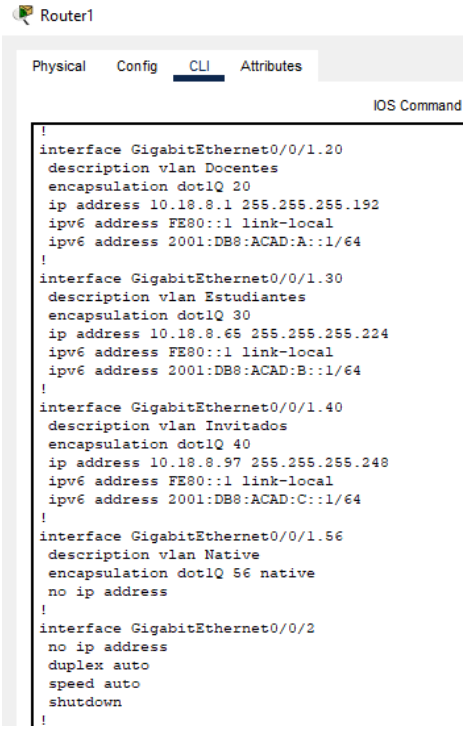
	Aquí muestra que fue activa la interface Se agrega la ipv4 del loopback con su respectiva dirección ipv6 y el link-local R1(config-if) #ip address 209.165.201.1 255.255.255.224 R1(config-if) #ipv6 address 2001:db8: acad:209::1/64 R1(config-if) #ipv6 address fe80::1 link-local R1(config-if) #description Cindy R1(config-if) #exit
Generar una clave de cifrado RSA	La clave de cifrado RSA habilita el servidor SSH en el router para poder generar la clave RSA. Y para habilitarla se usa el comando crypto key rsa: R1(config)#crypto key generate rsa Muestra el nombre del dominio creado anteriormente y el rango de bits disponibles. 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 Al crear la clave se solicita que se introduzca una longitud de módulo, en este caso se coloca 1024, ya que una longitud mayor es más segura, se puede tardar más al generarlo y utilizarla

	How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] R1(config)#exit

Show running-config

En esta figura se muestra la configuración de la VLAN´s con su respectiva descripción, direcciones ipv4 e ipv6 y su respectivo Gateway y link-local.

Figura 21. Show running-config 1



Fuente: autor

Paso 4: configurar S1

En la siguiente tabla se plasma los comandos utilizados para la configuración del switch 1:

Tabla 9. Configuración S1 1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS Nombre del switch	El DNS viene activado por defecto. Este comando sirve para cuando se cometa un error en el nombre, el enrutador supondrá que debe buscar en el DNS Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Se asigna el nombre al switch como S1, para identificar de otros dispositivos en el entorno lógico: Switch(config)#hostname S1
Nombre de dominio	Se define un nombre de dominio predeterminado que el Cisco IOS utiliza para completar los nombres del host incompetentes: S1(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado	Aquí se configura una contraseña para la conexión de consola al modo privilegiado. Se utiliza secret ya que ésta se guarda encriptada en los ficheros de configuración del switch 1 S1(config)#enable secret class S1(config)#line console 0
Contraseña de acceso a la consola	Se genera una segunda contraseña para la conexión de consola al modo de usuario y se utiliza secret también para que esta sea encriptada en los ficheros del switch S1(config-line) #password cisco S1(config-line) #login S1(config-line) #exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S1(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Estas líneas de terminal virtual del switch se utilizan para controlar las conexiones telnet entrantes: S1(config)#line vty 0 15 S1(config-line) #login local
Configurar VTY solo aceptando SSH	S1(config-line) #transport input ssh S1(config-line) #exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configure un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. S1(config)#banner motd "S1 Cindy Carolina Poveda Gonzalez Ingeniera de Sistemas"
Generar una clave de cifrado RSA	a clave de cifrado RSA habilita el servidor SSH en el switch para poder generar la clave RSA. Y para habilitarla se usa el comando crypto key rsa S1(config)#crypto key generate rsa general-key modulus 1024 The name for the keys will be: S1.ccna-sa.com al crear la clave se solicita que se introduzca una longitud de módulo, en este caso se coloca 1024, ya que una longitud mayor es más segura, se puede tardar más al generarlo y utilizarla. % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] *Mar 1 3:1:32.997: %SSH-5-ENABLED: SSH 1.99 has been enabled

	S1(config)#
Configurar interfaz de administraciones (SVI)	Se configura la interface vlan1 con su respectiva dirección IP y máscara de subred, 25 esto para que haya conexión en ambas LAN y para activarla para poder hacer ping con el comando no shutdown: S1(config)#interface vlan 4 S1(config-if) #ip address 10.18.8.98 255.255.255.248 S1(config-if) #ipv6 address 2001:db8: acad:c::98/64 S1(config-if) #ipv6 address fe80::98 link-local S1(config-if) #no shutdown S1(config)#exit
Configuración del Gateway predeterminado	También se configura el Gateway para comunicación entre ambas LAN, entre computadoras: S1(config)#ip default-gateway 10.18.8.97 S1(config)#

Switch 2

La configuración del S2 incluye las siguientes tareas:

Tabla 10. Configuración S2 1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS Nombre del switch	El DNS viene activado por defecto. Este comando sirve para cuando se cometa un error en el nombre, el enrutador supondrá que debe buscar en el DNS: Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Se asigna el nombre al router como R1, para identificar de otros dispositivos en el entorno lógico: Switch(config)#hostname S2
Nombre de dominio	Se define un nombre de dominio predeterminado que el Cisco IOS utiliza para completar los nombres del host incompetentes: S2(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	Aquí se configura una contraseña para la conexión de consola al modo privilegiado S2(config)#enable secret class S2(config)#line console 0
Contraseña de acceso a la consola	S2(config-line) #password cisco S2(config-line) #login

	S2(config-line) #exit
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S2(config)#username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se configura esta línea para todos los usuarios con contraseñas específicas a los usuarios para que puedan configurar de manera local el switch S2(config)#line vty 0 4 S2(config-line) #login local
Configurar VTY solo aceptando SSH	Anteriormente se configura la línea virtual del switch con usuario y contraseñas específicas, mientras que con el protocolo SSH lo que hace es encriptar la comunicación entre el cliente, evitando que terceras personas puedan descubrir el usuario y contraseña. S2(config-line) #transport input ssh S2(config-line) #exit
Cifrar las contraseñas de texto no cifrado	Este comando service password-encryption utiliza un cifrado débil a las contraseñas que no están cifradas S2(config)#service password-encryption
Configure un MOTD Banner	S2(config)#banner motd "S2 Cindy Carolina Poveda Gonzalez Ingeniera de Sistemas"
Generar una clave de cifrado RSA	Módulo de 1024 bits

	S2(config)#crypto key generate rsa general-key modulus 1024 The name for the keys will be: S2.ccna-sa.com % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] *Mar 1 3:1:32.997: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config)#
Configurar interfaz de administraciones (SVI)	Se configura la interface VLAN's con su respectiva dirección IP y máscara de subred, 25 esto para que haya conexión en ambas LAN. S2(config)#interface vlan 40 S2(config-if) #ip address 10.18.8.99 255.255.255.248 S2(config-if) #ipv6 address 2001:db8: acad:c :: 99/64 S2(config-if) #ipv6 address fe80::99 link-local S2(config-if) #description vlan management S2(config-if) #no shutdown S2(config-if) #exit S2(config)# ip default-gateway 10.18.8.97 S2(config-if) #exit
Configuración del Gateway predeterminado	También se configura el Gateway para comunicación entre ambas LAN, entre computadoras:

	S2(config)#ip default-gateway 10.18.8.97

Parte 2: Configuración (VLAN, Trunking, EtherChannel)

Tabla 11. Configuración VLAN S2 1

TAREA	ESPECIFICACIÓN
Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	Se nombra cada una de las vlans S1 Cindy Carolina Poveda Gonzalez Ingenieria de Sistemas User Access Verification Password: S1>enable Password: S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. 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) #

