

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

CARLOS EDUARDO PEÑA ROJAS

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

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

CARLOS EDUARDO PEÑA ROJAS

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

DIRECTOR:
PAULITA FLOR

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Valledupar, 27 de noviembre de 2022

CONTENIDO

LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCIÓN	11
ESCENARIO 1.....	13
ESCENARIO 2.....	22
CONCLUSIONES	51
BIBLIOGRAFÍA.....	52
ANEXOS.....	54

LISTA DE TABLAS

Tabla 1. Asignación de direcciones.....	13
Tabla 2. Configuración del Router R1.....	14
Tabla 3. Configuración del Switch S1.....	15
Tabla 4. Configuración del equipo PC-A.....	17
Tabla 5. Configuración del equipo PC-B.....	17
Tabla 6. Pruebas de conectividad.....	17
Tabla 7. Tabla de VLAN.....	22
Tabla 8. Asignación de direcciones.....	23
Tabla 9. Configuración del Router R1.....	24
Tabla 10. Configuración del Switch S1.....	25
Tabla 11. Configuración del Switch S2.....	26
Tabla 12. Configuración S1.....	28
Tabla 13. Configuración S2.....	30
Tabla 14. Configuración R1.....	33
Tabla 15. Configuración del equipo PC-A.....	34
Tabla 16. Configuración del equipo PC-B.....	35
Tabla 17. Pruebas de conectividad.....	36

LISTA DE FIGURAS

Figura 1. Topología de red escenario 1.....	13
Figura 2. Conectividad entre PC-A – R1 G0/0/0.....	18
Figura 3. Conectividad entre PC-A – R1 G0/0/1.....	19
Figura 4. Conectividad entre PC-A – S1 VLAN1.....	19
Figura 5. Conectividad entre PC-A – PC-B.....	20
Figura 6. Conectividad entre PC-B – R1 G0/0/0.....	20
Figura 7. Conectividad entre PC-B – R1 G0/0/1.....	21
Figura 8. Conectividad entre PC-B – S1 VLAN1.....	21
Figura 9. Topología de red escenario No. 2.....	22
Figura 10. Configuración PC-A.....	35
Figura 11. Configuración PC-B.....	36
Figura 12. Conectividad entre PC-A – R1 G0/0/1.20 IPv4	38
Figura 13. Conectividad entre PC-A – R1 G0/0/1.20 IPv6	38
Figura 14. Conectividad entre PC-A – R1 G0/0/1.30 IPv4	39
Figura 15. Conectividad entre PC-A – R1 G0/0/1.30 IPv6	39
Figura 16. Conectividad entre PC-A – R1 G0/0/1.40 IPv4	40
Figura 17. Conectividad entre PC-A – R1 G0/0/1.40 IPv6	40
Figura 18. Conectividad entre PC-A – S1 VLAN 40 IPv4.....	41
Figura 19. Conectividad entre PC-A – S1 VLAN 40 IPv6.....	41
Figura 20. Conectividad entre PC-A – S2 VLAN 40 IPv4.....	42
Figura 21. Conectividad entre PC-A – S2 VLAN 40 IPv6.....	42
Figura 22. Conectividad entre PC-A – PC-B IPv4.....	43
Figura 23. Conectividad entre PC-A – PC-B IPv6.....	43

Figura 24. Conectividad entre PC-A – R1 Bucle 0 IPv4.....	44
Figura 25. Conectividad entre PC-A – R1 Bucle 0 IPv6.....	44
Figura 26. Conectividad entre PC-B – R1 Bucle 0 IPv4.....	45
Figura 27. Conectividad entre PC-B – R1 Bucle 0 IPv6.....	45
Figura 28. Conectividad entre PC-B – R1 G0/0/1.20 IPv4	46
Figura 29. Conectividad entre PC-B – R1 G0/0/1.20 IPv6	46
Figura 30. Conectividad entre PC-B – R1 G0/0/1.30 IPv4	47
Figura 31. Conectividad entre PC-B – R1 G0/0/1.30 IPv6	47
Figura 32. Conectividad entre PC-B – R1 G0/0/1.40 IPv4	48
Figura 33. Conectividad entre PC-B – R1 G0/0/1.40 IPv6	48
Figura 34. Conectividad entre PC-B – S1 VLAN 40 IPv4.....	49
Figura 35. Conectividad entre PC-B – S1 VLAN 40 IPv6.....	49
Figura 36. Conectividad entre PC-B – S2 VLAN 40 IPv4.....	50
Figura 37. Conectividad entre PC-B – S2 VLAN 40 IPv6.....	50

GLOSARIO

Dirección IP: es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.¹

Mascara de subred: es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores. Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.²

Enrutamiento: es el proceso que permite que los paquetes IP enviados por el host origen lleguen al host destino de forma adecuada.³

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.⁴

DHCP: (Dynamic Host Configuration Protocol) es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red.⁵

¹ DE LA CUADRA, Elena. Internet: Conceptos básicos.(1996)

² COBO YERA, Angel Luis, Direccionamiento IP – subredes.(2009)

³ VALVERDE CORTEZ, Betsabeth Yolanda, Analisis comparativo de los protocolos de enrutamiento dinámico de una red de transporte para la universidad de Guayaquil.(2016)

⁴ GARIMELLA, Prashant, et al. Characterizing VLAN usage in an operational network.(2007)

⁵ DROMS, Ralph. Stateless dynamic host configuration protocol (DHCP) service for IPv6. (2004).

RESUMEN

En el presente documento se da solución a dos escenarios que consisten en la configuración de cada uno de los dispositivos de una red pequeña, permitiendo el establecimiento de conexiones para cada elemento conectado a la red, que son las conexiones IPv4 del protocolo de Internet, la cual, es la forma de uso general de IP Addressing usada para identificar los host y utiliza un formato de 32 bits y la versión 6 (IPv6) del protocolo de Internet que es el estándar de la dirección IP de la última generación, previsto para substituir el formato del IPv4; es decir, que se realizan las configuraciones del IPv4 y del IPv6 en el dispositivo del punto de acceso de las redes y se hace el diagnóstico con el comando ping, para verificar el estado de determinada conexión de host local.

Palabras claves: Conexiones IPv4, host, ping. Protocolo de internet

ABSTRACT

This document provides a solution to two scenarios that consist of the configuration of each of the devices of a small network, allowing the establishment of connections for each element connected to the network, which are the IPv4 connections of the Internet protocol, the which is the commonly used form of IP addressing used to identify hosts and uses a 32-bit format and version 6 (IPv6) of the Internet Protocol which is the next generation IP address standard intended to replace the IPv4 format; that is to say, that the IPv4 and IPv6 configurations are made in the network access point device and the diagnosis is made with the ping command, to verify the status of a certain local host connection.

Keywords: IPv4 connections, host, ping. internet protocol

INTRODUCCIÓN

En atención al desarrollo tecnológico y las conectividades de las diferentes comunicaciones, utilizadas por toda la humanidad a través de diversos dispositivos electrónicos, se hace imperioso apropiarse de las arquitecturas de las redes de datos entre los sistemas que lo componen, como también contar con los elementos necesarios para la organización de la red, así mismo, es supremamente necesario realizar buenos diseños, que permitan o faciliten el almacenamiento, procesamiento y respaldo de la información que circula por medio de los canales de datos.

En este documento se evidencian los diseños de red dispuestos como proyecto de grado del programa de Ingeniería de sistemas, es así que se desarrollaron las topologías de red, como es el caso del primer escenario compuesto por un router, switch y dos equipos de cómputos, con una configuración básica y su respectivo direccionamiento con asignación de IP, lo anterior con los cálculos previos por medio de la estrategia de sub-neteo, subsiguientemente con los resultados obtenidos se da paso a la creación de dos subredes, para que estas alcancen a distribuir y recepción de paquetes como redes únicas y/o individuales.

Para el caso dos, implementado con un router, dos switch y dos PC, con una configuración más avanzada que en simulación de permitirá al usuario final contar con una red direccionado con IPv4 e IPv6, igualmente con previo estudio con el método de sub-neteo para identificar las direcciones y posteriormente plasmar a los dispositivos sus respectivos ajustes; con los ejercicios planteados se realizan múltiples pruebas de conexión entre los equipos que competen cada una de las redes, por medio de navegación, envío de paquetes y comandos ping, para las fallas halladas se realizaron correcciones correspondientes.

Es preciso decir, que en este documento encontrará en la solución de los dos casos, muestra de los conceptos y conocimientos obtenidos, mediante la configuración de

las redes planteadas para este diplomado de profundización CISCO, entre los temas a encontrar están las configuraciones iniciales de los dispositivos, configuración manual y automática por DHCP de las direcciones IP, creación y configuración de VLAN, parámetros de configuración de los dispositivos, los cuales se pueden configurar mediante consola y/o equipo de cómputo, esto nos permite como administradores de redes conocer herramientas y metodologías para el diseño, configuración y la actualización de los conceptos de redes basados en la gestión e implementación de estándares internacionales, que le permitan al usuario final disfrutar de una buena comunicación, dando alcance a los parámetros de las tecnologías aplicables a internet, considerando las redes planteadas en los casos como proyectos confiables y aplicables según las especificaciones descritas en las normatividades vigentes.

