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

LEIDY JOHANA RINCON RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERIA DE SISTEMAS

CHIPAQUE

2022

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

LEIDY JOHANA RINCON RIVERA

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

PAULITA FLOR

DIRECTORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERIA DE SISTEMAS

CHIPAQUE

2022

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CHIPAQUE, 27 DE NOVIEMBRE DE 2022

AGRADECIMIENTO

En primer lugar, agradezco infinitamente a Dios por permitirme mejorar. Estoy constantemente agradecido con mi familia, mis padres, por su apoyo. Me han dado lo que es posible lograr a lo largo de mi carrera. Estoy agradecido con la Universidad Nacional Abierta y a Distancia UNAD gracias al apoyo de todos, la que me permitió ser profesional con el apoyo de los todos los tutores y de más personal.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURA

GLOSARIO

Cisco: es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa, también presta el servicio de soluciones de red, su objetivo es conectar a todos y demostrar las cosas asombrosas que se pueden lograr con una visión clara del futuro.[1]

Lan: Red de Área Local (LAN) (Local Área Network) Red de comunicación entre ordenadores situados en el mismo edificio o en edificios cercanos, de forma que permite a sus usuarios el intercambio de datos y la compartición de recursos.[2]

RED: La red informática nombra al conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios. Puede a su vez dividirse en diversas categorías, según su alcance (red de área local o LAN, red de área metropolitana o MAN, red de área amplia o WAN, etc.), su método de conexión (por cable coaxial, fibra óptica, radio, microondas, infrarrojos) o su relación funcional (cliente-servidor, persona a persona), entre otras.[3]

SSH: es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente.[4]

Tracert: es una utilidad similar a ping pero que nos muestra información más detallada acerca de los saltos que va dando el paquete hasta llegar al destino. Esto es especialmente interesante cuando tenemos problemas con nuestra conexión, pero no sabemos exactamente qué es lo que está fallando o hasta dónde llega la continuidad de la red.[5]

[1] ¿Qué es Cisco? | Cisco definición - Netec Global Knowledge.
[2] Definición Red de Área Local (LAN). (s. f.).
[3] Definición de red - Definicion.de. (s. f.).
[4] Protocolo SSH. (s. f.)
[5] CASTILLO,Jose Antonio, Comando tracert o traceroute, que es y para utilizarlo (2018)

Wan: Una red de área amplia (WAN) es una red que existe en una zona geográfica amplia. Tu módem envía y recibe información de Internet a través del puerto WAN.[6]

[6] WAN y LAN - Ayuda de Google Nest. (s. f.).

RESUMEN

Este trabajo propone avances correspondientes al desarrollo del diplomado CISCO CCNA con enfoque de una profundización denominada "Proyecto Aplicado", el director del curso propone dos escenarios con características y requisitos específicos, donde el primer escenario se desarrollará en base al tema del Módulo 1. Aplicar los conocimientos adquiridos en las Unidades 1, 2, 3, 4, 5

En el primer escenario, se configurará una pequeña red de dispositivos. En este se configura un router, un swicth y dispositivos y diseñar esquemas de direccionamiento IPv4 para la LAN recomendada. De igual manera el router y switch se deben configurar de forma segura y adecuada para su funcionamiento correcto.

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

Palabras claves: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

This work proposes corresponding to the development of the CISCO CCNA diploma with an in-depth approach called "Applied Project", the director of the course proposes two advanced scenarios with specific characteristics and requirements, where the first scenario will be developed based on the topic of Module 1. Apply the knowledge acquired in Units 1, 2, 3, 4, 5

In the first scenario, a small network of devices will be set up. It configures a router, switch, and devices, and designs IPv4 addressing schemes for the recommended LAN. In the same way, the router and switch must be configured in a safe and adequate way for its correct operation.

In the second scenario, the devices of a small network will be configured. This will go on to configure a router, a switch, and equipment that supports both IPv4 and IPv6 connectivity for the supported hosts. The router and switch must also be managed securely. You will configure routing between VLANs, DHCP, Etherchannel, and port-security.

Keywords: CISCO, CCNA, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

El presente trabajo tiene como objetivo utilizar la modalidad “Proyecto Aplicado”, del diplomado como opción de grado CISCO CCNA, en donde la directora del curso propone dos escenarios, estos cuenta con diversas características y requerimientos específicos con el fin de establecer y utilizar las herramientas de simulación y laboratorios de acceso remoto para realizar escenario LAN/WAN que permitan fundamentar un análisis de los diversos protocolos y métricas que se requiere para un enrutamiento.

El principal beneficio que nos brindan estas redes es que nos permiten compartir los recursos disponibles entre los distintos equipos que tenemos, ya sean base de datos, periféricos o conexión a internet.

El objetivo principal que se pretende demostrar con el desarrollo del escenario 1, es construir la red en el simulador Cisco Packet Tracer de acuerdo a la topología dada, en esta desarrollar el esquema de direccionamiento IP para las redes LAN, realizar las respectivas configuraciones básicos de los dispositivos de red, sus respectivos ajustes de seguridad en el Router y Swicth, configurar los hosts y verificar la conectividad entre los dispositivos.

Para el escenario 2 el objetivo es configurar los dispositivos de la red para que permita tanto la conectividad de IPv4 y IPv6, teniendo en cuenta que el Router y Switch también deben configurar de forma segura, además realizar sus respectivas configuraciones entre VLAN, DCHP, EtherChannel y port-security. Inicialmente se identificarán los dispositivos, seguidamente se realizará la topología, posteriormente se realizará las respectivas configuraciones en el router, los Switch y los equipos de cómputo y por último se realizará las respectivas verificaciones de conectividad en toda la red.

1. Escenario 1

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

Topología

Figura 1. Topología del escenario 1

Fuente: Documento cisco

Objetivos

Parte 1: Construir en el simulador la red

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

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

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

Parte 3: Configurar los hosts y verificar la conectividad entre los equipos

Aspectos básicos/situación

En el desarrollo del caso de estudio se implementa la topología mostrada en la figura y configurar el Router R1 y el switch S1 y los PCS. Con la dirección suministrada realizar el subnetting y cumplirá el requerimiento para LAN1 (60 host) y LAN2 (20 hosts).

1.1. Parte 1: Construya la Red

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

1.2. Parte 2: Desarrolle el esquema de direccionamiento IP

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con 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.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.

Tabla 1. Tabla de direccionamiento escenario 1

Item	**Requerimiento**	**Respuesta**
Dirección de Red	172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cedula.	172.42.3.0
Requerimiento de host Subred LAN1	60	
Requerimiento de host Subred LAN2	20	
R1 G0/0/1	Ultima dirección de host de la subred LAN 1	172.42.3.62
R1 G0/0/0	Ultima dirección de host de la subred LAN 2	172.42.3.94

S1 SV1	Segunda dirección de host de la subred LAN 1	172.42.3.2
PC-A	Decima dirección de host de la subred LAN 1	172.42.3.10
PC-B	Decima dirección de host de la subred LAN 2	172.42.3.75

Fuente: Autor

1.3. Parte 3: Configure aspectos básicos

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

1.3.1. Paso 1: configurar los ajustes básicos

Las tareas de configurar para R1 incluyen las siguientes:

Tabla 2.Configuración en Consola para el R1

Descripción	**Comando**
Ingresa al modo privilegiado	Router>enable
Ingresa a modo de configuración	Router#configure terminal
Desactiva la búsqueda DNS	Router(config)#no ip domain-lookup
Salir del modo de configuración	Router(config)#exit
Guardar la configuración	Router#copy running-config startup-config
Confirmación	Router#show startup-config
Se asigna el nombre del router R1	Router(config)#hostname R1
Se nombre el dominio del router R1: ccna-sa.com	R1(config)#ip domain-name ccna-sa.com
Activa contraseña cifrada para modo EXEC privilegiado: ciscoenpass	R1(config)#enable secret ciscoenpass
Ingresa a configuración de consola	R1(config)#line console 0

Contraseña de acceso a la consola: ciscoconpass	R1(config-line)#password ciscoconpass
Habilita la contraseña	R1(config-line)#login
Sale de consola para volver a modo de configuración	R1(config-line)#exit
Se establece la longitud mínima para las contraseñas que son de 10 caracteres	R1(config)#security passwords min-length 10
Crea un usuario administrativo en la base de datos local Nombre de usuario: admin Contraseña: admin1pass	R1(config)#username admin password admin1pass
Configurar inicio de sesión en las líneas VTY para que use la base de datos local en R1	R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit
Configurar solo aceptando SSH en R1	R1(config)#line vty 0 4
Configura el inicio de sesión en las líneas VTY para que use base de datos local	R1(config-line)#login local
Configura VTY solo aceptado SSH	R1(config-line)#transport input SSH
Salir de líneas VTY para volver a modo de configuración	R1(config-line)#exit
Cifra las contraseñas de texto no cifrado	R1(config)#service password-encryption
Se configura un MOTD banner con el texto "Router ISR4331, Leidy Johana Rincon Rivera, Ingenieria de Sistemas"	R1(config)#banner motd "Router ISR4331, Leidy Johana Rincon Rivera, Ingenieria de Sistemas"
Se ingresa a configuración de la interfaz G0/0/0	R1(config)#interface gigabitEthernet 0/0/0

Se configura interfaz G0/0/0 se establece la dirección IPv4	R1(config-if)#ip address 172.42.3.94 255.255.255.224
Se configura interfaz G0/0/0 se establece la descripción	R1(config-if)#description "Interface Red LAN2
Se configura interfaz G0/0/0 se activa la interfaz	R1(config-if)#no shutdown
Se ingresa configuración de la interfaz G0/0/1	R1(config)#interface gigabitethernet 0/0/1
Se configura interfaz G0/0/1 se establece la descripción	R1(config)#interface gigabitethernet 0/0/1
Se configura interfaz G0/0/1 se establece la dirección IPv4	R1(config-if)#ip address 172.42.3.62 255.255.255.192
Se configura interfaz G0/0/1 Se activa la interfaz	R1(config-if)#no shutdown R1(config-if)#exit
Se llama al dominio ccna-sa.com	R1(config)#ip domain name ccna-sa.com
Se genera una clave de cifrada RSA módulo de 1024 bits	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024

	% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Se guarda la configuración en la memoria	R1#wr Building configuration... [OK] R1#