	%LINK-5-CHANGED: Interface Vlan40, changed state to upS1(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 S1(config)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Se crean los troncales 802.1Q que usan la vlan Native con las interfacaz fa0/5 S1(config)#interface fa0/5 S1(config-if) #switchport trunk encapsulation dot1q El siguiente código se utiliza para cambiar al modo de enlace troncal permanente. Este comando es el único método utilizado para configurar las troncales: S1(config-if) #switchport mode trunk Luego muestra que cada uno de las interfaces de Vlan 56 Native fueron encendidas. S1(config-if) #switchport trunk Native vlan 56
Crear un grupo de puertos	S1(config)#interface fa0/5 Se utiliza el siguiente comando

EtherChannel de capa 2 que use interface F0/1 y F0/2 Usar el protocolo LACP para la negociación.	S1(config-if) #switchport trunk encapsulation dot1q Y para implementarla la interface S1(config-if) #switchport mode trunk Para direccionarla a la vlan 56 S1(config-if) # %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down Se da un rango de la interface y luego se enciende. S1(config-if) #switchport trunk Native vlan 56 S1(config-if) #interface range fa0/1-2 S1(config-if-range) #shutdown Aquí muestra que la fastEthernet 0/1 fue encendida %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down S1(config-if-range) #switchport trunk encapsulation dot1q S1(config-if-range) #switchport mode trunk S1(config-if-range) #switchport trunk Native vlan 56 S1(config-if-range)#exit

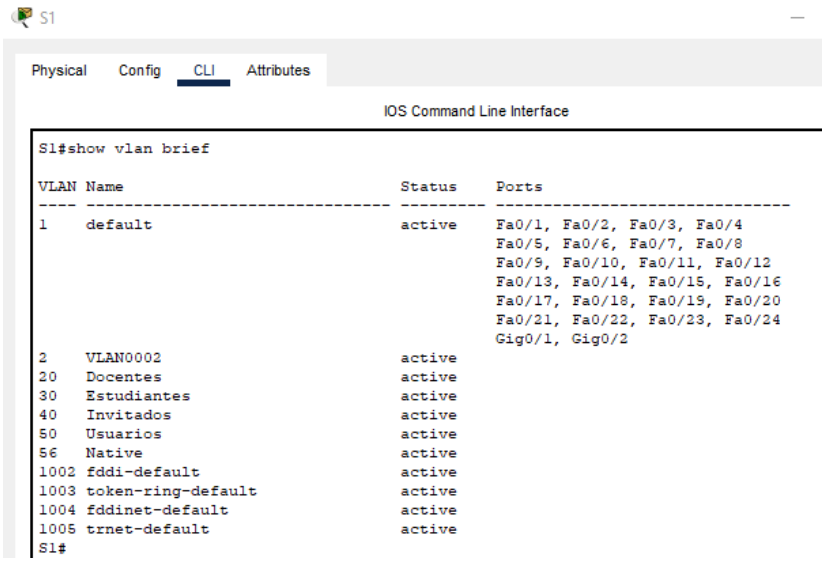
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6 S1(config-if) #interface fa0/6 S1(config-if) #switchport mode acces S1(config-if) #switchport acces vlan 20
Configurar la seguridad del puerto en los puertos de acceso	Este comando lo que hace es sobre escribir el número máximo de direcciones MAC asociadas a la vlan: S1(config-if) #switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	Se aseguran todas las interfaces sin usar, asignándolas a la vlan 50, colocando un rango y dejando un mensaje donde especifique que están apagadas o no disponibles. S1(config-if) #interface range fa0/3-4 S1(config-if-range) #shutdown %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down S1(config-if-range) #switchport acces vlan 50 S1(config-if-range) #description No está disponible S1(config-if-range) #shutdown

	S1(config-if-range) #interface range fa0/7-24 S1(config-if-range) #switchport acces vlan 50 S1(config-if-range) #description No está disponible S1(config-if-range) #shutdown S1(config-if-range) #interface range g0/1-2 S1(config-if-range) #switchport mode acces S1(config-if-range) #switchport acces vlan 50 S1(config-if-range) #description No est disponible S1(config-if-range) #shutdown %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down S1(config-if-range) #
Se habilita nuevamente las interfaces 1 y 2	Anteriormente están deshabilitadas para que no genere problemas, y después de configurar las vlan e interfaces se encienden nuevamente las dos interfaces: S1(config)#interface range fa0/1-2 S1(config-if-range) #interface range fa0/1-2 S1(config-if-range) #no shutdown

	%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down S1(config-if-range) #exit S1(config)#exit

En la siguiente figura muestra las 5 interfaces con su respectivo número de asignación, nombre y que están activas.

Figura 22. Show vlan brief S1 1



Fuente: autor

Paso 5: configurar el S2

En la siguiente tabla se muestra la configuración del switch 1 donde se asignan las vlan, con su respectivo nombre:

Tabla 12. Configuración vlan S2 1

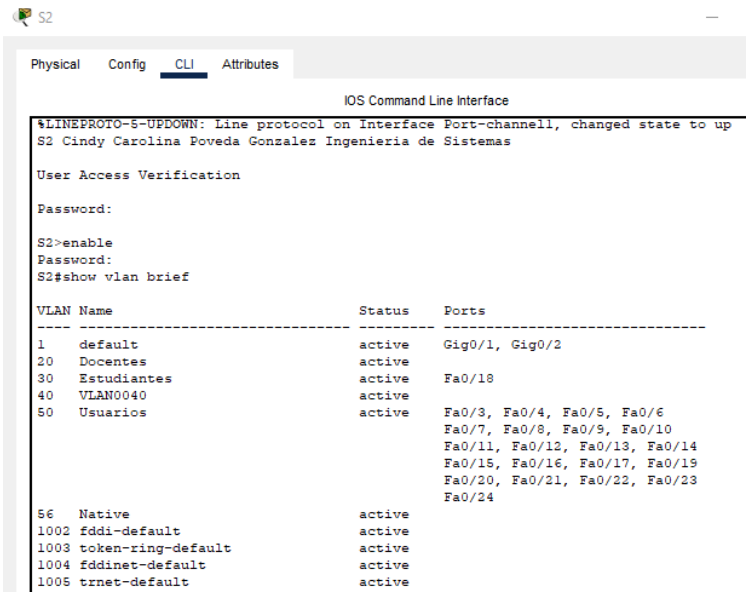
TAREA	ESPECIFICACIÓN
Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S2 Cindy Carolina Poveda Gonzalez Ingenieria de Sistemas User Access Verification Password: S2>enable Password: S2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#vlan 20 S2(config-vlan) #name Docentes S2(config-vlan) #vlan 30 S2(config-vlan) #name Estudiantes S2(config-vlan) #vlan 40 S2(config-vlan) # %LINK-5-CHANGED: Interface Vlan40, changed state to up S2(config-vlan) #vlan 50 S2(config-vlan) #name Usuarios S2(config-vlan) #vlan 56 S2(config-vlan) #name Native S2(config-vlan) #Exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Se crean los troncos de los puertos fa01 y 02 S2(config)#interface range fa0/1-2 S2(config-if-range) #shutdown El siguiente código se utiliza para cambiar al modo de enlace troncal permanente. Este comando es el único método utilizado para configurar las troncales: S2(config-if-range) #switchport trunk encapsulation dot1q S2(config-if-range) #switchport mode trunk S2(config-if-range) #switchport trunk Native vlan 56
crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Se crea el etherchannel que utiliza la interfaz 1 y 2 con el siguiente comando, se usa LACP para crear el grupo numero 1 S2(config-if-range) #channel-group 1 mode active Luego se entra a la interfaz por medio del comando: S2(config-if-range) # Creating a port-channel interface Port-channel 1 Y configurar las troncales S2(config-if-range) #interface port-channel 1