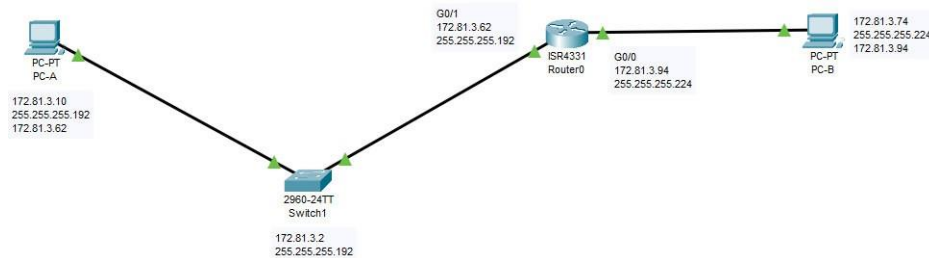
DESARROLLO DE ESCENARIOS

ESCENARIO 1

Construcción de la red

Se realiza la conexión de los dispositivos de una pequeña red. En este primer escenario se configurarán los dispositivos de una pequeña red, la cual está compuesta por un router, un switch y equipos, así mismo se realizará el diseño del esquema de direccionamiento IPv4 para las LAN propuestas. El router y switch también se administran de forma segura.

Figura 1. Topología de red escenario 1



Fuente: Autor

Desarrollo del esquema de direccionamiento IP

Tabla 1. Asignación de direcciones

ÍTEM	REQUERIMIENTO
Dirección de Red	172.81.3.0
Requerimiento de host Subred LAN1	60
Requerimiento de host Subred LAN2	20
R1 G0/0/1	172.81.3.62
R1 G0/0/0	172.81.3.94
S1 SVI	172.81.3.2
PC-A	172.81.3.10
PC-B	172.81.3.74

Fuente: Autor

Configuración de ajustes básicos

Tabla 2. Configuración del Router R1

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Router	Router>
Ingresar a modo privilegiado	Router>enable
Ingresar a modo de configuración	Router#configure terminal
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombrar Router R1	Router(config)#hostname R1
Nombrar dominio ccna-sa.com	R1(config)#ip domain-name ccna-sa.com
Asignar contraseña cifrada "ciscoenpass" para el modo EXEC privilegiado	R1(config)#enable password ciscoenpass
Asignar contraseña "ciscoconpass" de acceso a la consola	R1(config)#line console 0
	R1(config-line)#password ciscoconpass
	R1(config-line)#login
Establecer la longitud mínima 10 caracteres para las contraseñas	R1(config)#security passwords min-length 10
Crear un usuario "admin" administrativo y contraseña "admin1pass" en la base de datos local	R1(config)#username admin password admin1pass
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
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configurar un banner MOTD	R1(config)#banner motd "R1 CARLOS EDUARDO PENA ROJAS INGENIERIA DE SISTEMAS"
Configurar interface G0/0/0	R1(config)#interface g0/0/0
	R1(config-if)#ip address 172.81.3.94 255.255.255.224

	Activar la interfaz. R1(config-if)#no shutdown
Configurar de interface G0/0/1	R1(config)#interface g0/0/1
	IPv4 R1(config-if)#ip address 172.81.3.62 255.255.255.192
	Activar la interfaz. R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R1(config)#crypt key generate rsa 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]
Guardar cambios	R1#cop run star

Fuente: Autor

Tabla 3. Configuración del Switch S1

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Switch	Switch>
Ingresar a modo privilegiado	Switch>enable
Ingresar a modo de configuración	Switch#configure terminal
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombrar Switch S1	Switch(config)#hostname S1
Nombrar dominio ccna-sa.com	S1(config)#ip domain-name ccna-sa.com
Asignar contraseña cifrada "ciscoenpass" para el modo EXEC privilegiado	S1(config)#enable password ciscoenpass

Asignar contraseña "ciscoconpass" de acceso a la consola	S1(config)#line console 0
	S1(config-line)#password ciscoconpass
	S1(config-line)#login
Apagar todos los puertos sin usar	S1(config)#interface range F0/1-4, F0/7-24, G0/1-2
Crear un usuario "admin" administrativo y contraseña "admin1pass" en la base de datos local	S1(config)#username admin password admin1pass
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
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un banner MOTD	S1(config)#banner motd "S1 CARLOS EDUARDO PENA ROJAS INGENIERIA DE SISTEMAS"
Generar una clave de cifrado RSA	S1(config)#crypt key generate rsa 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]
Configurar interfaz de administración (SVI) en la VLAN1	S1(config)#interface vlan1
	S1(config-if)#ip address 172.81.3.94 255.255.255.224
	Activar la interfaz. S1(config-if)#no shutdown
Guardar cambios	S1#cop run star

Fuente: Autor

Configuración de los equipos

Tabla 4. Configuración del equipo PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	FE80::202:16FF:FED3:CE36
Dirección IPv4	172.81.3.10
Máscara de subred	255.255.255.192
Puerta de enlace IPv4 predeterminada	172.81.3.62

Fuente: Autor

Tabla 5. Configuración equipo PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	FE80::201:43FF:FE0E:6378
Dirección IPv4	172.81.3.74
Máscara de subred	255.255.255.224
Puerta de enlace IPv4 predeterminada	172.81.3.94

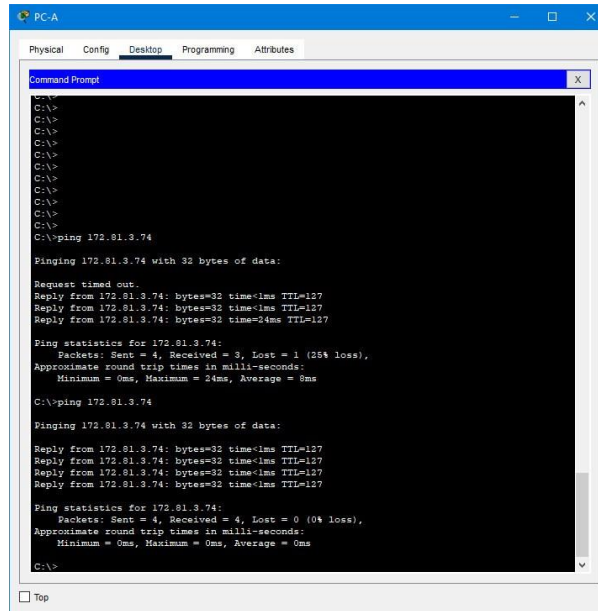
Fuente: Autor

Prueba y verificación de la conectividad de extremo a extremo

Tabla 6. Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
PC-A	R1 G0/0/0	172.81.3.94	Sin pérdida de paquetes.
	R1 G0/0/1	172.81.3.62	Se realiza prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface G0/0/1 del Router R1.
	S1 VLAN 1	172.81.3.2	Se realiza prueba de conectividad con el comando ping sin pérdida de

Figura 5. Conectividad entre PC-A – PC-B



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 172.81.3.74

Pinging 172.81.3.74 with 32 bytes of data:
Request timed out.
Reply from 172.81.3.74: bytes=32 time<1ms TTL=127
Reply from 172.81.3.74: bytes=32 time<1ms TTL=127
Reply from 172.81.3.74: bytes=32 time=24ms TTL=127

Ping statistics for 172.81.3.74:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 0ms

C:\>ping 172.81.3.74

Pinging 172.81.3.74 with 32 bytes of data:
Reply from 172.81.3.74: bytes=32 time<1ms TTL=127
Reply from 172.81.3.74: bytes=32 time<1ms TTL=127
Reply from 172.81.3.74: bytes=32 time<1ms TTL=127
Reply from 172.81.3.74: bytes=32 time<1ms TTL=127

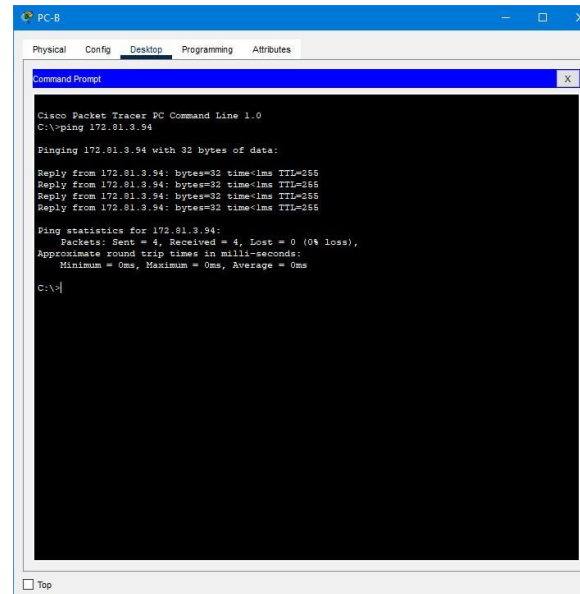
Ping statistics for 172.81.3.74:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la **Figura 5**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A al PC-B.

