

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

DICXON ENRIQUE CONTRERAS SALCEDO

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

INGENIERÍA DE SISTEMAS

PAMPLONA

2022

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

DICXON ENRIQUE CONTRERAS SALCEDO

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

DIRECTOR:
PAULITA FLOR

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

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Pamplona, 22 de noviembre de 2022

AGRADECIMIENTOS

Doy Gracias a Dios, a mi familia a mi esposa, hijas y a cada uno de los tutores que me apoyaron durante estos años para alcanzar mi meta de ser ingeniero de sistemas, ha sido un largo y difícil camino pero al llegar a la meta se logra divisar que todo este esfuerzo ha valido la pena, poder colocar en práctica los conocimientos adquiridos y la satisfacción de lograr ser Ingeniero de Sistemas y ser un ejemplo para mis hijas Natalia y Emily de que se pueden alcanzar esas metas que nos ponemos en la vida.

CONTENIDO

| | |
|---|----|
| CONTENIDO..... | 5 |
| LISTA DE TABLAS..... | 7 |
| LISTA DE FIGURAS | 8 |
| LISTA DE ANEXOS | 10 |
| GLOSARIO..... | 11 |
| RESUMEN | 13 |
| ABSTRACT | 14 |
| Keywords: IP address, IPV4, IPV6; Tunk, Gateway, Network, Router, Switch... | 14 |
| INTRODUCCIÓN | 15 |
| DESARROLLO ESCENARIO 1..... | 16 |
| Paso 1: configurar los ajustes básicos..... | 18 |
| Parte 3: Probar y verificar la conectividad de extremo a extremo..... | 25 |
| Desarrollo Escenario 2 | 31 |
| Instrucciones | 34 |
| Paso 2: Configurar R1 Escenario 2..... | 36 |
| Paso 3: Configure S1 y S2 Escenario 2 | 40 |
| Configurar los servidores Escenario 2..... | 59 |
| Probar y verificar la conectividad de extremo a extremo | 61 |

| | |
|--------------------|----|
| CONCLUSIONES..... | 77 |
| BIBLIOGRAFÍA | 78 |
| ANEXOS | 82 |

LISTA DE TABLAS

| | |
|--|----|
| Tabla 1 Configuración Router Escenario 1 | 18 |
| Tabla 2 Configuración Switch 1 Escenario 1 | 21 |
| Tabla 3 Configuración PC-A 1 Escenario | 24 |
| Tabla 4 Configuración PC-B 1 Escenario | 24 |
| Tabla 5 Verificación de los dispositivos de red | 25 |
| Tabla 6 VLAN Escenario 2 | 32 |
| Tabla 7 Asignación de direcciones | 33 |
| Tabla 8 Inicialización y carga del Router | 35 |
| Tabla 9 Inicialización y carga del Switch 1 y 2 | 35 |
| Tabla 10 Configuración de plantilla SDM en Switch 1 y 2 | 36 |
| Tabla 11 Configuración del Router | 36 |
| Tabla 12 configuración del Switch 1 | 40 |
| Tabla 13 Configuración del Switch 2 | 43 |
| Tabla 14 Configuración S1 VLAN, Trunking, EtherChannel | 45 |
| Tabla 15 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 2 | 51 |
| Tabla 16 Activación interface fa0/1-2 en s1 y S2 | 56 |
| Tabla 17 Configuración de soporte de host en Router | 56 |
| Tabla 18 Configuración de red del PC-A | 59 |
| Tabla 19 Configuración de red del PC-A | 60 |
| Tabla 20 Verificación de los dispositivos de red | 62 |

LISTA DE FIGURAS

| | |
|--|----|
| Figura 1 Topología Escenario 1 | 16 |
| Figura 2 Simulación Escenario 1 en Packet Tracer..... | 16 |
| Figura 3 Prueba desde PC-A a R1 G0/0/0 | 26 |
| Figura 4 Prueba desde PC-A a R1 G0/0/1 | 27 |
| Figura 5 Prueba desde PC-A a S1 | 27 |
| Figura 6 Prueba desde PC-A a PC-B..... | 28 |
| Figura 7 Prueba desde PC-B a R1 G0/0/0 | 28 |
| Figura 8 Prueba desde PC-B a R1 G0/0/1 | 29 |
| Figura 9 Prueba desde PC-B a S1 | 29 |
| Figura 10 Prueba desde PC-B a PC-A..... | 30 |
| Figura 11 Topología Escenario 2 | 31 |
| Figura 12 Simulación Escenario 2 en Packet Tracer..... | 32 |
| Figura 13 Verificación configuración VLAN S1 | 49 |
| Figura 14 Verificación Configuración trunk S1 | 49 |
| Figura 15 Verificación Configuración EtherChannel S1 | 50 |
| Figura 16 Verificación Configuración VLAN Brief..... | 50 |
| Figura 17 Verificación Configuración VLAN S2..... | 54 |
| Figura 18 Verificación Configuración trunk S2 | 54 |
| Figura 19 Verificación Configuración EtherChannel S2 | 55 |
| Figura 20 Verificación Configuración VLAN Brief..... | 55 |
| Figura 21 Verificación Configuración R1 | 59 |
| Figura 22 Verificación Configuración PC-A..... | 60 |
| Figura 23 Verificación Configuración PC-B..... | 61 |
| Figura 24 Ping desde PC-A a R1, G0/0/1.2 – Ipv4 10.64.8.1 | 63 |
| Figura 25 Ping desde PC-A a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a :1 | 64 |
| Figura 26 Ping desde PC-A a R1, G0/0/1.3 – Ipv4 10.64.8.65 | 64 |
| Figura 27 Ping desde PC-A a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b :1 | 65 |

| | |
|---|----|
| Figura 28 Ping desde PC-A a R1, G0/0/1.4 – Ipv4 10.64.8.97 | 65 |
| Figura 29 Ping desde PC-A a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c: :1 | 66 |
| Figura 30 Ping desde PC-A a S1 VLAN4 – Ipv4 10.64.8.98 | 66 |
| Figura 31 Ping desde PC-A a S1 VLAN40 – Ipv6 2001:db8:acad:c: :1 | 67 |
| Figura 32 Ping desde PC-A a S2 VLAN4 – Ipv4 10.64.8.99 | 67 |
| Figura 33 Ping desde PC-A a S2 VLAN4 – Ipv6 2001:db8:acad:c: :1 | 68 |
| Figura 34 Ping desde PC-A a PC-B – Ipv4 10.64.8.85..... | 68 |
| Figura 35 Ping desde PC-A a PC-B – Ipv6 2001:db8:acad:b: :50..... | 69 |
| Figura 36 Ping desde PC-A a R1 Bucle 0 – IPv4 209.165.201.1 | 69 |
| Figura 37 Ping desde PC-A a R1 Bucle 0 – Ipv6 2001:db8:acad:209: :1 | 70 |
| Figura 38 Ping desde PC-B a R1 Bucle 0 – Ipv4 209.165.201.1..... | 70 |
| Figura 39 Ping desde PC-B a R1 Bucle 0 – Ipv6 2001:db8:acad:209: :1 | 71 |
| Figura 40 Ping desde PC-B a R1, G0/0/1.2 – Ipv4 10.64.8.1..... | 71 |
| Figura 41 Ping desde PC-B a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a: :1 | 72 |
| Figura 42 Ping desde PC-B a R1, G0/0/1.3 – Ipv4 10.64.8.65..... | 72 |
| Figura 43 Ping desde PC-B a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b: :1 | 73 |
| Figura 44 Ping desde PC-B a R1, G0/0/1.4 – Ipv4 10.64.8.97 | 73 |
| Figura 45 Ping desde PC-B a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c: :1 | 74 |
| Figura 46 Ping desde PC-B a S1 VLAN4 – Ipv4 10.64.8.98 | 74 |
| Figura 47 Ping desde PC-B a S1 VLAN4 – Ipv6 2001:db8:acad:c: :98..... | 75 |
| Figura 48 Ping desde PC-B a S2 VLAN40 – Ipv4 10.64.8.99 | 75 |
| Figura 49 Ping desde PC-B a S2 VLAN40 – Ipv6 2001:db8:acad:c: :99..... | 76 |

LISTA DE ANEXOS

| | |
|--|----|
| Anexo A. Link de descarga Escenario 1, archivo ptk | 82 |
| Anexo B. Link de descarga Escenario 2, archivo ptk | 82 |

GLOSARIO

PROTOCOLO: ¹un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información

VLAN: ²Red virtual, es un método para crear redes lógicas independientes dentro de una misma red física

ROUTER³: El Router o enrutador es un dispositivo conectado, por lo menos a dos redes y decide hacia donde se dirige cada paquete de información conforme a lo que hallamos configurado.

DHCP⁴: Protocolo Cliente/Servidor que proporciona a un equipo o host su dirección IP o alguna otra información necesaria para la configuración, como lo son puerta de enlace, máscara de red.

BANNER MOTD⁵: Comando que muestra un mensaje, por ejemplo, un error de conexión,

ETHERCHANNEL⁶: Tecnología de agregación de enlaces de puertos desarrollada por Cisco, estos enlaces de alta velocidad son tolerantes a fallas entre servidores, conmutadores y enrutadores. El EtherChannel permite que varios enlaces Ethernet físicos (Fast Ethernet o Gigabit Ethernet) se combinen en un canal lógico.

¹ Cisco, Protocolos y modelos. Introducción a las redes, 2020

² Cisco, las redes en la actualidad, Introducción a las redes, 2020.

³ Cisco, Configuración básica de un Router. Introducción a las redes, 2020.

⁴ Cisco, Fundamentos de seguridad de la red. Introducción a las redes, 2020.

⁵ JI Cuesta Vargas - repositorio.unad.edu.co

⁶ Cisco, Capa de red, Introducción a las redes, 2020.

GATEWAY⁷: Un Gateway (puerta de enlace) es un dispositivo, que permite interconectar redes usando diferentes protocolos y arquitecturas con varios niveles de comunicación. Su propósito es traducir los datos hacia la red de destino.

NVRAM⁸: La NVRAM o “Non-Volatile Random Access Memory”, es una memoria de acceso aleatorio no volátil capaz de almacenar información que no desaparece al tener una falla eléctrica.

PORT-SECURITY⁹: Es una característica que poseen los switches Cisco para almacenar las direcciones MAC conectadas en cada uno de los puertos del dispositivo y permitir que solo esas direcciones MAC puedan comunicarse a través del switch. Si otro dispositivo con una dirección MAC diferente intenta comunicarse la entrada, port-security deshabilitará el puerto.

TRUNKING¹⁰: En redes el enlace troncal es una forma que tiene el sistema de proteger y configurar el acceso a la red a los usuarios para él envío de información de manera privada y privilegiada.

⁷ Cisco, Configuración de una puerta de enlace de último recurso mediante comandos IP 2020

⁸ José Manuel Méndez Cuadros Dpto. Arquitectura de Computadores y Automática Universidad Complutense de Madrid 2018

⁹ Cisco, Capa de Red, Introducción a las redes. 2020

¹⁰ Cisco, fundamentos de seguridad de la red, Introducción a las redes 2020

RESUMEN

En el desarrollo de la ingeniería de Sistemas, nos incentiva a la adquisición y uso de habilidades, destrezas, amplios conocimientos sobre diversos temas y el manejo de redes de información, con el fin de ser competitivos en el mercado de la tecnología, informática, redes y sistemas; así estar más preparado para los diferentes retos que se presenten, estar a la vanguardia en las nuevas tecnologías y herramientas que se desarrollan cada día en el área de sistemas.

El desarrollo de este diplomado de CISCO CCNA pondremos a prueba nuestras diferentes habilidades adquiridas mediante la solución de dos escenarios, donde se deben diagnosticar, configurar y dar solución a las problemáticas en redes mediante la herramienta Packet Tracer en la cual se desarrollarán los simuladores para el desarrollo de esta actividad.

Palabras clave: Dirección IP, IPv4, IPv6; Enlace troncal, Puerta de enlace, Red, Router, Switch.

ABSTRACT

In the development of Systems engineering, it encourages us to acquire and use abilities, skills, extensive knowledge on various topics and the management of information networks, in order to be competitive in the market for technology, computing, networks and systems; Thus, being more prepared for the different challenges that arise, being at the forefront of new technologies and tools that are developed every day in the systems area.

The development of this CISCO CCNA diploma will test our different acquired skills by solving two scenarios, where network problems must be diagnosed, configured and solved using the Packet Tracer tool in which simulators will be developed for the development of this activity.

Keywords: IP address, IPV4, IPV6; Tunk, Gateway, Network, Router, Switch

INTRODUCCIÓN

La prueba de habilidades practicas dentro de las actividades de Diplomado CCNA CISCO, en el cual se evalúan las competencias y habilidades de los estudiantes que adquirieron durante el desarrollo de este diplomado y donde se pondrá en práctica lo aprendido en los diferentes niveles de Networking. Mediante el desarrollo de escenarios aplicables a la vida real, donde se dará solución a una problemática planteada, desarrollando su solución en el simulador de Packet Tracer, con su respectiva documentación, configuración de los dispositivos de cada uno de los escenarios, descripción de los procesos y verificación de la conectividad

Para el escenario 1 se configurarán dos redes con una cantidad de host (equipos PC) determinada para la solución de este ejercicio creando la correcta configuración de este escenario y poniendo a prueba lo aprendido durante el desarrollo de este diplomado en la seguridad de la red y pruebas de configuración.

Para el escenario 2 usaremos las configuraciones de seguridad aprendidas durante el curso al crear diferentes redes troncales y protocolos de seguridad de red de igual manera la configuración de conexión SSH para los equipos.

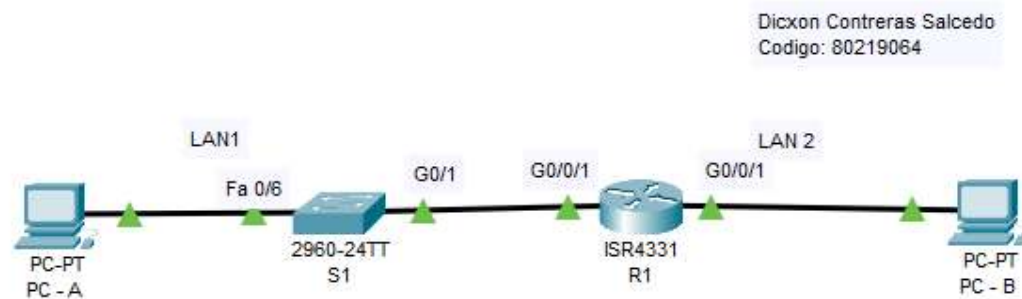
DESARROLLO ESCENARIO 1

Figura 1 Topología Escenario 1



Fuente: Documento Cisco

Figura 2 Simulación Escenario 1 en Packet Tracer



Fuente: Autor

Para el desarrollo del escenario 1 se realizará

Desarrolle el esquema de direccionamiento IP. Para la dirección IPv4 cree las dos subredes con la cantidad requerida de hosts. Asigne las direcciones de acuerdo con los requisitos mencionados en la tabla de direccionamiento

Número de Cédula: 80219064

Para el desarrollo de la actividad se usa el direccionamiento: 172.64.3.0

Utilizamos la máscara: 255.255.255.0

Formula $2n^2 - 2 \geq \text{Host}$

Tabla 1 Esquema de direccionamiento Escenario 1

| Ítem | Requerimiento |
|-----------------------------------|---|
| Dirección de Red | 172.XY.3.0 donde XY corresponde a los últimos dos dígitos de su cédula. |
| Requerimiento de host Subred LAN1 | 60 |
| Requerimiento de host Subred LAN2 | 20 |
| R1 G0/0/1 | Última dirección de host de la subred LAN1 |
| R1 G0/0/0 | Última dirección de host de la subred LAN2 |
| S1 SVI | Segunda dirección de host de la subred LAN1 |
| PC-A | Décima dirección de host de la subred LAN1 |
| PC-B | Décima dirección de host de la subred LAN2 |

Fuente: Autor

Tabla 2 Direccionamiento LAN Escenario 1

| | DIRECCION DE RED | MASCARA | PRIMERA IP | BROADCAST |
|-------|------------------|-----------------|-------------|-------------|
| LAN 1 | 172.64.3.0/26 | 255.255.255.192 | 172.64.3.1 | 172.64.3.63 |
| LAN 2 | 172.64.3.0/27 | 255.255.255.224 | 172.64.3.65 | 172.64.3.95 |

| ITEM | REQUERIMIENTO |
|-----------|---------------|
| R1 G0/0/1 | 172.64.3.62 |
| R1 G0/0/0 | 172.64.3.94 |
| S1 | 172.64.3.2 |
| PC1 | 172.64.3.10 |
| PC2 | 172.64.3.75 |

Fuente: Autor

Se procede a configurar cada uno de los dispositivos

Se asignan nombre y elementos de configuración de seguridad

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 1 Configuración Router Escenario 1

| Tarea | Especificación |
|---|--|
| Desactivar la búsqueda DNS | Utilizamos el comando “no ip domain lookup” para desactivar la búsqueda DNS Router(config)#no ip domain lookup |
| Nombre del Router | Con el uso del comando “hostname R1” cambiamos el nombre del Router a R1 Router(config)#hostname R1 |
| Nombre de dominio | Este commando “ip domain-name ccna-sa.com” nos permite agregar el dominio dentro del Router R1 R1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | Con el uso de estos comandos colocamos la clave ciscoenpass y encriptamos el servicio Enable secret ciscoenpass service password-encryption R1(config)#enable secret class |
| Contraseña de acceso a la consola | A continuación, ingresamos a la consola con la línea de comando “Line console 0” y colocamos la clave o Password ciscoconpass R1(config)#line console 0 R1(config-line)#password cisco |

| | |
|---|--|
| | <pre>R1(config-line)#login R1(config-line)#exit</pre> |
| Establecer la longitud mínima para las contraseñas | <p>Ahora usamos la línea de comando “security passwords min-length 10” para determinar la longitud de las contraseñas que coloquemos</p> <pre>R1(config)# security passwords min-length 10</pre> |
| Crear un usuario administrativo en la base de datos local | <p>Al utilizar “username” se crea el usuario “admin” y para su seguridad se asigna la contraseña “admin1pass”</p> <pre>R1(config)# username admin secret adminpass</pre> |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | <p>Continuamos configurando el inicio de sección del Router, colocando una clave y solicitando el acceso de manera local</p> <pre>R1(config)# Line vty 0 15 R1(config-line)# Password admin1pass R1(config-line)#Login local</pre> |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | <p>Usando la línea de comando “transport input ssh” se configura el Router para que acepte solo conexiones SSH</p> <pre>R1(config-line)#transport input ssh R1(config-line)#exit</pre> |
| Cifrar las contraseñas de texto no cifrado | <p>Esta línea de comando “Service password-encryption” nos permite encriptar las claves</p> <pre>R1(config)#service password-encryption</pre> |
| Configurar un banner MOTD | <p>El banner es un mensaje que contiene el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece.</p> |

| | |
|-----------------------------------|--|
| | R1(config)# banner motd %R1 Dicxon Enrique Contreras Salcedo Ingeniería de Sistemas% |
| Configuración de interface G0/0/0 | Ahora establecemos la configuración IPV4 para el puerto g0/0/1 R1(config)# Int g0/0/1 R1(config-if)# Ip address 172.64.3.62 255.255.255.192 R1(config-if)# Description #interfaz de lan 1# R1(config-if)# No shutdown Exit |
| Configuración de interface G0/0/1 | Ahora establecemos la configuración IPV4 para el puerto g0/0/0 R1(config)# Int g0/0/0 R1(config-if)# Ip address 172.64.3.94 255.255.255.224 R1(config-if)# Description #interfaz de lan 2# R1(config-if)# No shutdown R1(config-if)# Exit |
| Generar una clave de cifrado RSA | Configuramos el Módulo de 512 a 1024 bits R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 |