	S2(config-if) #switchport trunk encapsulation dot1q S2(config-if) #switchport mode trunk S2(config-if) #switchport trunk Native vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Se configura un puerto de acceso para la vlan 30 Estudiantes que use la interfaz fa0/18: S2(config-if) #interface fa0/18 S2(config-if) #switchport mode acces S2(config-if) #switchport acces vlan 30 S2(config-if) #
Configure port-security en los access ports	Y que permita el acceso a 4 direcciones MAC S2(config-if) #switchport port-security maximum 4 Se activa la seguridad de la interfaz estableciendo mínimo 4 direcciones.
Asegure todas las interfaces no utilizadas	Se establecen los rangos de las interfaces que no van a ser usadas: S2(config-if) #interface range fa0/3-17 S2(config-if-range) #switchport mode access S2(config-if-range) #switchport access vlan 50 S2(config-if-range) #description No está disponible S2(config-if-range) #shutdown %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

	S2(config-if-range) #interface range fa0/19-24 S2(config-if-range) #switchport mode access S2(config-if-range) #switchport access vlan 50 S2(config-if-range) #description No está disponible S2(config-if-range) #shutdown %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
Se habilita nuevamente las dos interfaces 1 y 2	S2(config)#interface range fa0/1-2 S2(config-if-range) #interface range fa0/1-2 S2(config-if-range) #no shutdown S2(config-if-range) # %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Figura 23. Show vlan brief S2 1



Fuente: autor

Parte 3: configurar soporte de host

Paso1: configure R1

Tabla 13. Configuración R1-soporte host 1

TAREA	ESPECIFICACIÓN
Configure Default Routing	Al router se le asigna una ruta predeterminada ipv4 y ipv6, de las cuales direccionaran el tráfico a la interfaz loopback 0 R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0

	%Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route: :/0 loopback 0 Es una ruta estática para conectar con internet
Configurar IPv4 DHCP para VLAN 2	Se configura ipv4 DHCP con la vlan 20 Docentes conformada por las ultimas 10 direcciones de subred: R1(config)#ip dhcp excluded-address 10.18.8.1 10.18.8.52 R1(config)#ip dhcp pool vlan20-Docentes R1(dhcp-config) #network 10.18.8.0 255.255.255.192 R1(dhcp-config) #default-router 10.18.8.1 R1(dhcp-config) #domain-name unad-ccna-sa.net R1(dhcp-config) #exit
Configurar DHCP IPv4 para VLAN 3	Se configura ipv4 DHCP con la vlan 30 Estudiantes conformada por las ultimas 10 direcciones de subred, con su respectiva mascara, red network., puerta de enlace y configuración del dominio.: R1(config)#ip dhcp excluded-address 10.18.8.65 10.18.8.84 R1(config)#ip dhcp pool vlan30-Estudiantes R1(dhcp-config) #network 10.18.8.64 255.255.255.224 R1(dhcp-config) #default-router 10.18.8.65 R1(dhcp-config) #domain-name unad-ccna-sb.net R1(dhcp-config) #exit

	R1(config)#

Paso 2: configurar los servidores

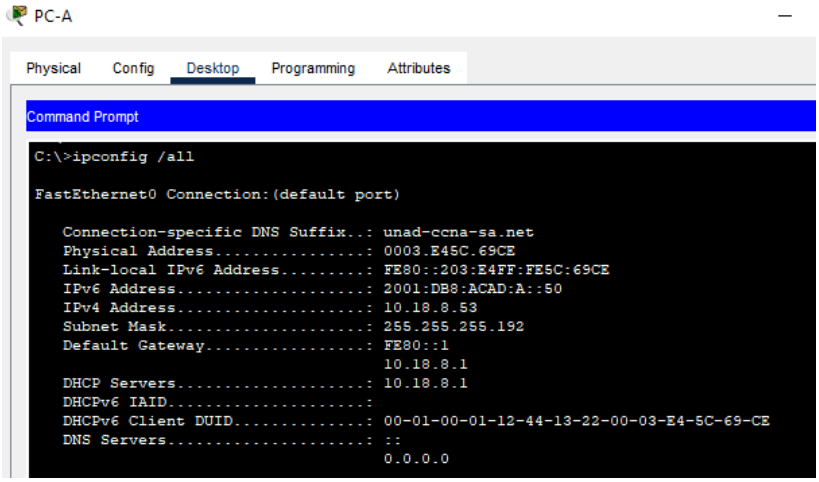
Se configura el quipo A donde se asigna dhcp y el automáticamente arroja la dirección, submascara, Gateway y el link local de la ipv6, se muestra en la siguiente tabla:

Tabla 14. Config PC-A 1

Configuración de red de PC-A	
Dirección IP	10.18.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.18.8.1
Gateway predeterminado IPv6	FE80::1

En la siguiente figura se muestra la configuración del pc-A donde arroja el nombre del dominio, la descripción física, el link-local de la ipv6, la dirección de ipv6 la direcciones y Gateway de la ipv4 y la dirección del servidor DHCP.

Figura 24. ipconfig /all PC-A 1



Fuente: autor

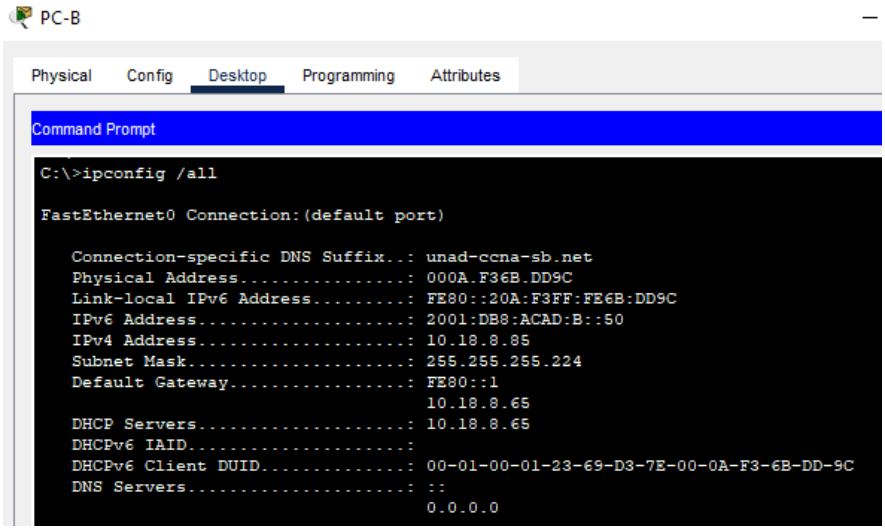
Se configura el quipo B donde se asigna dhcp y el automáticamente arroja la dirección, submascara, Gateway y el link local de la ipv6, se muestra en la siguiente tabla:

Tabla 15. Configuración PC-B 1

Configuración de red de PC-B	
Descripción	Por DHCP
Dirección física	FE80::20A:F3FF: FE6B:DD9C
Dirección IP	10.18.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.18.8.65
Gateway predeterminado IPv6	FE80::1

En la siguiente figura se muestra la configuración del pc-A donde arroja el nombre del dominio, la descripción física, el link-local de la ipv6, la dirección de ipv6 la direcciones y Gateway de la ipv4 y la dirección del servidor DHCP.

Figura 25. ipconfig /all PC-B 1



Fuente: autor

Parte 4: probar y verificar la conectividad de extremo a extremo.