Figura 6. Conectividad entre PC-B – R1 G0/0/0



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.81.3.94

Pinging 172.81.3.94 with 32 bytes of data:
Reply from 172.81.3.94: bytes=32 time<1ms TTL=255
Reply from 172.81.3.94: bytes=32 time<1ms TTL=255
Reply from 172.81.3.94: bytes=32 time<1ms TTL=255
Reply from 172.81.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.81.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la **Figura 6**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la interface G0/0/0 del Router R1.

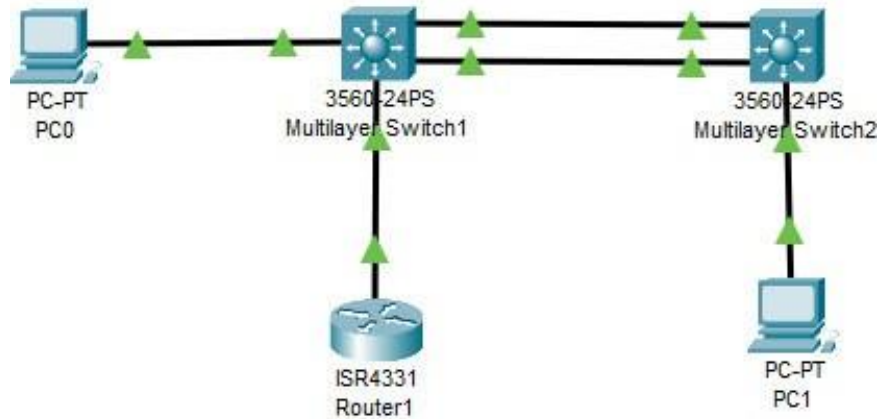
ESCENARIO 2

Construcción de la red

Se realizó la conexión de los dispositivos de una pequeña red.

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

Figura 9. Topología de red escenario No. 2



Fuente: Autor

Tabla 7. Tabla de VLAN

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

Fuente: Autor

Tabla 8. Asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.20	10.81.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.30	10.81.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.40	10.81.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.56	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1/64	No corresponde
S1 VLAN 40	10.81.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 40	10.81.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b::50 /64	fe80::1

Fuente: Autor

Configuración de ajustes básicos

Para el presente ejercicio, se hace necesario la configuración del router que proporcione conectividad a nivel de red en el modelo OSI con el fin de encaminar paquete de datos de una red a otra, la configuración será básica y se inicia con la desactivación del servicio DNS para que más adelante no cause retrasos, luego colocamos el nombre del router y el de dominio, protección por contraseña para proteger el acceso a EXEC privilegiado y así proporcionar seguridad, la contraseña de acceso a la consola la longitud mínima de 5 caracteres, crear un usuario administrativo en la base de datos local para la autenticación.

Así mismo, se configura el inicio de sesión en las líneas VTY para que use la base de datos local, encriptación del mensaje, se establecen las subinterfaces para Ipv4 e Ipv6 y para finalizar se genera una clave de cifrado RSA para encriptar y descifrar datos.

Por consiguiente, en la tabla 9 se pautan los códigos para la configuración del router.

Tabla 9. Configuración del Router R1

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Router	Router>
Ingresar a modo privilegiado	Router>enable
Ingresar a modo de configuración	Router#configure terminal
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup
Nombrar Router R1	Router(config)#hostname R1
Nombrar dominio ccna-sa.com	R1(config)#ip domain-name ccna-sa.com
Asignar contraseña cifrada "class" para el modo EXEC privilegiado	R1(config)#enable password class
Asignar contraseña "cisco" de acceso a la consola	R1(config)#line console 0
	R1(config-line)#password cisco
	R1(config-line)#login
Establecer la longitud mínima 5 caracteres para las contraseñas	R1(config)#security passwords min-length 5
Crear un usuario "admin" administrativo y contraseña "admin1pass" en la base de datos local	R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas	R1(config)#line vty 0 4

VTY para que use la base de datos local	R1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	R1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configurar un banner MOTD	R1(config)#banner motd "R1 CARLOS EDUARDO PENA ROJAS INGENIERIA DE SISTEMAS"
Habilitar el routing IPv6	R1(config)# ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	R1(config)#interface g0/0/1.20
	R1(config-if)# encapsulation dot1q 20
	R1(config-if)# ip address 10.81.8.1 255.255.255.192
	R1(config-if)#ipv6 address 2001:db8:acad:a::1/64
	Activar la interfaz. R1(config-if)#no shutdown
	R1(config)#interface g0/0/1.30
	R1(config-if)# encapsulation dot1q 30
	R1(config-if)# ip address 10.81.8.65 255.255.255.224
	R1(config-if)#ipv6 address 2001:db8:acad:b::1/64
	Activar la interfaz. R1(config-if)#no shutdown
	R1(config)#interface g0/0/1.40
	R1(config-if)# encapsulation dot1q 40
	R1(config-if)# ip address 10.81.8.97 255.255.255.248
	R1(config-if)#ipv6 address 2001:db8:acad:c::1/64
	Activar la interfaz. R1(config-if)#no shutdown
	R1(config-if)#exit
R1(config)# interface g0/0/1	
R1(config-if)# ipv6 address fe80::1 link-local	

	Activar la interfaz. R1(config-if)#no shutdown
Configure el Loopback0 interface	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
	Activar la interfaz. R1(config-if)#no shutdown
Generar una clave de cifrado RSA	R1(config)#crypt key generate rsa RSA The name for the keys will be: R1.ccn- 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]
Guardar cambios	R1#cop run star

Fuente: Autor

Tabla 10. Configuración del Switch S1

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Switch	Switch>
Ingresar a modo privilegiado	Switch>enable
Ingresar a modo de configuración	Switch#configure terminal
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombrar Switch S1	Switch(config)#hostname S1
Nombrar dominio	S1(config)#ip domain-name ccna- sa.com

Contraseña cifrada para el modo EXEC privilegiado	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0
	S1(config-line)#password cisco
	S1(config-line)#login
Crear un usuario administrativo en la base de datos local	S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15
	S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un banner MOTD	S1(config)#banner motd "S1 CARLOS EDUARDO PENA ROJAS INGENIERIA DE SISTEMAS"
Generar una clave de cifrado RSA	S1(config)#crypt key generate rsa 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]
Configurar interfaz de administración (SVI)	S1(config)#sdm prefer dual-ipv4-and-ipv6 default
	S1(config)#end
	S1#reload
	S1(config)#interface vlan40
	S1(config-if)#ip address 10.81.8.98 255.255.255.248

	S1(config-if)#ipv6 address 2001:db8:acad:c: :98 /64
	S1(config-if)# ipv6 address fe80::98 link-local
	S1(config-if)# description Administración Interface
	Activar la interfaz. S1(config-if)#no shutdown
Configuración del gateway predeterminado	S1(config)# ip default-gateway 10.81.8.97

Fuente: Autor

Tabla 11. Configuración del Switch S2

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Switch	Switch>
Ingresar a modo privilegiado	Switch>enable
Ingresar a modo de configuración	Switch#configure terminal
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombrar Switch S1	Switch(config)#hostname S2
Nombrar dominio	S2(config)#ip domain-name ccna- sa.com
Contraseña cifrada para el modo EXEC privilegiado	S2(config)#enable secret class
Contraseña de acceso a la consola	S2(config)#line console 0
	S2(config-line)#password cisco
	S2(config-line)#login
Crear un usuario administrativo en la base de datos local	S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15
	S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S2(config)#service password- encryption

Configurar un banner MOTD	S2(config)#banner motd "S2 CARLOS EDUARDO PENA ROJAS INGENIERIA DE SISTEMAS"
Generar una clave de cifrado RSA	S2(config)#crypt key generate rsa 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]
Configurar interfaz de administración (SVI)	S2(config)#sdm prefer dual-ipv4-and-ipv6 default
	S2(config)#end
	S1#reload
	S1(config)#interface vlan40
	S1(config-if)#ip address 10.81.8.99 255.255.255.248
	S1(config-if)#ipv6 address 2001:db8:acad:c: :99/64
	S1(config-if)# ipv6 address fe80::99 link-local
	S1(config-if)# description Administración Interface
Activar la interfaz. S1(config-if)#no shutdown	
Configuración del gateway predeterminado	S1(config)# ip default-gateway 10.81.8.97