Fuente: Autor

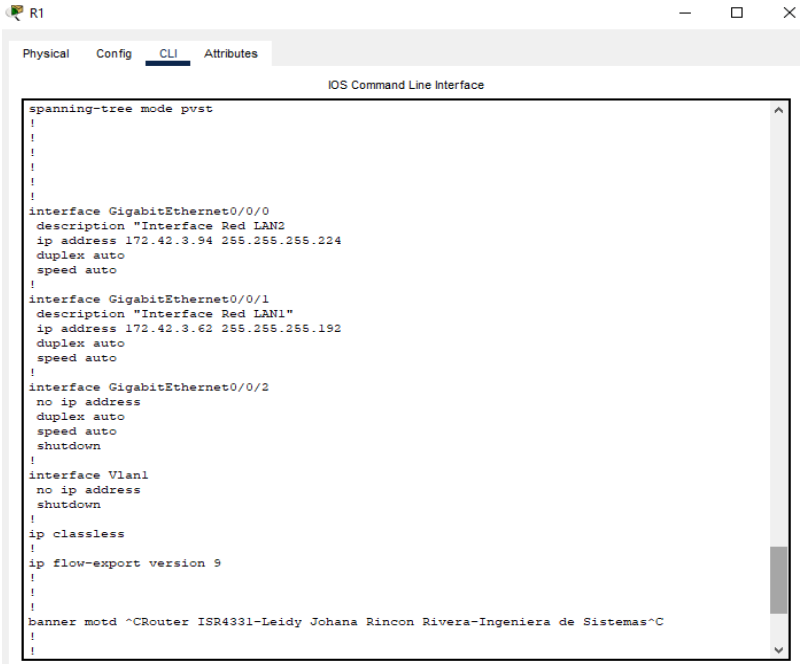
Se ingresa al modo privilegiado, en donde se procede a realizar las diferentes configuraciones requeridas para Router 1, se realiza la desactivación de la búsqueda DNS, luego se le asigna el nombre al dispositivo, se le asigna nombre el dominio del router R1: ccna-sa.com, se configura la contraseña de acceso a la consola: ciscoconpass, se habilita mediando en comando login, se establece la longitud mínima para las contraseñas que son de 10 caracteres, se crea un usuario administrativo en la base de datos local con nombre de usuario: admin y contraseña: admin1pass, se configura inicio de sesión en las líneas VTY para que use la base de datos local en R1 y configurar VTY solo aceptado SSH, luego se cifra las contraseñas de texto no cifrado, se configura un MOTD banner con el mensaje sugerido, luego se ingresa a configuración de la interfaz G0/0/0, se configura interfaz G0/0/0 se establece la dirección IPv4, se realiza la descripción y se activa la interfaz, de igual forma se ingresa configuración de la interfaz G0/0/1, se configura interfaz G0/0/1 se establece la dirección IPv4, se realiza la descripción y se activa la interfaz, luego se llama al dominio ccna-sa.com y por último se genera una clave de cifrada RSA módulo de 1024 bits y guardar configuraciones.

Mediante el comando show run podemos observar las configuraciones que se realizó al R1

Figura 2.Evidencia del Comando Show run

Fuente: Autor

Figura 3. Evidencia del comando Show run en R1



Fuente: Autor

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Tareas de Configuración para S1

Descripción	**Comando**
Ingresa al modo privilegiado	Swtich>enable
Ingresa a modo de configuración	Swtich #configure terminal
Desactiva la búsqueda DNS	Swtich (config)#no ip domain-lookup
Se asigna el nombre del Swtich S1	Swtich (config)#hostname S1
Se nombre el dominio del Swtich S1: ccna-sa.com	S1(config)#ip domain-name ccna-sa.com
Activa contraseña cifrada para modo EXEC privilegiado: ciscoenpass	S1(config)#enable secret ciscoenpass
Ingresa a configuración de consola	S1(config)#line console 0
Contraseña de acceso a la consola: ciscoconpass	S1(config-line)#password ciscoconpass
Habilita la contraseña	S1(config-line)#login
Sale de consola para volver a modo de configuración	S1(config-line)#exit
Crea un usuario administrativo en la base de datos local Nombre de usuario: admin Contraseña: admin1pass	S1(config)#username admin password admin1pass
Se configurará el inicio de sesión en las líneas VTY para que use la base de datos local en S1 Se establece conexión Telnet	S1(config)#line vty 0 15
se ingresa autenticación	S1(config-line)#login local

Salida para volver a modo de configuración	S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH en S1 Acceso al dispositivo a cisco	S1(config)#line vty 0 4
se ingresa autenticación	S1(config-line)#login local
Configura VTY solo aceptado SSH	S1(config-line)#transport input SSH
Salir de líneas VTY para volver a modo de configuración	S1(config-line)#exit
Cifra las contraseñas de texto no cifrado	S1(config)#service password-encryption
Se configura un MOTD banner con el texto " Swicth 2960 24TT, Leidy Johana Rincon Rivera, Ingenieria de Sistemas"	S1(config)#banner motd "Swicth 2960 24TT, Leidy Johana Rincon Rivera, Ingenieria de Sistemas"
Genera una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Configure la interfaz de administración (SVI) en VLAN1	S1(config)#interface vlan 1 *Mar 1 0:18:42.741: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip address 172.42.3.2 255.255.255.192 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up S1(config-if)#exit S1(config)#ip default-Gateway 172.42.3.62 S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#

Fuente: Autor

se ingresa al modo al privilegiado para iniciar con las respectivas configuraciones Switch 1, se inicia con desactivar la búsqueda DNS, luego se le asigna un nombre al dispositivo, se crea el nombre el dominio del Swtich S1: ccna-sa.com, se crea y se activa contraseña cifrada para modo EXEC privilegiado: ciscoenpass, se ingresa

a configuración de consola, se crea la contraseña de acceso a la consola: ciscoconpass y se activa mediante el comando login, luego se crea un usuario administrativo en la base de datos local con nombre de usuario: admin y contraseña: admin1pass, luego se configurar el inicio de sesión en las líneas VTY para que use la base de datos local en S1, en esta se configura las líneas VTY para que acepten únicamente las conexiones SSH en S1 acceso al dispositivo a cisco, se configura VTY solo aceptado SSH, luego se cifra las contraseñas de texto no cifrado, se configura un MOTD banner según los parámetros dados, enseguida se genera una clave de cifrado RSA de 1024 bits y por último se configura la interfaz de administración (SVI) en VLAN1.

1.3.2. Paso 2: configurar los equipos

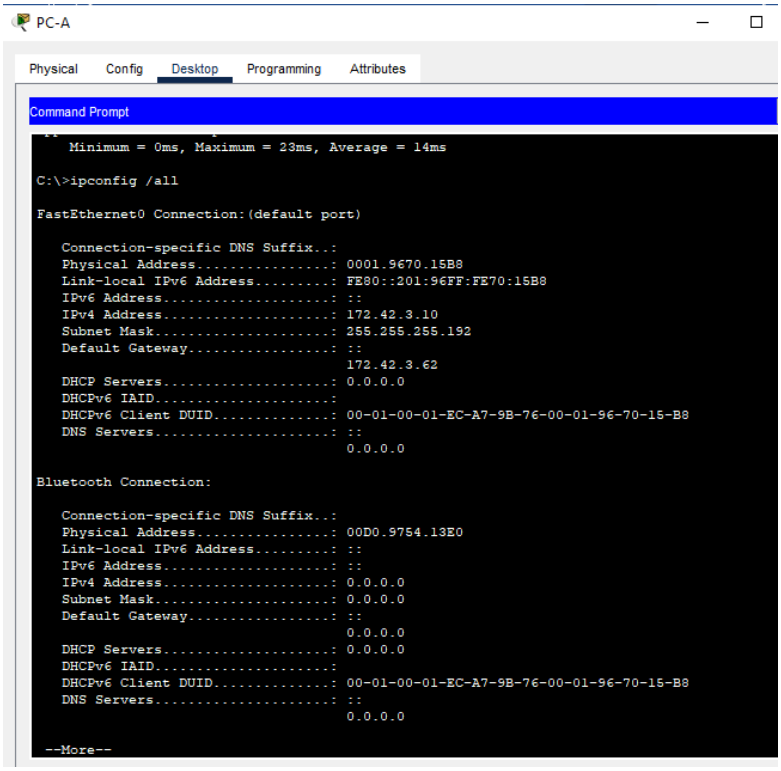
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 4. Configuración de PC-A

Configuración de red de PC-A	
Descripción	FastEthernet0
Dirección física	0001.9670.15B8
Dirección IPv4	172.42.3.10
Mascara de subred	255.255.255192
Puerta de enlace IPv4 predeterminada	172.42.3.62

Fuente: Autor

Figura 4. Configuración de PC-A



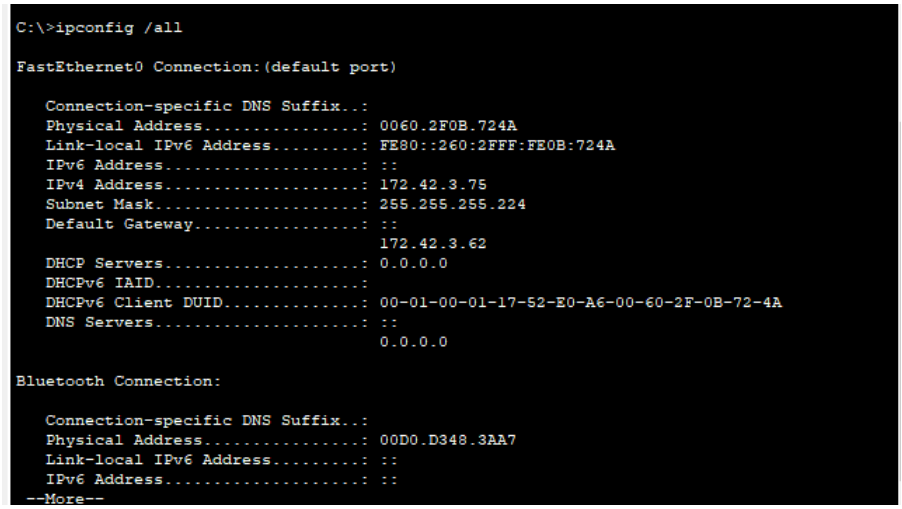
Fuente: Autor

Tabla 5. Configuración de PC-B

Configuración de red de PC-B	
Descripción	FastEthernet0
Dirección física	0060.2F0B.724ª
Dirección IPv4	172.42.3.75
Mascara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.42.3.62

Fuente: Autor

Figura 5. Configuración de PC-B



Fuente:Autor

1.4. 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 y vuelva a realizar la verificación.