En la siguiente tabla se muestra la conectividad de cada uno de los pc entre los dispositivos de red:

Tabla 16. Conectividad 1

Desde	A		Dirección IP	Resultados ping
PC-A	R1, G0/0/1.20	IPv4	10.18.8.1	Completada
		IPv6	2001:db8: acad: a::1	SI respuesta
	R1, G0/0/1.30	IPv4	10.18.8.65	Si respuesta
		IPv6	2001:db8: acad: b::1	Si respuesta
	R1, G0/0/1.40	IPv4	10.18.8.97	Si respuesta
		IPv6	2001:db8: acad: c::1	No respuesta
	S1, VLAN 40	IPv4	10.18.8.98	No completa
		IPv6	2001:db8: acad:c::98	No completa
	S2, VLAN 40	IPv4	10.18.8.99	No completa
		IPv6	2001:db8: acad:c::99	no
	PC-B	IPv4		

		IPv6	2001:db8: acad: b::50	Si respuesta
	R1 Bucle 0	IPv4	209.165.201.1	Si respuesta
		IPv6	2001:db8: acad: a::1	Si respuesta
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Si respuesta
		IPv6	2001:db8: acad:209::1	
	R1, G0/0/1.20	IPv4	10.18.8.1	Si respuesta
		IPv6	2001:db8: acad: a::1	Si respuesta
	R1, G0/0/1.30	IPv4	10.18.8.65	Si respuesta
		IPv6	2001:db8: acad: b::1	Si respuesta
	R1, G0/0/1.40	IPv4	10.18.8.97	Si respuesta
		IPv6	2001:db8: acad: c::1	Si respuesta
	S1, VLAN 40	IPv4	10.18.8.98	Si respuesta
		IPv6	2001:db8: acad: c::98	No respuesta
	S2, VLAN 40	IPv4	10.18.8.99	Si respuesta
		IPv6	2001:db8: acad: c::99	No respuesta

Ping:

Desde: PC-A

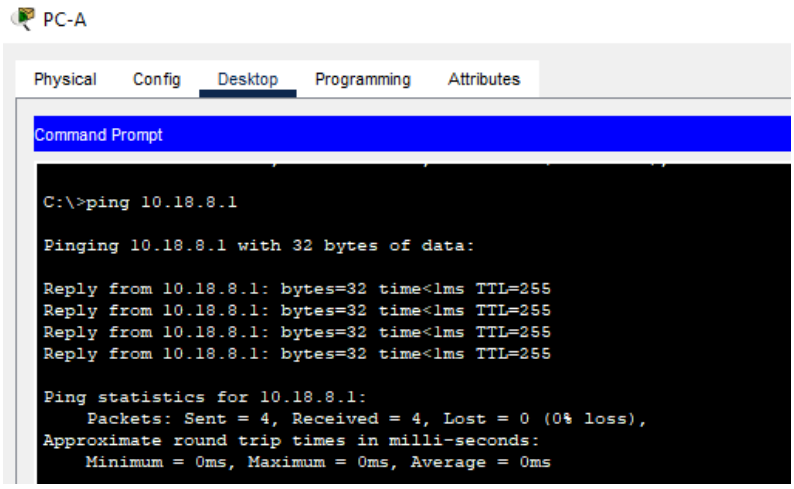
A: R1, G0/0/1.20

Dirección IP: 10.18.8.1

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 10.18.8.1 que es la interfaz del Router G 0/0/1.20, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 26. A = R1 G0/0/1.20 IPV4 1



Fuente: autor

Desde: PC-A

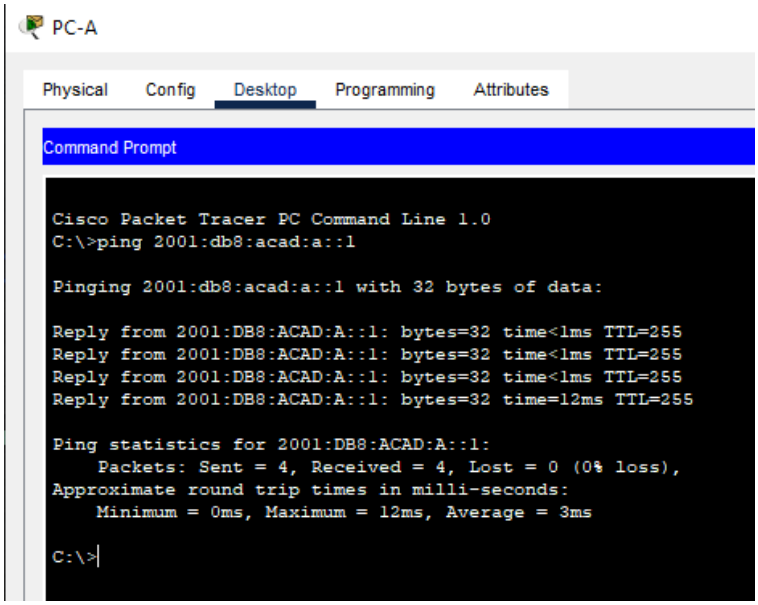
A: R1, G0/0/1.20

Dirección IP: 2001:db8:acad:a::1

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:a::1 que es la interfaz del Router G 0/0/1.20 , logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 27. A: R1, G0/0/1.20 IPV6 1



Fuente: autor

Desde: PC-A

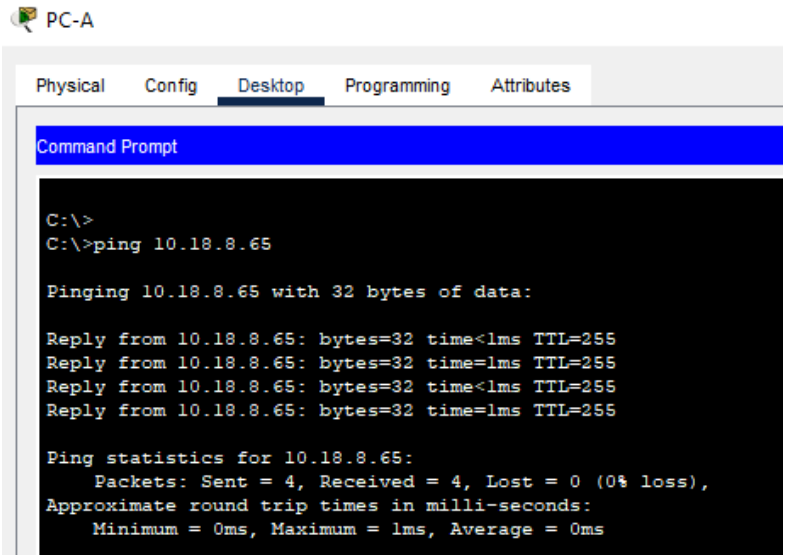
A: R1, G0/0/1.30

Dirección IP: 10.18.8.65

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 10.18.8.65 que es la interfaz del Router G 0/0/1.30, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 28. A: R1, G0/0/1.30 IPV4 1



Fuente: autor

Desde: PC-A

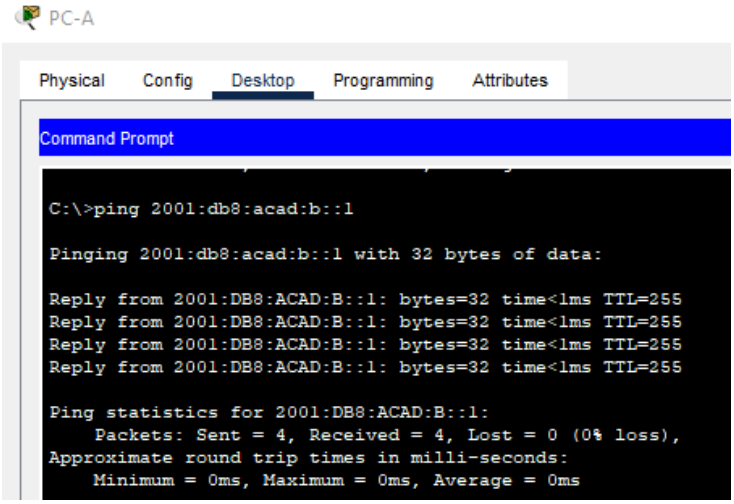
A: R1, G0/0/1.30

Dirección IP: 2001:db8:acad:b::1

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:b::1 que es la interfaz del Router G 0/0/1.30, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 29. A: R1, G0/0/1.30 ipv6 1



