SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

CARLOS ALFREDO SIERRA ALARCÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
CEAD SANTA MARTA
SANTA MARTA - MAGDALENA
2022

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

CARLOS ALFREDO SIERRA ALARCÓN

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

DIRECTOR:
MSc. HECTOR JULIAN PARRA MOGOLLON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS - ECBTI
INGENIERIA DE SISTEMAS
CEAD SANTA MARTA
SANTA MARTA- MAGDALENA
2022

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Santa Marta, 25 de junio 2022

CONTENIDO

Pág.

LISTA DE TABLAS 5
LISTA DE FIGURAS 6
RESUMEN 7
GLOSARIO 9
DESARROLLO 12
1. ESCENARIO 1 12
1.1 Topología de simulación escenario 1: 12
Aspectos básicos/situación 13
1.1 Parte 1: Construya la Red 13
1.2. Parte 2: Desarrolle el esquema de direccionamiento IP 13
1.3 Parte 3: Configure aspectos básicos 15
2. ESCENARIO 2 29
Topología de simulación escenario 2 29
2.1 Parte 1: Inicializar dispositivos 30
2.2 Parte 2: Configurar los parámetros básicos de los dispositivos 30
2.3 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN 42
2.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2 47
2.5 Parte 5: Verificar la información de RIP 49
2.6 Parte 6: Implementar DHCP y NAT para IPv4 52
2.7 Parte 7: Configurar NTP 57
2.8 Parte 8: Configurar y verificar las listas de control de acceso (ACL) 58
CONCLUSIONES 64
BIBLIOGRAFÍA 65

LISTA DE TABLAS

Tabla 1. De direccionamiento 14
Tabla 2 Configuración y direccionamiento del router 15
Tabla 3 configuración del switch 20
Tabla 4. Configuración computador A.....25
Tabla 5. Configuración computador B. Fuente: Autor 27
Tabla 6. . Configuración de direcciones en la computadora de Internet. 30
Tabla 7. Subnnetting : red 209.165.200.232 31
Tabla 8. Verificación de conectividad de red.....41
Tabla 9. Verificar la conectividad de la red 47
Tabla 10. Verificar la información de RIP a través de comandos.....50
Tabla 11. Verificar el protocolo DHCP y la NAT estática 55

LISTA DE FIGURAS

Figura 1 Topología de simulación escenario 1 12
Figura 2 comando show ip interface brief. Fuente: Autor. 20
Figura 3 Comando show runing-config. Fuente: Autor 24
Figura 4 Comando ipconfig /all PC-A. Fuente: Autor 26
Figura 5 Comando ipconfig /all PC-B Fuente: Autor 28
Figura 6 Escenario de red 2 29
Figura 7 Verificación de tabla de enrutamiento IPV6 en R1 33
Figura 8 Tabla de enrutamiento IPV4 en R1 34
Figura 9 Verificación de tabla de enrutamiento IPV6 en R2 36
Figura 10 Tabla de enrutamiento IPV4 en R2 37
Figura 11 Verificación tabla de enrutamiento IPV6 en R3 39
Figura 12 Tabla de enrutamiento IPV6 en R3 39
Figura 13 Verificación de conectividad entre R1 y R2 41
Figura 14 Verificación de conectividad a Servidor de Internet 42
Figura 15 Verificación de VLAN en S1 y S2 45
Figura 16 Verificación de asignación de VLAN en S1 (21 a F0/6) y S3 (23 A F0/18) 45
Figura 17 Comprobación de conexiones S3 a R1 y S1 a R1 47
Figura 18 Verificación del comando show ip protocols en R1, R2 y R3 50
Figura 19 Verificación del comando show ip route rip R1 y R2 51
Figura 20 Verificación del protocolo RIPv2 a través del comando show running-config | section router rip R1, R2 y R3 52
Figura 21 Verificación servidor DHCP en PC-A y PC-C 56
Figura 22 Verificación Ping PC-A y PC-C 56
Figura 23 Verificación comando show ntp associations 58
Figura 24 Verificación del funcionamiento de Telnet en R2 59
Figura 25 Verificar Interfaz y la dirección ACL a que se aplica 61
Figura 26 Verificación del comando show ip nat translations 62
Figura 27 Verificación de conexión entre PC-A y PC-C al servidor web desde el Command Prompt 62
Figura 28 Verificación de conexión entre PC-A y PC-C al servidor web desde el navegador. 63
Figura 29 Verificación de la ruta de destino de PC-A y PC-C hasta el servidor de internet a través del comando tracert. 63

RESUMEN

El siguiente trabajo tiene como objetivo, evaluar competencias y habilidades para el diseño e implementación de soluciones de red escalables, LAN y WAN, a través del uso de la herramienta de simulación Packet Tracer. En este documento se describen cada uno de los pasos ejecutados y los resultados obtenidos en el desarrollo de 2 escenarios de red propuestos, que ponen a prueba la comprensión y aplicación de las temáticas vistas en los módulos CP CCNA1 Y CP CCNA 2.

Palabras claves: Configuración, red, Internet, enrutamiento, CISCO, VLAN, LAN, WAN, protocolo.

ABSTRACT

The following work aims to evaluate skills and abilities for the design and implementation of scalable network solutions, LAN and WAN, through the use of the Packet Tracer simulation tool. This document describes each of the steps executed and the results obtained in the development of 2 proposed network scenarios, which test the understanding and application of the topics seen in the CP CCNA1 and CP CCNA 2 modules.

Keywords: Configuration, network, Internet, routing, CISCO, VLAN, LAN, WAN, protocol.

GLOSARIO

DHCP: Siglas del inglés "Dynamic Host Configuración Protocolo." Protocolo Dinámico de Configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red.

Dirección IP: Dirección que se utiliza para identificar un equipo o dispositivo en una red.

DNS: Servidor de Nombres de Dominio. Servidor automatizado utilizado en el internet cuya tares es convertir a nombres fáciles de Recordar (como www.panamacom.com) a direcciones numéricas de IP.

LAN (Local Área Network). Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones.

NAT: Network Address Translation o Network Address Translator es la traducción de IPs privados de una red en IP públicos, para que la red pueda enviar paquetes al exterior, y viceversa**.**

Ping (Buscador de paquetes de Internet): Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

Red: Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta

por diferentes combinaciones de diversos tipos de redes. En inglés se le conoce como Network. El internet está compuesto de miles de redes, por lo tanto, internet también se le conoce como "la red".

Router: Un router es un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino.

Servidor: Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

Switch: permiten que los dispositivos en su red se comuniquen entre sí, recibiendo paquetes de datos y direccionándolos al destinatario correcto. Al hacer posible que la información y los recursos sean compartidos, los switches le ayudan a ahorrar dinero e incrementar la productividad.

Telnet: Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.

VLAN: Siglas de virtual LAN (red de área local virtual)- Es un método que permite crear redes lógicas independientes compartiendo dispositivos físicos de red, ofreciendo una subdivisión por grupos garantizando la comunicación y envío de los datos en la red como si se tratará de redes aisladas.

WAN: Siglas del inglés Wide Área Network (Red de área Amplia). Es una red de computadoras conectadas entre sí. Usando líneas terrestres o satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

INTRODUCCIÓN

El crecimiento del internet a lo largo de la historia ha generado una evolución significativa en el área de las telecomunicaciones , ya que actividades que requerían de grandes esfuerzo y tiempo para realizarse como: reuniones de negocios, clases, conferencias, discusiones y hasta una simple llamada se ha podido reducir a un simple clic a través de múltiples servicios como videoconferencias, chats, e-mail, foros de discusión, transferencia de archivos, etc. lo que a su vez permite una mayor interacción entre las partes involucradas ya que pueden encontrarse de forma sincrónica sin importar la ubicación.

Todo lo anterior es posible gracias a un trabajo conjunto entre hardware y software que permite aprovechar al máximo los beneficios que ofrece el internet. Para lograr mejorar los procesos comunicativos ha sido de suma importancia la aparición de muchas herramientas tecnológicas, tal como la aparición de IPv6, el cual representa la solución a la escasez de direcciones IP que es un hecho que se había previsto hace muchos años. Sin embargo, se veía como algo lejano y casi imposible de lograr no obstante hoy en día razón por la cual se ofrece la posibilidad de mejorar este inconveniente a través de IPv6 ya que al ser una tecnología con una vasta experiencia permite el crecimiento del internet apoyándose en otras tecnologías que permitan usar y aprovechar todos los beneficios que esta ofrece. Lo que constituye el cimiento que posibilitará el despliegue de Internet de las cosas.

En el presente trabajo se propone la implementación de infraestructuras de red a través de dos casos de estudios que ponen a prueba la comprensión y aplicación de las temáticas vistas en los módulos CP CCNA1 Y CP CCNA 2 de Cisco Networking Academy. Con la ejecución de los escenarios 1 y 2, se busca consolidar los conocimientos para el manejo de asignación de direccionamiento IPv4 e IPv6, ruteo para las VLAN, configuración de protocolos dinámicos y estáticos, configuraciones OSPF, NAT, NTP, listas de control de acceso (ACL), entre otros requerimientos solicitados por la guía de actividades. Este se ejecuta con el esfuerzo de educarse y efectuar los comandos necesarios que se utilizaran en el día a día de nuestra vida profesional.

DESARROLLO

1. ESCENARIO 1

1.1 Topología de simulación escenario 1:

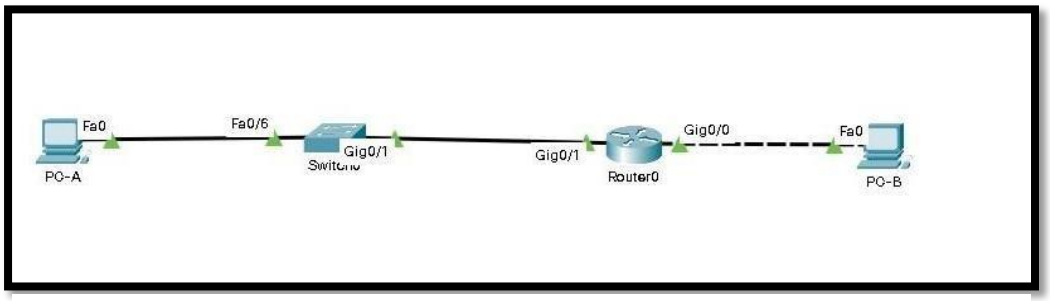

Figura 1 Topología de simulación escenario 1

En este primer escenario se configurarán los dispositivos de una red pequeña.

Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos:

Parte 1: Construir en el simulador la Red
Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2
Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1
Parte 5: Configurar los hosts y verificar la conectividad entre los equipos.

Aspectos básicos/situación:

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swicht S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

1.1 Parte 1: Construya la Red

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

El swicht maneja tramas de internet, tiene una dirección IP para la administración de red, y para la etapa de enrutamiento lo realizará el router.

1.2. Parte 2: Desarrolle el esquema de direccionamiento IP

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

Tabla 1. De direccionamiento.

