

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

CRISITIAN CHAYANE SALGUERO VALERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGÍA E INGENIERÍA-ECBTI
INGENIERIA DE SISTEMAS

TUNJA

2022

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

CRISTIAN CHAYANE SALGUERO VALERO

Diplomado de opción de grado presentado para optar el
título de ingeniero de sistemas

PAULITA FLOR SALAZAR
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS

TUNJA

2022

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Tunja 27 noviembre 2022

AGRADECIMIENTOS

Agradezco principalmente a mi familia por brindarme la oportunidad de llegar a la educación superior, posteriormente quiero agradecer a la UNAD por acompañarme en todo el proceso que hoy me convierten en profesional, agradezco a toda la red de tutores y administrativos que hicieron posible este momento, también quiero agradecer a todos esos compañeros que me apoyaron y que espero que todos lleguemos a cumplir nuestras metas, agradezco a todas las personas que de una u otra forma estuvieron dándome animo y apoyo para que pudiera ser posible esta meta.

TABLA DE CONTENIDO

AGRADECIMIENTOS.....	3
TABLA DE CONTENIDO	4
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN	11
1. DESARROLLO.....	12
1.1 Escenario 1.....	12
1.2 Escenario 2.....	29
CONCLUSIONES	63
REFERENCIAS BIBLIOGRÁFICAS.....	64
ANEXOS.....	65

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento escenario 1	13
Tabla 2. Configuración en Consola para el R1.....	14
Tabla 3. Tareas de Configuración para S1	16
Tabla 4. Configuración de PC-A	18
Tabla 5. Configuración de PC-B	19
Tabla 6. Verificación de conectividad.....	21
Tabla 7 Configuración R1	33
Tabla 8 Configuración S1.....	36
Tabla 9 Configuración S2.....	37
Tabla 10 Configuración infraestructural S1, creación de VLAN y troncales	39
Tabla 11 Configuración infraestructural S2, Creación de VLAN y Troncales	41
Tabla 12 Configuración Para Host	43
Tabla 13 configuración PC-A	44
Tabla 14. Configuración PC-B	45
Tabla 15: Pruebas.....	47

LISTA DE FIGURAS

	Pág
Figura 1 Red 1 diseño.....	12
Figura 2. Configuración de PC-A	19
Figura 3. Configuración de PC-B	20
Figura 4. Ping PC-A a R1 G0/0/0.....	22
Figura 5. Ping Pc-A a R1 G0/1.....	23
Figura 6. Ping PC-A a VLAN 1	24
Figura 7. Ping Pc-A a Pc-B	25
Figura 8. Ping Pc-B a G0/0	26
Figura 9. Ping Pc-B a G0/1	27
Figura 10. Ping Pc-B a S1 VLAN1	28
Figura 11. Topología básica.....	29
Figura 12 Topología en el simulador.....	30
Figura 13 PCA prueba de ipconfig	45
Figura 14. PCB prueba de ipconfig	46
Figura 15. PC-A a G0/1.2 IPV4.....	49
Figura 16. PC-A a G0/1.2 IPV6.....	50
Figura 17. PC-A a G0/1.3 IPV4.....	50
Figura 18. PC-A a G0/1.3 IPV6.....	51
Figura 19. PC-A a G0/1.4 IPV4.....	51
Figura 20. PC-A a G0/1.4 IPV6.....	52
Figura 21. PC-A a S1 VLAN 40 IPV4.....	52
Figura 22 PC-A a S1 VLAN 40 IPV6.....	53
Figura 23. PC-A a S2 VLAN 40 IPV4.....	53
Figura 24 PC-A a S2 VLAN 40 IPV6.....	54
Figura 25. PC-A a PC-B IPV4.....	54
Figura 26. PC-A a PC-B IPV6.....	55
Figura 27. PC-A a loopback 0 IPV6	55
Figura 28. PC-A a loopback 0 IPV6	56

Figura 29. PC-B a loopback 0 IPV4	56
Figura 30. PC-B a loopback 0 IPV6	57
Figura 31. PC-B G0/1.2 IPV4.....	57
Figura 32. PC-B a G0/1.2 IPV6.....	58
Figura 33. PC-B a G0/1.3 IPV4.....	58
Figura 34. PC-B a G0/1.3 IPV6.....	59
Figura 35. PC-B a G0/1.4 IPV4.....	59
Figura 36. PC-B a G0/1.4 IPV6.....	60
Figura 37. PC-B a S1 VLAN 40 IPV4.....	60
Figura 38 PC-B a S1 VLAN 40 IPV6.....	61
Figura 39. PC-B a S2 VLAN 40 IPV4.....	61
Figura 40 PC-B a S2 VLAN 40 IPV6.....	62

GLOSARIO

Cable directo: es el tipo de cable que se suele usar para conectar dispositivos diferentes entre sí¹

Cisco: es una empresa dedicada a la interconexión de redes actualmente es una de las más influyentes tanto que tienen su propio estándar para la creación de redes informáticas.²

CLI: es una interfaz propia de CISCO para componentes de redes, suele ser una interfaz principalmente tipo consola.³

IP: (dirección de protocolo de internet) es un protocolo que asigna la comunicación entre las redes, está compuesta por cuatro bloques numéricos que van del 0 hasta el 255 y a su vez están separados por puntos⁴

LAN: (Red de Área Local) es una red de comunicación normalmente alojada en un edificio o un par de estos no suelen ser muy grandes⁵

Router: también es conocido como enrutador porque precisamente es lo que hace encaminar segmentos de red para que se conecten con otros haciendo pasar paquetes de datos.⁶

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 remotamente⁷

¹GÓMEZ, Joaquín Andréu. Redes locales. (2011).

² CISCO, CISCO IoT Networking. Cisco. (2014).

³ TEJEDOR DORIA, Jesús Alberto. Diseño, implementación, administración y enrutamiento avanzado bajo el núcleo IOS CLI (Cisco). 2015.

⁴ DÍAZ, Walter Marcelo Fuertes. Definición de un modelo genérico para la caracterización de escenarios virtuales de redes IP. (2010).

⁵ VARGAS MERCHAN, EDISON KLEBER. Diseño de una red lan y wan segura para la compañía automotores latinoamericanos SA Autolasa. 2016

⁶ LANZA-GUTIERREZ, Jose M. Un nuevo enfoque para el posicionamiento de routers sobre redes de sensores inalámbricos. (2013)

⁷ GARDOKI, Cardenal. Qué es el protocolo SSH y cómo configurarlo para mejorar la seguridad de acceso a los servidores Linux. Hostalia whitepapers, p. 1-8.

RESUMEN

Este documento es la culminación del proceso de formación por parte del diplomado CISCO CNNA como un método de evaluar todo el conocimiento y competencias adquiridas a lo largo del mismo, el diplomado hace parte de una de las opciones de grado de la carrera ingeniería de sistemas de la universidad Nacional Abierta y a Distancia en el cual se solicitó la solución de dos escenarios, con problemas relacionados con redes en el cual se emplearan diferentes temas como lo es redes LAN, WAN, VLAN, direccionamiento IPv4, direccionamiento IPV6, direccionamiento mediante DHCP y seguridad de dispositivos.

Para el primer escenario se requiere un cálculo de direccionamiento IPv4 también partiendo del número de cédula del estudiante, luego se realiza la topología necesaria y a través de cable directo conectar una red simple que consta de un Router, un Switch y dos PC para posteriormente realizar todo lo referente al Subneteo para que la red pueda enviar información, esto último verificado con el comando Ipconfig.

Para el segundo escenario se nos presenta la topología de una Red LAN la cual debe contar con una seguridad a través de protocolos como SSH, el Router se debe configurar para que a través del protocolo DHCP pueda direccionar y gestionar un Pool para cada sub red así como para cada host; es necesario que la seguridad de la red sea de calidad por lo cual se especifican ciertas contraseñas y protocolos de seguridad basadas en la encriptación por último se realizan conexiones troncales entre switchs esto con el propósito de aumentar la velocidad de transmisión de datos y disminuir el tráfico de la misma red, todo esto antes mencionado se comprueba a través del comando ping.

Palabras Clave: CISCO, IPv4, cable directo, Router, LAN, SSH

ABSTRACT

This document is the culmination of the training process by the CISCO CNNA diploma as a method of evaluating all the knowledge and skills acquired throughout it, the diploma is part of one of the degree options of the systems engineering career National Open and Distance University in which the solution of two scenarios was requested, with problems related to networks in which different topics were used such as LAN, WAN, VLAN networks, IPv4 addressing, IPV6 addressing, addressing through DHCP and security of devices.

For the first scenario, a calculation of IPv4 addressing is required, also starting from the student's ID number, then the necessary topology is carried out and through direct cable connects a simple network consisting of a Router, a Switch and two PCs to later carry out everything regarding Subnetting so that the network can send information, the latter verified with the Ipconfig command.

For the second scenario we are presented with the topology of a LAN Network which must have security through protocols such as SSH, the Router must be configured so that through the DHCP protocol it can address and manage a Pool for each subnet as well. as for each host; It is necessary that the security of the network is of quality, for which certain passwords and security protocols based on encryption are specified. Lastly, trunk connections are made between switches, this with the purpose of increasing the speed of data transmission and decrease the traffic of the same network, all this mentioned above is checked through the ping command.

Keywords: CISCO, IPv4, direct cable, Router, LAN, SHH

INTRODUCCIÓN

El siguiente informe consta de dos escenarios en el primero se realiza un Subneteo de redes en una topología sencilla además se configura las medidas de seguridad básicas, se cifran las contraseñas a través del protocolo Crypto password por último se direccionan las redes asignándoles una IP con el formato IPV4 para las dos redes y en última instancia se recurre al comando Ping para realizar las debidas pruebas de envío de información.

Para el segundo escenario se empleará configuración básica de seguridad, enlaces troncales usando el protocolo 802.1Q, ether Channel y seguridad de puertos, empezamos utilizando una configuración básica para un Router, dos switches y dos hosts, posteriormente se realiza la configuración de direccionamiento por medio de dos métodos el primero con direccionamiento IPV4 usando DHCP y direccionamiento IPV6 de manera manual.

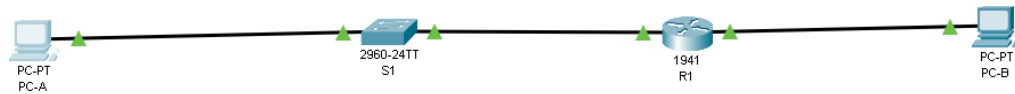
1. DESARROLLO

1.1 Escenario 1

1.1.1 Construya la Red

Se construye la red de acuerdo con la topología lógica que se plantea en el documento prueba de habilidades CNNA-2022; se cablea conforme se indica en la topología, y se conectan los equipos de cómputo.

