SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

ABEL ANTONIO ALGARRA PAEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - CBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2021

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

ABEL ANTONIO ALGARRA PAEZ

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

TUTOR:
HECTOR MANUEL HERRERA HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 16 de julio de 2021

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por que me ha brindado la oportunidad y la sabiduría para presentar este trabajo, y seguidamente a mi hijo Jhoan, quien ha sido mi motor y principal motivación para culminar mis estudios profesionales. A mi familia que me ha apoyado incondicionalmente y a todas esas personas que de una u otra manera me han impulsado en los momentos que me he sentido agotado y he querido desfallecer.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

RED: Es un conjunto de equipos entrelazados y encargados de transmitir información y servicios en forma de datos entre los diferentes elementos que la conforman.

PACKET TRACER: Es un software diseñado por CISCO para el montaje y simulación de escenarios de redes en donde el estudiante puede diseñar diferentes tipologías de redes y de manera virtual poder realizar una simulación y verificación del funcionamiento del montaje.

SWITCH: Es un equipo que se encarga de la interconexión de los diferentes equipos en una red de área local. Permitiendo comunicarse y compartir información entre sí.

ROUTER: Un router es un dispositivo que permite la interconexión de varias redes. Igualmente nos facilita la conexión con internet. Igualmente es el encargado de dirigir la comunicación en la red y dirigir los datos para que el tráfico se realice de la forma más optima.

HOST Son los terminales, o equipos conectados a una red ya sean computadores, celulares, tablet o impresoras que proveen información e igualmente aprovechan los datos presentes en la red.

RESUMEN

Se realiza en este trabajo la implementación y solución de dos escenarios donde se debemos poner en práctica las habilidades adquiridas a través de los diferentes temas vistos a lo largo del presente curso de CCNA. Con la ayuda del software Packet Tracer se implementarán, configuraran y verificaran los diferentes equipos en los dos escenarios propuestos y se documentara los resultados para sustentar el trabajo realizado y que sustenten los conocimientos previamente adquiridos en los diferentes laboratorios y trabajos colaborativos y que nos afianzaran para diseñar y administrar cualquier red con un alto nivel de calidad y profesionalismo.

Palabras Clave: CISCO, CCNA, Conmutación, VLAN, Enrutamiento, Redes, Packet Tracer.

ABSTRACT

The implementation and solution of two scenarios where we must put into practice the skills acquired through the different topics seen throughout this CCNA course is carried out in this work. With the help of the Packet Tracer software, the different equipment will be implemented, configured and verified in the two proposed scenarios and the results will be documented to support the work carried out and that support the knowledge previously acquired in the different laboratories and collaborative works and that will strengthen us to design and manage any network with a high level of quality and professionalism.

Keywords: CISCO, CCNA, Routing, VLAN, Swicthing, Networking, Packet Tracer.

INTRODUCCIÓN

No es desconocido por nadie que actualmente el mundo se mueve en un ámbito digita, manejamos todo desde la palma de la mano, podemos desde configurar el nivel de las luces de nuestra habitación, hasta realizar una compra a miles de kilómetros con solo un clic. Todo esto es gracias a las redes de comunicaciones ya sean alámbricas o inalámbricas, toda esa telaraña de equipos que conforman la una red de comunicaciones o de datos, está conformada por equipo que de no ser configurados o administrados correctamente solo serial elementos sin importancia. Es ahí donde resalta la importancia de saber diseñar y configurar una red de datos. Y es gracias a este Diplomado de Profundización CISCO CCNA donde aprenderemos a realizar estas tareas de una forma profesional.

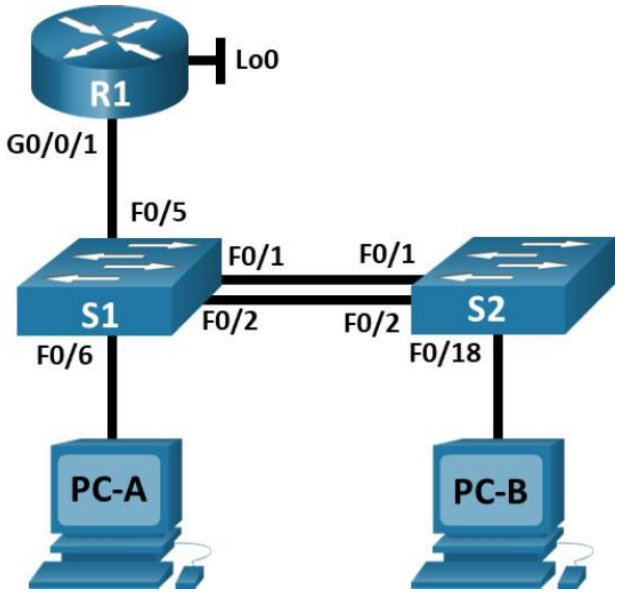
Para este trabajo se plantearon dos escenarios, donde con la ayuda del software Packet Traicer y de los conocimientos adquiridos a lo largo del curso se llevará acabo la implementación, análisis y configuración de los diferentes equipos para dar una solución óptima a estos escenarios.

DESARROLLO

ESCENARIO 1

Topología

Figura 1. Topología del Escenario 1.



Fuente: Prueba de habilidades CCNA CISCO

En este primer 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. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla 1. Tabla de VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management

5	Parking
6	Native

Asignación de nombres a las redes VLAN.

Tabla 2. Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.21.5.1 /26	No corresponde
	2001:db5:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.21.5.65 /27	No corresponde
	2001:db5:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.21.5.97 /29	No corresponde
	2001:db5:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.21.5.98 /29	10.21.5.97
	2001:db5:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.21.5.99 /29	10.21.5.97
	2001:db5: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:db5:acad:a: :50 /64	fe80::1

PC-B NIC	DHCP para dirección IPv4 2001:db5:acad:b: :50 /64	DHCP para puerta de enlace predeterminada IPv4 fe80::1

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

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.

  En el Router:

  Router>enable
  Router#erase startup-config
  Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
  [OK]
  Erase of nvram: complete
  %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
  Router#reload
  Proceed with reload? [confirm]

  En los Switch´s:

  Switch>enable
  Switch#erase startup-config
  Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]y[OK]
  Erase of nvram: complete
  %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
  Switch#delete vlan.dat
  Delete filename [vlan.dat]?y
  Delete flash:/y? [confirm]
  %Error deleting flash:/y (No such file or directory)

  Switch#reload

Proceed with reload? [confirm]y

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

  Se confirma si la plantilla SDM de los switch´s admiten IPv6:

  Switch>enable
  Switch#show sdm prefer
  The current template is "desktop default" template.
  The selected template optimizes the resources in
  the switch to support this level of features for
  8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses: 6K
  number of IPv4 IGMP groups + multicast routes: 1K
  number of IPv4 unicast routes: 8K
  number of directly-connected IPv4 hosts: 6K
  number of indirect IPv4 routes: 2K
  number of IPv4 policy based routing aces: 0
  number of IPv4/MAC qos aces: 0.5K
  number of IPv4/MAC security aces: 1K

  Se observa que la plantilla SDM de los switch´s no admiten IPv6. Por lo cual es necesario configurar la plantilla SDM de los switch para que admitan IPv6:

  Switch#configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
  Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
  Use 'show sdm prefer' to see what SDM preference is currently active.
  Switch(config)#end
  Switch#
  %SYS-5-CONFIG_I: Configured from console by console

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

  Ahora se vuelve a confirmar que la plantilla SDM de los switch´s soporte IPv6:

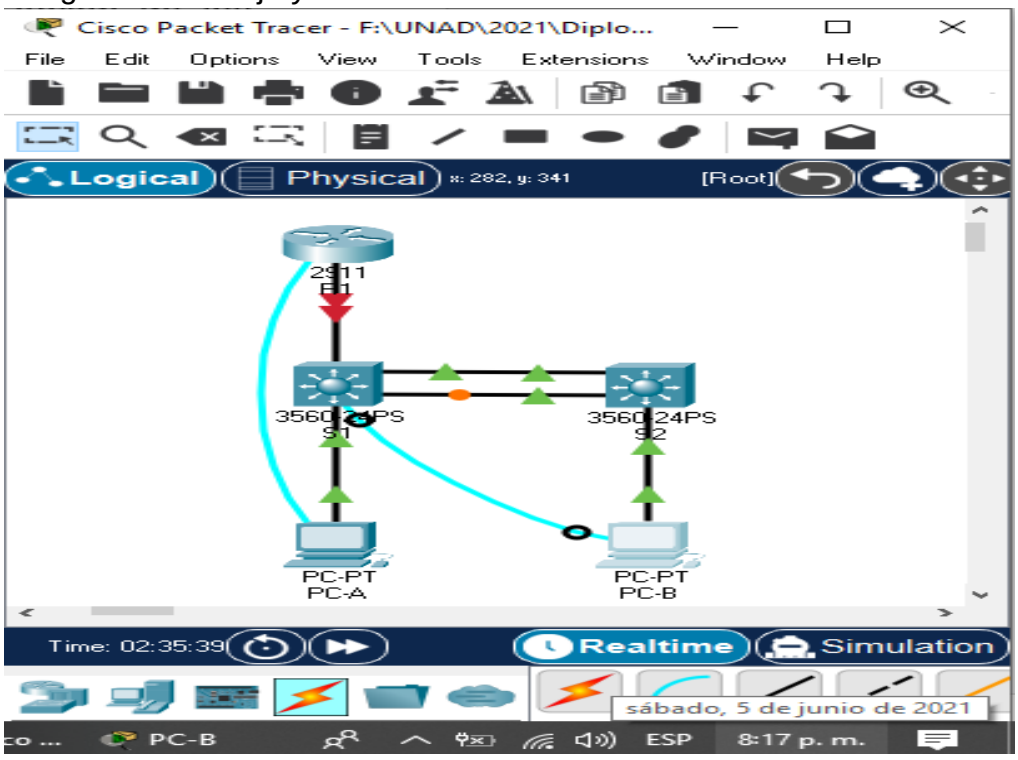
  Switch>enable
  Switch#show sdm prefer

The current template is "desktop IPv4 and IPv6 default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 2K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 3K
number of directly-connected IPv4 hosts: 2K
number of indirect IPv4 routes: 1K
number of IPv6 multicast groups: 1.125k
number of directly-connected IPv6 addresses: 2K
number of indirect IPv6 unicast routes: 1K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K
number of IPv6 policy based routing aces: 0
number of IPv6 qos aces: 0.625k
number of IPv6 security aces: 0.5K

Se observa que la plantilla SDM de los switch´s soporta IPv6.

Figura 2. Montaje y simulación del Escenario 1 en Packet Tracer.



Fuente: Autor

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Tareas de configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	**R1** Router(config)#hostname R1
Nombre de dominio	**ccna-lab.com** R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass** R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	**10 caracteres** R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin** **Password: admin1pass** R1(config)#username admin password admin1pass

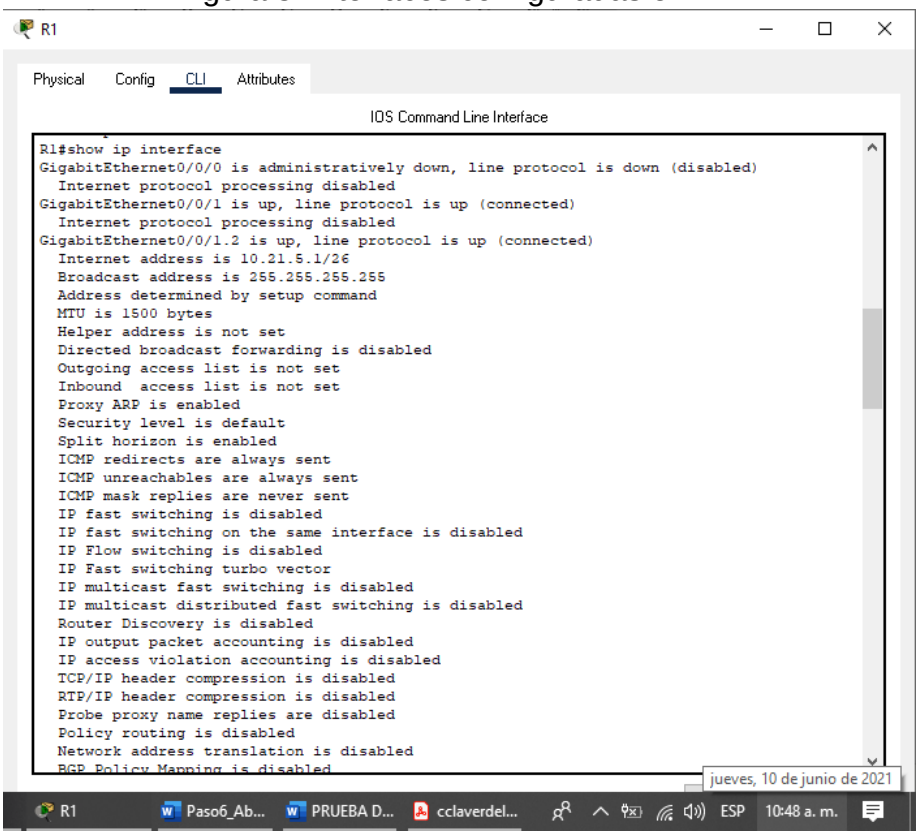
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 15 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input ssh R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd %Prohibido el acceso a personal no autorizado% R1(config)#exit
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	**Establezca la descripción** **Establece la dirección IPv4.** **Establezca la dirección local de enlace IPv6 como fe80: :1** **Establece la dirección IPv6.** **Activar la interfaz.** R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.21.5.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown

	R1(config-subif)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description Native R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description Management R1(config-subif)#ip address 10.21.5.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db5:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown
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** R1(config)#interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)#description Servicio-Internet R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	**Módulo de 1024 bits** R1(config)#crypto key generate rsa general-keys modulus 1024 % Invalid input detected at '^' marker. 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]

En este paso se realiza la configuración inicial del router R1, se desactiva la búsqueda de DNS, se le asigna nombre al router, al dominio y se asignan las diferentes contraseñas de protección tanto para ingreso a la consola como al modo privilegiado, etas contraseñas son encriptadas para que no se puedan visualizar en el archivo de configuración. Se configuran las líneas VTY y el aviso o banner de bienvenida. Adicionalmente se configuran las diferentes interfaces del router.

Figura 3. Interfaces configuradas en R1.



Fuente: Autor

Por medio del comando show ip interface podemos revisar el estado y configuración de todas las interfaces del router R1.

Paso 3: Configurar S1 y S2.

Las tareas de configuración incluyen lo siguiente:

Tabla 4. Tareas de configuración para S1

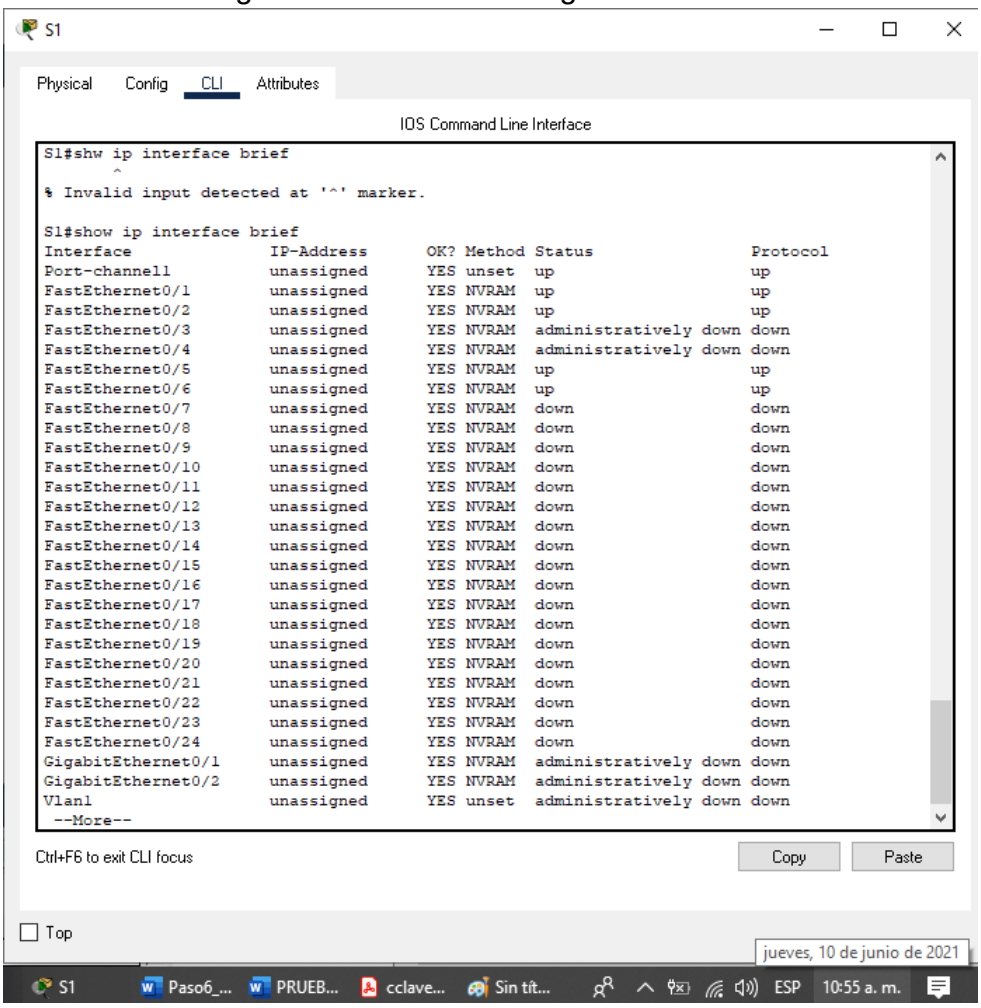
Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda** Switch(config)#hostname S1
Nombre de dominio	**ccna-lab.com** S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass** S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin** **Password: admin1pass** S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local

Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd %Acceso restringido. Solo personal autorizado%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1(config)#crypto key generate rsa general-keys modulus 1024 % Invalid input detected at '^' marker. S1(config)#crypto key generate rsa The name for the keys will be: S1.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]
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 4 *Mar 1 4:6:20.775: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip address 10.21.5.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db5:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local

	S1(config-if)#description Magnament Interface S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	**Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4** S1(config)#ip default-gateway 10.21.5.97

En la configuración de los switch se le asignan nombre, contraseñas de protección para el acceso general y el privilegiado y se muestra un mensaje de advertencia al iniciar el switch. Y se configuran las líneas VTY y se encriptan las contraseñas.

Figura 4. Interfaces configuradas en S1.



Fuente: Autor

Por medio de la instrucción show ip interface brief podemos revisar el estado y configuración de todas las interfaces del switch S1.

