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

LEONARDY YEPEZ FRAGOZO

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

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

LEONARDY YEPEZ FRAGOZO

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO *DE SISTEMAS*

DIRECTOR:

PAULITA FLOR

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

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

VALLEDUPAR 27 DE NOVIEMBRE DE 2022

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN: (Redes de área local virtual) son redes lógicas autónomos centralmente de una igual red física.

DHCP: Es un protocolo de proporción dinámica el cual un servidor DHCP determina rápidamente una dirección IP, mascara de red y Gateway establecido a un host.

OSPF: Es un protocolo de enrutamiento sin clase que utiliza el conocimiento de áreas para ejecutar la escalabilidad, desarrollado como substitución del protocolo de routing vector distancia RIP.

EtherChannel: Es una tecnología que consiente que dos o más puertos físicos se ajusten en un puerto lógico que proporciona alta disponibilidad y mayor ancho de banda.

Loopback: Es una interfaz lógica interna del router. Y no se determina a ningún puerto físico y perpetuamente está activa.

[1] ALVARO, M. Tipos de Banner en Dispositivos Cisco. (2019)
[2] MICROSOFT. Protocolo de configuración dinámica de host (DHCP). (2019)
[3] WALTON, Alex. Qué es default Gateway.
[4] FERNÁNDEZ, Yubal. IPv6: qué es, para qué sirve y qué ventajas tiene. (2019)
[5] García, F. ¿Que son las líneas vty Cisco?. (2018)
[6] DE LUZ, Sergio. VLANs: Qué son, tipos y para qué sirven. (2022)

RESUMEN

Como En esta actividad lleva a cabo se avala el aprendizaje de lo visto en el diplomado de CCNA en cada una de sus unidades, por medio de actividades en donde se puso en práctica estos conocimientos con base a ejercicios prácticos, esta practicidad se debe evidenciar en los escenarios 1 y 2, que se encuentran en este trabajo, en el cual se desarrollaron los ejercicios propuestos en la guía, en los cuales se hace una configuración de una red, su esquema de direccionamiento y subnetting, la configuración de sus dispositivos como lo son el Reuter y el switch desde su parte inicial y los ajustes básicos de seguridad de los mismos así como el direccionamiento ip de los equipos de cómputo conectados a estos, lo cual se puede observar en las diferentes figuras que se encuentran en este documento en donde se refleja el desarrollo de las actividades mencionadas.

PALABRAS CLAVES: Configuración, Dispositivos, Ip, Seguridad, Redes, Electrónica

ABSTRACT

In this activity, the learning of what was seen in the CCNA diploma in each of its units is endorsed, through activities where this knowledge was put into practice based on practical exercises, this practicality must be evidenced in the scenarios 1 and 2, found in this work, in which the exercises proposed in the guide were developed, in which a network configuration is made, its addressing and subnetting scheme, the configuration of its devices as they are the Router and the switch from its initial part and the basic security settings of the same as well as the ip addressing of the computer equipment connected to them, which can be seen in the different figures found in this document where reflects the development of the aforementioned activities.

KEY WORDS: Configuration, Devices, Ip, Security, Networks

INTRODUCCIÓN

El En esta actividad, explorará una red relativamente compleja que pone de relieve algunas de las características de Packet Tracer.
En el escenario 1, se llevó a cabo la secuencia de los pasos solicitados en donde se realizó una codificación, en la red que se ha venido manejando, en donde por medio de cada función y su respectivo código se busca generar el comportamiento requerido en el sistema que se desarrolla en este caso se busca Reuter Swiss que requiere para una buena seguridad informática de envío de paquetes en su recomendación, siguiendo la secuencia en el Packet Tracer.
En el escenario 2, se llevó a cabo una codificación de seguridad para el router los Swiss, además de la respectiva configuración de las VLANs, los puertos de acceso y trocales de cada uno de los switches, en donde se tiene de referencia las tablas de función y respectivo código para el desarrollo de los parámetros requeridos en el desarrollo del sistema que se ha venido trabajo de la red.

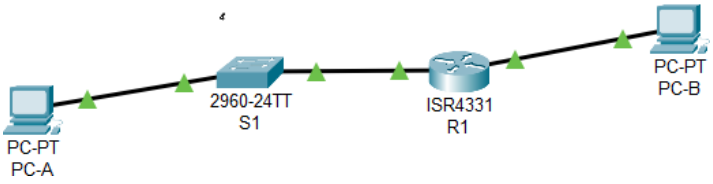
Teniendo presente los adelantos tecnológicos referente a la conectividad y las múltiples maneras de comunicación, tanto entre seres vivos, como en dispositivos electrónicos, se prueba la urgente necesidad como ingeniero en sistemas de conocer dominar y ejercer las múltiples maneras de diseñar las construcciones de red que permiten transmitir datos entre sistemas y contar con los recursos de los dispositivos que son parte de la red, del mismo modo, el diseño de red permite el almacenamiento y procesamiento de la información debido a que posibilita compartir programas, archivos y datos.
protocolos de red, configuración de estabilidad de los dispositivos y demás límites de configuración, lo anterior es viable por medio de la consola de los dispositivos o por medio de un pc conectado de forma directa al dispositivo por medio de una secuencia de comandos para tal fin.

DESARROLLO ESCENARIOS

ESCENARIO 1

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 administrarse de forma segura

Figura 1: topología de red escenario 1



Fuente: Autor

Tabla 1. Direccionamiento IP Escenario 1

Item	**Requerimiento**
Dirección de Red	172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	Última dirección de host de la subred LAN1
R1 G0/0/0	Última dirección de host de la subred LAN2

S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Décima dirección de host de la subred LAN1
PC-B	Décima dirección de host de la subred LAN2

Tabla 2. direccionamiento para LAN 1 y LAN 2

	Dirección de Red	**Máscara**	**Primer IP**	**Broadcast**
LAN1	172.26.3.128	255.255.255.128	172.26.3.1	172.26.3.127
LAN2	172.26.3.192	255.255.255.192	172.26.3.129	172.26.3.191

Fuente: Autor

Tabla 3. direccionamiento escenario 1

Item	**Requerimiento**
Dirección de Red	Dirección de Red 172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula. (26)
Requerimiento de host Subred LAN1	60=62 Host 172.26.3.128 172.26.3.127 255.255.255.128
Requerimiento de host Subred LAN2	20=30 Host 172.26.3.192 172.26.3.191 255.255.255.192
R1 G0/0/1	172.26.3.1
R1 G0/0/0	172.26.3.129
S1 SVI	172.26.3.2
PC-A	172.26.3.126
PC-B	172.26.3.194

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 4. Configuración R1

Tarea	**Especificación**
Desactivar la búsqueda DNS	Router> Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	Router> Router>enable Router#configure terminal Router(config)#Hostname R1
Nombre de dominio	R1> R1>enable R1#configure terminal R1(config)# ip domain-name ccna-sa.com
Contraseña cifrada para el modo EXEC privilegiado	R1> R1>enable R1#configure terminal R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	R1> R1>enable R1#configure terminal R1#line console 0 R1(config-line)#password ciscoconpass R1 (config-line) #login R1 (config-line) #exit
Establecer la longitud mínima para las contraseñas	R1> R1>enable R1#configure terminal

	R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1> R1>enable R1#configure terminal R1(config)# username admin secret admin1pass
Configure el inicio de sesión en las líneas VTY para que use la base de datos local	R1> R1>enable R1#configure terminal R1(config)# line vty 0 6 R1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1> R1>enable R1#configure terminal R1(config)# line vty 0 6 R1(config-line) #login local R1(config-line) # transport input ssh R1(config-line) #exit
Cifrar las contraseñas de texto no cifrado	R1> R1>enable R1#configure terminal R1(config)# service password-encryption
Configurar un banner MOTD	R1> R1>enable R1#configure terminal R1(config)# banner motd "R1 -Leonardy Yepez Fragozo - Ing.Sistemas" R1(config)#exit
	R1> R1>enable

Configuración de interface G0/0/0	R1#configure terminal R1(config)#int g0/0/1 R1(config-if) #description to Lan 1 R1(config-if) #ip address 172.26.3.126 255.255.255.128 R1(config-if) #no shutdown R1(config-if) #exit
Configuración de interface G0/0/1	R1> R1>enable R1#configure terminal R1(config)#int g0/0/0 R1(config-if) #description to Lan 2 R1(config-if) ip address 172.26.3.129 255.255.255.192 R1(config-if) #no shutdown R1(config-if) #exit
Generar una clave de cifrado RSA	R1(config)#**domain name ccnalab.com** R1(config)#**crypto keys generate RSA** The name for the keys will be: 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] R1(config)#exit *Mar 1 5:14:40.398: %SSH-5-ENABLED: SSH 1.99 has been enabled R1#

	%SYS-5-CONFIG_I: Configured from console by console

Fuente: Autor

Configuración Router R1

- Nuestro primer paso será desactivar la búsqueda DNS del Router entonces debemos dar clic en el dispositivo, luego en la pestaña ¨CLI¨ y luego presionamos la tecla ENTER nos permita escribir, y escribimos los siguientes comandos esto nos permitirá realizar esta configuración.

Router>enable **Código para ingresar a el modo privilegiado**

Router#configure terminal **Entramos en modo configuración**

Router(config)#no ip domain-lookup **desactivamos la búsqueda DNS**

- Ya estando en modo de configuración escribimos el siguiente comando para ponerle nombre a nuestro dispositivo y también el nombre del dominio.

Router(config)#hostname R1 **Asignamos el nombre del dispositivo**

R1(config)#ip domain-name ccna-sa.com **Asignamos el nombre del Dominio**

- Para la parte de seguridad se asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

R1(config)#enable secret ciscoenpass **Asignamos contraseña modo privilegiado**

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

R1(config)#line console 0 **Ingresamos a la consola**

- Luego, dentro del line console 0, asignamos la contraseña con el siguiente comando, y dar exit para salir de la consola

R1(config-line) #password ciscoconpass **Asignamos contraseña acceso consola**

R1(config-line) #loginR1(config-line) #exit

- Con el siguiente comando security passwords min-length ya dentro del modo de configuración asignamos la longitud mínima para las contraseñas.

R1(config)#security passwords min-length 10 **Longitud minima para contraseña**

- Creación de un usuario administrativo en la base de datos local, dentro del modo de configuración-

R1(config)#username admin password admin1pass **Asignamos un usuario y una contraseña**

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

R1(config)#line vty 0 4 **Con el siguiente código cambiamos del modo de configuraciónGlobal a las líneas vty 0 4**

- Estando en el menú de la base local se escribe el siguiente comando para el inicio de sesión.

R1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

R1(config-line) #transport input ssh **Configuración VTY para solo conexiones ssh**

- Para cifrar las contraseñas, dentro del menú de configuración:

R1(config)#service password-encryption **Código de cifrado de contraseñas**

Configuración del banner motd, con el nombre del dispositivo, nombre del estudiantey programa continuando en el menú de configuración:

R1(config)#banner motd "R1 LEONARDY JOSE YEPEZ FRAGOZO PROGRAMA: INGENIERIA DE SISTEMAS" **Configuramos el motd banner**

- Configuración de la interface G0/0/0, asignación de IP:

R1(config)#interface g0/0/0 **Acedemos a la interface**

R1(config-if) #ip address 172.26.3.126 255.255.255.128 **Asignamos la dirección IP y mascarade RED**

R1(config-if) #no shutdown **Realizamos la activación de Puerto**

- Configuración de la interface G0/0/1, asignación de IP:

R1(config)#interface g0/0/1 **Acedemos a la interface**

R1(config-if) #ip address 172.26.3.129 255.255.255.192 **Asignamos la dirección IP y mascarade RED**

R1(config-if) #no shutdown **Realizamos la activación de Puerto**

- Generar una clave de cifrado RSA: 1024 bit

R1(config)#crypto key generate rsa

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 5. Configuración S1

Tarea Especificación	**Especificaciones y Configuración**
Desactivar la búsqueda DNS	Switch> Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup
Nombre del Switch	Switch> Switch>enable Switch#configure terminal Switch(config)#Hostname S1 S1(config)#
Nombre de dominio	S1> S1>enable S1#configure terminal S1(config)# ip domain-name ccna-lab.com

Contraseña cifrada para el modo EXEC privilegiado	S1> S1>enable S1#configure terminal S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	S1> S1>enable S1#configure terminal S1(config)#line console 0 S1(config-line) #password ciscoconpass S1 config-line) #login S1 (config-line) #exit
Crear un usuario administrativo en la base de datos local	S|> S1>enable S1#configure terminal S1(config)#username admin secret admin1pass

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1> S1>enable S1#configure terminal S1(config)# line vty 0 6 S1(config-line) #login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1> S1>enable S1#configure terminal S1(config)# line vty 0 6 S1(config-line) #login local S1(config-line) # transport input ssh S1(config-line) #exit

Cifrar las contraseñas de texto no cifrado	S1> S1>enable S1#configure terminal S1(config)# service password-encryption
Configurar un MOTD Banner	S1> S1>enable S1#configure terminal S1(config)# banner motd "prohibido el acceso no autorizado"
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccnalab.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)	S1(config)#interface vlan 1 *Mar 1 5:59:3.643: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if) #ip address 172.26.3.2 255.255.255.192
Configuración del gateway predeterminado	S1(config)#ip default-gateway 172.26.3.126

Configuración Switch S1

- Nuestro primer paso será desactivar la búsqueda DNS del Router entonces debemos dar clic en el dispositivo, luego en la pestaña ¨CLI¨ y luego presionamos la tecla ENTER nos permita escribir, y escribimos los siguientes comandos esto nos permitirá realizar esta configuración.