Figura 1 Red 1 diseño



Fuente: Autoría propia

1.1.2 Desarrolle el esquema de direccionamiento IP

Se desarrolla el esquema de direccionamiento IP. Para la dirección IPv4 se crean las dos subredes con la cantidad requerida de hosts. Se asigna las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento

Cedula: 1049652609

Tabla 1. Tabla de direccionamiento escenario 1

Ítem	Requerimiento
Dirección de Red	172.09.3.0 donde XY corresponde a los últimos dos dígitos de su cedula.
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.09.3.62
R1 G0/0/0	172.09.3.94
S1 SV1	172.09.3.2
PC-A	172.09.3.10
PC-B	172.09.3.75

Fuente: Autoría propia

Tabla 2. Configuración en Consola para el R1

Descripción	Comando
Ingresa al modo privilegiado	Router>en
Ingresa a modo de configuración	Router#conf t
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 nombra 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
Se configura interfaz G0/0/0 se establece la dirección IPv4	R1(config-if)#ip address 172.09.3.94 255.255.255.224
Se configura interfaz G0/0/0 se establece la descripción	R1(config-if)#description " 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)#in g0/1

Se configura interfaz G0/0/1 se establece la descripción	R1(config-if)#description "Red Lan 1"
Se configura interfaz G0/0/1 se establece la dirección IPv4	R1(config-if)#ip address 172.09.3.62 255.255.255.192
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

Fuente: Autoría propia

Tabla 3. Tareas de Configuración para S1

Descripción	Comando
Ingresa al modo privilegiado	Switich>en
Ingresa a modo de configuración	Switich #con t
Desactiva la búsqueda DNS	Switich (config)#no ip domain-lookup
Se asigna el nombre del Switich S1	Switich (config)#hostname S1
Se nombra el dominio del Switich 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 para usuario	S1(config-line)#login
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	S1(config)#line vty 0 15

se ingresa autenticación de usuario	S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH en S1 Acceso al dispositivo a cisco	S1(config)#line vty 0 4
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	S1(config)#banner motd "S1Cristian Chayane salguero valero Ingenieria de Sistemas"
Genera una clave de cifrado RSA	S1(config)#crypto key generate rsa The name for the keys will be: S1.ccnasa.com How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keyswill be non-exportable...[OK]

Configure la interfaz de administración (SVI) en VLAN1	<pre>S1(config)#interface vlan 1 S1(config-if)#ip address 172.09.3.2 255.255.255.192 S1(config-if)#no shutdown S1(config)#ip default-Gateway</pre>
--	--

Fuente: Autoría propia

1.1.3 Parte 3. configurar los equipos

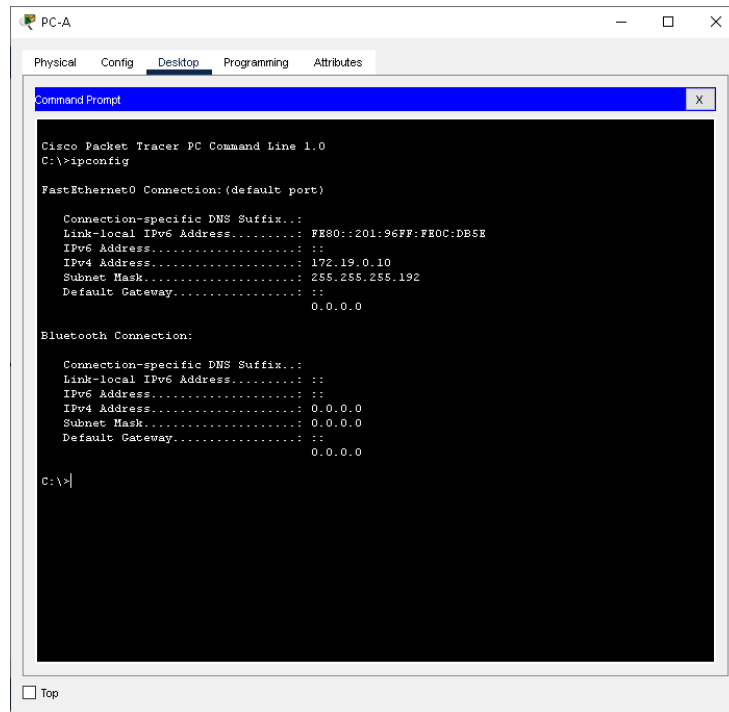
Se configuran los equipos host PC-A y PC-B conforme a la tabla de direccionamiento registrando las configuraciones de red del host con el comando ipconfig /all.

Tabla 4. Configuración de PC-A

Configuración de red de PC-A	
Descripción	FastEthernet1
Dirección física	0001.960C.DB5E
Dirección IPv4	172.09.3.10
Mascara de subred	255.255.255192
Puerta de enlace IPv4 predeterminada	172.09.3.62

Fuente: Autoría Propia

Figura 2. Configuración de PC-A



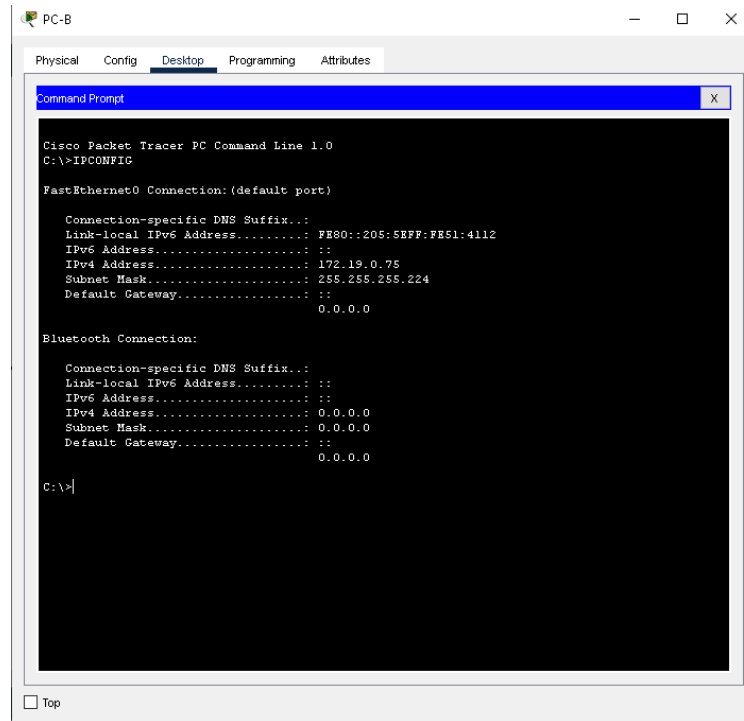
Fuente: Autoría Propia

Tabla 5. Configuración de PC-B

Configuración de red de PC-B	
Descripción	FastEthernet0
Dirección física	0005.5E51.4112
Dirección IPv4	172.09.3.75
Mascara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.09.3.62

Fuente: Autoría Propia

Figura 3. Configuración de PC-B



Fuente: Autoría Propia

1.1.4 Parte 4 Probar y verificar

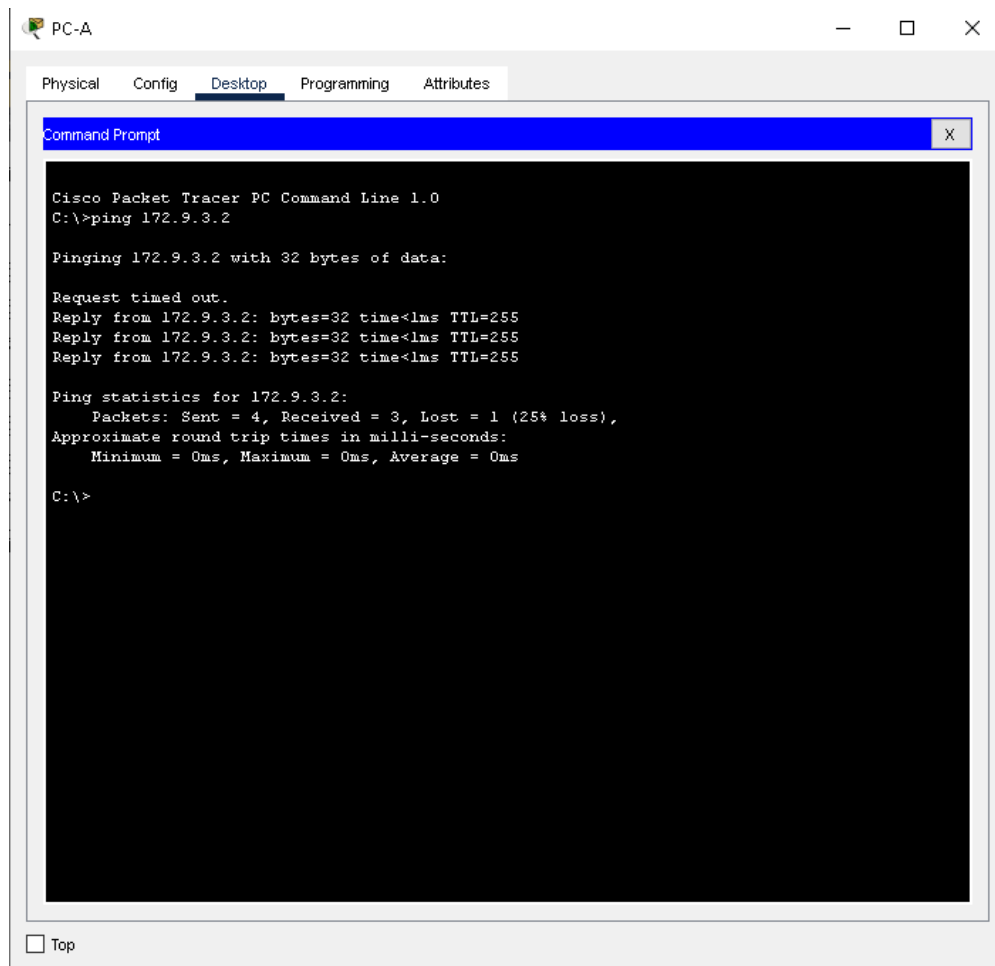
Se prueba y verifica la conectividad de extremo a extremo utilizando el comando ping para probar la conectividad entre todos los dispositivos de red.