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

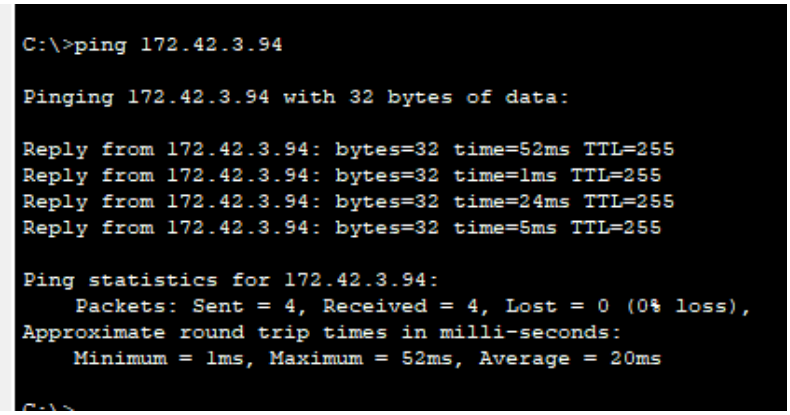
Tabla 6.Verificación de conectividad

Desde	A	Direcciones IP	Resultado de ping
PC-A	R1 G0/0/0	172.42.3.94	Figura 6
	R1 G0/0/1	172.42.3.62	Figura 7

	S1 VLAN 1	172.42.3.2	
	PC-B	172.42.3.75	Figura 8
PC-B	R1 G0/0/0	172.42.3.94	Figura 9
	R1 G0/0/1	172.42.3.62	Figura 10
	S1 VLAN 1	172.42.3.2	

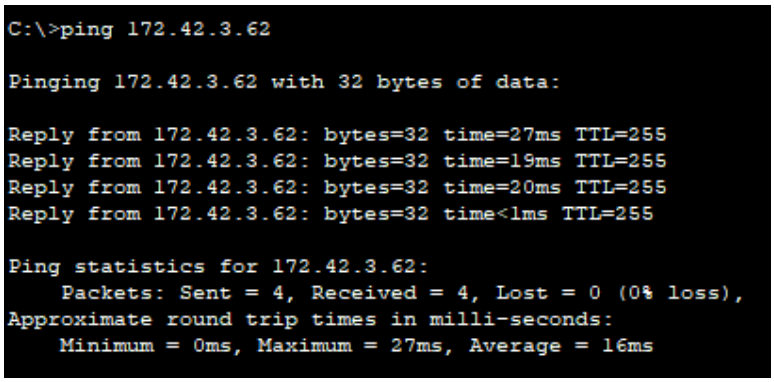
Fuente: Autor

Figura 6. Verificación conectividad PC-A – R1 G0/0/0



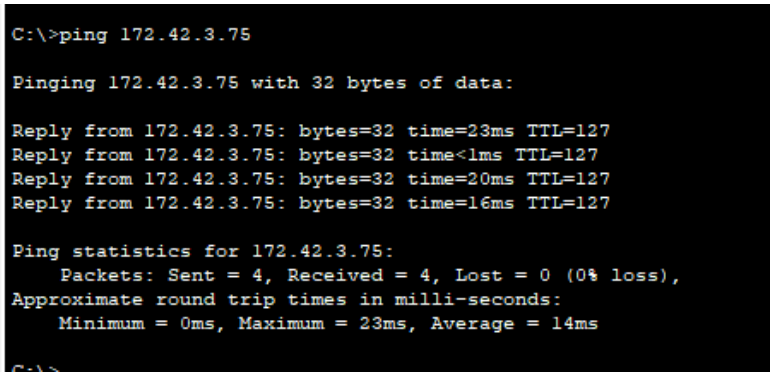
Fuente: Autor

Figura 7. Verificación conectividad PC-A - G0/0/1



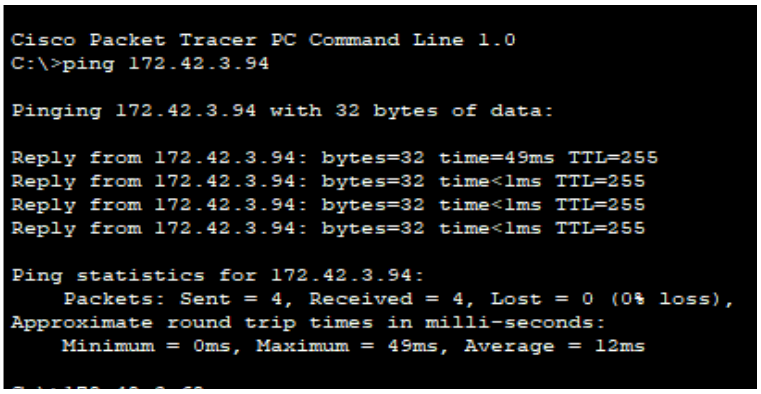
Fuente: Autor

Figura 8. verificación conectividad PC-A - PC-B



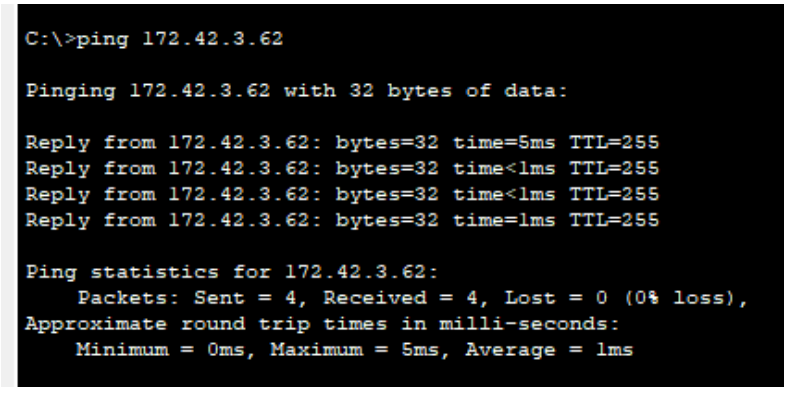
Fuente: Autor

Figura 9. verificación conectividad PC-B - R1 G0/0/0



Fuente: Autor

Figura 10. verificación conectividad PC-B - R1 G0/0/1

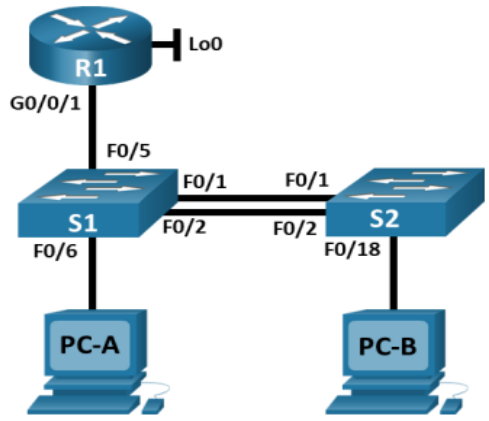


Fuente: Autor

2. Escenario 2

Topología

Figura 11. Topología escenario 2

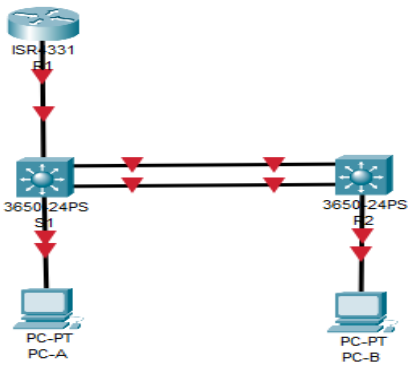


Fuente: Autor

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

Se realiza el escenario utilizando la herramienta Packet Tracer, se utiliza un router, dos switches y dos dispositivos finales.

Figura 12. Topología en Cisco Packet Tracer



Fuente: Autor

Esta es la tabla para las vlans:

Tabla 7. Tabla de vlans escenario 2

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

Fuente: Autor

Tabla de asignación de direcciones para la red

Tabla 8.Direccionamiento de red escenario 2

Dispositivo/interfaz	**Dirección IP/Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.42.8.1/26 2001:db8:acad:a::1/64	No corresponde

R1 G0/0/1.30	10.42.8.65 /27 2001:db8:acad:b::1 /64	No corresponde No corresponde
R1 G0/0/1.40	10.42.8.97 /29 2001:db6:acad:c::1/64	No corresponde No corresponde No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Lookback0	209.165.201.1/27 2001:db8:acad:209::1/64	No corresponde No corresponde
S1 VLAN 4	10.42.8.98/29 2001:db8:acad:c::98/64 fe80: :98	10.19.8.97 No corresponde No corresponde
S2 VLAN 4	10.42.8.99 /29 2001:db8:acad:c: :99/64 fe80: : 99	10.19.8.97 No corresponde No corresponde
PC-A NIC PC-B NIC	Dirección DHCP para IPv4 2001:db8:acad:a: :50/64 DHPCP para direccione IPv4 2001.db8:acad:b: :50/64	DHCP para puerta de enlace predeterminada IPv4 Fe80::1 DHCP para puerta de enlace predeterminada IPv4 Fe80::1

Fuente: Autor

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

Instrucciones

2.1. Parte 1: inicializar y recargar y configurar aspectos básicos de los dispositivos

2.1.1. 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 cargar los dispositivos.

Router R1

Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload

Se accede al router 1 a través de la consola en modo privilegiado para borrar cualquier configuración de inicio con el comando erase startup-config este borra el contenido de la NVRAM, enseguida se reinicia el Router con el comando reload, asi quedadno listo para sus configuraciones.

Switch S1

Switch>enable
Switch#erase sta
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]

Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Switch#reload

Switch S2

Switch>enable
Switch#erase sta
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Switch#reload

Se accede al switch 1 y 2 a través de la consola en modo privilegiado para ejecutar el comando eras-startup-config, este borra el contenido de la NVRAM junto con el comando delete vlan.dat, este elimina la base de datos de la vlan, este proceso permite restaurar el switch y por lo tanto borrar cualquier configuración de inicio, enseguida se reinicia con el comando reload, quedando listo para sus configuraciones.

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

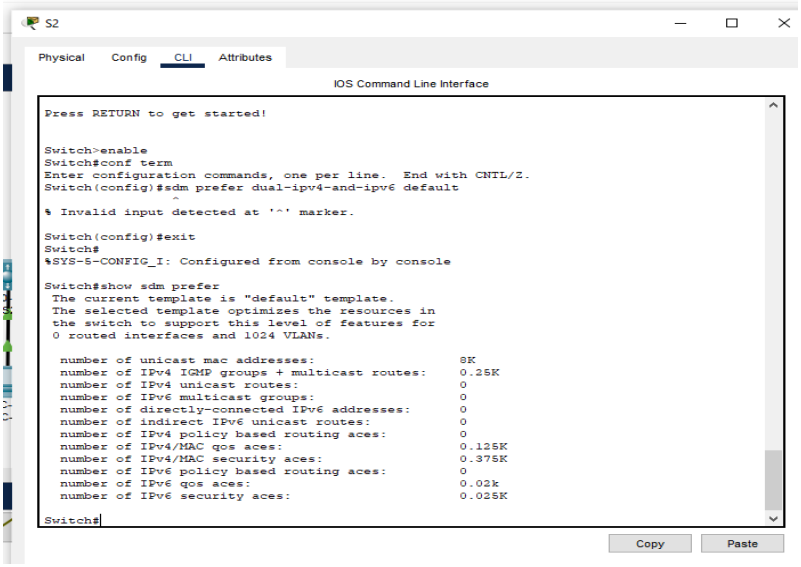
Tabla 9. Activación plantilla SDM

Tarea	Resultado
Ingresar al modo privilegiado	Switch>enable
Activar plantilla predeterminada	Switch#show sdm prefer
Habilitar plantilla SDM para IPv4 e IPv6	Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Reiniciar el Switch	

Fuente: Autor

Se debe tener en cuenta que el switch Cisco 3560 no soporta capacidades IPv6, debido a esto se debe configurar la plantilla SDM para que permita IPv6 junto con IPv4, se verifica desde el modo provilegiado la configuración con el comando show sdm prefer, esta muestra que solo soporta configuración IPv4, para activar la configuración IPv6 se ejecuta el comando sdm prefer-ipv4-and-ipv6 default, se procede a reiniciar como el comando reload para que la nueva plantilla se cargue.