Swtich>enable **Código para ingresamos a el modo privilegiado**

Switch#Configure termina **Entramos en modo configuración**

Switch(config)#no ip domain-lookup **Desactivamos las búsqueda DNS**

- Ya estando en modo de configuración escribimos el siguiente comando para ponerle nombre a nuestro dispositivo y también el nombre del dominio
-

Router(config)#hostname S1 **Asignamos el Nombre del dispositivo**

S1(config)#ip domain-name ccna-sa.com **Asignamos el nombre del Dominio**

S1(config)#enable secret ciscoenpass **Asignamos la contraseña del modo privilegiado**

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

S1(config)#line console 0 **Ingresamos a la consola**

- Luego, dentro del line console 0, asignamos la contraseña con el siguiente comando, y damos exit para salir de la consola

S1(config-line) #password ciscoconpass **Asigno la contraseña acceso a la consola**

S1(config-line) #login

S1(config-line) #exit

S1(config-if-range) #shutdown

S1(config)#username admin password admin1pass **Asignamos un usuario y una contraseña**

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

S1(config)#line vty 0 4 **Realizamos el cambio del modo de**

configuración global las

líneas vty 0 4

- Luego en el menú de la base local escribir el siguiente comando para el inicio de sesión

S1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH.

S1(config-line) #transport input ssh **Configuracion VTY solo conexiones ssh**

- Para cifrar las contraseñas, dentro del menú de configuración:

S1(config)#service password-encryption **Cifrado de contraseñas**

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

S1(config)#banner motd "S1 LEONARDY JOSE YEPEZ FRAGOZO PROGRAMA: INGENIERIA DE SISTEMAS" **Realizamos la configuración motd banner**

- Configuración de la interface Vlan1, asignación de IP:

S1(config)# interface vlan1 **Acedemos a la VLAN**

*Mar 1 0:24:35.474: %SSH-5-ENABLED: SSH 1.99 has been enabled

S1(config-if) #ip address 172.26.3.2 255.255.255.192 **Asignacinamos la IP y Mascarade red**

S1(config-if) #no shutdown

- Generar una clave de cifrado RSA: 1024 bit

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.

Paso 2. Configurar los equipos

Tabla 6. Configuración PC-A

Configuración de red de PC-A	
Descripción	**PC-A**
Dirección Física	0009.7C84.E193
Dirección Ip	172.26.3.10
Mascara de subred	255.255.255.128
Gateway predeterminado	172.26.3.62

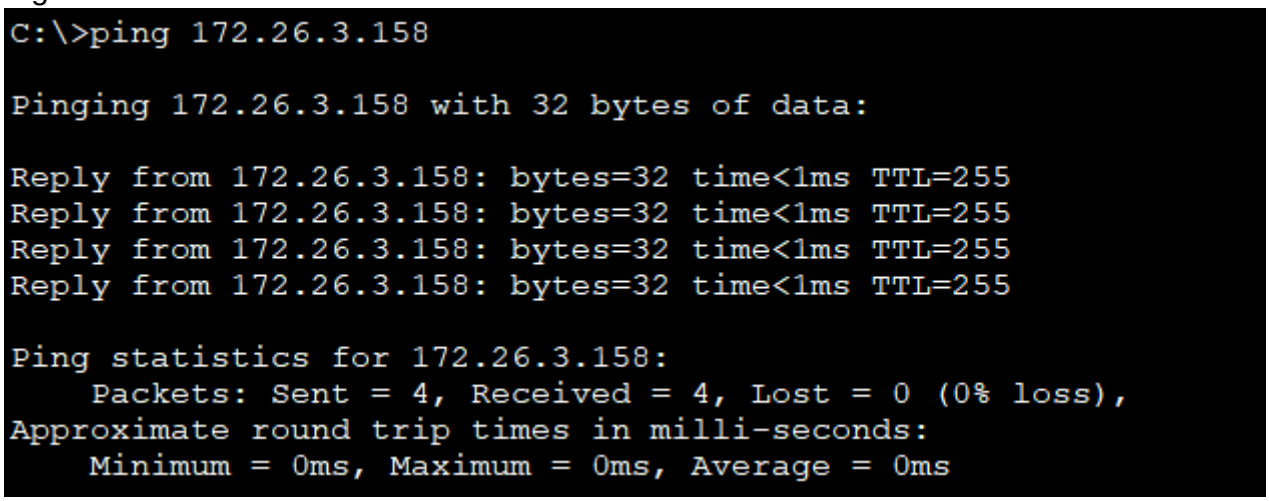
Fuente: Autor

Tabla 7. Configuración PC-B

Configuración de red de PC-B	
Descripción	**PC-B**
Dirección Física	0001.C744.92C3
Dirección Ip	172.26.3.138
Mascara de subred	255.255.255.192
Gateway predeterminado	172.26.3.158

Fuente: Autor

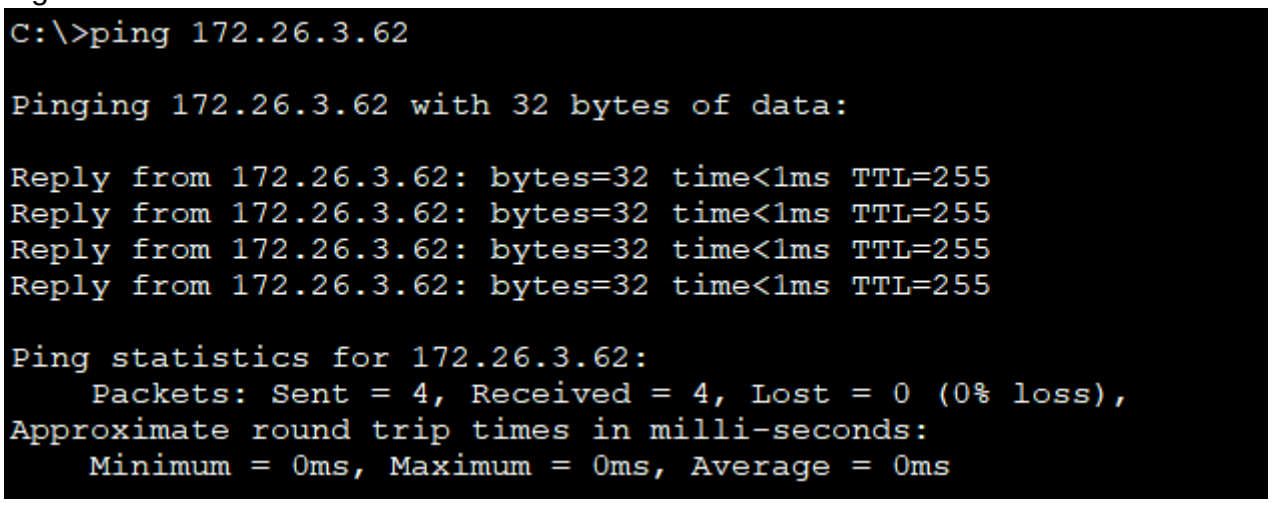
ping PC-A a R1 G0/0/0
Figura 2.



Fuente: Autor

Como se evidencia en la figura 2, el 172.26.3.158 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

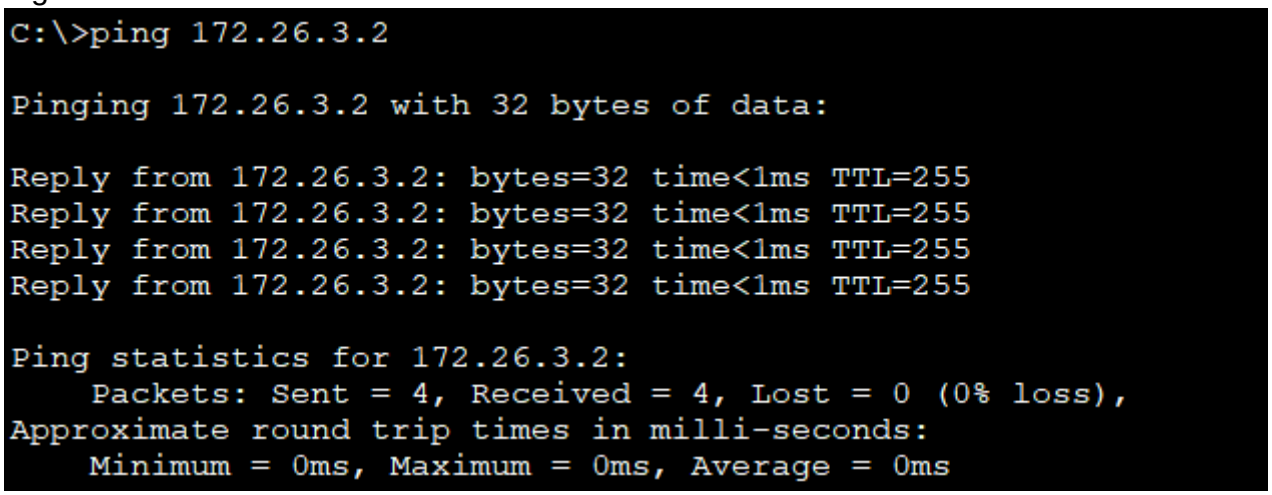
ping PC-A a R1 G0/0/1
Figura 3.



Fuente: Autor

Como se evidencia en la figura 3, el 172.26.3.62 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

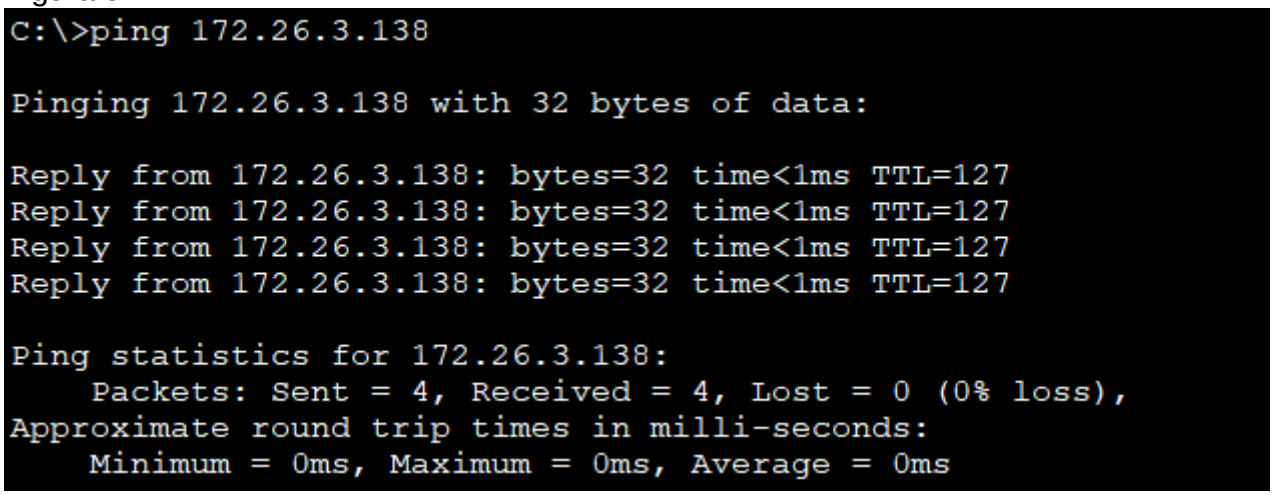
ping PC-A a S1 VLAN 1
Figura 4.