Tabla 6. Verificación de conectividad

Desde	A	Direcciones IP	Resultado de ping
PC-A	R1 G0/0/0	172.09.3.94	Correcto. Figura 4
	R1 G0/0/1	172.09.3.62	Correcto. Figura 5
	S1 VLAN 1	172.09.3.2	Correcto. Figura 6
	PC-B	172.09.3.75	Correcto. Figura 7
PC-B	R1 G0/0/0	172.09.3.94	Correcto. Figura 8
	R1 G0/0/1	172.09.3.62	Correcto. Figura 9
	S1 VLAN 1	172.09.3.2	Correcto. Figura 10

Fuente: Autoría propia

Figura 6. Ping PC-A a VLAN 1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.9.3.2

Pinging 172.9.3.2 with 32 bytes of data:

Request timed out.
Reply from 172.9.3.2: bytes=32 time<1ms TTL=255
Reply from 172.9.3.2: bytes=32 time<1ms TTL=255
Reply from 172.9.3.2: bytes=32 time<1ms TTL=255

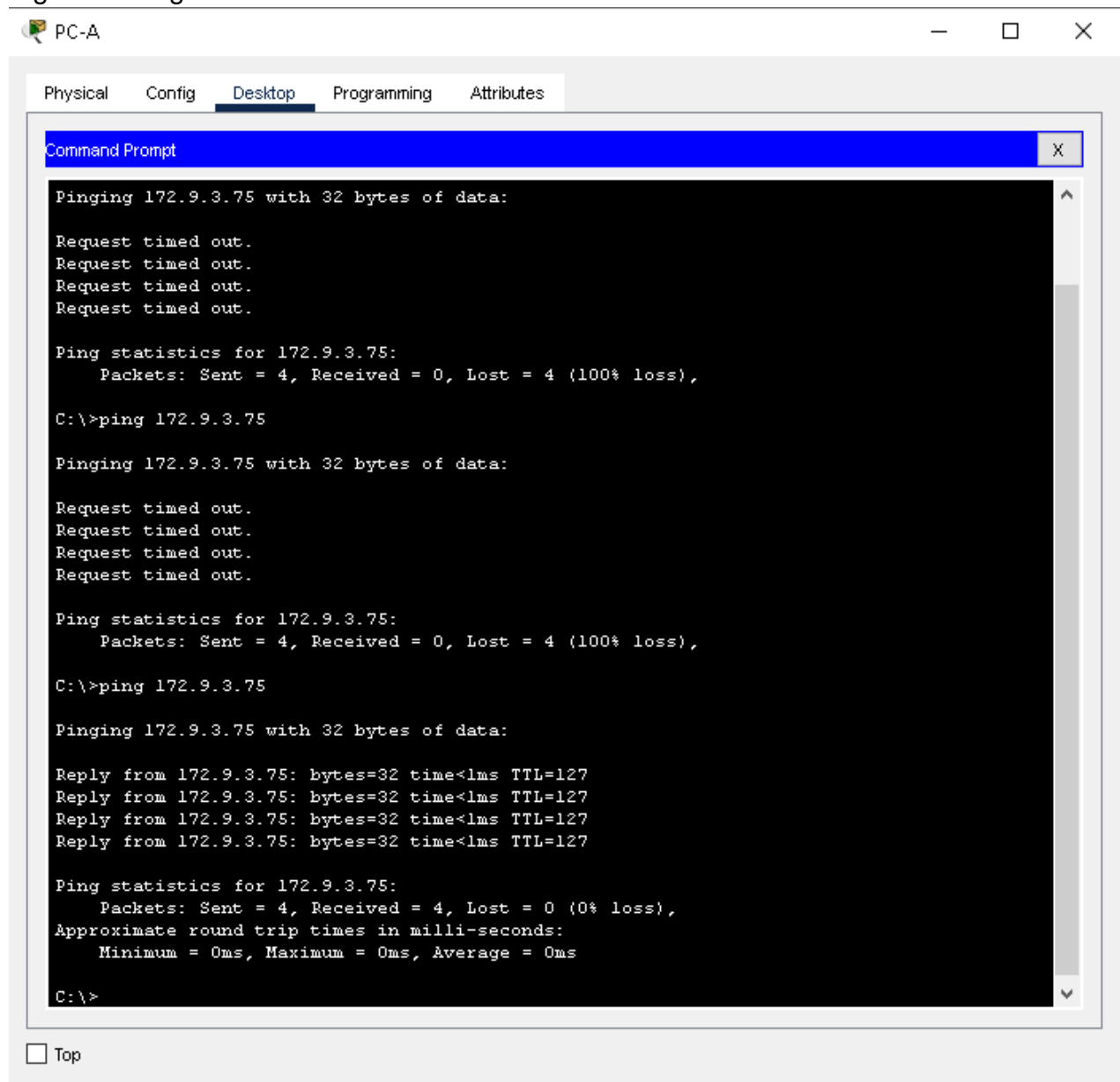
Ping statistics for 172.9.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Autor: Autoría propia

Se logra establecer conexión entre el PC-A y la red Virtual creada en el Router denominada VLAN 1.

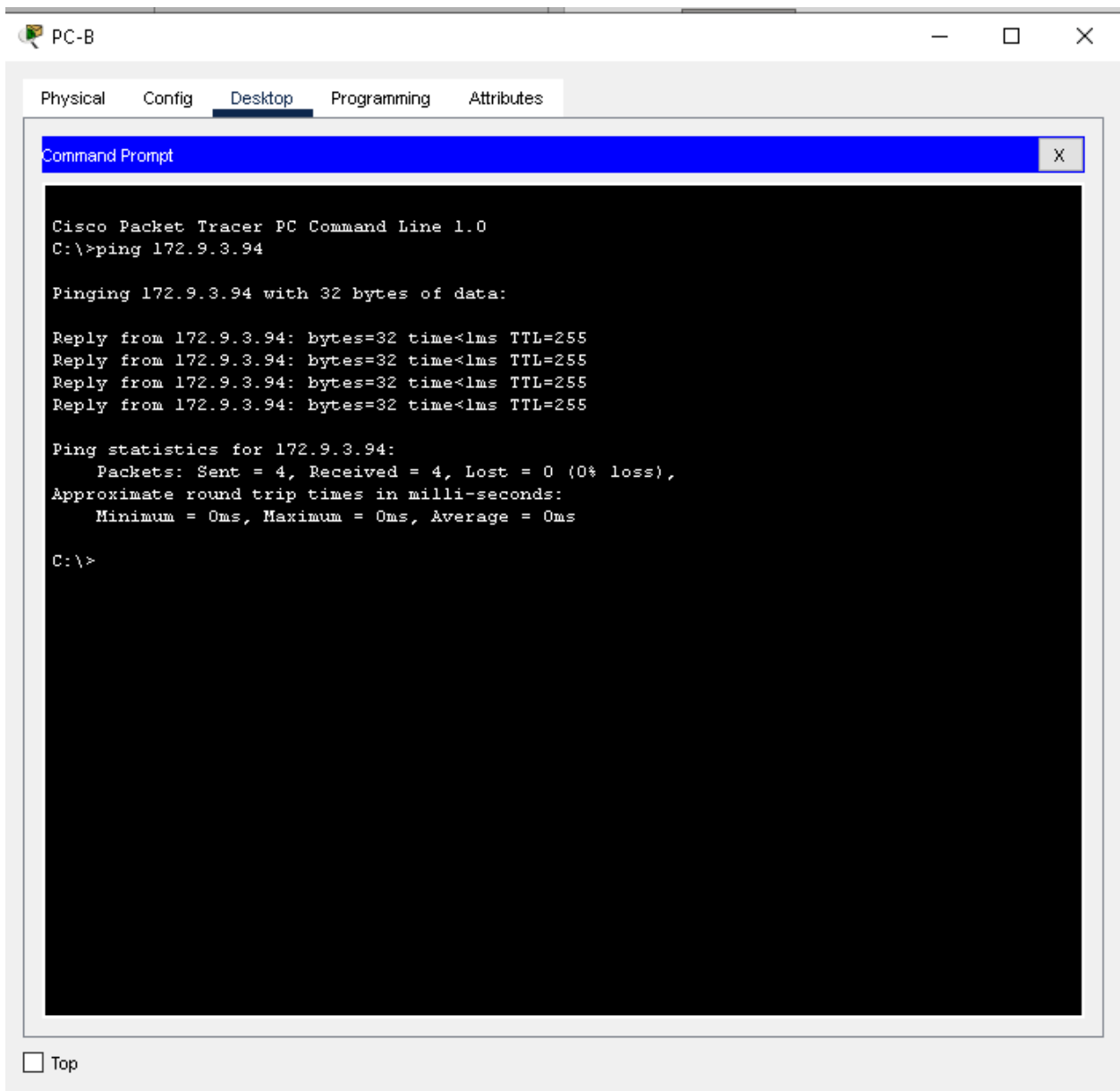
Figura 7. Ping Pc-A a Pc-B



Fuente: Autoría propia

Se realiza conexión entre los dos hosts estableciendo flujo de datos entre ambas redes.