Figura 13. verificación de soporte de protocolo IPv6 en el S1 y S2



Fuente: Autor

Se puede observar como el S1 y S2 soporta el protocolo IPv6

2.1.2. Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguiente:

Tabla 10. Configuraciones R1

Tarea	Especificación	Resultado
Desactivar la búsqueda DNS		Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	R1	Router(config)#hostname R1
Nombre de dominio	ccna-sa.com	R1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class	R1(config)#enable secret class
Contraseña de acceso a la consola	cisco	R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	5 caracteres	R1(config)#security passwords min-length 5
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass	R1(config)#username admin privilege 15 secret admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH		R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado		R1(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.	R1(config)#banner motd "Router R1,Leidy Johana Rincon Rivera, Ingenieria de sistemas"
Habilitar el routing IPv6		R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1 Establece la dirección IPv6.	R1(config)#interface g0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description vlan docentes R1(config-subif)#ip address 10.42.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link-local

	Activar la interfaz.	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 10.42.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 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 10.42.8.97 255.255.255.248 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 R1(config-if)#no shutdown
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1	R1(config-if)#interface loopback 0 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 internet R1(config-if)#exit
Generar una clave de cifrado RSA	Módulo de 1024 bits	R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

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

Fuente: Autor

Se estableció las respectivas subinterfaces, encapsulándolas con su vlan y asignando el direccionamiento IPv4 y IPv6, de igual manera se genera una clave de cifrado RSA, en donde se configuran las medidas de seguridad, así como la transferencia de autenticación por medio de RSA

2.1.3. Paso 3: Configure S1 y S2.

Configuración S1

Las tareas de configuración incluyen lo siguiente:

Tabla 11. Configuraciones Switch (S1).

Tarea	Especificación	Resultado
Desactivar la búsqueda DNS.		Switch(config)#no ip domain-lookup
Nombre del switch	S1 o S2, según proceda	Switch(config)#hostname S1
Nombre de dominio	ccna-sa.com	S1(config)#ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	class	S1(config)#enable secret class
Contraseña de acceso a la consola	cisco	S1(config)#line con 0 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 privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		S1(config)#line vty 0 15 S1(config-line)#login local S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado		S1(config)#service password-encryption
Configurar 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,Leidy Johana Rincon Rivera, Ingeniera de sistemas"
Generar una clave de cifrado RSA	Módulo de 1024 bits	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your

		General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la dirección IPv6 de capa 3	S1(config)#interface vlan 4 *Mar 1 1:47:29.949: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip add 10.42.8.98 255.255.255.248 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 S1(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.42.8.97 para IPv4	S1(config)#ip default-gateway 10.42.8.97

Fuente: Autor

Se realiza las respectivas configuraciones al Switch 1, desde consola modo privilegiado se procede a ejecutar el comando no ip domain lookup, perimite desactivas la búsqueda DNS para indicar que si hemos cometido un error en el scrip de configuración, se establece el nombre del dispositivo y nombre del dominio junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, se configura la contraseña para ingresas a la consola con el comando password acitivandola con login, se crea un usuario administrativo con usuario y contraseña y se configuran las líneas vty para usar la base datos local line vty 0 15 , se activan con login local, las líneas vty se configuran para admitir solo correcciones SSH con el comando transport input ssh, en seguida se configuran las contraseñas de texto no cifrado service password-encryption, luego se genera el mensaje del día en el banner motd, se crea una llave de encription RSA con el comando crypto key generate rsa, este se le asigna una longitud de 1024 bits, ya finalizando se realiza la respectiva configura la interfaz administrativa correspondiente a la vlan4 asignándole la IPv4 y dirección IPv6, y por último se configura la puerta de enlace predeterminando para IPv4, la de IPv6 no se configura porque se asigna automática.

Configuraciones para el Swictch

Tabla 12. Configuraciones de Switch (S2).

Tarea	**Especificación**	**Resultado**
Desactivar la búsqueda DNS.		Switch(config)#no ip domain-lookup
Nombre del switch	S1 o S2, según proceda	Switch(config)#hostname S2
Nombre de dominio	ccna-sa.com	S2(config)#ip domain-name ccna-sa.com

Contraseña cifrada para el modo EXEC privilegiado	Class	S2(config)#enable secret class
Contraseña de acceso a la consola	Cisco	S2(config)#line con 0 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 privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local		S2(config)#line vty 0 15 S2(config-line)#login local S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH		S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado		S2(config)#service password-encryption
Configurar un MOTD Banner	Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa	S2(config)#banner motd "S2, Leidy Johana Rincon Rivera, Ingenieria de sistemas"

	académico al que pertenece.	
Generar una clave de cifrado RSA	Módulo de 1024 bits	S2(config)#crypto key generate rsa The name for the keys will be: S2.ccna-sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80: :98 para S1 y FE80: :99 para S2 Establecer la	S2(config)#interface vlan 4 *Mar 1 2:10:14.857: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config-if)#ip add 10.42.8.99 255.255.255.248 S2(config-if)#ipv6 add 2001:db8:acad:c::99/64

	dirección IPv6 de capa 3	S2(config-if)#ipv6 add fe80::99 link-local S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.42.8.97 para IPv4	S2(config)#ip default-gateway 10.42.8.97

Fuente: Autor

Se realiza las respectivas configuraciones al Switch 2, desde consola modo privilegiado se procede a ejecutar el comando no ip domain lookup, perimite desactivas la búsqueda DNS para indicar que si hemos cometido un error en el scrip de configuración, se establece el nombre del dispositivo y nombre del dominio junto con la contraseña cifrada para ingresar al modo privilegiado a través del comando enable secret, se configura la contraseña para ingresas a la consola con el comando password activándola con login, se crea un usuario administrativo con usuario y contraseña y se configuran las líneas vty para usar la base datos local line vty 0 15 , se activan con login local, las líneas vty se configuran para admitir solo correcciones SSH con el comando transport input ssh, en seguida se configuran las contraseñas de texto no cifrado service password-encryption, luego se genera el mensaje del día en el banner motd, se crea una llave de encription RSA con el comando crypto key generate rsa, este se le asigna una longitud de 1024 bits, ya finalizando se realiza la respectiva configura la interfaz administrativa correspondiente a la vlan4 asignándole la IPv4 y dirección IPv6, y por último se configura la puerta de enlace predeterminando para IPv4, la de IPv6 no se configura porque se asigna automática.

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

2.2.1. Paso 4: Configurar S1

La configuración del S1 incluyen las siguientes tareas:

Tabla 13. Configuración de la infraestructura de red (VLAN,Trunking, EtherChannel) en Switch 1

Tarea	Especificación	Resultado
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#vlan 40 S1(config-vlan)#name Invitados S1(config-vlan)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5	S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56 S1(config-if)#interface range fa0/1-2

		S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(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	Usar el protocolo LACP para la negociación	S1(config)#interface range fa0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56
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	Permitir 4 direcciones MAC	S1(config-if)#switchport port-security maximum 4

puertos de acceso		
Proteja todas las interfaces no utilizadas	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar	S1(config-if-range)#interface range fa0/3-4 S1(config-if-range)#switchport acces vlan 50 S1(config-if-range)#description No esta en uso S1(config-if-range)# 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 esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown

Fuente: Autor

Se realiza las configuraciones desde consola, modo privilegiado, configurando global se crean las vlan asignadas, se crean las trocales 802.1Q que usen la vlan nativa fa0/, fa0/2 y fa0/5, se inicia configurando la interface fa0/5 con solo esta referencia de switch con el comando de encapsulación switchport trunk encapsulation dot1q, para implementar la interface con el código switchport mode trunk direccionándola a la vlan 56 nativa, se configura las fa0/1 y fa0/2 este se usa un rango interface range fa0/1-2, en el momento que se configura EtherChanel se desactiva el rango anterior con el comando shutdown, así evitar problemas, se configura la interface range fa0/1-2 con el comando de encapsulación switchport trunk encapsulation dot1q, para implementar la interface con el código switchport mode trunk direccionándola a la vlan56 nativa, se crea la EtherChannel que se utilizó en el grupo de las interface fa0/1-2 con el código channel-group 1 mode active, luego se usa LACP creando grupo 1, enseguida se entra a la interfaz de este con el comando innterface port-channel 1 y se configura las troncales, el puerto de acceso para la vlan 20 docentes que use la fa0/2 con el comando switchport acces vlan 20, se configuran la seguridad en la interfaz estableciendo máximo 4 direcciones MAC, se aseguran todas las interfaces sin usar asignándoles a la vlan 50 indicando que no está en uso y apagar con shutdown, estas son fa0/3-4, fa0/1-24 y g0/1-2 y por último se activa el rango de interfaz fa0/1-2.

2.2.2. Paso 5: Configure el S2

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

Tabla 14. Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 2

Tarea	Especificación	
Crear VLAN	VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes	S2>enable Password: Password: S2#configure terminal

	VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native	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)#name invitados 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	Interfaces F0/1 y F0/2	S2(config)#interface range fa0/1-2 S2(config-if-range)#shutdown 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	Usar el protocolo LACP para la negociación	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

Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18	S2(config-if)#interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30
Configure port-security en los access ports	permite 4 MAC addresses	S2(config-if)#switchport port-security maximum 4
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar	S2(config-if)#interface range fa0/3-7 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown 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 esta en uso S2(config-if-range)#shutdown

Fuente: Autor

Desde consola, modo privilegiado y se realiza la configuración global se crean las vlan, se crean las troncales 802.1Q que usen la valn nativa interfaces fa0/1 y fa0/2, para configurar estas se usa un rango interface range fa1/1-2, mientras se configura

la EtherChannel se desactiva el rango anterior con el comando shutdown para evitar problemas, se configura la interface range fa0/1-2 utilizando el comando de encapsulación switchport trunk encapsulation dot1q direccionándola a la vlan 56, se crea la EtherChannel que utilice el grupo de interfaces fa0/1-2 con el código channel-group 1 mode active, usar LACP creando el grupo 1, luego se entra a la interfaz de este con interface Port-channel 1 y se configura las troncales, configurar un puerto de acceso para la vlan 30 estudiantes que use la fa0/18 con el comando switchport acces vlan 30, se configura la seguridad en la interfaz estableciendo máximo 3 direcciones MAC, se aseguran todas las interfaces sin usar asignándolas a la vlan 50 que no está en uso y apagar con el comando shutdown, estas son fa0/3-17, fa0/19-24 y g0/1-2 y por último se activa el rango de interfaz fa0/1-2 con no shutdown.