Fuente: Autor

Como se evidencia en la figura 4, el 172.26.3.2 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

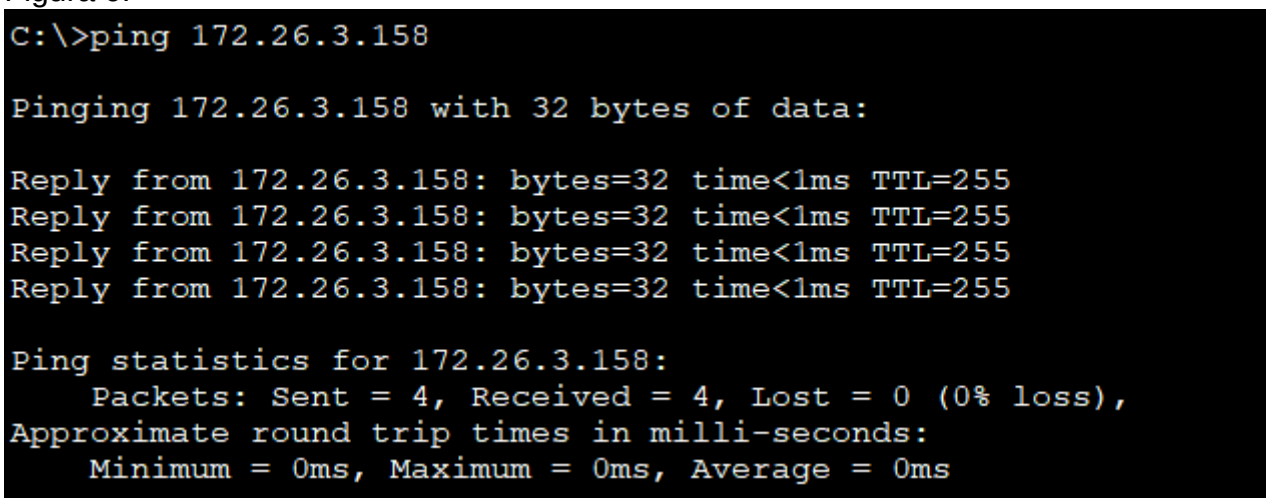
ping PC-A a pc-b
Figura 5.



Fuente: Autor

Como se evidencia en la figura 5, el 172.26.3.138 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

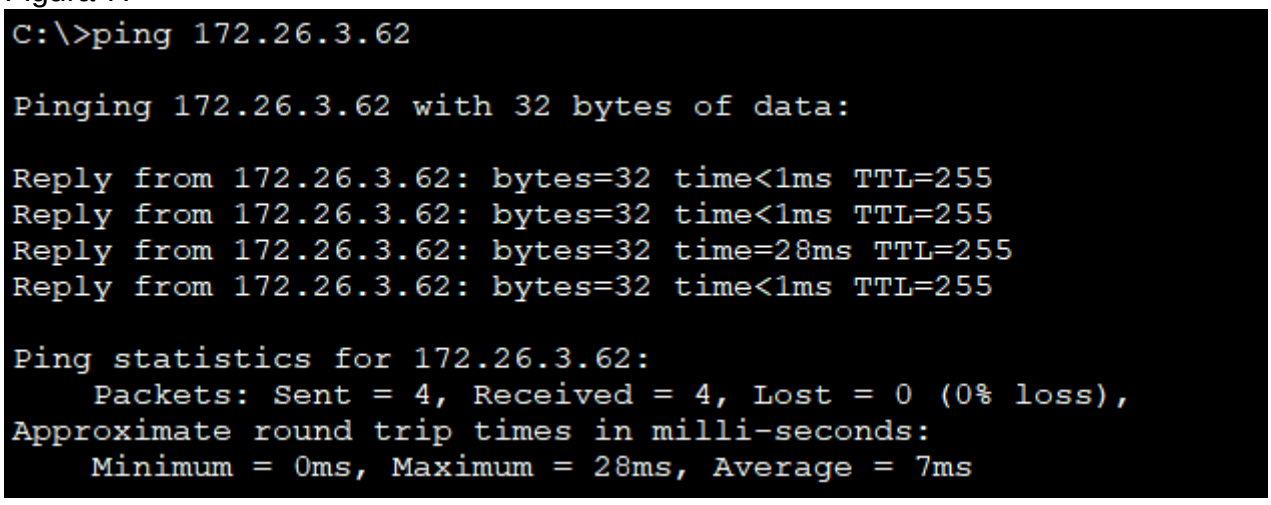
ping de PC-B a R1 G0/0/0
Figura 6.



Fuente: Autor

Como se evidencia en la figura 6, el 172.26.3.158 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

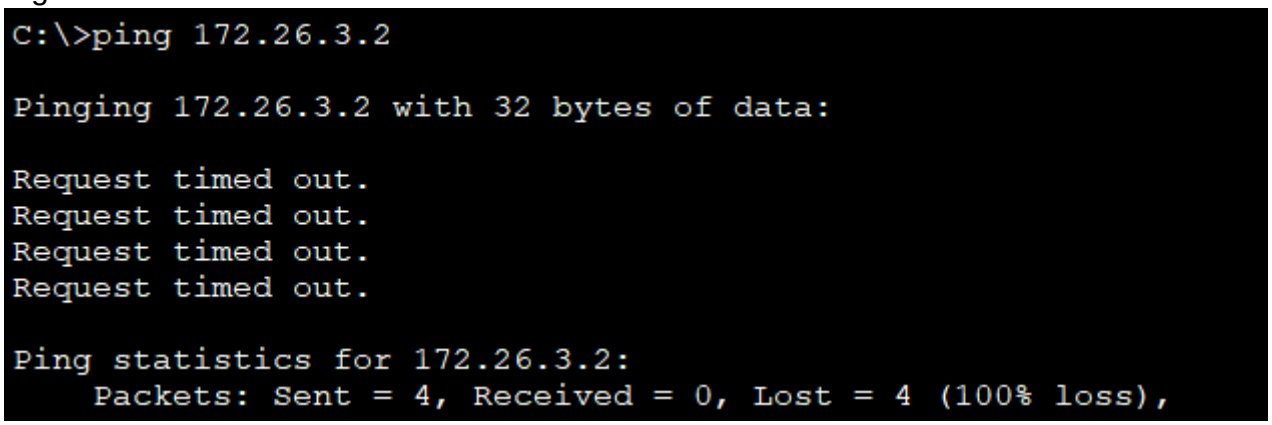
ping de PC-B a R1 G0/0/1
Figura 7.



Fuente: Autor

Como se evidencia en la figura 7, el 172.26.3.62 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a S1 VLAN1
Figura 8.



Fuente: Autor

ESCENARIO 2

Topología

Figura 3. Topología de red escenario 2

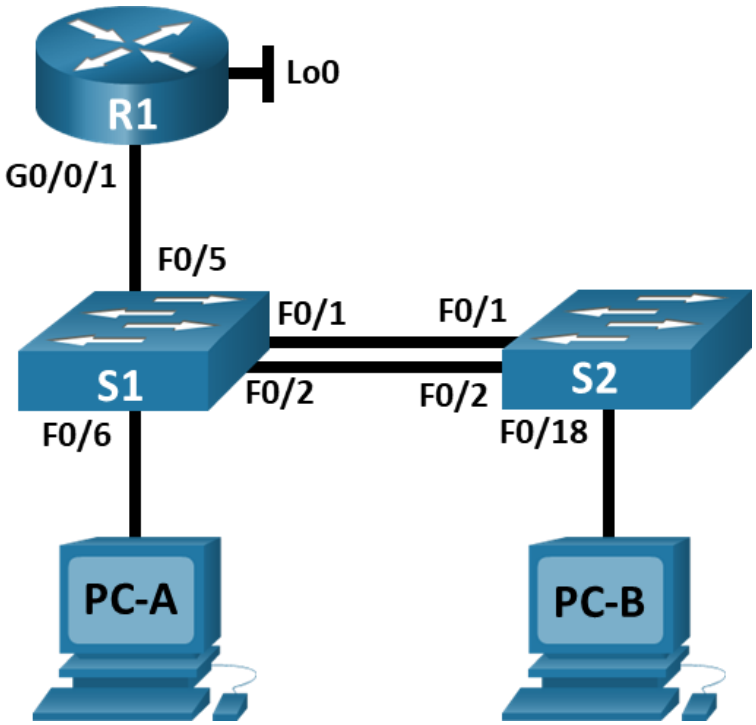


Tabla 8. VLAN Escenario 2

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

Tabla 9. Asignación de Direcciones IP

Dispositivo / interfaz	**Dirección IP / Prefijo**	**Puerta de enlace predeterminada**
R1 G0/0/1.20	10.XY.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.XY.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.XY.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
	209.165.201.1 /27	No corresponde
R1 Loopback0	2001:db8:acad:209: :1 /64	No corresponde

S1 VLAN 4	10.XY.8.98 /29	10.26.8.97
S2 VLAN 4	2001:db8:acad:c: :98 /64 fe80: :98 10.XY.8.99 /29 2001:db8:acad:c: :99 /64	No corresponde No corresponde 10.26.8.97 No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4 2001:db8:acad:a: :50 /64	DHCP para puerta de enlace predeterminado IPv4 Fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminado IPv4
	2001:db8:acad:b: :50 /64	Fe80::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 vuelva acargar los dispositivos.
- Después de recargar el switch, configure la plantilla SDM para que admita IPv6según sea necesario y vuelva a cargar el switch.

Tabla 10. Comandos inicializar y recargar Router y Switch escenario

Tarea Comando de IOS	Tarea Comando de IOS
Eliminar el archivo del Router	Router > enable Router # erase startup-config
Volver a cargar el routers	Router # reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch > enable Switch # delete vlan.dat Switch # erase startup-config
Volver a cargar ambos switches	Switch # reload
Configure la plantilla SDM en los switch para que admita IPv6	Switch > enable Switch # config t Switch(config)# sdm prefer dual-ipv4-and-ipv6 routing

Fuente: Autor

Se elimina el archivo de configuración de inicio de la NVRAM del Router 0, Se accede al modo privilegiado con el comando enable, estando en el modo privilegiado se le da el comando erase startup-config, le pregunta que si está seguro confirmar y se le da clic enter.

Se recarga el Switch 0 con el comando reload

Configuración Planilla SDM de Switch 0

En modo privilegiado se accede a configuración terminal, se le da comando sdm prefer dual-ipv4-and-ipv6 routing. Se copia las permutas con el comando copy run start y luego se recarga con el comando reload.