Fuente: Autor

Se procede a realizar la configuración del Router (R1) procedemos a acceder a la consola en modo privilegiado ejecutamos el comando no ip domain lookup para desactivar la búsqueda DNS, ahora configuramos el nombre del dispositivo el dominio y la contraseña cifrada mediante el comando enable secret, la contraseña con el comando password y

login, establecemos la longitud de configuración global a mínima de 5 caracteres para las claves, ahora se crea el usuario y su clave, se configura las líneas VTY para la base de datos local comando line vty 0 15, se configura solo aceptar correcciones SSH con el comando transport input ssh, se configuran las contraseñas de texto no cifrado con el comando service password-encryption, realizamos la configuración del banner con el mensaje “R1 Dixxon Enrique Contreras Salcedo Ingeniería de Sistemas”, se configura la interfaz G0/0/1 y G/0/0 con su configuración IPV4

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 2 Configuración Switch 1 Escenario 1

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Utilizamos el comando “no ip domain lookup” para desactivar la búsqueda DNS Switch(config)#no ip domain lookup |
| Nombre del switch | Con el uso del comando “hostname S1” cambiamos el nombre del Switch a S1 Switch(config)#hostname S1 |
| Nombre de dominio | Este comando “ip domain-name ccna-sa.com” nos permite agregar el dominio dentro del Switch S1 Switch(config)#hostname S1 |
| Contraseña cifrada para el modo EXEC privilegiado | Con el uso de este comando colocamos la clave ciscoenpass Enable secret ciscoenpass S1(config)#Enable secret ciscoenpass |
| Contraseña de acceso a la consola | A continuación, ingresamos a la consola con la línea de comando “Line console 0” y colocamos la clave o Password ciscoconpass |

| | |
|---|--|
| | <pre>S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit</pre> |
| Apagar todos los puertos sin usar | <p>Procedemos a seleccionar los puertos que no estamos utilizando a través "interface range f0/1-4,f0/7-24 ,g0/2" y a continuación los apagamos usando "shutdown"</p> <pre>S1(config)#interface range f0/1-4,f0/7-24 ,g0/2 S1(config-line)#no shutdown</pre> |
| Crear un usuario administrativo en la base de datos local | <p>Creamos el usuario: admin y se le asigna la contraseña: admin1pass usando la instrucción "username admin secret admin1pass"</p> <pre>S1(config)#username admin secret admin1pass</pre> |
| Configure el inicio de sesión en las líneas VTY para que use la base de datos local | <p>Continuamos configurando el inicio de sección del Switch, colocando una clave y solicitando el acceso de manera local</p> <pre>S1(config)# Line vty 0 15 S1(config-line)#Password admin1pass S1(config-line)#Login local</pre> |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | <p>Usando la línea de comando "transport input ssh" se configura el Router para que acepte solo conexiones SSH</p> <pre>S1(config-line)#transport input ssh S1(config-line)#exit</pre> |

| | |
|--|---|
| Cifrar las contraseñas de texto no cifrado | Esta línea de comando "Service password-encryption" nos permite encriptar las claves S1(config)#service password-encryption |
| Configurar un banner MOTD | El banner es un mensaje que contiene el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. S1(config)#banner motd "S1 Dixxon Enrique Contreras Salcedo Ingeniería de Sistemas" |
| Generar una clave de cifrado RSA | Configuramos el Módulo de 512 a 1024 bits crypto key generate rsa S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 |
| Configure la interfaz de administración (SVI) en VLAN1 | Procedemos a configurar la dirección IPv4 para el Switch S1 usando las instrucciones: S1(config)#Int vlan 1 S1(config-if)#ip address 172.64.3.2 255.255.255.192 S1(config-if)#No shutdown Configuramos la puerta de enlace del Switch S1(config-if)# ip default-gateway 172.64.3.62 |

Fuente: Autor

Se procede a realizar la configuración del Switch (S1) procedemos a acceder a la consola en modo privilegiado ejecutamos el comando no ip domain lookup para desactivar la búsqueda DNS, ahora configuramos el nombre del dispositivo el dominio y la contraseña cifrada mediante el comando enable secret, la contraseña con el comando password y login, establecemos la longitud de configuración global a mínima de 5 caracteres para las claves, ahora se crea el usuario y su clave, se configura las líneas VTY para la base de datos local comando line vty 0 15, se configura solo aceptar correcciones SSH con el

comando `transport input ssh`, se configuran las contraseñas de texto no cifrado con el comando `service password-encryption`, realizamos la configuración del banner con el mensaje “S1 Dicxon Enrique Contreras Salcedo Ingeniería de Sistemas”, se realiza la encriptación RSA con el comando `crypto key generate rsa` pasándolo a 1024 bits, se configura la Interfaz (SVI) `vlan 1` Usuarios asignándole la IPv4 172.64.3.2 y mascara de red 255.255.255.192,

Paso 2. Configurar los equipos

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

Tabla 3 Configuración PC-A 1 Escenario

| Configuración de red de PC-A | |
|--------------------------------------|-----------------|
| Descripción | PC-A |
| Dirección física | 172.64.3.10/26 |
| Dirección IPv4 | 172.64.3.10 |
| Máscara de subred | 255.255.255.192 |
| Puerta de enlace IPv4 predeterminada | 172.64.3.92 |

Fuente: Autor

Tabla 4 Configuración PC-B 1 Escenario

| Configuración de red de PC-B | |
|------------------------------|----------------|
| Descripción | PC-B |
| Dirección física | 172.64.3.75/27 |
| Dirección IPv4 | 172.64.3.75 |

| | |
|---|-----------------|
| Máscara de subred | 255.255.255.224 |
| Puerta de enlace IPv4 predeterminada | 172.64.3.94 |

Fuente: Autor

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

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

Nota: Si los pings a los servidores fallan, deshabilite temporalmente el firewall del equipo y vuelva a realizar la verificación.

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

Tabla 5 Verificación de los dispositivos de red

| Desde | A | Dirección IP | Resultados de ping |
|-------|--------------|--------------|---|
| PC-A | R1 G0/0/0 | 172.64.3.62 | Se realiza ping para comprobar la conectividad del PC-A al puerto G0/0/0 del Router funcionando correctamente |
| | R1 G0/0/1 | 172.64.3.94 | Se realiza ping para comprobar la conectividad del PC-A al puerto G0/0/1 del Router funcionando correctamente |
| | S1 VLAN 1 | 172.64.3.2 | Se realiza ping para comprobar la conectividad del PC-A al switch (S1) la cual funciona |
| | PC-B | 172.64.3.75 | Se realiza ping para comprobar la conectividad del PC-A de la red LAN1 al PC-B de la red LAN2, se realiza la prueba de manera exitosa |

| | | | |
|------|--------------|-------------|--|
| PC-B | R1 G0/0/0 | 172.64.3.62 | Se realiza ping para comprobar la conectividad del PC-B al puerto G0/0/0 del Router |
| | R1 G0/0/1 | 172.64.3.94 | Se realiza ping para comprobar la conectividad del PC-B al puerto G0/0/1 del Router funcionando correctamente |
| | S1 VLAN1 | 172.64.3.2 | Se realiza ping para comprobar la conectividad del PC-B al switch (S1), se realiza la prueba de manera exitosa |
| | | 172.64.3.10 | Se realiza ping para comprobar la conectividad del PC-B de la red LAN2 al PC-A de la red LAN1 |

Fuente: Autor

Se realizan las pruebas de verificación de la correcta configuración de la red y se procede a realizar capturas de funcionamiento

Figura 3 Prueba desde PC-A a R1 G0/0/0

```

PC - A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.64.3.62

Pinging 172.64.3.62 with 32 bytes of data:

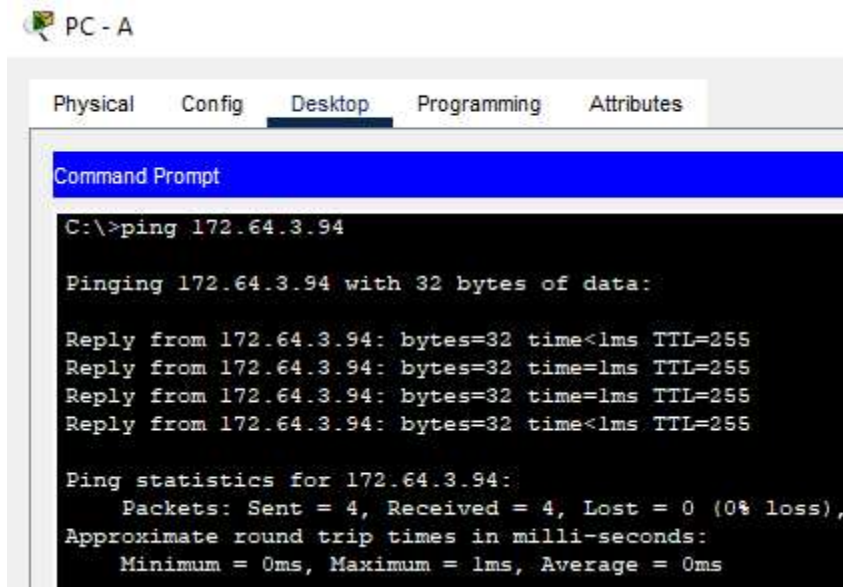
Reply from 172.64.3.62: bytes=32 time<lms TTL=255
Reply from 172.64.3.62: bytes=32 time<lms TTL=255
Reply from 172.64.3.62: bytes=32 time<lms TTL=255
Reply from 172.64.3.62: bytes=32 time<lms TTL=255

Ping statistics for 172.64.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Fuente: Autor

Figura 4 Prueba desde PC-A a R1 G0/0/1



The screenshot shows the 'Desktop' tab of a PC configuration window. A Command Prompt window is open, displaying the execution of a ping command to the IP address 172.64.3.94. The output shows four successful replies with 32 bytes of data, a time of 1ms, and a TTL of 255. The ping statistics indicate that all four packets were received with 0% loss, and the round trip times were all 0ms.

```
PC - A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.64.3.94

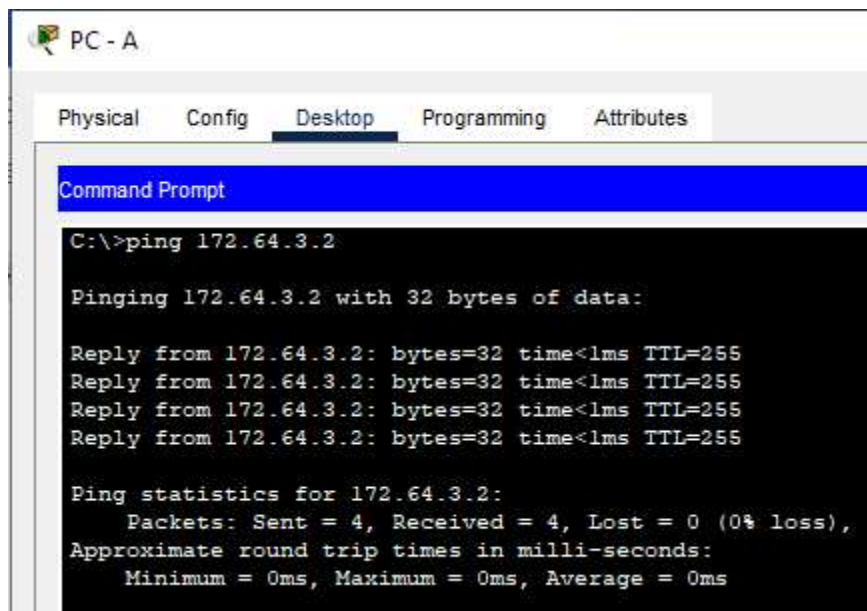
Pinging 172.64.3.94 with 32 bytes of data:

Reply from 172.64.3.94: bytes=32 time<1ms TTL=255
Reply from 172.64.3.94: bytes=32 time=1ms TTL=255
Reply from 172.64.3.94: bytes=32 time=1ms TTL=255
Reply from 172.64.3.94: bytes=32 time<1ms TTL=255

Ping statistics for 172.64.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autor

Figura 5 Prueba desde PC-A a S1



The screenshot shows the 'Desktop' tab of a PC configuration window. A Command Prompt window is open, displaying the execution of a ping command to the IP address 172.64.3.2. The output shows four successful replies with 32 bytes of data, a time of 1ms, and a TTL of 255. The ping statistics indicate that all four packets were received with 0% loss, and the round trip times were all 0ms.

```
PC - A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.64.3.2

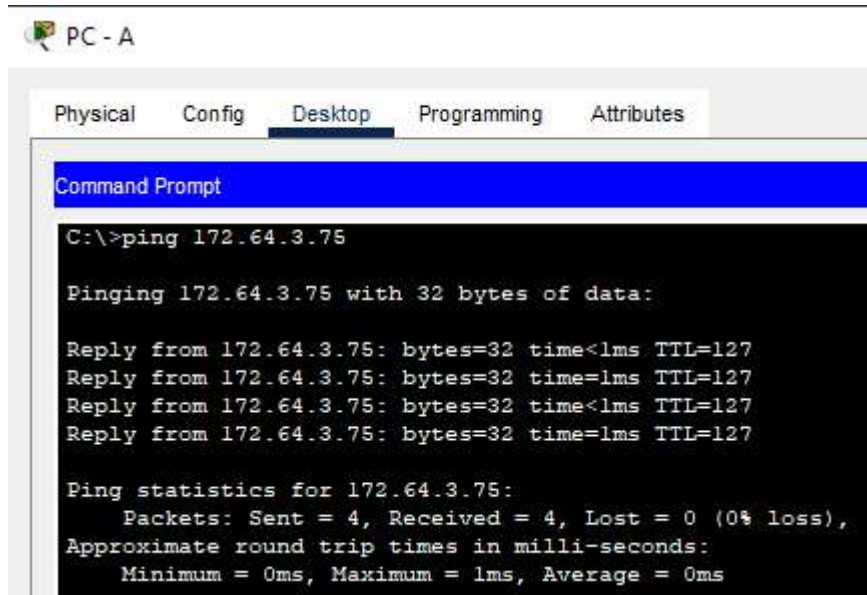
Pinging 172.64.3.2 with 32 bytes of data:

Reply from 172.64.3.2: bytes=32 time<1ms TTL=255
Reply from 172.64.3.2: bytes=32 time<1ms TTL=255
Reply from 172.64.3.2: bytes=32 time<1ms TTL=255
Reply from 172.64.3.2: bytes=32 time<1ms TTL=255

Ping statistics for 172.64.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 6 Prueba desde PC-A a PC-B



PC - A

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 172.64.3.75

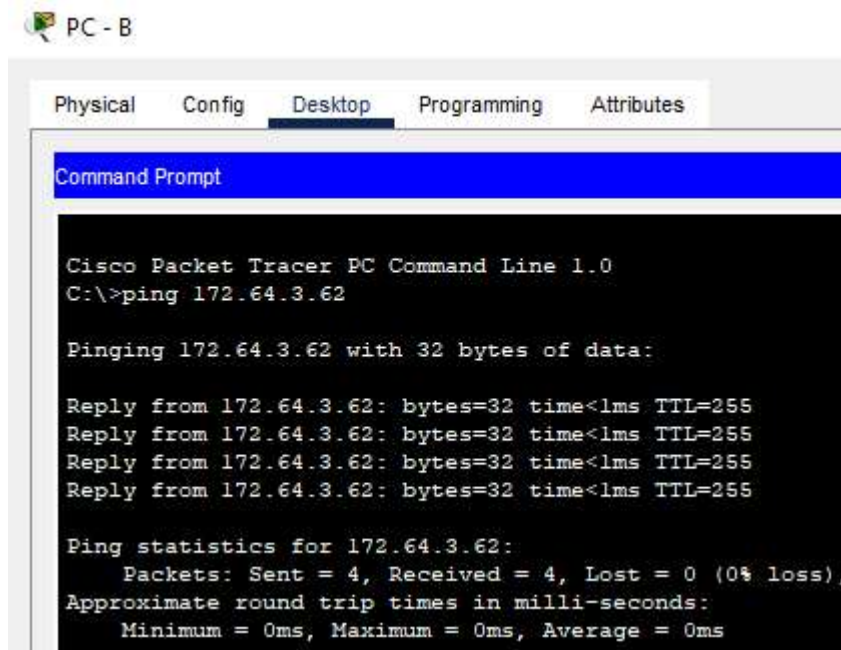
Pinging 172.64.3.75 with 32 bytes of data:

Reply from 172.64.3.75: bytes=32 time<lms TTL=127
Reply from 172.64.3.75: bytes=32 time=lms TTL=127
Reply from 172.64.3.75: bytes=32 time<lms TTL=127
Reply from 172.64.3.75: bytes=32 time=lms TTL=127

Ping statistics for 172.64.3.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autor

Figura 7 Prueba desde PC-B a R1 G0/0/0



PC - B

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.64.3.62

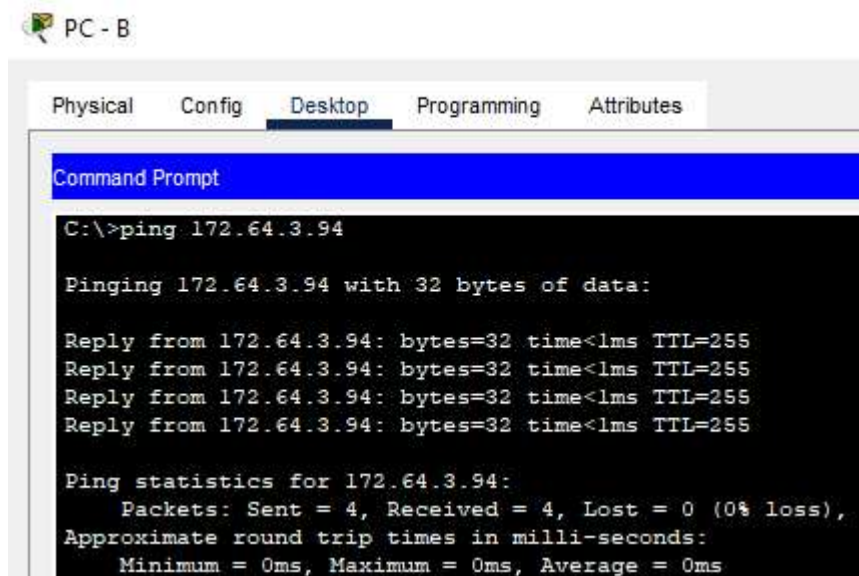
Pinging 172.64.3.62 with 32 bytes of data:

Reply from 172.64.3.62: bytes=32 time<lms TTL=255
Reply from 172.64.3.62: bytes=32 time<lms TTL=255
Reply from 172.64.3.62: bytes=32 time<lms TTL=255
Reply from 172.64.3.62: bytes=32 time<lms TTL=255

Ping statistics for 172.64.3.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 8 Prueba desde PC-B a R1 G0/0/1



PC - B

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 172.64.3.94

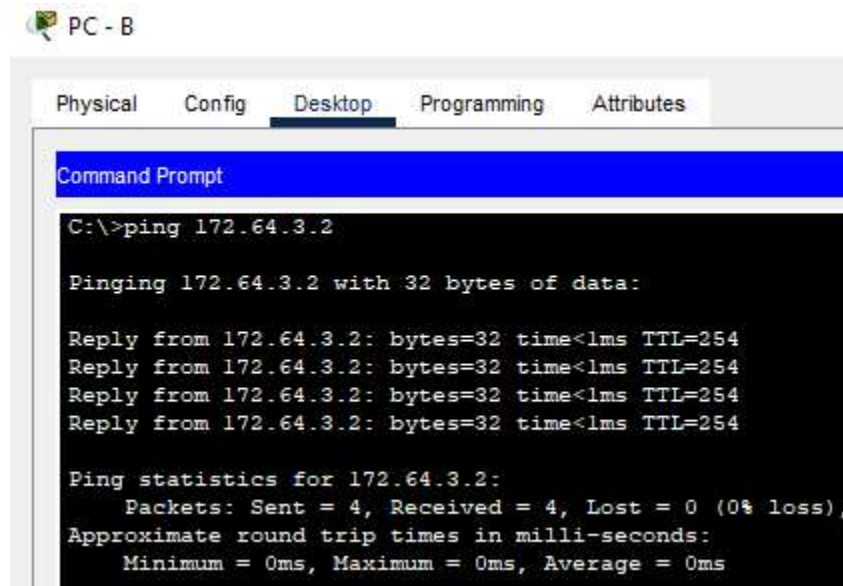
Pinging 172.64.3.94 with 32 bytes of data:

Reply from 172.64.3.94: bytes=32 time<lms TTL=255
Reply from 172.64.3.94: bytes=32 time<lms TTL=255
Reply from 172.64.3.94: bytes=32 time<lms TTL=255
Reply from 172.64.3.94: bytes=32 time<lms TTL=255

Ping statistics for 172.64.3.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 9 Prueba desde PC-B a S1



PC - B

Physical Config **Desktop** Programming Attributes

Command Prompt