Fuente: autor

Desde: PC-A

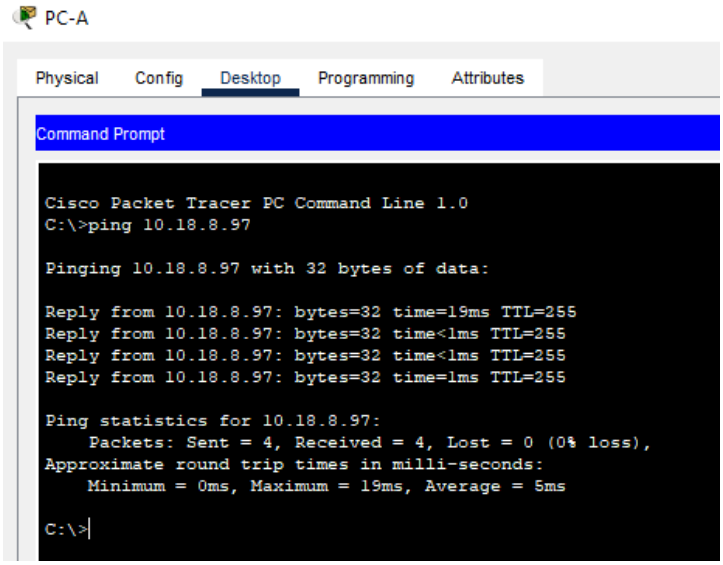
A: R1, G0/0/1.40

Dirección IP: 10.18.8.97

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 10.18.8.97 que es la interfaz del Router G 0/0/1.40, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 30. A: R1, G0/0/1.40 ipv4 1



Fuente: autor

Desde: PC-A

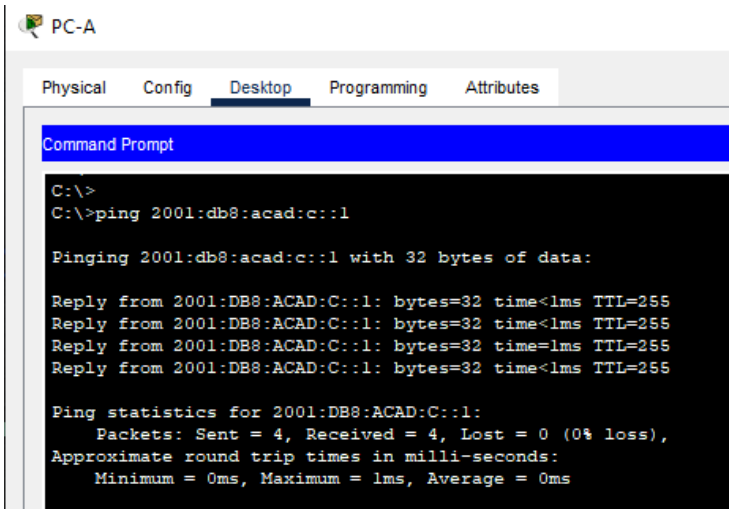
A: R1, G0/0/1.40

Dirección IP: 2001:db8:acad:c::1

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:c::1 que es la interfaz del Router G 0/0/1.40, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 31. A: R1, G0/0/1.40 ipv6 1



Fuente: autor

Desde: PC-A

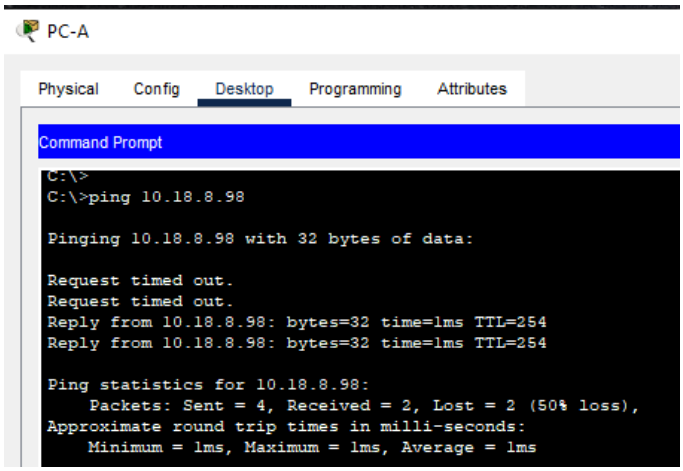
A: S1 vlan 40

Dirección IP: 10.18.8.98

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 10.18.8.98 que es la interfaz S1 VLAN 40 y primero dice que el tiempo de espera está agotado, luego logró enviar 3 paquetes de los cuales solo recibió 3 en un tiempo estimado de 1 ms, 2 archivos se perdieron.

Figura 32. A: S1 vlan 40 IPV4 1



Fuente: autor

Desde: PC-A

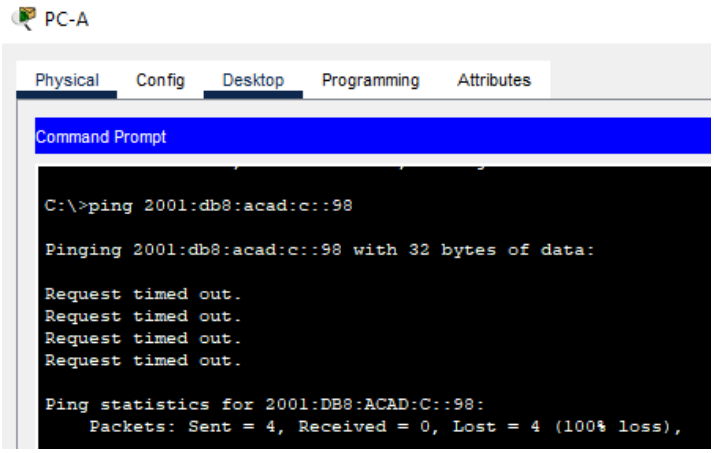
A: S1 vlan 40

Dirección IP: 2001:db8:acad:c::98

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:c::98 que es la interfaz S1 VLAN 40, no logra enviar ningún paquete.

Figura 33. A: S1 vlan 40 ipv6 1



Fuente: autor

Desde: PC-A

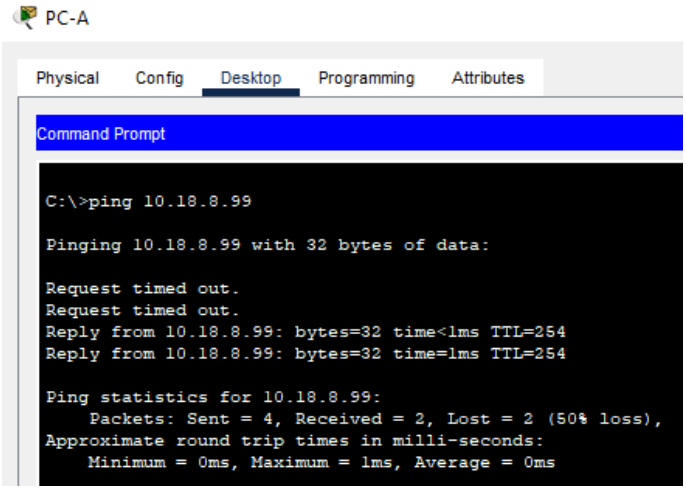
A: S2 vlan 40

Dirección IP: 10.18.8.99

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 10.18.8.99 que es la interfaz S2 VLAN 40 y primero dice que el tiempo de espera está agotado, luego logró enviar 2 paquetes de los cuales solo recibió 2 en un tiempo estimado de 1 ms, 2 archivos se perdieron.