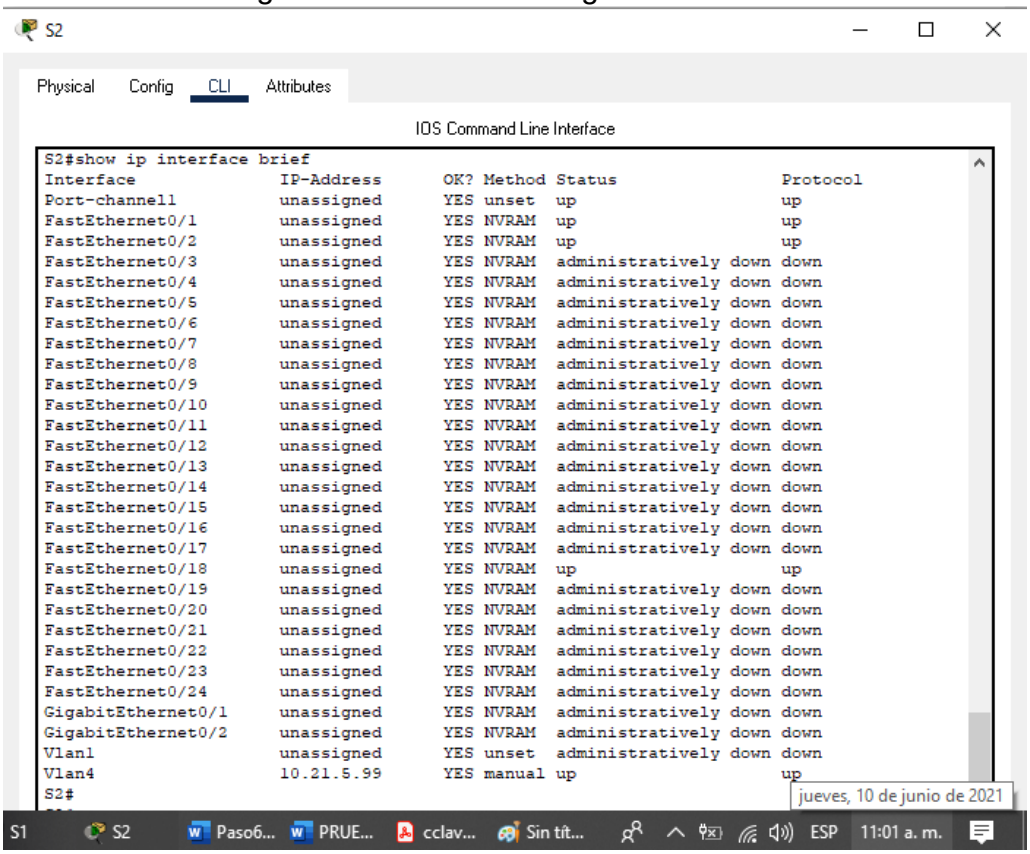
Tabla 5. Tareas de configuración para S2

Tarea	Especificación
Desactivar la búsqueda DNS.	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda** Switch(config)#hostname S2
Nombre de dominio	**ccna-lab.com** S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass** S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin** **Password: admin1pass** S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd %Acceso restringido. Solo personal autorizado%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S2(config)#crypto key generate rsa general-keys modulus 1024 % Invalid input detected at '^' marker. S1(config)#crypto key generate rsa The name for the keys will be: S2.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]
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** S2(config)#interface vlan 4 *Mar 1 4:6:20.775: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config-if)#ip address 10.21.5.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db5:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Magnament Interface S2(config-if)#no shutdown S2(config-if)#exit

Configuración del gateway predeterminado	**Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4** S2(config)#ip default-gateway 10.21.5.97

Figura 5. Interfaces configuradas en S2.



Fuente: Autor

Por medio de la instrucción show ip interface brief podemos revisar el estado y configuración de todas las interfaces del switch S2.

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configuración VLAN del S1

Tarea	Especificación
Crear VLAN	**VLAN 2, nombre Bikes** **VLAN 3, nombre Trikes** **VLAN 4, name Management** **VLAN 5, nombre Parking** **VLAN 6, nombre Native** S1>enable Password: S1#config terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)# %LINK-5-CHANGED: Interface Vlan4, changed state to up S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**Interfaces F0/1, F0/2 y F0/5** S1#config terminal Enter configuration commands, one per line. End with CNTL/Z. S1(config)#interface f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#

	%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up S1(config-if)#switchport trunk native vlan 6 S1(config-if)#interface range f0/1-2 S1(config-if-range)#shutdown S1(config-if-range)# %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación**

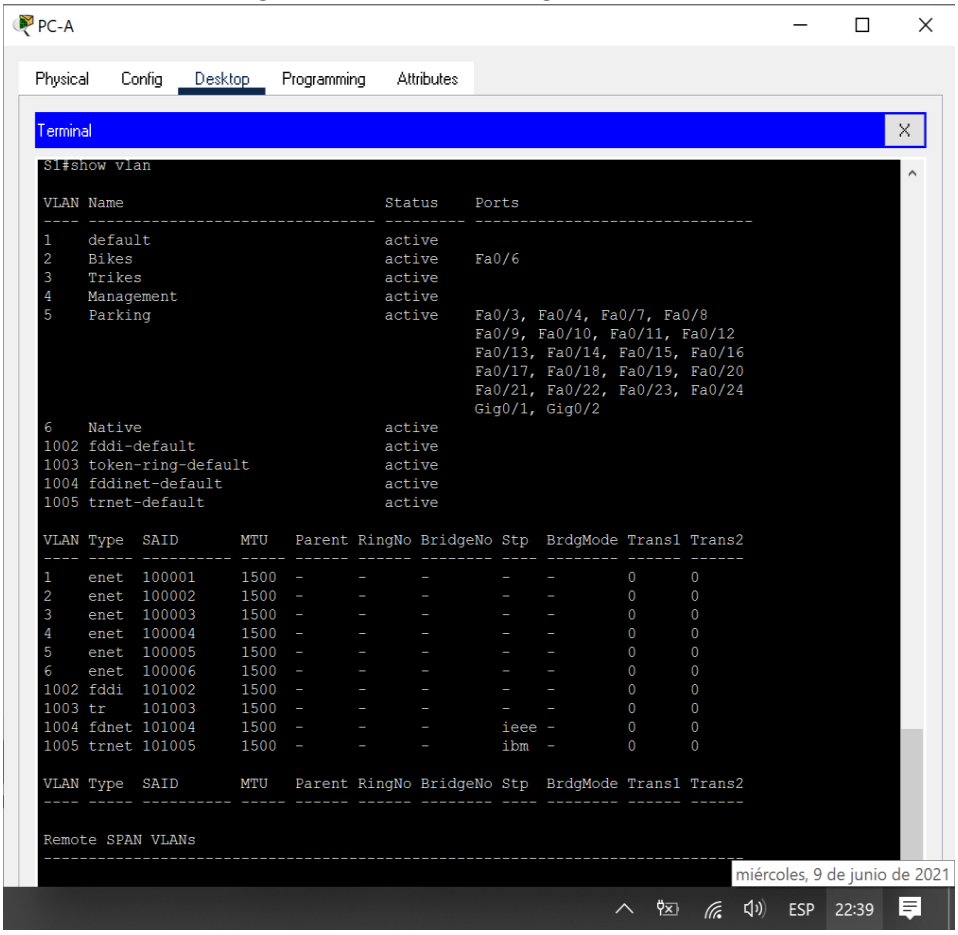
	S1(config-if-range)#channel-group 1 mode active S1(config-if-range)# Creating a port-channel interface Port-channel 1 %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1) %EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (native vlan of Fa0/2 is 6, Po1 id 1) S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	**Interface F0/6** S1(config-if)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	**Permitir 3 direcciones MAC** S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	**Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar.** S1(config-if)#interface range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5

	S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down S1(config-if-range)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

Figura 6. VLANs configuradas en S1



Fuente: Autor

Por medio de la instrucción show vlan se observan el nombre, el estado y los puertos asignados a las redes VLAN creada en el switch S1.

Paso 2: Configurar el S2.

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

Tabla 7. Configuración VLAN del S2

Tarea	Especificación
Crear VLAN	**VLAN 2, name Bikes** **VLAN 3, name Trikes** **VLAN 4, name Management** **VLAN 5, nombre Parking**

	VLAN 6, nombre Native S2>enable Password: S2#config terminal Enter configuration commands, one per line. End with CNTL/Z. S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)# %LINK-5-CHANGED: Interface Vlan4, changed state to up S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**Interfaces F0/1 y F0/2** S2(config)#interface range f0/1-2 S2(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down S2(config-if-range)#switchport trun encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6

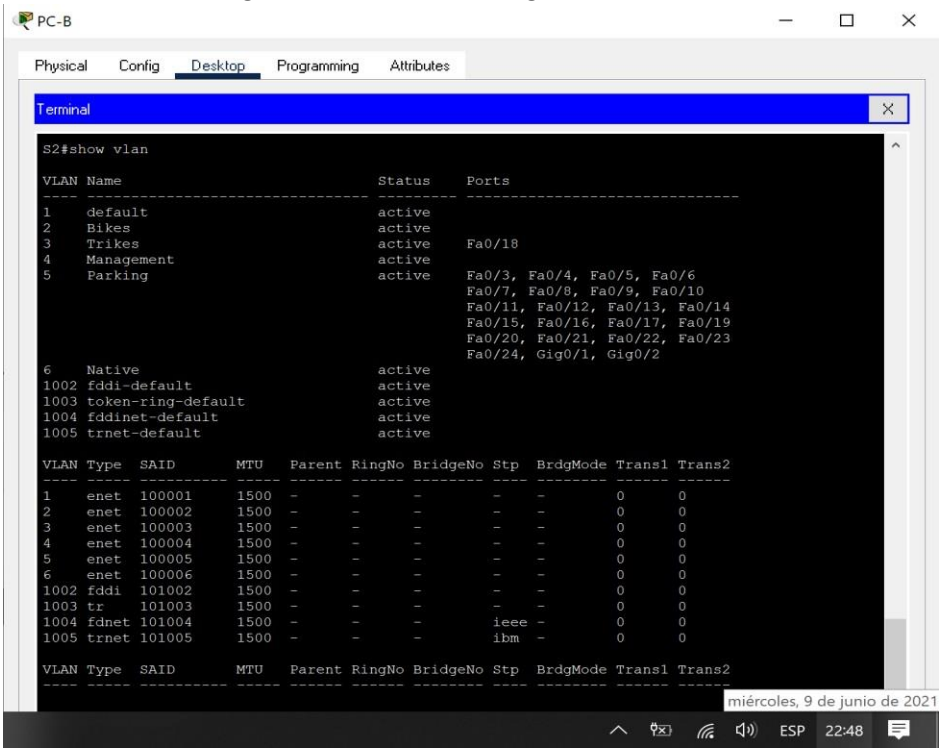
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 %EC-5-CANNOT_BUNDLE2: Fa0/1 is not compatible with Po1 and will be suspended (native vlan of Fa0/1 is 6, Po1 id 1) %EC-5-CANNOT_BUNDLE2: Fa0/2 is not compatible with Po1 and will be suspended (native vlan of Fa0/2 is 6, Po1 id 1) 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 6
Configurar el puerto de acceso del host para la VLAN 3	**Interfaz F0/18** S2(config-if)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	**permite 3 MAC addresses** S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	**Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar** S2(config-if)#interface range f0/3-17 S2(config-if-range)#switchport mode access

	S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down S2(config-if-range)#interface range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

	%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down S2(config-if-range)#interface range g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down

Figura 7. VLANs configuradas en S2



Fuente: Autor

Por medio de la instrucción show vlan se observan el nombre, el estado y los puertos asignados a las redes VLAN creada en el switch S1.

Luego de realizar esta configuración se deben encender las dos interfaces FastEthernet que se habían apagado durante la configuración.

Para S1:

S1(config)#interface range f0/1-2
S1(config-if-range)#no shutdown

S1(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Para S2:

S2(config-if-range)#interface range f0/1-2
S2(config-if-range)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to down

Parte 3: Configurar soporte de host

Paso 1: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 8. Configuración soporte host para R1

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 Loopback0 R1(config)#ipv6 route ::/0 Loopback 0 R1(config)#exit
Configurar IPv4 DHCP para VLAN 2	**Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada**

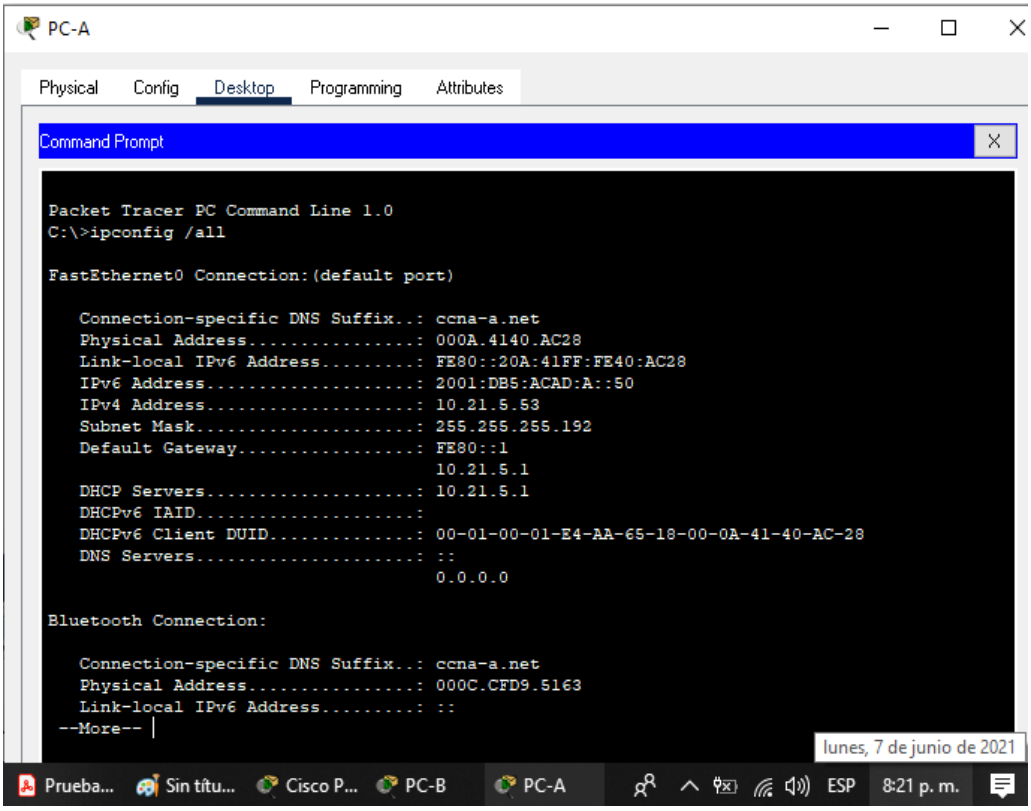
	R1(config)#ip dhcp excluded-address 10.21.5.1 10.21.5.52 R1(config)#ip dhcp pool Vlan2_Bikes R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	**Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.** R1(config)#ip dhcp excluded-address 10.21.5.65 10.21.5.84 R1(config)#ip dhcp pool Vlan3_Trikes R1(dhcp-config)#network 10.21.5.64 255.255.255.224 R1(dhcp-config)#default-router 10.21.5.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit R1#copy running-config startup-config

En esta parte se crea la ruta predeterminada para IPv4 e IPv6 que enrutaran el tráfico hacia internet. Luego se configuran el rango en los cuales se asignarán automáticamente las ip de los equipos que se conecten a la VLAN 2 y VLAN 3.

Paso 2: Configurar los servidores

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

Figura 8. Configuración parámetros de red PC-A

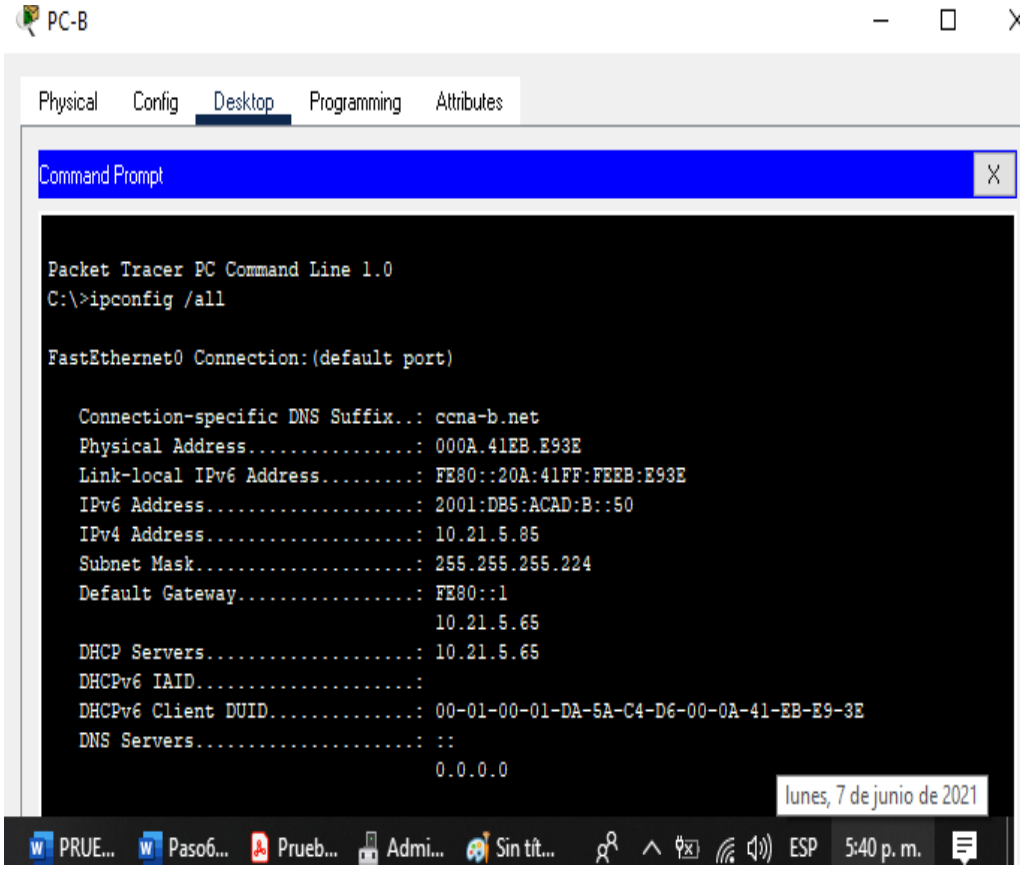


Fuente: Autor

Tabla 9. Configuración de host PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	000A.4140.AC28
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Figura 9. Configuración parámetros de red PC-B



Fuente: Autor

Tabla 10. Configuración de host PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000A.41EB.E93E
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Parte 4: Probar y verificar la conectividad de extremo a extremo

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

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.
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:

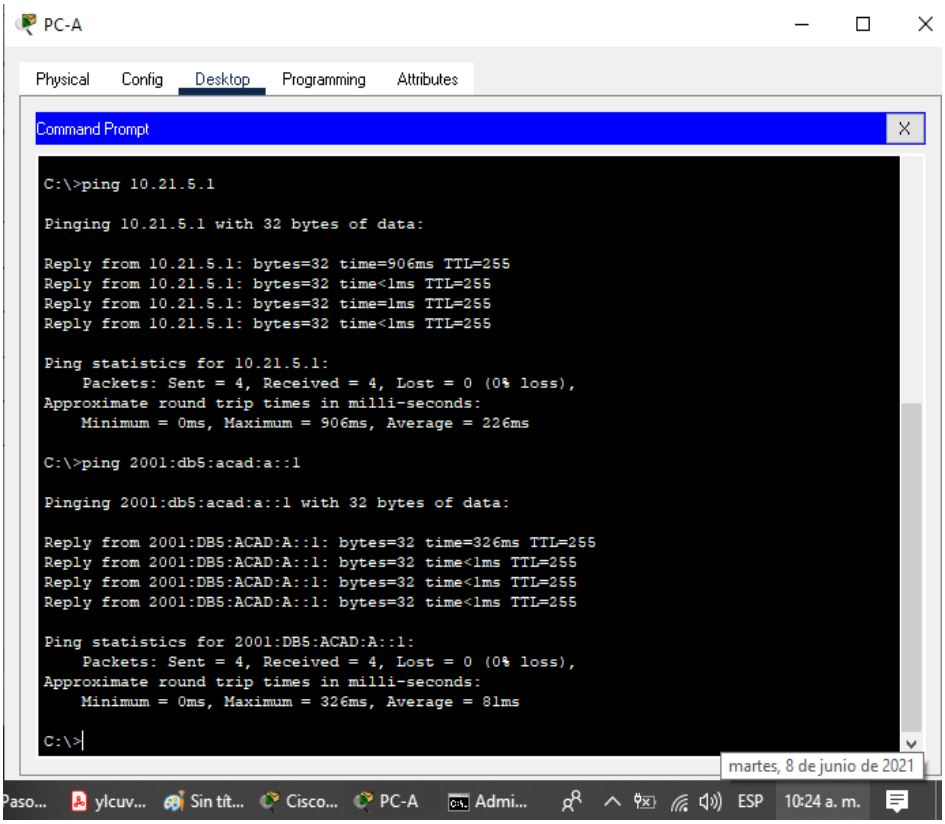
Tabla 11. Conectividad IPv4 e IPv6 entre dispositivos de la red.