```
C:\>ping 172.64.3.2

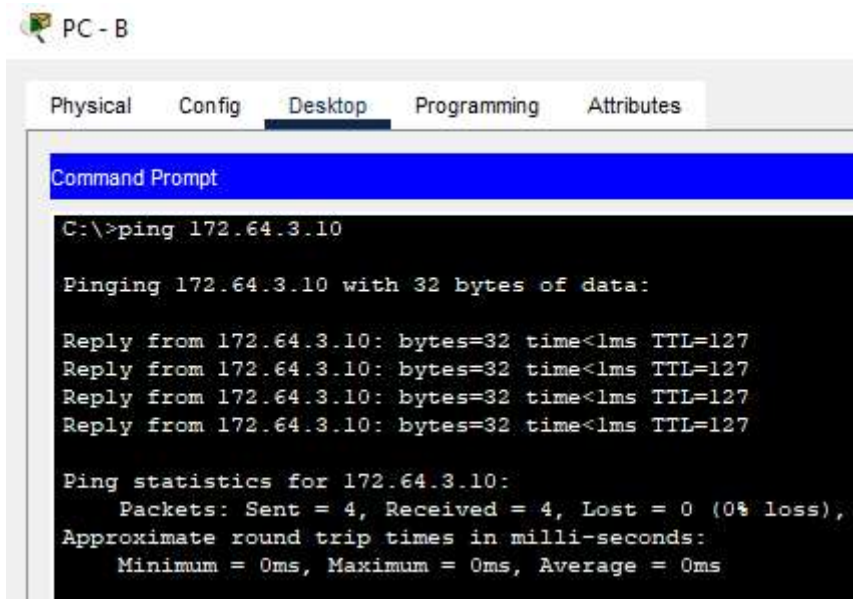
Pinging 172.64.3.2 with 32 bytes of data:

Reply from 172.64.3.2: bytes=32 time<lms TTL=254
Reply from 172.64.3.2: bytes=32 time<lms TTL=254
Reply from 172.64.3.2: bytes=32 time<lms TTL=254
Reply from 172.64.3.2: bytes=32 time<lms TTL=254

Ping statistics for 172.64.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 10 Prueba desde PC-B a PC-A