Figura 34. A: S2 vlan 40 IPV4 1



Fuente: autor

Desde: PC-A

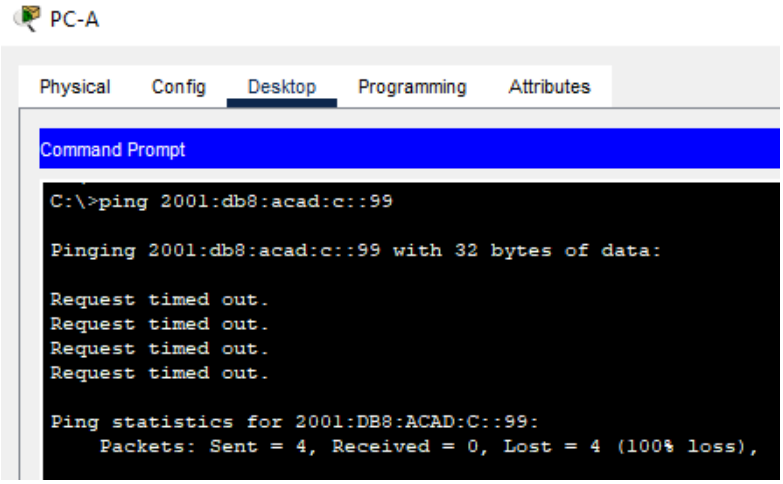
A: S2 vlan 40

Dirección IP: 2001:db8:acad:c::99

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:c::99 que es la interfaz S2 VLAN 40, no logra enviar ningún paquete:

Figura 35. A: S2 vlan 40 IPV6 1



Fuente: autor

Pc-b

Desde: PC-A

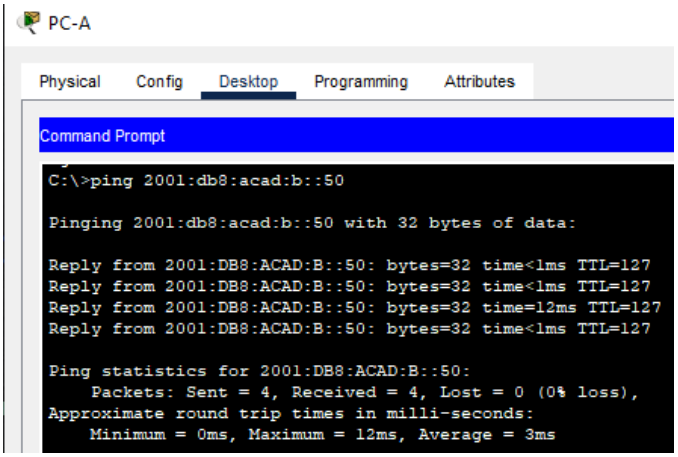
A: PC- B

Dirección IP: 2001:db8:acad:b::50

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:b::50 que es el equipo del pc-b, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 36. A: PC- B IPV6 1



Fuente: autor

Desde: PC-A

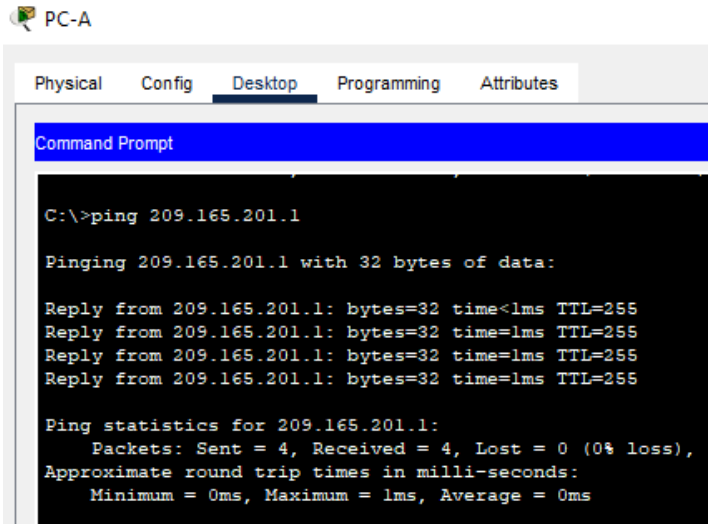
A: R1 bucle 0

Dirección IP: 209.165.201.1

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 209.165.201.1 que es el R1 Bucle, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 37. A: R1 bucle 0 ipv4 1



Fuente: autor

Desde: PC-A

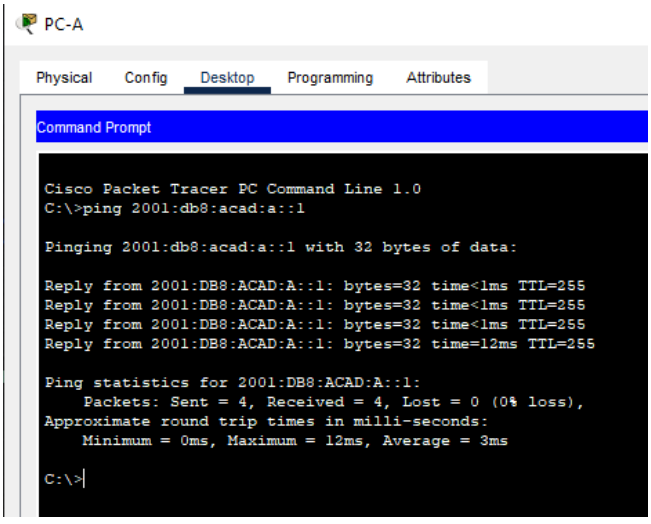
A: R1 bucle 0

Dirección IP: 2001:db8:acad:a::1

Resultado ping:

Desde la computadora PC-A se hace ping a la dirección 2001:db8:acad:a::1 que es la interfaz del R1 BUCLE 0 logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 38. A: R1 bucle 0 IPV6 1



Fuente: autor

Desde: PC-B

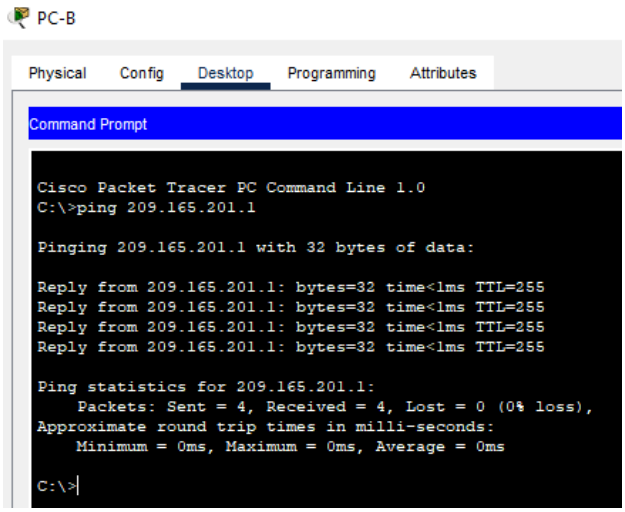
A: R1 bucle 0

Dirección IP: 209.165.201.1

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 209.165.201.1 que es la interfaz del R1 BUCLE 0, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 39. A: R1 bucle 0 ipv4 1



Fuente: autor

Desde: PC-B

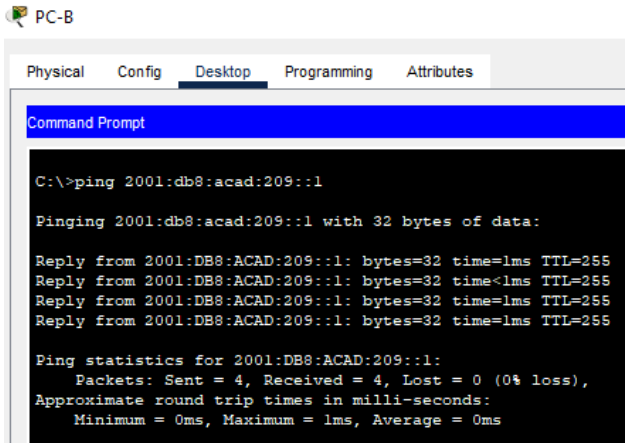
A: R1 bucle 0

Dirección IP: 2001:db8:acad:209::1

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 2001:db8:acad:209::1 que es la interfaz del R1 BUCLE 0, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 40. A: R1 bucle 0 IPV6 1



Fuente: autor

Desde: PC-B

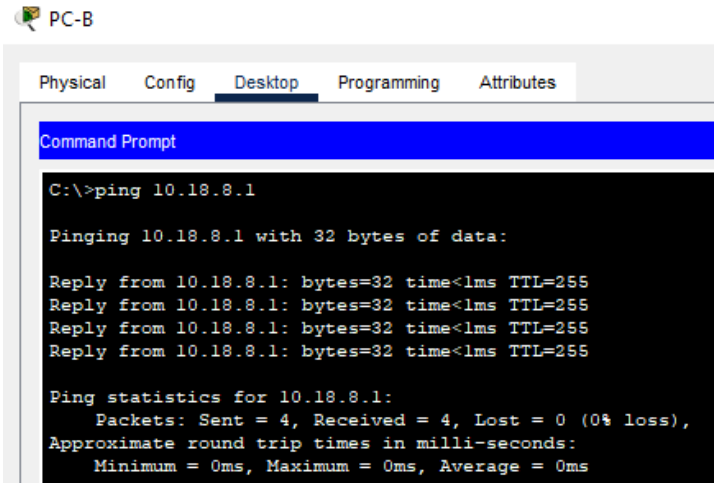
B: R1 g0/0/1.20

Dirección IP: 10.18.8.65

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 10.18.8.65 que es la interfaz del Router G 0/0/1.20, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 41. B: R1 g0/0/1.20 IPV4 1