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	**Satisfactorio**
		IPv6	2001:db5:acad:a: :1	**Satisfactorio**
	R1, G0/0/1.3	Dirección	10.21.5.65	**Satisfactorio**
		IPv6	2001:db5:acad:b: :1	**Satisfactorio**
	R1, G0/0/1.4	Dirección	10.21.5.97	**Satisfactorio**
		IPv6	2001:db5:acad:c: :1	**Satisfactorio**
	S1, VLAN 4	Dirección	10.21.5.98	**Satisfactorio**
		IPv6	2001:db5:acad:c: :98	**Satisfactorio**
	S2, VLAN 4	Dirección	10.21.5.99.	**Satisfactorio**
		IPv6	2001:db5:acad:c: :99	**Satisfactorio**
	PC-B	Dirección	IP address will vary.	**Satisfactorio**
		IPv6	2001:db5:acad:b: :50	**Satisfactorio**
	R1 Bucle 0	Dirección	209.165.201.1	**Satisfactorio**
PC-B	R1 Bucle 0	Dirección	209.165.201.1	**Satisfactorio**
		IPv6	2001:db5:acad:209: :1	**Satisfactorio**
		Dirección	10.21.5.1	**Satisfactorio**

	R1, G0/0/1.2	IPv6	2001:db5:acad:a: :1	**Satisfactorio**
	R1, G0/0/1.3	Dirección	10.21.5.65	**Satisfactorio**
		IPv6	2001:db5:acad:b: :1	**Satisfactorio**
	R1, G0/0/1.4	Dirección	10.21.5.97	**Satisfactorio**
		IPv6	2001:db5:acad:c: :1	**Satisfactorio**
	S1, VLAN 4	Dirección	10.21.5.98	**Satisfactorio**
		IPv6	2001:db5:acad:c: :98	**Satisfactorio**
	S2, VLAN 4	Dirección	10.21.5.99.	**Satisfactorio**
		IPv6	2001:db5:acad:c: :99	**Satisfactorio**

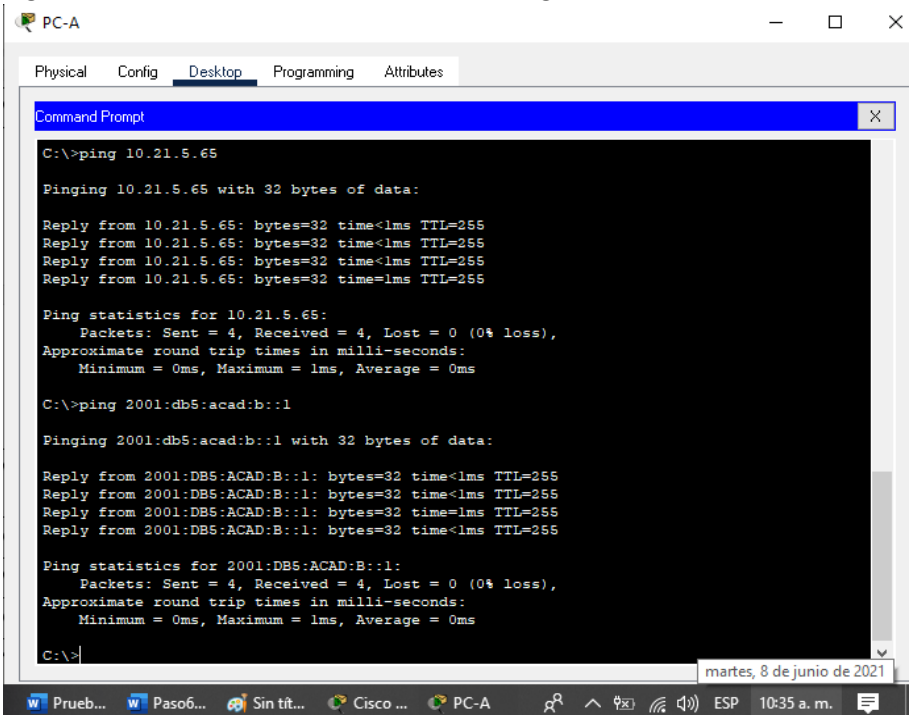
Pruebas de conectividad

Figura 10. Prueba de conectividad Ping del PC-A a R1, G0/0/1.2.



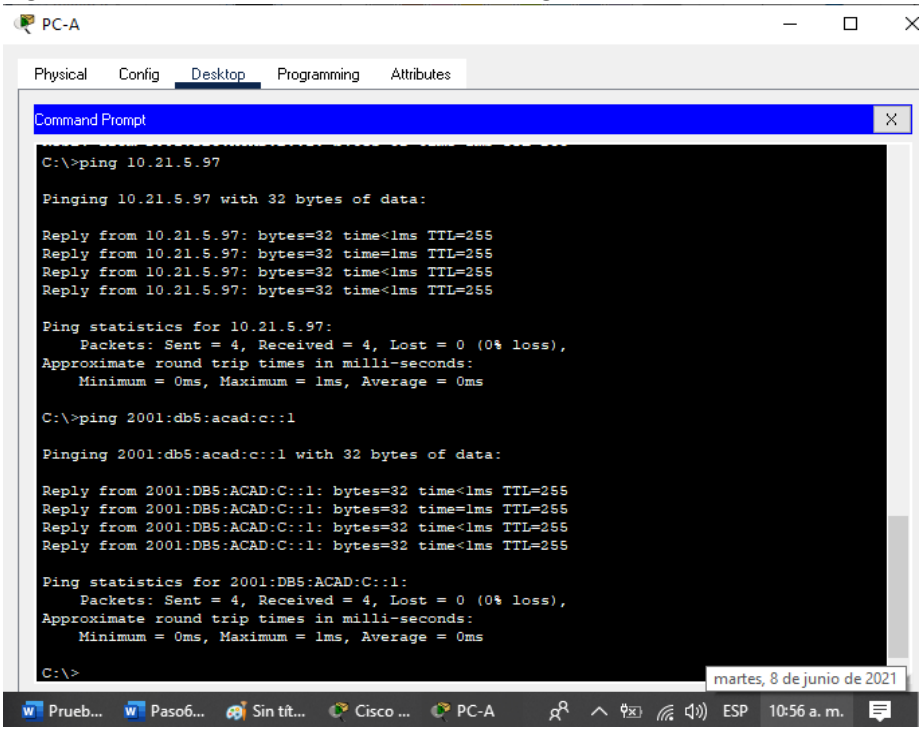
Fuente: Autor

Figura 11. Prueba de conectividad Ping del PC-A a R1, G0/0/1.3.



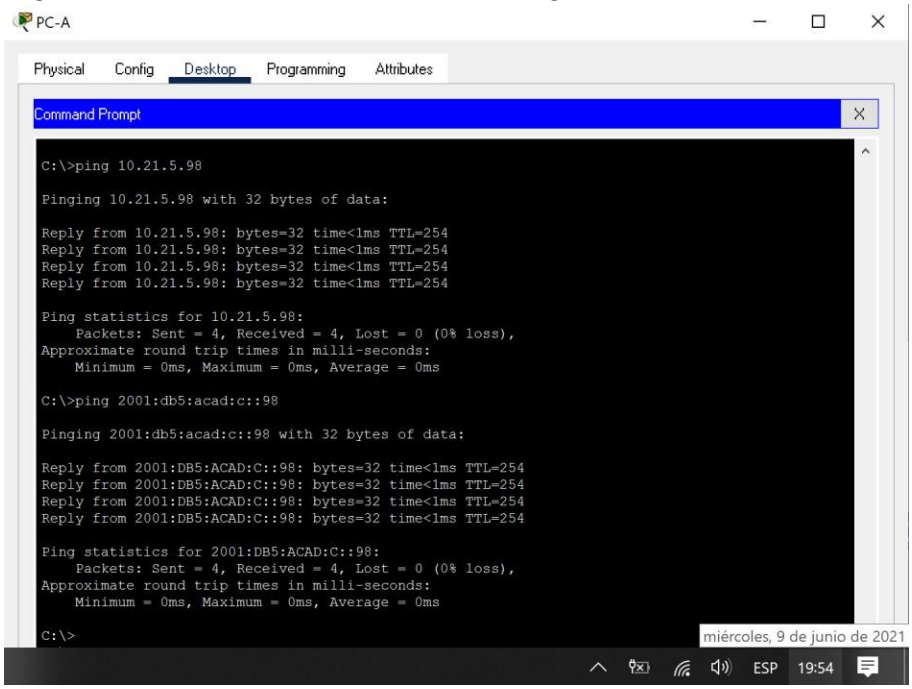
Fuente: Autor

Figura 12. Prueba de conectividad Ping del PC-A a R1, G0/0/1.4.



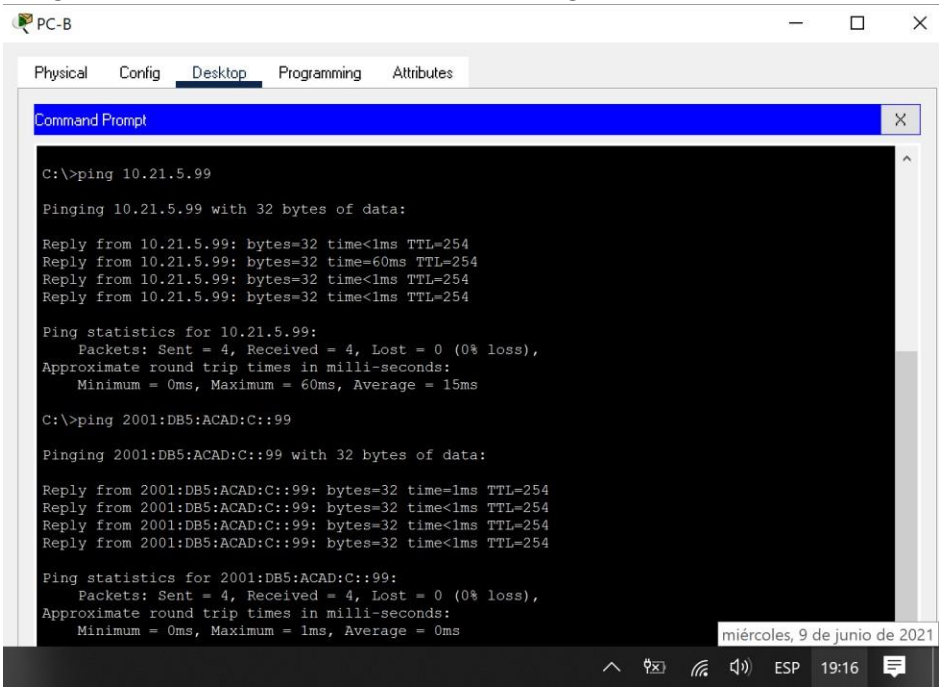
Fuente: Autor

Figura 13. Prueba de conectividad Ping del PC-A a S1, VLAN 4.



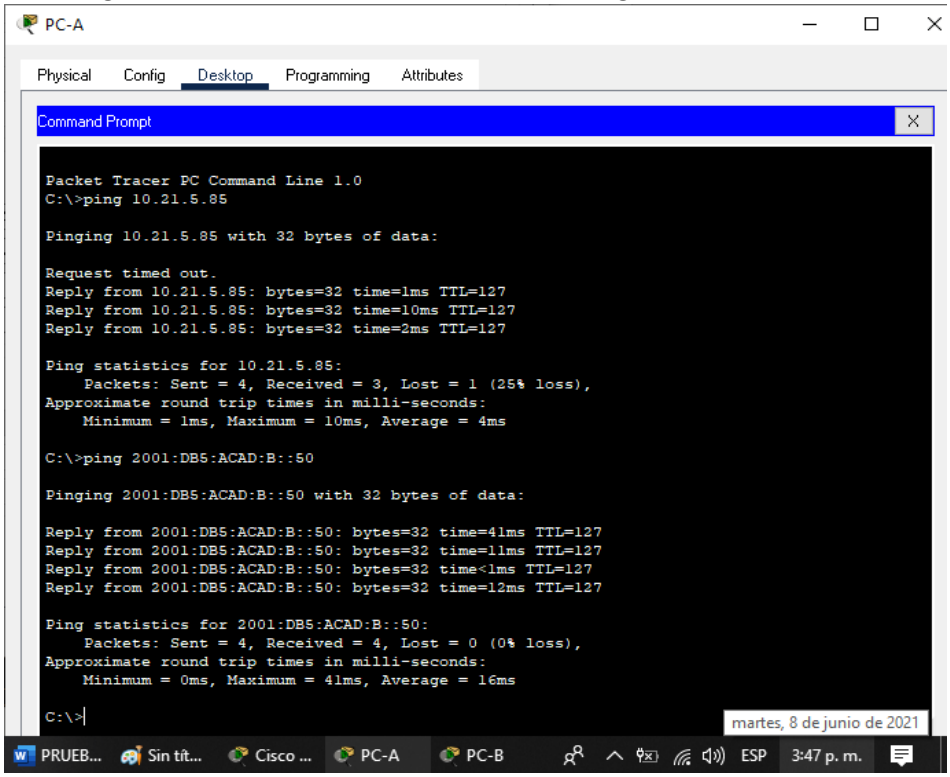
Fuente: Autor

Figura 14. Prueba de conectividad Ping del PC-A a S2, VLAN 4



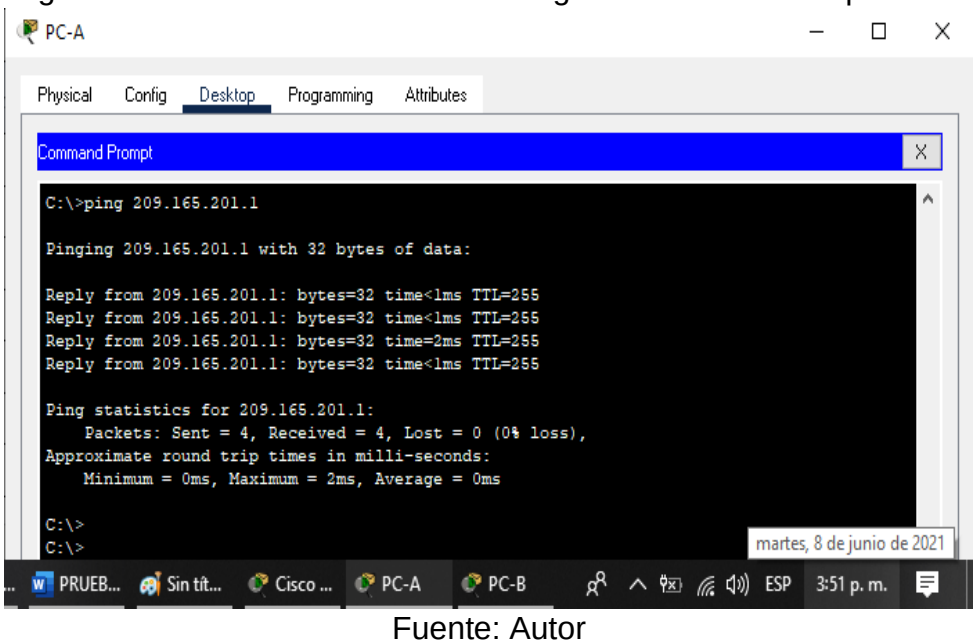
Fuente: Autor

Figura 15. Prueba de conectividad Ping del PC-A a PC-B



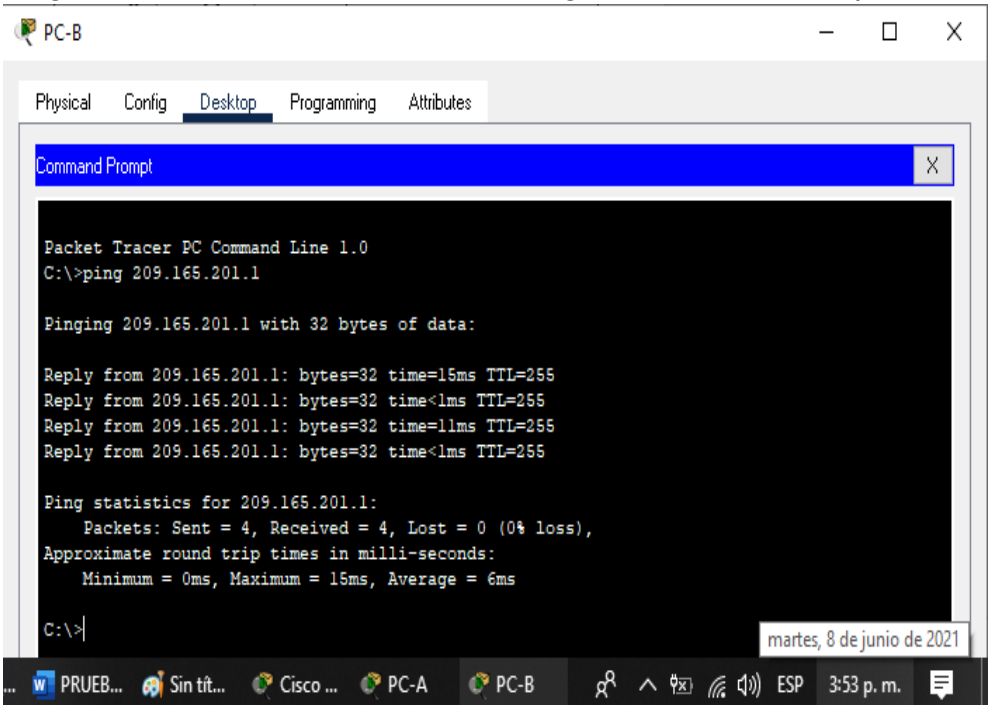
Fuente: Autor

Figura 16. Prueba de conectividad Ping del PC-A a R1 Loopback 0.



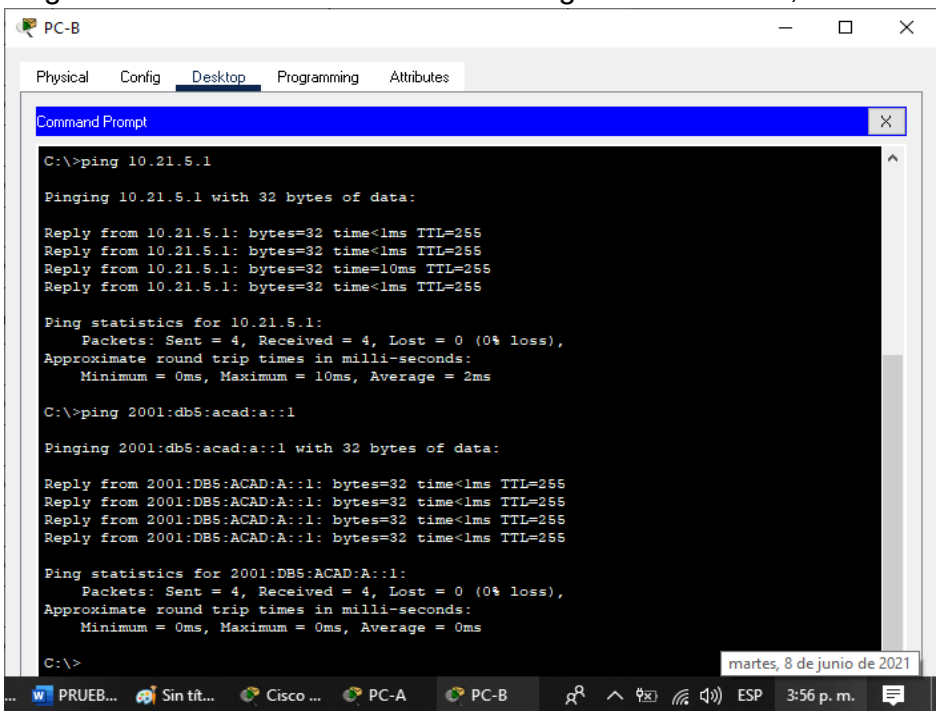
Fuente: Autor

Figura 17. Prueba de conectividad Ping del PC-B a R1 Loopback 0.