Fuente: Autor

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

Tabla 12. Configuración S1

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Switch	S1>
Ingresar a modo privilegiado	S1>enable
Ingresar a modo de configuración	S1#configure terminal
Crear VLAN	S1(config)#vlan 20 name Docentes
	S1(config)#vlan 30 name Estudiantes
	S1(config)#vlan 40 name Invitados
	S1(config)#vlan 50 name Usuarios
	S1(config)#vlan 56 name Native
Crear troncos 802.1Q que utilicen la VLAN 56 native	S1(config)# interface f0/5
	S1(config-if)# switchport trunk encapsulation dot1q
	S1(config-if)# switchport mode trunk
	S1(config-if)# switchport trunk native vlan 56
	S1(config)# interface range f0/1-2
	S1(config-if-range)# shutdown
	S1(config-if-range)# switchport trunk encapsulation dot1q
	S1(config-if-range)# switchport mode trunk
	S1(config-if-range)# switchport trunk native vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1(config)#interface range f0/1-2
	S1(config-if-range)#channel-group 1 mode active
	S1(config-if-range)#interface port-channel 1
	S1(config-if)# switchport trunk

	encapsulation dot1q
	S1(config-if)# switchport mode trunk
	S1(config-if)# switchport trunk native vlan 56
Configurar el puerto de acceso de host para VLAN 20	S1(config)#interface f0/6
	S1(config-if)# switchport mode access
	S1(config-if)# switchport access vlan 20
Configurar la seguridad del puerto en los puertos de acceso	S1(config-if)# switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	S1(config-if)#int range f0/3-4
	S1(config-if-range)#switchport mode access
	S1(config-if-range)#switchport access vlan 56
	S1(config-if-range)#description FUERA DE SERVICIOS
	S1(config-if-range)#shutdown
	S1(config-if-range)#interface range f0/7-24
	S1(config-if-range)#switchport mode access
	S1(config-if-range)#switchport access vlan 56
	S1(config-if-range)#description FUERA DE SERVICIOS
	S1(config-if-range)#shutdown
	S1(config-if-range)#interface range g0/1-2
	S2(config-if-range)#switchport mode Access
	S1(config-if-range)#switchport access vlan 56
	S1(config-if-range)#description FUERA DE SERVICIOS
	S1(config-if-range)#shutdown
S1(config-if-range)#	

Fuente: Autor

Tabla 13. Configuración S2

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del Switch	S2>
Ingresar a modo privilegiado	S2>enable
Ingresar a modo de configuración	S2#configure terminal
Crear VLAN	S2(config)#vlan 20 name Docentes
	S2(config)#vlan 30 name Estudiantes
	S2(config)#vlan 40 name Invitados
	S2(config)#vlan 50 name Usuarios
	S2(config)#vlan 56 name Native
Crear troncos 802.1Q que utilicen la VLAN 56 native	S2(config)# interface f0/1-2
	S2(config-if)#shutdown
	S2(config-if)# switchport trunk encapsulation dot1q
	S2(config-if)# switchport mode trunk
	S2(config-if)# switchport trunk native vlan 56
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface range f0/1-2
	S2(config-if-range)#channel-group 1 mode active
	S2(config-if-range)#interface port-channel 1
	S2(config-if)# switchport trunk encapsulation dot1q
	S2(config-if)# switchport mode trunk
	S2(config-if)# switchport trunk native vlan 56
Configurar el puerto de acceso de host para VLAN 20	S2(config)#interface f0/18
	S2(config-if)# switchport mode access
	S2(config-if)# switchport access vlan 30

Configurar la seguridad del puerto en los puertos de acceso	S2(config-if)# switchport port-security maximum 4
Proteja todas las interfaces no utilizadas	S2(config-if)#interface range f0/3-17
	S2(config-if-range)#switchport mode access
	S2(config-if-range)#switchport access vlan 56
	S2(config-if-range)#description FUERA DE SERVICIOS
	S2(config-if-range)#shutdown
	S2(config-if-range)#interface range f0/19-24
	S2(config-if-range)#switchport mode access
	S2(config-if-range)#switchport access vlan 56
	S2(config-if-range)#description FUERA DE SERVICIOS
	S2(config-if-range)#shutdown
	S2(config-if-range)#interface range g0/1-2
	S2(config-if-range)#switchport mode Access
	S2(config-if-range)#switchport access vlan 56
	S2(config-if-range)#description FUERA DE SERVICIOS
	S2(config-if-range)#shutdown
S2(config-if-range)#	

Fuente: Autor

Configuración soporte de host

Tabla 14. Configuración R1

TAREA	ESPECIFICACIÓN
Ingresar a la configuración del router	R1>
Ingresar a modo privilegiado	R1>enable

Ingresar a modo de configuración	R1#configure terminal
Configure Default Routing	R1(config)# ip route 0.0.0.0 0.0.0.0 loopback 0
	R1(config)#ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 20	R1(config)#ip dhcp excluded-address 10.81.8.3 10.81.8.52
	R1(config)# ip dhcp pool vlan20- Docentes
	R1(config)# network 10.81.8.0 255.255.255.192
	R1(config)#default-router 10.81.8.1
	R1(config)# domain-name unad-ccna- a.net
Configurar IPv4 DHCP para VLAN 30	R1(config)#ip dhcp excluded-address 10.81.8.67 10.81.8.84
	R1(config)# ip dhcp pool vlan30- Estudiantes
	R1(config)#network 10.81.8.64 255.255.255.224
	R1(config)#default-router 10.81.8.65
	R1(config)# domain-name unad-ccna- sb.net

Fuente: Autor

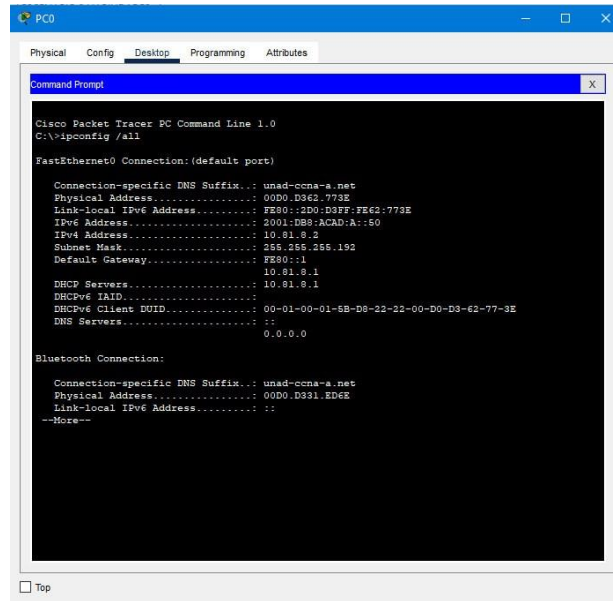
Configuración de los servidores

Tabla 15. Configuración del equipo PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	FE80::2D0:D3FF:FE62:773E
Dirección IP	10.81.8.2
Máscara de subred	255.255.255.192
Gateway predeterminado	10.81.8.1
Gateway predeterminado IPv6	fe80::1

Fuente: Autor

Figura 10. Configuración PC-A



Fuente: Autor

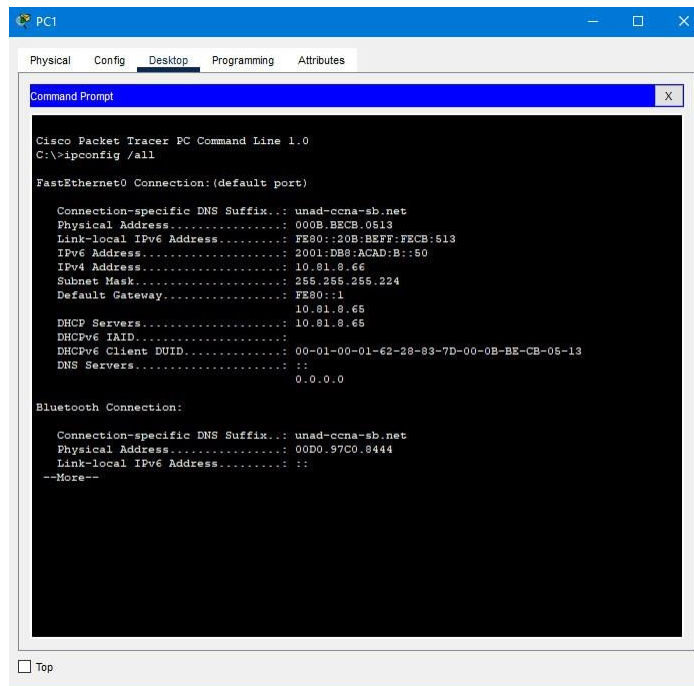
En la **Figura 10**. Se evidencia por medio del comando ipconfig /all la configuración registrada para el servidor nombrado PC-A.

Tabla 16. Configuración equipo PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	FE80::20B:BEFF:FECB:513
Dirección IP	10.81.8.66
Máscara de subred	255.255.255.224
Gateway predeterminado	10.81.8.65
Gateway predeterminado IPv6	fe80::1

Fuente: Autor

Figura 11. Configuración PC-B



Fuente: Autor

En la **Figura 11**. Se evidencia por medio del comando ipconfig /all la configuración registrada para el servidor nombrado PC-B.