Item	Requerimiento
Dirección de Red 192.168.**X**.0 donde X corresponde a los últimos dos dígitos de su cédula.	192.168.9.0 / 24
Requerimiento de host Subred LAN1 100	Dirección de red: 192.168.9.0 Masc: /25 Cantidad de direcciones: 128 Cantidad de direcciones útiles: 126 Primera dirección valida: 192.168.9.1 Ultima dirección valida: 192.168.9.126 Broadcast: 192.168.9.127 Mascara decimal 255.255.255.128
Requerimiento de host Subred LAN2 50	Dirección de red: 192.168.9.128 Masc: /26 Cantidad de direcciones: 64 Cantidad de direcciones útiles: 62 Primera dirección valida: 192.168.9.129 Ultima dirección valida: 192.168.9.190 Broadcast: 192.168.9.191 Mascara decimal 255.255.255.192
R1 G0/0/1 Primera dirección de host de la subred LAN1	192.168.9.1 /26
R1 G0/0/0 Primera dirección de host de la subred LAN2	192.168.9.129 /25
S1 SVI Segunda dirección de host de la subred LAN1	192.168.9.1
PC-A Última dirección de host de la subred LAN1	192.168.9.129 /26
PC_A Última dirección de host de la subred LAN2	192.168.9.99 /25

Nota: Se desarrolla la tabla de direccionamiento de acuerdo a los requerimientos de la actividad. Fuente: Autor

1.3 Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Tabla 2 Configuración y direccionamiento del router

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	Deshabilite la búsqueda DNS Si se desactiva la búsqueda DNS un router no podría resolver los nombres, lo cual provocaría posibles problemas cuando el router necesite una dirección IP para enviar un paquete (se desactiva cuando se hacen pruebas para que el Router no intente buscas una entrada DNS para un nombre que en realidad es un error de escritura). Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router(config)#exit Router# %SYS-5-CONFIG_I: Configured from console by console Router#
Nombre del router R1	Asigne el nombre de dispositivo al Router (R1). Se utiliza el comando hostname con el fin de que establezca el nombre de Router a R1. Router#configure terminal

	Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1 R1(config)#exit
Nombre de dominio	Asigne el nombre del dominio en el router para el usuario ingrese a la dirección que es ccna-lab.com R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name ccna-lab.com R1(config)#exit R1#
Contraseña cifrada para el modo EXEC privilegiado	El usuario ingrese con la contraseña que es ciscoenpass. R1# R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#enable secret ciscoenpass R1(config)#exit R1#
Contraseña de acceso a la consola	Asigne ciscoconpass como la contraseña de consola 0 y habilite el inicio de la sesión. Y pueda ingresar a la consola con la contraseña que aparece y el login es para deshabilitar la autenticación. R1# %SYS-5-CONFIG_I: Configured from console by console R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#exit R1#

Establecer la longitud mínima para las contraseñas en 10 caracteres.	Se utiliza el comando security passwords min-length longitud en el modo de configuración global. En el ejemplo, cualquier contraseña nueva configurada debería tener una longitud mínima de ocho caracteres. Password: Password: R1>enable Password: R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#security password min-length 10 R1(config)#exit R1#
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#username admin secret admin1pass R1(config)#exit
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)# R1(config)#line vty 0 15 R1(config-line)#login local R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)# R1(config)#service password-encryption R1(config)#exit R1#
Configure un MOTD Banner	R1#configure terminal R1(config)#banner motd $Prohibido el acceso no autorizado$ R1(config)#exit R1#

Configurar interfaz G0/0/0	R1>enable Password: Password: R1#configure terminal R1(config)#interfa R1(config)#interface gi R1(config)#interface gigabitEthernet 0/0 R1(config-if)#ip address 192.168.9.129 255.255.255.192 R1(config-if)#no shut R1(config-if)#no shutdown
Establezca la descripción Establece la dirección IPv4.	R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up R1(config-if)#
Configurar interfaz G0/0/1	R1>enable Password:
Establezca la descripción Establece la dirección IPv4.	Password:
Activar la interfaz.	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#inter R1(config)#interface gig R1(config)#interface gigabitEthernet 0/1 R1(config-if)#ip address 192.168.9.1 255.255.255.128 R1(config-if)#no sh R1(config-if)#no shutdown R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Generar una clave de cifrado RSA	R1#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	R1(config)#no ip domain-lookup R1(config)#crypto key generate rsa % Please define a domain-name first. R1(config)#ip domain-name ccna-lab.com R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Nota: El desarrollo de la tabla está enfocada a la configuración del router y al direccionamiento del mismo según las especificaciones de la guía.

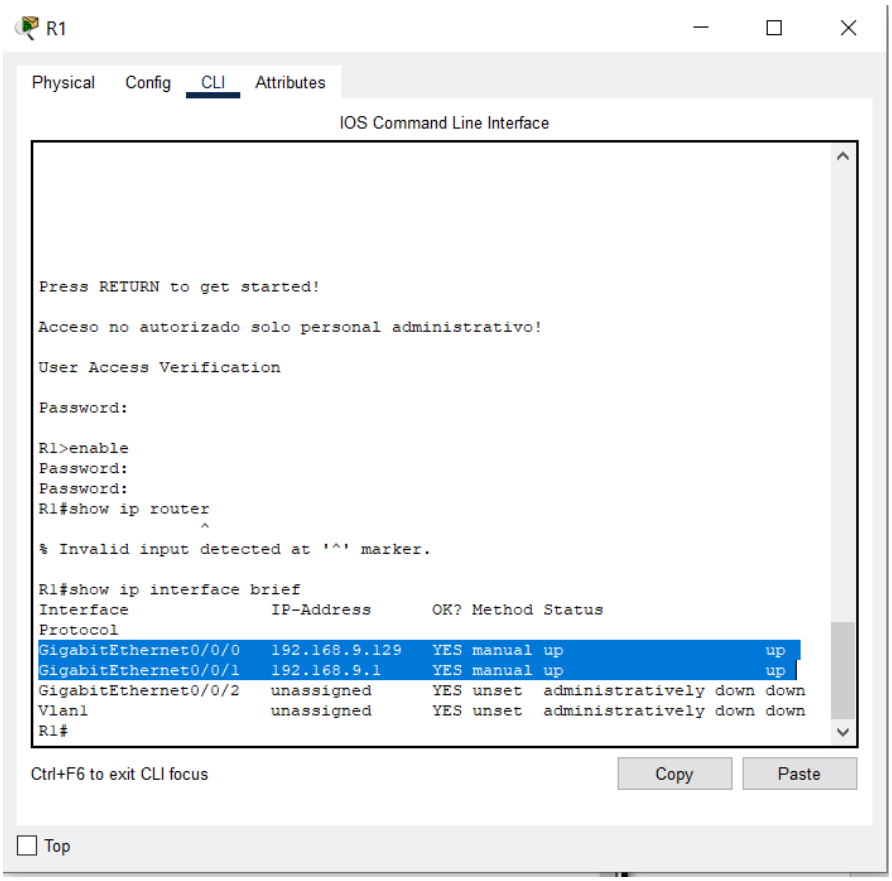

Figura 2 comando show ip interface brief. Fuente: Autor.

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3 configuración del switch

Tarea	Especificación
Desactivar la búsqueda DNS.	Enter configuration commands, one per line. End with CNTL/Z. S1(config)#no ip domain-lookup S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#
Nombre del	S1

switch	Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname S1 S1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console S1#
Nombre de dominio	S1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#ip domain-name ccna-lab.com S1(config)#exit S1# %SYS-5-CONFIG_I: Configured from console by console S1#
Contraseña cifrada para el modo EXEC privilegiado	Ciscoenpass S1(config)#enable secret ciscoenpass S1(config)#line console 0
Contraseña de acceso a la consola	ciscoconpass S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass S1(config)#username admin password admin1pass S1(config)# S1(config)#^Z S1# %SYS-5-CONFIG_I: Configured from console by console S1#exit
Configurar el inicio de sesión en las líneas VTY para que use la	Switch 1

base de datos local	S1(config)#line vty 0 4
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#privilege level 5 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Configurar un MOTD	S1(config)#banner motd $PROHIBIDO EL ACCESO
Banner	NO AUTORIZADO$
Generar una clave de cifrado RSA	Módulo de 1024 bits S1(config)#crypto key generate rsa general-keys modulus 1024 % You already have RSA keys defined named S1.ccna-lab.com % They will be replaced. % The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non- exportable...[OK] *Mar 1 0:23:55.506: %SSH-5-ENABLED: SSH 1.99 has been enabled
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento S1(config)#interface vlan1 S1(config-if)#ip address 192.168.9.1 255.255.255.128 S1(config-if)#no shutdown S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up

	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
	%IP-4-DUPADDR: Duplicate address 192.168.9.1 on Vlan1, sourced by 0003.E4C5.E202 S1(config-if)#exit S1(config)#exit S1# %SYS S1(config)# S1(config)#interface vlan2 S1(config-if)#ip address 192.168.9.128 255.255.255.192 Bad mask /26 for address 192.168.9.128 S1(config-if)#no shutdown S1(config-if)#
Configuración del Gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento. S1(config-if)# S1(config-if)#ip default-gateway 192.168.9.1 S1(config)#exit S1#

Nota: El desarrollo de la tabla es enfocado en la configuración del switch de acuerdo a los parámetrossolicitados en la guía.

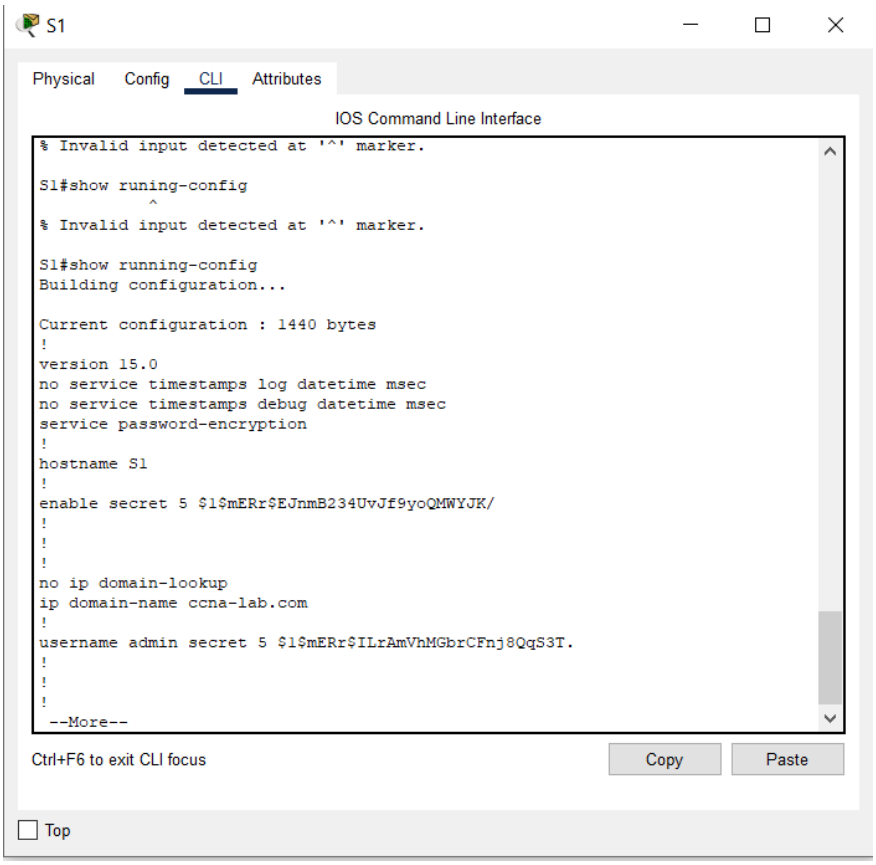

Figura 3 Comando show runing-config. Fuente: Autor

Paso 2. Configurar los equipos

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

Tabla 4. Configuración computador A

	PC-A Network Configuration
Descripción	*PC-A*
Dirección física	*en blanco*
Dirección IP	*192.168.9.190*
Máscara de subred	*255.255.255.0*
Gateway predeterminado	*192.168.9.129*

Nota: El desarrollo de la tabla está enfocado a la configuración del computador A de acuerdo alos parámetros solicitados en la guía

Fuente: Autor.