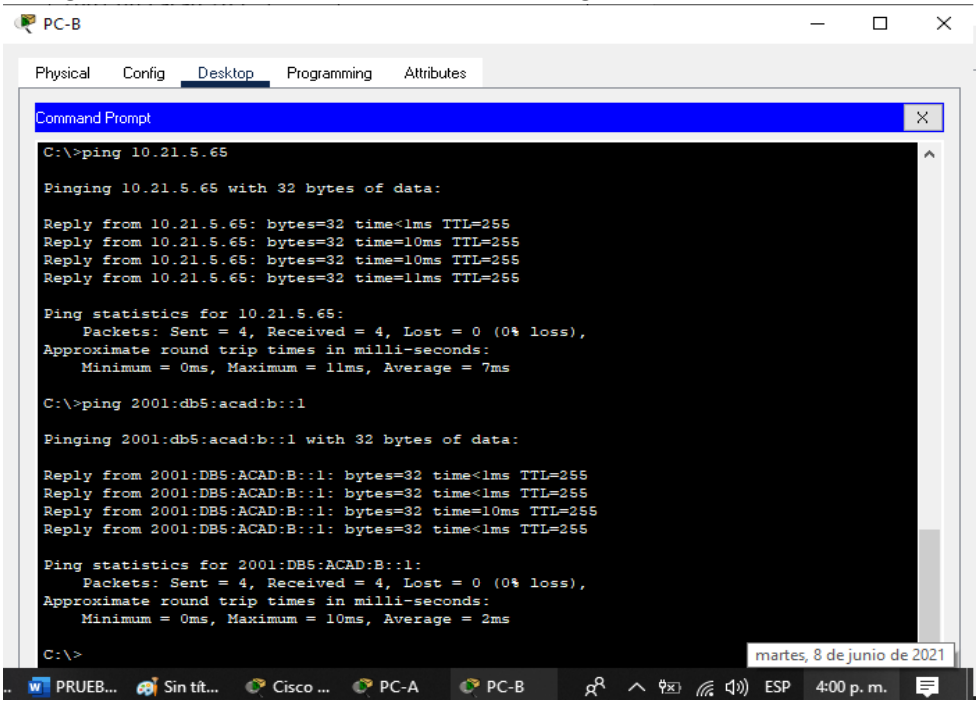
Fuente: Autor

Figura 18. Prueba de conectividad Ping del PC-B a R1, G0/0/1.2



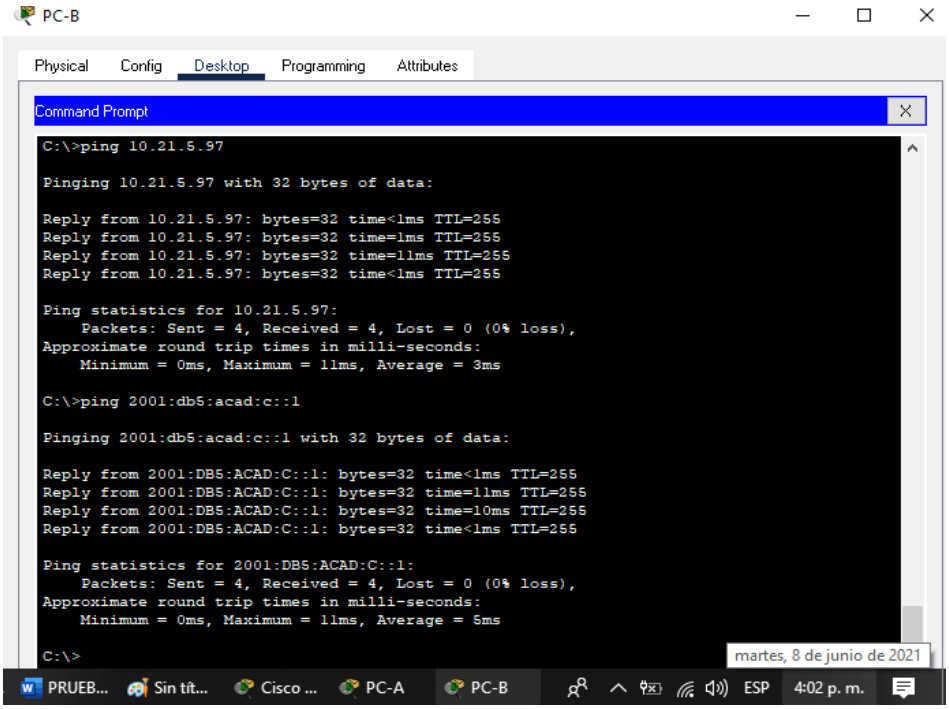
Fuente: Autor

Figura 19. Prueba de conectividad Ping del PC-B a R1, G0/0/1.3



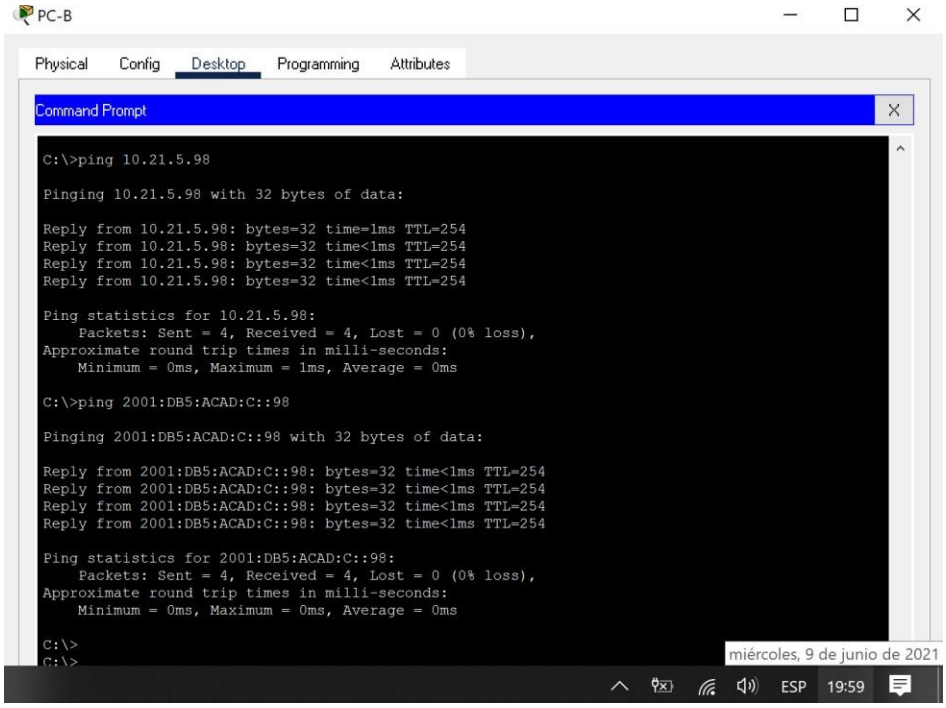
Fuente: Autor

Figura 20. Prueba de conectividad Ping del PC-B a R1, G0/0/1.4



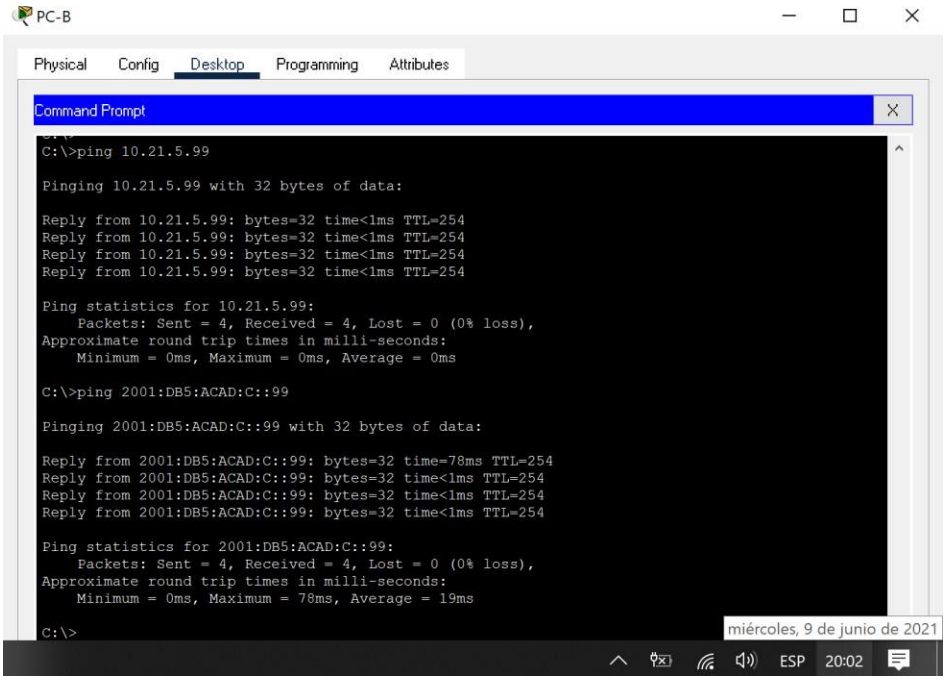
Fuente: Autor

Figura 21. Prueba de conectividad Ping del PC-B a S1, VLAN 4



Fuente: Autor

Figura 22. Prueba de conectividad Ping del PC-B a S2, VLAN 4

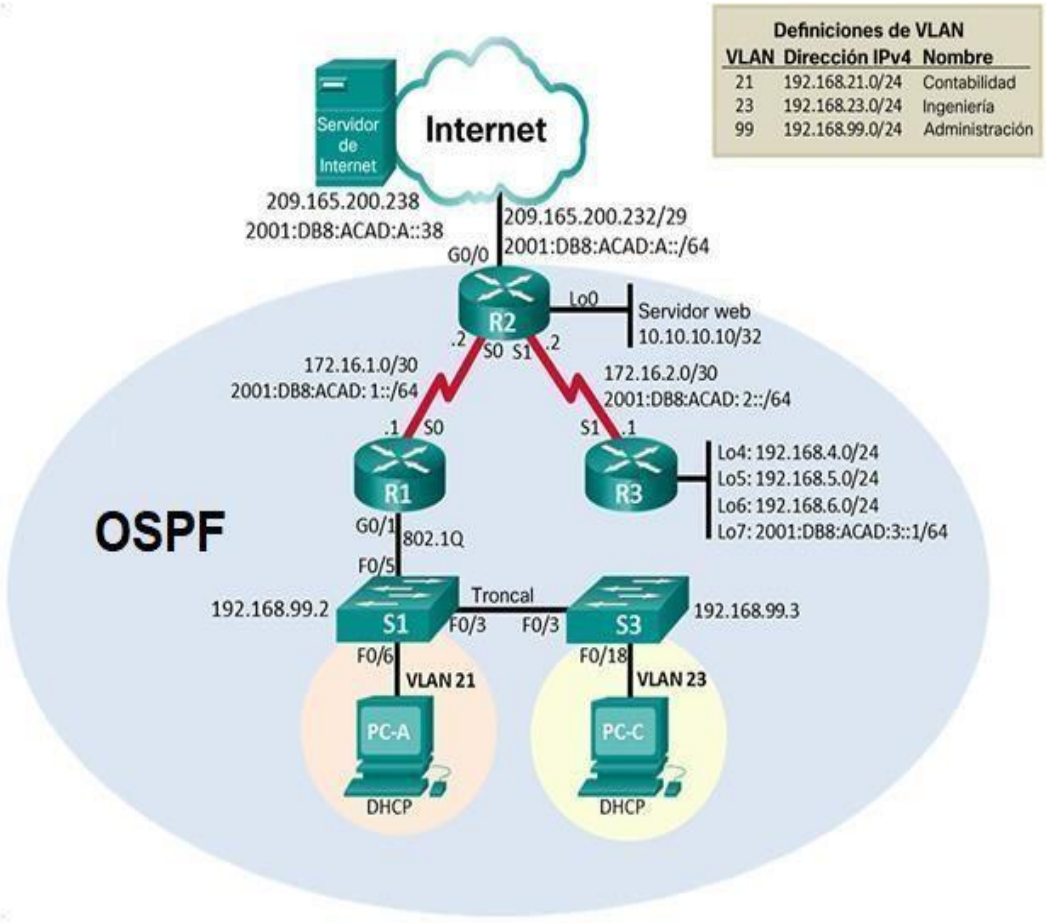


Fuente: Autor

ESCENARIO 2

Topología

Figura 23. Topología del Escenario 2.



Fuente: Prueba de habilidades CCNA CISCO

Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, 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.

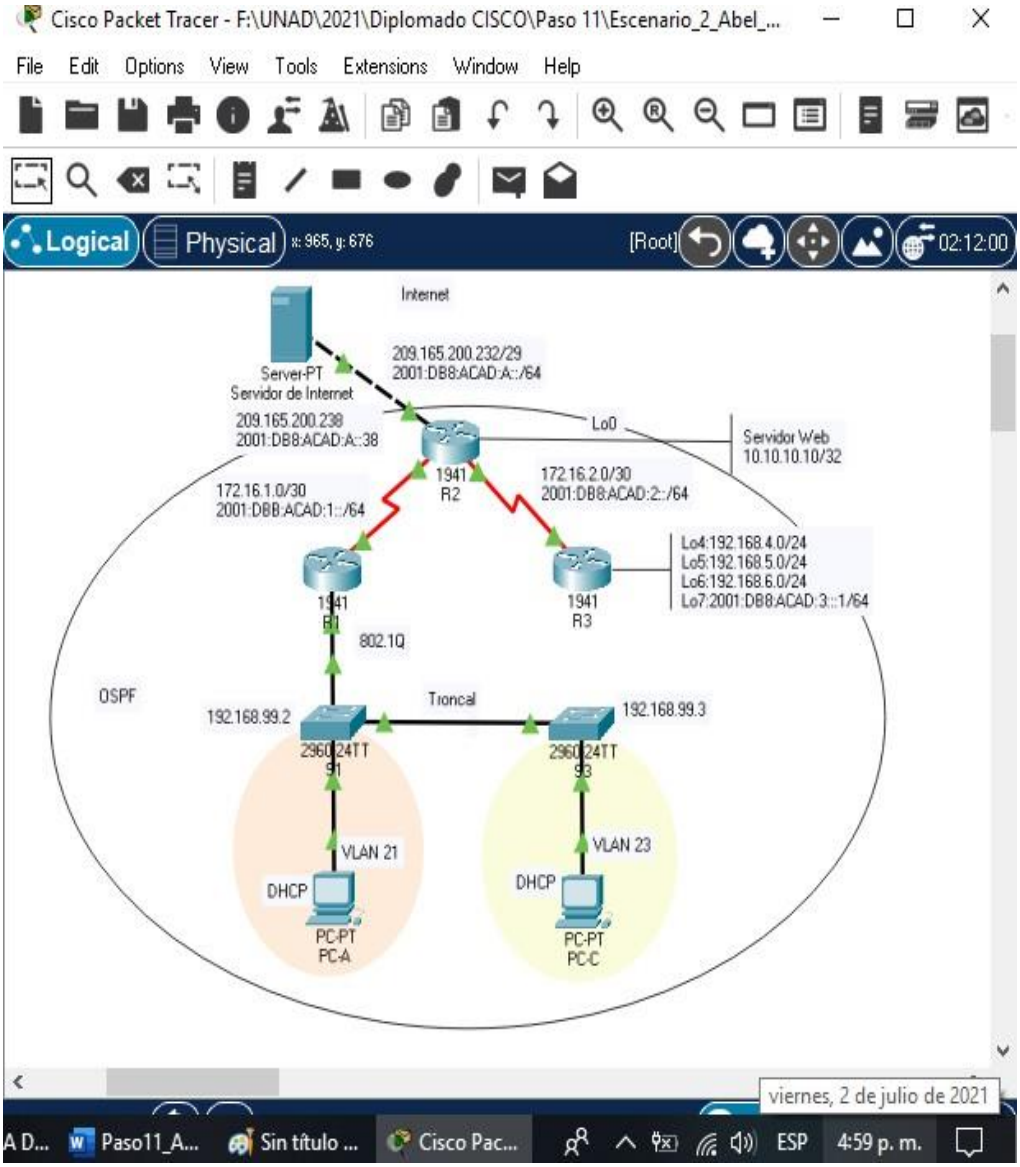
Parte 1: Inicializar dispositivos

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

- Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

  Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Figura 24. Montaje y simulación del escenario 2 en Packet Tracer.

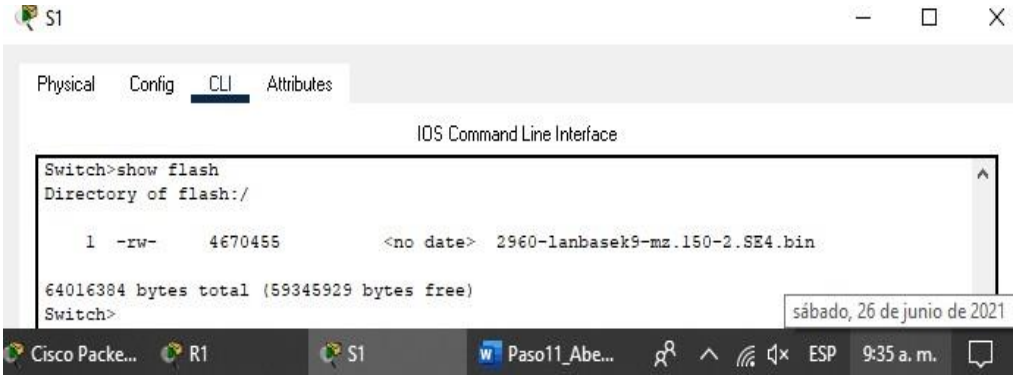


Fuente: Autor

Tabla 12. Inicialización y recarga de routers y switchs.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#**erase startup-config** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router#
Volver a cargar todos los routers	Router#**reload** Proceed with reload? [confirm]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch #**erase startup-config** Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete Switch #**delete vlan.dat** Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]
Volver a cargar ambos switches	Switch #**reload** Proceed with reload? [confirm]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>**show flash** Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free)

Figura 25. Verificación que no existe la base de datos VLAN en la memoria flash.



Fuente: Autor

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

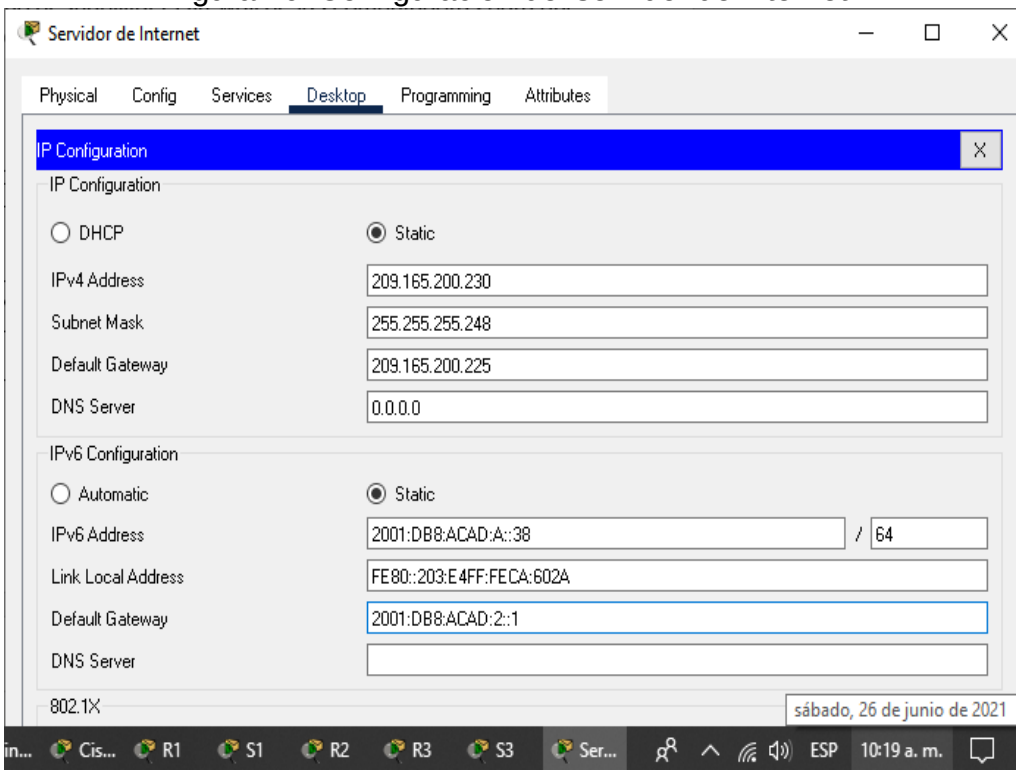
- Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 13. Configuración de la computadora de internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
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:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Figura 26. Configuración del servidor de internet.



Fuente: Autor

Paso 2: Configurar R1

- Las tareas de configuración para R1 incluyen las siguientes:

Tabla 14. Configuración básica router R1.