Prueba y verificación de la conectividad de extremo a extremo

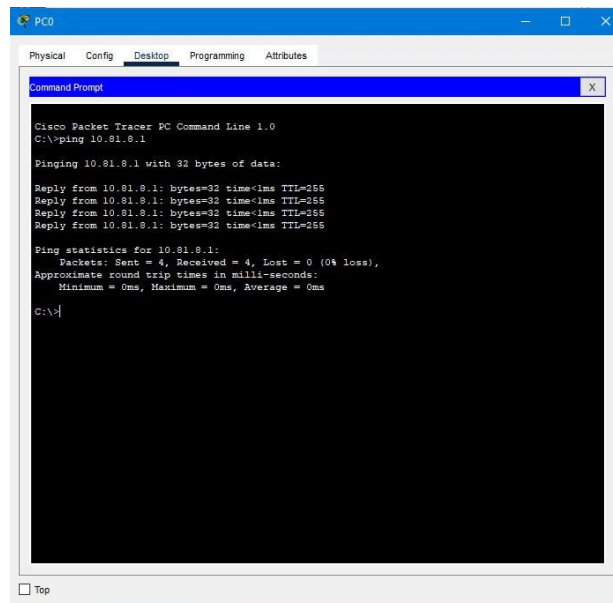
Tabla 17. Pruebas de conectividad

Desde	A		Dirección IP	Resultados de ping
PC-A	R1 G0/0/1.20	IPv4	10.81.8.1	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:a::1	Sin pérdida de paquetes.
	R1 G0/0/1.30	IPv4	10.81.8.65	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:b::1	Sin pérdida de paquetes.
	R1 G0/0/1.40	IPv4	10.81.8.97	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:c::1	Sin pérdida de paquetes.
S1 VLAN 40	IPv4	10.81.8.98	Sin pérdida de	

				paquetes.
		IPv6	2001:db8:acad:c::98	Sin pérdida de paquetes.
	S2 VLAN 40	IPv4	10.81.8.99	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:c: :99	Sin pérdida de paquetes.
	PC-B	IPv4	10.81.8.66	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:b::50	Sin pérdida de paquetes.
	R1 Bucle 0	IPv4	209.165.201.1	Sin pérdida de paquetes.
IPv6		2001:db8:acad:209::1	Sin pérdida de paquetes.	
PC-B	R1 Bucle 0	IPv4	209.165.201.1	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:209::1	Sin pérdida de paquetes.
	R1 G0/0/1.20	IPv4	10.81.8.1	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:a::1	Sin pérdida de paquetes.
	R1 G0/0/1.30	IPv4	10.81.8.65	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:b::1	Sin pérdida de paquetes.
	R1 G0/0/1.40	IPv4	10.81.8.97	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:c::1	Sin pérdida de paquetes.
	S1 VLAN 40	IPv4	10.81.8.98	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:c::98	Sin pérdida de paquetes.
	S2 VLAN 40	IPv4	10.81.8.99	Sin pérdida de paquetes.
		IPv6	2001:db8:acad:c: :99	Sin pérdida de paquetes.

Fuente: Autor

Figura 12. Conectividad entre PC-A – R1 G0/0/1.20 IPv4



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.81.8.1

Pinging 10.81.8.1 with 32 bytes of data:

Reply from 10.81.8.1: bytes=32 time<1ms TTL=255
Reply from 10.81.8.1: bytes=32 time<1ms TTL=255
Reply from 10.81.8.1: bytes=32 time<1ms TTL=255
Reply from 10.81.8.1: bytes=32 time<1ms TTL=255

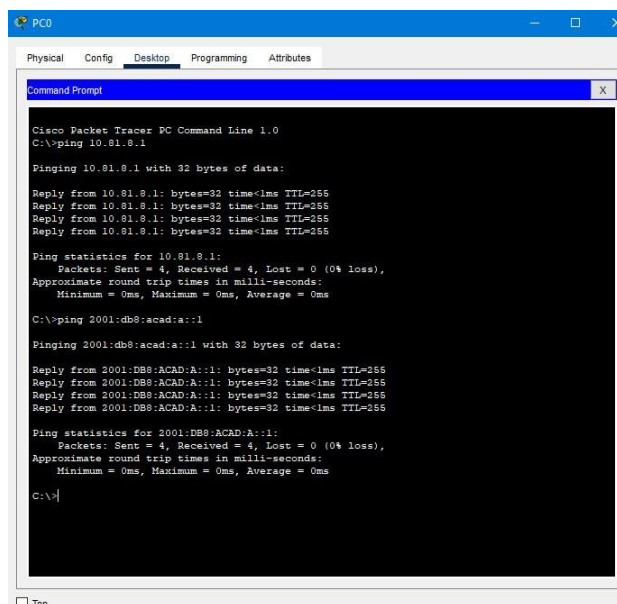
Ping statistics for 10.81.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la **Figura 12**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface R1 G0/0/1.20 a la dirección IPv4 10.81.8.1.

Figura 13. Conectividad entre PC-A – R1 G0/0/1.20 IPv6



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.81.8.1

Pinging 10.81.8.1 with 32 bytes of data:

Reply from 10.81.8.1: bytes=32 time<1ms TTL=255
Reply from 10.81.8.1: bytes=32 time<1ms TTL=255
Reply from 10.81.8.1: bytes=32 time<1ms TTL=255
Reply from 10.81.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.81.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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<1ms 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

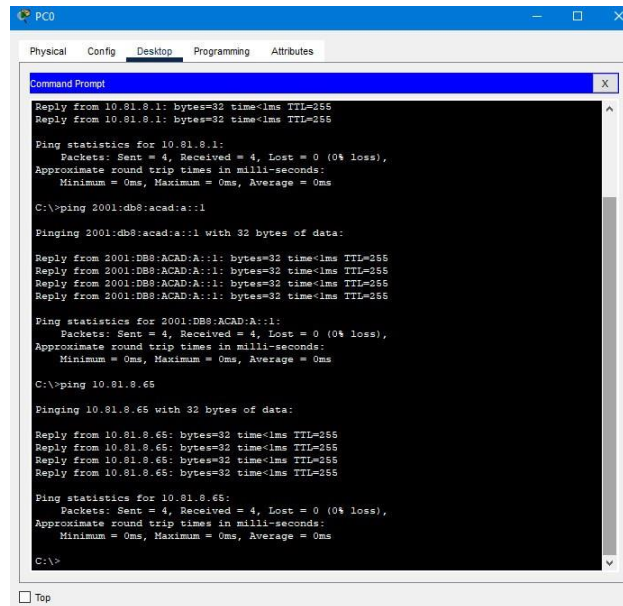
Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Autor

En la **Figura 13**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface R1 G0/0/1.20 a la dirección IPv6 2001:db8:acad:a::1.

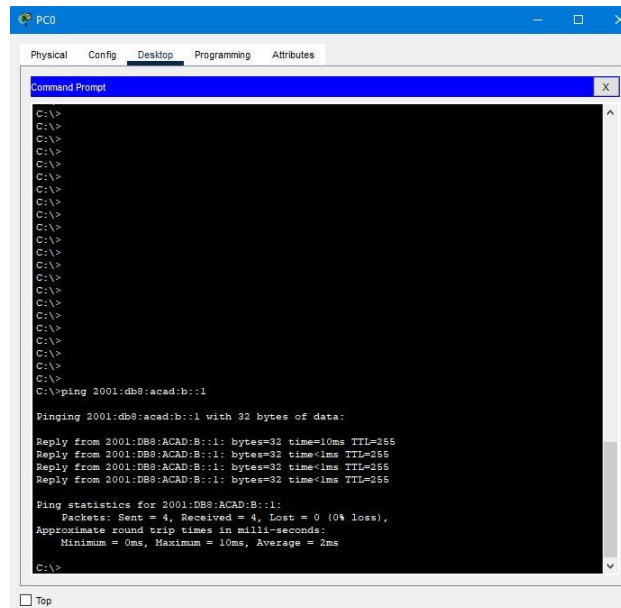
Figura 14. Conectividad entre PC-A – R1 G0/0/1.30 IPv4



Fuente: Autor

En la **Figura 14**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface R1 G0/0/1.30 a la dirección IPv4 10.81.8.65.