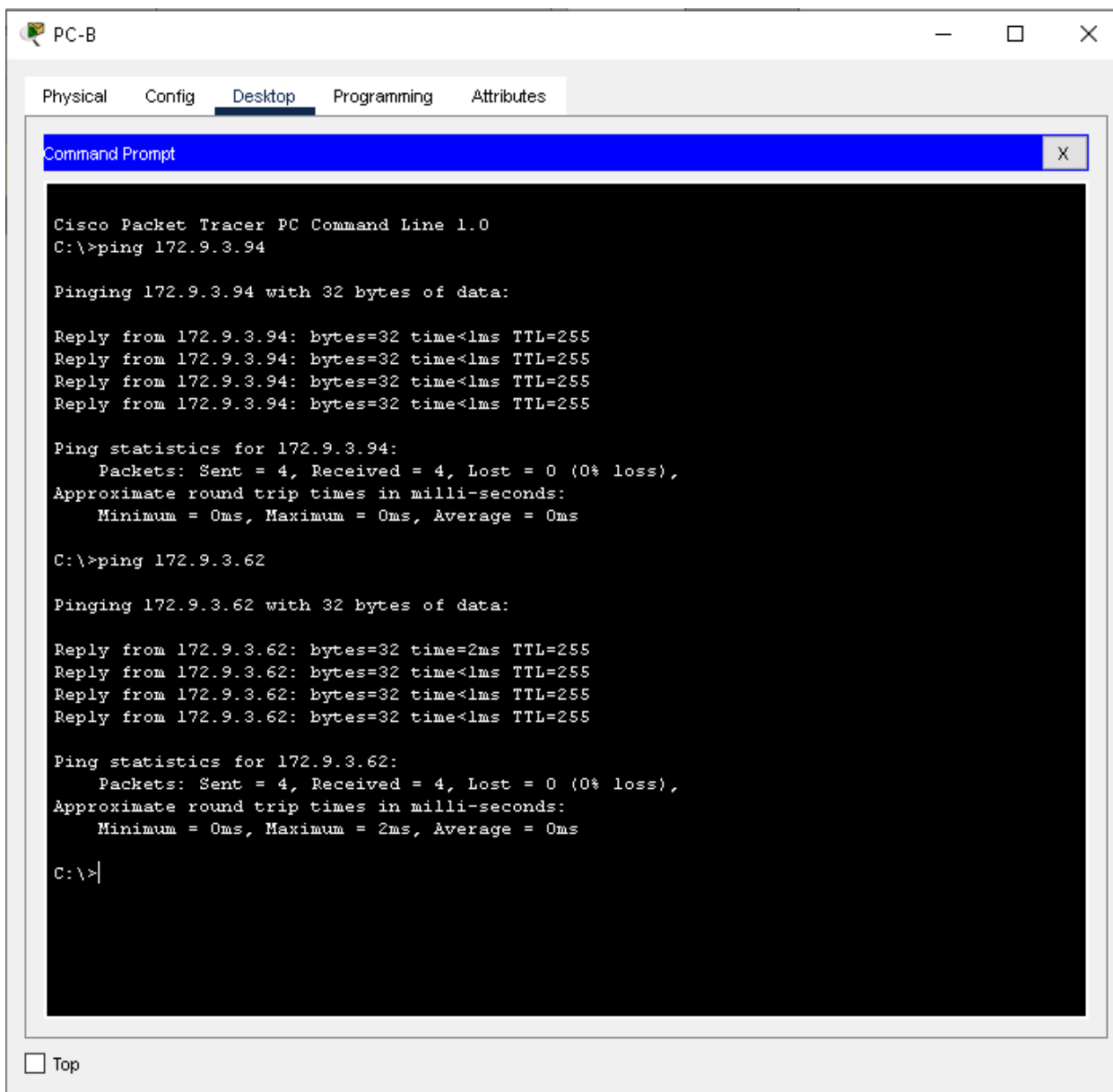
Figura 26. Ping Pc-B a G0/0



Fuente: Autoría Propia

Se vuelve a comprobar la conexión entre la red Gigabit ethernet 0/0 y la pc-B.

Figura 27. Ping Pc-B a G0/1



The screenshot shows a window titled "PC-B" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.9.3.94

Pinging 172.9.3.94 with 32 bytes of data:

Reply from 172.9.3.94: bytes=32 time<1ms TTL=255
Reply from 172.9.3.94: bytes=32 time<1ms TTL=255
Reply from 172.9.3.94: bytes=32 time<1ms TTL=255
Reply from 172.9.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.9.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.9.3.62

Pinging 172.9.3.62 with 32 bytes of data:

Reply from 172.9.3.62: bytes=32 time=2ms TTL=255
Reply from 172.9.3.62: bytes=32 time<1ms TTL=255
Reply from 172.9.3.62: bytes=32 time<1ms TTL=255
Reply from 172.9.3.62: bytes=32 time<1ms TTL=255

Ping statistics for 172.9.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

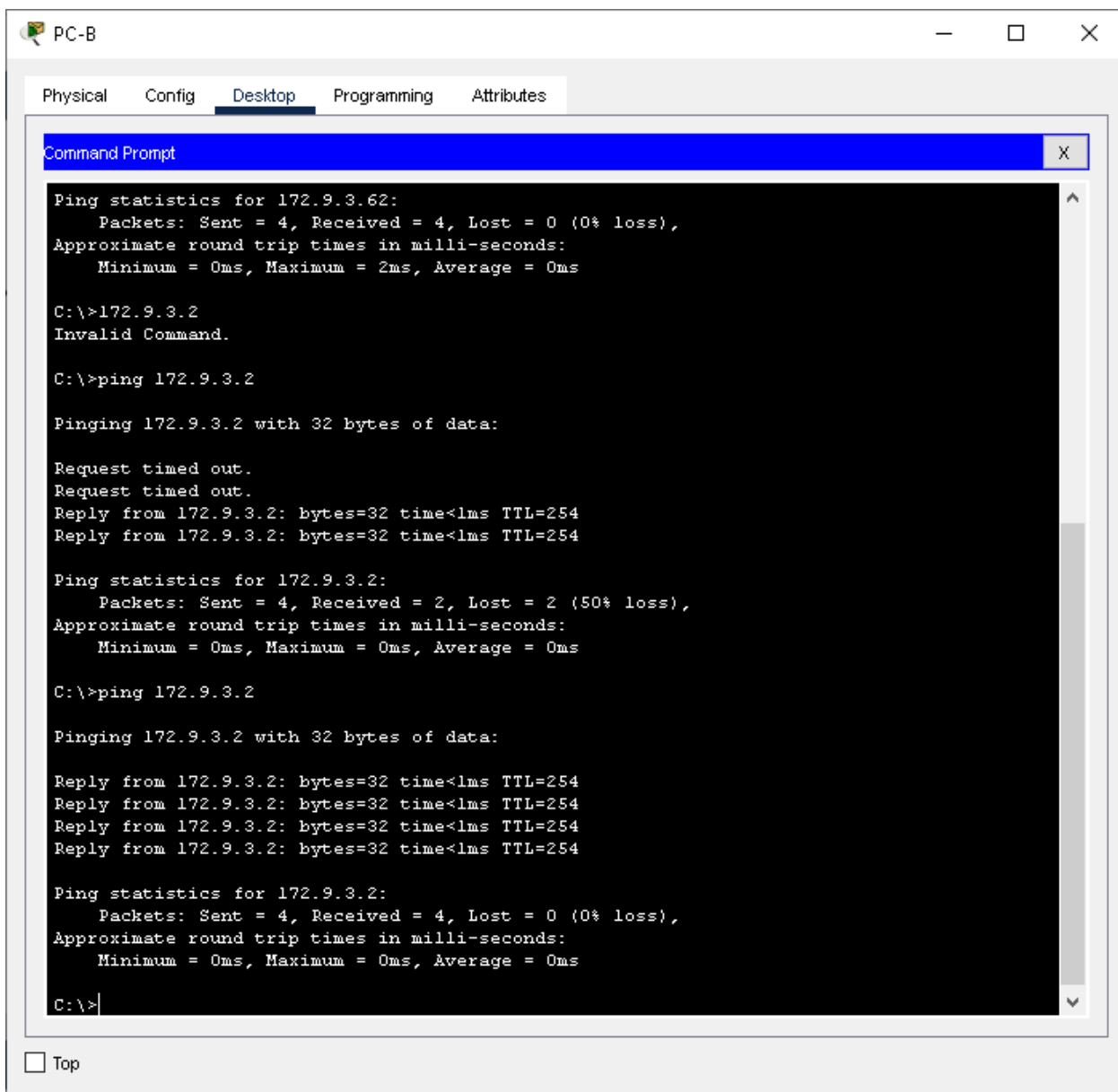
C:\>|
```

At the bottom left of the window, there is a checkbox labeled "Top".

Fuente: Autoría propia

Se comprueba que haya conexión entre la segunda red y el Pc-B.

Figura 10. Ping Pc-B a S1 VLAN1



The screenshot shows a window titled "PC-B" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the following output:

```
Ping statistics for 172.9.3.62:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>172.9.3.2
Invalid Command.

C:\>ping 172.9.3.2

Pinging 172.9.3.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 172.9.3.2: bytes=32 time<1ms TTL=254
Reply from 172.9.3.2: bytes=32 time<1ms TTL=254

Ping statistics for 172.9.3.2:
  Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.9.3.2

Pinging 172.9.3.2 with 32 bytes of data:

Reply from 172.9.3.2: bytes=32 time<1ms TTL=254
Reply from 172.9.3.2: bytes=32 time<1ms TTL=254
Reply from 172.9.3.2: bytes=32 time<1ms TTL=254
Reply from 172.9.3.2: bytes=32 time<1ms TTL=254

Ping statistics for 172.9.3.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

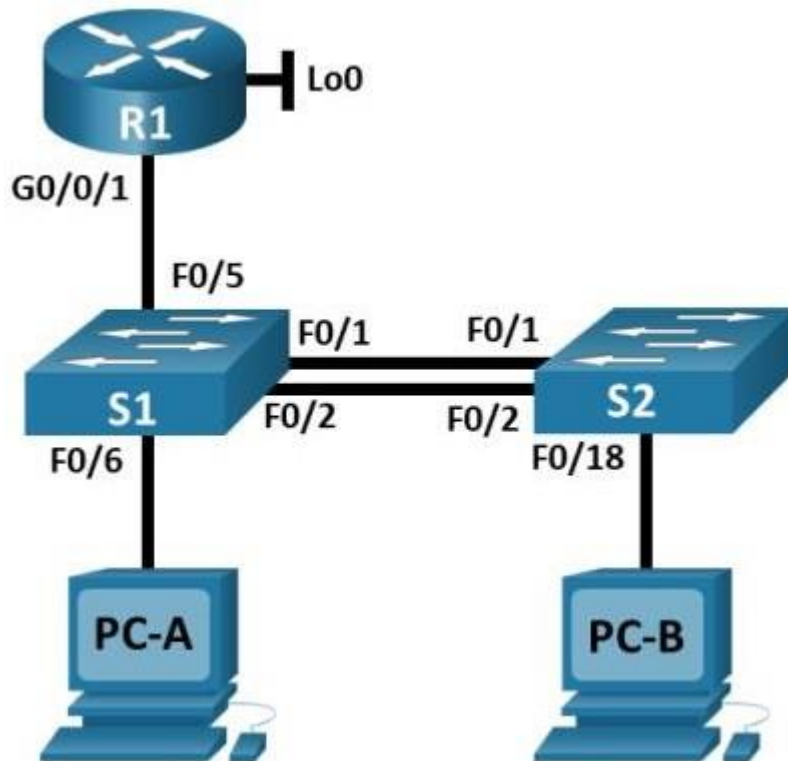
At the bottom left of the Command Prompt window, there is a checkbox labeled "Top".