Tabla 15. Activación interface fa0/1-2 en s1 y S2

Tarea	Especificación
Activar el rango fa0/1-2 en switch 1	S1(config)#interface range fa0/1-2 S1(config-if-range)#interface range fa0/1-2 S1(config-if-range)#no shutdown
Activar el rango fa0/1-2 en switch 2	S2(config)#interface range fa0/1-2 S2(config-if-range)#interface range fa0/1-2 S2(config-if-range)#no shutdow

Fuente: Autor

2.3. Parte 2: Configurar soporte de host

2.3.1. Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 16. Configuración de soporte de host en Router

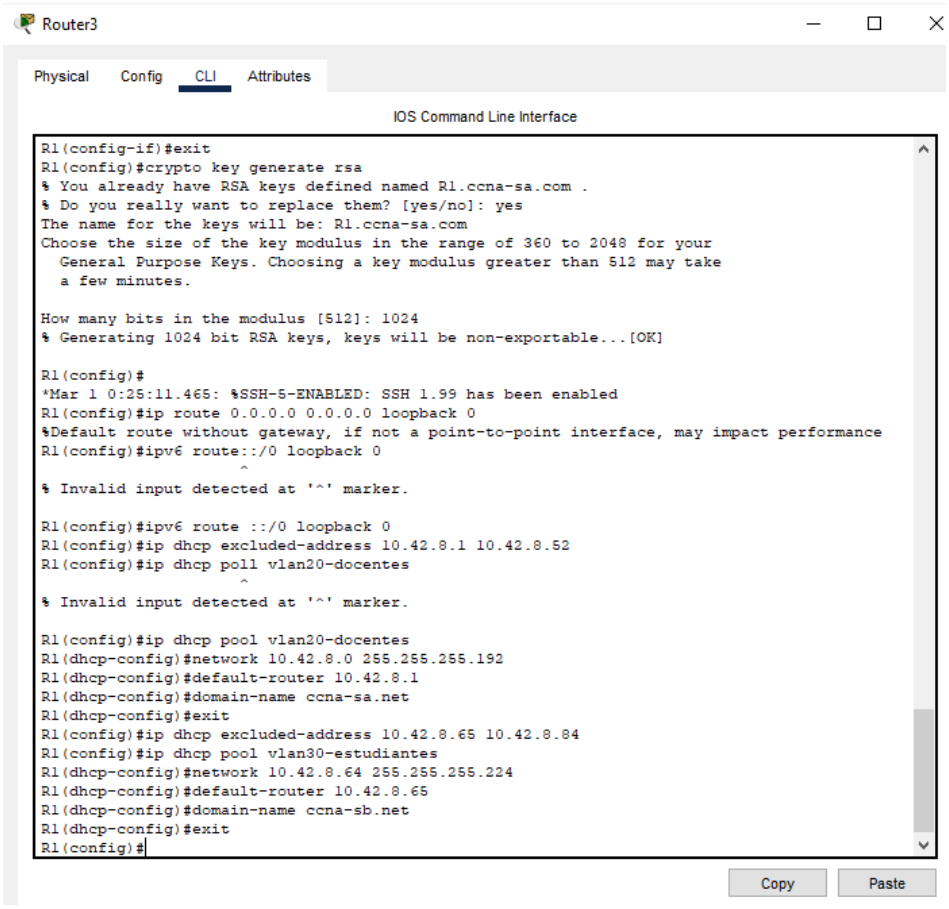
Tarea	Especificación	
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(config)#ip dhcp excluded-address 10.42.8.1 10.42.8.52 R1(config)#ip dhcp pool vlan20-docentes R1(dhcp-config)#network 10.42.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.42.8.1 R1(dhcp-config)#domain-name ccna-sa.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de	R1(config)#ip dhcp excluded-address 10.42.8.65 10.42.8.84 R1(config)#ip dhcp pool vlan30-estudiantes R1(dhcp-config)#network 10.42.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.42.8.65

	enlace predeterminada como dirección de interfaz del router para la subred involucrada	R1(dhcp-config)#domain-name ccna-s b.net R1(dhcp-config)#exit

Fuente: Autor

El router se asignan las rutas predeterminadas Ipv4 ip route 0.0.0.0 0.0.0.0 loopback 0 y Ipv6 route ::/0 loopback 0, este direccionan el tráfico a la interfaz loopback 0, estas son rutas estáticas para conectar con el internet, enseguida se configura IPv4 DCHP para la valn 20 docentes conformando solamente por las ultimas 10 direcciones de subred, esta son en el rango 10.42.8.1-10.42.8.52, para esto se aplicó para excluir estas 10 direcciones el comando ip dchp excluded-address 10.42.8.1 10.42.8.52 y para el pool de DCHP ip dchp pool vlan20 docentes, red y mascara de red network 10.42.8.0 255.255.255.192, puerta de enlace predeterminada default-router 10.42.8.1, nombre de dominio domain-name ccna-sa.net, luego se configura DCHP ipv4 para la vlan30 y grupo DCHP conformado por las ultimas 10 direcciones con sus respectivas especificaciones, esta de un rango de 10.42.8.65 – 10.42.8.84, en este se aplica excluir estas 10 direcciones y para pool de DCHP con el comando ip dchp pool vlan30 estudiantes, red y mascara de red network 10.42.8.64 255.255.255.224, puerta de enlace predeterminada default-router 10.42.8.65 con el nombre de dominio domain-name ccna-sb.net.

Figura 14. Evidencia soporte de host en Router



Fuente: Autor

2.3.2. Paso 2: Configurar los servidores

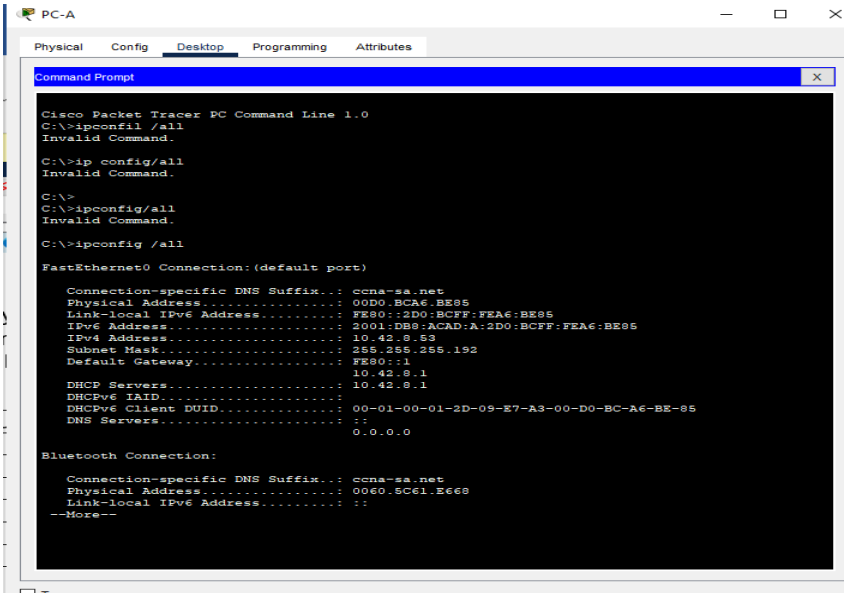
Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 17. Configuración de red del PC-A

Configuración de red de PC-A	
Descripción	Datos po DHCP
Dirección física	00D0.BCA6.BE85
Dirección IP	10.42.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.42.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Figura 15. Evidencia de configuración de red del PC-A



Fuente: Autor

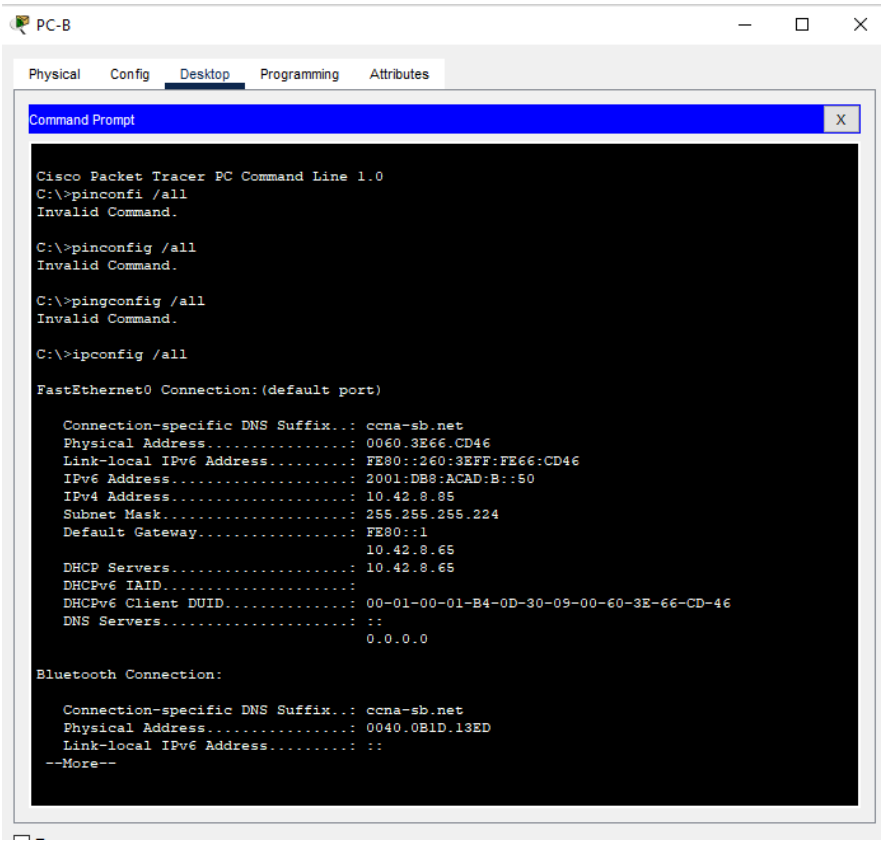
Tabla 18. Configuración de red del PC-B

Configuración de red de PC-B	
Descripción	
Dirección física	0060.3E66.CD46

Dirección IP	10.42.8.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.42.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Figura 16. Evidencia de configuración de red del PC-B



Fuente: Autor

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

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

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

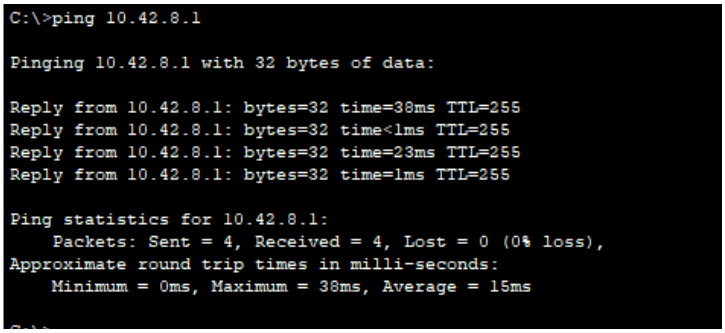
Tabla 19. Verificación de los dispositivos de red.