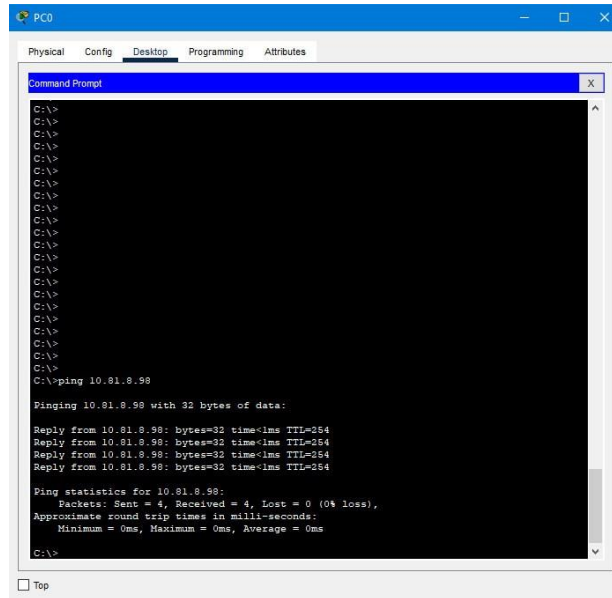
Figura 15. Conectividad entre PC-A – R1 G0/0/1.30 IPv6



Fuente: Autor

En la **Figura 15**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface R1 G0/0/1.30 a la dirección IPv6 2001:db8:acad:b:1.

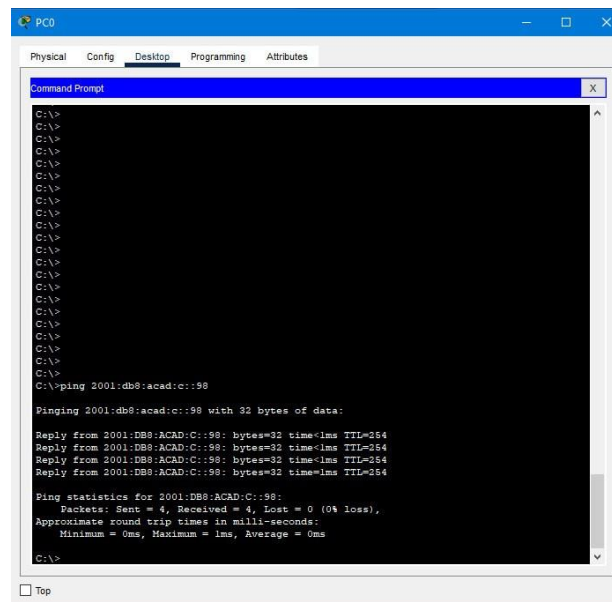
Figura 18. Conectividad entre PC-A – S1 VLAN 40 IPv4



Fuente: Autor

En la **Figura 18**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface S1 VLAN 40 a la dirección IPv4 10.81.8.98.

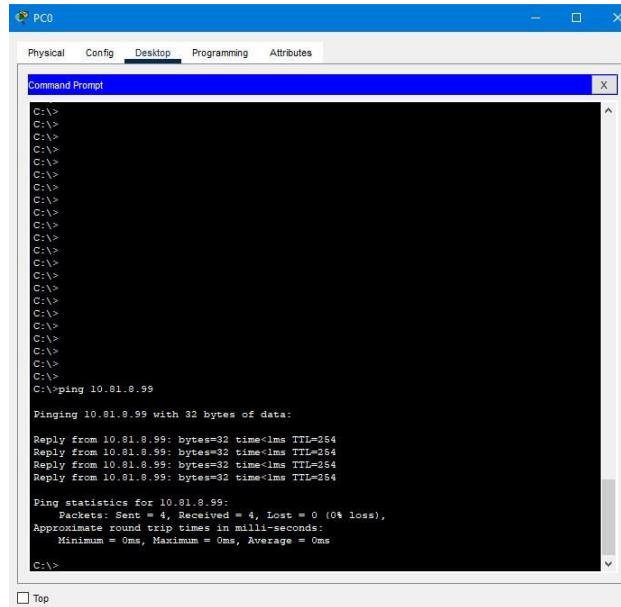
Figura 19. Conectividad entre PC-A – S1 VLAN 40 IPv6



Fuente: Autor

En la **Figura 19**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface S1 VLAN 40 a la dirección IPv6 2001:db8:acad:c::98.

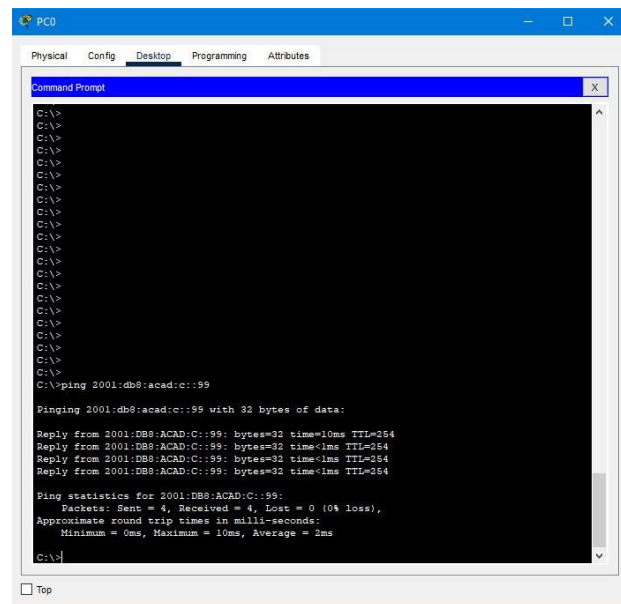
Figura 20. Conectividad entre PC-A – S2 VLAN 40 IPv4



Fuente: Autor

En la **Figura 20**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface S2 VLAN 40 a la dirección IPv4 10.81.8.99.

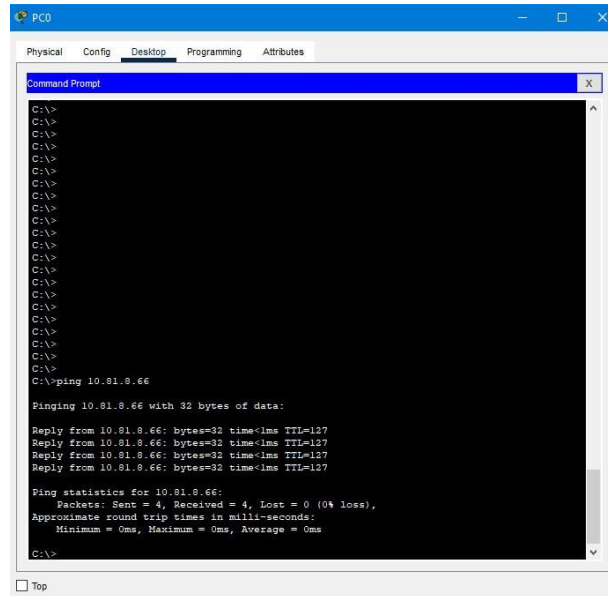
Figura 21. Conectividad entre PC-A – S2 VLAN 40 IPv6



Fuente: Autor

En la **Figura 21**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la interface S2 VLAN 40 a la dirección IPv6 2001:db8:acad:c: :99.

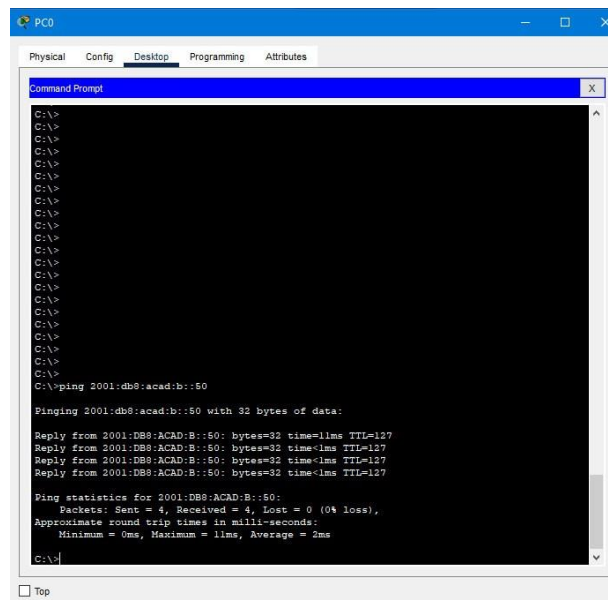
Figura 22. Conectividad entre PC-A – PC-B IPv4



Fuente: Autor

En la **Figura 22**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la dirección IPv4 10.81.8.66 del PC-B.

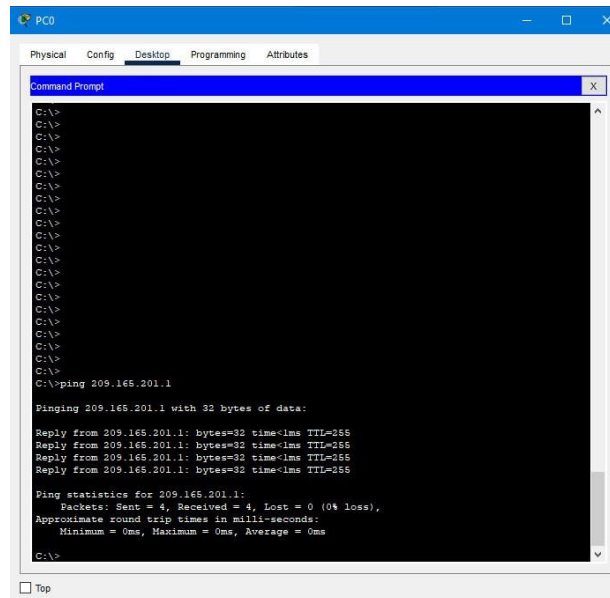
Figura 23. Conectividad entre PC-A – PC-B IPv6



Fuente: Autor

En la **Figura 23**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la dirección IPv6 2001:db8:acad:b::50 del PC-B.