Fuente: autor

Desde: PC-B

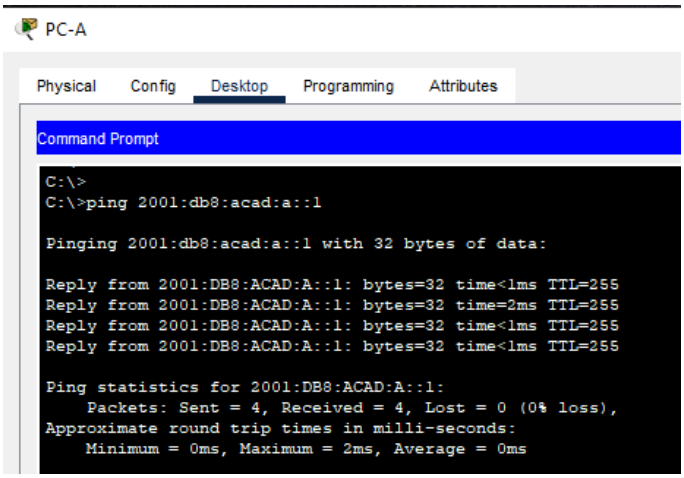
B: R1 g0/0/1.20

Dirección IP: 2001:db8:acad:a::1

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 2001:db8:acad:a::1 que es la interfaz del Router G 0/0/1.20, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 42. B: R1 g0/0/1.20 IPV6 1



Fuente: autor

Desde: PC-B

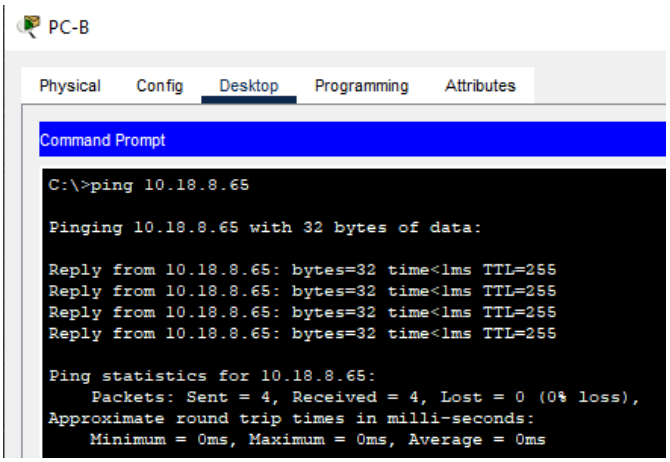
B: R1 g0/0/1.30

Dirección IP: 2001:db8:acad:a::1

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 10.18.8.65 que es la interfaz del Router G 0/0/1.30, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 43. B: R1 g0/0/1.30 ipv4 1



Fuente: autor

Desde: PC-B

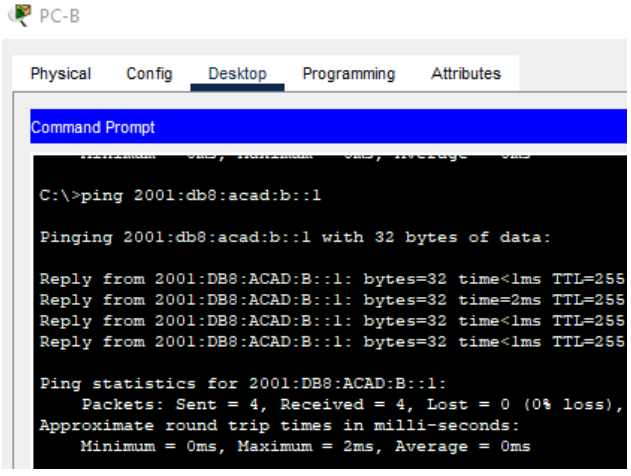
B: R1 g0/0/1.30

Dirección IP: 2001:db8:acad:B::1

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 2001:db8:acad:B::1 que es la interfaz del Router G 0/0/1.30, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 44. B: R1 g0/0/1.30 IPV6 1



Fuente: autor

Desde: PC-B

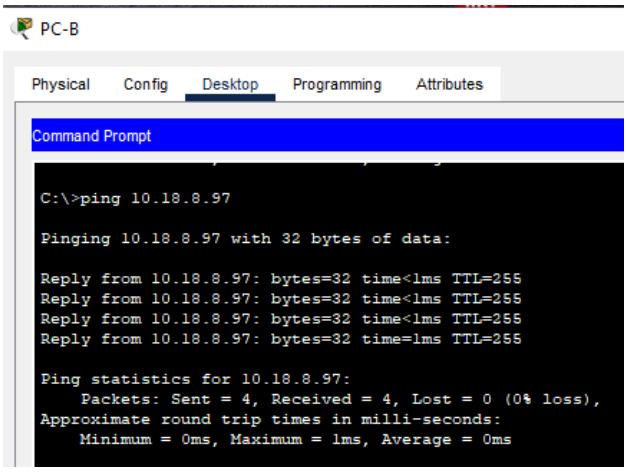
B: R1 g0/0/1.40

Dirección IP: 10.18.8.97

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 10.18.8.97 que es la interfaz del Router G 0/0/1.40, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 45. B: R1 g0/0/1.40 IPV4 1



Fuente: autor

Desde: PC-B

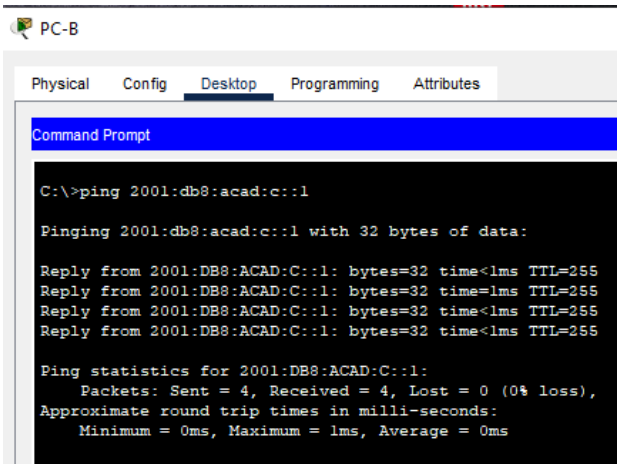
B: R1 g0/0/1.40

Dirección IP: 2001:db8:acad:C::1

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 2001:db8:acad:C::1 que es la interfaz del Router G 0/0/1.40, logra enviar 4 paquetes de los cuales recibe 4 en un tiempo estimado de 0 ms

Figura 46. B: R1 g0/0/1.40 IPV6 1



Fuente: autor

Desde: PC-B

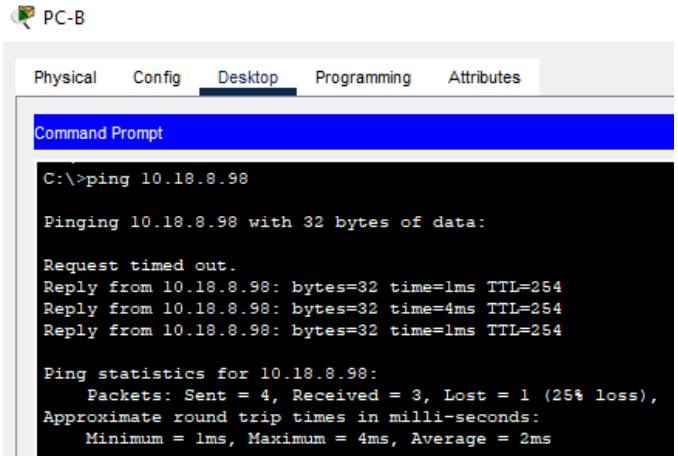
B: S1 vlan 40

Dirección IP: 10.18.8.97

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 10.18.8.98 que es la interfaz del S1 vlan 40, logra enviar 3 paquetes de los cuales recibe 3 y se pierde 1, con un tiempo estimado de 0 ms