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Router>enable Router#config terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#**no ip domain-lookup**
Nombre del router	**R1** Router(config)#**hostname R1**
Contraseña de exec privilegiado cifrada	Contraseña: **class** R1(config)#enable secret class

Contraseña de acceso a la consola	Contraseña: **cisco** R1(config)#line console 0 R1(config-line)#**password cisco** R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	Contraseña: **cisco** R1(config)#line vty 0 4 R1(config-line)#**password cisco** R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#**service password-encryption**
Mensaje MOTD	**Se prohíbe el acceso no autorizado**. R1(config)#**banner motd #Se prohibe el acceso no autorizado#**
Interfaz S0/0/0	**Establezca la descripción** R1(config)#interface s0/0/0 R1(config-if)#**description conectado a R2** **Establecer la dirección IPv4** Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#**ip address 172.16.1.1 255.255.255.252** **Establecer la dirección IPv6** Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)#**ipv6 address 2001:DB8:ACAD:1::1/64** **Establecer la frecuencia de reloj en 128000**

	R1(config-if)#**clock rate 128000** **Activar la interfaz** R1(config-if)#**no shutdown** R1(config-if)#exit
Rutas predeterminadas	**Configurar una ruta IPv4 predeterminada de S0/0/0** R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 **Configurar una ruta IPv6 predeterminada de S0/0/0** R1(config)#ipv6 route ::/0 s0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

- La configuración del R2 incluye las siguientes tareas:

Tabla 15. Configuración básica router R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#**no ip domain-lookup**
Nombre del router	**R2** Router(config)#**hostname R2**
Contraseña de exec privilegiado cifrada	**class** R2(config)#**enable secret class**
Contraseña de acceso a la consola	**cisco** R2(config)#line con 0 R2(config-line)#**password cisco**

	R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	**cisco** R2(config)#line vty 0 4 R2(config-line)#**password cisco** R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#**service password-encryption**
Habilitar el servidor HTTP	R2(config)#**ip http server**
Mensaje MOTD	**Se prohíbe el acceso no autorizado.** R2(config)#**banner motd #Se prohíbe el acceso no autorizado#**
Interfaz S0/0/0	**Establezca la descripción** R2(config)#interface s0/0/0 R2(config-if)#**description conectado a R1** **Establezca la dirección IPv4.** Utilizar la siguiente dirección disponible en la subred. R2(config-if)#**ip address 172.16.1.2 255.255.255.252** **Establezca la dirección IPv6.** Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#**ipv6 address 2001:DB8:ACAD:1::2/64** **Activar la interfaz** R2(config-if)#**no shutdown** R2(config-if)#exit

Interfaz S0/0/1	**Establecer la descripción** R2(config)#interface serial 0/0/1 R2(config-if)#**description conectado a R3** **Establezca la dirección IPv4.** Utilizar la primera dirección disponible en la subred. R2(config-if)#**ip address 172.16.2.2 255.255.255.252** **Establezca la dirección IPv6.** Consulte el diagrama de topología para conocer la información de direcciones. R2(config-if)#**ipv6 address 2001:DB8:ACAD:2::2/64** **Establecer la frecuencia de reloj en 128000.** R2(config-if)#**clock rate 128000** **Activar la interfaz** R2(config-if)#**no shutdown** R2(config-if)#exit
Interfaz G0/0 (simulación de Internet)	**Establecer la descripción.** R2(config)#interface g0/0 R2(config-if)#**description conectado a Internet** **Establezca la dirección IPv4.** Utilizar la primera dirección disponible en la subred.

	R2(config-if)#**ip address 209.165.200.233 255.255.255.248** **Establezca la dirección IPv6.** Utilizar la primera dirección disponible en la subred. R2(config-if)#**ipv6 address 2001:DB8:ACAD:A::1/64** **Activar la interfaz** R2(config-if)#**no shutdown** R2(config-if)#exit
Interfaz loopback 0 (servidor web simulado)	**Establecer la descripción.** R2(config)#interface Lo0 R2(config-if)#**description Servidor Web Simulado** **Establezca la dirección IPv4.** R2(config-if)#**ip address 10.10.10.10 255.255.255.255** R2(config-if)#no shutdown R2(config-if)#exit
Ruta predeterminada	**Configure una ruta IPv4 predeterminada de G0/0.** R2(config)#**ip route 0.0.0.0 0.0.0.0 g0/0** **Configure una ruta IPv6 predeterminada de G0/0.** R2(config)#**ipv6 route ::/0 g0/0** R2(config)#exit

Paso 4: Configurar R3

- La configuración del R3 incluye las siguientes tareas:

Tabla 16. Configuración básica del router R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#**no ip domain-lookup**
Nombre del router	**R3** Router(config)#**hostname R3**
Contraseña de exec privilegiado cifrada	**class** R3(config)#enable secret **class**
Contraseña de acceso a la consola	**cisco** R3(config)#enable secret class R3(config)#line console 0 R3(config-line)#**password cisco** R3(config-line)#login R3(config-line)#exit
Contraseña de acceso Telnet	**cisco** R3(config)#line vty 0 4 R3(config-line)#**password cisco** R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#**service password-encryption**
Mensaje MOTD	**Se prohíbe el acceso no autorizado.** R3(config)#**banner motd #Se prohibe el acceso no autorizado#**

Interfaz S0/0/1	**Establecer la descripción** R3(config)#interface s0/0/1 R3(config-if)#**description conectado a R2** **Establezca la dirección IPv4.** Utilizar la siguiente dirección disponible en la subred. R3(config-if)#**ip address 172.16.2.1 255.255.255.252** **Establezca la dirección IPv6.** Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#**ipv6 address 2001:DB8:ACAD:2::1/64** **Activar la interfaz** R3(config-if)#**no shutdown**
Interfaz loopback 4	**Establezca la dirección IPv4.** Utilizar la primera dirección disponible en la subred. R3(config)#interface Lo4 R3(config-if)#**ip address 192.168.4.1 255.255.255.0** R3(config-if)#exit
Interfaz loopback 5	**Establezca la dirección IPv4.** Utilizar la primera dirección disponible en la subred. R3(config)#interface Lo5 R3(config-if)#**ip address 192.168.5.1 255.255.255.0** R3(config-if)#exit

Interfaz loopback 6	**Establezca la dirección IPv4.** Utilizar la primera dirección disponible en la subred. R3(config)#interface Lo6 R3(config-if)#**ip address 192.168.6.1 255.255.255.0** R3(config-if)#exit
Interfaz loopback 7	**Establezca la dirección IPv6.** Consulte el diagrama de topología para conocer la información de direcciones. R3(config)#interface Lo7 R3(config-if)#**ipv6 address 2001:DB8:ACAD:3::1/64** R3(config-if)#exit
Rutas predeterminadas	**Configure una ruta IPv4 predeterminada de S0/0/1.** R3(config)#**ip route 0.0.0.0 0.0.0.0 s0/0/1** **Configure una ruta IPv6 predeterminada de S0/0/1.** R3(config)#**ipv6 route ::/0 s0/0/1**

Paso 5: Configurar S1

- La configuración del S1 incluye las siguientes tareas:

Tabla 17. Configuración básica del switch S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**no ip domain-lookup**

Nombre del switch	**S1** Switch(config)#**hostname S1** S1(config)#
Contraseña de exec privilegiado cifrada	**class** S1(config)#**enable secret class**
Contraseña de acceso a la consola	**cisco** S1(config)#line con 0 S1(config-line)#**password cisco** S1(config-line)#login S1(config-line)#exit
Contraseña de acceso Telnet	**cisco** S1(config)#line vty 0 15 S1(config-line)#**password cisco** S1(config-line)#login S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#**service password-encryption**
Mensaje MOTD	**Se prohíbe el acceso no autorizado.** S1(config)#**banner motd #Se prohibe el acceso no autorizado#**

Paso 6: Configurar S3

- La configuración del S3 incluye las siguientes tareas:

Tabla 18. Configuración básica del switch S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#**no ip domain-lookup**

Nombre del switch	**S3** Switch(config)#hostname S3 S3(config)#
Contraseña de exec privilegiado cifrada	**class** S3(config)#**enable secret class**
Contraseña de acceso a la consola	**cisco** S3(config)#line con 0 S3(config-line)#**password cisco** S3(config-line)#login S3(config-line)#exit
Contraseña de acceso Telnet	**cisco** S3(config)#line vty 0 15 S3(config-line)#**password cisco** S3(config-line)#login S3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S3(config)#**service password-encryption**
Mensaje MOTD	**Se prohíbe el acceso no autorizado.** S3(config)#**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:

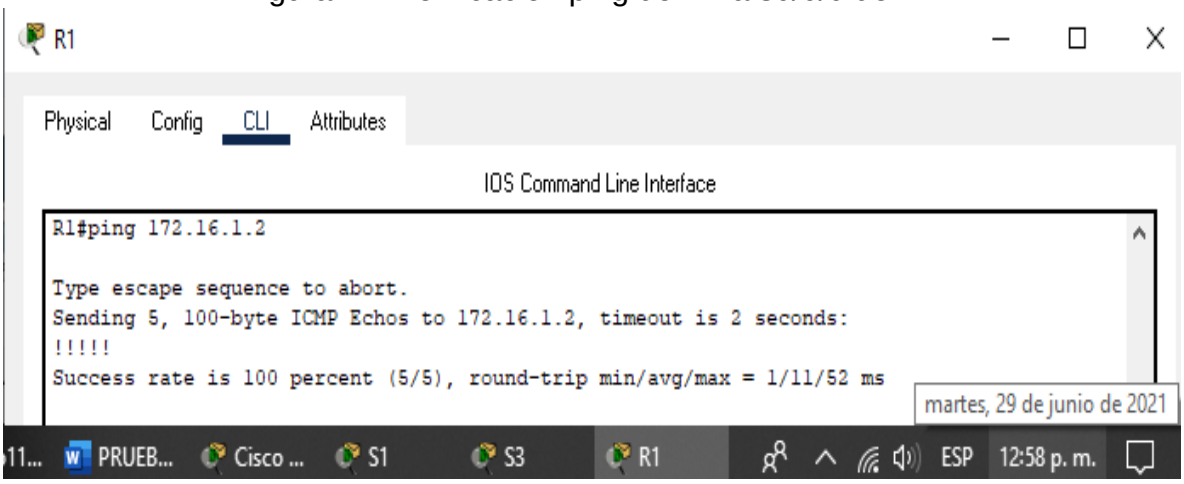
Tabla 19. Verificación de conectividad de la red.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	**Satisfactorio**
R2	R3, S0/0/1	172.16.2.1	**Satisfactorio**

PC de Internet	Gateway predeterminado	209.165.200.233	**Satisfactorio**

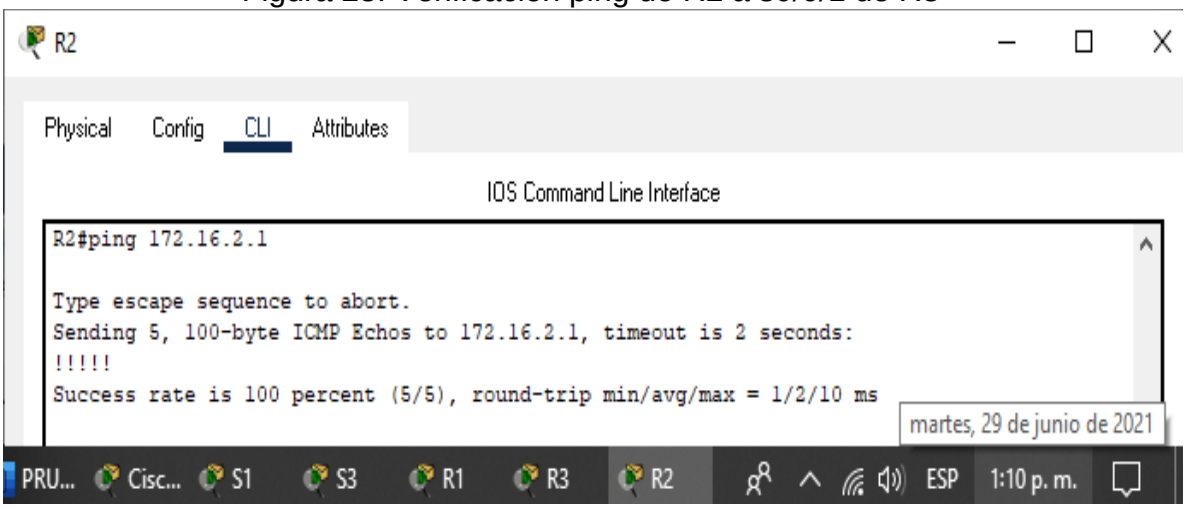
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Figura 27. Verificación ping de R1 a s0/0/0 de R2



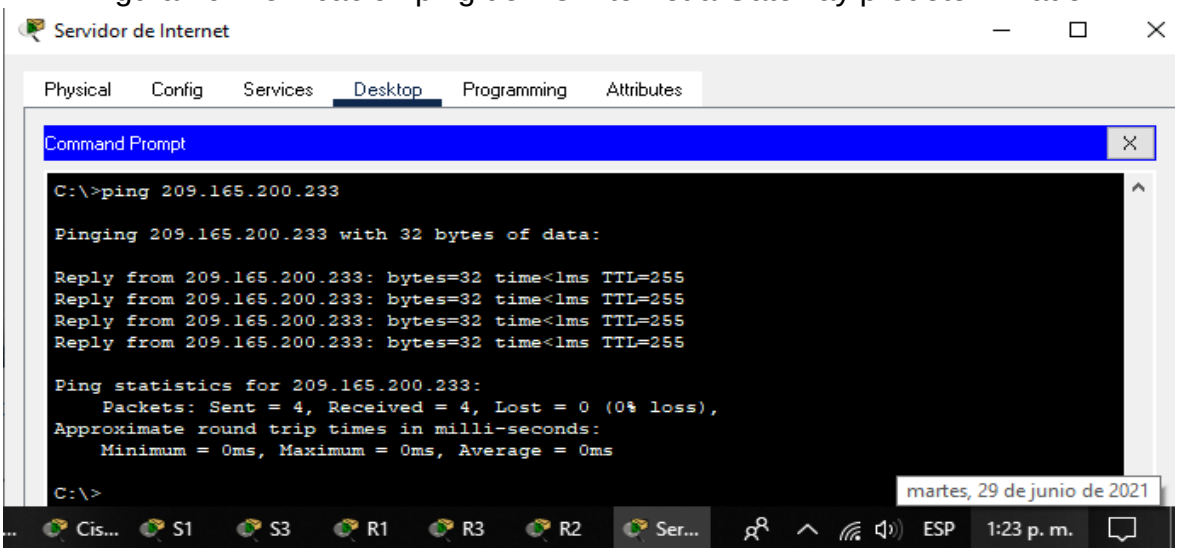
Fuente: Autor

Figura 28. Verificación ping de R2 a s0/0/1 de R3



Fuente: Autor

Figura 29. Verificación ping de PC Internet a Gateway predeterminado.



Fuente: Autor

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:

Tabla 20. Configuración de las VLAN´s en S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	**Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican.** 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 Administracion** S1(config-vlan)#**exit**
Asignar la dirección IP de administración.	**Asigne la dirección IPv4 a la VLAN de administración.** Utilizar la dirección IP asignada al S1 en el diagrama de topología

	S1(config)#interface vlan 99 S1(config-if)# **ip address 192.168.99.2 255.255.255.0** S1(config-if)#no shutdown S1(config-if)#exit
Asignar el gateway predeterminado	**Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.** S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	**Utilizar la red VLAN 1 como VLAN nativa** S1(config)#interface f0/3 S1(config-if)#**switchport mode trunk** S1(config-if)#**switchport trunk native vlan 1** S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	**Utilizar la red VLAN 1 como VLAN nativa** S1(config)#interface f0/5 S1(config-if)#**switchport mode trunk** S1(config-if)#**switchport trunk native vlan 1** S1(config-if)#exit
Configurar el resto de los puertos como puertos de acceso	**Utilizar el comando interface range** S1(config)#**interface range f0/1-2, f0/4, f0/6-24, g0/1-2** S1(config-if-range)#**switchport mode access** S1(config-if-range)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if-range)#**switchport access vlan 21** S1(config-if-range)#exit
Apagar todos los puertos sin usar	S1(config)#**interface range f0/1-2, f0/4, f0/7-24, g0/1-2** S1(config-if-range)#**shutdown** S1(config-if-range)#exit

Paso 2: Configurar el S3

- La configuración del S3 incluye las siguientes tareas:

Tabla 21. Configuración de las VLAN´s en S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	**Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican.** **Dé nombre a cada 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** S3(config-vlan)#exit
Asignar la dirección IP de administración	**Asigne la dirección IPv4 a la VLAN de administración.** **Utilizar la dirección IP asignada al S3 en el diagrama de topología** S3(config)#interface vlan 99 S3(config-if**)# ip address 192.168.99.3 255.255.255.0** S3(config-if)#no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	**Asignar la primera dirección IP en la subred como gateway predeterminado.** S3(config)#**ip default-gateway 192.168.99.1**
Forzar el enlace troncal en la interfaz F0/3	**Utilizar la red VLAN 1 como VLAN nativa** S3(config)#interface f0/3 S3(config-if)#**switchport mode trunk** S3(config-if)#**switchport trunk native vlan 1** S3(config-if)#exit

Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#**interface range f0/1-2, f0/4-24, g0/1-2** S3(config-if-range)#**switchport mode access** S3(config-if-range)#exit
Asignar F0/18 a la VLAN 23	S3(config)#interface f0/18 S3(config-if)#**switchport access vlan 23** S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#**interface range f0/1-2, f0/4-17, f0/19-24, g0/1-2** S3(config-if-range)#**shutdown** S3(config-if-range)#exit

Paso 3: Configurar R1

- Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22. Configuración el routing entre VLANs

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: **LAN de Contabilidad** Asignar la **VLAN 21** Asignar la primera dirección disponible a esta interfaz R1(config)#interface 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** R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: **LAN de Ingeniería** Asignar la **VLAN 23** Asignar la primera dirección disponible a esta interfaz

	R1(config)#interface 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** R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: **LAN de Administración** Asignar la **VLAN 99** Asignar la primera dirección disponible a esta interfaz R1(config)#interface 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** R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#interface g0/1 R1(config-if)#**no shutdown** R1(config-if)#exit

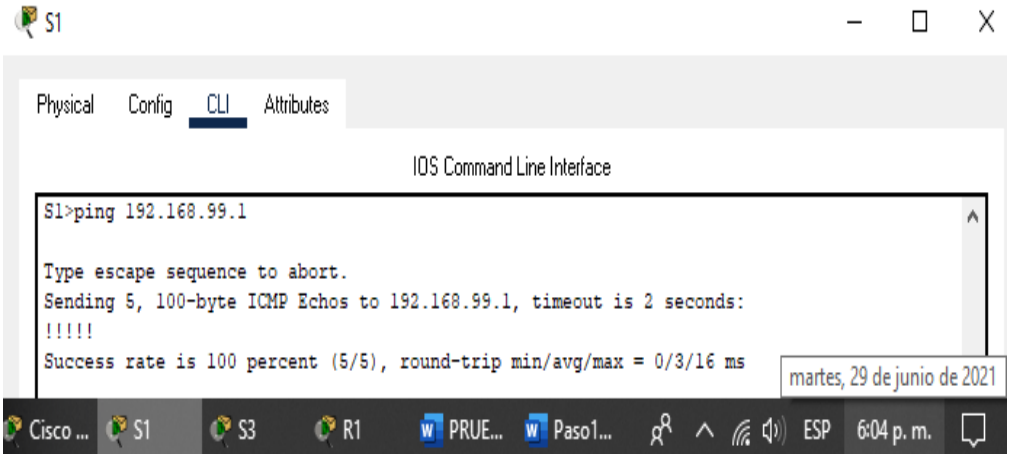
Paso 4: Verificar la conectividad de la red

- 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 23. Verificación de continuidad entre los switchs y R1

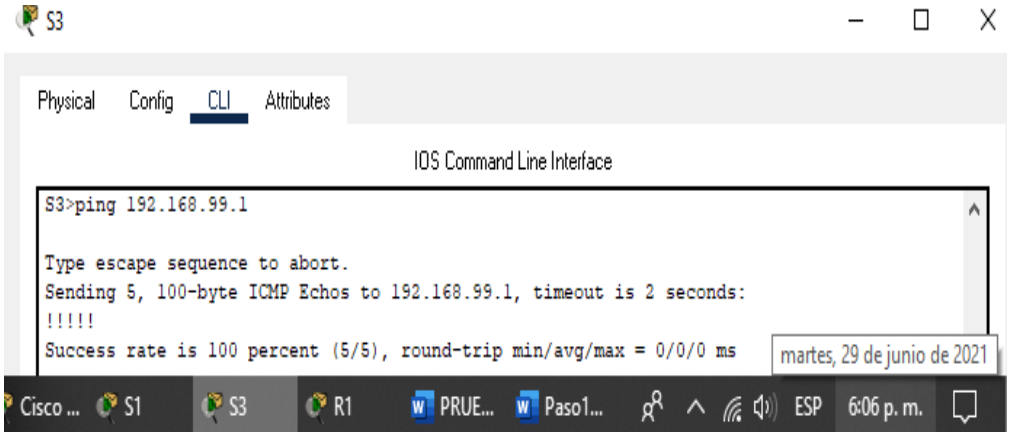
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	**Satisfactorio**
S3	R1, dirección VLAN 99	192.168.99.1	**Satisfactorio**
S1	R1, dirección VLAN 21	192.168.21.1	**Satisfactorio**
S3	R1, dirección VLAN 23	192.168.23.1	**Satisfactorio**

Figura 30. Verificación de conectividad entre S1 a R1 (VLAN99)



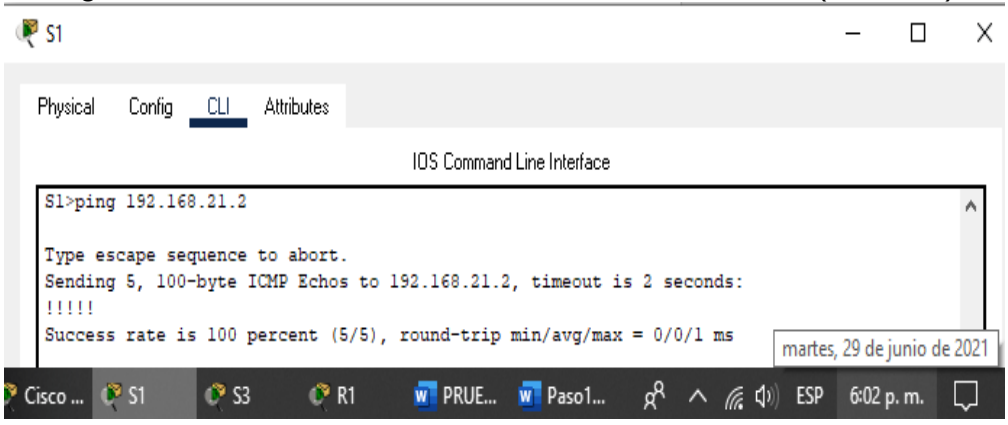
Fuente: Autor

Figura 31. Verificación de conectividad entre S3 a R1 (VLAN99)



Fuente: Autor

Figura 32. Verificación de conectividad entre S3 a R1 (VLAN21)



Fuente: Autor

Figura 33. Verificación de conectividad entre S3 a R1 (VLAN23).