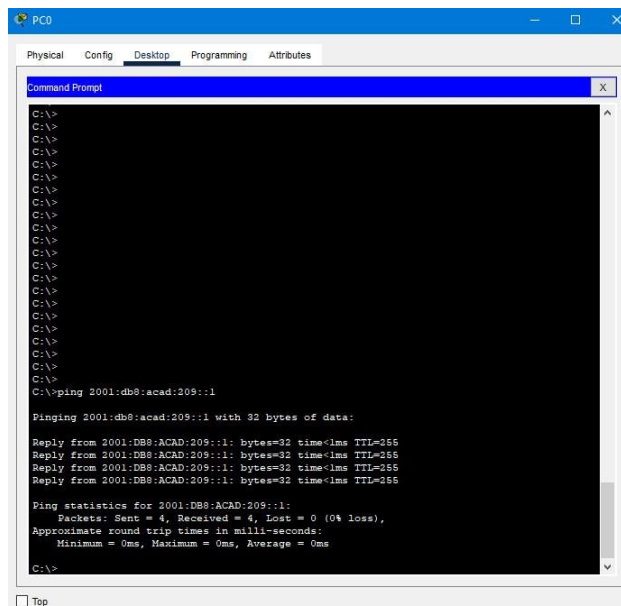
Figura 24. Conectividad entre PC-A – R1 Bucle 0 IPv4



Fuente: Autor

En la **Figura 24**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la dirección IPv4 209.165.201.1 del dispositivo R1 Bucle 0.

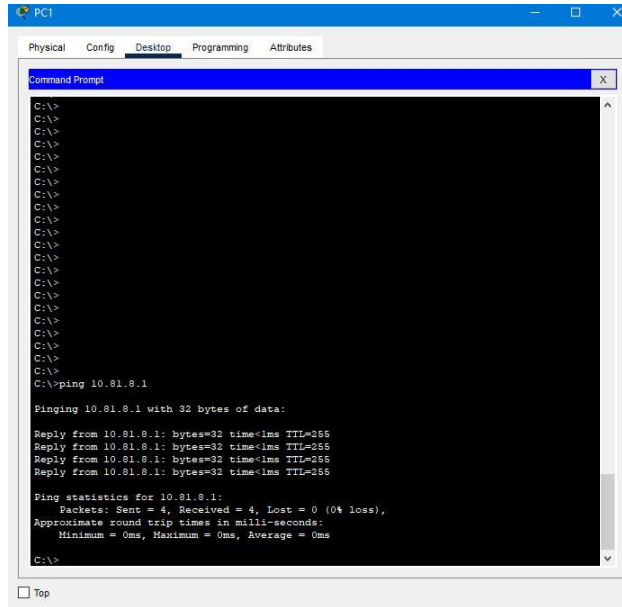
Figura 25. Conectividad entre PC-A – R1 Bucle 0 IPv6



Fuente: Autor

En la **Figura 25**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-A a la dirección IPv6 2001:db8:acad:209::1 del dispositivo R1 Bucle 0.

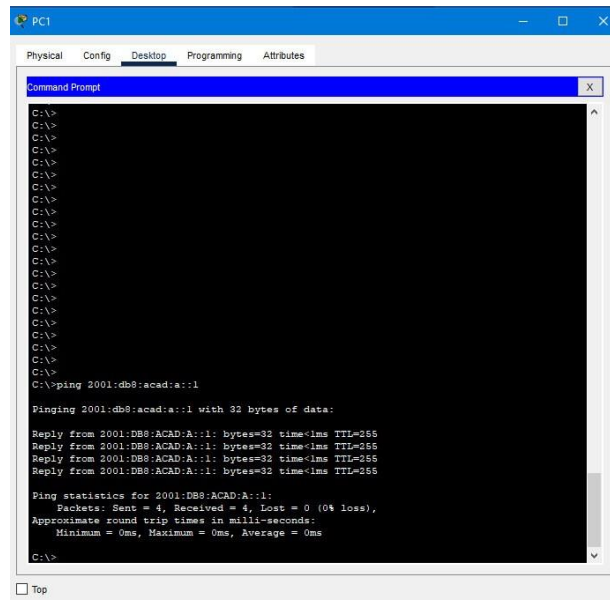
Figura 28. Conectividad entre PC-B – R1 G0/0/1.20 IPv4



Fuente: Autor

En la **Figura 28**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv4 10.81.8.1 de la interfaz R1 G0/0/1.20.

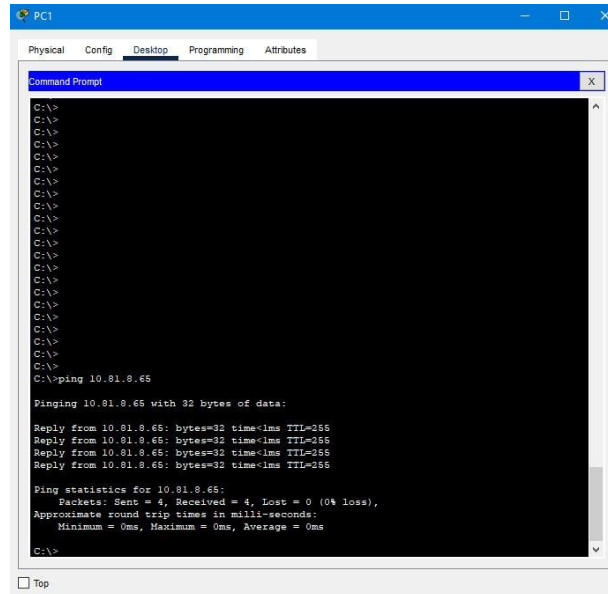
Figura 29. Conectividad entre PC-B – R1 G0/0/1.20 IPv6



Fuente: Autor

En la **Figura 29**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv6 2001:db8:acad:a::1 de la interfaz R1 G0/0/1.20.

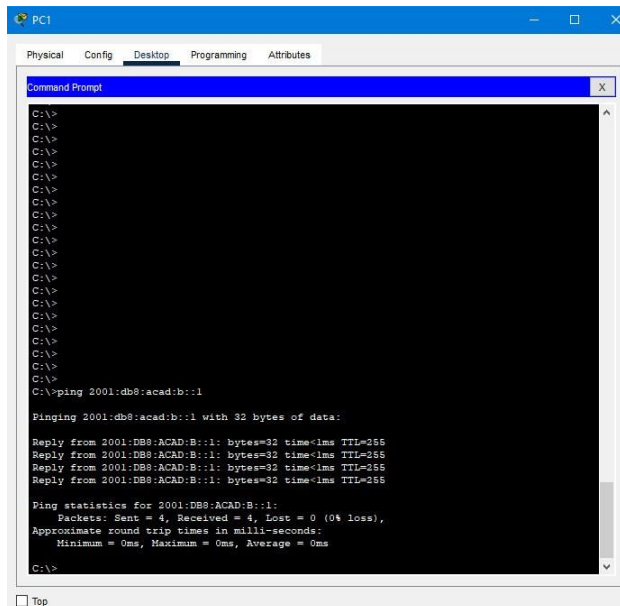
Figura 30. Conectividad entre PC-B – R1 G0/0/1.30 IPv4



Fuente: Autor

En la **Figura 30**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv4 10.81.8.65 de la interfaz R1 G0/0/1.30.

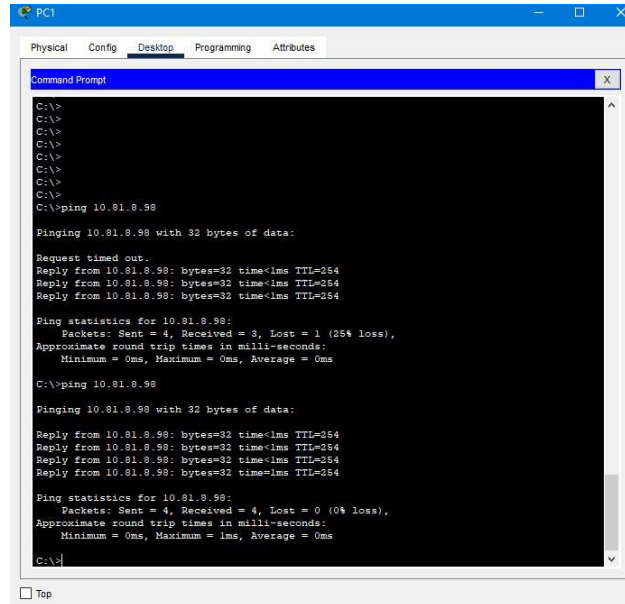
Figura 31. Conectividad entre PC-B – R1 G0/0/1.30 IPv6



Fuente: Autor

En la **Figura 31**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv6 2001:db8:acad:b::1 de la interfaz R1 G0/0/1.30.