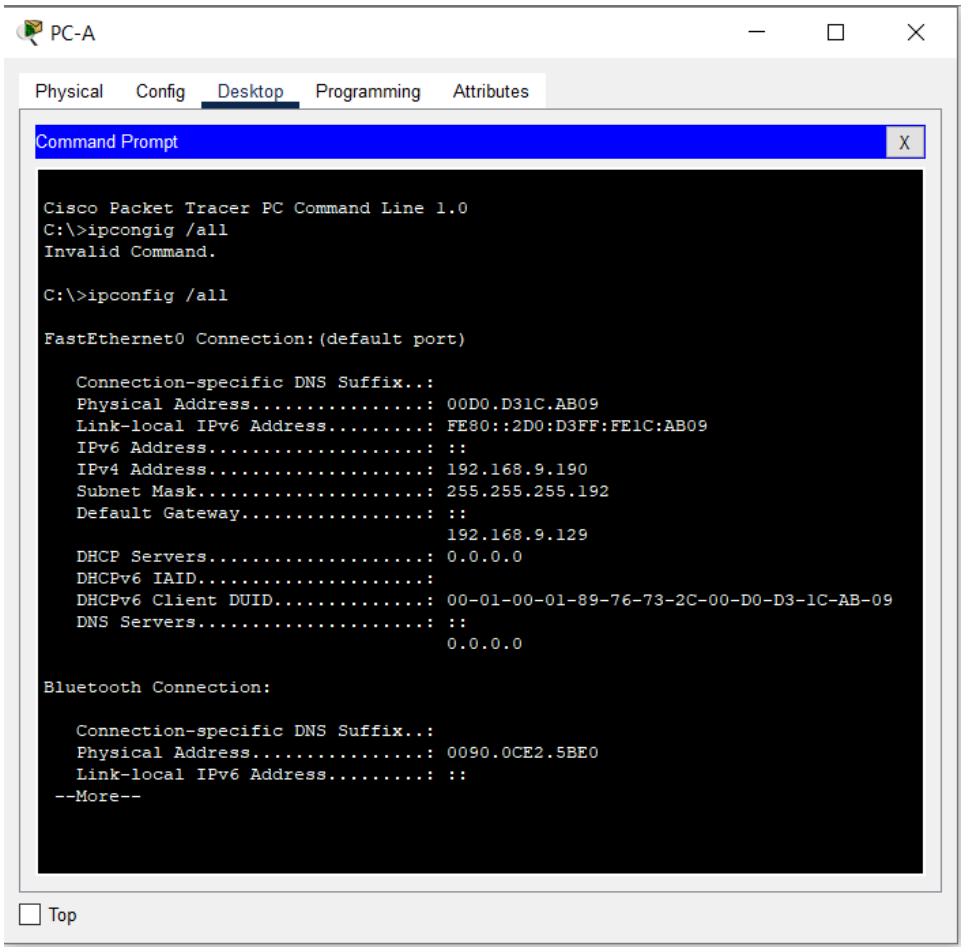

Figura 4 Comando ipconfig /all PC-A. Fuente: Autor

Tabla 5. Configuración computador B. Fuente: Autor

	PC-B Network Configuration
Descripción	*PC-B*
Dirección física	*en blanco*
Dirección IP	*192.168.9.126*
Máscara de subred	*255.255.255.0*
Gateway predeterminado	*192.168.9.1*

Nota: El desarrollo de la tabla está enfocado a la configuración del computador B de acuerdo a los parámetros solicitados en la guía.

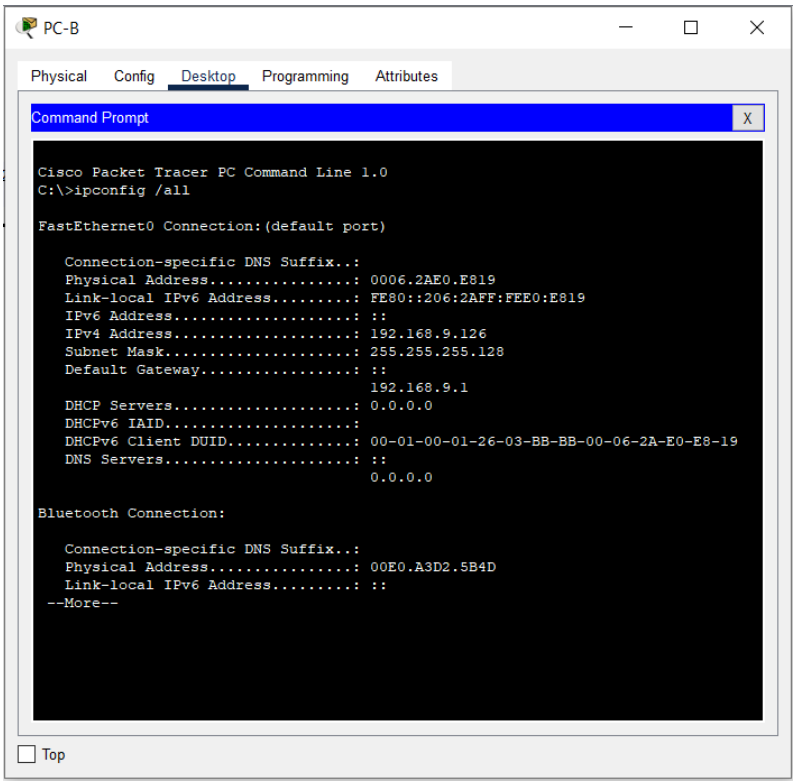

Figura 5 Comando ipconfig /all PC-B Fuente: Autor

2. ESCENARIO 2

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico RIPv2, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Topología de simulación escenario 2:

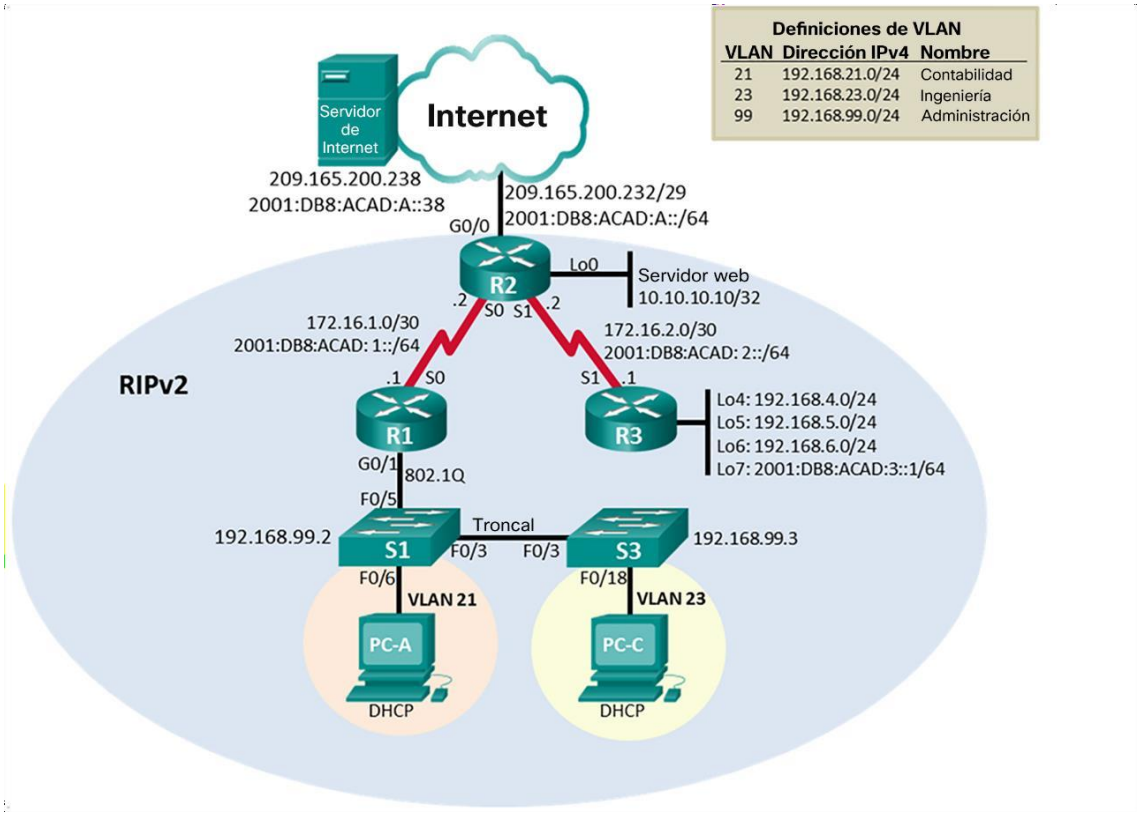

Figura 6 Escenario de red 2

2.1 Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches.

Router#erase startup-config // Eliminar el archivo startup-config de todos los routers
Router#reload // Volver a cargar todos los routers

Switch>en
Switch#erase startup-config // Eliminar el archivo startup-config de todos los switches
Switch#delete vlan.dat // eliminar la base de datos de VLAN anterior
Switch#reload // Volver a cargar ambos switches
Switch>show flash //Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Nota: Estas configuraciones se hacen por lo general en laboratorios físicos.

2.2 Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 6. . Configuración de direcciones en la computadora de Internet.