The image shows a screenshot of a Command Prompt window titled "PC - B". The window has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes", with "Desktop" selected. The Command Prompt displays the following text:

```
C:\>ping 172.64.3.10

Pinging 172.64.3.10 with 32 bytes of data:

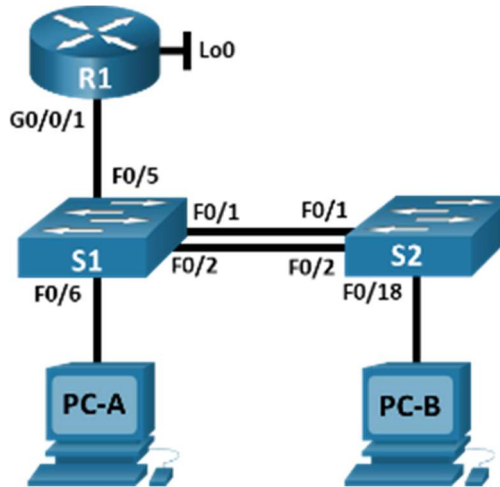
Reply from 172.64.3.10: bytes=32 time<1ms TTL=127
Reply from 172.64.3.10: bytes=32 time<1ms TTL=127
Reply from 172.64.3.10: bytes=32 time<1ms TTL=127
Reply from 172.64.3.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.64.3.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Desarrollo Escenario 2

Figura 11 Topología Escenario 2

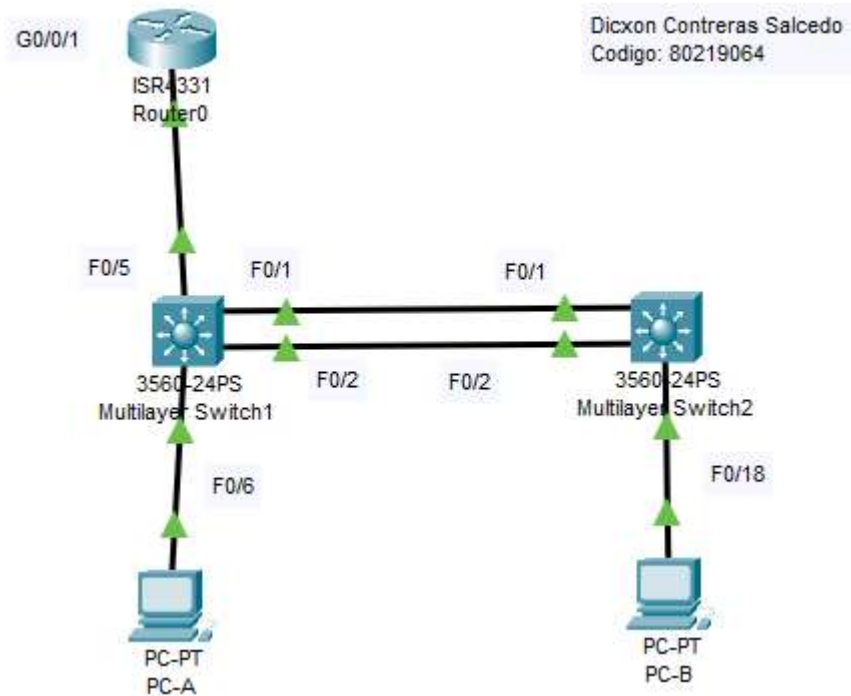


Fuente: Documento Cisco

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

Se procede a crear la topología en el simulador de Packet Tracer para ello utilizamos Router Cisco 43331, 2 Switch Cisco 3560, 2 PCs, sus respectivos cables para la conexión.

Figura 12 Simulación Escenario 2 en Packet Tracer



Fuente: Autor

Tabla 6 VLAN Escenario 2

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

Fuente: Cisco

Tabla de asignación de direcciones

NOTA: Tenga en cuenta que para el direccionamiento donde aparezca XY deberá reemplazarlos por los últimos dos dígitos de su número de identificación.

Tabla 7 Asignación de direcciones

| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
|-------------------------------|-------------------------------|--|
| R1 G0/0/1.20 | 10.64.8.1 /26 | No corresponde |
| | 2001:db8:acad:a: :1 /64 | No corresponde |
| R1 G0/0/1.30 | 10.64.8.65 /27 | No corresponde |
| | 2001:db8:acad:b: :1 /64 | No corresponde |
| R1 G0/0/1.40 | 10.64.8.97 /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 4 | 10.64.8.98 /29 | 10.19.8.97 |
| | 2001:db8:acad:c: :98 /64 | No corresponde |
| | fe80: :98 | No corresponde |
| S2 VLAN 4 | 10.64.8.99 /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 |
| Dispositivo / interfaz | Dirección IP / Prefijo | Puerta de enlace predeterminada |
| | 2001:db8:acad:b: :50 /64 | fe80::1 |

Fuente: Autor

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

PARTE 1: INICIALIZAR Y RECARGAR Y CONFIGURAR ASPECTOS BÁSICOS DE LOS DISPOSITIVOS

Instrucciones

Paso 1: Inicializar y volver a cargar el Router y el Switch

Borre las configuraciones de inicio y las VLAN del Router y del Switch y vuelva a cargar los dispositivos.

Tabla 8 Inicialización y carga del Router

| Tarea | Especificación |
|-------------------------------------|-----------------------------|
| Ingresar al modo privilegiado | Router>enable |
| Restablecer valores predeterminados | Router#erase startup-config |
| Reiniciar el Router | Router#reload |

Fuente: Autor

Procedemos a ingresar al Router 1 usando la consola y por medio del modo privilegiado borramos cualquier configuración con el comando startup-config el cual borra el contenido de la NVRAM, de ahí reiniciamos el Router usando el comando reload.

Tabla 9 Inicialización y carga del Switch 1 y 2

| Tarea | Especificación |
|-------------------------------------|-----------------------------|
| Ingresar al modo privilegiado | Switch>enable |
| Restablecer valores predeterminados | Switch#erase startup-config |
| Eliminar Vlan | Switch#delete vlan.dat |
| Reiniciar el Switch | Switchr#reload |

Fuente: Autor

Procedemos a ingresar al Switch 1 y 2 usando la consola y por medio del modo privilegiado borramos cualquier configuración con el comando startup-config el cual borra el contenido de la NVRAM a continuación usamos el comando delete vlan.dat que nos permite eliminar la base de datos vlan, a continuación, reiniciamos los Switch usando el comando reload.

Después de recargar el Switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el Switch.

Tabla 10 Configuración de plantilla SDM en Switch 1 y 2

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

Fuente: Autor

Procedemos a configurar el Switch Cisco 3560 que no soporta IPV6, configuramos la plantilla SDN para que admita IPV6 junto a IPV4, a continuación, ingresamos a la consola y desde modo privilegiado usamos el comando show sdm prefer, donde observamos que solo soporta IPV4, para poder activar IPV6 se ejecuta el comando sdm prefer dual-ipv4-and-ipv6 default, y se reinicia con el comando reload para que cargue la nueva plantilla que soporta IPV4 y IPV6.

Paso 2: Configurar R1 Escenario 2

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configuración del Router

| Tarea | Especificación |
|---|---------------------------------------|
| Desactivar la búsqueda DNS | Router(config)#no ip domain lookup |
| Nombre del router | Router(config)#hostname R1 |
| Nombre de dominio | R1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXEC privilegiado | R1(config)#enable secret class |

| | |
|--|--|
| Contraseña de acceso a la consola | R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit |
| Establecer la longitud mínima para las contraseñas 5 caracteres | R1(config)#security passwords min-length 5 |
| Crear un usuario administrativo en la base de datos local Nombre de usuario: admin Password: admin1pass | R1(config)# username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTY para que use la base de datos local | R1(config)#line vty 0 15 R1(config-line)#login local |
| Configurar VTY solo aceptando SSH | R1(config-line)#transport input ssh R1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | R1(config)#service password-encryption |
| Configure un MOTD Banner Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. | R1(config)#banner motd "R1 Dixon Enrique Contreras Salcedo Ingeniería de Sistemas" |
| Habilitar el routing IPv6 | R1(config)#ipv6 unicast-routing |

| | |
|---|--|
| <p>Configurar interfaz G0/0/1 y subinterfases Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como fe80: :1</p> | <pre>R1(config)#interface g0/0/1.20 R1(config-subif)#encapsulation dot1q 20 R1(config-subif)#description vlan Docentes R1(config-subif)#ip address 10.64.8.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)# interface g0/0/1.30</pre> |
| <p>Establece la dirección IPv6. Activar la interfaz.</p> | <pre>R1(config-subif)#encapsulation dot1q 30 R1(config-subif)#description vlan Estudiantes R1(config-subif)#ip address 10.64.8.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)#interface g0/0/1.40 R1(config-subif)#encapsulation dot1q 40 R1(config-subif)#description vlan Invitados R1(config-subif)#ip address 10.64.8.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)#interface g0/0/1.56</pre> |

| | |
|---|---|
| | <pre>R1(config-subif)#encapsulation dot1q 56 Native R1(config-subif)#description vlan Native R1(config-subif)#interface g0/0/1 R1(config-if)#no shutdown</pre> |
| <p>Configure el Loopback0 interface Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como fe80::1</p> | <pre>R1(config-if)# interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link- local R1(config-if)#description Internet R1(config-if)#exit</pre> |
| <p>Generar una clave de cifrado RSA Módulo de 1024 bits</p> | <pre>R1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024</pre> |

Fuente: Autor

Se procede a realizar la configuración del Router (R1) procedemos a acceder a la consola en modo privilegiado ejecutamos el comando `no ip domain lookup` para desactivar la búsqueda DNS, ahora configuramos el nombre del dispositivo el dominio y la contraseña cifrada mediante el comando `enable secret`, la contraseña con el comando `password` y `login`, establecemos la longitud de configuración global a mínima de 5 caracteres para las claves, ahora se crea el usuario y su clave, se configura las líneas VTY para la base de datos local comando `line vty 0 15`, se configura solo aceptar correcciones SSH con el comando `transport input ssh`, se configuran las contraseñas de texto no cifrado con el comando `service password-encryption`, realizamos la configuración del banner con el mensaje "R1 Dicxon Enrique Contreras Salcedo Ingeniería de Sistemas", se habilita el enrutamiento IPV6 comando `ipv6 unicast-routing`, configuramos la interfaz G0/0/1 y

subinterfaces verificando la encapsulación respectiva VLAN junto con la dirección IPv4, IPv6 y el enlace IPv6. Ahora configuramos las demás interfaces g0/0/1.20, interface g0/0/1.30, interface g0/0/1.40, interface g0/0/1.56, la última asignándole la vlan nativa y activamos la interfaz G0/0/1 comando no shutdown, se procede a configurar la interface Loopback0 interface loopback 0 asignándole una dirección IPv4, IPv6 y dirección local.

Paso 3: Configure S1 y S2 Escenario 2

Las tareas de configuración incluyen lo siguiente:

Tabla 12 configuración del Switch 1

| Tarea | Especificación |
|--|--|
| Desactivar la búsqueda DNS. | Switch(config)#no ip domain lookup |
| Nombre del switch | Switch(config)#hostname S1 |
| Nombre de dominio (ccna-sa.com) | S1(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXECprivilegiado (class) | S1(config)#enable secret class |
| Contraseña de acceso a la consola (cisco) | S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exit |
| Crear un usuario administrativo en la base dedatos local Nombre de usuario: admin Password: admin1pass | S1(config)#username admin secret admin1pass |

| Tarea | Especificación |
|---|--|
| 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 S1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S1(config)#service password-encryption |
| Configurar un MOTD Banner Debe contener el nombre del dispositivo, el nombre completo del estudiante y el programa académico al que pertenece. | S1(config)#banner motd "S1 Dixon Enrique Contreras Salcedo Ingenieria de Sistemas" |
| Generar una clave de cifrado RSA Módulo de 1024 bits | S1(config)#crypto key generate rsa How many bits in the modulus [512]: 1024 |
| Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como FE80::98 para S1 y FE80::99 para S2 Establecer la dirección IPv6 de capa 3 | S1(config)#interface vlan 40 S1(config-if)#ip address 10.64.8.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db8:acad:c::98/64 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#description vlan Usuarios S1(config-if)#no shutdown |

| | |
|--|---|
| | S1(config-if)#exit |
| Configuración del gateway predeterminado Configure la puerta de enlace predeterminada como 10.64.8.97 para IPv4 | S1(config)#ip default-gateway 10.64.8.97 |

Fuente: Autor

Se procede a realizar la configuración del Switch (S1) procedemos a acceder a la consola en modo privilegiado ejecutamos el comando `no ip domain lookup` para desactivar la búsqueda DNS, ahora configuramos el nombre del dispositivo el dominio y la contraseña cifrada mediante el comando `enable secret`, la contraseña con el comando `password` y `login`, establecemos la longitud de configuración global a mínima de 5 caracteres para las claves, ahora se crea el usuario y su clave, se configura las líneas VTY para la base de datos local comando `line vty 0 15`, se configura solo aceptar correcciones SSH con el comando `transport input ssh`, se configuran las contraseñas de texto no cifrado con el comando `service password-encryption`, realizamos la configuración del banner con el mensaje "R1 Dixon Enrique Contreras Salcedo Ingeniería de Sistemas", se realiza la encriptación RSA con el comando `crypto key generate rsa` pasándolo a 1024 bits, se configura la Interfaz (SVI) VLAN 4 Usuarios asignándole la IPv4 10.64.8.98 y máscara de red 255.255.255.248, la dirección IPv6 2001:db8:acad:c::98 prefijo /64 con la puerta de enlace local fe80::98, ahora realizamos la descripción y procedemos a habilitarla con el comando `no shutdown`, terminamos al configurar la puerta de enlace predeterminada 10.64.8.97 en IPv4, no realizamos la configuración de la puerta de enlace en IPv6 ya que se habilita de manera automática.

Tabla 13 Configuración del Switch 2

| Tarea | Especificación |
|--|--|
| Desactivar la búsqueda DNS. | Switch(config)#no ip domain lookup |
| Nombre del switch | Switch(config)#hostname S2 |
| Nombre de dominio (ccna-sa.com) | S2(config)#ip domain-name ccna-sa.com |
| Contraseña cifrada para el modo EXECprivilegiado (class) | S2(config)#enable secret class |
| Contraseña de acceso a la consola (cisco) | S2(config)#line console 0 S2(config-line)#password cisco S2(config-line)#login S2(config-line)#exit |
| Crear un usuario administrativo en la base dedatos local Nombre de usuario: admin Password: admin1pass | S2(config)#username admin secret admin1pass |
| Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local | S2(config)#line vty 0 15 S1(config-line)#login local |
| Configurar las líneas VTY para que acepten únicamente las conexiones SSH | S2(config-line)#transport input ssh S1(config-line)#exit |
| Cifrar las contraseñas de texto no cifrado | S2(config)#service password-encryption |

| | |
|---|---|
| <p>Configurar un MOTD Banner</p> <p>Debe contener el nombre del dispositivo, el nombre completo delestudiante y el programa académicoal que pertenece.</p> | <pre>S2(config)#banner motd "S1 Dicxon Enrique Contreras Salcedo Ingeniería de Sistemas"</pre> |
| <p>Generar una clave de cifrado RSA</p> <p>Módulo de 1024 bits</p> | <pre>S2(config)#crypto key generate rsa How many bits in the modulus [512]: 1024</pre> |
| <p>Configurar la interfaz de administración (SVI)</p> <p>Establecer la dirección IPv4 de capa3</p> <p>Establezca la dirección local de enlace IPv6 como FE80: :98 para S1y FE80: :99 para S2</p> <p>Establecer la dirección IPv6 de capa3</p> | <pre>S2(config)#interface vlan 40 S2(config-if)#ip address 10.64.8.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db8:acad:c::99/64 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#description vlan Usuarios S2(config-if)#no shutdown S2(config-if)#exit</pre> |
| <p>Configuración del gateway predeterminado</p> <p>Configure la puerta de enlace predeterminada como 10.64.8.97para IPv4</p> | <pre>S2(config)#ip default-gateway 10.64.8.97</pre> |

Fuente: Autor

Se procede a realizar la configuración del Switch (S2) procedemos a acceder a la consola en modo privilegiado ejecutamos el comando `no ip domain lookup` para desactivar la búsqueda DNS, ahora configuramos el nombre del dispositivo el dominio y la contraseña cifrada mediante el comando `enable secret`, la contraseña con el comando `password` y `login`, establecemos la longitud de configuración global a mínima de 5 caracteres para

las claves, ahora se crea el usuario y su clave, se configura las líneas VTY para la base de datos local comando line vty 0 15, se configura solo aceptar correcciones SSH con el comando transport input ssh, se configuran las contraseñas de texto no cifrado con el comando service password-encryption, realizamos la configuración del banner con el mensaje “R1 Dixxon Enrique Contreras Salcedo Ingeniería de Sistemas”, se realiza la encriptación RSA con el comando crypto key generate rsa pasándolo a 1024 bits, se configura la Interfaz (SVI) VLAN 4 Usuarios asignándole la IPv4 10.64.8.98 y mascara de red 255.255.255.248, la dirección IPv6 2001:db8:acad:c::98 prefijo /64 con la puerta de enlace local fe80::98, ahora realizamos la descripción y procedemos a habilitarla con el comando no shutdown, terminamos al configurar la puerta de enlace predeterminada 10.64.8.97 en IPv4, no realizamos la configuración de la puerta de enlace en IPv6 ya que se habilita de manera automática.

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

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 14 Configuración S1 VLAN, Trunking, EtherChannel

| Tarea | Especificación |
|--|--|
| Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados | S1#configure terminal S1(config)#vlan 20 S1(config-vlan)#name Docentes S1(config-vlan)#vlan 30 S1(config-vlan)#name Estudiantes S1(config-vlan)#vlan 40 S1(config-vlan)#name Invitados |

| | |
|---|--|
| <p>VLAN 50, nombre Usuarios</p> <p>VLAN 56, nombre Native</p> | <pre>S1(config-vlan)#vlan 50 S1(config-vlan)#name Usuarios S1(config-vlan)#vlan 56 S1(config-vlan)#name Native S1(config-vlan)#exit</pre> |
| <p>Crear troncos 802.1Q que utilicen la VLAN 6 nativa</p> <p>Interfaces F0/1, F0/2 y F0/5</p> | <pre>S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 56 S1(config-if)#interface range fa0/1-2 S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 56</pre> |
| <p>Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2</p> <p>Usar el protocolo LACP para la negociación</p> | <pre>S1(config)#interface range fa0/1-2 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</pre> |

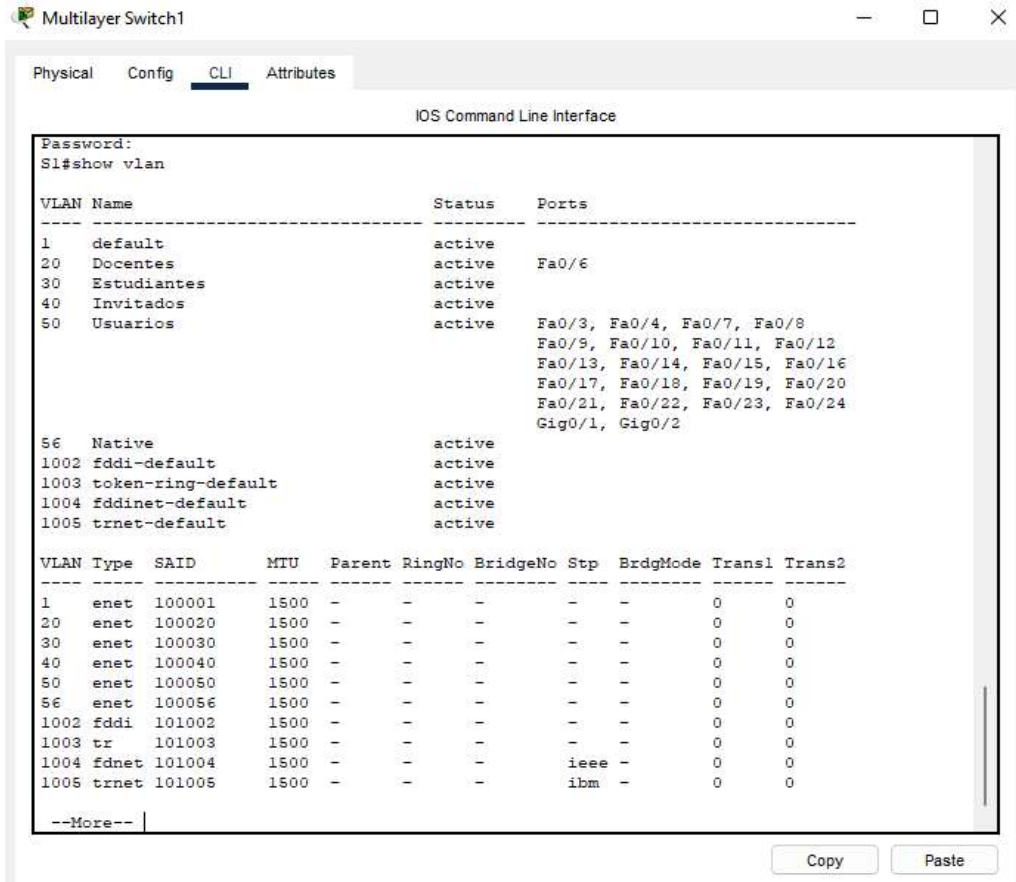
| | |
|---|---|
| | trunk native vlan 56 |
| Configurar el puerto de acceso de host para VLAN 2 Interface F0/6 | S1(config-if)#interface fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 |
| Configurar la seguridad del puerto en los puertos de acceso Permitir 4 direcciones MAC | S1(config-if)#switchport port-security maximum 4 |
| Proteja todas las interfaces no utilizadas Asignar a VLAN 50, Establecer en modo de acceso, agregar una descripción y apagar | S1(config-if-range)#interface range fa0/3-4 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta utilizándose S1(config-if-range)#shutdown S1(config-if-range)#interface range fa0/7-24 S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta utilizándose S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#switchport mode access |

| | |
|--|--|
| | <pre>S1(config-if-range)#switchport access vlan 50 S1(config-if-range)#description No esta utilizándose S1(config-if-range)#shutdown</pre> |
|--|--|

Fuente: Autor

Ingresamos a la consola en modo privilegiado para realizar la configuración global se crean las vlan 20 Docentes, vlan 30 Estudiantes, vlan 40 Invitados, vlan 50 Usuarios y vlan 56-Native, se crean las troncales que usen la vlan nativa interfaces fa0/1, fa0/2 y fa0/5, inicialmente configuraremos la interface fa0/5 utilizando la referencia de Switch, el comando de encapsulación switchport trunk encapsulation dot1q, para implementar la interface código switchport mode trunk direccionándola a la vlan 56 nativa switchport trunk native vlan 56, para configurar las fa0/1 y fa0/2 usamos un rango interface range fa0/1-2, ahora se configura la EtherChannel y se desactiva el rango anterior con shutdown para evitar conflictos en la configuración, la interface range fa0/1-2 usaremos el comando de encapsulación switchport trunk encapsulation dot1q, y para implementar la interface switchport mode trunk direccionándola a la vlan 56 nativa switchport trunk native vlan 56, creamos la EtherChannel del grupo de interfaces fa0/1-2 con el código channel-group 1 mode active y usar LACP creando el grupo 1, ahora se entra a la interfaz de este con interface Port-channel 1 para configurar las troncales, procedemos a configurar un puerto de acceso para la vlan 20- Estudiantes que use la fa0/2 con el comando switchport access vlan 20, configuración de seguridad en los puertos de acceso que permita 4 direcciones MAC, activamos la seguridad en la interfaz estableciendo máximo 4 direcciones MAC con switchport port-security maximum 4, aseguramos todas las interfaces sin usar asignándolas a la vlan 50-Usuarios indicando que no están utilizándose y apagamos con shutdown, siendo estas fa0/3-4, fa0/7-24 y g0/1-2, finalmente se activa el rango de interfaz fa0/1-2 con no shutdown.

Figura 13 Verificación Configuración VLAN S1



Fuente: Autor

Figura 14 Verificación Configuración Trunk S1

```

S1#show interface trunk

```

| Port | Mode | Encapsulation | Status | Native vlan |
|-------|------|---------------|----------|-------------|
| Pol | on | 802.lq | trunking | 56 |
| Fa0/5 | on | 802.lq | trunking | 56 |


```

Port      Vlans allowed on trunk
Pol       1-1005
Fa0/5     1-1005

```



```

Port      Vlans allowed and active in management domain
Pol       1,20,30,40,50,56
Fa0/5     1,20,30,40,50,56

```



```

Port      Vlans in spanning tree forwarding state and not pruned
Pol       1,20,30,40,50,56
Fa0/5     1,20,30,40,50,56

```

S1#

Fuente: Autor

Figura 15 Verificación Configuración EtherChannel S1

```

S1#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Pol(SU)        LACP        Fa0/1(P) Fa0/2(P)
S1#

```

Fuente: Autor

Figura 16 Verificación Configuración VLAN Brief

```

S1#show vlan brief
VLAN Name                Status    Ports
-----+-----+-----
1    default                active
20   Docentes                active    Fa0/6
30   Estudiantes            active
40   Invitados              active
50   Usuarios                active    Fa0/3, Fa0/4, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
56   Native                  active
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
S1#

```

Fuente: Autor

Paso 5: Configure el S2.

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

Tabla 15 Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel) en Switch 2

| Tarea | Especificación |
|--|---|
| Crear VLAN VLAN 20, nombre Docentes VLAN 30, nombre Estudiantes VLAN 40, nombre Invitados VLAN 50, nombre Usuarios VLAN 56, nombre Native | S2>enable S2#configure terminal S2(config)#vlan 20 S2(config-vlan)#name Docentes S2(config-vlan)#vlan 30 S2(config-vlan)#name Estudiantes S2(config-vlan)#vlan 40 S2(config-vlan)#name Invitados S2(config-vlan)#vlan 50 S2(config-vlan)#name Usuarios S2(config-vlan)#vlan 56 S2(config-vlan)#name Native S2(config-vlan)#exit |
| Crear troncos 802.1Q que utilicen la VLAN 6nativa Interfaces F0/1 y F0/2 | S2(config)#interface range fa0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 56 |

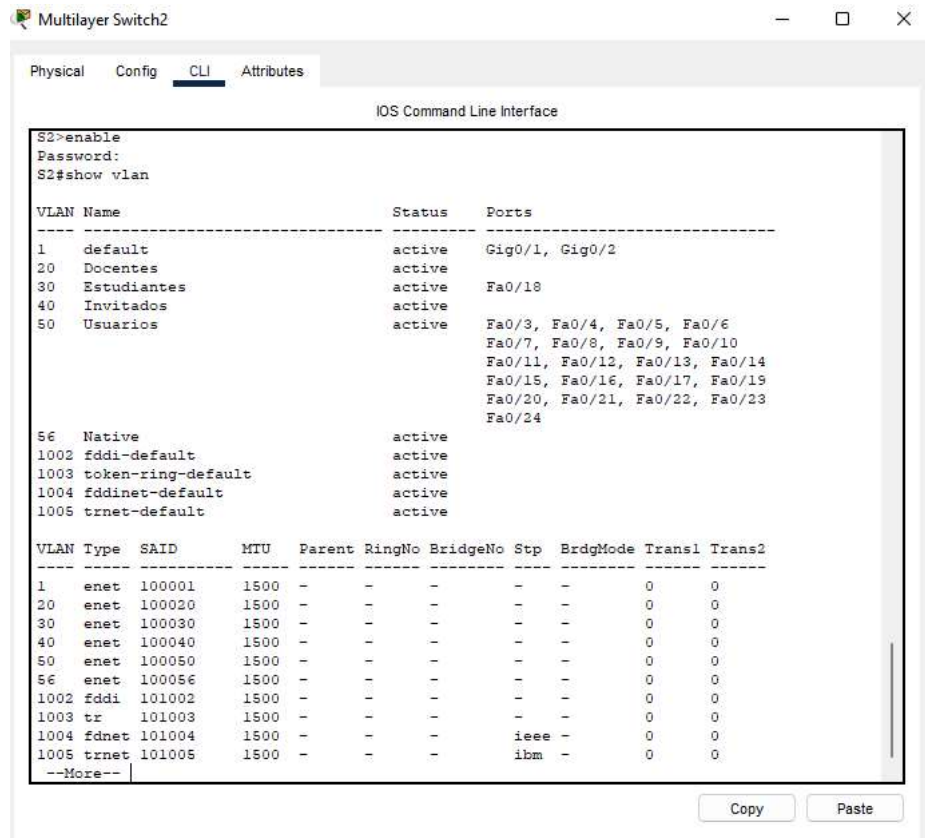
| | |
|---|--|
| <p>Crear un grupo de puertos EtherChannel deCapa 2 que use interfaces F0/1 y F0/2</p> <p>Usar el protocolo LACP para la negociación</p> | <pre>S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface Port-channel 1 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 56</pre> |
| <p>Configurar el puerto de acceso del host para laVLAN 30</p> <p>Interfaz F0/18</p> | <pre>S2(config-if)# interface fa0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 30</pre> |
| <p>Tarea</p> | <p>Especificación</p> |
| <p>Configure port-security en los access ports permite 4 MAC addresses</p> | <pre>S2(config-if)#switchport port-security maximum 4</pre> |
| <p>Asegure todas las interfaces no utilizadas. Asignar a VLAN 50, Establecer en modode acceso, agregar una descripción y apagar</p> | <pre>S2(config-if)#interface range fa0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta utilizándose S2(config-if-range)#shutdown S2(config-if-range)#interface range fa0/19-24</pre> |

| | |
|--|---|
| | <pre>S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 50 S2(config-if-range)#description No esta utilizándose S2(config-if-range)#shutdown</pre> |
|--|---|

Fuente: Autor

Ingresando en modo privilegiado, configuración global se crean las vlan 20 Docentes, vlan 30 Estudiantes, vlan 40-Invitados, vlan 50 Usuarios y vlan 56-Native, se crean las troncales que usen la Vlan nativa 56 interfaces fa0/1 y fa0/2, se configura las fa0/1 y fa0/2 usamos el rango interface range fa0/1-2, a continuación se configura la EtherChannel, desactivamos el rango anterior con shutdown evitando conflictos, se configura la interface range fa0/1-2 con el comando de encapsulación switchport trunk encapsulation dot1q, y implementamos la interface con el comando switchport mode trunk direccionándola a la vlan 56 nativa switchport trunk native vlan 56, creamos la EtherChannel para que utilice el grupo de interfaces fa0/1-2 con el comando channel-group 1 mode active y usar LACP creando el grupo 1, ahora ingresamos a la interfaz con interface Port-channel 1, configurar las troncales, se configura un puerto de acceso para la vlan 30 Invitados que use la fa0/18 con el comando switchport access vlan 30, configuración de seguridad para los puertos de acceso que permita 4 direcciones MAC, se activa la seguridad en la interfaz estableciendo máximo 4 direcciones MAC con switchport port-security maximum 4, aseguramos todas las interfaces sin usar asignándolas a la vlan 50-Usuarios indicando que no están utilizándose y apagamos con shutdown, siendo estas fa0/3-17, fa0/19-24 y g0/1-2, finalmente se activa el rango de interfaz fa0/1-2 con no shutdown.

Figura 17 Verificación Configuración VLAN S2



Fuente: Autor

Figura 18 Verificación Configuración Trunk S2