Fuente: Autoría propia

Se comprueba que haya conexión a la VLAN 1 normalmente salta error en esta prueba, pero solo basta con activar la VLAN en el Router con el comando no shutdown.

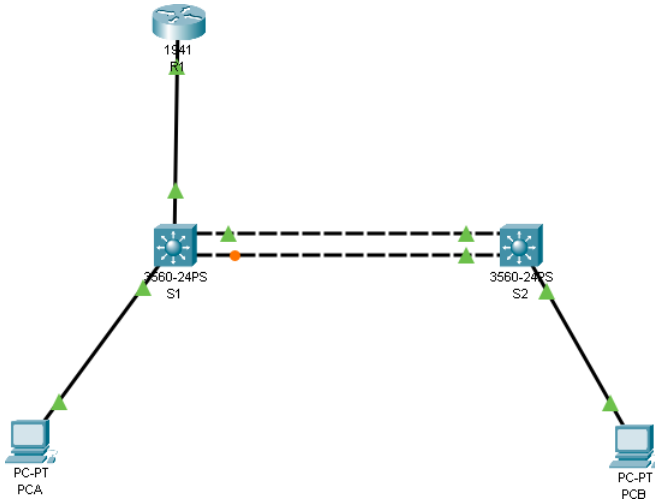
1.2 Escenario 2

Figura 11. Topología básica



Fuente: Prueba de habilidades CNNA 2022

Figura 12 Topología en el simulador



Fuente: Cristian Salguero

Paso 1. Reseteo de Router y Switch.

Router 1 reseteo

```
Router#delete vlan.data
Delete filename [vlan.data]?
Delete flash:/vlan.data? [confirm]
%Error deleting flash:/vlan.data (No such file or directory)
```

```
Router#erase star
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
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Switch 1 reseteo

```
Switch>en
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

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

Switch 2 reseteo

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#delete vlan. dat
^
% Invalid input detected at '^' marker.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase s
```

```
Switch#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
Switch#
Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

Paso 2 Configuración SDM.

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

Switch 1 configuración IPV6

```
Switch>en
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sdm prefer dual-
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
Changes to the running SDM preferences have been stored, but cannot take effect until
the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
```

Switch 2 configuración IPV6

```
Switch>en
Switch# configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sdm prefer du
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
Changes to the running SDM preferences have been stored, but cannot take effect until
the next reload.
```

```

Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#
Switch(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]

```

Paso 3: Configuraciones básicas Router y switches

Tabla 7 Configuración R1

Tarea	Código
Desactivar la búsqueda DNS	R1(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R1
Nombre del dominio	R1(config)#username ccna-sa.com
Contraseña cifrada del modo EXEC Privilegiado	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#enable password cisco
Establecer la longitud mínima para contraseñas	R1(config)#security passwords min-length 5
Crear un usuario administrativo en la base de datos local	R1#configure t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#username admin password admin1pass R1(config)#line console 0 R1(config-line)#login local R1(config-line)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY Solo aceptando SSH	R1(config)#line vty 0 4 R1(config-line)#transport input ssh R1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption R1(config)#exit

Configure un MOTD Banner	<pre>R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#banner motd %R1 Cristian Chayane salguero valero ingenieria de sistemas% R1(config)#</pre>
Habilitar el routing IPV6	<pre>R1(config)#ipv6 unicast-routing R1(config)#exit</pre>
Configurar interfaz G0/0/1 y subinterfaces	<pre>R1(config)#in g0/1.20 R1(config-subif)#ip add 10.09.8.1 255.255.255.192 R1(config-subif)#exit R1(config)#in g0/1.30 R1(config-subif)#ip add 10.09.8.1 255.255.255.224 % 10.9.8.0 overlaps with GigabitEthernet0/1.20 R1(config-subif)#ip add 10.09.8.65 255.255.255.224 R1(config-subif)#exit R1(config)# R1(config)#in g0/1.40 R1(config-subif)#description puerta de enlace predeterminada vlan 40 R1(config-subif)#encapsulation dot1Q 40 R1(config-subif)#ip add 10.09.8.97 255.255.255.248 R1(config-subif)#exit R1(config)#</pre>

	<p>Configuración IPV6</p> <pre>R1(config-subif)#ipv6 add 2001:db8:acad:a::1/64 R1(config-subif)#exit R1(config)#in g0/1.30 R1(config-subif)#ipv6 add 2001:db8:acad:b::1/64 R1(config-subif)#exit R1(config)#in g0/1.40 R1(config-subif)#ipv6 add 2001:db8:acad:c::1/64 R1(config-subif)#exit R1(config)#in g0/1 R1(config-if)#no shutdown</pre>
<p>Configurar el loopback0 interface</p>	<pre>R1(config)#in loopback 0 R1(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up R1(config-if)#description puerta de enlace loopback 0 R1(config-if)#ip add 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address fe80::1 link-local R1(config-if)#exit</pre>
<p>Generar una clave de cifrado RSA</p>	<pre>R1(config)#ip domain-name ccna-sa.com R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna- sa.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</pre>

Fuente: Autoría propia

Tabla 8 Configuración S1

Tarea	Código
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup S1(config)#
Nombre del Switch	Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#host S1 S1(config)#
Nombre del dominio	S1(config)#ip domain-name ccna-sa.com
Contraseñas cifradas para el modo EXEC privilegiado	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#enable password cisco
Crear un usuario administrativo en la base de datos local	S1(config)#enable password cisco S1(config)#username admin password admin1pass S1(config)#line console 0 S1(config-line)#login local S1(config-line)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 4 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 4 S1(config-line)#transport input ssh S1(config-line)#login local
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd %S1 Cristian Chayane Salguero Vlaero Ingenieria de Sistemas%
Generar una clave de cifrar 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

	<p>modulus greater than 512 may take a few minutes.</p> <p>How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]</p>
Configurar la interfaz de administración (SVI)	<pre>S1(config)#in vlan 40 S1(config-if)#ip add 10.09.8.98 255.255.255.248 S1(config)#in vlan 40 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#exit</pre>
Configuración del Gateway predeterminado	<pre>S1(config)#ip default-gateway 10.09.8.97 S1(config)#exit</pre>

Fuente: Autoría propia

Tabla 9 Configuración S2

Tarea	Código
Desactivar la búsqueda DNS	<pre>S2(config)#no ip domain-lookup S2(config)#</pre>
Nombre del Switch	<pre>Switch>en Switch#conf t Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#host S1 S2(config)#</pre>
Nombre del dominio	<pre>S2(config)#ip domain-name ccna-sa.com</pre>
Contraseñas cifradas para el modo EXEC privilegiado	<pre>S2(config)#enable secret class</pre>
Contraseña de acceso a la consola	<pre>S2(config)#enable password cisco</pre>
Crear un usuario administrativo en la base de datos local	<pre>S2(config)#enable password cisco S2(config)#username admin password</pre>

	admin1pass S2(config)#line console 0 S2(config-line)#login local S2(config-line)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 4 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 4 S2(config-line)#transport input ssh S2(config-line)#login local
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd %S2 Cristian Chayane Salguero Vlaero Ingenieria de Sistemas%
Generar una clave de cifrar RSA	S2(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)	S2(config)#in vlan 40 S2(config-if)#ip add 10.09.8.99 255.255.255.248 S2(config-if)#ipv6 add FE80::99 link-local S2(config-if)#exit
Configuración del Gateway predeterminado	S2(config)#ip default-gateway 10.09.8.97 S2(config)#exit

Fuente: Autoría propia

Paso 4: Configuración de VLAN, troncos y EtherChannel

Tabla 10 Configuración infraestructural S1, creación de VLAN y troncales

Tarea	Código
Crear VLAN	<pre>S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#exit S1(config)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#exit S1(config)#vlan 40 S1(config-vlan)# %LINK-5-CHANGED: Interface Vlan40, changed state to up S1(config-vlan)#name invitados S1(config-vlan)#exit S1(config)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#exit S1(config)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)#</pre>
Crear Troncos 802.1Q que utilicen VLAN 56 nativa	<pre>S1(config)#in range fa0/1-2 S1(config-if-range)#sw S1(config-if-range)#switchport mode trunk S1(config-if-range)#sw S1(config-if-range)#switchport trunk native vlan 56 S1(config-if-range)#exit</pre>
Crear Un grupo de Puertos EtherChannel de capa 2 que use interfaces f0/1y f0/2	<pre>S1(config)#in range fa0/1-2 S1(config-if-range)#channel-protocol lacp S1(config-if-range)#channel-group 1 mode active</pre>
Configurar el puerto de acceso de host para VLAN 20	<pre>S1(config)#int f0/6 S1(config-if)#sw mo access S1(config-if)#sw access vlan 20 S1(config-if)#exit</pre>
Configurar la seguridad del puerto en	<pre>S1(config)#in fa0/6</pre>

los puertos de acceso	<pre> S1(config-if)#sw mode access S1(config-if)#sw mode access S1(config-if)#sw S1(config-if)#switchport port- S1(config-if)#switchport port-security S1(config-if)#switch S1(config-if)#switchport port S1(config-if)#sw S1(config-if)#switchport por S1(config-if)#switchport port-security maximum 4 S1(config-if)# </pre>
Proteja todas las interfaces no usadas	<pre> S1(config)#in range fa0/7-24 S1(config-if-range)#sw S1(config-if-range)#switchport mode acces S1(config-if-range)#sw S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description no usadas/no habilitadas S1(config-if-range)#shutdown S1(config)#in range fa0/3-4 S1(config-if-range)#sw S1(config-if-range)#switchport mode access S1(config-if-range)#sw S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description no usadas/no habilitadas S1(config-if-range)#shutdown </pre>

Fuente: Autoría Propia

Se configuran 5 VLAN que alojaran a todos los hosts, además se crea la VLAN nativa que albergara los enlaces troncales, luego de eso se configura el protocolo 802.1Q, para poder crear los enlaces troncales para un mejor flujo de datos

Por último, usamos la función Ether channel para crear un grupo esto es muy útil para conexione entre switches aumenta la velocidad y el flujo.