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238/29
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Clase c

Tabla 7. Subnnetting : red 209.165.200.232

Network:	209.165.200.232/29	11010001.10100101.11001000.11101**000**
HostMin:	209.165.200.233	11010001.10100101.11001000.11101 **001**
HostMax:	209.165.200.238	11010001.10100101.11001000.11101 **110**
Broadcast:	209.165.200.239	11010001.10100101.11001000.11101 111
Hosts:	6	

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Configuraciones básicas en R1

Router(config)#no ip domain-lookup **// Desactivar la búsqueda DNS**
Router(config)#hostname R1 **// Nombre del router**
R1(config)#enable secret class **// Contraseña de exec privilegiado cifrada**
R1(config)#line console 0 **// Contraseña de acceso a la consola**
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15 **// Contraseña de acceso Telnet**
R1(config-line)#password cisco
R1(config-line)#login

R1(config-line)#service password-encryption **// Cifrar las contraseñas de texto no cifrado**
R1(config)#banner motd #Se prohibe el acceso no autorizado. # **// Mensaje MOTD**

Configuración Interfaz S0/0/0

R1(config)#int s0/0/0
R1(config-if)#description Connection R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:ACAD:1::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

Configuración de rutas predeterminadas IPV4 e IPV6: Permite al router enviar paquetes a las redes que no están incluidas en la tabla de enrutamiento

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 unicast-routing **//Habilitar protocolo IPV6**
R1(config)#ipv6 route ::/0 s0/0/0

Verificación de tabla de enrutamiento en R1

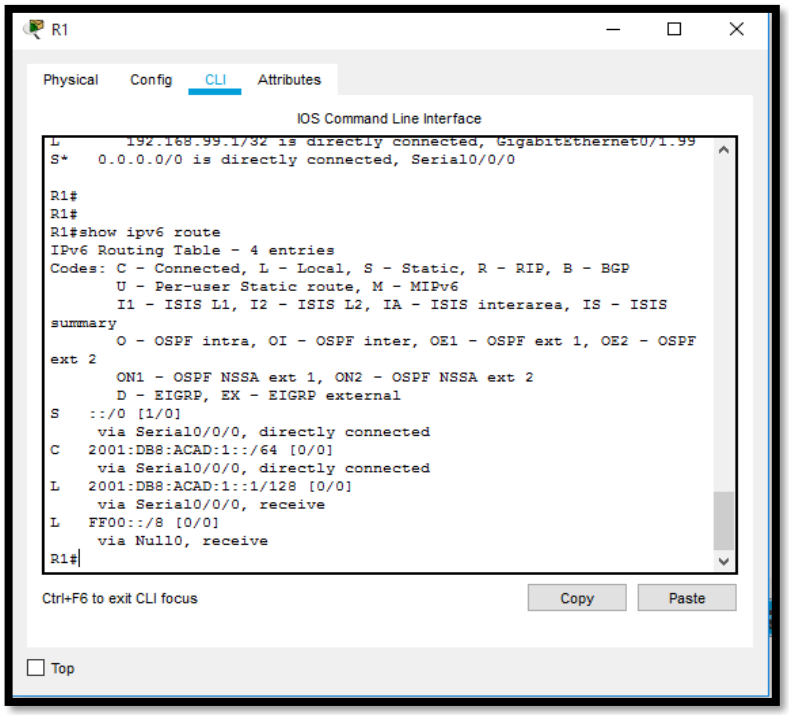

Figura 7 Verificación de tabla de enrutamiento IPV6 en R1

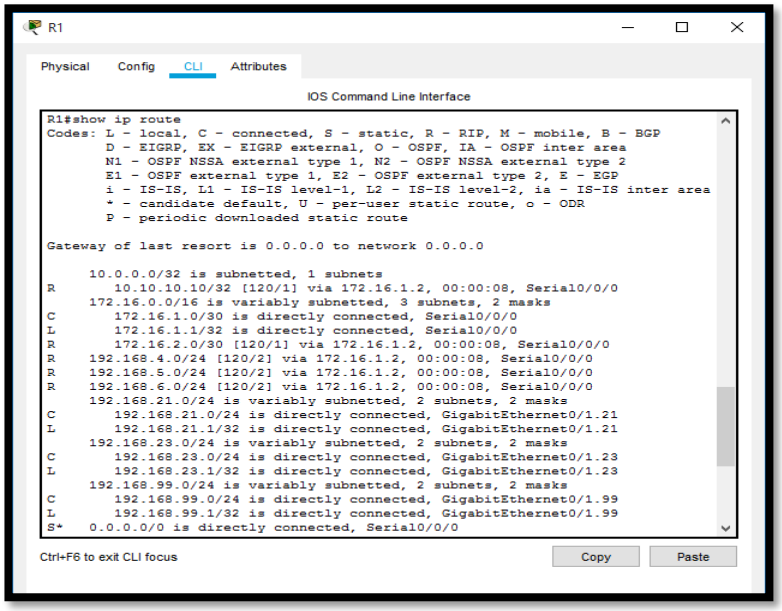

Figura 8 Tabla de enrutamiento IPV4 en R1

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

```
Router>en
Router#config t
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service  password-encryption
R2(config)#banner motd #Se prohibe el acceso no autorizado.#
```

Habilitar el servidor HTTP

```
R2(config)#ip http server
```

Configuración de interfaz S0/0/0

R2(config)#int s0/0/0
R2(config-if)#description Connection to R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown

Configuración de interfaz S0/0/1

R2(config-if)#int s0/0/1
R2(config-if)#description Connection to R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown

Configuración de interfaz g0/0

R2(config-if)#int g0/0
R2(config-if)#description Connection to Internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown

Interfaz loopback o (servidor web simulado)

R2(config-if)#int loopback 0
R2(config-if)#description servidor web simulado
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#no shutdown

Ruta predeterminada

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0

R2(config)#ipv6 unicast-routing

R2(config)#ipv6 route ::/0 g0/0

Verificación de tabla de enrutamiento R2

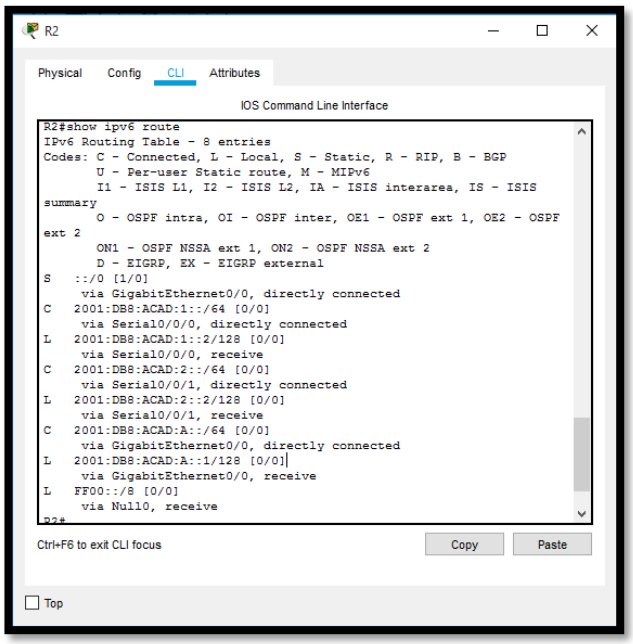

Figura 9 Verificación de tabla de enrutamiento IPV6 en R2

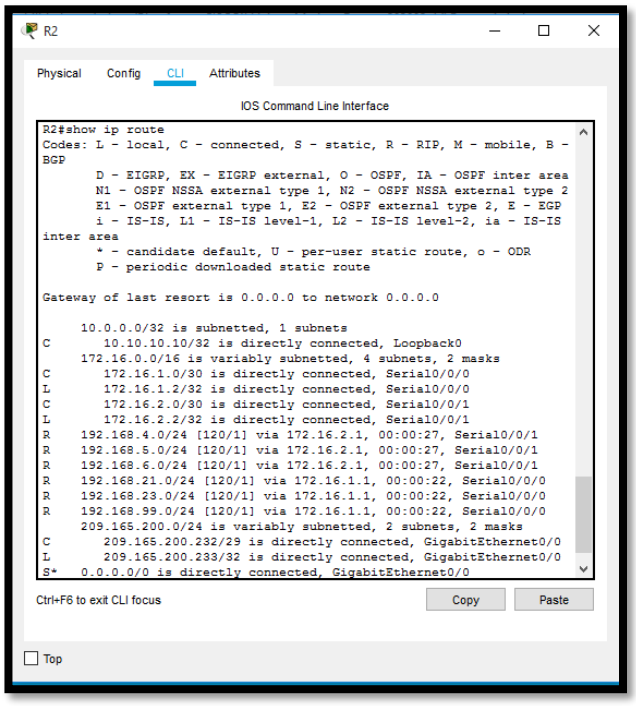

Figura 10 Tabla de enrutamiento IPV4 en R2

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd #Se prohibe el acceso no autorizado.#
Interfaz S0/0/1
R3(config)#int s0/0/1
R3(config-if)#Description Connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64

R3(config-if)#no shutdown

Interfaz loopback 4
R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0

Interfaz loopback 5
R3(config-if)#int loopback 5
R3(config-if)#
R3(config-if)#ip address 192.168.5.1 255.255.255.0

Interfaz loopback 6
R3(config-if)#int loopback 6
R3(config-if)#
R3(config-if)#ip address 192.168.6.1 255.255.255.0

Interfaz loopback 7
R3(config-if)#int loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64

Rutas predeterminadas
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 route::/0 s0/0/1

Verificación de tabla de enrutamiento R3

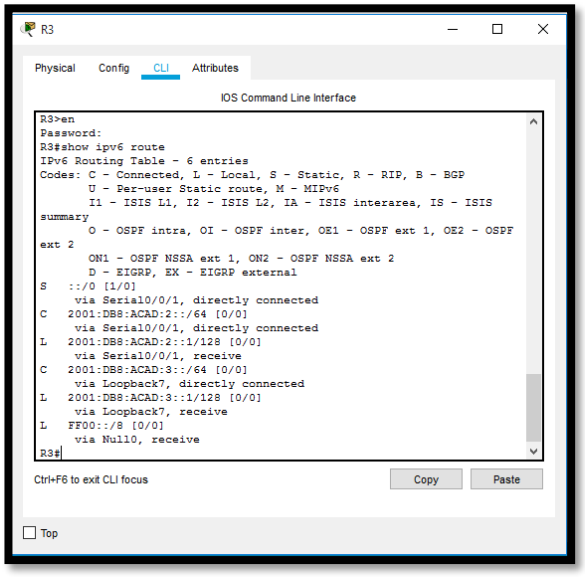

Figura 11 Verificación tabla de enrutamiento IPV6 en R3

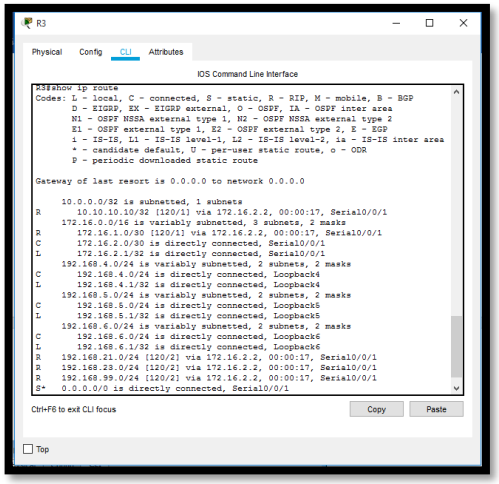

Figura 12 Tabla de enrutamiento IPV6 en R3

.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Switch(config)#no ip domain-lookup
Switch(config)#hostname S1

```
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service  password-encryption
S1(config)#banner motd #Se prohibe el acceso no autorizado.#
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config-line)# banner motd #Se prohibe el acceso no autorizado.#
```

.