```

S2#show interface trunk

Port      Mode      Encapsulation  Status      Native vlan
Pol       on        802.1q         trunking    56

Port      Vlans allowed on trunk
Pol       1-1005

Port      Vlans allowed and active in management domain
Pol       1,20,30,40,50,56

Port      Vlans in spanning tree forwarding state and not pruned
Pol       1,20,30,40,50,56

S2#
    
```

Fuente: Autor

Figura 19 Verificación Configuración EtherChannel S2

```

S2#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Pol(SU)        LACP       Fa0/1(P) Fa0/2(P)
S2#

```

Fuente: Autor

Figura 20 Verificación Configuración VLAN Brief

```

S2#show vlan brief

VLAN Name                             Status    Ports
-----+-----+-----+-----
1      default                               active    Gig0/1, Gig0/2
20     Docentes                               active
30     Estudiantes                             active    Fa0/18
40     Invitados                               active
50     Usuarios                                active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24

56     Native                                active
1002   fddi-default                            active
1003   token-ring-default                       active
1004   fddinet-default                         active
1005   trnet-default                           active
S2#

```

Fuente: Autor

Tabla 16 Activación interface fa0/1-2 en s1 y S2

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

Fuente: Autor

Parte 3: Configurar soporte de host

Paso 1: Configure R1 Escenario 2

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Configuración de soporte de host en Router

| Tarea | Especificación |
|---|---|
| Configure Default Routing Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0 | R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)#ipv6 route ::/0 loopback 0 |
| Configurar IPv4 DHCP para VLAN 2 | R1(config)#ip dhcp excluded-address 10.64.8.1 10.64.8.52 R1(config)#ip dhcp pool vlan2-Docentes R1(dhcp-config)#network 10.64.8.0 255.255.255.192 |

| | |
|---|---|
| <p>Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente.</p> <p>Asigne el nombre de dominio unad-ccna-sa.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada</p> | <pre>R1(dhcp-config)#default-router 10.64.8.1 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit</pre> |
| <p>Configurar DHCP IPv4 para VLAN 3</p> <p>Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente.</p> <p>Asigne el nombre de dominio unad-ccna-sb.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz</p> | <pre>R1(config)#ip dhcp excluded-address 10.64.8.65 10.64.8.84 R1(config)#ip dhcp pool vlan3- Estudiantes R1(dhcp-config)#network 10.64.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.64.8.65 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#exit</pre> |

| | |
|---------------------------------------|--|
| del router para la subred involucrada | |
|---------------------------------------|--|

Fuente: Autor

En el Router se asignan las rutas predeterminadas IPv4 `ip route 0.0.0.0 0.0.0.0 loopback 0` y IPv6 `ipv6 route ::/0 loopback 0`, con las cuales se direcciona la interfaz Loopback 0 (Lo0), estas rutas estáticas para conectar a Internet, se configura IPv4 DHCP para vlan 20 Estudiantes usando solamente las ultimas 10 direcciones de subred, rango 10.64.8.1 10.64.8.52, para ello se procede a excluir estas 10 direcciones el comando `ip dhcp excluded-address 10.64.8.1 10.64.8.52`, y para el pool de DHCP `ip dhcp pool vlan20 Estudiantes`, red y mascara de red `network 10.64.8.0 255.255.255.192`, la puerta de enlace predeterminada `default-router 10.64.8.1`, nombre de dominio `domain-name ccna-sa.com`, finalmente se configura DHCP IPv4 para vlan 30 Invitados y grupo DHCP conformado por las ultimas 10 direcciones con sus especificaciones, procedemos a configurar IPv4 DHCP para vlan 30 Estudiantes usando solamente por las ultimas 10 direcciones de subred rango 10.64.8.65 – 10.64.8.84, se aplica para excluir estas 10 direcciones el comando `ip dhcp excluded-address 10.64.8.65 10.64.8.84`, y para el pool de DHCP `ip dhcp pool vlan30 Estudiantes`, red y mascara de red `network 10.64.8.64 255.255.255.224`, puerta de enlace predeterminada `default-router 10.64.8.65`, nombre de dominio `domain-name ccna-sa.com`

Figura 21 Verificación Configuración R1

```

R1>enable
Password:
R1#show run | section dhcp
ip dhcp excluded-address 10.64.8.1 10.64.8.52
ip dhcp excluded-address 10.64.8.65 10.64.8.84
ip dhcp pool vlan20-Doctentes
  network 10.64.8.0 255.255.255.192
  default-router 10.64.8.1
  domain-name ccna-sa.com
ip dhcp pool vlan30-Estudiantes
  network 10.64.8.64 255.255.255.224
  default-router 10.64.8.65
  domain-name ccna-sa.com
R1#

```

Fuente: Autor

Configurar los servidores Escenario 2

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

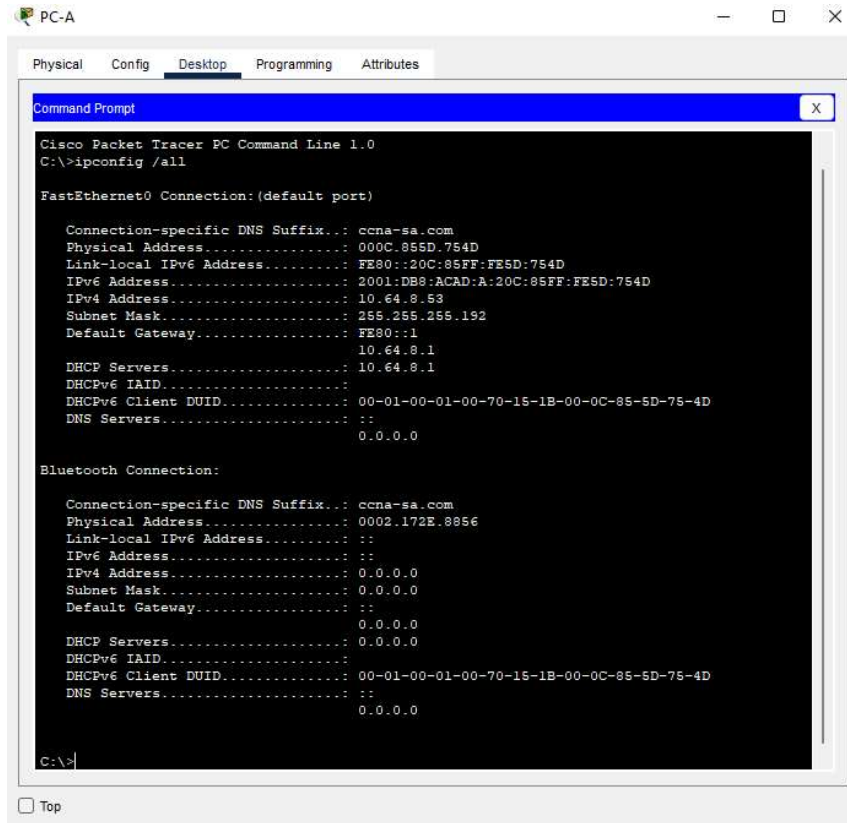
En las PC-A y B se activa el DHCP para IPv4 y configuración automática para IPv6

Tabla 18 Configuración de red del PC-A

| Configuración de red de PC-A | |
|------------------------------|-----------------|
| Descripción | Datos por DHCP |
| Dirección física | 0060.7042.6446 |
| Dirección IP | 10.64.8.53 |
| Máscara de subred | 255.255.255.192 |
| Gateway predeterminado | 10.64.8.1 |
| Gateway predeterminado IPv6 | FE80::1 |

Fuente: Autor

Figura 22 Verificación Configuración PC-A



Fuente: Autor

Tabla 19 Configuración de red del PC-A

| Configuración de red de PC-B | |
|---------------------------------|-----------------|
| Descripción | Datos por DHCP |
| Dirección física | Datos por DHCP |
| Dirección IP | 10.64.8.65 |
| Máscara de subred | 255.255.255.224 |
| Gateway predeterminado | 10.64.8.65 |
| Gateway predeterminado IPv6 | FE80::1 |

Fuente: Autor

Figura 23 Verificación Configuración PC-B

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...: ccna-sa.com
Physical Address.....: 00D0.D35A.B6C8
Link-local IPv6 Address.....: FE80::2D0:D3FF:FE5A:B6C8
IPv6 Address.....: 2001:DB8:ACAD:B:2D0:D3FF:FE5A:B6C8
IPv4 Address.....: 10.64.8.85
Subnet Mask.....: 255.255.255.224
Default Gateway.....: FE80::1
                        10.64.8.65
DHCP Servers.....: 10.64.8.65
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-A1-9E-C0-76-00-D0-D3-5A-B6-C8
DNS Servers.....:
                        0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix...: ccna-sa.com
Physical Address.....: 0005.5E3B.4D22
Link-local IPv6 Address.....:
IPv6 Address.....:
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....:
                        0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-A1-9E-C0-76-00-D0-D3-5A-B6-C8
DNS Servers.....:
                        0.0.0.0

C:\>
```

Fuente: Autor

Probar y verificar la conectividad de extremo a extremo

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

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

Tabla 20 Verificación de los dispositivos de red

| Desde | A | | Dirección IP | Resultados de ping | |
|-------|-----------------|------------|-----------------------|--|--|
| PC-A | R1, G0/0/1.2 | IPv4 | 10.64.8.1 | Si hay respuesta | |
| | | IPv6 | 2001:db8:acad:a: :1 | Si hay respuesta | |
| | R1, G0/0/1.3 | IPv4 | 10.64.8.65 | Si hay respuesta | |
| | | IPv6 | 2001:db8:acad:b: :1 | Si hay respuesta | |
| | R1, G0/0/1.4 | IPv4 | 10.64.8.97 | Si hay respuesta | |
| | | IPv6 | 2001:db8:acad:c: :1 | Si hay respuesta | |
| | S1, VLAN 4 | IPv4 | 10.64.8.98 | Si hay respuesta | |
| | | IPv6 | 2001:db8:acad:c: :98 | Se configura puerta de enlace IPv6 route ::/0 2001:db8:acad:c::1 y Si hay respuesta | |
| | Desde | A | | Dirección IP | Resultados de ping |
| | | S2, VLAN 4 | IPv4 | 10.64.8.99 | Si hay respuesta |
| | | | IPv6 | 2001:db8:acad:c: :99 | Se configura puerta de enlace IPv6 route ::/0 2001:db8:acad:c::1 y Si hay respuesta |
| | | PC-B | IPv4 | 10.64.8.85 | Si hay respuesta |
| | | IPv6 | 2001:db8:acad:b: :50 | Si hay respuesta | |
| | R1 Bucle 0 | IPv4 | 209.165.201.1 | Si hay respuesta | |
| | | IPv6 | 2001:db8:acad:209: :1 | Si hay respuesta | |
| PC-B | R1 Bucle 0 | IPv4 | 09.165.201.1 | Si hay respuesta | |

| | | | | |
|--|-----------------|------|-----------------------|------------------|
| | | IPv6 | 2001:db8:acad:209: :1 | Si hay respuesta |
| | R1, G0/0/1.2 | IPv4 | 10.64.8.1 | Si hay respuesta |
| | | IPv6 | 2001:db8:acad:a: :1 | Si hay respuesta |
| | R1, G0/0/1.3 | IPv4 | 10.64.8.65 | Si hay respuesta |
| | | IPv6 | 2001:db8:acad:b: :1 | Si hay respuesta |
| | R1, G0/0/1.4 | IPv4 | 10.64.8.97 | Si hay respuesta |
| | | IPv6 | 2001:db8:acad:c: :1 | Si hay respuesta |
| | S1, VLAN 4 | IPv4 | 10.64.8.98 | Si hay respuesta |
| | | IPv6 | 2001:db8:acad:c: :98 | Si hay respuesta |
| | S2, VLAN 4 | IPv4 | 10.64.8.99. | Si hay respuesta |
| | | IPv6 | 2001:db8:acad:c: :99 | Si hay respuesta |

Fuente: Autor

Figura 24 Ping desde PC-A a R1, G0/0/1.2 – Ipv4 10.64.8.1

The screenshot shows a Cisco Packet Tracer PC Command Line interface for PC-A. The 'Desktop' tab is active. The command prompt shows the execution of a ping command to 10.64.8.1. The output indicates that 4 packets were sent and received successfully with 0% loss. The round trip times are all 0ms.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.64.8.1

Pinging 10.64.8.1 with 32 bytes of data:

Reply from 10.64.8.1: bytes=32 time<1ms TTL=255
Reply from 10.64.8.1: bytes=32 time<1ms TTL=255
Reply from 10.64.8.1: bytes=32 time=1ms TTL=255
Reply from 10.64.8.1: bytes=32 time<1ms TTL=255

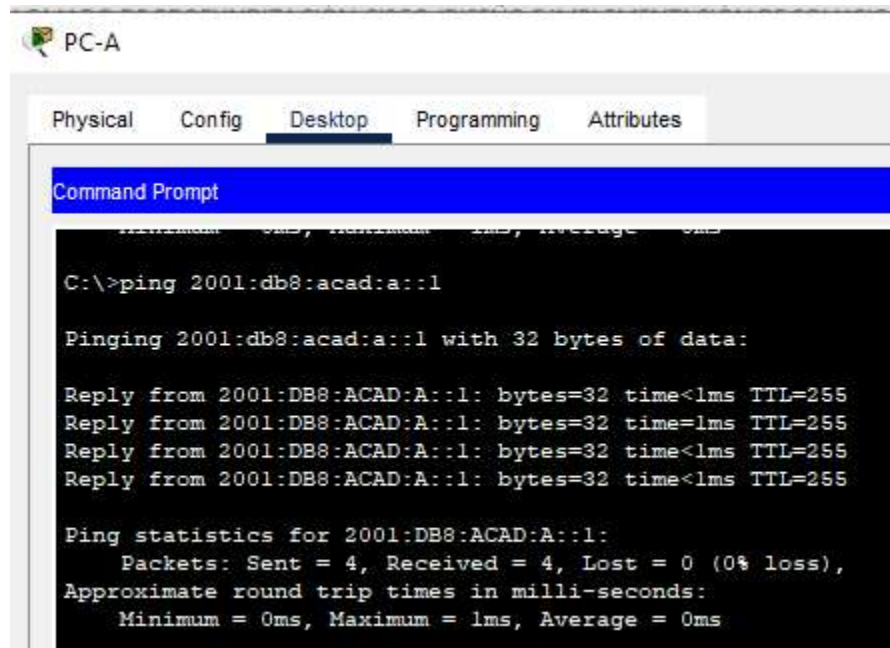
Ping statistics for 10.64.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>

```

Fuente: Autor

Figura 25 Ping desde PC-A a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a::1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:a::1

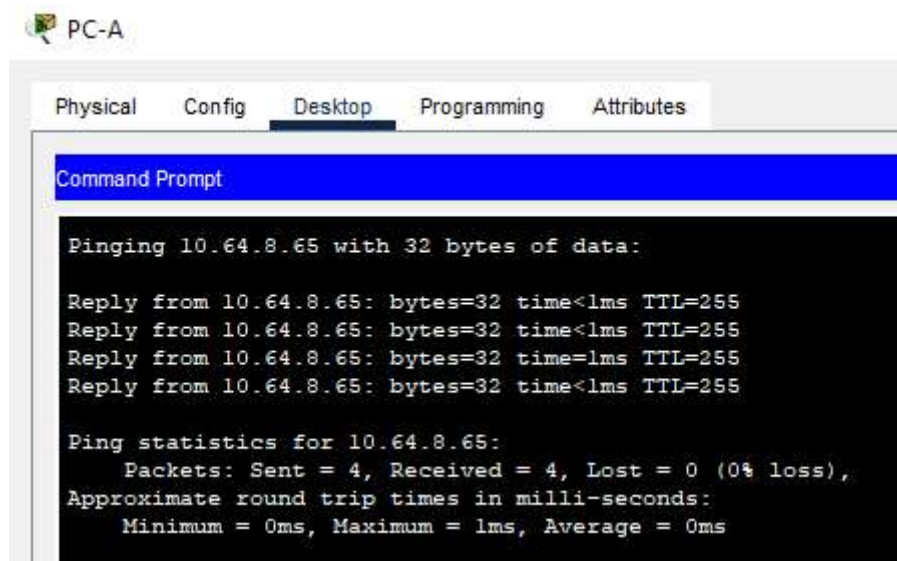
Pinging 2001:db8:acad:a::1 with 32 bytes of data:

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 = 1ms, Average = 0ms
```