Paso 1 Configurar R0

En la configuración del Router 0 se ejecutará las sucesivas configuraciones como se muestra en la tabla 4. donde procedemos a desactivar la búsqueda DNS, creamos el nombre al router, se crea un dominio, se instauran las contraseñas cifrada para el modo privilegiado, se configura contraseña de acceso a consola, se establece una longitud mínima para la contraseña, se crear un usuario administrador en la base de datos local, se configurar el inicio de sesión en las líneas VTY hacia que use la base de datos local, se configurar líneas VTY solo aceptando conexiones SSH, se Cifran las contraseñas de texto no cifrado, se Dispone un MOTD Banner, se habilita el routing IPv6, se configurar la interfaz G0/0/1 y subinterfaces, se configura la interfaz Loopback0 y se forma la clave de cifrado RSA.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configuración R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router>enable Router# configure terminal Router(config)#hostname R1 R1(config)#
Nombre de dominio	R1>enable R1#configure terminal R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	R1> enable R1# configure terminal R1(config)# enable secret ciscoenpass R1(config)#
Contraseña de acceso a la consola	R1> enable R1# configure terminal R1(config)# line console 0 R1(config-line)# password ciscoconpass R1(config-line)# login R1(config-line)# exit R1(config)#
Establecer la longitud mínima para las contraseñas	R1#configure terminal R1(config)#security passwords min-length 10

Crear un usuario administrativo en la base de datos local	R1#configure terminal R1(config)#username admin password admin1pass R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#configure terminal R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit R1(config)#
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#exec-timeout 10 R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit
Configure un MOTD Banner	R1# configure terminal R1(config)# banner motd "R1 - Leonardy José Yepez Fragozo - Ing.Sistemas" R1(config)# exit
Habilitar el routing IPv6	R1# configure terminal R1(config)# ipv6 unicast-routing R1(config)# exit

Configurar interfaz G0/0/1 y subinterfaces	R1#config terminal R1(config)#interface gigabitEthernet 0/0/1.2 R1(config-subif)#encapsulation dot1Q 2 R1(config-subif)#ip address 10.26.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a: :1 /64 R1(config-subif)#ipv6 address Fe80::1 link-local R1(confiig-subif)#description vlan 2 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.3 R1(config-subif)#encapsulation dot1Q 3 R1(config-subif)#ip address 10.26.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b: :1 /64 R1(config-subif)#ipv6 address Fe80::1 link-local R1(config-subif)#description vlan3 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1.4 R1(config-subif)#encapsulation dot1Q 4

	R1(config-subif)#ip address 10.26.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c: :1 /64 R1(config-subif)#ipv6 address Fe80::1 link-local R1(config-subif)#description vlan4 R1(config-subif)#no shutdown R1(config-subif)#exit R1(config)#interface gigabitEthernet 0/0/1 R1(config-if)#no shutdown
Configure el Loopback0 interface	R1#configure terminal R1(config)#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
Generar una clave de cifrado RSA	R1(config)#crypto key generate rsa Chose the size of the key modulus in the range of 360 to 2048 for your general purpose key. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:1024

Fuente: Autor

Configuración Router R1

- Para desactivar la búsqueda DNS del Router lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Router>enable **Ingresamos a el modo privilegiado**
Router#configure terminal **luego ingresamos al modo de configuración**

Router(config)#no ip domain-lookup **También desactivar la búsqueda DNS**

- Como se encuentra en el modo de configuración, se pueden escribir los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname R1 **Asignamos nombre del dispositivo**

R1(config)#ip domain-name ccna-sa.com **Asignamos nombre del Dominio**

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando.

R1(config)#enable secret ciscoenpass **Creamos la contraseña de modo privilegiado**

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración.

R1(config)#line console 0 **Luego ingresamos a la consola**

- Luego, dentro del line console 0, asignamos la contraseña con el siguiente comando, y dar exit para salir de la consola

R1(config-line) #password ciscoconpass **Creamos la contraseña de acceso a la consola**

R1(config-line) #login

R1(config-line) #exit

- Con el comando security passwords min-length dentro del modo de configuración asignamosla longitud mínima para las contraseñas, en este escenario será de 10

R1(config)#security passwords min-length 10 **LA longitud minima de contraseña**

- Creación de un usuario administrativo en labase de datos local, dentro del modo de configuración

R1(config)#username admin password admin1pass **Asignamos un usuario y una contraseña**

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

R1(config)#line vty 0 15 **Cambio del modo de configuración Global a las líneas vty 0 15**

- Dentro del menú de la base local se escribe el siguiente comando para el inicio de sesión

R1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

R1(config-line) #transport input ssh **Configuración VTY solo conexiones ssh**

Para cifrar las contraseñas, dentro del menú de configuración:

R1(config)#service password-encryption **Cifrado de contraseñas**

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

R1(config)#banner motd "R1 LEONARDY JOSE YEPEZ FRAGOZO PROGRAMA: INGENIERIA DE SISTEMAS" **Configuración motd banner**

- Configuración del enrutamiento IPv6

R1(config)#ipv6 unicast-routing **Se activa el enrutamiento IPv6**

- Configuración de la interface G0/0/1, Sub interfaces y asignación de IPv4 e IPv6:

R1(config)#int g0/0/1.20 **Se accede a la sub interface**
R1(config-subif) #encapsulation dot1q 2 0 **Se establece el modo de encapsulación**

R1(config-subif) #description Docentes **Se asigna una descripción**

R1(config-subif) #ip address 10.26.8.1 255.255.255.192 **se configura la IPv4 con su respectiva mascara de sub red**

R1(config-subif) #ipv6 address 2001:db8:acad:a::1/64 **Asignacion de Ipv6**

R1(config-subif)#ipv6 address fe80::1 link-local **Enlace local de la Ipv6**

- Se repite el anterior procedimiento para las sub interfaces g0/0/1.30, g0/0/1.40 y g0/0/1.56, variando únicamente su direccionamiento IP el cual está establecido en la tabla nº titulada, asignación de direcciones IP

- Configuracion de la Interface Loopback0

R1(config-if)#int loopback 0 **Se accede a la Interface**

R1(config-if)#ip address 209.165.201.1 255.255.255.224 **Asignacion de IPv4 con su respectiva mascara de red**

R1(config-if)#ipv6 address 2001:db8:acad:209: :1/64 **Asignacion de IPv6**

R1(config-if)#ipv6 address fe80::1 link-local **Enlace local de IPv6**

R1(config-if)#description internet **Descripcion de la interface**

- Generar una clave de cifrado RSA: 1024 bit

Paso 3: Configure S1

Las tareas de configuración incluyen lo siguiente:

SWITCH 1:

Tabla 12. Configuración S1

Tarea	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#
Nombre del switch	switch>enable switch# configure terminal switch(config)#hostname S1 S1(config)#

Nombre de dominio	S1>enable S1#configure terminal S1(config)#ip domain-name ccnalab.com
Contraseña cifrada para el modo EXEC privilegiado	S1> enable S1# configure terminal S1(config)# enable secret ciscoenpass S1(config)#
Contraseña de acceso a la consola	S1> enable S1# configure terminal S1(config)# line console 0 S1(config-line)# password ciscoconpass S1(config-line)# login S1(config-line)# exit S1(config)#
Crear un usuario administrativo en la base de datos local	S1#configure terminal S1(config)#username admin password admin1pass S1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1#configure terminal S1(config)#line vty 0 4 S1(config-line)#login local S1(config-line)#exit S1(config)#
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 4 S1(config-line)#exec-timeout 10 S1(config-line)#transport input ssh S1(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#exit
Configurar un MOTD Banner	S1# configure terminal S1(config)# banner motd"S1 -Leonardy Jose Yepez Fragozo - Ing.Sistemas" S1(config)# exit
Generar una clave de cifrado RSA	S1(config)#crypto key generate rsa Chose the size of the key modulus in the range of 360 to 2048 for your general purpose key. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:1024

Configurar la interfaz de administración (SVI)	S1#configure terminal S1(config)#interface vlan 4 S1(config-vlan)#ip address 10.26.8.98 255.255.255.248 S1(config-vlan)#ipv6 address 2001:db8:acad:c: :98 /64 S1(config-vlan)#ipv6 address Fe80::98 link-local S1(config)#ipv6 route ::/0 2001:db8:acad:c::1 S2#configure terminal S2(config)#interface vlan 4 S2(config-vlan)#ip address 10.26.8.99 255.255.255.248 S2(config-vlan)#ipv6 address 2001:db8:acad:c: :99/64 S2(config-vlan)#ipv6 address fe80::99 link-local S2(config)#ipv6 route ::/0 2001:db8:acad:c::1
Configuración del gateway predeterminado	S1#configure terminal S1(config)#ip default-gateway 10.26.8.97

Fuente: Autor

Configuración Switch S1

- Para desactivar la búsqueda DNS del Switch lo primero que se debe hacer es dar clic en el dispositivo, luego en la pestaña CLI y esperar que el dispositivo permita escribir, posteriormente se utilizan los siguientes comandos para realizar la respectiva configuración

Swtich>enable **Ingresamos a el modo privilegiado**
Switch#Configure terminal **Ingresamos a el modo de configuración**

Switch(config)#no ip domain-lookup **También desactivar la búsqueda DNS**

- Como el dispositivo está en el modo de configuración, se escriben los comandos para asignar el nombre del dispositivo y el nombre del dominio

Router(config)#hostname S1 **Asignamos nombre del dispositivo**

S1(config)#ip domain-name ccna-sa.com **Asignamos nombre del Dominio**

- Para asignar una contraseña cifrada para el modo EXEC privilegiado, dentro del modo de configuración se escribe el comando:

S1(config)#enable secret ciscoenpass **Asignamos la contraseña de modo privilegiado**

- Para asignar la contraseña Ciscoconpass en el acceso a la consola, dentro del modo de configuración:

S1(config)#line console 0 **Luego ingresamos a la consola**

- Luego, dentro del line console 0, asignamos la contraseña con el siguiente comando, y damos exit para salir de la consola

S1(config-line) #password ciscoconpass **Creamos la contraseña de acceso a la consola**

S1(config-line) #login

- Creación de un usuario administrativo en la base de datos local, dentro del modo de configuración

S1(config)#username admin password admin1pass **Asignamos un usuario y una contraseña**

- Para la configuración del inicio de sesión en las líneas VTY para que use la base de datos local, en el modo de configuración, se ingresa el siguiente comando:

S1(config)#line vty 0 15 **Cambio del modo de configuración Global a las líneas vty 0 15**

- Dentro del menú de la base local escribir el siguiente comando para el inicio de sesión

S1(config-line) #login local

- Configuración de la base de datos local para configurar las líneas VTY para que acepten únicamente las conexiones SSH

S1(config-line) #transport input ssh **Configuramos la VTY para solo conexiones ssh**

Para cifrar las contraseñas, dentro del menú de configuración:

S1(config)#service password-encryption **Cifrado de contraseñas**

- Configuración del banner motd, con el nombre del dispositivo, nombre del estudiante y programa continuando en el menú de configuración:

S1(config)#banner motd "S1 LEONARDY JOSE YEPEZ FRAGOZO PROGRAMA: INGENIERIA DE SISTEMAS" **Configuramos el motd banner**

- Configuración de la interface Vlan 40, asignación de IP:

S1(config)# interface vlan 40 **Se accede a la VLAN**
S1(config-if)#ip address 10.26.8.98 255.255.255.248 **Asignamos la IPv4 con mascara de red**

S1(config-if)#ip default-gateway 10.26.8.97 **Configuramos la puerta de enlace preterminado para IPv4**

S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 **Asignamos la direccion IPv6**

S1(config-if)#ipv6 address fe80::98 link-local **Enlace local de IPv6**

S1(config-if)#description Administration **Se asigna una Descripción**

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

Paso 1 Configurar S1

Para la configuración de la construcción de red (VLAN, Trunking, EtherChannel) del Switch 0 se ejecutan las configuraciones como se muestra en la tabla 6. se antecede a crear las Vlan, se crean troncos 802.1Q que utilicen la VLAN 6 nativa, se Crea un grupo de puertos EtherChannel de Capa 2 que use interfaces

F0/1 y F0/2, se Configura el puerto de acceso de host para VLAN 2, se configura la seguridad del puerto en los puertos de acceso y se protegen las interfaces no utilizadas.

Tabla 13. Configuración de la infraestructura de red en S1(Vlan, Trunking, Etherchannel*)*

Tarea	Especificación
Crear VLAN	S1(config)#vlan 2 S1(config-vlan)#name vlanBikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name vlanTrikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name vlanManagement S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name vlanParking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name vlanNative S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#configure terminal S1(config)#interface range f0/1,f0/2,f0/5 S1(config-if-range)# switchport trunk encapsulation dot1q S1(config-if-range)# switchport mode trunk S1(config-if-range)#switchport trunk allowed vlan 6

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1#configure terminal S1(config)#int range f0/1-2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 1 mode active
Configurar el puerto de acceso de host para VLAN 2	S1#configuere terminal S1(config)#int f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	S1#configure terminal S1(config)#int f0/6 S1(config-if)#switchport port-security S1(config-if)#switchport port-security Maximum 3 S1(config-if)#switchport port-security violation shutdown
Proteja todas las interfaces no utilizadas	S2#configure terminal S2(config)#int range f0/3-4,f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5

Se verifica que este configurado correctamente los pasos de la tabla 6 en Switch1

- Creacion de las VLAN, desde la consola en el modo privilegiado, posterioermente en la configuración global con el siguiente comando se proceden a crear las diferentes vlan:

S1(config)#vlan 20 **Vreamos la vlan 20**

S1(config-vlan)#name Docentes **Asignación de Nombre**

- Se repite el mismo procedimiento para las vlan, 30- Estudiantes, 40- Invitados, 50- Usuarios, 56-Nativa

- Creación de troncos 802.1Q que utilicen la VLAN 56 nativa en la interfaz fa0/5

S1(config)#interface fa0/5 **Acedemos a la interface de conexióncon el Router**

S1(config-if)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulación IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S1(config-if)#switchport trunk native vlan 56 **Direccionamiento a la VLAN 56**

- Creación de troncos 802.1Q que utilicen la VLAN 56 nativa en la interfaz fa0/1 y fa0/1-2

S1(config-if)#interface range fa0/1-2 **Acedemos a el rango con las dosinterfaces a modificar**

S1(config-if-range)# shutdown **Apagamos el grupo de la interfacepara realizar la configuración**

S1(config-ifrange)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulación IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo deenlace control permanente**

S1(config-if-range)#switchport trunk native vlan 56

Se direcciona el rango de la interface a la VLAN 56.

- Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

S1(config)#interface range fa0/1-2 **Se accede a el rango con las dosinterfaces a modificar**

S1(config-if-range)#channel-group 1 mode active **Luego de que se crea el grupo se realiza su activación**

S1(config-if-range)#interface Port-channel 1 **Se accede a la interface del canal**

S1(config-if)#switchport trunk encapsulation dot1q **Se indica al switch que en la Interfaz debe usar la encapsulación IEEE 802.1Q en las tramas, cuando esta esté configurada como troncal, Se cambia la interface a modo de enlace control permanente**

S1(config-if)#switchport trunk native vlan 56 **Se re direcciona el rango de la interface a la VLAN 56 native**

- Configuracion del puerto de acceso del host para la VLAN 20

S1(config-if)#interface fa0/6 **Acedemos a la interface**

S1(config-if)#switchport mode acces **Se configura el modo operativo de enlace truncal en una interfaz de capa 2**

S1(config-if)#switchport acces vlan 20 **Se redireccióna la interfaz a la vlan20**

- configuración de seguridad en los puertos de acceso

S1(config-if)#switchport port-security máximum

4 **Se configura la seguridad de los puertos de la interface para que el acceso solo permita 4 direcciones Mac**.

- Interfaces no utilizadas

se aseguran todas las interfaces sin usar, mediante una serie de rangos (fa0/3-4, fa0/7-24, range g0/1-2) para así re direccionarlas a la vlan 50-Usuarios, asignamosuna descripción: “sin uso” y finalmente se apagan

S1(config-if-range)#interface range fa0/3-4

S1(config-if-range)#switchport acces vlan 50

S1(config-if-range)#description Sin uso

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 Sin 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 Sin uso

S1(config-if-range)#shutdown

Tabla 14. Configuración de la infraestructura de red en S2 (Vlan, Trunking, Etherchannel)

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name vlanBikes S2(config-vlan)#exit S2(config)#vlan 3 S2(config-vlan)#name vlanTrikes S2(config-vlan)#exit S2(config)#vlan 4 S2(config-vlan)#name vlanManagement S2(config-vlan)#exit S2(config)#vlan 5 S2(config-vlan)#name vlanParking S2(config-vlan)#exit S2(config)#vlan 6 S2(config-vlan)#name vlanNative S2(config-vlan)#exit

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2#configure terminal S2(config)#int range f0/1,f0/2 S2(config-if-range)# switchport trunk encapsulation dot1q S2(config-if-range)# switchport mode trunk S2(config-if-range)#switchport trunk allowed vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2#configure terminal S2(config)#int range f0/1-2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 1 mode passive
Configurar el puerto de acceso del host para la VLAN 3	S2#configure terminal S2(config)#int f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	S2#configure terminal S2(config)#int f0/18 S2(config-if)#switchport port-security Maximum 3 S2 (config-if)#switchport port-security violation shutdown
Asegure todas las interfaces no utilizadas	S2#configure terminal S2(config)#int range f0/3-17,f0/19-24 S0(config-if-range)#switchport mode access S0(config-if-range)#switchport access vlan 5

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Configurar soporte de host en R1

Tarea	Especificación
Configure Default Routing	R0#configure terminal R0(config)#ip route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2	R0#configure terminal R0(config)#ip dhcp pool ccna-a.net R0(dhcp-config)#network 10.26.8.0 255.255.255.192 R0(dhcp-config)#default-router 10.26.8.1 R0(dhcp-config)#exit R0(config)#ip dhcp excluded-address 10.26.8.1 10.26.8.52
Configurar DHCP IPv4 para VLAN 3	R0#configure terminal R0(config)#ip dhcp pool ccna-b.net R0(dhcp-config)#network 10.26.8.64 255.255.255.224 R0(dhcp-config)#default-router 10.26.8.65 R0(dhcp-config)#exit R0(config)#ip dhcp excluded-address 10.26.8.65 10.26.8.84

Fuente: Autor

- Configure Default Routing

Asignacion de las rutas predeterminadas IPv4 y IPv6, las cuales direccionan 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 paraVLAN 20

R1(config)#ip dhcp excluded-address 10.26.8.3 10.26.8.52 **Comando para excluir el rango de direcciones establecidas**

R1(config)#ip dhcp pool vlan20-Docentes **Configuracion de DHCP en la vlan 20- docentes**

R1(dhcp-config)#network 10.26.8.0 255.255.255.192 **Red y mascara de sub red de la sub interface g0/0/1.20**

R1(dhcp-config)#default-router 10.26.8.1 **Puerta de enlace preterminada**

R1(dhcp-config)#domain-name unad-ccna-sa.net **Asignamos nombre del dominio**

- Configurar DHCP IPv4 paraVLAN 30

R1(config)#ip dhcp excluded-address 10.26.8.65 10.26.8.84 **Comando para excluir el rango de direcciones establecidas**

R1(config)#ip dhcp pool vlan30-Estudiantes **Configuracion de DHCP en la vlan 20- docentes**

R1(dhcp-config)#network 10.26.8.64 255.255.255.224 **Red y mascara de sub red de la sub interface g0/0/1.30**

R1(dhcp-config)#default-router 10.26.8.65 **Puerta de enlace preterminada**

R1(dhcp-config)#domain-name unad-ccna-sb.net **Asignamos nombre del dominio**

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 16. Configuración de red de PC-A

Configuración de red del PC-A	
Descripción	**PC-A**
Dirección física	0000.0CEE. C951
Dirección IP	10.26.8.53
Máscara de subred	*255.255.25* *5.192*
Gateway predeterminado	10.26.8.1
Gateway predeterminado IPv6	FE80::1

Tabla 17. Configuración de red de PC-B

Configuración de red del PC-B	
Descripción	**PC-B**
Dirección física	0001.6404. D7D2
Dirección IP	10.26.8.85
Máscara de subred	255.255.25 5.224
Gateway predeterminado	10.26.8.65
Gateway predeterminado IPv6	FE80::1

Fuente: Autor

Parte 4 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.

Tabla 18. Prueba de conectividad de red

Desde	Hacia	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.26.8.1	correcto
		IPv6	2001:db8:acad:a: :1	correcto
	R1, G0/0/1.3	Dirección	10.26.8.65	correcto
		IPv6	2001:db8:acad:b: :1	correcto
	R1, G0/0/1.4	Dirección	10.26.8.97	correcto
		IPv6	2001:db8:acad:c: :1	correcto
	S1, VLAN 4	Dirección	10.26.8.98	correcto
		IPv6	2001:db8:acad:c: :98	Correcto
	S2, VLAN 4	Dirección	10.26.8.99.	correcto
		IPv6	2001:db8:acad:c: :99	Correcto
	PC-B	Dirección	10.26.8.85	Correcto
		IPv6	2001:db8:acad:b: :50	Correcto
	R1 Bucle 0	Dirección	209.165.201.1	Correcto
		IPv6	2001:db8:acad:209: :1	Correcto
	R1 Bucle 0	Dirección	209.165.201.1	Correcto
		IPv6	2001:db8:acad:209: :1	Correcto
	R1, G0/0/1.2	Dirección	10.26.8.1	Correcto
		IPv6	2001:db8:acad:a: :1	Correcto

PC-B	R1, G0/0/1.3	Dirección	10.26.8.65	Correcto
		IPv6	2001:db8:acad:b: :1	Correcto
	R1, G0/0/1.4	Dirección	10.26.8.97	Correcto
		IPv6	2001:db8:acad:c: :1	Correcto
	S1, VLAN 4	Dirección	10.26.8.98	Correcto
		IPv6	2001:db8:acad:c: :98	Correcto
	S2, VLAN 4	Dirección	10.26.8.99.	Correcto
		IPv6	2001:db8:acad:c: :99	Correcto