Paso 7 Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre 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 8. Verificación de conectividad de red.

	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	5-may
R2	R3, S0/0/1	172.16.2.2	5-may
PC de Internet	Gateway predeterminado	209.165.200.233	Packets: Sent = 4, Received = 4, Lost = 0

Verificación de ping R1 a R2 y viceversa

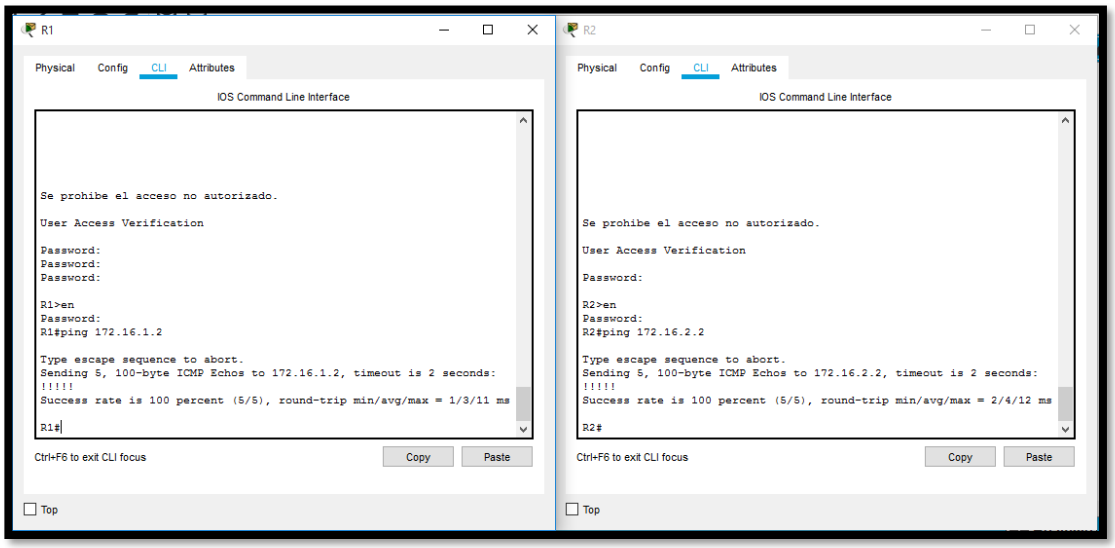

Figura 13 Verificación de conectividad entre R1 y R2

Servidor de Internet: Conexión.

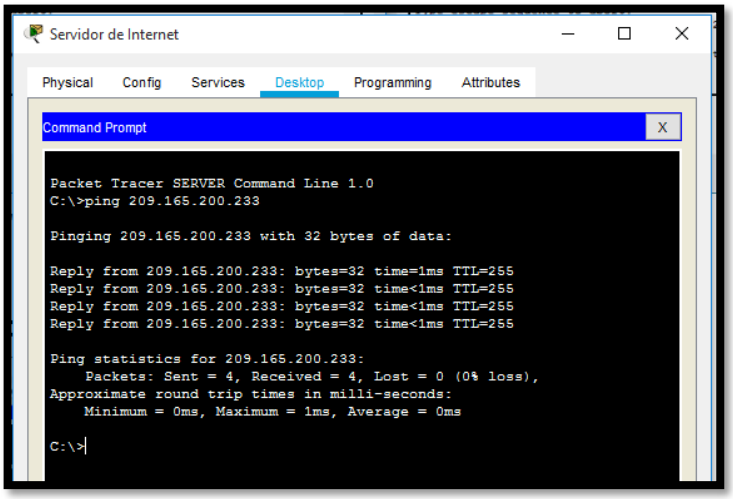

Figura 14 Verificación de conectividad a Servidor de Internet

2.3 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Crear la base de datos de VLAN

S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administración

Asignar la dirección IP de administración.

S1(config)#int vlan 99

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown

Asignar el gateway predeterminado
S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

Forzar el enlace troncal en la interfaz F0/5
S1(config)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso
S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode Access

Asignar F0/6 a la VLAN 21
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21

Apagar todos los puertos sin usar
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Crear la base de datos de VLAN
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion

Asignar la dirección IP de administración
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown

Asignar el gateway predeterminado.
S3(config)#ip default-gateway 192.168.99.1

Forzar el enlace troncal en la interfaz F0/3
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso
S3(config)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode Access

Asignar F0/18 a la VLAN 23
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23

Apagar todos los puertos sin usar
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown

Verificación de VLAN configuradas S1 Y S2

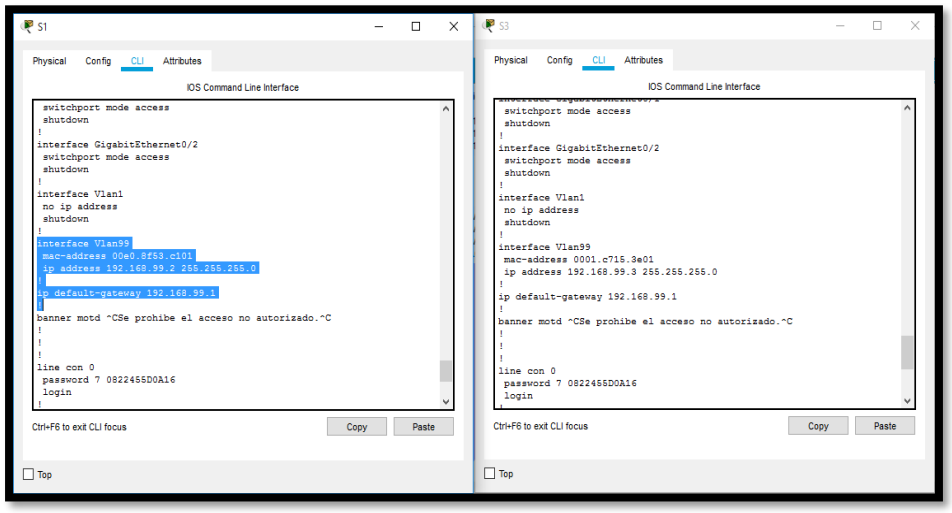

Figura 15 Verificación de VLAN en S1 y S2

Verificación de asignación de vlan en S1(21 a F0/6) y S2(23 a F0/18)

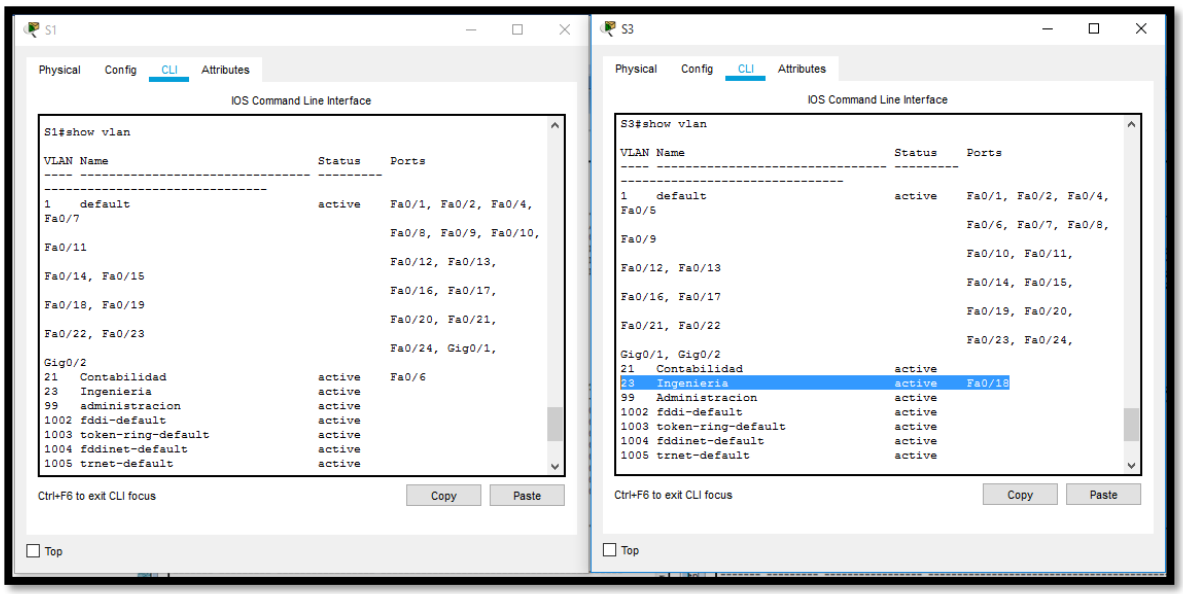

Figura 16 Verificación de asignación de VLAN en S1 (21 a F0/6) y S3 (23 A F0/18)

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar la subinterfaz 802.1Q .21 en G0/1
R1(config)#int g0/1.21
R1(config-subif)#description LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0

Configurar la subinterfaz 802.1Q .23 en G0/1
R1(config-subif)#int g0/1.23
R1(config-subif)#description LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0

Configurar la subinterfaz
802.1Q .99 en G0/1R1(config-subif)#int g0/1.99
R1(config-subif)#description LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0

Activar la interfaz G0/1
R1(config-subif)#int g0/1
R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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 9. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	5/5
S3	R1, dirección VLAN 99	192.168.99.1	5/5
S1	R1, dirección VLAN 21	192.168.21.1	5/5
S3	R1, dirección VLAN 23	192.168.23.1	5/5

Comprobacion de conexiones S3 a R1 y S1 a R1

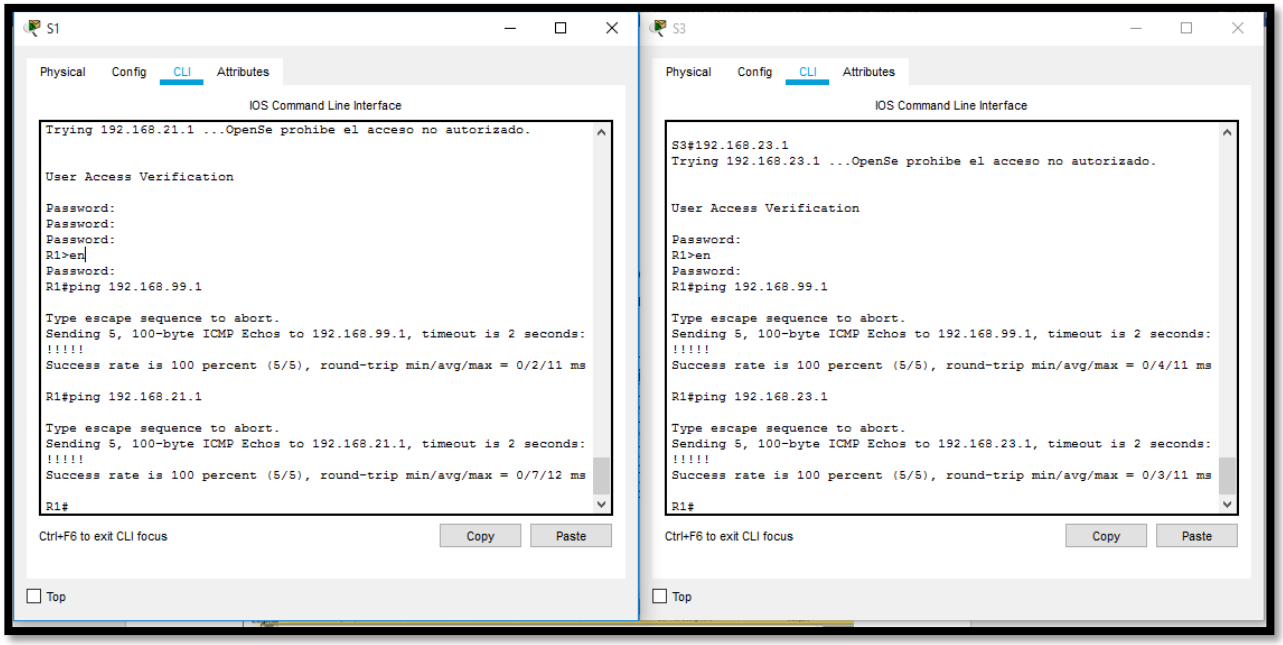

Figura 17 Comprobación de conexiones S3 a R1 y S1 a R1

2.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Configurar RIP versión 2
R1(config)#router rip
R1(config-router)#version 2