Fuente: Autor

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

- Las tareas de configuración para R1 incluyen las siguientes:

Tabla 24. Configuración de OSPF en R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1>enable Password: R1#config terminal Enter configuration commands, one per line. End with CNTL/Z. R1(config)#**router ospf 1** R1(config-router)#

Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config-router)#**network 172.16.1.0 0.0.0.3 area 0** R1(config-router)#**network 192.168.21.0 0.0.0.255 area 0** R1(config-router)#**network 192.168.23.0 0.0.0.255 area 0** R1(config-router)#**network 192.168.99.0 0.0.0.255 area 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 OSPF en el R2

- La configuración del R2 incluye las siguientes tareas:

Tabla 25. Configuración de OSPF en R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2>enable Password: R2#config terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#**router ospf 1** R2(config-router)#
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0. R2(config)#**router ospf 1** R2(config-router)#**network 10.10.10.10 0.0.0.0 area 0**

	R2(config-router)#**network 172.16.1.0 0.0.0.3 area 0** R2(config-router)#**network 172.16.2.0 0.0.0.3 area 0**
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#**passive-interface Lo0**
Desactive la sumarización automática.	R2(config-router)#**no auto-summary**

Paso 3: Configurar OSPFv3 en el R3

- La configuración del R3 incluye las siguientes tareas:

Tabla 26. Configuración de OSPFv3 en R3.

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	R3>enable Password: R3#config terminal Enter configuration commands, one per line. End with CNTL/Z. R3(config)#**route ospf 1**
Anunciar redes IPv4 conectadas directamente	R3(config-router)#**network 172.16.2.0 0.0.0.3 area 0** R3(config-router)#**network 192.168.4.0 0.0.0.255 area 0** R3(config-router)#**network 192.168.5.0 0.0.0.255 area 0** R3(config-router)#**network 192.168.6.0 0.0.0.255 area 0**
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#**passive-interface Lo4** R3(config-router)#**passive-interface Lo5** R3(config-router)#**passive-interface Lo6**
Desactive la sumarización automática.	R3(config-router)#**no auto-summary**

Paso 4: Verificar la información de OSPF

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

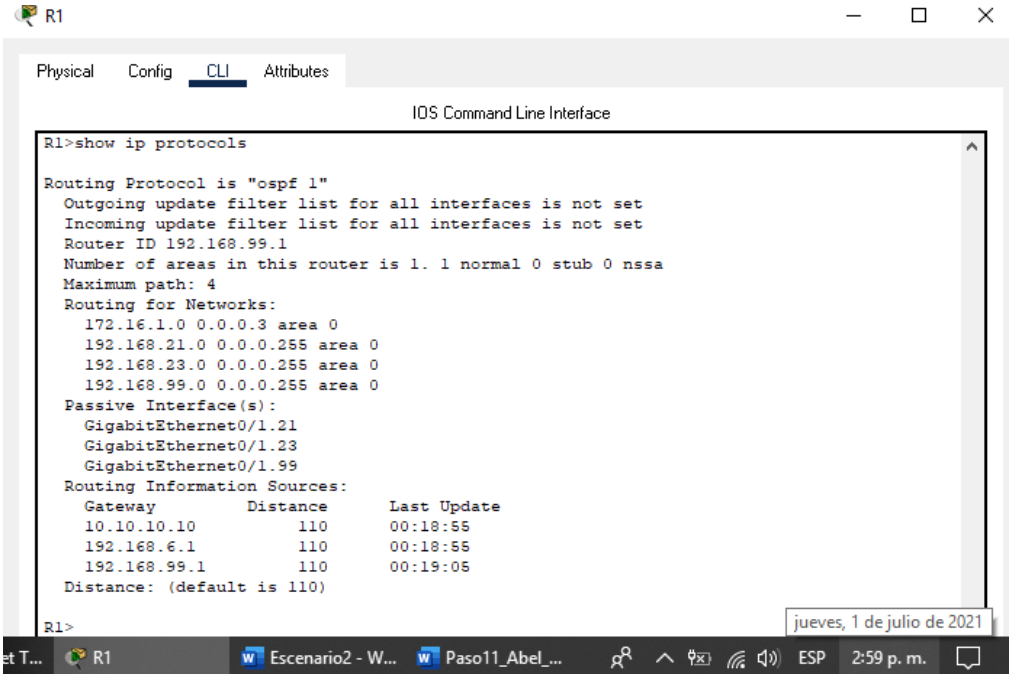
Tabla 27. Verificación de funcionamiento de OSPF

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	**show ip protocols**
¿Qué comando muestra solo las rutas OSPF?	**show ip route ospf**
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	**show running-config**

Verificación de funcionamiento del protocolo OSPF:

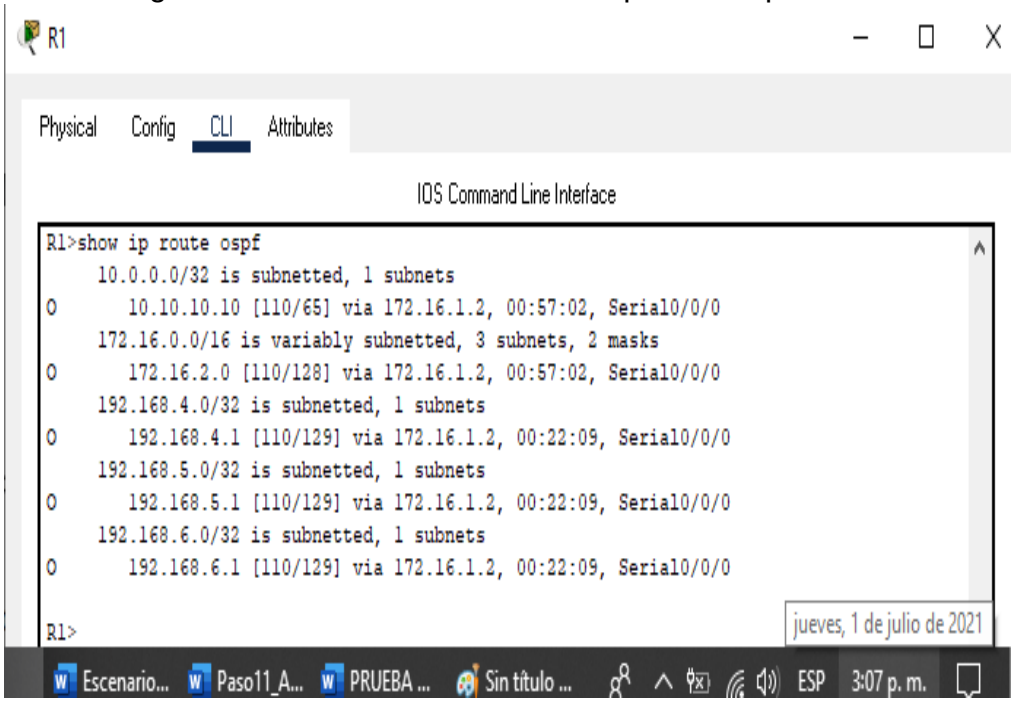
En el router R1:

Figura 34. Uso del comando show ip protocols en R1.



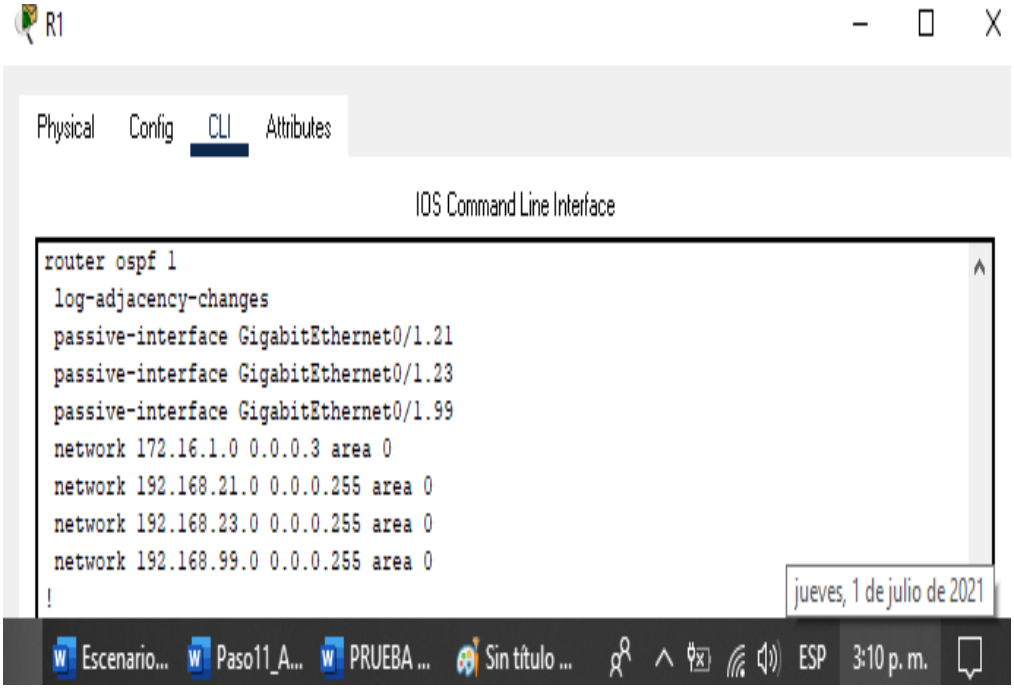
Fuente: Autor

Figura 35. Uso del comando show ip route ospf en R1.



Fuente: Autor

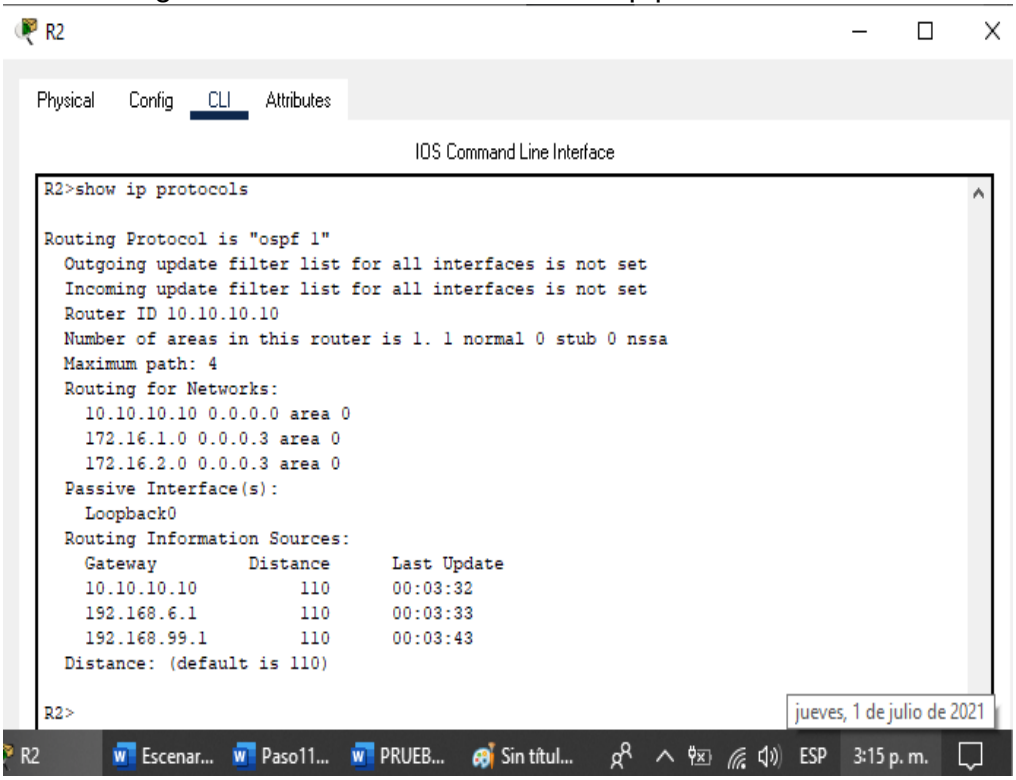
Figura 36. Uso del comando show running-config en R1.



Fuente: Autor

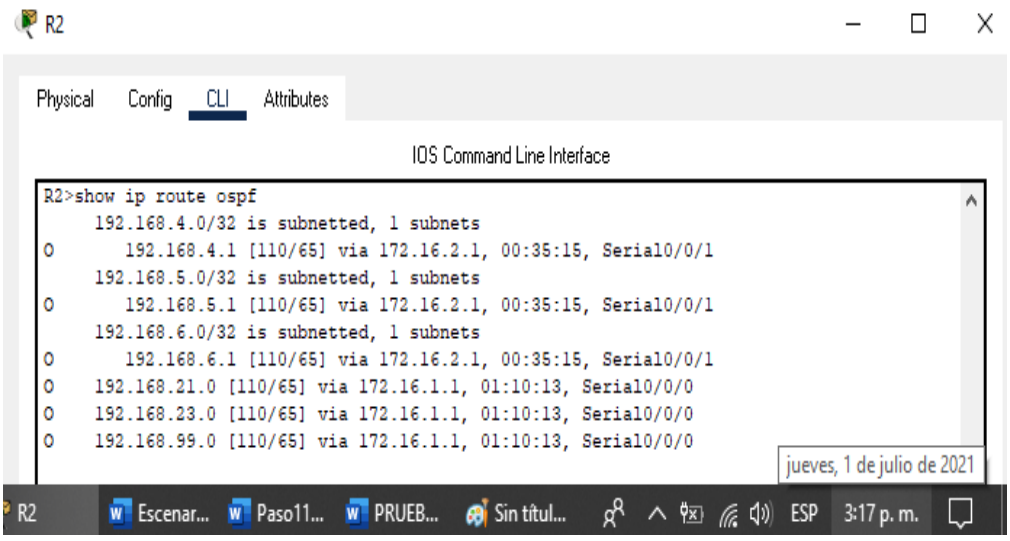
En el router R2:

Figura 37. Uso del comando show ip protocols en R2.



Fuente: Autor

Figura 38. Uso del comando show ip route ospf en R2.



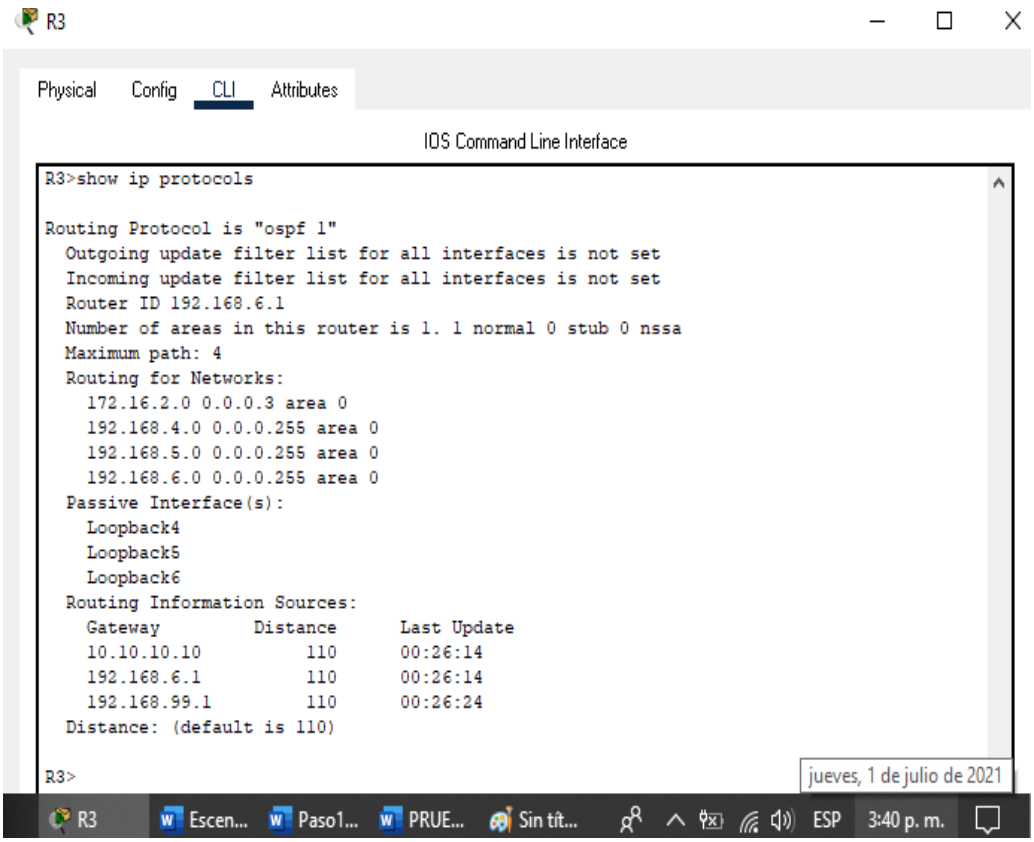
Fuente: Autor

Figura 39. Uso del comando show running-config en R2.