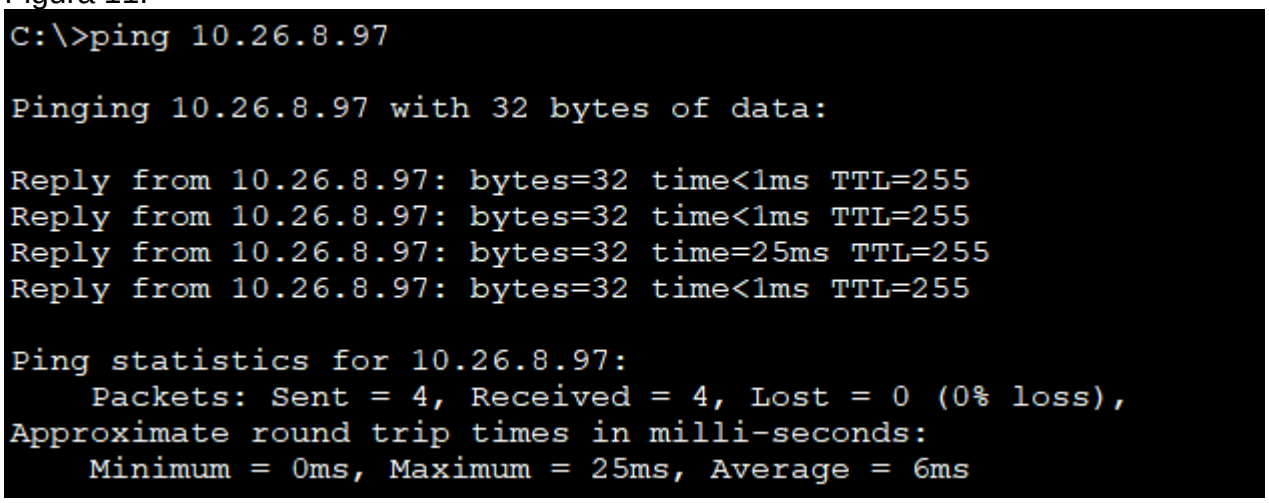
ping de PC-A a R1 G0/0/1.3 Ipv6 - 2001:db8:acad:b: :1
Figura 10

```
C:\>ping 2001:db8:acad:b::1

Pinging 2001:db8:acad:b::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:B::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Como se evidencia en la figura 10, el 2001:db8:acad:b: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

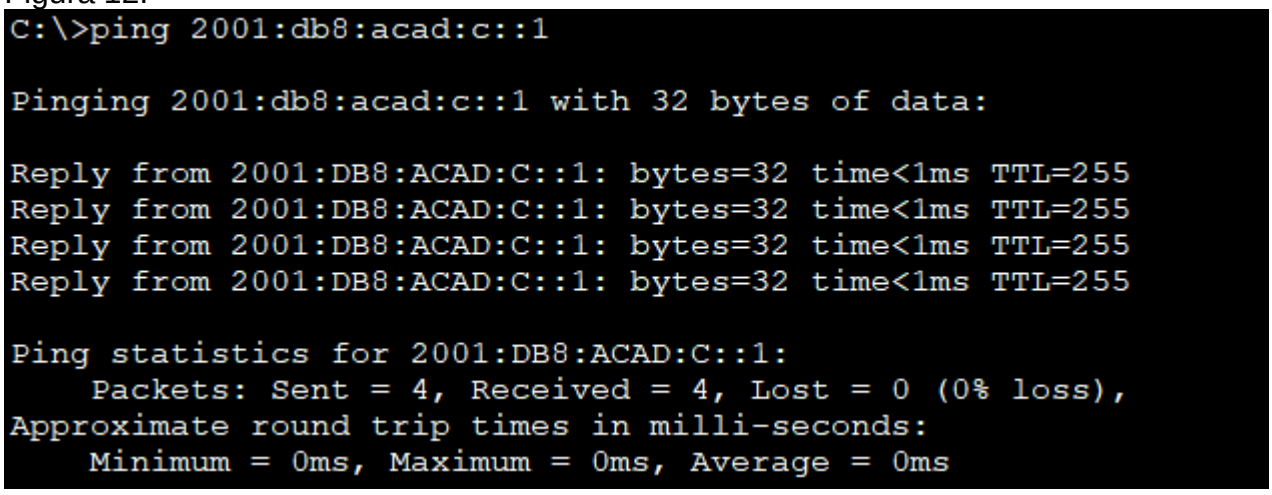
ping de PC-A a R1 G0/0/1.4 Ipv4 - 10.26.8.97
Figura 11.



Fuente: Autor

Como se evidencia en la figura 11, el 10.26.8.97 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-A a R1 G0/0/1.4 Ipv6 - 2001:db8:acad:c: :1
Figura 12.

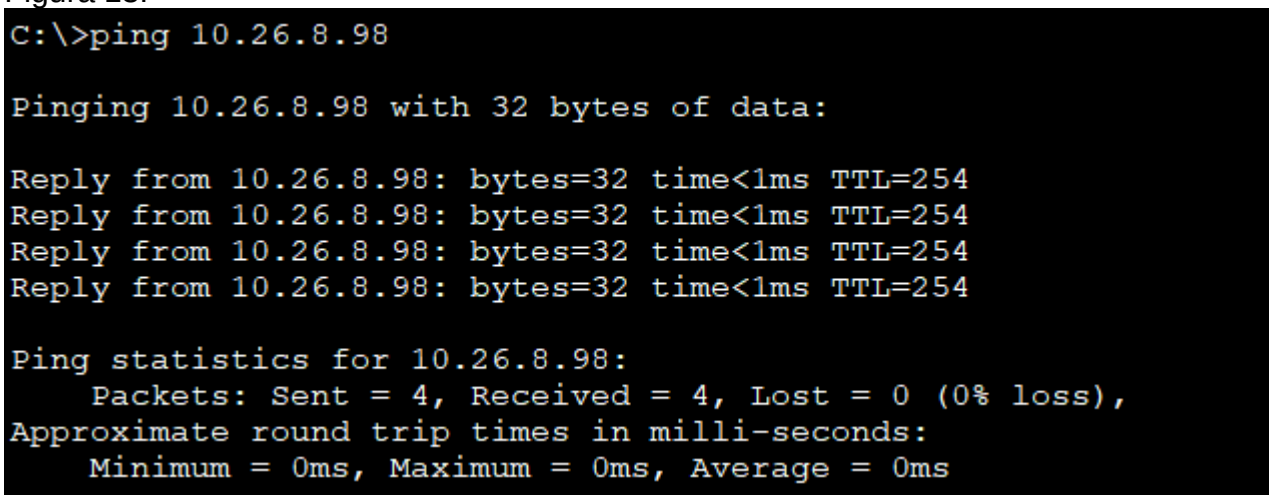


Fuente: Autor

Como se evidencia en la figura 12, el 2001:db8:acad:c: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-A a S1, VLAN 4 Ipv4 - 10.26.8.98

Figura 13.

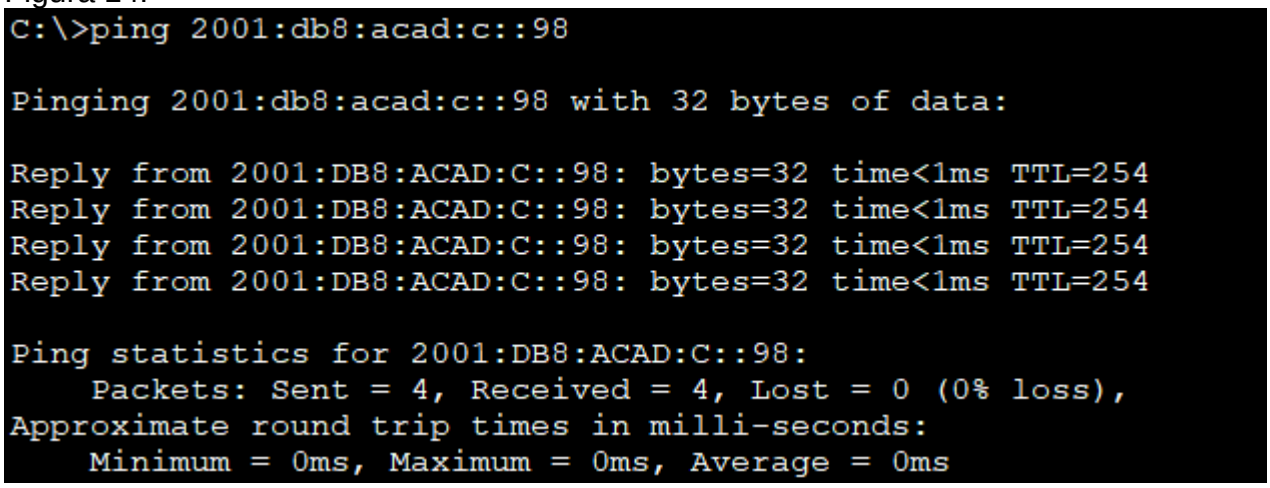


Fuente: Autor

Como se evidencia en la figura 13, el 10.26.8.98 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-A a S1, VLAN 4 Ipv6 - 2001:db8:acad:c: :98

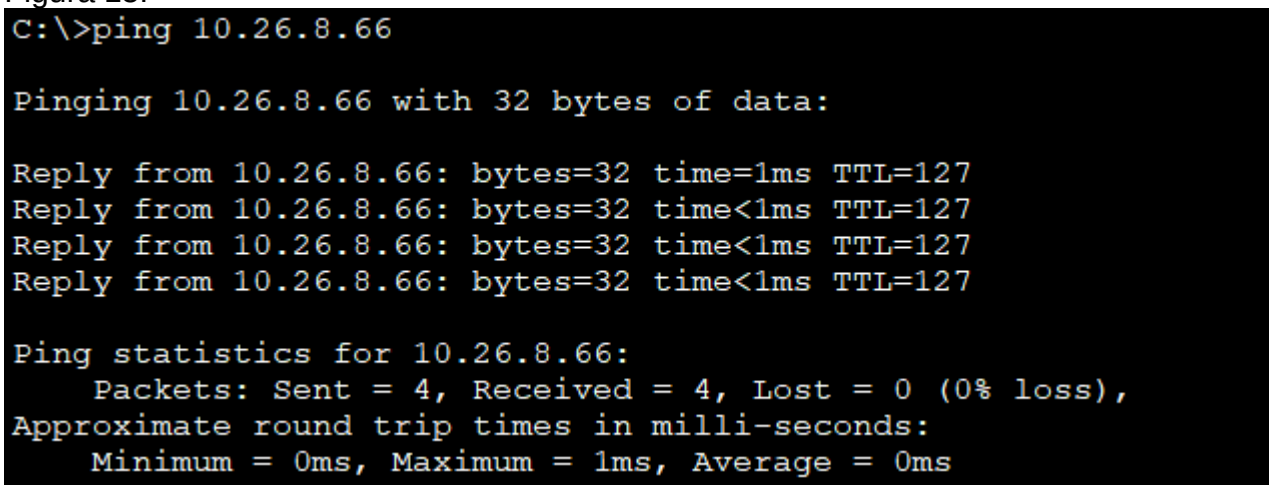
Figura 14.



Fuente: Autor

Como se evidencia en la figura 14, el 2001:db8:acad:c: :98 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

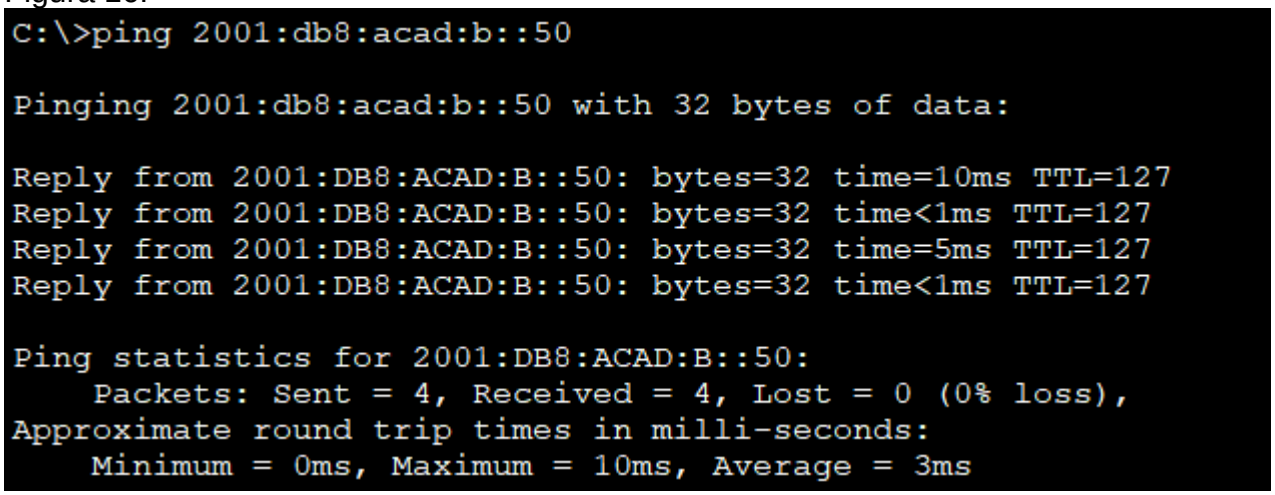
ping de PC-A a PC-B - 10.26.8.66
Figura 15.



Fuente: Autor

Como se evidencia en la figura 15, el 10.26.8.66 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-A a PC-B Ipv6 - 2001:db8:acad:b: :50
Figura 16.

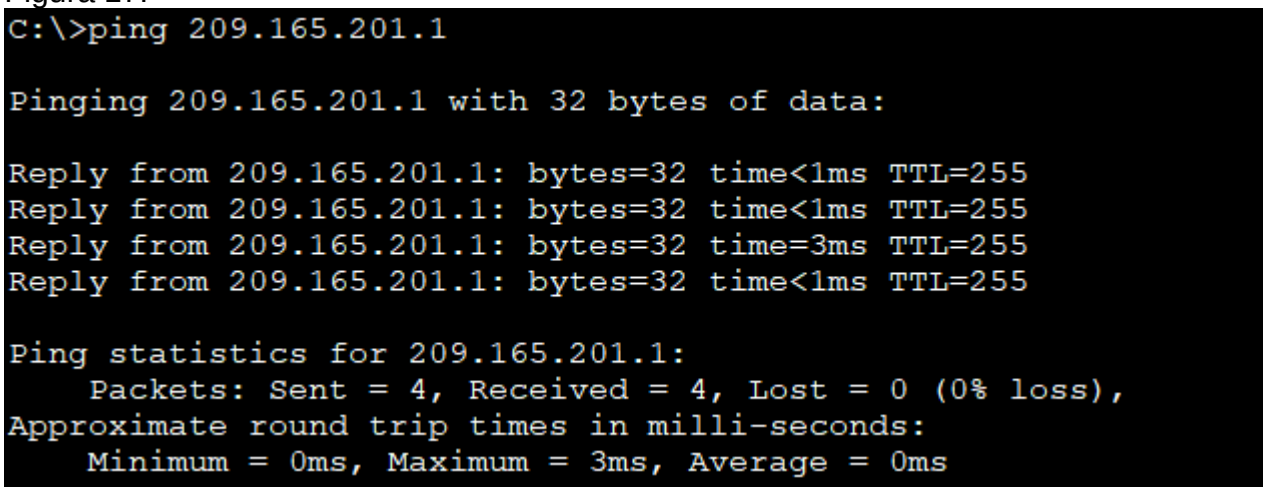


Fuente: Autor

Como se evidencia en la figura 16, el 2001:db8:acad:b: :50 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-A a LoopBack 0 - 209.165.201.1

Figura 17.

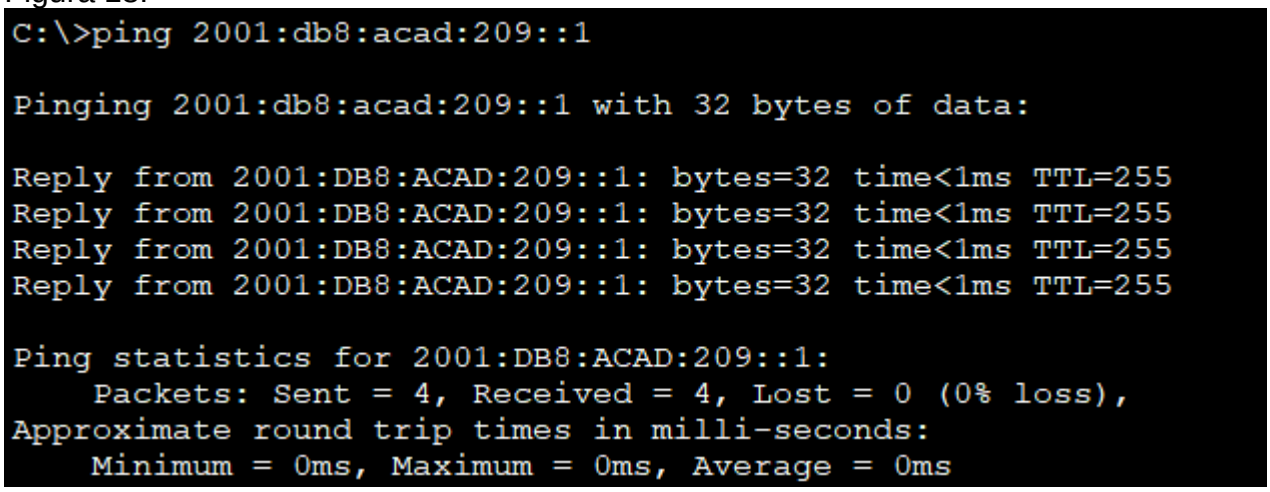


Fuente: Autor

Como se evidencia en la figura 17, el 209.165.201.1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-A a LoopBack 0 Ipv6 - 2001:db8:acad:209: :1

Figura 18.

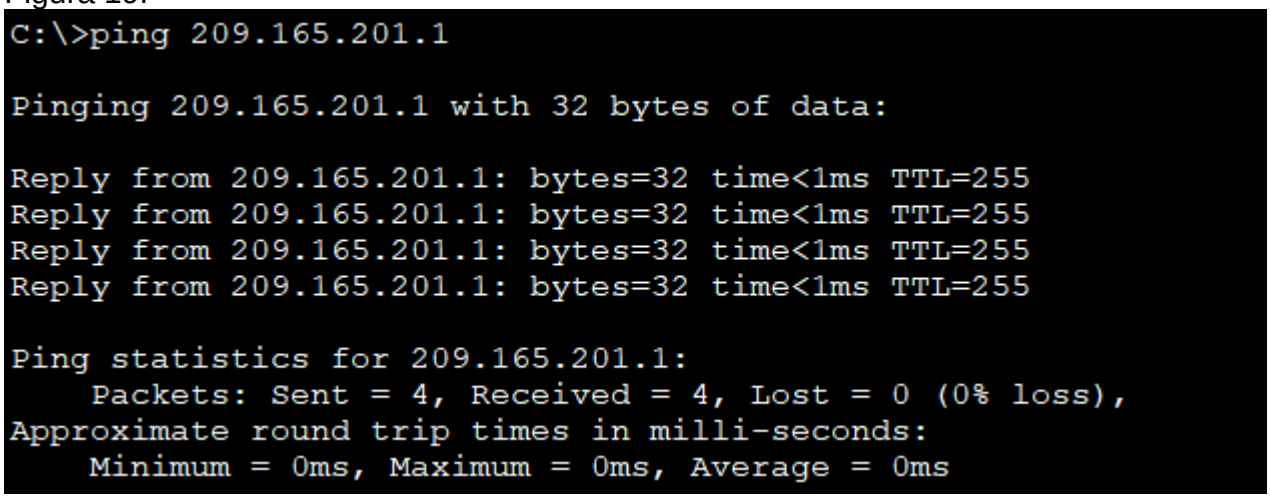


Fuente: Autor

Como se evidencia en la figura 18, el 2001:db8:acad:209: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, LoopBack 0 - 209.165.201.1

Figura 19.

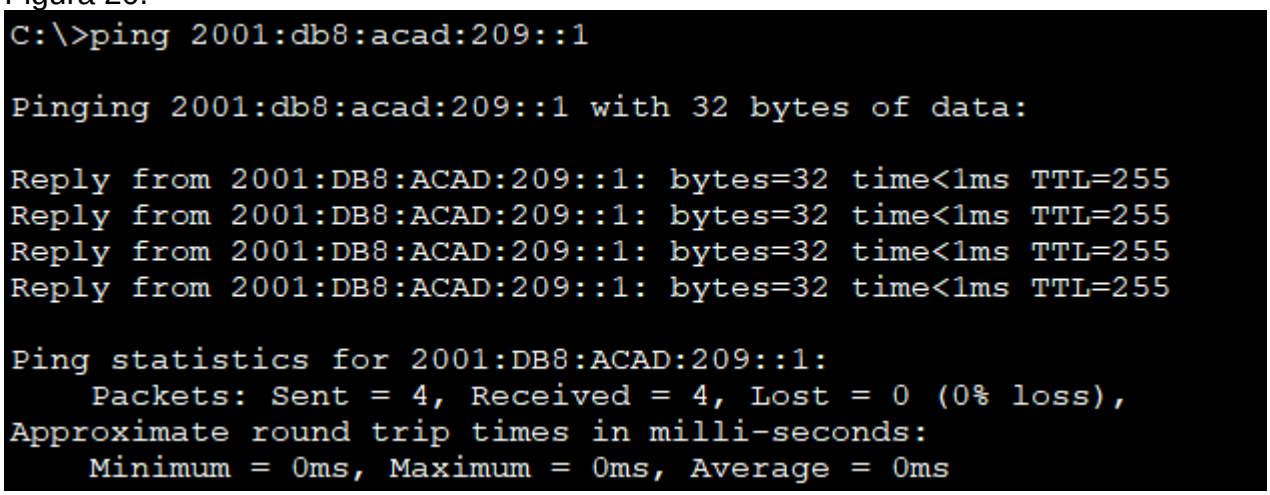


Fuente: Autor

Como se evidencia en la figura 19, el 209.165.201.1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, LoopBack 0 IPv6 - 2001:db8:acad:209: :1

Figura 20.



Fuente: Autor

Como se evidencia en la figura 20, el 2001:db8:acad:209: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, G0/0/1.2 Ipv4 - 10.26.8.1

Figura 21.