Tabla 11 Configuración infraestructural S2, Creación de VLAN y Troncales

Tarea	Código
Crear VLAN	<pre>S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#exit S2(config)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#exit S2(config)#vlan 40 S2(config-vlan)# %LINK-5-CHANGED: Interface Vlan40, changed state to up S2(config-vlan)#name invitados S2(config-vlan)#exit S2(config)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#exit S2(config)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit S2(config)#</pre>
Crear Troncos 802.1Q que utilicen VLAN 56 nativa	<pre>S2(config)#in range fa0/1-2 S2(config-if-range)#sw S2(config-if-range)#switchport mode trunk S2(config-if-range)#sw S2(config-if-range)#switchport trunk native vlan 56 S2(config-if-range)#exit</pre>
Crear Un grupo de Puertos EtherChannel de capa 2 que use interfaces f0/1y f0/2	<pre>S2(config)#in range fa0/1-2 S2(config-if-range)#channel-protocol lacp S2(config-if-range)#channel-group 1 mode passive</pre>
Configurar el puerto de acceso de host para VLAN 30	<pre>S1(config)#int f0/18 S1(config-if)#sw mo access S1(config-if)#sw access vlan 30 S1(config-if)#exit</pre>
Configurar la seguridad del puerto en	<pre>S2(config)#in fa0/18 S2(config-if)#sw</pre>

los puertos de acceso	<pre> S2(config-if)#switchport mode access S2(config-if)#sw S2(config-if)#switchport port S2(config-if)#switchport port-security S2(config-if)#sw S2(config-if)#switchport port S2(config-if)#switchport port-security maximum 4 S2(config-if)#exit S2(config)# </pre>
Proteja todas las interfaces no usadas	<pre> S2(config)#in range fa0/3-17 S2(config-if-range)#sw S2(config-if-range)#switchport mode access S2(config-if-range)#sw S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description no usadas/deshabilitadas S2(config-if-range)#shutdown S2(config-if-range)#exit S2(config)#in range fa0/19-24 S2(config-if-range)#sw S2(config-if-range)#switchport mode access S2(config-if-range)#sw S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description no usados/deshabilitadas S2(config-if-range)#shutdown </pre>

Fuente: Autoría propia

Parte 5: Configurar soporte de host

Tabla 12 Configuración Para Host

Tareas	Código
Configure Default Routing	<pre>R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip route 0.0.0.0 0.0.0.0 loopback0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)# R1(config)#ipv6 route ::/0 loopback0</pre>
Configurar ipv4 dhcp para VLAN 20	<pre>R1(config)#service dhcp R1(config)#ip dhcp pool vlan20 R1(dhcp-config)#network 10.09.8.1 255.255.255.192 R1(config)#ip dhcp excluded-address 10.09.8.2 10.09.8.53 R1(config)#ip dhcp pool vlan20 R1(dhcp-config)#default-router 10.09.8.2 R1(dhcp-config)#domain-name unad-ccna- sa.net R1(dhcp-config)#exit</pre>
Configurar DHCP ipv4 para VLAN 30	<pre>R1(config)#service dhcp R1(config)#ip dhcp pool vlan30 R1(dhcp-config)#network 10.09.8.64 255.255.255.224 R1(dhcp-config)#ip dhcp excluded-address 10.09.8.65 10.09.8.84 R1(config)#ip dhcp pool vlan30 R1(dhcp-config)#default-router 10.09.8.65 R1(dhcp-config)#domain-name unad-cnna- sb.net R1(dhcp-config)#exit R1(config)#</pre>

Fuente: Autoría propia

Paso 6: Configurar los servidores

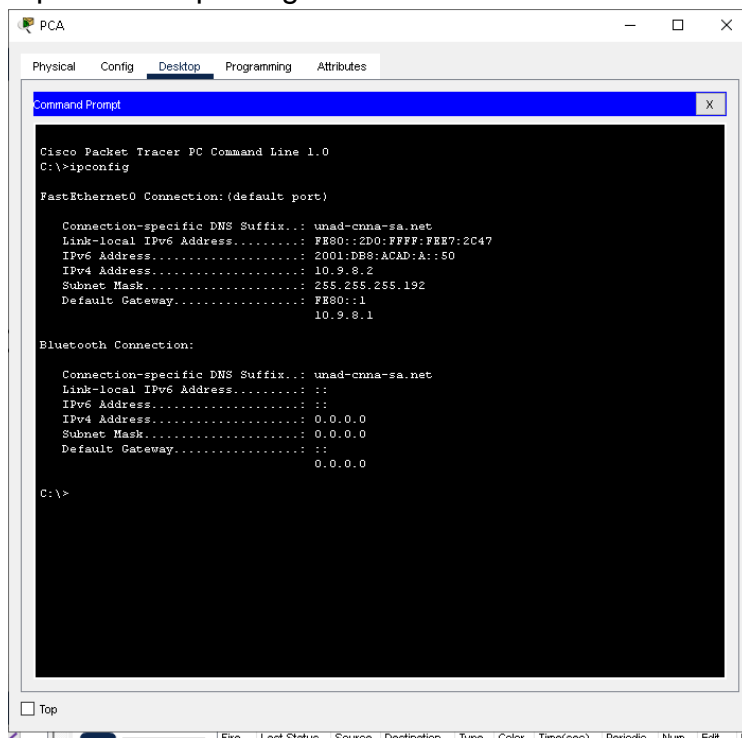
Tabla 13 Configuración PC-A

Configuración de red de PC-A	
Descripción	unad-ccna-sa.com
Dirección física	00D0.FFE7.2C47
Dirección IP	10.9.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.9.8.1
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría propia

Se configura los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y se asigna manualmente de manera estática las direcciones IPv6 GUA y Link Local. Después se configura cada servidor, por último, se evidencian las configuraciones de red del host con el comando `ipconfig /all`.

Figura 13 PCA prueba de ipconfig



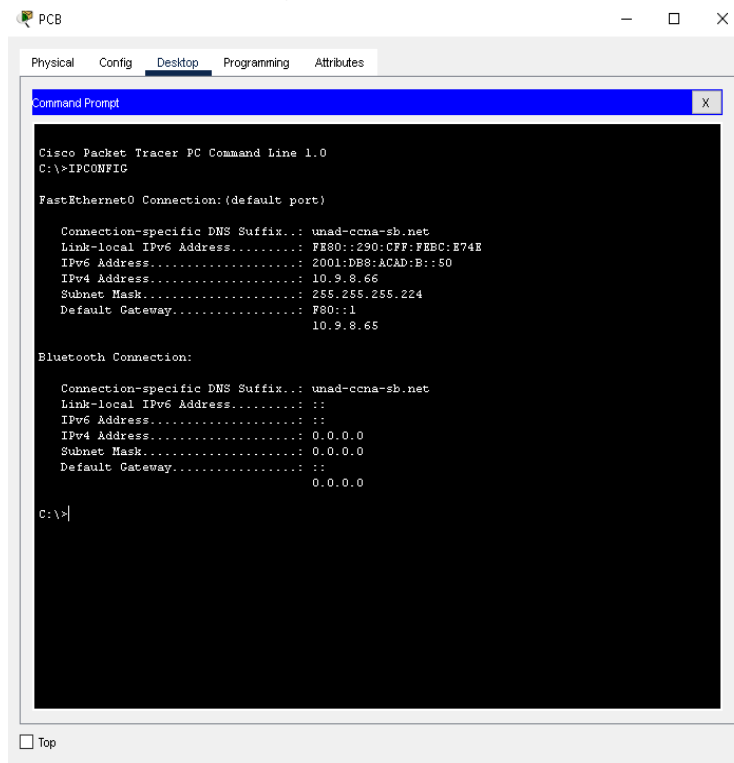
Fuente: Autoría propia

Tabla 14. Configuración PC-B

Configuración de red de PC-B	
Descripción	unad-ccna-sb.com
Dirección física	0090.OCBC.E74E
Dirección IP	10.9.8.52
Máscara de subred	255.255.255.224
Gateway predeterminado	10.9.8.66
Gateway predeterminado IPv6	FE80::1

Fuente: Autoría Propia

Figura 14. PCB prueba de ipconfig



```
PCB
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>IPCONFIG

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: unad-ccna-sb.net
Link-local IPv6 Address...: FE80::290:CFE:FEEC:E74E
IPv6 Address...: 2001:DB8:ACAD:B::50
IPv4 Address...: 10.9.8.66
Subnet Mask...: 255.255.255.224
Default Gateway...: F80::1
10.9.8.65

Bluetooth Connection:

Connection-specific DNS Suffix...: unad-ccna-sb.net
Link-local IPv6 Address...: ::
IPv6 Address...: ::
IPv4 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...: ::
0.0.0.0

C:\>
```

Fuente: Autoría propia

Paso 7: Conectividad

Tabla 15: Pruebas

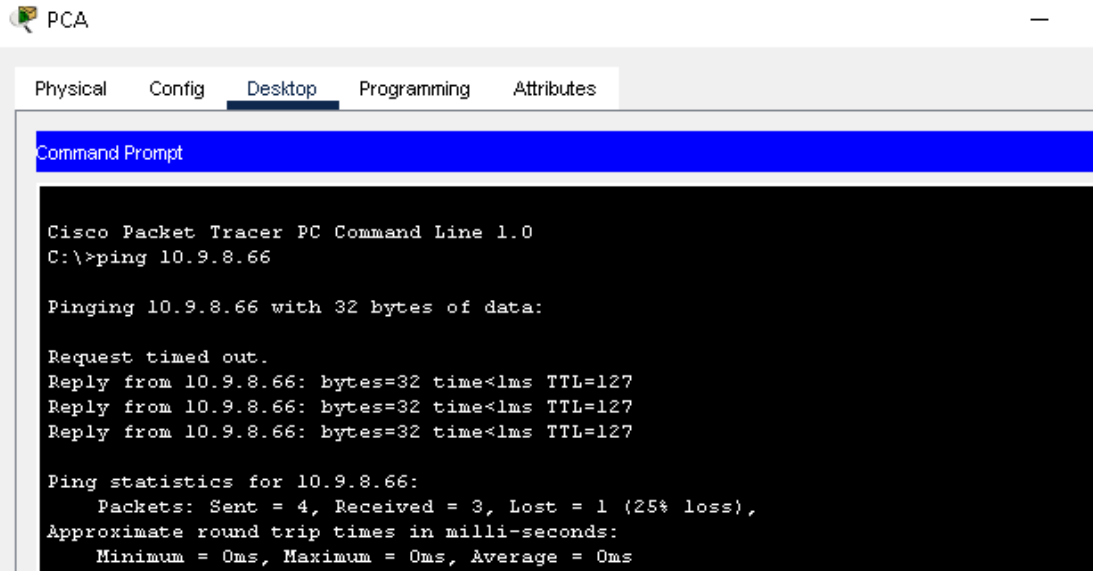
Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.9.8.1	Afirmativo. Figura 15
		IPv6	2001:db8:acad:a: :1	Afirmativo Figura 16
	R1, G0/0/1.3	Dirección	10.9.8.66	Afirmativo Figura 17
		IPv6	2001:db8:acad:b: :1	Afirmativo Figura 18
	R1, G0/0/1.4	Dirección	10.9.8.97	Afirmativo Figura 19
		IPv6	2001:db8:acad:c: :1	Afirmativo Figura 20
	S1, VLAN 40	Dirección	10.9.8.98	Afirmativo Figura 21
		IPv6	2001:db8:acad:c: :98	Negativo Figura 22
	S2, VLAN 40	Dirección	10.9.8.99.	Afirmativo Figura 23
		IPv6	2001:db8:acad:c: :99	Negativo Figura 24