Fuente: Autor

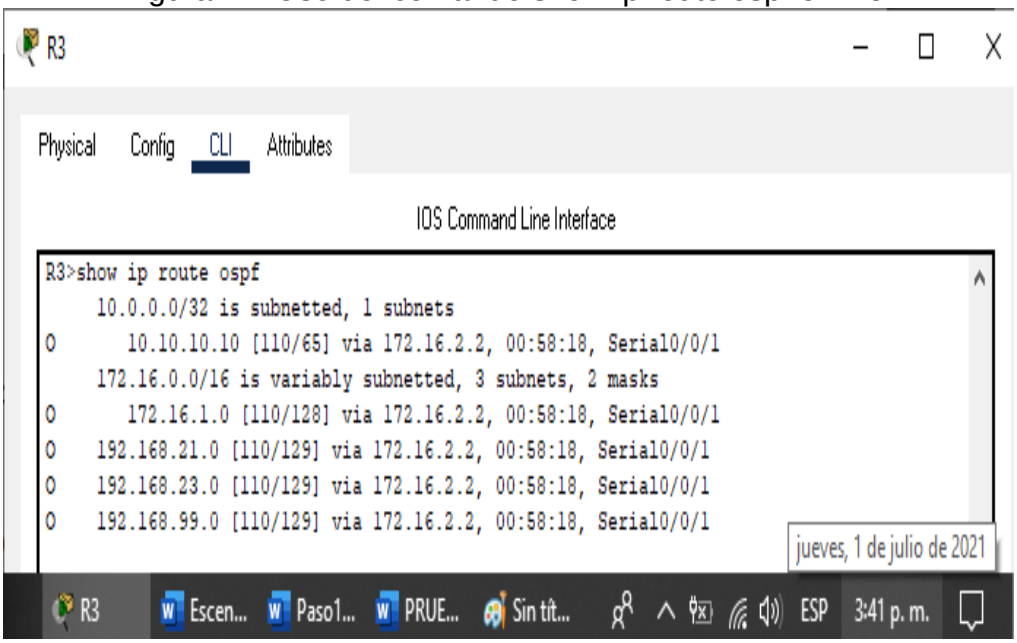
En el router R3:

Figura 40. Uso del comando show ip protocols en R3.



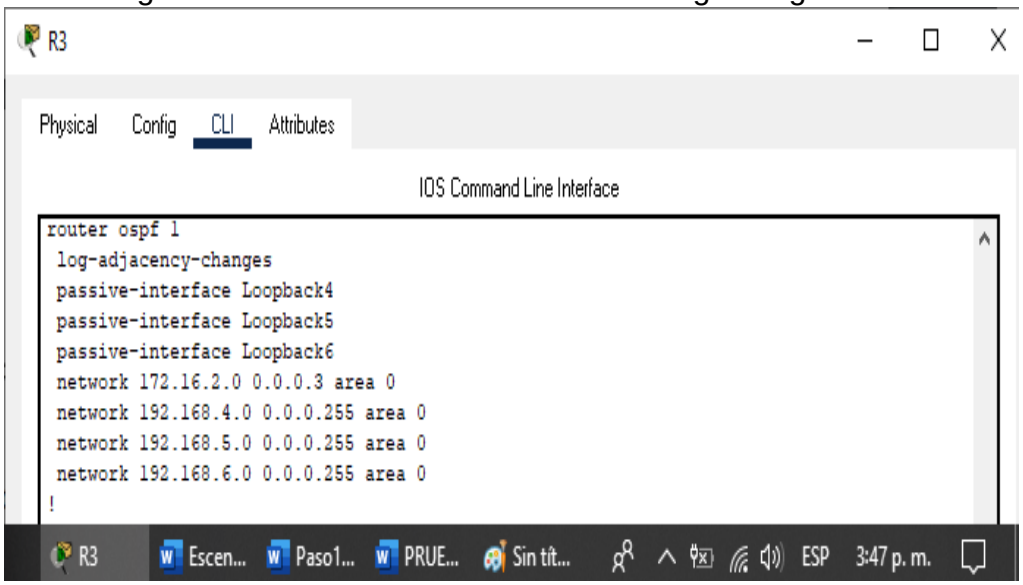
Fuente: Autor

Figura 41. Uso del comando show ip route ospf en R3.



Fuente: Autor

Figura 42. Uso del comando show running-config en R3.



Fuente: Autor

Parte 5: 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:

Tabla 28. Configuración de R1 como servidor DHCP

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>enable Password: R1#config terminal Enter configuration commands, one per line. End with CNTL/Z. 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.	**Nombre: ACCT** R1(config)#**ip dhcp pool ACCT** **Servidor DNS: 10.10.10.10** R1(dhcp-config)#**dns-server 10.10.10.10** **Nombre de dominio: ccna-sa.com** R1(dhcp-config)#**domain-name ccna-sa.com** **Establecer el gateway predeterminado** R1(dhcp-config)#**default-router 192.168.21.1** R1(dhcp-config)#**network 192.168.21.0 255.255.255.0**
Crear un pool de DHCP para la VLAN 23	**Nombre: ENGNR** R1(config)#**ip dhcp pool ENGNR** **Servidor DNS: 10.10.10.10** R1(dhcp-config)#**dns-server 10.10.10.10** **Nombre de dominio: ccna-sa.com** R1(dhcp-config)#**domain-name ccna-sa.com** **Establecer el gateway predeterminado**

	R1(dhcp-config)#**default-router 192.168.23.1** R1(dhcp-config)#**network 192.168.23.0 255.255.255.0**

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

- La configuración del R2 incluye las siguientes tareas:

Tabla 29. Configuración de NAT en R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2>enable Password: R2#config terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#**user webuser privilege 15 secret cisco12345**
Habilitar el servicio del servidor HTTP	R2(config)#**ip http server**
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#**ip http authetication local**
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)# int s0/0/0 R2(config-if)# **ip nat inside** R2(config)#exit R2(config)# int s0/0/1

	R2(config-if)# **ip nat inside**
Configurar la NAT dinámica dentro de una ACL privada	**Lista de acceso: 1** **Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1** R2(config)#**access-list 1 permit 192.168.21.0 0.0.0.255** R2(config)#**access-list 1 permit 192.168.23.0 0.0.0.255** **Permitir la traducción de un resumen de las redes LAN (loopback) en el R3** R2(config)#**access-list 1 permit 192.168.4.0 0.0.3.255**
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

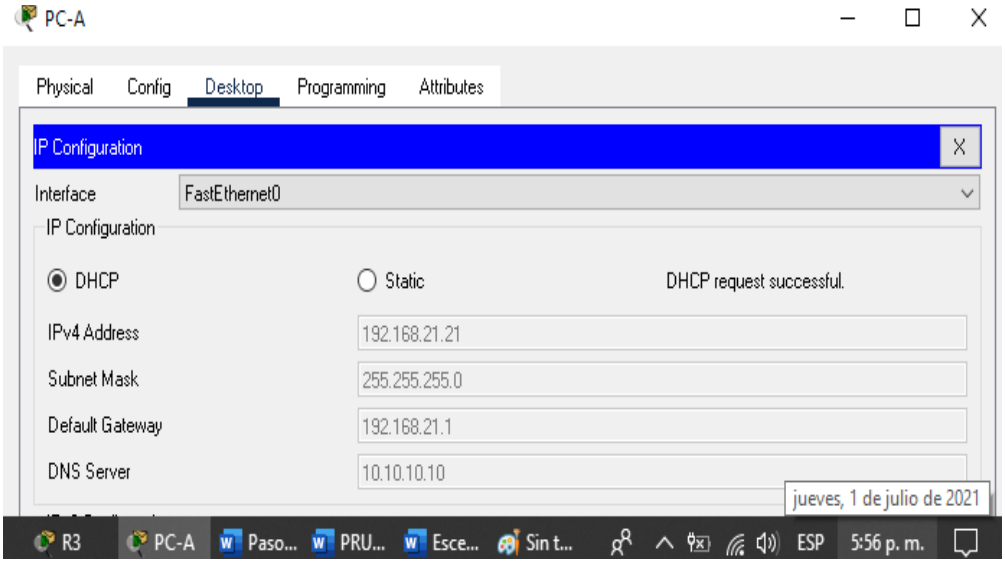
Paso 3: Verificar el protocolo DHCP y la NAT estática

- 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 30. Verificación de protocolo DHCP y NAT

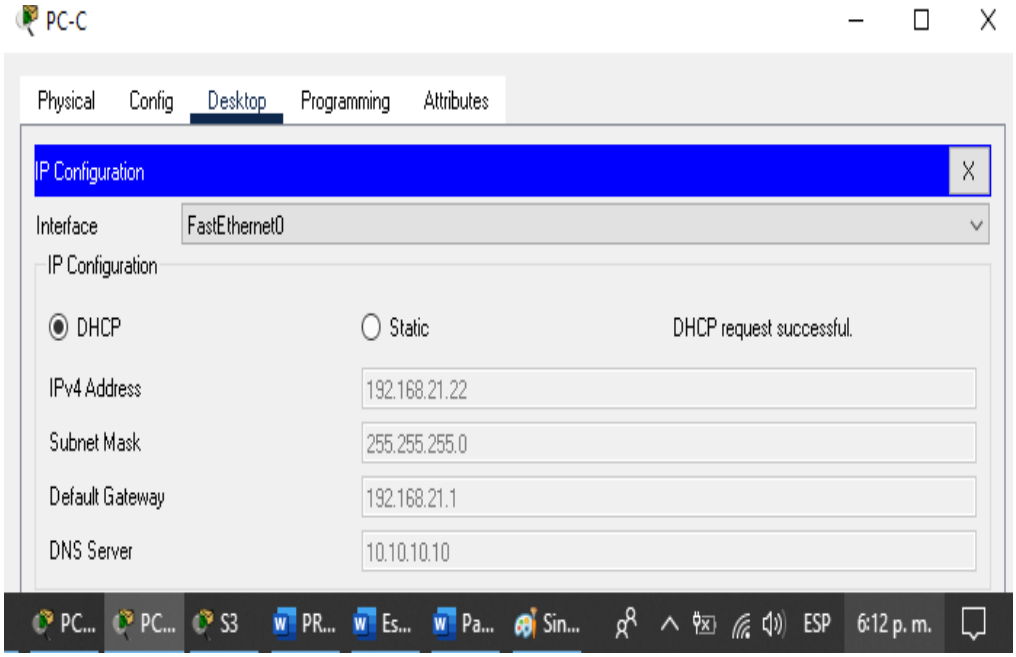
Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	**Satisfactorio.** Ver figura 43.
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	**Satisfactorio.** Ver figura 44.
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	**Satisfactorio.** Ver figura 45.
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Packet Tracer no soporta la activación del servicio http. Por lo cual no se puede comprobar el acceso al servidor.

Figura 43. Comprobación de adquisición de IP del servidor de HDCP en PC-A



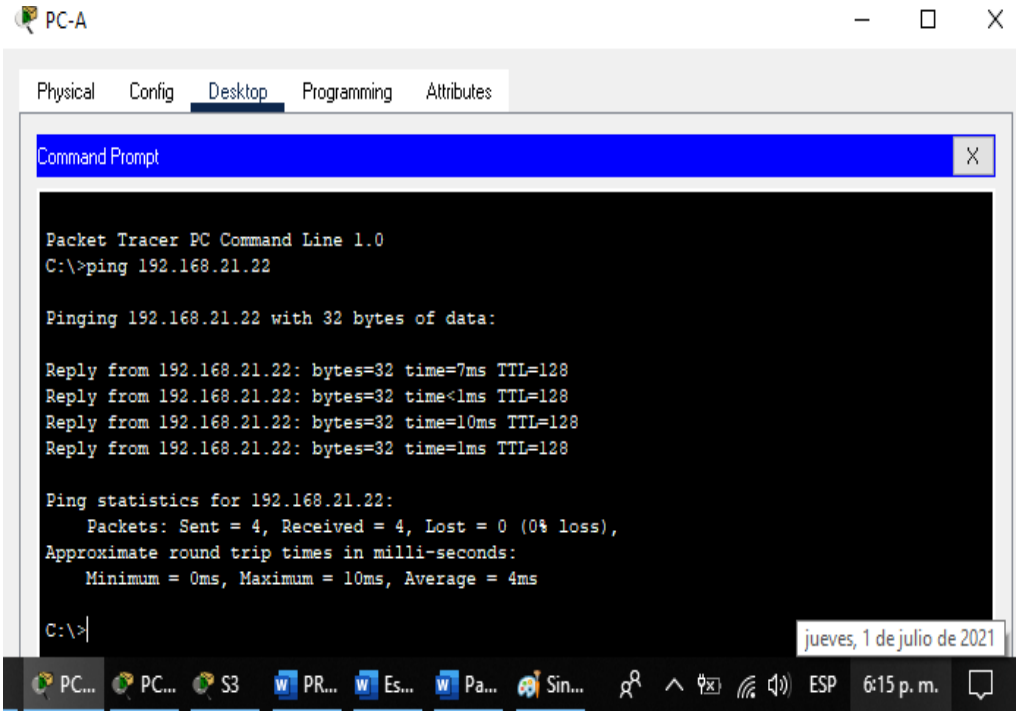
Fuente: Autor

Figura 44. Comprobación de adquisición de IP del servidor de HDCP en PC-C



Fuente: Autor

Figura 45. Comprobación de comunicación entre el PC-A y PC-C.



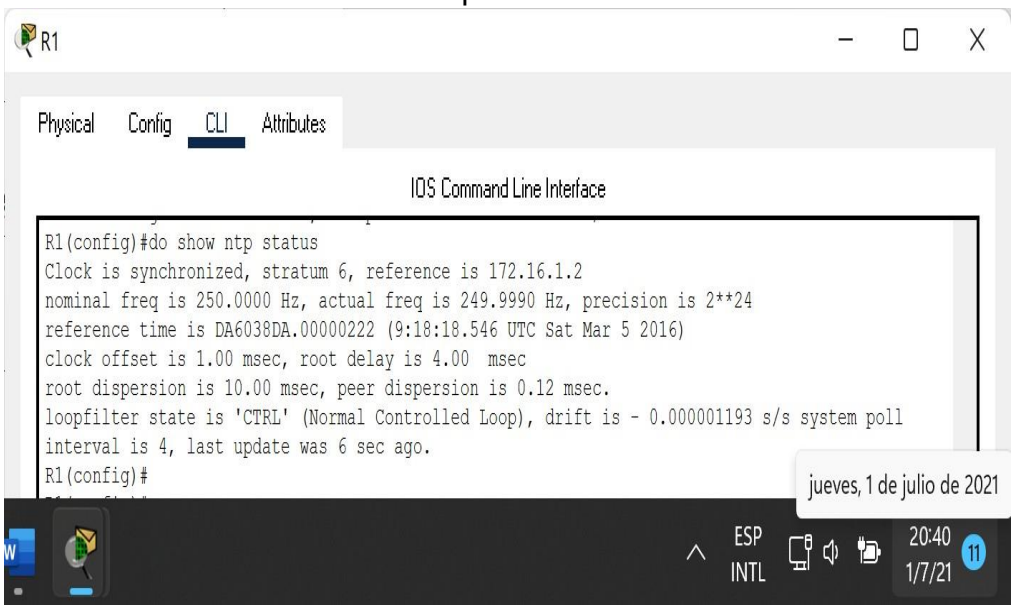
Fuente: Autor

Parte 6: Configurar NTP

Tabla 31. Configuración de NTP.

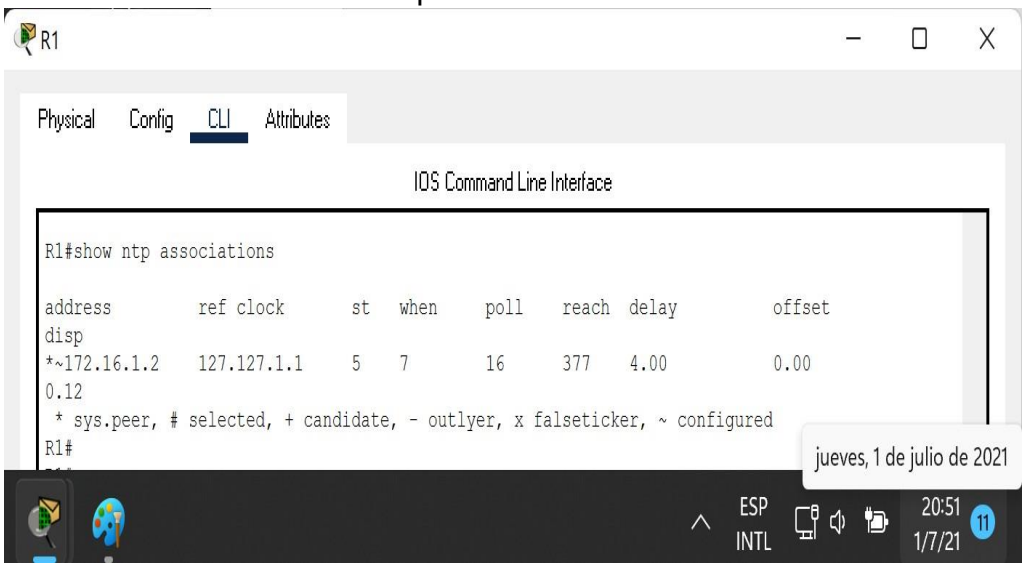
Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.** R2#**clock set 9:00:00 5 march 2016**
Configure R2 como un maestro NTP.	Nivel de estrato: **5** R2#config terminal R2(config)#**ntp master 5**
Configurar R1 como un cliente NTP.	Servidor: **R2** 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(config)#**do show ntp status** R1#**show ntp associations**

Figura 46. Verificación de la configuración de NTP en R1 con el comando do show ntp status.



Fuente: Autor

Figura 47. Verificación de la configuración de NTP en R1 con el comando show ntp associations.



Fuente: Autor

Parte 7: Configurar y verificar las listas de control de acceso (ACL)
Paso 1: Restringir el acceso a las líneas VTY en el R2

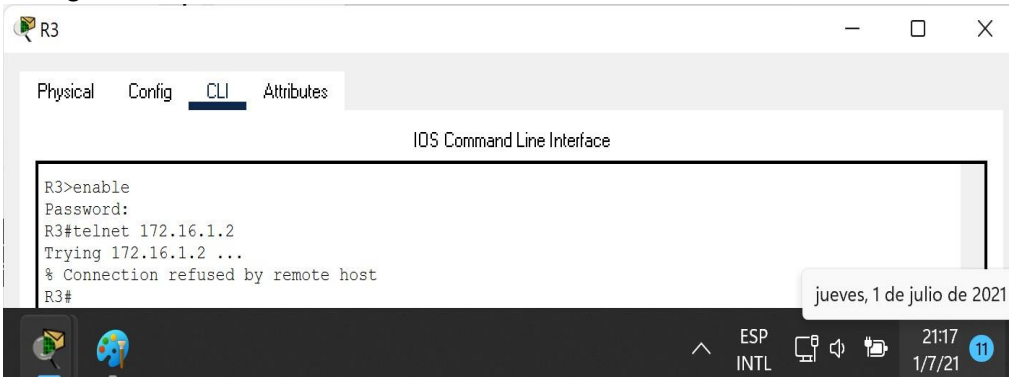
Tabla 32. Configuración de listas de control de acceso (ACL) en R2.

Elemento o tarea de configuración	Especificación
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** R2(config-std-nacl)#exit
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 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	Satisfactoria. Ver figuras # y #.

Figura 48. Verificación de funcionamiento de acceso de ACL desde R1.

Fuente: Autor

Figura 49. Verificación de restricción de acceso de ACL desde R3.



Fuente: Autor

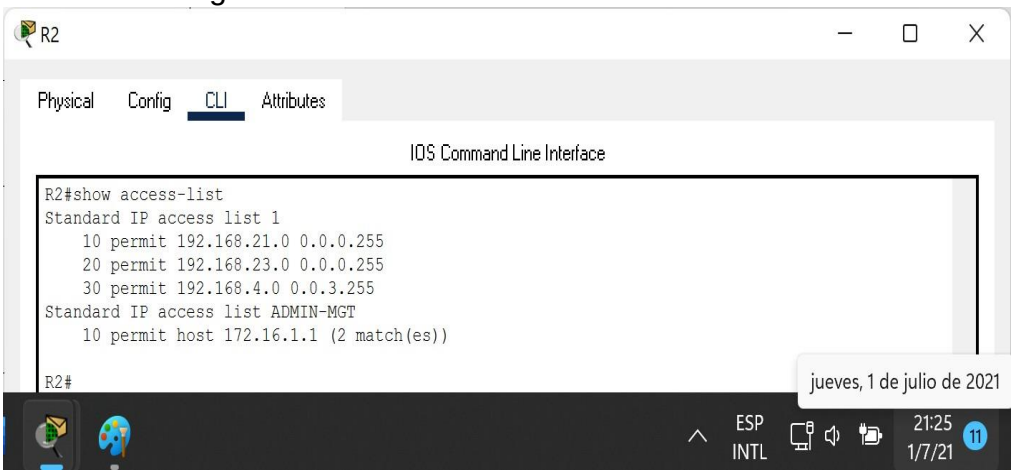
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente:

Tabla 33. Comandos para mostrar listas

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2>enable Password: R2#**show access-list** R2#**show ip access-list**

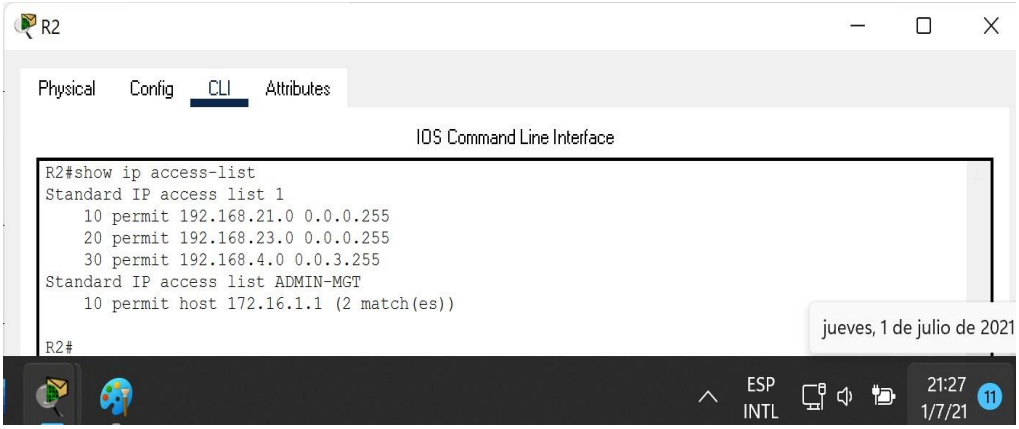
Restablecer los contadores de una lista de acceso	R2#**clear access-list counters**
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#**show ip interface**
¿Con qué comando se muestran las traducciones NAT?	R2#**show ip nat translations** **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#**clear ip nat translation ***

Figura 50. Uso del comando show access-list.