Anunciar las redes conectadas directamente
R1(config-router)#do show ip route connected
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0

Establecer todas las interfaces LAN como pasivas
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
Desactive la sumarización automática R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Configurar RIP versión 2
R2(config)#router rip
R2(config-router)#version 2

Anunciar las redes conectadas directamente
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10

R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0

Establecer la interfaz LAN (loopback) como pasiva
R2(config-router)#passive-interface loopback 0

Desactive la sumarización automática.
R2(config-router)#no auto-summary

Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

Anunciar redes IPv4 conectadas directamente
R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6
R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0

Establecer todas las interfaces de LAN IPv4 (Loopback) como
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6

Desactive la sumarización automática.
R3(config-router)#no auto-summary

2.5 Parte 5: Verificar la información de RIP

Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 10. Verificar la información de RIP a través de comandos.

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	**R1#show ip protocols**
¿Qué comando muestra solo las rutas RIP?	**R2#show ip route rip**
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	**R1#show running-config | section router rip** % Invalid input detected at '^' marker. Comando no soportado por PACKET TRACER, se debe usar Usar **show run**

Verificación del comando show ip protocols en R1, R2 y R3

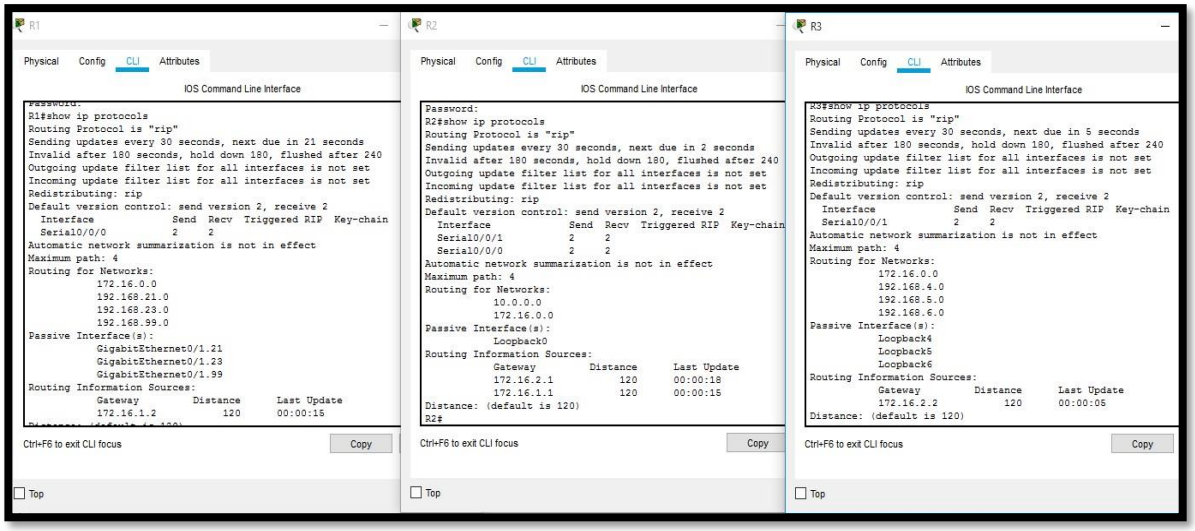

Figura 18 Verificación del comando show ip protocols en R1, R2 y R3

Verificación del comando show ip route rip R1, R2 y R3

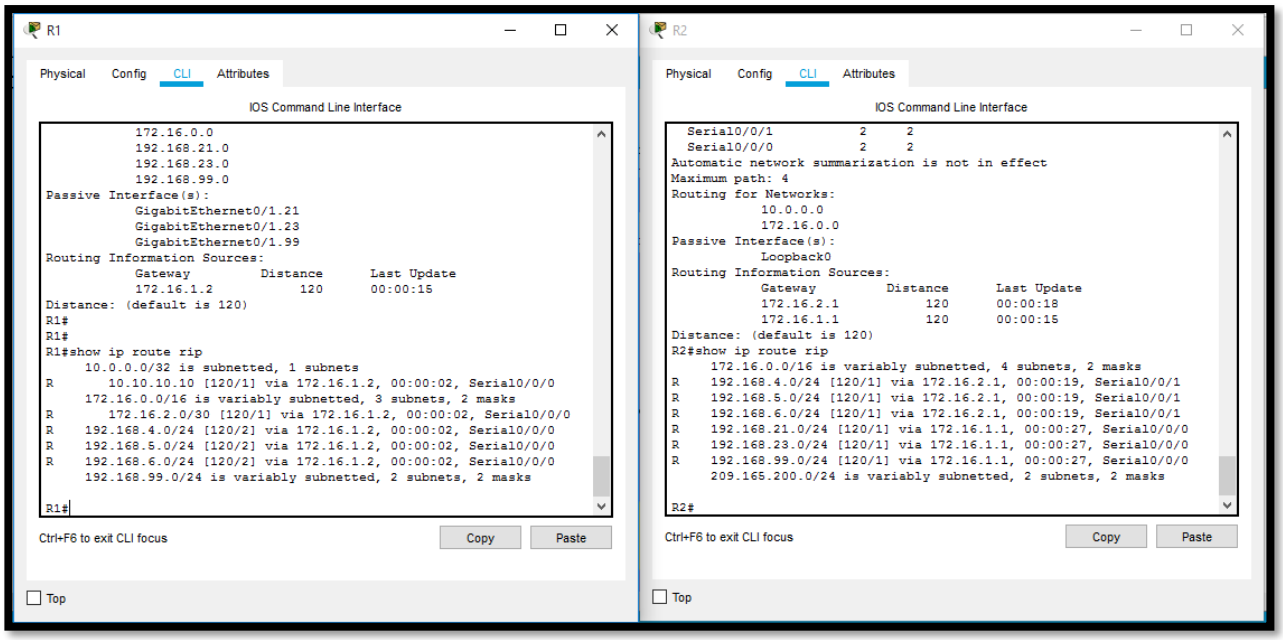

Figura 19 Verificación del comando show ip route rip R1 y R2

Verificación del protocolo RIPv2 a través del comando show run R1, R2 y R3

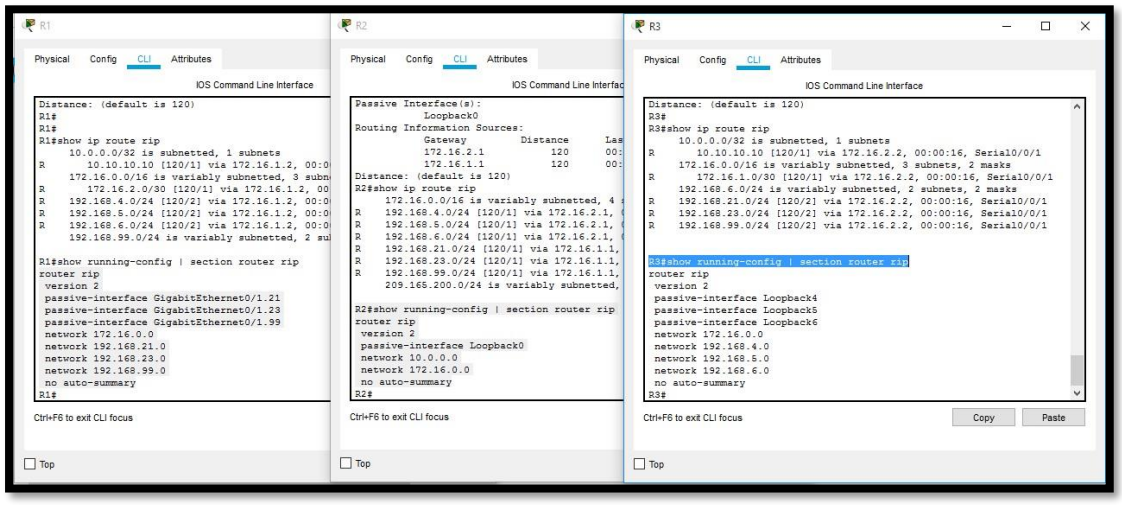

Figura 20 Verificación del protocolo RIPv2 a través del comando show running-config | section router rip R1, R2 y R3.

2.6 Parte 6: Implementar DHCP y NAT para IPv4

Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20

Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20

Crear un pool de DHCP para la VLAN 21.

R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com

Crear un pool de DHCP para la VLAN 23
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com

Paso 2: Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Crear una base de datos local con una cuenta de usuario
R2(config)#username webuser privilege 15 secret cisco12345

Habilitar el servicio del servidor HTTP
R2(config)#ip http server
Nota. ip http server no es soportado por Packet Tracer.

Configurar el servidor HTTP para utilizar la base de datos local para la autenticación
R2(config)#ip http authentication local
Nota. ip http authentication local no es soportado por Packet Tracer.

Crear una NAT estática al servidor web (Dirección global interna: 209.165.200.237**).**
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237

Asignar la interfaz interna y externa para la NAT estática
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside

Configurar la NAT dinámica dentro de una ACL privada

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255**// Permitir la traducción de las redes de Contabilidad**

R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255**// Permitir la traducción de las redes Ingeniería**

R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255 **// Permitir la traducción de un resumen de las redes LAN (loopback) en el R3**

Defina el pool de direcciones IP públicas utilizables.
Nombre del conjunto: INTERNET
El conjunto de direcciones incluye: 209.165.200.233 – 209.165.200.236
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248

Definir la traducción de NAT dinámica
R2(config)#ip nat inside source list 1 pool INTERNET

NOTA: Para crear una NAT estática al servidor web se usó la dirección global interna: **209.165.200.237**, recordemos que el rango de direcciones está comprendido desde la **209.165.200.233** ocupada por la G0/0 **hasta la 209.165.200.238** ocupada por el servidor de internet.