Desde	**A**		**Dirección IP**	**Resultado**
PC-A	R1, G0/0/1.20	IPv4	10.42.8.1	Figura 17
		IPv6	2001:DB8:ACAD:A::1	Figura 18
	R1,G0/0/1.30	IPv4	10.42.8.65	Figura 19
		IPv6	2001:DB8:ACAD:B::1	Figura 20
	R1, G0/0/1.40	IPv4	10.42.8.97	Figura 21
		IPv6	2001:DB8:ACAD:C::1	Figura 22
	S1, VLAN 4	IPv4	10.42.8.98	Figura 23
		IPv6	2001:DB8:ACAD:C::98	Figura 24 Se configura puerta de enlace IPv6 route ::/0 2001:db8:acad:c::1
	S2, VLAN 4	IPv4	10.42.8.99	Figura 25
		IPv6	2001:DB8:ACAD:C::99	Figura 26 Se configura puerta de enlace IPv6 route ::/0 2001:db8:acad:c::1
	PC-B	IPv4	10.42.8.85	Figura 27
		IPv6	2001:DB8:ACAD:B::50	Figura 28
	R1 Bucle 0	IPv4	209.165.201.1	Figura 29
		IPv6	2001:DB8:ACAD:209::1	Figura 30
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Figura 31

		IPv6	2001:DB8:ACAD:209::1	Figura 32
	R1, G0/0/1.20	IPv4	10.42.8.1	Figura 33
		IPv6	2001:DB8:ACAD:A::1	Figura 34
	R1, G0/0/1.30	IPv4	10.42.8.65	Figura 35
		IPv6	2001:DB8:ACAD:B::1	Figura 36
	R1, G0/0/1.40	IPv4	10.42.8.97	Figura 37
		IPv6	2001:DB8:ACAD:C::1	Figura 38
	S1, VLAN 4	IPv4	10.42.8.98	Figura 39
		IPv6	2001:DB8:ACAD:C::98	Figura 40
	S2, VLAN 4	IPv4	10.42.8.99	Figura 41
		IPv6	2001:DB8:ACAD:C::99	Figura 42