Desde	A	de Internet	Dirección IP	Resultados de ping
	PC-B	Dirección	10.9.8.66	Afirmativo Figura 25
		IPv6	2001:db8:acad:a :50	Negativo Figura 26
	R1 loopback 0	Dirección	209.165.201.1	Afirmativo Figura 27
		IPv6	2001:db8:acad:209: :1	Afirmativo Figura 28
PC-B	R1 loopback 0	Dirección	209.165.201.1	Afirmativo Figura 29
		IPv6	2001:db8:acad:209: :1	Afirmativo Figura 30
	R1, G0/0/1.2	Dirección	10.9.8.1	Afirmativo Figura 31
		IPv6	2001:db8:acad:a :1	Afirmativo Figura 32
	R1, G0/0/1.3	Dirección	10.9.8.65	Afirmativo Figura 33
		IPv6	2001:db8:acad:b :1	Afirmativo Figura 34
	R1, G0/0/1.4	Dirección	10.9.8.97	Afirmativo Figura 35
		IPv6	2001:db8:acad:c :1	Afirmativo

				Figura 36
S1, VLAN 40	Dirección	10.9.8.98		Afirmativo Figura 37
	IPv6	2001:db8:acad:c :98		Negativo Figura 38
S2, VLAN 40	Dirección	10.9.8.99.		Afirmativo Figura 39
	IPv6	2001:db8:acad:c :99		Negativo Figura 40

Fuente: Autoría propia

Figura 15. PC-A a G0/1.2 IPV4



```

PCA
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.9.8.66

Pinging 10.9.8.66 with 32 bytes of data:

Request timed out.
Reply from 10.9.8.66: bytes=32 time<1ms TTL=127
Reply from 10.9.8.66: bytes=32 time<1ms TTL=127
Reply from 10.9.8.66: bytes=32 time<1ms TTL=127

Ping statistics for 10.9.8.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Fuente: Autoría propia

Figura 16. PC-A a G0/1.50 IPV6

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

C:\>
```

Top

Fuente: Autoría propia

Figura 17. PC-A a G0/1.3 IPV4

```
Pinging 10.9.8.66 with 32 bytes of data:

Reply from 10.9.8.66: bytes=32 time<lms TTL=127
Reply from 10.9.8.66: bytes=32 time<lms TTL=127
Reply from 10.9.8.66: bytes=32 time<lms TTL=127
Reply from 10.9.8.66: bytes=32 time<lms TTL=127

Ping statistics for 10.9.8.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 18. PC-A a G0/1.51 IPV6

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

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

C:\>
```

Top

Fuente: Autoría propia

Figura 19. PC-A a G0/1.4 IPV4

```
C:\>ping 10.9.8.97

Pinging 10.9.8.97 with 32 bytes of data:

Reply from 10.9.8.97: bytes=32 time<lms TTL=255
Reply from 10.9.8.97: bytes=32 time<lms TTL=255
Reply from 10.9.8.97: bytes=32 time<lms TTL=255
Reply from 10.9.8.97: bytes=32 time<lms TTL=255

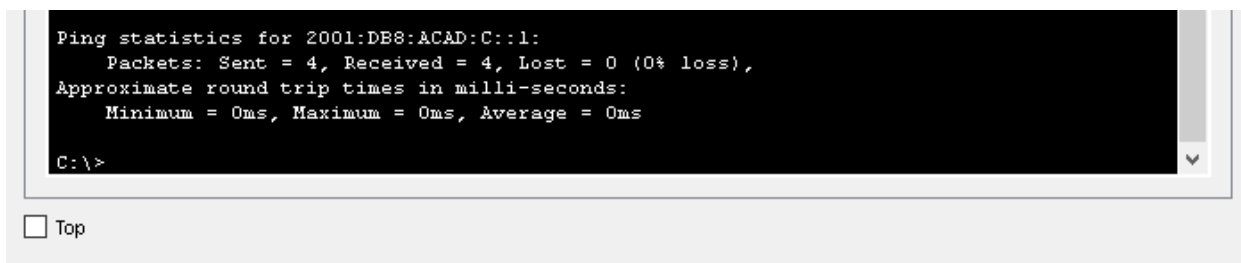
Ping statistics for 10.9.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 20. PC-A a G0/1.52 IPV6

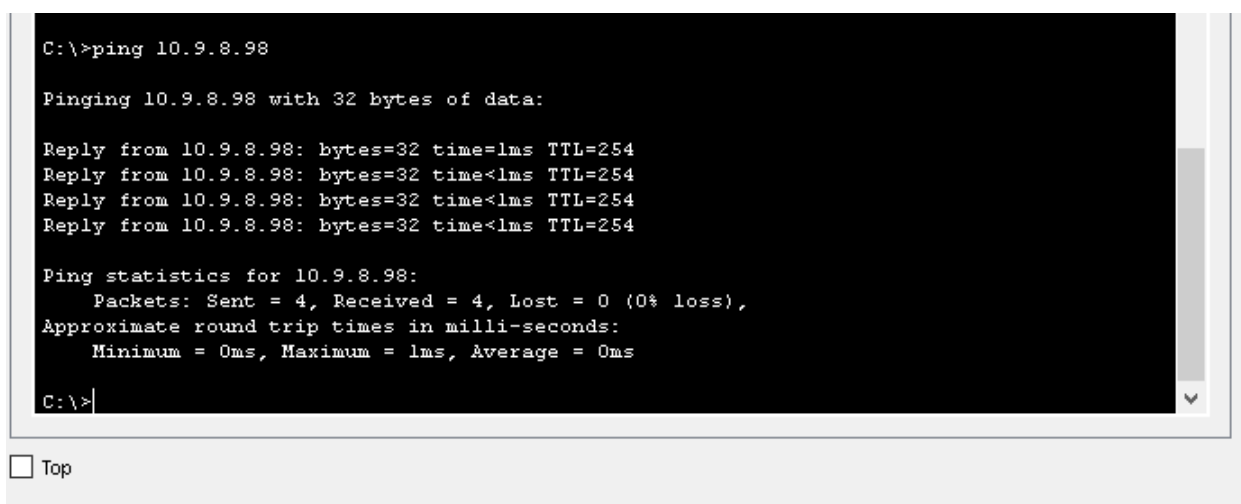


```
Ping statistics for 2001:DB8:ACAD:C::1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
C:\>
```

Top

Fuente: Autoría propia

Figura 21. PC-A a S1 VLAN 40 IPV4



```
C:\>ping 10.9.8.98  
  
Pinging 10.9.8.98 with 32 bytes of data:  
  
Reply from 10.9.8.98: bytes=32 time=1ms TTL=254  
Reply from 10.9.8.98: bytes=32 time<1ms TTL=254  
Reply from 10.9.8.98: bytes=32 time<1ms TTL=254  
Reply from 10.9.8.98: bytes=32 time<1ms TTL=254  
  
Ping statistics for 10.9.8.98:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 1ms, Average = 0ms  
C:\>
```

Top

Fuente: Autoría propia

Figura 22 PC-A a S53 VLAN 40 IPV6

```
C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

Fuente: Autoría propia

Este ping es incorrecto por un problema en la IOS del Switch pero la configuración es correcta.

Figura 23. PC-A a S2 VLAN 40 IPV4

```
Pinging 10.9.8.99 with 32 bytes of data:

Reply from 10.9.8.99: bytes=32 time=12ms TTL=254
Reply from 10.9.8.99: bytes=32 time<1ms TTL=254
Reply from 10.9.8.99: bytes=32 time<1ms TTL=254
Reply from 10.9.8.99: bytes=32 time=8ms TTL=254

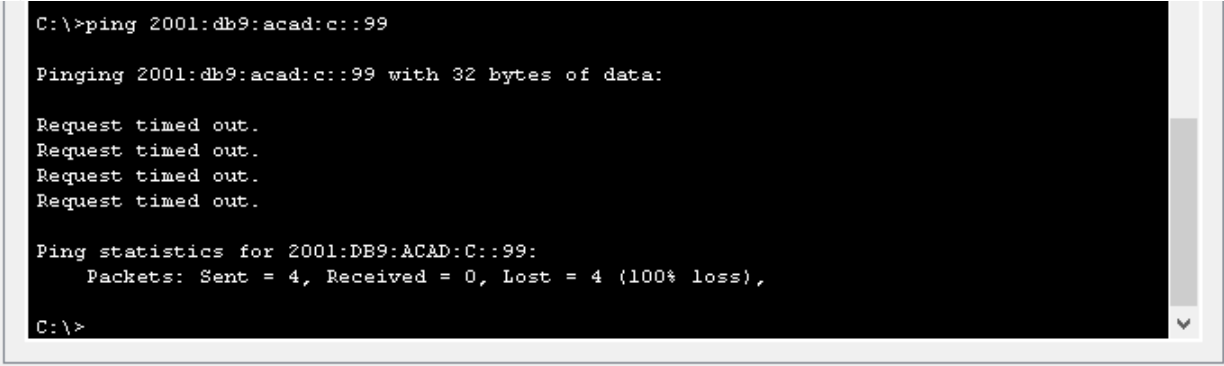
Ping statistics for 10.9.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\>
```

Top

Fuente: Autoría propia

Figura 24 PC-A a S54 VLAN 40 IPV6



```
C:\>ping 2001:db9:acad:c::99

Pinging 2001:db9:acad:c::99 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB9:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

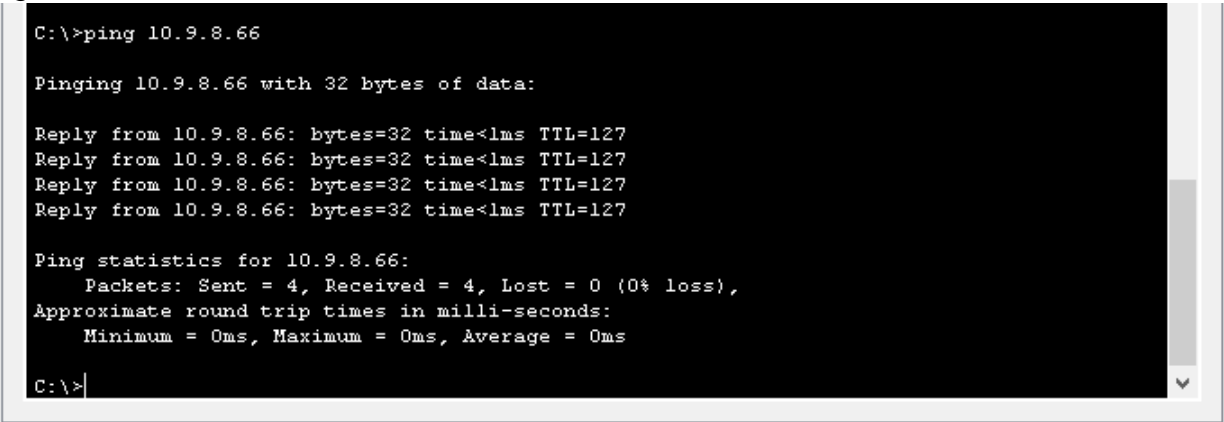
C:\>
```

Top

Fuente: Autoría propia

No es exitoso este ping por un problema de IOS del switch.