Fuente: Autor

Figura 26 Ping desde PC-A a R1, G0/0/1.3 – Ipv4 10.64.8.65



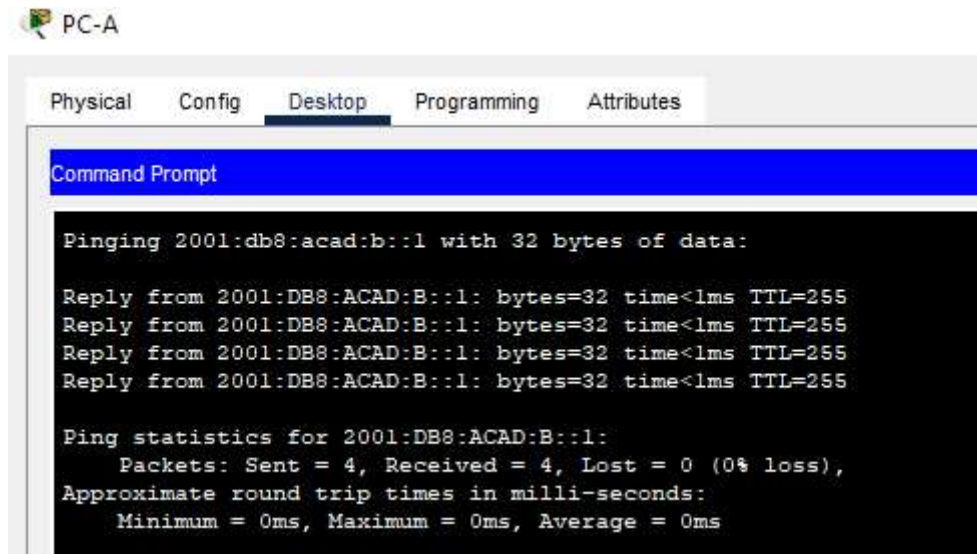
```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 10.64.8.65 with 32 bytes of data:

Reply from 10.64.8.65: bytes=32 time<1ms TTL=255
Reply from 10.64.8.65: bytes=32 time<1ms TTL=255
Reply from 10.64.8.65: bytes=32 time=1ms TTL=255
Reply from 10.64.8.65: bytes=32 time<1ms TTL=255

Ping statistics for 10.64.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autor

Figura 27 Ping desde PC-A a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b::1



The screenshot shows the 'Desktop' tab of the PC-A interface. The Command Prompt window displays the following text:

```
Command Prompt

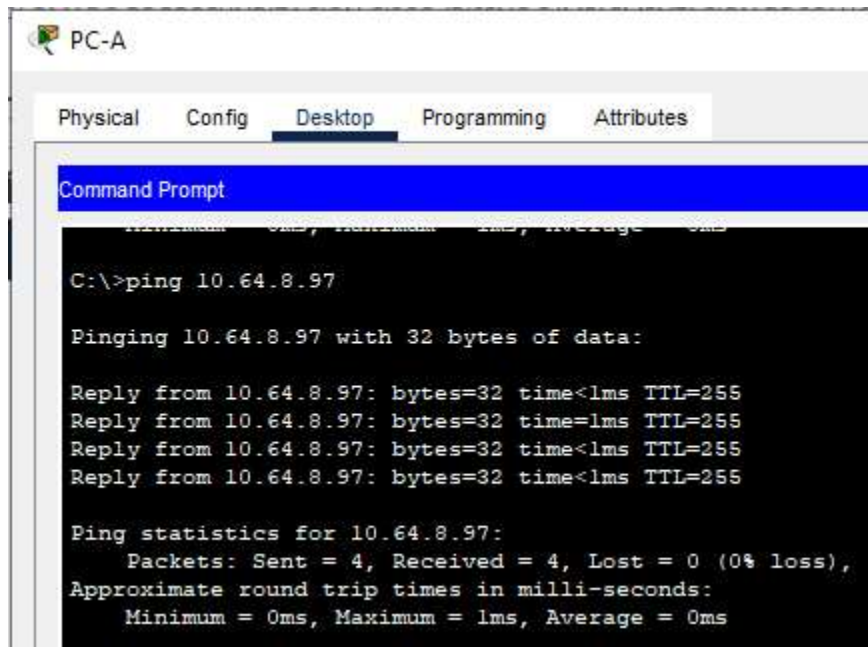
Pinging 2001:db8:acad:b::1 with 32 bytes of data:

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

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

Fuente: Autor

Figura 28 Ping desde PC-A a R1, G0/0/1.4 – Ipv4 10.64.8.97



The screenshot shows the 'Desktop' tab of the PC-A interface. The Command Prompt window displays the following text:

```
Command Prompt

C:\>ping 10.64.8.97

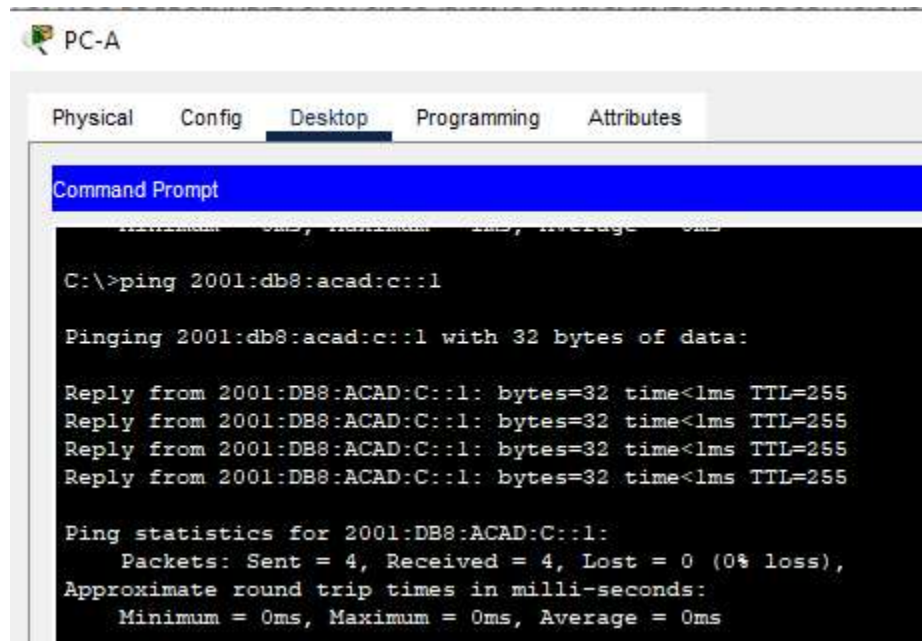
Pinging 10.64.8.97 with 32 bytes of data:

Reply from 10.64.8.97: bytes=32 time<1ms TTL=255
Reply from 10.64.8.97: bytes=32 time<1ms TTL=255
Reply from 10.64.8.97: bytes=32 time<1ms TTL=255
Reply from 10.64.8.97: bytes=32 time<1ms TTL=255

Ping statistics for 10.64.8.97:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autor

Figura 29 Ping desde PC-A a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c::1



The screenshot shows a Windows Command Prompt window titled "PC-A" with the "Desktop" tab selected. The command prompt displays the execution of a ping command to the IPv6 address 2001:db8:acad:c::1. The output shows four successful replies, each with 32 bytes of data, a time of less than 1ms, and a TTL of 255. The ping statistics indicate that 4 packets were sent and received, with 0% loss, and all round trip times were 0ms.

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

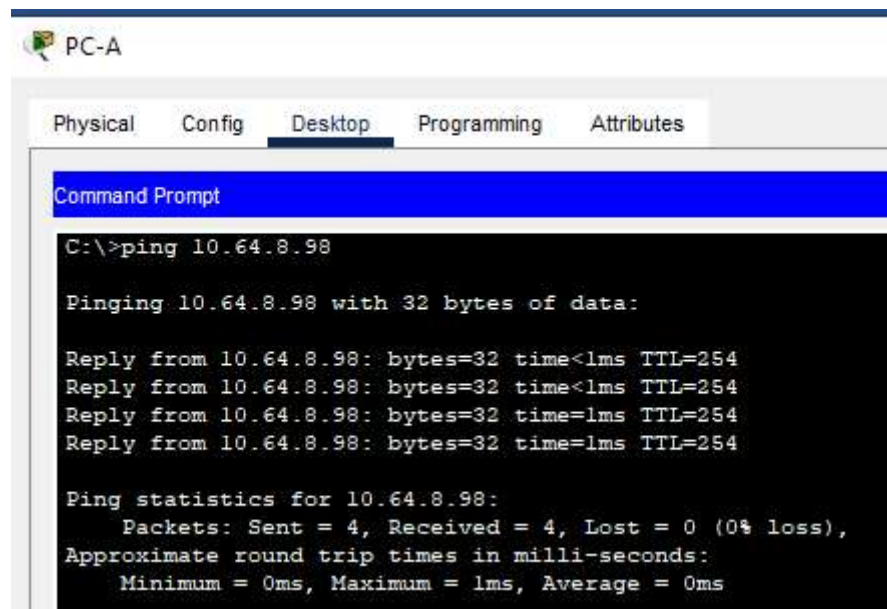
Pinging 2001:db8:acad:c::1 with 32 bytes of data:

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
```

Fuente: Autor

Figura 30 Ping desde PC-A a S1 VLAN4 – Ipv4 10.64.8.98



The screenshot shows a Windows Command Prompt window titled "PC-A" with the "Desktop" tab selected. The command prompt displays the execution of a ping command to the IPv4 address 10.64.8.98. The output shows four successful replies, each with 32 bytes of data, a time of less than 1ms, and a TTL of 254. The ping statistics indicate that 4 packets were sent and received, with 0% loss, and all round trip times were 0ms.

```
C:\>ping 10.64.8.98

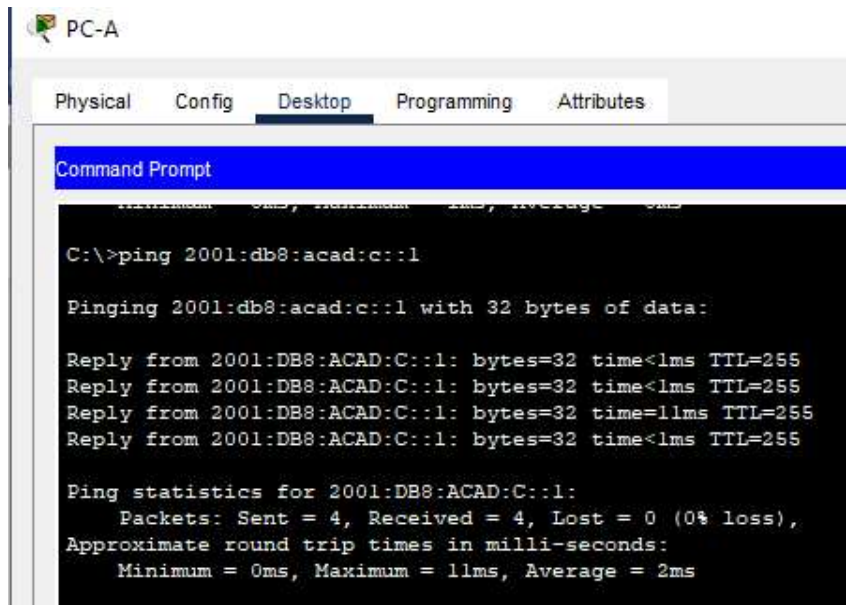
Pinging 10.64.8.98 with 32 bytes of data:

Reply from 10.64.8.98: bytes=32 time<1ms TTL=254
Reply from 10.64.8.98: bytes=32 time<1ms TTL=254
Reply from 10.64.8.98: bytes=32 time<1ms TTL=254
Reply from 10.64.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.64.8.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Autor

Figura 31 Ping desde PC-A a S1 VLAN40 – Ipv6 2001:db8:acad:c::1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:c::1

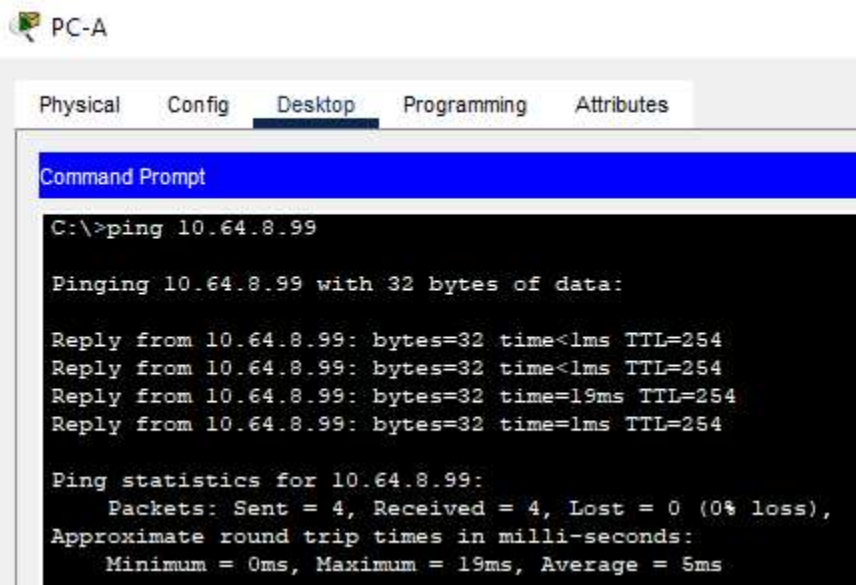
Pinging 2001:db8:acad:c::1 with 32 bytes of data:

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=11ms 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 = 11ms, Average = 2ms
```

Fuente: Autor

Figura 32 Ping desde PC-A a S2 VLAN4 – Ipv4 10.64.8.99



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.64.8.99

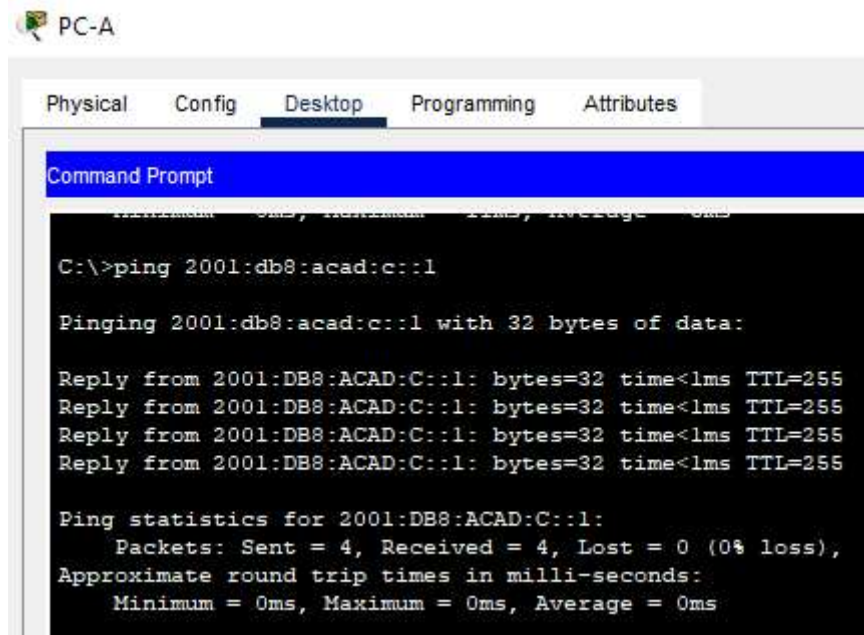
Pinging 10.64.8.99 with 32 bytes of data:

Reply from 10.64.8.99: bytes=32 time<1ms TTL=254
Reply from 10.64.8.99: bytes=32 time<1ms TTL=254
Reply from 10.64.8.99: bytes=32 time=19ms TTL=254
Reply from 10.64.8.99: bytes=32 time=1ms TTL=254

Ping statistics for 10.64.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 19ms, Average = 5ms
```

Fuente: Autor

Figura 33 Ping desde PC-A a S2 VLAN4 – Ipv6 2001:db8:acad:c::1



The screenshot shows the Command Prompt window on PC-A. The 'Desktop' tab is selected. The command prompt displays the following output:

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

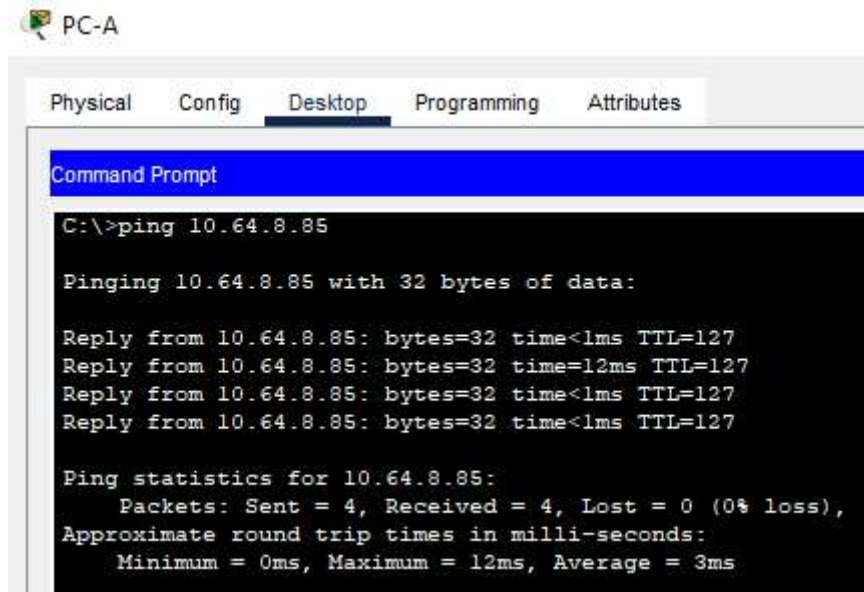
Pinging 2001:db8:acad:c::1 with 32 bytes of data:

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
```

Fuente: Autor

Figura 34 Ping desde PC-A a PC-B – Ipv4 10.64.8.85



The screenshot shows the Command Prompt window on PC-A. The 'Desktop' tab is selected. The command prompt displays the following output:

```
C:\>ping 10.64.8.85

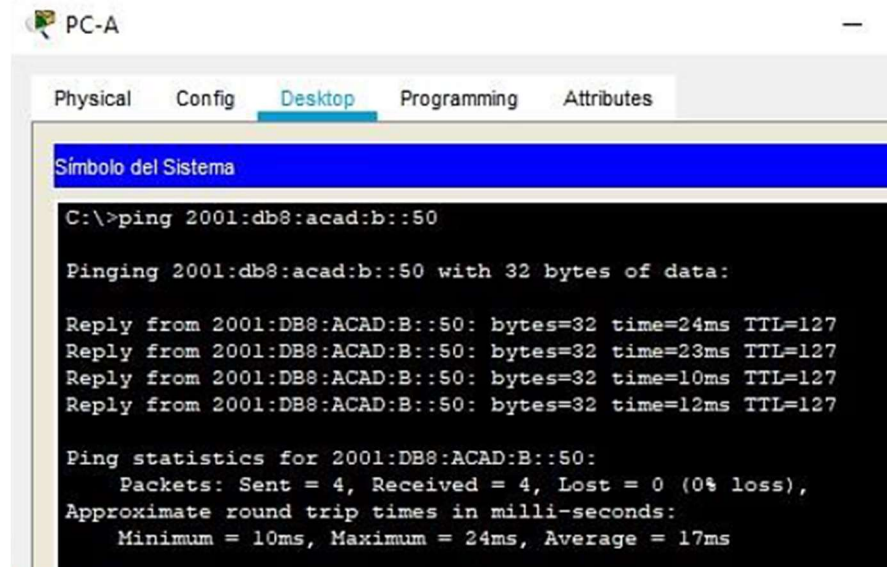
Pinging 10.64.8.85 with 32 bytes of data:

Reply from 10.64.8.85: bytes=32 time<1ms TTL=127
Reply from 10.64.8.85: bytes=32 time=12ms TTL=127
Reply from 10.64.8.85: bytes=32 time<1ms TTL=127
Reply from 10.64.8.85: bytes=32 time<1ms TTL=127

Ping statistics for 10.64.8.85:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

Fuente Autor

Figura 35 Ping desde PC-A a PC-B – Ipv6 2001:db8:acad:b::50