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 11. Verificar el protocolo DHCP y la NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Satisfactorio
Verificar que la PC-A pueda hacer ping a la PC-C	Satisfactorio
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.2237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet tracer no soporta este procedimiento, ya que el comando ip http server en R2 tampoco es soportado por este este software

Verificación servidor DHCP en PC-A y PC-C

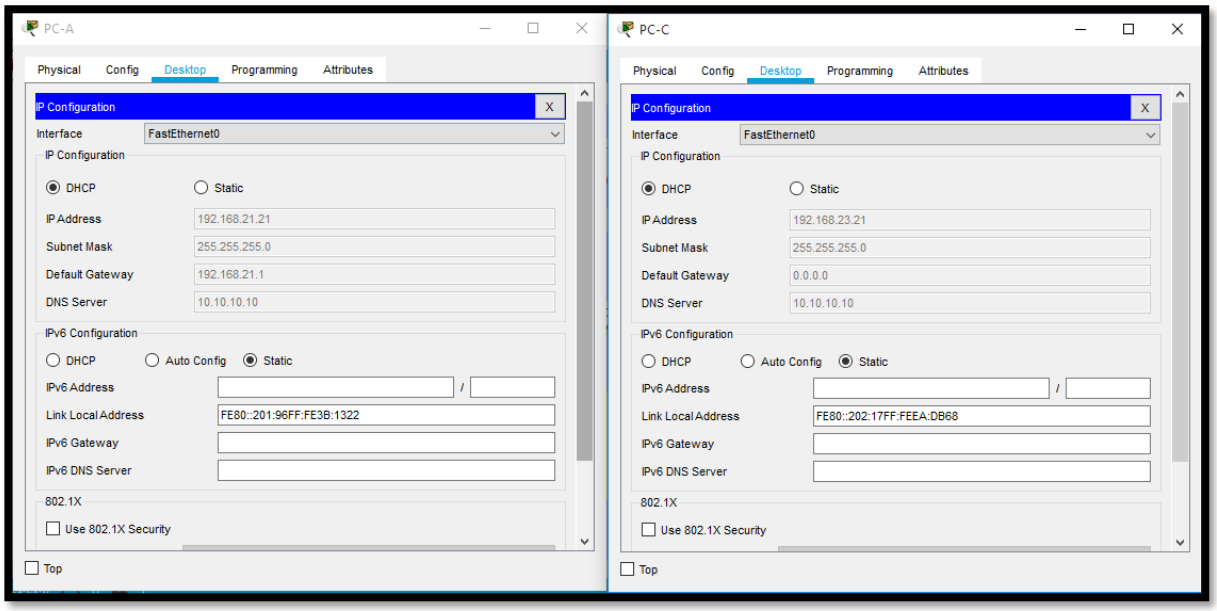

Figura 21 Verificación servidor DHCP en PC-A y PC-C

Verificación Ping PC-A y PC-C

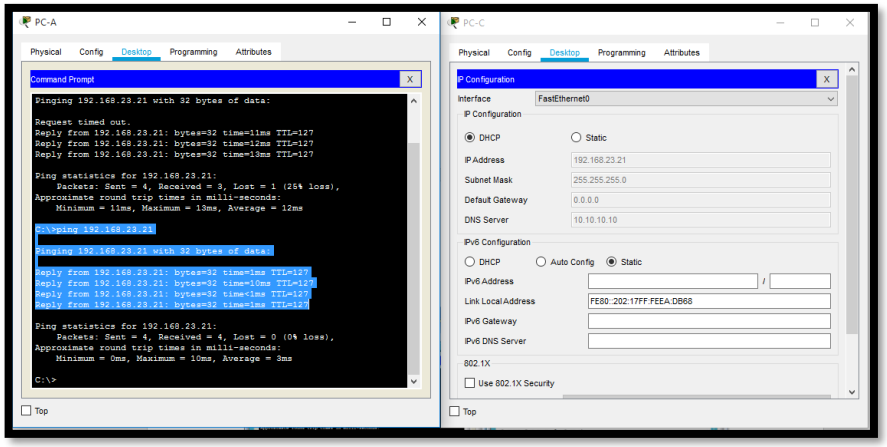

Figura 22 Verificación Ping PC-A y PC-C

2.7 Parte 7: Configurar NTP

Ajuste la fecha y hora en R2.
R2#clock set 14:25:00 july 01 2020

Configure R2 como un maestro NTP.
R2(config)#ntp master 5

Configurar R1 como un cliente NTP.
R1(config)#ntp server 172.16.1.2

Configure R1 para actualizaciones de calendario periódicas con hora NTP.R1(config)#ntp update-calendar

Verifique la configuración de NTP en R1.
R1#show ntp associations

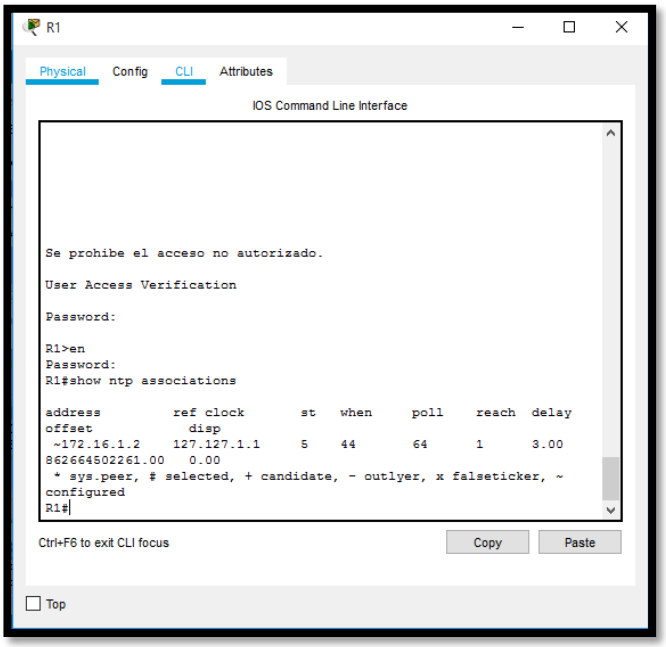

Figura 23 Verificación comando show ntp associations

2.8 Parte 8: Configurar y verificar las listas de control de acceso (ACL)

Restringir el acceso a las líneas VTY en el R2

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión
Telnet con R2 Nombre de la ACL: ADMIN-MGT

R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1

Aplicar la ACL con nombre a las líneas VTY
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in

Permitir acceso por Telnet a las líneas de VTY
R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera Satisfactorio
R1>en

Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ..OpenSe prohibe el acceso no autorizado.

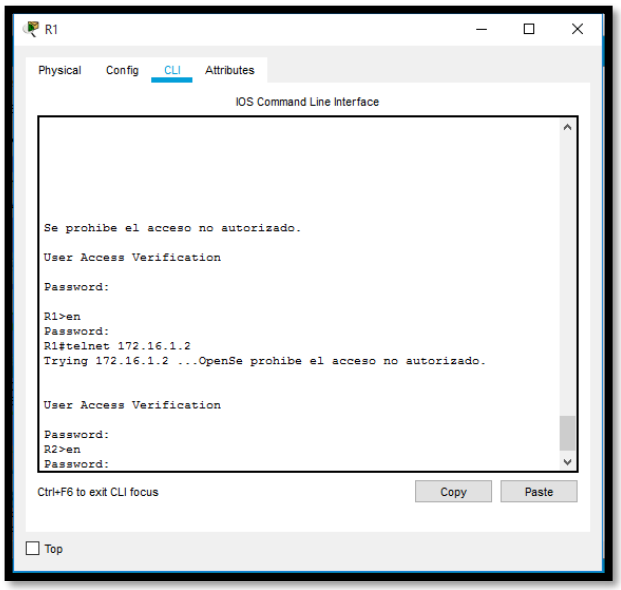

Figura 24 Verificación del funcionamiento de Telnet en R2.

Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

R2#show access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))
R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255

20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1 (2 match(es))

Restablecer los contadores de una lista de acceso

R2#clear access-list counters
R2#show ip access-list
Standard IP access list 1
10 permit 192.168.21.0 0.0.0.255
20 permit 192.168.23.0 0.0.0.255
30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
10 permit host 172.16.1.1

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? R/show ip interface

¿Con qué comando se muestran las traducciones NAT?
R/show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---
tcp 209.165.200.234:1025192.168.23.2:1025 209.165.200.238:80 209.165.200.238:80
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?R2#/respuesta clear ip nat translation *

R2#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.237 10.10.10.10 --- ---

Interfaz y la dirección ACL en que se aplica

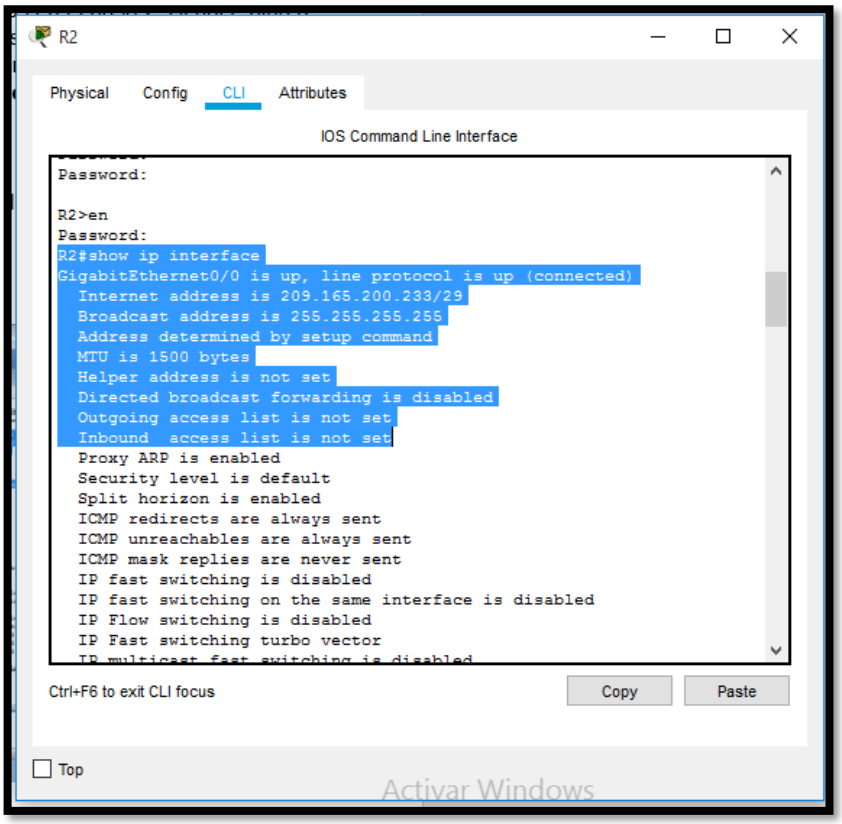

Figura 25 Verificar Interfaz y la dirección ACL a que se aplica

Verificación del comando show ip nat translations

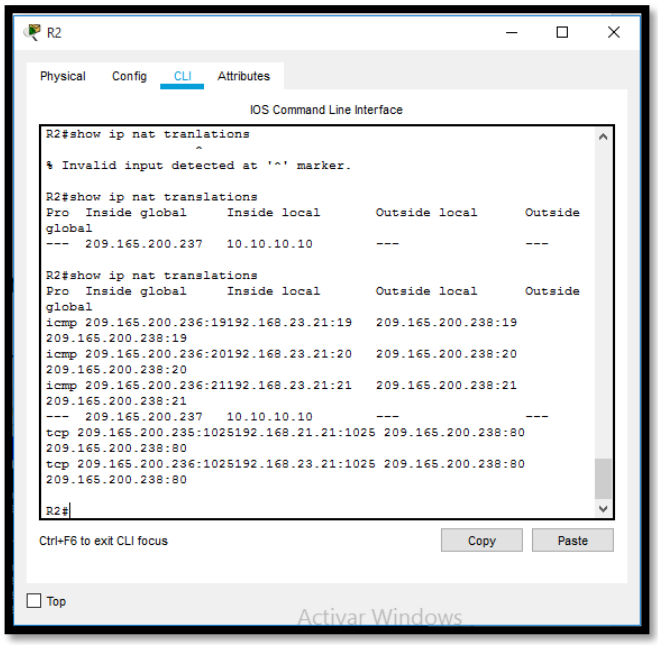

Figura 26 Verificación del comando show ip nat translations.