Figura 25. PC-A a PC-B IPV4



```
C:\>ping 10.9.8.66

Pinging 10.9.8.66 with 32 bytes of data:

Reply from 10.9.8.66: bytes=32 time<1ms TTL=127
Reply from 10.9.8.66: bytes=32 time<1ms TTL=127
Reply from 10.9.8.66: bytes=32 time<1ms TTL=127
Reply from 10.9.8.66: bytes=32 time<1ms TTL=127

Ping statistics for 10.9.8.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 26. PC-A a PC-B IPV6

```
C:\>
C:\>ping 2001:DB8:ACAD:B::50

Pinging 2001:DB8:ACAD:B::50 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

Fuente: Autoría propia

Figura 27. PC-A a loopback 0 IPV6

```
C:\>PING 209.165.201.1

Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 28. PC-A a loopback 0 IPV6

```
C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<lms TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

Figura 29. PC-B a loopback 0 IPV4

```
Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255
Reply from 209.165.201.1: bytes=32 time<lms TTL=255

Ping statistics for 209.165.201.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 30. PC-B a loopback 0 IPV6

```
C:\>ping 2001:db8:acad:209::1

Pinging 2001:db8:acad:209::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255
Reply from 2001:DB8:ACAD:209::1: bytes=32 time<1ms
TTL=255

Ping statistics for 2001:DB8:ACAD:209::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

Figura 31. PC-B G0/1.2 IPV4

```
C:\>ping 10.9.8.1

Pinging 10.9.8.1 with 32 bytes of data:

Reply from 10.9.8.1: bytes=32 time=12ms TTL=255
Reply from 10.9.8.1: bytes=32 time<1ms TTL=255
Reply from 10.9.8.1: bytes=32 time<1ms TTL=255
Reply from 10.9.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.9.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

Fuente: Autoría propia

Figura 32. PC-B a G0/1.58 IPV6

```
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<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<lms 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 = 0ms, Average = 0ms

C:\>
```

Fuente: Autoría propia

Figura 33. PC-B a G0/1.3 IPV4

```
C:\>ping 10.9.8.65

Pinging 10.9.8.65 with 32 bytes of data:

Reply from 10.9.8.65: bytes=32 time<lms TTL=255
Reply from 10.9.8.65: bytes=32 time<lms TTL=255
Reply from 10.9.8.65: bytes=32 time=8ms TTL=255
Reply from 10.9.8.65: bytes=32 time<lms TTL=255

Ping statistics for 10.9.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Top

Fuente: Autoría propia

Figura 34. PC-B a G0/1.59 IPV6

```
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 = 1ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 35. PC-B a G0/1.4 IPV4

```
C:\>ping 10.9.8.97

Pinging 10.9.8.97 with 32 bytes of data:

Reply from 10.9.8.97: bytes=32 time<1ms TTL=255
Reply from 10.9.8.97: bytes=32 time<1ms TTL=255
Reply from 10.9.8.97: bytes=32 time<1ms TTL=255
Reply from 10.9.8.97: bytes=32 time=8ms TTL=255

Ping statistics for 10.9.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>
```

Fuente: Autoría propia

Figura 36. PC-B a G0/1.60 IPV6

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

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

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

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

C:\>
```

Fuente: Autoría propia

Figura 37. PC-B a S1 VLAN 40 IPV4

```
C:\>
C:\>ping 10.9.8.98

Pinging 10.9.8.98 with 32 bytes of data:

Reply from 10.9.8.98: bytes=32 time=1ms TTL=254
Reply from 10.9.8.98: bytes=32 time<1ms TTL=254
Reply from 10.9.8.98: bytes=32 time<1ms TTL=254
Reply from 10.9.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.9.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 38 PC-B a S61 VLAN 40 IPV6

```
C:\>ping 2001:db8:acad:c::98

Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top

Fuente: Autoría propia

En este caso no es exitoso puesto que hay un problema en la IOS del Switch que no lo permite, pero la configuración es correcta.

Figura 39. PC-B a S2 VLAN 40 IPV4

```
C:\>ping 10.9.8.99

Pinging 10.9.8.99 with 32 bytes of data:

Reply from 10.9.8.99: bytes=32 time<1ms TTL=254
Reply from 10.9.8.99: bytes=32 time<1ms TTL=254
Reply from 10.9.8.99: bytes=32 time=1ms TTL=254
Reply from 10.9.8.99: bytes=32 time<1ms TTL=254

Ping statistics for 10.9.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Top

Fuente: Autoría propia

Figura 40 PC-B a S62 VLAN 40 IPV6

```
C:\>ping 2001:db8:acad:c::99

Pinging 2001:db8:acad:c::99 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fuente: Autoría propia

En este caso no es éxito debido a un problema en la IOS.

CONCLUSIONES

La importancia de que los sistemas sean seguros es uno de los principales pilares de las redes en la actualidad, con miles y miles de millones de usuarios diarios, en una gran red como lo es internet es bastante increíble que no haya muchos ataques o robo de información en esta super red.

Los protocolos y estándares que cisco nos ofrece logran revolucionar y además superar las mayorías de fallas de seguridad en una red, teniendo en cuenta mi proceso formativo se puede identificar todas las vulnerabilidades que puede llegar a tener una red y lo fácil que resulta entrar en una red que no cumpla con los básicos estándares de seguridad.

El direccionamiento IPv4 es uno de los pocos estándares que, aunque teniendo ya una versión más reciente sigue utilizándose hoy en día en la mayoría de nuestros dispositivos.

Los enlaces troncales permiten un mejor flujo de datos normalmente es de vital importancia para redes de mucho tráfico, en este caso se configuró el protocolo 802.1Q para que pueda ser soportado por los switches. Siempre hay que configurar no solo las interfaces Fast Ethernet, sino que también, como en este caso los grupos ether channel.

Incluso aunque la configuración este bien a veces solo la IOS de algún dispositivo tiene fallas como por ejemplo los Switchs 3560 que no permiten ciertos pings en especial con las configuraciones IPv6 que marcaron muchos errores a lo largo de la actualidad.

REFERENCIAS BIBLIOGRÁFICAS

CISCO. Configuración básica de un router. netacad [en línea]. (2020). [Consultado el 27, septiembre, 2022]. Disponible en Internet: <<https://contenthub.netacad.com/itn/10.0.1>>.

DÍAZ, Walter Marcelo Fuertes. Definición de un modelo genérico para la caracterización de escenarios virtuales de redes IP. Universidad Autónoma de Madrid. {en línea}. (2010). {17 de noviembre de 2022} disponible en <<https://dialnet.unirioja.es/servlet/tesis?codigo=34220>>

GARDOKI, Cardenal. Qué es el protocolo SSH y cómo configurarlo para mejorar la seguridad de acceso a los servidores Linux. Hostalia whitepapers{en línea}(sin año) {12 de noviembre de 2022} disponible en <<https://pressroom.hostalia.com/contents/ui/theme/images/WP-Hostalia-protocolo-SSH.pdf>>

GÓMEZ, Joaquín Andréu. Redes locales. Editex, {en línea} (2011).{22 noviembre 2022} disponible en <https://books.google.es/books?hl=es&lr=&id=Tqz4mj2mtAC&oi=fnd&pg=PA126&dq=G%C3%93MEZ,+Joaqu%C3%ADn+Andr%C3%A9u.+Redes+locales.+Editex,+2011.&ots=TieBebIEz_&sig=uce4uWXnw_ZriTHhxACHphA4sdw#v=onepage&q=G%C3%93MEZ%2C%20Joaqu%C3%ADn%20Andr%C3%A9u.%20Redes%20locales.%20Editex%2C%202011.&f=false>

LANZA-GUTIERREZ, Jose M.; GOMEZ-PULIDO, Juan A.; VEGA-RODRIGUEZ, Miguel A. Un nuevo enfoque para el posicionamiento de routers sobre redes de sensores inalámbricos. Universidad de Extremadura {en línea} (2013). {1 diciembre 2022} disponible en <https://www.researchgate.net/profile/Jose-Lanza-Gutierrez/publication/299529512_Un_Nuevo_Enfoque_para_el_Posicionamiento_de_Routers_Sobre_Redde_s_de_Sensores_Inalambricos/links/56fd4e5708aec9f5e7008107/Un-Nuevo-Enfoque-para-el-Posicionamiento-de-Routers-Sobre-Redes-de-Sensores-Inalambricos.pdf>

TEJEDOR DORIA, Jesús Alberto. Diseño, implementación, administración y enrutamiento Avanzado bajo el núcleo IOS CLI (Cisco). Universitat Politècnica de València.{en línea} (2015).{28 noviembre 2022} disponible en <<https://riunet.upv.es/handle/10251/48355>>

VARGAS MERCHAN, EDISON KLEBER. Diseño de una red lan y wan segura para la compañía automotores latinoamericanos SA Autolasa., Universidad de Guayaquil {en línea} (2016). {5 noviembre 2022} disponible en <<http://repositorio.ug.edu.ec/handle/redug/11713>>

ANEXOS

Anexo A

descarga de archivos de simulación

Enlace: https://drive.google.com/drive/folders/1RK-jM-V-eB9R9EJ_X4RE4AvdArCyTp7T?usp=sharing