Figura 47. B: S1 vlan 40 IPV4 1



Fuente: autor

Desde: PC-B

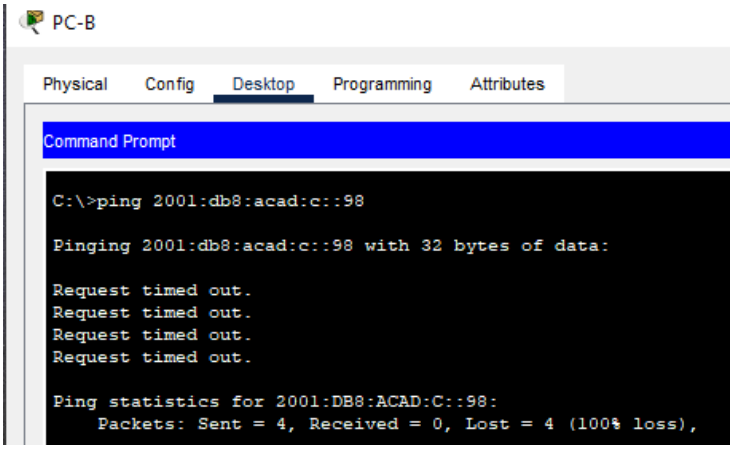
B: S1 vlan 40

Dirección IP: 2001:db8:acad:c::98

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 2001:db8:acad:c::98 que es la interfaz S1 VLAN 40, no logra enviar ningún paquete.

Figura 48. B: S1 vlan 40 IPV6 1



Fuente: autor

Desde: PC-B

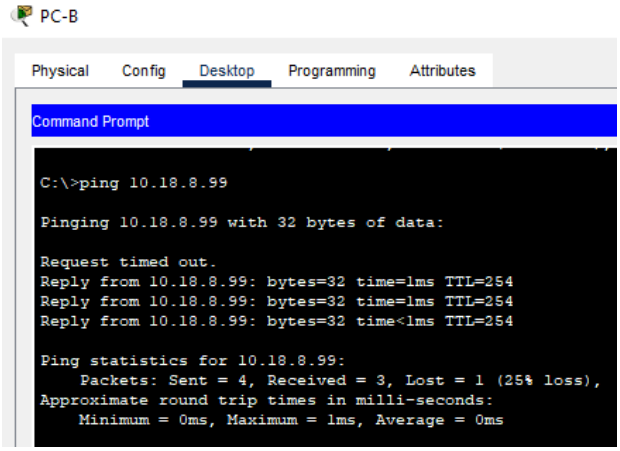
B: S2 vlan 40

Dirección IP: 2001:db8:acad:c::98

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 10.18.8.99 que es la interfaz del S2 vlan 40, logra enviar 3 paquetes de los cuales recibe 3 y se pierde 1, con un tiempo estimado de 0 ms

Figura 49. B: S2 vlan 40 IPV4 1



Fuente: autor

Desde: PC-B

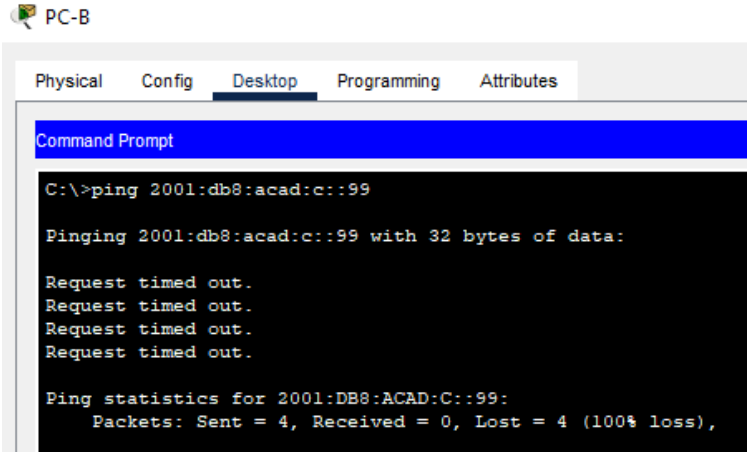
B: S2 vlan 40

Dirección IP: 2001:db8:acad:c::99

Resultado ping:

Desde la computadora PC-B se hace ping a la dirección 2001:db8:acad:c::99 que es la interfaz S2LAN 40, no logra enviar ningún paquete.

Figura 50. B: S2 vlan 40 IPV6 1



Fuente: autor

CONCLUSIONES

Con esta actividad se percibe lo mucho que son importantes las redes de telecomunicación en la sociedad, y de lo necesarias que se volvieron, así como, saber los componentes que se utilizan para realizar diferentes instalaciones de red, en diferentes ámbitos, a pesar de que solo se puede ver y configurar los dispositivos finales, intermediarios por medio del simulador cada red, el análisis que debe hacer una persona encargada de un diseño o implementación revisando cada componente, herramienta, servicios, dispositivos, se nota lo grandísimo que es este medio, y el cuidado que debe tenerse a la hora de desarrollar una tarea, por más mínima que sea.

La plataforma de CISCO nos brinda un trabajo virtual que nos permite adquirir conocimiento, desarrollar habilidades para aportar soluciones a problemas reales de la vida cotidiana en redes informáticas, el desarrollar la configuración de una red pequeña del escenario uno, utilizando la herramienta packet tracer, lo enseña a analizar, a diseñar los esquemas de direcciones para permitir administrar de manera más eficiente la capacidad de las redes, como también que estas puedan crecer según los cambios del tiempo.

Realizando los ejercicios, aparecen problemas a resolver como en el caso del estudiante 1 configurando la SVI VLAN1, a esta se le configura la interfaz, y en seguida se enciende, pero al realizar ping en cada uno de los dispositivos y no me conectó con la primera LAN ni la segunda, entonces realicé la configuración de la interfaz de la VLAN2 en el switch y le di encender. Cuando realicé nuevamente la verificación de transmisión de datos, me funciono en cada uno de los dispositivos, hay que entender como es el funcionamiento de cada dispositivo para así poder configurarlos al igual que utilizar la lógica.

En el segundo escenario se utiliza el switch 3560 uno de los que permite configurar redes ipv6, administración de puertos, configuración de “doble pila” y VLAN. El uso de subredes mediante administración de VLAN, encapsulamiento de dot1q indica que la configuración básica de los enrutadores y conmutadores utilizados ha cambiado. Una red que escala el número de dispositivos que queremos gestionar, implementando un modo “trunk” de su comunicación y maximizando la utilidad de los elementos. Se utiliza en la red para configurar.

BIBLIOGRAFÍA

CISCO. “Crear una red pequeña”. {En línea}. {2020}. Disponible en: https://contenthub.netacad.com/itn/17.0.1

IBM. “Lenguaje de control de datos”. {En línea}. {03 de agosto de 2021}. Disponible en: https://normasicontec.co/bibliografia/.

IBM.” OSPF (open shortest path first)”. {En línea}. {14 de abril de 2021}. Disponible en: https://www.ibm.com/docs/es/i/7.2?topic=routing-open-shortest-path-first

MARTINEZ, Víctor. Configuración de RIPv2 (protocolo dinámico). (en línea). (25 febrero de 2013). Disponible en: Configuración de RIPv2 (protocolo dinámico) - (theosnews.com)

ANEXO

Enlace de descarga de archivo de simulación.

https://drive.google.com/file/d/1FQr4s5E1AmWwK_1ZAZLcyZx50O9Wre1V/view?usp=share_link