Verificación de conexión entre PC-A y PC-C al servidor web

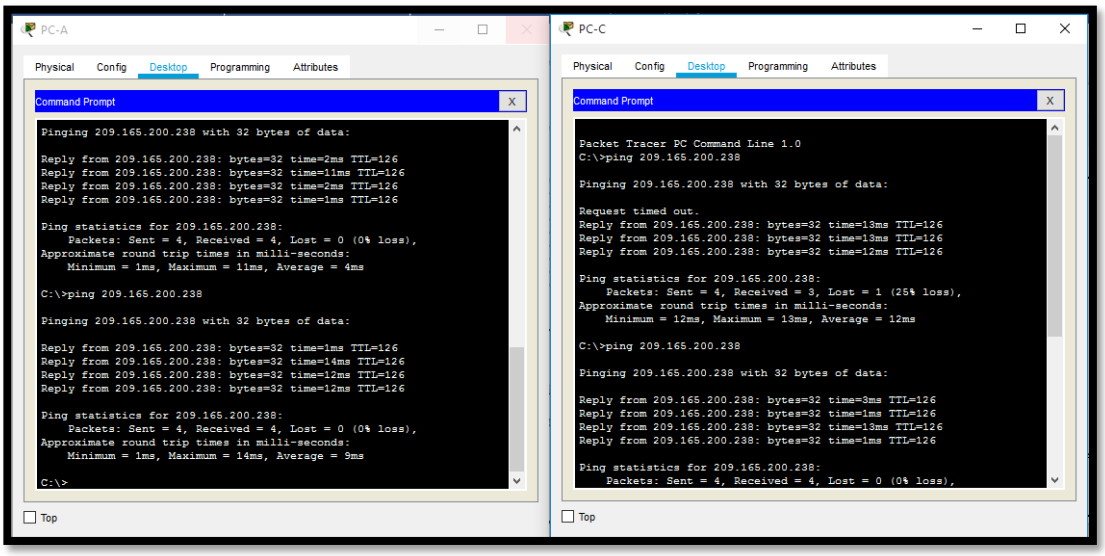

Figura 27 Verificación de conexión entre PC-A y PC-C al servidor web desde el Command Prompt

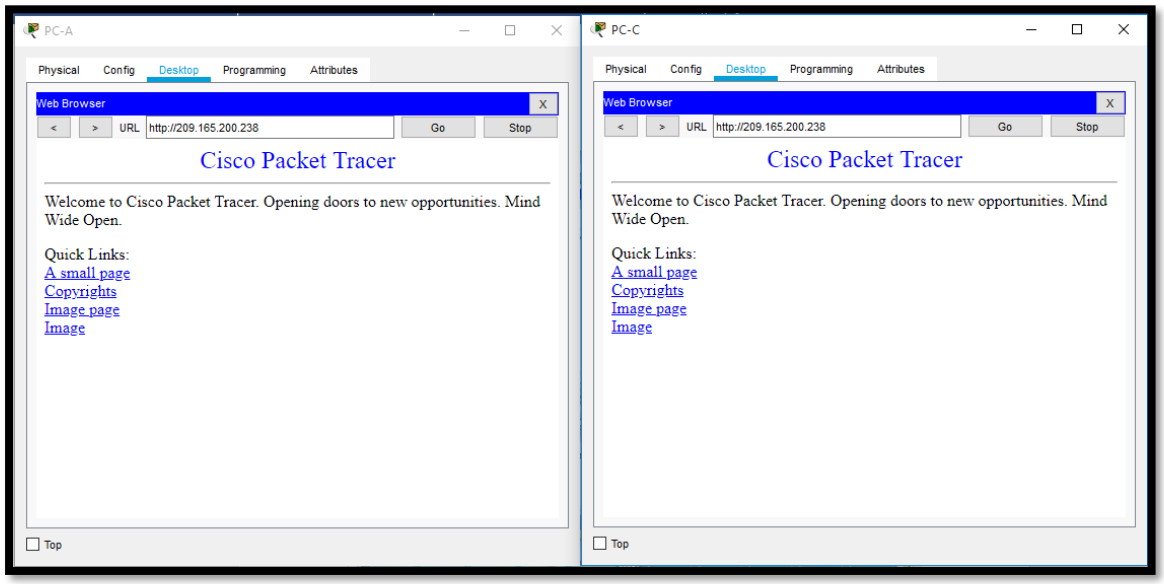

Figura 28 Verificación de conexión entre PC-A y PC-C al servidor web desde el navegador.

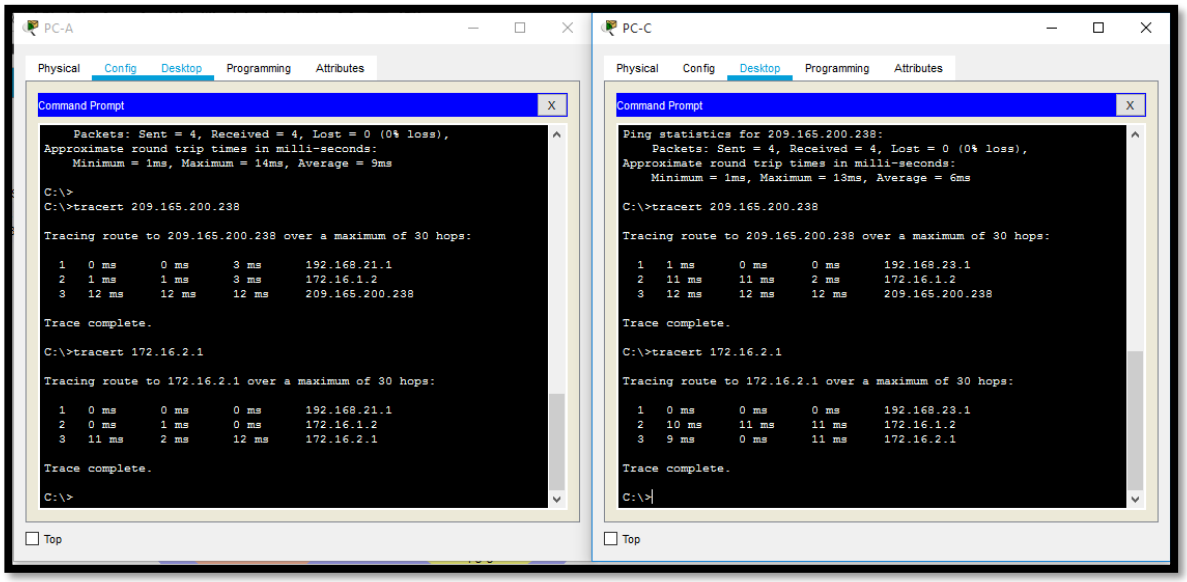

Figura 29 Verificación de la ruta de destino de PC-A y PC-C hasta el servidor de internet a través del comando tracert.

CONCLUSIONES

Con el desarrollo de este trabajo se alcanza satisfactoriamente cada uno de los objetivos solicitados por la guía, adquiriendo buenas prácticas en la solución de problemas de la vida profesional.

Se identifican las herramientas de supervisión y los protocolos de administración de red disponibles en el IOS para solucionar dificultades de las redes de datos
Se configuran los protocolos de enrutamiento solicitados en el ejercicio 2, de acuerdo con las especificaciones de la guía.

Se hacen las configuraciones pedidas en cada uno de los laboratorios de acceso para establecer los escenarios propuestos, para realizar un análisis sobre el comportamiento de los diferentes protocolos y métodos de enrutamiento.

Se solucionan correctamente los problemas de conectividad, asignando seguridad a los dispositivos a través de línea de comandos sobre la consola de los dispositivos de la red.

BIBLIOGRAFÍA

AbaNet. Glosario de términos. [En línea]. [30 junio de 2020] (http://www.abanet.net/glosario.html)

Ariganello, Ernesto. (2016). REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada. Grupo Editorial RA-MA. [En línea]. [30 junio de 2020]. (https://books.google.com.co/books?hl=en&lr=&id=tpBFDwAAQBAJ&oi=fnd&pg=PT7&dq=redes+y+cisco&ots=k5T0x7_M1O&sig=2Y2r0L57mQs-Q3rU1VhstqkAF2s&redir_esc=y#v=onepage&q=redes%20y%20cisco&f=false)

CISCO. Conceptos sobre tecnología de redes [En línea]. [30 junio de 2022] (https://www.cisco.com/c/dam/global/es_mx/solutions/small- business/pdfs/smb-redes-mx.pdf)

CISCO. Cisco.com Worldwide [En línea]. [21 mayo de 2020]. (https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_network_assistant/version5_0/quick/guide/Spanish/gsg_esp/cnapref.html)

Cruz Domínguez José Martín, Mora Cárdenas Gloria Evila], Beatriz Sauza Avila, Pérez Castañeda Suly Sendy, Cruz Ramírez Dorie. Seguridad en redes LAN implementando VLAN [En línea]. [30 Junio de 2020] (https://repository.uaeh.edu.mx/revistas/index.php/sahagun/article/download/2355/2357?inline=1)

MARION, Luis. [mariontechacademy]. (2013, Noviembre 11). CS071 21.04 OSPF - Ruta Acceso a Internet en Packet Tracer [Archivo de video].(https://www.youtube.com/watch?v=vQROsYyB89Q&t=4838s)

Matturro, Gerardo (2007). Introducción a la configuración de routers cisco. [En línea]. [30 junio de 2020]. https://www. ort. edu. uy/fi/pdf/configuracionroutersciscomatturro. Pdf)

SOLUTECSA. Glosario de Internet e informática. [En línea]. [30 junio de 2020] (https://www.internetglosario.com/450/Protocolo.html)