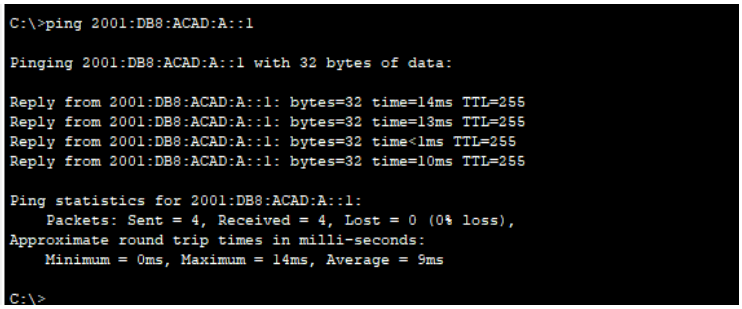
Fuente: Autor

Figura 17. Verificación conectividad PC-A - R1 G0/0/1.20 IPV4



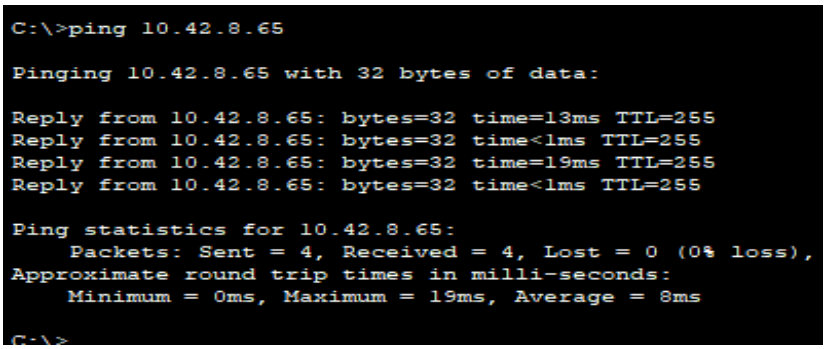
Fuente: Autor

Figura 18. verificación conectividad PC-A - R1 G0/0/1.20 IPV6



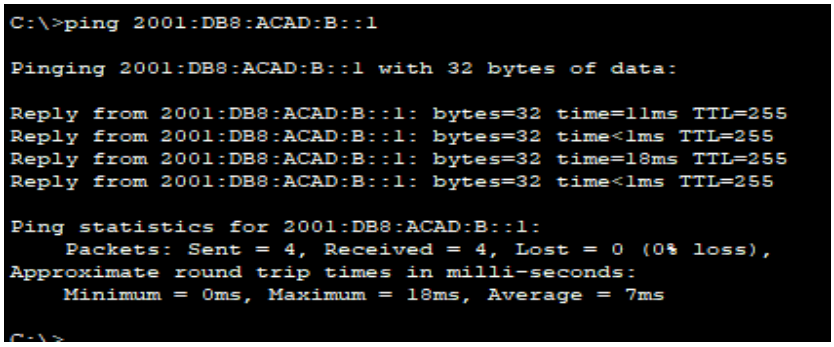
Fuente: Autor

Figura 19. verificación conectividad PC-A - R1 G0/0/1.30 IPV4



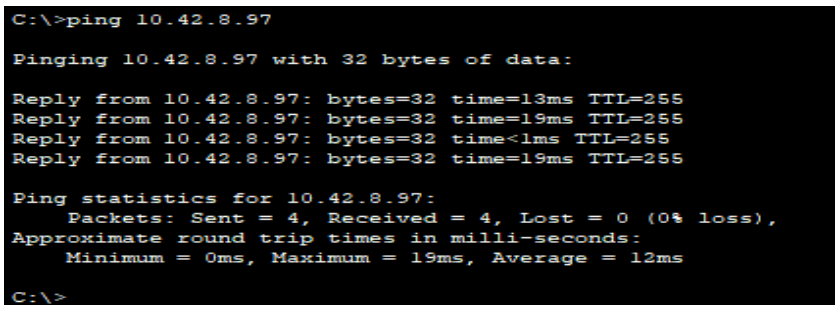
Fuente: Autor

Figura 20. verificación conectividad PC-A - R1 G0/0/1.30 IPV 6



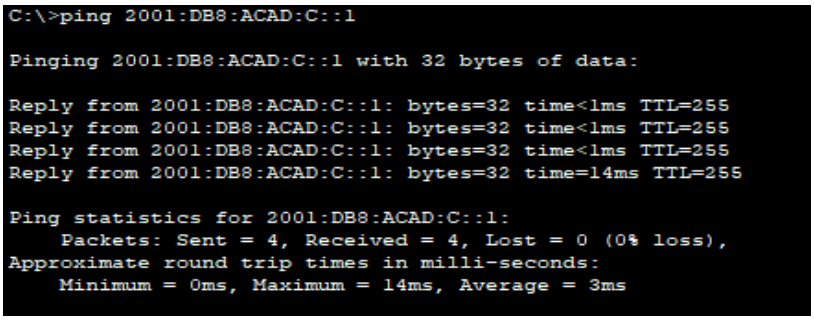
Fuente: Autor

Figura 21. verificación conectividad PC-A - R1 G0/0/1.40 IPV4



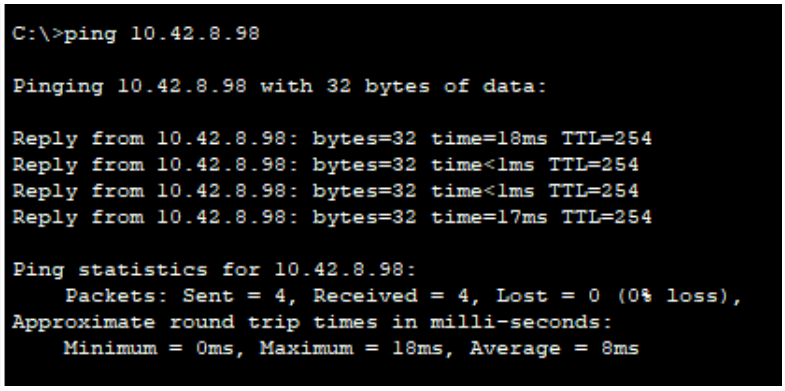
Fuente: Autor

Figura 22. verificación conectividad PC-A - R1 G0/0/1.40 IPV6



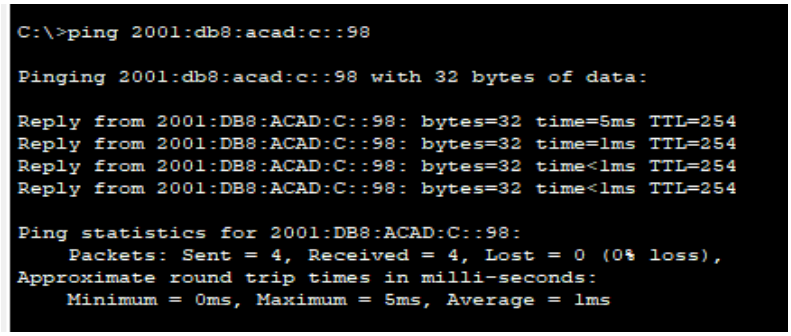
Fuente: Autor

Figura 23. Verificación conectividad PC-A - S1,VLAN 40 IPV4



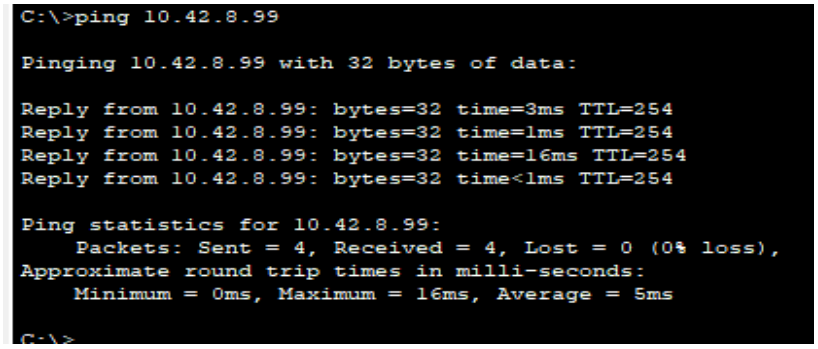
Fuente: Autor

Figura 24. Verificación conectividad PC-A - S1,VLAN 40 IPV6



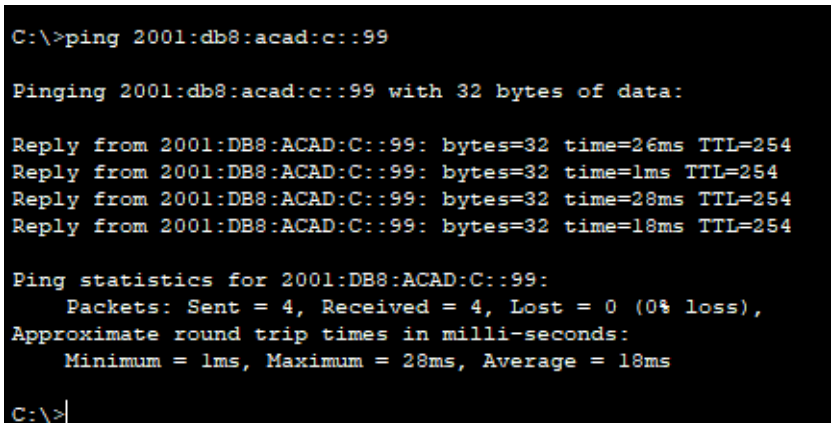
Fuente: Autor

Figura 25.Verificacion conectividad PC-A - S2, VLAN 40 IPV4



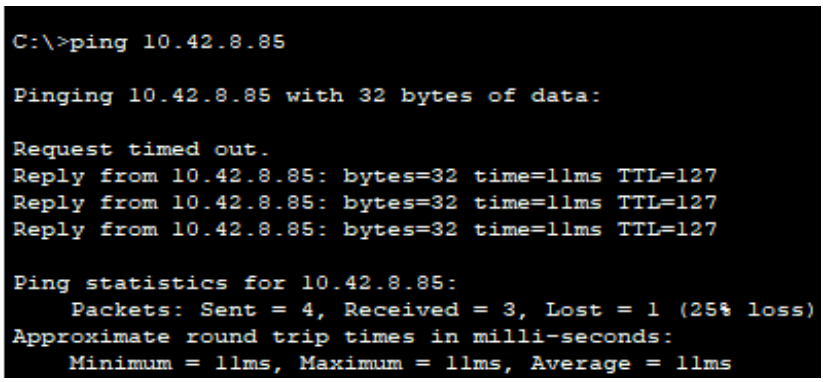
Fuente: Autor

Figura 26. Verificación conectividad PC-A - S2,VLAN 40 IPV6



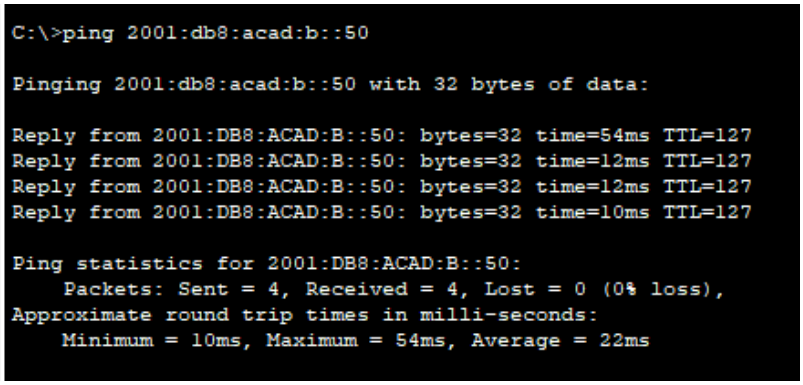
Fuente: Autor

Figura 27. verificación conectividad PC-A - PCB IPV4



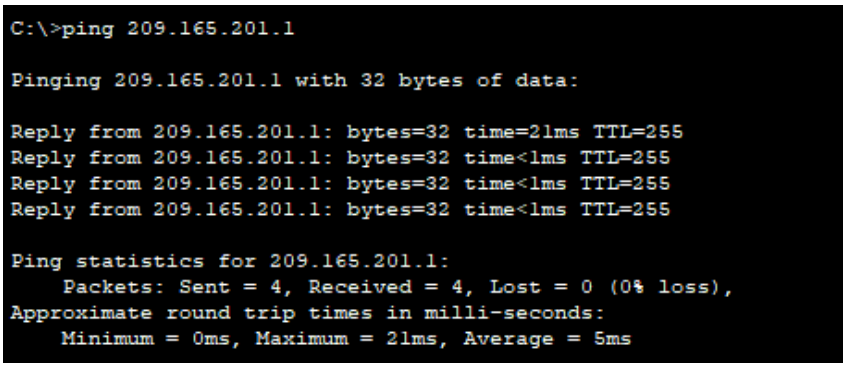
Fuente: Autor

Figura 28. Verificación conectividad PC-A - PC-B IPV6



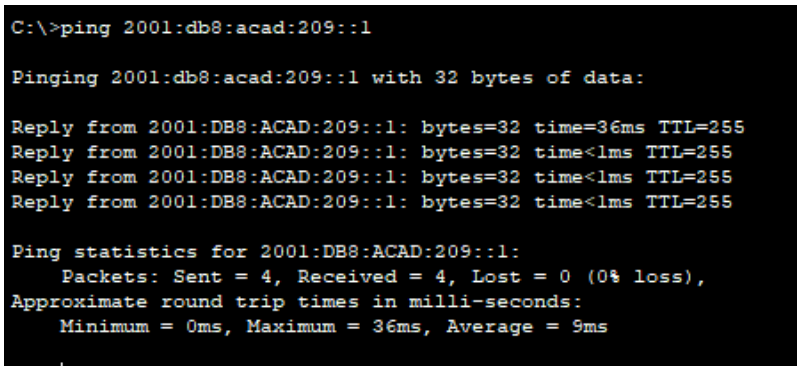
Fuente: Autor

Figura 29.Verificacion conectividad PC-A - R1 BUCLE 0 IPV4



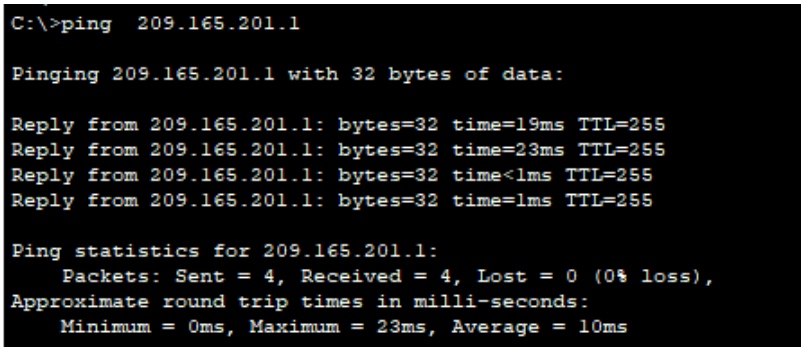
Fuente: Autor

Figura 30.Verificacion conectividad PC-A - R1 BUCLE 0 IPV6



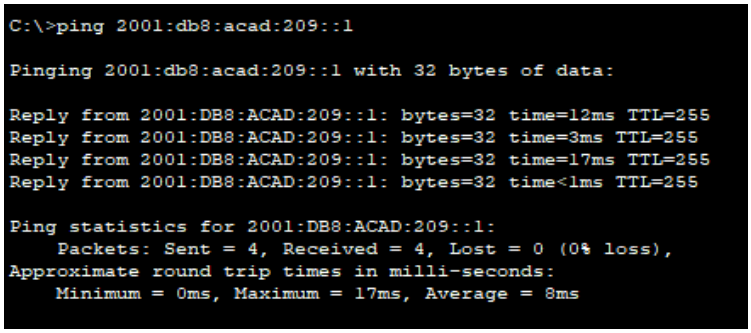
Fuente: Autor

Figura 31. Verificación conectividad PC-B - R1 BUCLE 0 IPV4



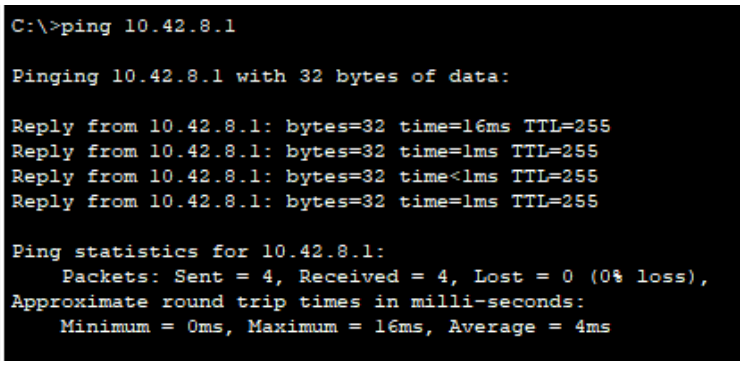
Fuente: Autor

Figura 32. Verificación conectividad PC-B - R1 BUCLE 0 IPV6



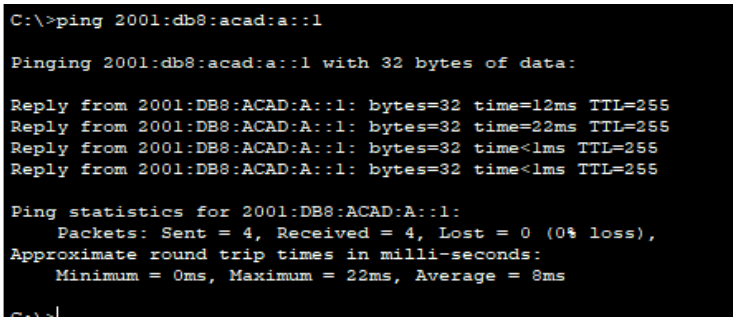
Fuente: Autor

Figura 33. Verificación conectividad PC-B - R1 G0/0/1.20 IPV4



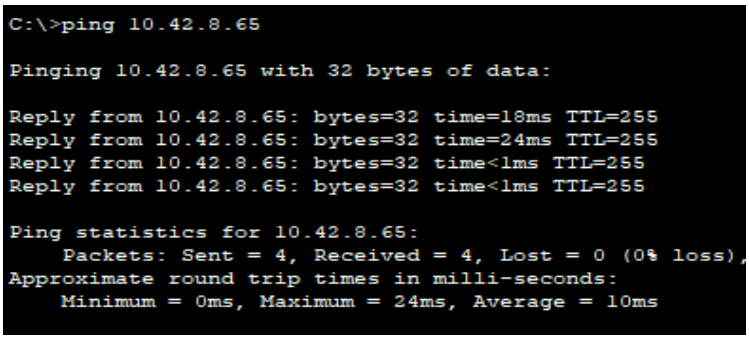
Fuente: Autor

Figura 34. Verificación conectividad PC-B - R1 G0/0/1.20 IPV6



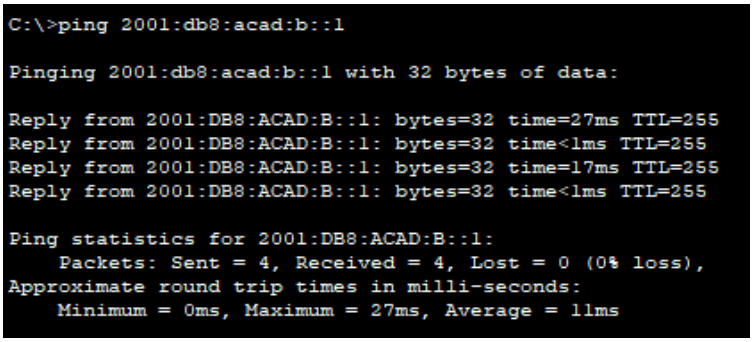
Fuente: Autor

Figura 35. verificación conectividad PC-B - R1 G0/0/1.30 IPV4



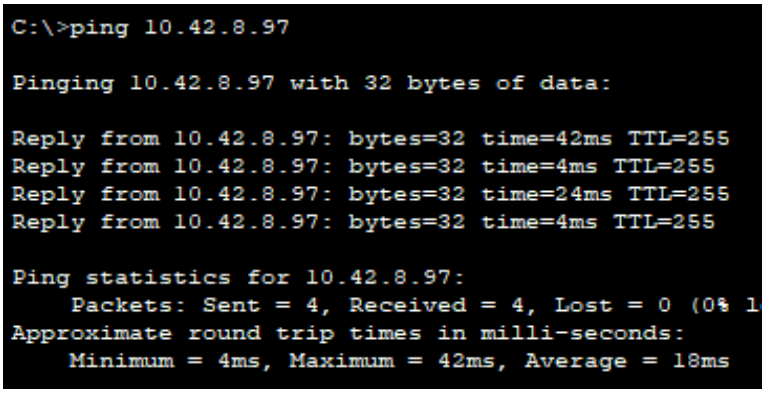
Fuente: Autor

Figura 36. Verificación conectividad PC-B - R1 G0/0/1.30 IPV6



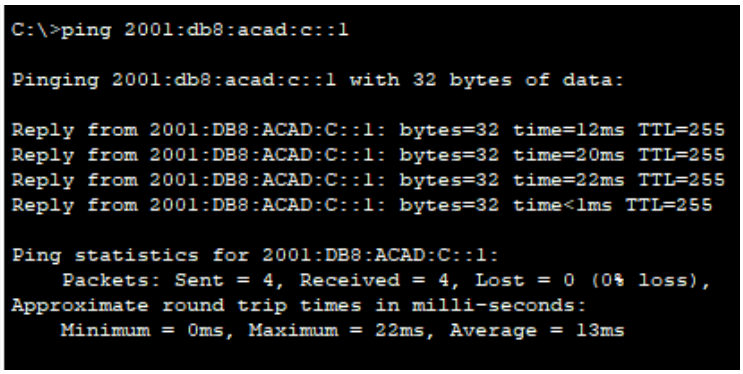
Fuente: Autor

Figura 37. Verificación conectividad PC-B - R1 G0/0/1.40 IPV4



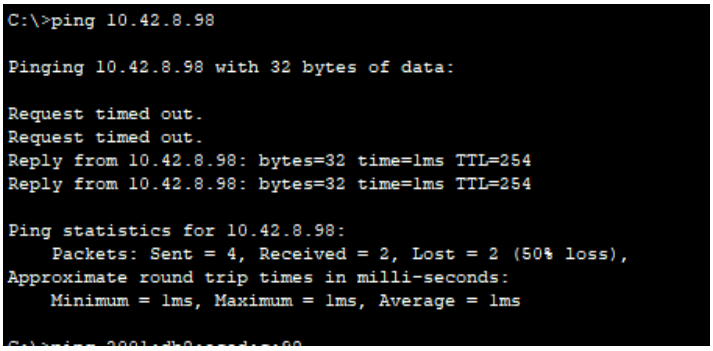
Fuente: Autor

Figura 38. verificación conectividad PC-B - R1 G0/0/1.40 IPV6



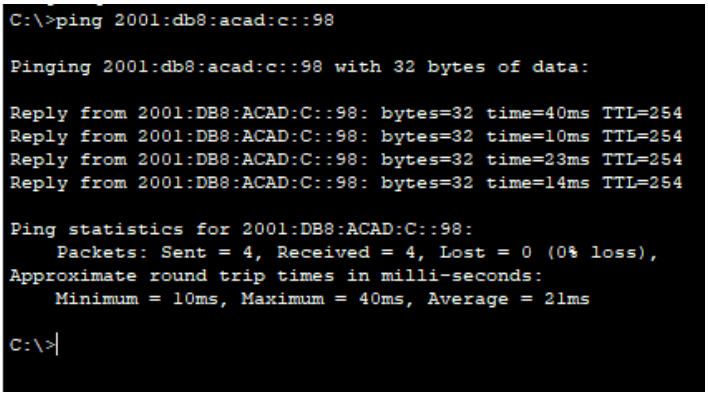
Fuente: Autor

Figura 39.Verificacion conectividad PC-B - S1, VLAN IPV4



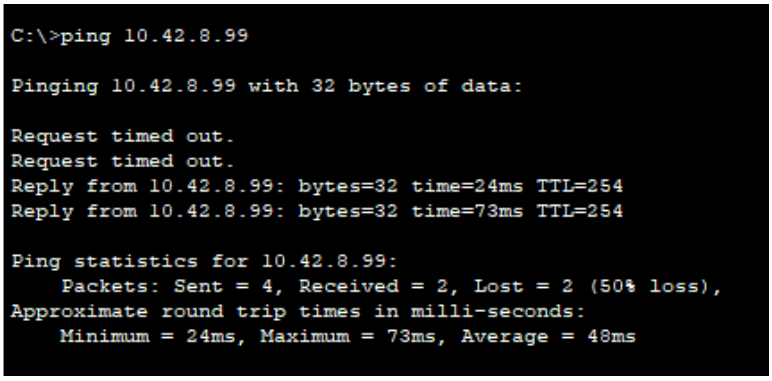