```
C:\>ping 10.26.8.1

Pinging 10.26.8.1 with 32 bytes of data:

Reply from 10.26.8.1: bytes=32 time<1ms TTL=255
Reply from 10.26.8.1: bytes=32 time<1ms TTL=255
Reply from 10.26.8.1: bytes=32 time<1ms TTL=255
Reply from 10.26.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.26.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Como se evidencia en la figura 21, el 10.26.8.1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, G0/0/1.2 Ipv6 - 2001:db8:acad:a: :1

Figura 22.

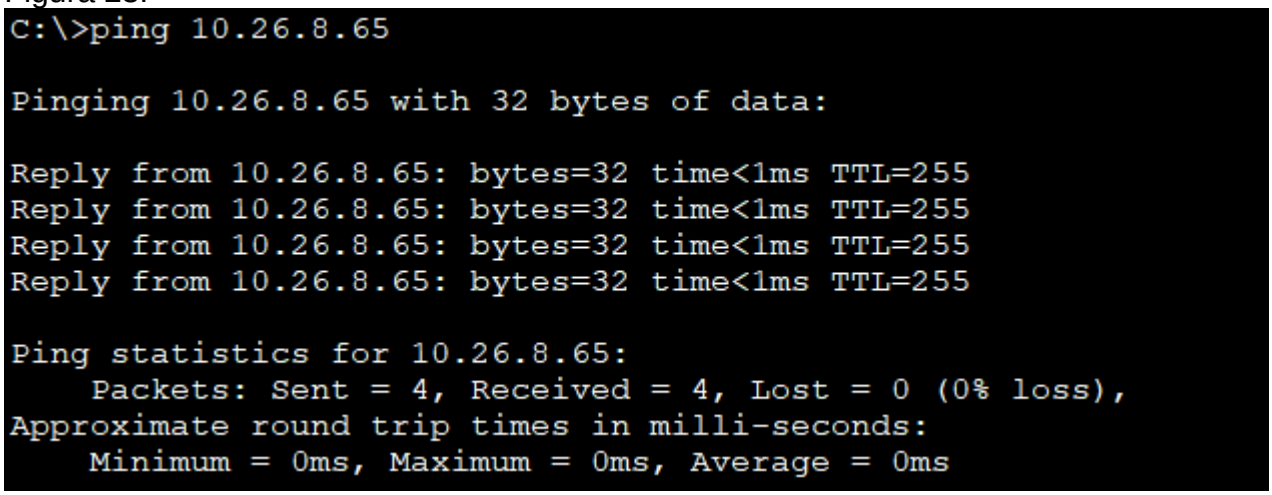
```
C:\>ping 2001:db8:acad:a::1

Pinging 2001:db8:acad:a::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=16ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms
```

Fuente: Autor

Como se evidencia en la figura 22, el 2001:db8:acad:a: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, G0/0/1.3 Ipv4 - 10.26.8.65

Figura 23.

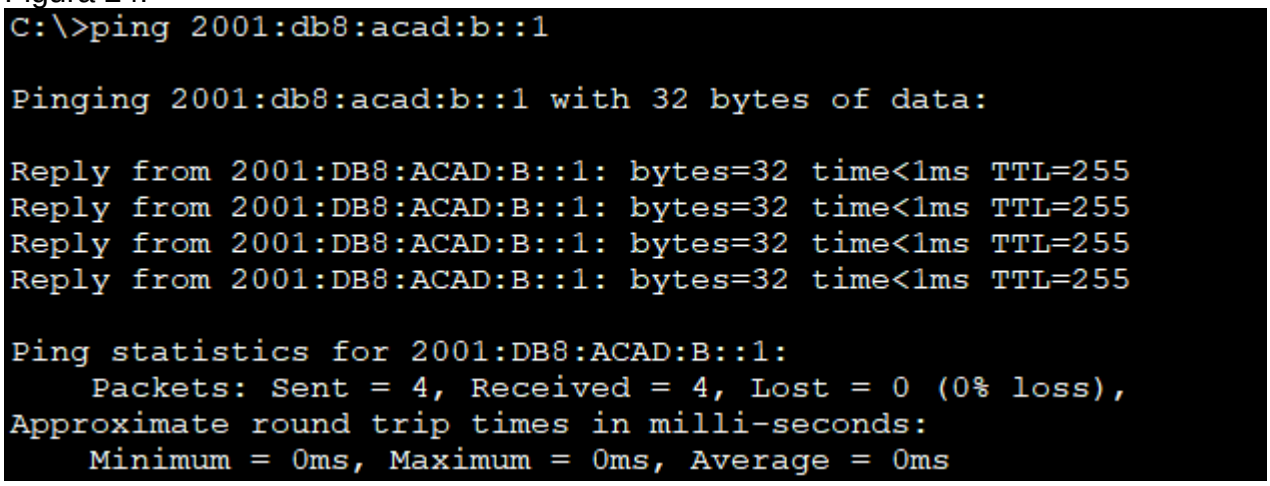


Fuente: Autor

Como se evidencia en la figura 23, el 10.26.8.65 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, G0/0/1.3 Ipv6 - 2001:db8:acad:b: :1

Figura 24.