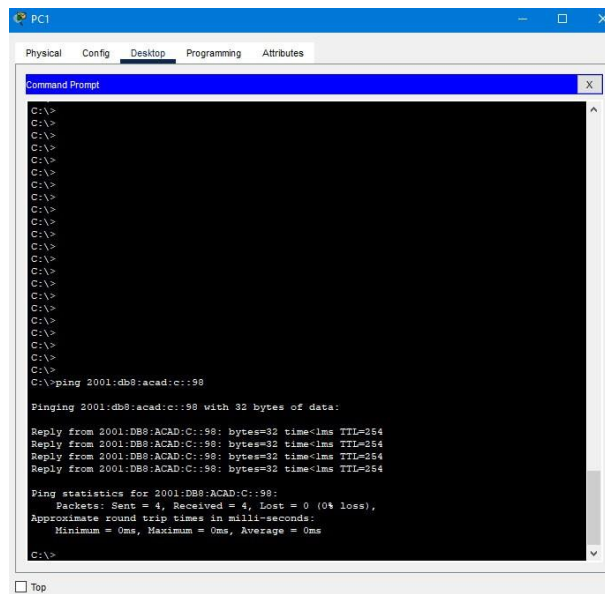
Figura 34. Conectividad entre PC-B – S1 VLAN 40 IPv4



Fuente: Autor

En la **Figura 34**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv4 10.81.8.98 de la interfaz S1 VLAN 40.

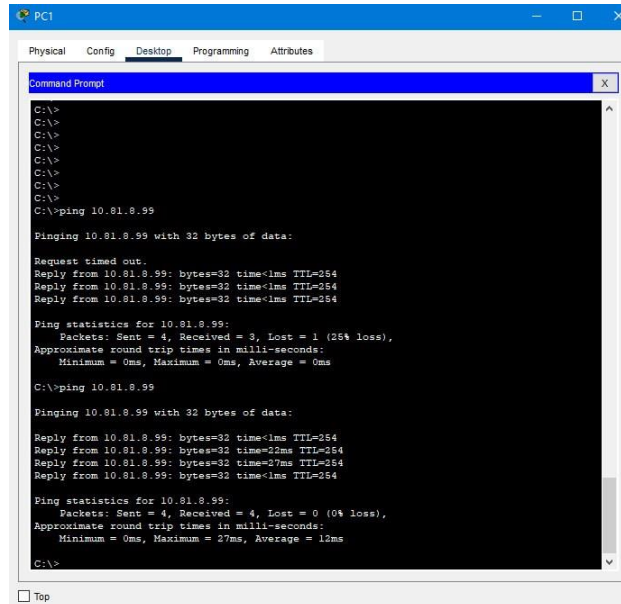
Figura 35. Conectividad entre PC-B – S1 VLAN 40 IPv6



Fuente: Autor

En la **Figura 35**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv6 2001:db8:acad:c::98 de la interfaz S1 VLAN 40.

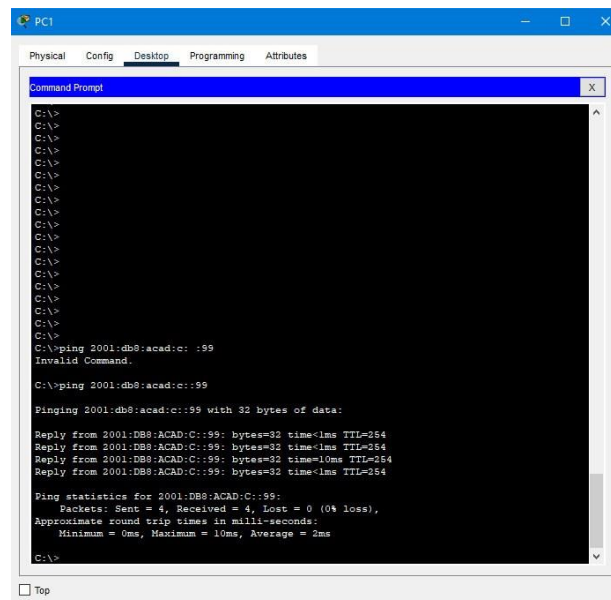
Figura 36. Conectividad entre PC-B – S2 VLAN 40 IPv4



Fuente: Autor

En la **Figura 36**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv4 10.81.8.99 de la interfaz S2 VLAN 40.

Figura 37. Conectividad entre PC-B – S2 VLAN 40 IPv6



Fuente: Autor

En la **Figura 37**. Se evidencia la prueba de conectividad con el comando ping sin pérdida de paquetes desde el PC-B a la dirección IPv6 2001:db8:acad:c::99 de la interfaz S2 VLAN 40.

CONCLUSIONES

Culminado el informe, es deducible que todos parámetros para la implementación y estructuración de una red son relativamente importantes, dado que estas deben cumplir con las normas establecidas, de lo contrario no tendrían comunicación alguna entre un equipo y otro, es por eso que el direccionamiento VLSM y enrutamiento estático son técnicas imperiosas, las cuales permiten administrar las redes eficientemente, toda vez que a la hora de dividir las se aprovechan al máximo de las mismas, desperdiciando en lo menos posible, adicional a esto la implementación de VLSM maximiza la eficiencia del direccionamiento y a su vez se le conoce como división de subredes en subredes, por otra parte el manejo de las direcciones IP facilita la identificación de los periféricos que hacen uso de una dirección de manera estática, igual que conocer a que grupo de trabajo pertenece una red, por lo anterior es importante tener los conocimientos claros acerca de las direcciones IP y cuál es su funcionamiento, lo que ayudará a decidir qué tipo o clase de direccionamiento IP debemos utilizar de acuerdo a nuestras necesidades ya sea en el hogar, empresa pública o privada.

Además, exponiendo las experiencias obtenidas en la práctica y desarrollo de cada uno de los escenarios, a los cuales no se les puede quitar lo realmente importante como lo son la configuración de los servidores ya sean remotos y/o locales mediante los protocolos de seguridad SSH, como también la conexión física entre las interfaces lógicas y las asignaciones de los mecanismos de seguridad entre esos la asignación de contraseñas de acceso a los dispositivos y poder evitar que a estos accedan personas no autorizadas que pueda vulnerar o distorsionar el correcto funcionamiento de la red.

Por otra parte, quiero mencionar que algo de contexto para tener una idea clara de lo estudiando en este documento, mencionando que las redes pequeñas se convierten en una herramienta para compartir recursos, asegurar la confiabilidad y disponibilidad de la información, reducir costos de las acciones. Por otra parte, la facilidad para acceder a documentos alojados en cualquier nodo de la red, es muy útil a la hora de realizar un trabajo en conjunto. Todo esto mejora el trabajo en equipo y la participación de todas los integrantes en determinada empresa.

En los dos casos se diferenciaron algunos temas como el etherchannel que fue muy práctico en el segundo caso y este hace como una especie de retorno entre los dos switch interconectados por puertos diferentes entre el uno y el otro, son temas de investigación, pero interesantes a la hora de administrar las redes y contar con estas tecnologías, además de las direcciones IPv6 que son muy útiles con su capacidad amplia de direccionar las IPv6 en los equipos designados para determinada red.

Para finalizar, es preciso indicar que se necesitan responsables del manejo de la red en caso de fallas y sobre todo para el mantenimiento de los dispositivos, esto requiere un mejor conocimiento y la responsabilidad estaría en las personas con más capacidades para cada una las necesidades que requiera el manejo de redes pequeña.

BIBLIOGRAFÍA

Ariganello, E. (2016). REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 159 – 165.

https://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2498326&lang=es&site=ehost-live&ebv=EB&ppid=pp_159

Castaño, R. R. J., y López, F. J. (2013). Redes locales. 192 - 199.

<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=193>

A. S. Tanenbaum, Redes de Computadoras, Editorial Prentice Hall, tercera edición, 1997. Recuperado de : https://www.academia.edu/25306593/Redes_de_Computadoras_3ra_Edici%C3%B3n_Andrew_S_Tanenbaum_F REELIBROS_ORG

GARIMELLA, Prashant, et al. Characterizing VLAN usage in an operational network. En Proceedings of the 2007 SIGCOMM workshop on Internet network management. 2007. p. 305-306.

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

Anexo A – Enlace de descarga de los archivos de simulación

Enlace : https://drive.google.com/drive/folders/1F-sfvqay32nM3lvjNHMBgylgLcyzG_me?usp=share_link