Fuente: Autor

Figura 40.Verificacion conectividad PC-B - S1, VLAN IPV6



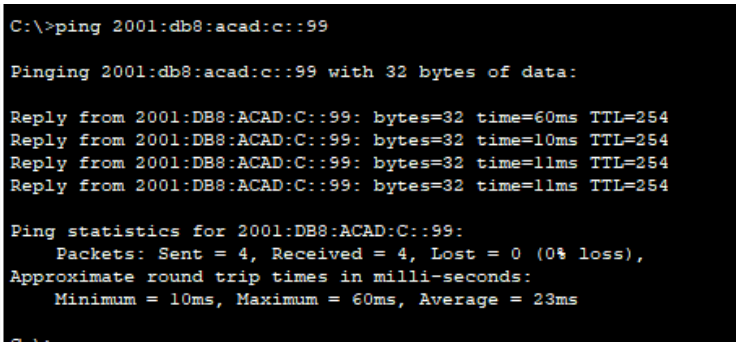
Fuente: Autor

Figura 41. Verificación conectividad PC-B - S2, VLAN IPV4



Fuente: Autor

Figura 42. Verificación conectividad PC-B - S2, VLAN IPV6



Fuente: Autor

CONCLUSIONES

Se cumple con los objetivos que se establecieron con el desarrollo del escenario 1, donde se construyó la solución en el simulado la red dada, desarrollando el esquema de direccionamiento IP para las redes LAN, de esta manera se procede a la configuración de aspectos básicos para los dispositivos como lo es nombramiento de los dispositivos, ajustes básicos de seguridad para el router y el switch, luego se configuro los hosts requeridos en la red y por último la verificación de conectividad.

Al realizar el escenario 2 se logra poner en práctica la habilidades, capacidades y destrezas, adquiridas previamente en el curso en esta se hizo énfasis en la aplicabilidad de procesos que cumplieran de manera satisfactoria con las exigencias del escenario, y se lleva a cabo la implementación de la topología diseñada para tal fin.

Luego de realizar las respectivas configuraciones para activar el protocolo DCHP para direccionamiento IPv4 e IPv6, en este se concluye que es indicado para la administración de direcciones por su facilidad. Fue indispensable manejar los fundamentos principales de los protocolos que existen actualmente para las redes, permitiendo así accedes o transferir información a todos los dispositivos de una forma segura y que admitan conectividad por cable o inalámbrica a una red desde cualquier lugar.

BIBLIOGRAFIA

Bitacora Byte. (18 de julio de 2017). Configurar DHCP en router CISCO. Recuperado el 13 de noviembre de 2022, de Bitacora Byte: https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/

Capitulo 4. Principios de Conmutación y Enrutamiento - ComDatosGrupo4. (s. f.). Recuperado 15 de octubre de 2022, de https://sites.google.com/site/comdatosgrupo4/contenidos/cap4_conmutacion-enrutamiento

Mistry, Z. & Patil, S. (2022, 16 agosto). Enrutamiento, conmutación, seguridad de puertos y protocolo VLAN Trunking (Spanish Edition). Ediciones Nuestro Conocimiento.

UNAD (2017). Configuración de Switches y Routers [OVA]. https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

3.1.4 Direccionamiento IP - Redes De Computadoras. (s. f.). Recuperado 15 de octubre de 2022, de https://sites.google.com/site/investigacionesitlm/3-capas-inferiores-del-modelo-osi-y-tcp-ip/3-1-4-direccionamiento-ip

ANEXOS

Link escenario 1

https://drive.google.com/file/d/172t0alOgdyDDhph760fd8PxQkmfhZhxA/view?usp=sharing

Link escenario 2

https://drive.google.com/file/d/1Q2IcMwGOOAoZqgbNWDwASfxopWwBMnfG/view?usp=sharing