```
PC-A
Physical Config Desktop Programming Attributes
Símbolo del Sistema
C:\>ping 2001:db8:acad:b::50

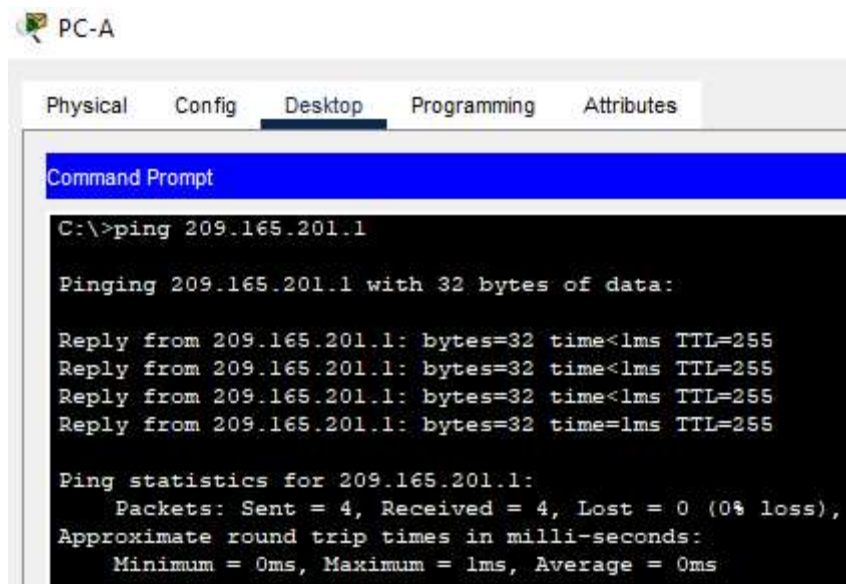
Pinging 2001:db8:acad:b::50 with 32 bytes of data:

Reply from 2001:DB8:ACAD:B::50: bytes=32 time=24ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=23ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=10ms TTL=127
Reply from 2001:DB8:ACAD:B::50: bytes=32 time=12ms TTL=127

Ping statistics for 2001:DB8:ACAD:B::50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 24ms, Average = 17ms
```

Fuente: Autor

Figura 36 Ping desde PC-A a R1 Bucle 0 – IPv4 209.165.201.1



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 209.165.201.1

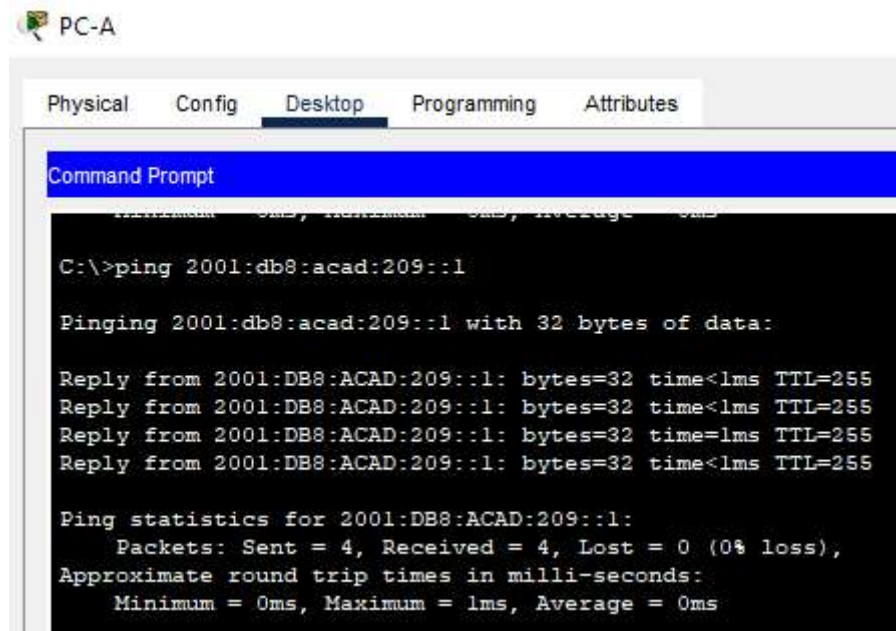
Pinging 209.165.201.1 with 32 bytes of data:

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 = lms, Average = 0ms
```

Fuente: Autor

Figura 37 Ping desde PC-A a R1 Bucle 0 – Ipv6 2001:db8:acad:209::1



The screenshot shows the Command Prompt window on PC-A. The window title is "Command Prompt" and the tabs are "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. The command prompt shows the following text:

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

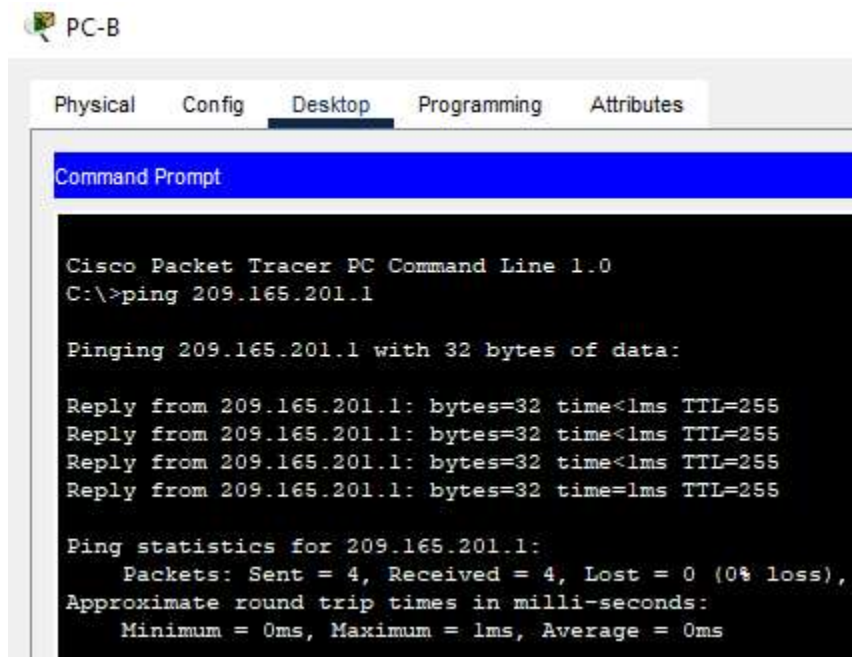
Pinging 2001:db8:acad:209::1 with 32 bytes of data:

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 = 1ms, Average = 0ms
```

Fuente: Autor

Figura 38 Ping desde PC-B a R1 Bucle 0 – Ipv4 209.165.201.1



The screenshot shows the Command Prompt window on PC-B. The window title is "Command Prompt" and the tabs are "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. The command prompt shows the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.1

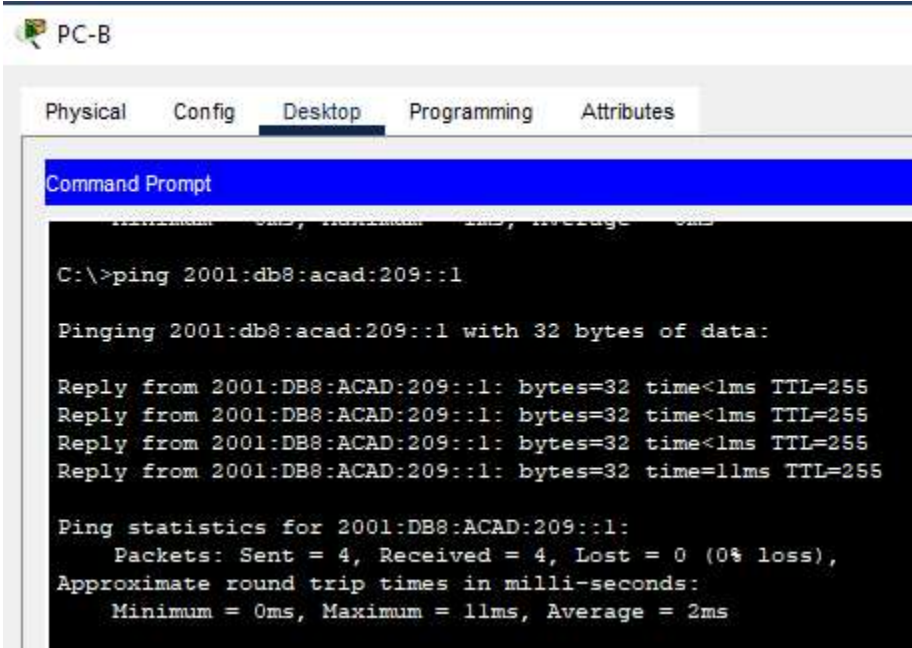
Pinging 209.165.201.1 with 32 bytes of data:

Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time<1ms TTL=255
Reply from 209.165.201.1: bytes=32 time=1ms 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 = 1ms, Average = 0ms
```

Fuente: Autor

Figura 39 Ping desde PC-B a R1 Bucle 0 – Ipv6 2001:db8:acad:209::1



```
PC-B
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 2001:db8:acad:209::1

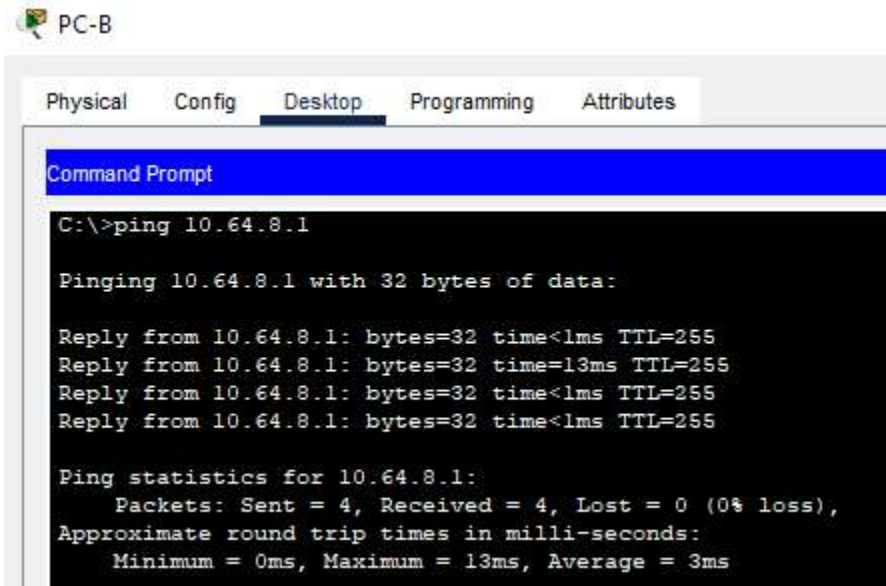
Pinging 2001:db8:acad:209::1 with 32 bytes of data:

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=11ms 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 = 11ms, Average = 2ms
```

Fuente: Autor

Figura 40 Ping desde PC-B a R1, G0/0/1.2 – Ipv4 10.64.8.1



```
PC-B
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 10.64.8.1

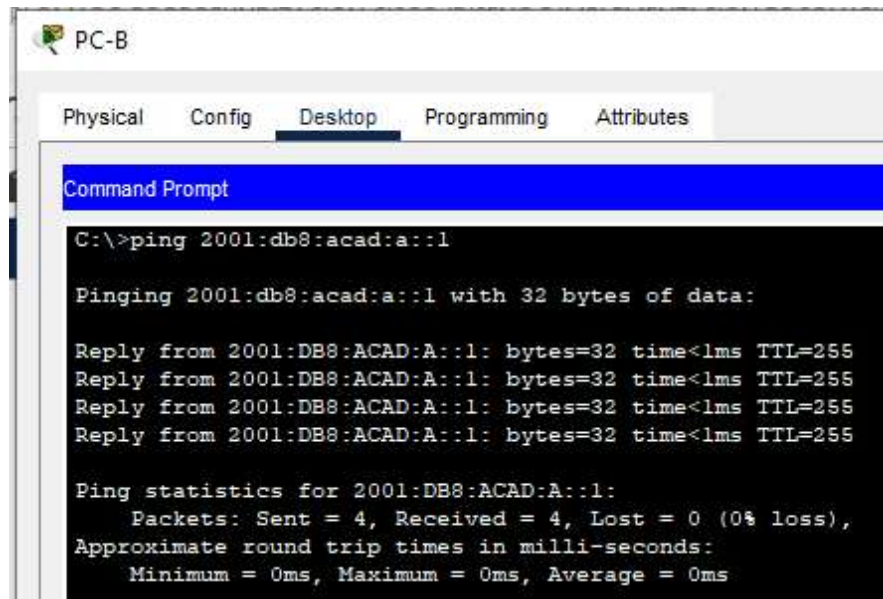
Pinging 10.64.8.1 with 32 bytes of data:

Reply from 10.64.8.1: bytes=32 time<1ms TTL=255
Reply from 10.64.8.1: bytes=32 time=13ms TTL=255
Reply from 10.64.8.1: bytes=32 time<1ms TTL=255
Reply from 10.64.8.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.64.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

Fuente: Autor

Figura 41 Ping desde PC-B a R1, G0/0/1.2 – Ipv6 2001:db8:acad:a::1



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:a::1

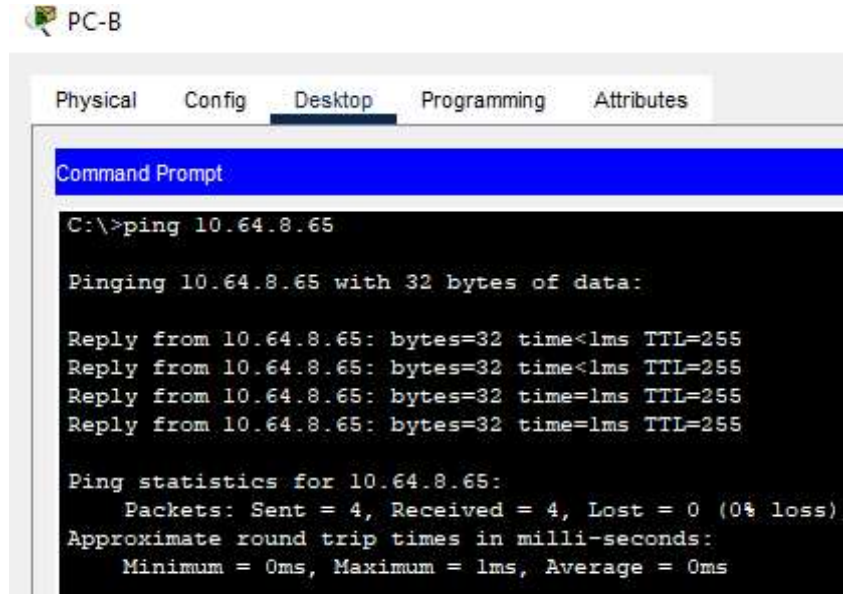
Pinging 2001:db8:acad:a::1 with 32 bytes of data:

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
```

Fuente: Autor

Figura 42 Ping desde PC-B a R1, G0/0/1.3 – Ipv4 10.64.8.65



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.64.8.65

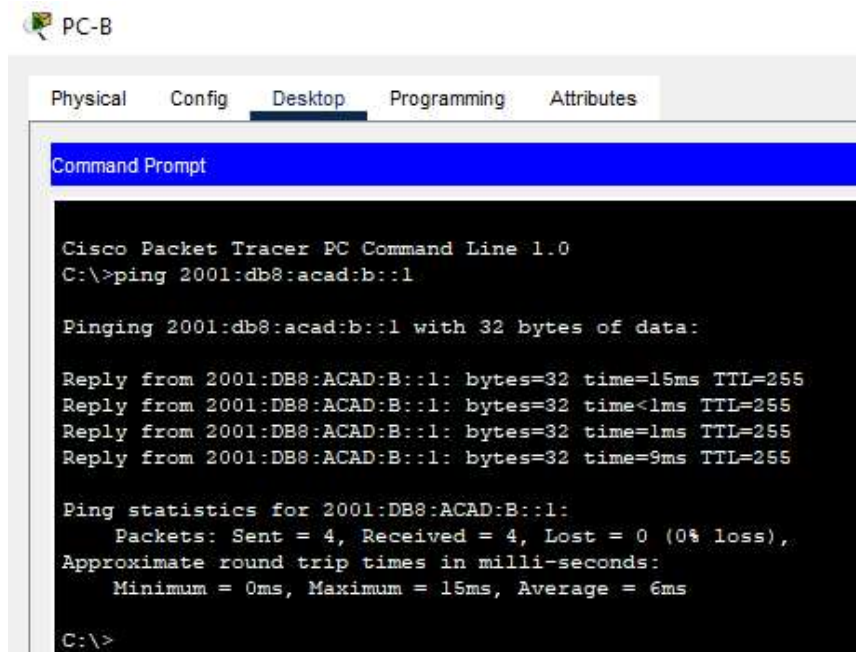
Pinging 10.64.8.65 with 32 bytes of data:

Reply from 10.64.8.65: bytes=32 time<lms TTL=255
Reply from 10.64.8.65: bytes=32 time<lms TTL=255
Reply from 10.64.8.65: bytes=32 time=lms TTL=255
Reply from 10.64.8.65: bytes=32 time=lms TTL=255