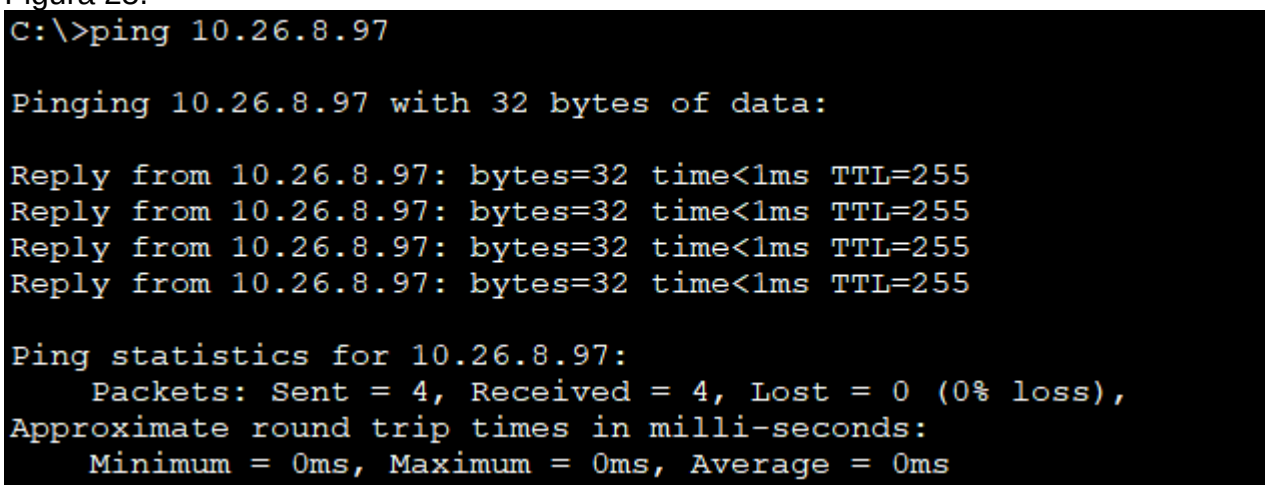


Fuente: Autor

Como se evidencia en la figura 24, el 2001:db8:acad:b: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, G0/0/1.4 Ipv4 - 10.26.8.97

Figura 25.

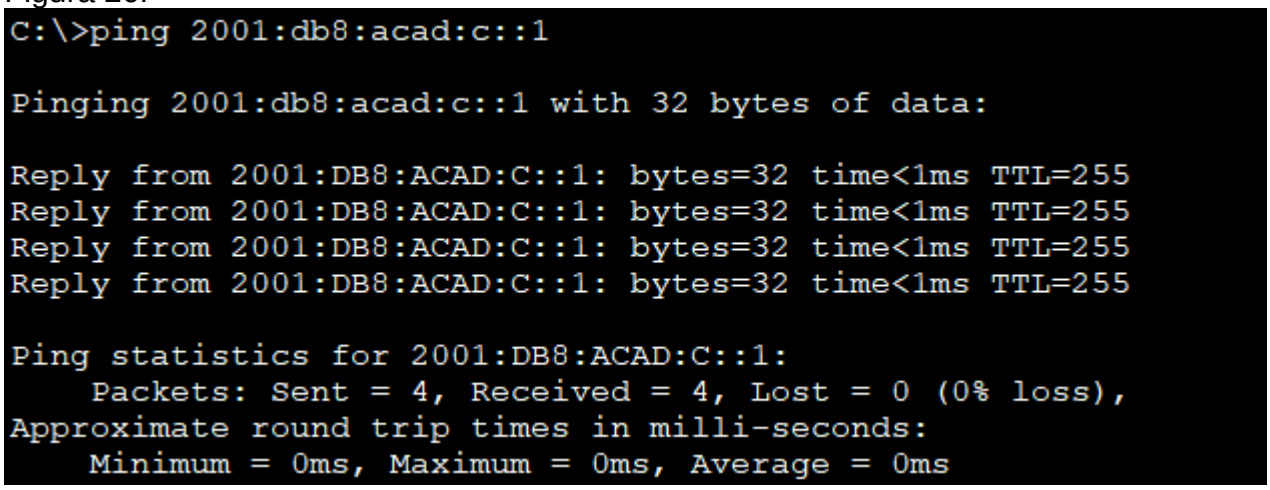


Fuente: Autor

Como se evidencia en la figura 25, el 10.26.8.97 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a R1, G0/0/1.4 Ipv6 -2001:db8:acad:c: :1

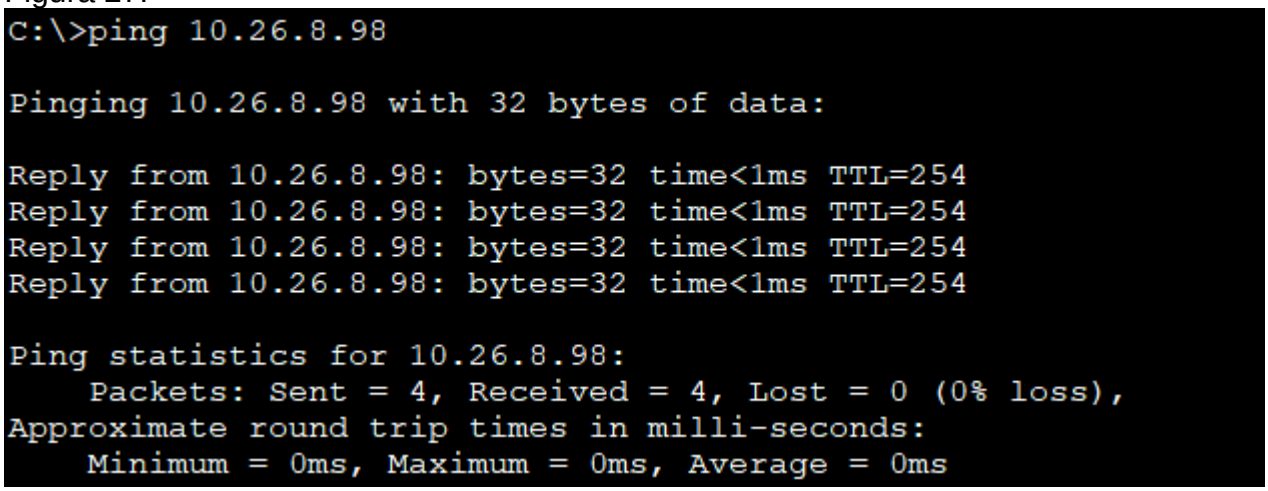
Figura 26.



Fuente: Autor

Como se evidencia en la figura 26, el 2001:db8:acad:c: :1 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

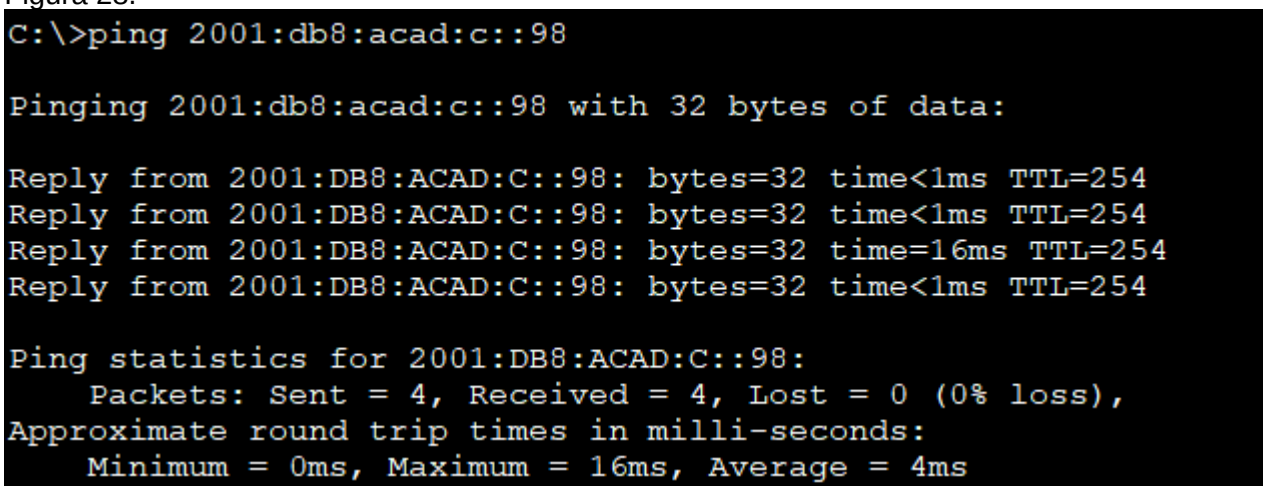
ping de PC-B a S1, VLAN 4 IPv4 - 10.26.8.98
Figura 27.



Fuente: Autor

Como se evidencia en la figura 27, el 10.26.8.98 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

ping de PC-B a S1, VLAN 4 IPv6 - 2001:db8:acad:c: :98
Figura 28.



Fuente: Autor

Como se evidencia en la figura 28, el 2001:db8:acad:c: :98 este funciona correctamente, obteniendo un resultado de 100% de los 4 paquetesenviados los 4 fueron recibidos.

CONCLUSIONES

Para realizar una red pequeña debemos dar seguridad que el cual cumpla con lo requerido para los usuarios, que pueda solo los empleados o administradores ingresar a ciertas partes de envíos de paquete configuración de red. esquemas de direccionamiento ip en el cual se detallan las construcciones de los dispositivos, sus propiedades y que sean admisibles a la utilización de direcciones a una LAN, pequeña (vista en el trabajo anterior) IPv4 e IPv6 donde podemos volverla aún más pequeñas gracias al Subneteo, para ese proceso utilizamos una serie de fórmulas, donde dividir las redes físicas a redes lógicas no perdiendo la presidencia de un dominio.

Por otro lado, se utilizan conceptos que permanecen involucrados con la aplicación de estabilidad, que va a partir de la aplicación de SSH en lugar de TELNET; la aplicación de servicios de cifrados de clave de escrito plano, la asignación de claves a la línea de consola y la línea de terminal, la asignación de banners que informen al administrador, advertencias sobre la utilización inadecuado o accesos no autorizados a los dispositivos, la configuración de direccionamiento en todas las interfaces, tanto físicas como lógicas y la verificación de la conectividad entre los host y los dispositivos.

Para concluirse debe destacar que el software utilizado es bastante intuitivo. Lo cual permitió un correcto desarrollo en la implementación de ambos diseños de

Con el desarrollo de esta prueba de capacidades se puede llevar a cabo los conceptos adquiridos en el lapso del diplomado de profundización y posibilita obtener destrezas que permitan resolver inconvenientes involucrados con la configuración de redes pequeñas como la iniciativa en el escenario 1, que comprende la creación de la simulación de la red con la herramienta packet tracer, el desarrollo de

red (enrutamiento estático y dinámico). Con esto podemos verificar la concordancia con lo que se estudió teóricamente sobre la diferencia entre el enrutamiento estático y dinámico, de lo cual podemos destacar la autonomía de este último sobre el primero, pues la ruta no siempre será la misma, debido al ‘aprendizaje’ que tiene el algoritmo, y con ello la eficiencia de este. A modo de plantear una interrogante, para un posible trabajo futuro sería ¿Cómo enfrenta una viable pérdida de energía todos los sistemas?

BIBLIOGRAFIA

ÁLVARO, M. Tipos de Banner en Dispositivos Cisco. [sitio web]. [Consultado 23 de noviembre de 2022]. Disponible en: https://netwgeeks.com/tipos-de-banner-en-dispositivos-cisco/

CISCO. Asignación de direcciones IPv4. Introducción a las redes. [sitio web]. [Consultado 22 de agosto de 2022]. Disponible en: https://contenthub.netacad.com/itn/11.0.1

CISCO. Información sobre los modos de LoopBack en routers de Cisco. [sitio web]. [Consultado 19 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/asynchronous-transfer-modeatm/permanent-virtual-circuits-pvc-switched-virtual-circuits-svc/6337atmloopback.html

DE LUZ, Sergio. VLANs: Qué son, tipos y para qué sirven. [sitio web]. [Consultado 19 de noviembre de 2022]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

GARCIA, Flores. Que son las líneas vty Cisco?. [sitio web]. [Consultado 19 de noviembre de 2022]. Disponible en: https://la-respuesta.com/preguntas-comunes/Que-son-las-lineas-vty-Cisco/

GUACA, N. Configuración básica de: Switches. [sitio web].[Consultado 03 de octubre de 2022] Disponible en: http://hdl.handle.net/10596/23215

LOBATO, G. CURSO 7-1 Explicación de protocolo OSPF. [Archivo de Vídeo]. [Consultado el 17 de noviembre de 2022]. Disponible en: https://www.youtube.com/watch?v=dwT5du44t_8

MICROSOFT. Protocolo de configuración dinámica de host (DHCP). [sitio web]. [Consultado el 17 de noviembre de 2022]. Disponible en: https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top

WALTON, Alex. Qué es default Gateway. [sitio web]. [Consultado el 17 de noviembre de 2022]. Disponible en: https://ccnadesdecero.es/que-es-gateway/

ANEXOS

https://drive.google.com/drive/folders/10OSwkum1j3MqWShVwEICNvZLYujk-DyB?usp=sharing