Ping statistics for 10.64.8.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = lms, Average = 0ms
```

Fuente: Autor

Figura 43 Ping desde PC-B a R1, G0/0/1.3 – Ipv6 2001:db8:acad:b::1



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC-B. The 'Desktop' tab is selected. The command prompt displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 2001:db8:acad:b::1

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

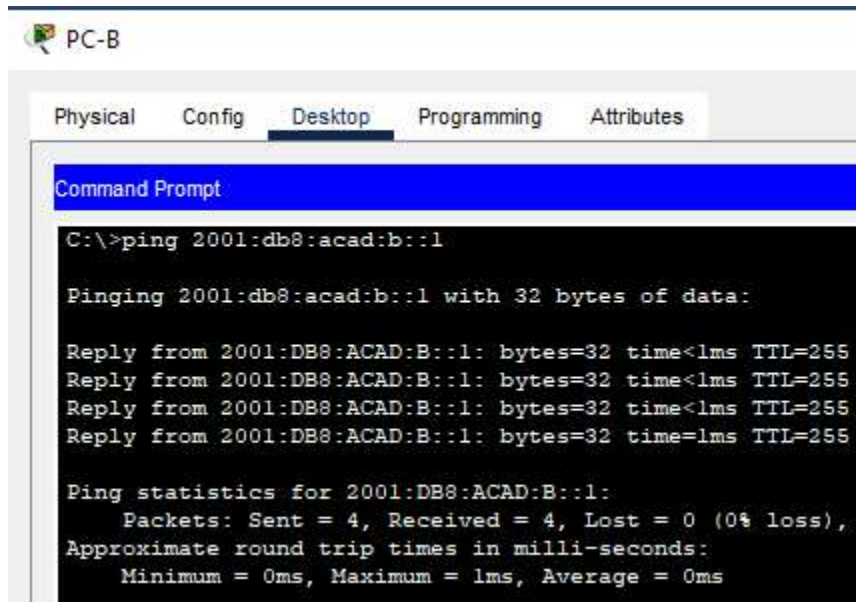
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=15ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=1ms TTL=255
Reply from 2001:DB8:ACAD:B::1: bytes=32 time=9ms TTL=255

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 = 15ms, Average = 6ms

C:\>
```

Fuente: Autor

Figura 44 Ping desde PC-B a R1, G0/0/1.4 – Ipv4 10.64.8.97



The screenshot shows a Cisco Packet Tracer PC Command Line window for PC-B. The 'Desktop' tab is selected. The command prompt displays the following text:

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

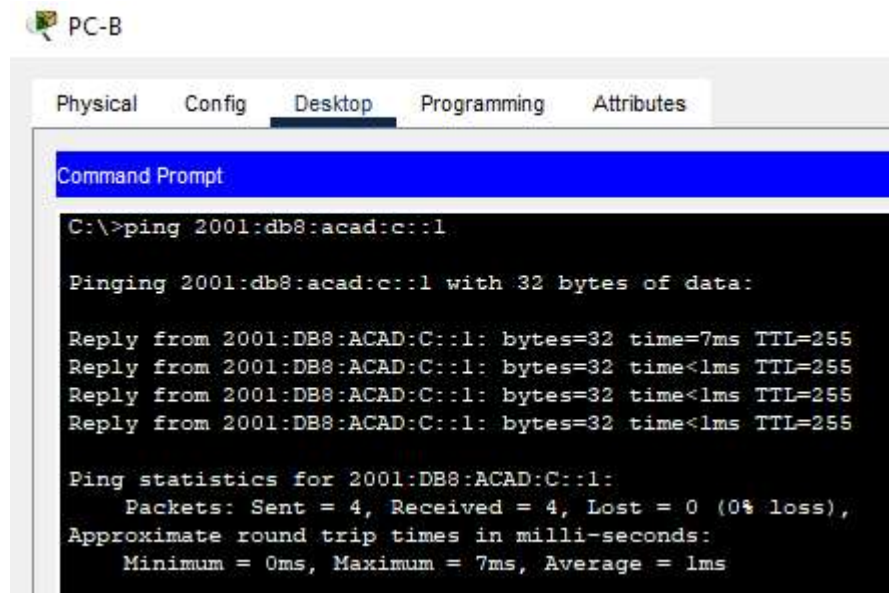
Pinging 2001:db8:acad:b::1 with 32 bytes of data:

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
```

Fuente: Autor

Figura 45 Ping desde PC-B a R1, G0/0/1.4 – Ipv6 2001:db8:acad:c::1



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:c::1

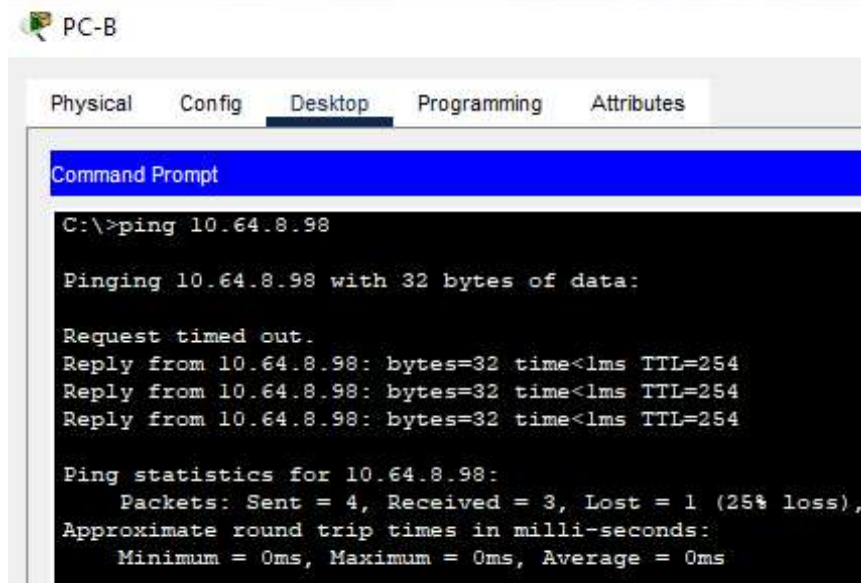
Pinging 2001:db8:acad:c::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::1: bytes=32 time=7ms 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 = 7ms, Average = 1ms
```

Fuente: Autor

Figura 46 Ping desde PC-B a S1 VLAN4 – Ipv4 10.64.8.98



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.64.8.98

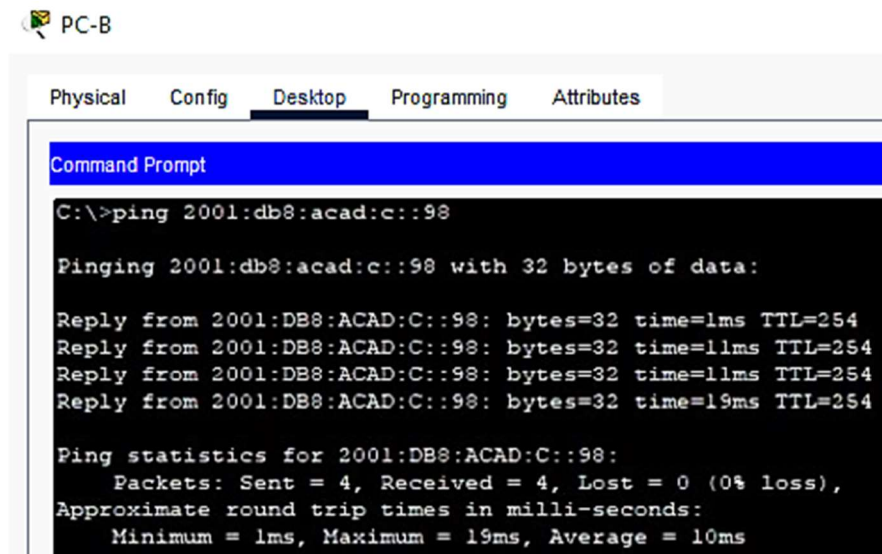
Pinging 10.64.8.98 with 32 bytes of data:

Request timed out.
Reply from 10.64.8.98: bytes=32 time<1ms TTL=254
Reply from 10.64.8.98: bytes=32 time<1ms TTL=254
Reply from 10.64.8.98: bytes=32 time<1ms TTL=254

Ping statistics for 10.64.8.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fuente: Autor

Figura 47 Ping desde PC-B a S1 VLAN4 – Ipv6 2001:db8:acad:c::98



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 2001:db8:acad:c::98

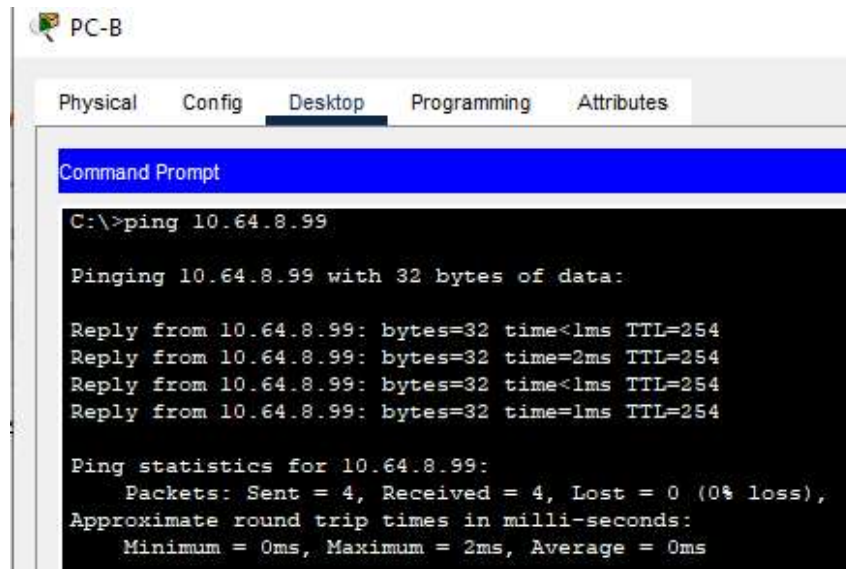
Pinging 2001:db8:acad:c::98 with 32 bytes of data:

Reply from 2001:DB8:ACAD:C::98: bytes=32 time=1ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::98: bytes=32 time=19ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 10ms
```

Fuente Autor

Figura 48 Ping desde PC-B a S2 VLAN40 – Ipv4 10.64.8.99



```
PC-B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.64.8.99

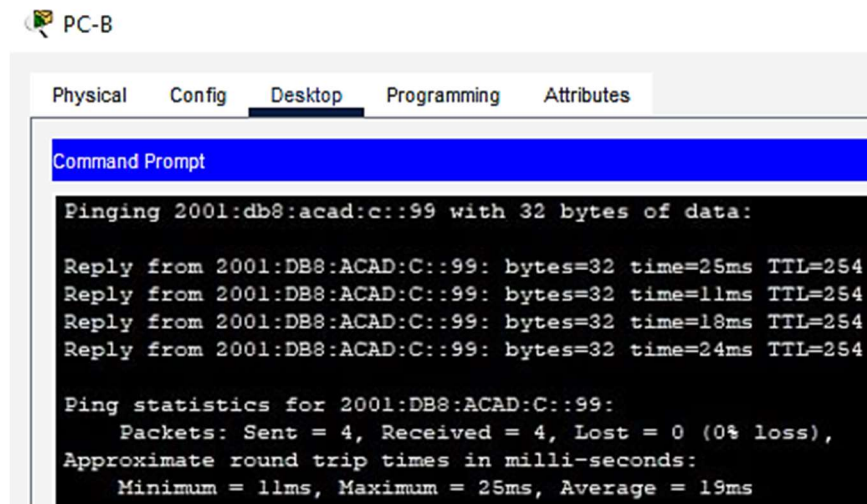
Pinging 10.64.8.99 with 32 bytes of data:

Reply from 10.64.8.99: bytes=32 time<1ms TTL=254
Reply from 10.64.8.99: bytes=32 time=2ms TTL=254
Reply from 10.64.8.99: bytes=32 time<1ms TTL=254
Reply from 10.64.8.99: bytes=32 time=1ms TTL=254

Ping statistics for 10.64.8.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Fuente: Autor

Figura 49 Ping desde PC-B a S2 VLAN40 – Ipv6 2001:db8:acad:c::99



The image shows a terminal window titled "PC-B" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, and the terminal displays the output of a ping command. The output shows four successful replies from the destination address 2001:DB8:ACAD:C::99, with varying round-trip times (11ms, 18ms, 24ms, and 25ms) and a TTL of 254. The ping statistics indicate that all four packets were sent and received, with 0% loss. The approximate round-trip times are: Minimum = 11ms, Maximum = 25ms, and Average = 19ms.

```
Command Prompt

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

Reply from 2001:DB8:ACAD:C::99: bytes=32 time=25ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=11ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=18ms TTL=254
Reply from 2001:DB8:ACAD:C::99: bytes=32 time=24ms TTL=254

Ping statistics for 2001:DB8:ACAD:C::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 25ms, Average = 19ms
```

Fuente Autor

CONCLUSIONES

Se logro utilizar el simulador Packet Tracen en la solución de una problemática al realizar la red solicitada en el simulador 1 que consistía en la conexión de un Router, un Switch y dos equipos de cómputo, realizando la conexión de los diferentes componentes de esta red de internet se y se asignó el direccionamiento IP, configuración de los diferentes dispositivos que hacen parte de esta red y desarrollo de pruebas de funcionamiento.

Se logra comprender como realizar la configuración de un Router y un Switch a través de los diferentes comandos utilizables en la consola, por el medio de los cuales utilizamos por ejemplo el comando Name para asignar el nombre de los dispositivos, igualmente la configuración de VLANs para la red LAN1 y LAN2, la configuración de los puertos utilizados, seguridad de los dispositivos acorde a lo solicitado en la actividad.

En el desarrollo del escenario 2 se realizan los procesos según la topología seleccionada se priorizan las configuraciones de los Routers y Switches con el objetivo de lograr la administración de la red con la configuración de los servidores locales y remotos mediante SSH teniendo en cuenta los protocolos e interfaces lógicas y físicas, configuración de passwords de seguridad, el uso del modo privilegiado de acceso de los usuarios, contraseñas encriptadas y los mensajes (banner-motd) entre los procesos que nos dan la seguridad de la red.

Se tuvo un acercamiento a las diferentes topologías de red, en el desarrollo de este diplomado en CCNA CISCO afianzamos nuestros conocimientos y los diferentes tipos de redes y el cómo podemos realizar la configuración IPV4 para este tipo de redes como lo hemos realizado En el escenario 1 y 2, esto afianza nuestros conocimientos y nuestra confianza para desarrollo de nuestras carreras y en el ámbito profesional y laboral.

BIBLIOGRAFÍA

BITACORA, Byte. “Configurar DHCP en Router CISCO”. {En línea}. (18 de julio de 2017) {22 de noviembre de 2022}. Disponible en:

<https://bitacorabyte.wordpress.com/2017/07/18/configurar-dhcp-en-router-cisco/>

CASTAÑO, R. R. J., y López, F. J. “Redes locales. Madrid, ES: Macmillan Iberia, S.A.” (pp. 214 – 227.) {En línea}. (2013) {22 de noviembre de 2022}. Disponible en:

<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=215>

CASTAÑO, R. R. J., y López, F. J. “Redes locales. Madrid, ES: Macmillan Iberia, S.A.” (pp. 232 - 247) {En línea}. (2013). {22 de noviembre de 2022}. Disponible en:

<https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/43257?page=233>

CISCO, cisco. “Configuración de una puerta de enlace de último recurso mediante comandos IP”. {En línea} (10 de agosto de 2005). {22 de noviembre de 2022}. Disponible en:

<https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocolrip/16448-default.html>

CISCO, cisco. “División de redes IP en subredes. Fundamentos de Networking”. {En línea} (2019). {22 de noviembre de 2022}. Disponible en:

<https://static-courseassets.s3.amazonaws.com/ITN6/es/index.html#8>

CISCO, cisco. “Asignación de direcciones IPv6. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/12.0.1>

CISCO, cisco. “Capa de red. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/8.0.1>

CISCO, cisco. “Capa de transporte. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/14.0.1>

CISCO, cisco. “Capa física. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/4.0.1>

CISCO, cisco. “Conceptos de Switching”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/srwe/2.0.1>

CISCO, cisco. “Configuración básica de dispositivos”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/srwe/1.0.1>

CISCO, cisco. “ICMP. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/13.0.1>

CISCO, cisco. “Las redes en la actualidad. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/5.0.1>

CISCO, cisco. “Protocolos y modelos. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/3.0.1>

CISCO, cisco. “Switching Ethernet. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/7.0.1>

CISCO, cisco. “Asignación de direcciones IPv4. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/11.0.1>

CISCO, cisco. “Capa de aplicación. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/15.0.1>

CISCO, cisco. “Capa de enlace de datos. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/6.0.1>

CISCO, cisco. “Configuración básica de switches y terminales. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/2.0.1>

CISCO, cisco. “Configuración básica de un Router. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/10.0.1>

CISCO, cisco. “Crear una red pequeña. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/17.0.1>

CISCO, cisco. “Enrutamiento inter VLAN”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/srwe/4.0.1>

CISCO, cisco. “Fundamentos de seguridad de la red. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/16.0.1>

CISCO, cisco. “Las redes en la actualidad. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/1.0.1>

CISCO, cisco. “Resolución de dirección. Introducción a las redes”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/itn/9.0.1>

CISCO, cisco. “VLANs”. {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://contenthub.netacad.com/srwe/3.0.1>

CISCO, cisco. “Información sobre los modos de loopback en routers de Cisco”. {En línea} (21 de noviembre de 2007). {22 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

CISCO, cisco. “Configurar el enrutamiento de InterVLAN en conmutadores de capa 3”. {En línea} (abril 21 de 2020). {22 de noviembre de 2022}. Disponible en:

<https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlanrouting/41860-howto-L3-intervlanrouting.html>

WF, Networking “Configuración básica IPv6 Router Cisco.” {En línea} (2020). {22 de noviembre de 2022}. Disponible en:

<https://www.w0lff4nq.org/configuracion-basica-ipv6router-cisco/>

ANEXOS

Anexo A. Link de descarga Escenario 1, archivo ptk

<https://drive.google.com/file/d/1nxn0DrFbMm5fJpEE7XD0qy9O60NmFr2r/view?usp=sharing>

Anexo B. Link de descarga Escenario 2, archivo ptk

https://drive.google.com/file/d/1m3-aBNYwo8gSsu4UI12EQObMMMw2ifn_/view?usp=sharing