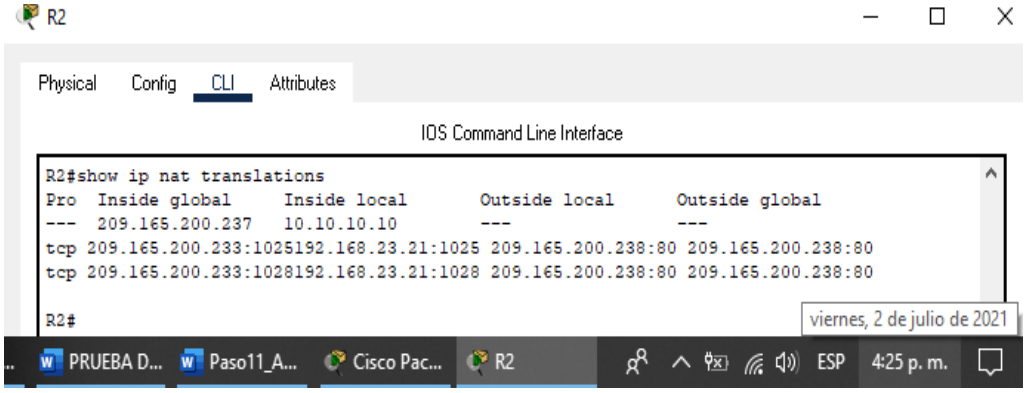
Fuente: Autor

Figura 51. Uso del comando show ip access-list.



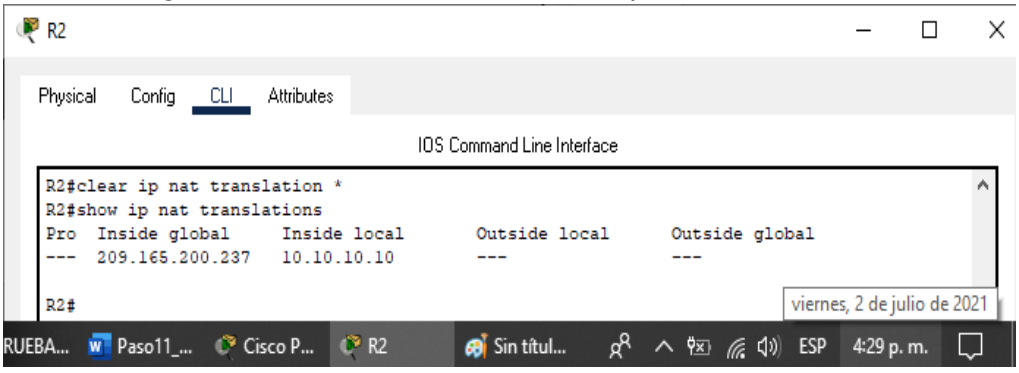
Fuente: Autor

Figura 52. Uso del comando show ip nat translations.



Fuente: Autor

Figura 53. Uso del comando clear ip nat translation *.



Fuente: Autor

CONCLUSIONES

Es importante al iniciar la configuración de cualquier equipo realizar una carga de las configuraciones iniciales y/o volver a configurar con el diseño o configuración deseado o con una copia de seguridad que se tenga de los parámetros del equipo operando satisfactoriamente.

Gracias a los conocimientos adquiridos en los laboratorio y trabajos colaborativos realizados a lo largo del curso de Diplomado, y con la ayuda del software Packet Tracer de CISCO para el montaje y simulación de la red a analizar; se logró la correcta y satisfactoria configuración de los escenarios propuestos como prueba de habilidades.

Es importante implementar correctamente las diferentes rutinas y comando aprendidos en el transcurso del Diplomado para que de una maneja eficaz y ágil los escenarios funcione sin mayores complicaciones.

BIBLIOGRÁFIA

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2017). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado

de https://static-courseassets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2017). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-courseassets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

CISCO. (2017). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2017). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2017). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2017). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2017). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2017). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2017). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2017). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2017). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

UNAD. (2017). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

UNAD. (2017). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

ANEXOS

ANEXO 1. Enlace de descarga del archivo Packet Tracer del Escenario 1:

https://drive.google.com/file/d/1jv_iK3v6NGIIQq94VqP3cUltQa4dVGDN/view?usp=sharing

ANEXO 2. Enlace de descarga del archivo Packet Tracer del Escenario 2:

https://drive.google.com/file/d/1loHj_AVBSK7YoxftVegeDgvUpt08s2J4/view?usp=sharing

ANEXO 3. Enlace de descarga del artículo científico IEEE:

https://drive.google.com/file/d/1m298Y-VpftcZU9Y2OpC6EjbIhFbRR957/view?usp=sharing

ANEXO 4. Artículo científico IEEE:

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO (Julio de 2021)

Abel Antonio Algarra Páez

Universidad Nacional Abierta y a Distancias UNAD, aaalgarra@unadvirtual.edu.co

Resumen

Se realiza en este trabajo la implementación y solución de dos escenarios donde se debemos poner en práctica las habilidades adquiridas a través de los diferentes temas vistos a lo largo del presente curso de CCNA. Con la ayuda del software Packet Tracer se implementarán, configuraran y verificaran los diferentes equipos en los dos escenarios propuestos y se documentara los resultados para sustentar el trabajo realizado y que sustenten los conocimientos previamente adquiridos en los diferentes laboratorios y trabajos colaborativos y que nos afianzaran para diseñar y administrar cualquier red con un alto nivel de calidad y profesionalismo.

Palabras claves: CISCO, CCNA, Conmutación, VLAN, Enrutamiento, Redes, Packet Tracer.

Abstract:

The implementation and solution of two scenarios where we must put into practice the skills acquired through the different topics seen throughout this CCNA course is carried out in this work. With the help of the Packet Tracer software, the different equipment will be implemented, configured and verified in the two proposed scenarios and the results will be documented to support the work carried out and that support the knowledge previously acquired in the different laboratories and collaborative works and that will strengthen us to design and manage any network with a high level of quality and professionalism.

Keywords: CISCO, CCNA, Routing, VLAN, Swicthing, Networking, Packet Tracer.

I. INTRODUCCION

No es desconocido por nadie que actualmente el mundo se mueve en un ámbito digita, manejamos todo desde la palma de la mano, podemos desde configurar el nivel de las luces de nuestra habitación, hasta realizar una compra a miles de kilómetros con solo un clic. Todo esto es gracias a las redes de comunicaciones ya sean alámbricas o inalámbricas, toda esa telaraña de equipos que conforman la una red de comunicaciones o de datos, está conformada por equipo que de no ser configurados o administrados correctamente solo serial elementos sin importancia. Es ahí donde resalta la importancia de saber diseñar y configurar una red de datos. Y es gracias a este Diplomado de Profundización CISCO CCNA donde aprenderemos a realizar estas tareas de una forma profesional.

Para este trabajo se plantearon dos escenarios, donde con la ayuda del software Packet Traicer y de los conocimientos adquiridos a lo largo del curso se llevará acabo la implementación, análisis y configuración de los diferentes equipos para dar una solución óptima a estos escenarios.

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

El trabajo de pruebas de habilidades consiste en el montaje, desarrollo y solución de dos escenarios planteados; para la realización de este artículo se escogió el escenario 1.

III. ESCENARIO 1

A. Topología de la red planteada.

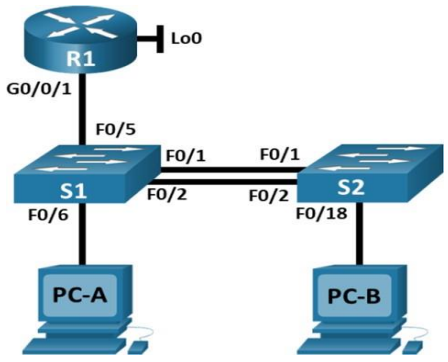


Fig. 1. Topología de la red planteada del Escenario 1

Documento recibido el 16 de julio de 2021.

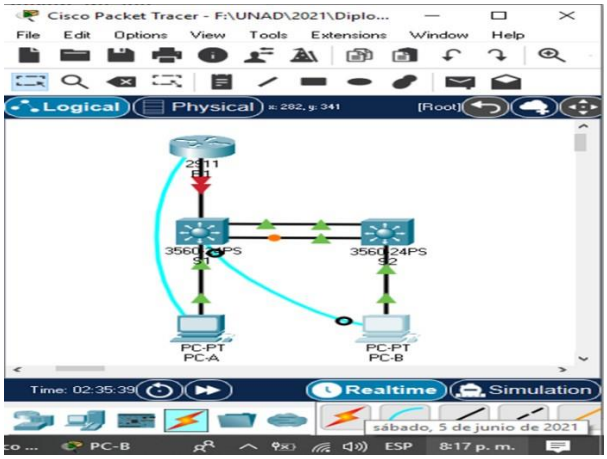


Fig. 2. Topología de la red montada y simulada en Packet Tracer.

B. Inicializar, Recargar y Configurar aspectos básicos de los dispositivos

1) Inicializar y volver a cargar el router y el switch

Es recomendable antes de iniciar la configuración de un dispositivo realizar el borrado de la configuración anterior, esto para evitar posibles errores y configuraciones innecesarias y que puedan llegar a interferir en el nuevo servicio que va a realizar, para ello se utiliza el comando **erase startup-config** en el modo EXEC y luego se debe reiniciar el dispositivo.

En el Router:

```
Router>enable
Router#erase startup-config
Router#reload
```

En los Switch´s:

```
Switch>enable
Switch#erase startup-config
Switch#reload
```

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

```
Switch>enable
Switch#show sdm prefer
Switch#configure terminal
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Switch(config)#end
Switch#reload
```

2) Configurar R1

Se configuran las siguientes tareas en R1:

Tabla 1. Tareas de configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#config terminal Router(config)#no ip domain-lookup
Nombre del router	**R1** Router(config)#hostname R1
Nombre de dominio	**ccna-lab.com** R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** R1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass** R1(config)#line console 0 R1(config-line)#password ciscoconpass R1(config-line)#login R1(config-line)#exit
Establecer la longitud mínima para las contraseñas	**10 caracteres** R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin** **Password: admin1pass** R1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 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	R1(config)#banner motd %Prohibido el acceso a

	personal no autorizado% R1(config)#exit
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces	**Establezca la descripción** **Establece la dirección IPv4.** **Establezca la dirección local de enlace IPv6 como fe80: :1** **Establece la dirección IPv6.** **Activar la interfaz.** R1(config)#interface g0/0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description Bikes R1(config-subif)#ip address 10.21.5.1 255.255.255.192 R1(config-subif)#ipv6 address 2001:db5:acad:a::1/64 R1(config-subif)#ipv6 address FE80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#interface g0/0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description Trikes R1(config-subif)#ip address 10.21.5.65 255.255.255.224 R1(config-subif)#ipv6 address 2001:db5:acad:b::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)#no shutdown R1(config-subif)#interface g0/0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description Native R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)#no shutdown R1(config-subif)#interface g0/0/1.4 R1(config-subif)#encapsulation dot1q 4

	R1(config-subif)#description Management R1(config-subif)#ip address 10.21.5.97 255.255.255.248 R1(config-subif)#ipv6 address 2001:db5:acad:c::1/64 R1(config-subif)#ipv6 address FE80::1 link- local R1(config-subif)#no shutdown
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** R1(config)#interface loopback 0 R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address 2001:db8:acad:209::1/64 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)#description Servicio-Internet R1(config-if)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA	**Módulo de 1024 bits** R1(config)#crypto key generate rsa general- keys modulus 1024 % Invalid input detected at '^' marker. 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]

3) Configurar S1 y S2.

Se deben configurar las siguientes tareas:

Tabla 2. Tareas de configuración para S1

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda** Switch(config)#hostname S1
Nombre de dominio	**ccna-lab.com** S1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** S1(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass** S1(config)#line console 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin Password: admin1pass** S1(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config-line)#transport input ssh S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd %Acceso restringido. Solo personal autorizado%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S1(config)#crypto key generate rsa general- keys modulus 1024 % Invalid input detected at '^' marker. S1(config)#crypto key generate rsa The name for the keys will be: S1.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]
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 4 *Mar 1 4:6:20.775: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip address 10.21.5.98 255.255.255.248 S1(config-if)#ipv6 address 2001:db5:acad:c::98/64 S1(config-if)#ipv6 address fe80::98 link-local S1(config-if)#description Magnament Interface S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado	**Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4**

	S1(config)#ip default-gateway 10.21.5.97

En la configuración de los switch se le asignan nombre, contraseñas de protección para el acceso general y el privilegiado y se muestra un mensaje de advertencia al iniciar el switch. Y se configuran las líneas VTY y se encriptan las contraseñas.

Tabla 3. Tareas de configuración para S2

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Switch>enable Switch#config terminal Switch(config)#no ip domain-lookup
Nombre del switch	**S1 o S2, según proceda** Switch(config)#hostname S2
Nombre de dominio	**ccna-lab.com** S2(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass** S2(config)#enable secret ciscoenpass
Contraseña de acceso a la consola	**ciscoconpass** S2(config)#line console 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit
Crear un usuario administrativo en la base de datos local	**Nombre de usuario: admin** **Password: admin1pass** S2(config)#username admin password admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	S2(config)#line vty 0 15 S2(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config-line)#transport input ssh S2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configurar un MOTD Banner	S2(config)#banner motd %Acceso restringido. Solo personal autorizado%
Generar una clave de cifrado RSA	**Módulo de 1024 bits** S2(config)#crypto key generate rsa general- keys modulus 1024 % Invalid input detected at '^' marker. S1(config)#crypto key generate rsa The name for the keys will be: S2.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]
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** S2(config)#interface vlan 4 *Mar 1 4:6:20.775: %SSH-5-ENABLED: SSH 1.99 has been enabled S2(config-if)#ip address 10.21.5.99 255.255.255.248 S2(config-if)#ipv6 address 2001:db5:acad:c::99/64 S2(config-if)#ipv6 address fe80::99 link-local S2(config-if)#description Magnament Interface S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado	**Configure la puerta de enlace**

	predeterminada como 10.21.5.97 para IPv4 S2(config)#ip default-gateway 10.21.5.97

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

1) Configurar S1

La configuración de S1 incluye las siguientes tareas:

Tabla 4. Configuración VLAN del S1

Tarea	**Especificación**
Crear VLAN	**VLAN 2, nombre Bikes** **VLAN 3, nombre Trikes** **VLAN 4, name Management** **VLAN 5, nombre Parking** **VLAN 6, nombre Native** S1>enable Password: S1#config terminal S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**Interfaces F0/1, F0/2 y F0/5** S1#config terminal S1(config)#interface f0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#interface range f0/1-2
	S1(config-if-range)#shutdown S1(config-if-range)#switchport trunk encapsulation dot1q S1(config-if-range)#switchport mode trunk S1(config-if-range)#switchport trunk native vlan 6 S1(config-if-range)#
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#interface port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6
Configurar el puerto de acceso de host para VLAN 2	**Interface F0/6** S1(config-if)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2
Configurar la seguridad del puerto en los puertos de acceso	**Permitir 3 direcciones MAC** S1(config-if)#switchport port-security S1(config-if)#switchport port-security maximum 3
Proteja todas las interfaces no utilizadas	**Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar.** S1(config-if)#interface range f0/3-4 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5

	S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range f0/7-24 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown S1(config-if-range)#interface range g0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description No esta en uso S1(config-if-range)#shutdown

2) Configurar el S2.

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

Tabla 5. Configuración VLAN del S2

Tarea	**Especificación**
Crear VLAN	**VLAN 2, name Bikes** **VLAN 3, name Trikes** **VLAN 4, name Management** **VLAN 5, nombre Parking** **VLAN 6, nombre Native** S2>enable Password: S2#config terminal S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 S2(config-vlan)# S2(config-vlan)#name Management S2(config-vlan)#vlan 5 S2(config-vlan)#name Parking S2(config-vlan)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	**Interfaces F0/1 y F0/2** S2(config)#interface range f0/1-2 S2(config-if-range)#shutdown S2(config-if-range)#switchport trun encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	**Usar el protocolo LACP para la negociación** S2(config-if-range)#channel-group 1 mode active S2(config-if-range)# Creating a port-channel interface Port-channel 1 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 6
Configurar el puerto de acceso del host para la VLAN 3	**Interfaz F0/18** S2(config-if)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3
Configure port-security en los access ports	**permite 3 MAC addresses** S2(config-if)#switchport port-security S2(config-if)#switchport port-security maximum 3
Asegure todas las interfaces no utilizadas.	**Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar**

	S2(config-if)#interface range f0/3-17 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown S2(config-if-range)#interface range f0/19-24 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown S2(config-if-range)#interface range g0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#description No esta en uso S2(config-if-range)#shutdown

D. Configurar soporte de host.

1) Configurar R1.

Las tareas de configuración del R1 son las siguientes:

Tabla 6. Configuración soporte host para R1

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 Loopback0 R1(config)#ipv6 route ::/0 Loopback 0 R1(config)#exit
Configurar IPv4 DHCP para VLAN 2	**Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada** R1(config)#ip dhcp excluded-address 10.21.5.1 10.21.5.52 R1(config)#ip dhcp pool Vlan2_Bikes R1(dhcp-config)#network 10.21.5.0 255.255.255.192 R1(dhcp-config)#default-router 10.21.5.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit
Configurar DHCP IPv4 para VLAN 3	**Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada.** R1(config)#ip dhcp excluded-address 10.21.5.65 10.21.5.84 R1(config)#ip dhcp pool Vlan3_Trikes R1(dhcp-config)#network 10.21.5.64 255.255.255.224 R1(dhcp-config)#default-router 10.21.5.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit

	R1#copy running-config startup-config

2) Configurar los servidores.

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

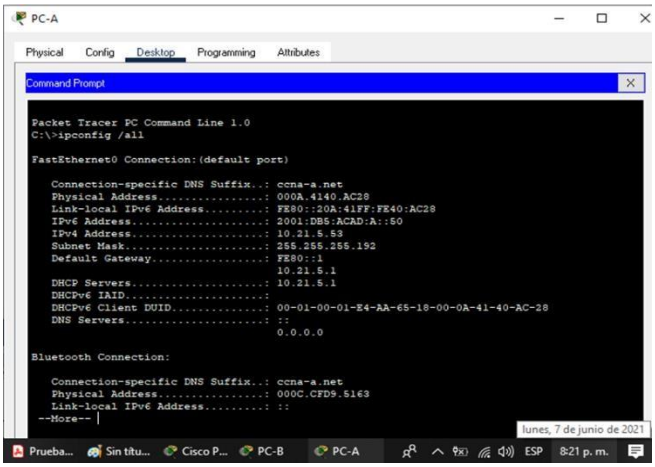


Fig. 3. Configuración parámetros de red PC-A

Tabla 7. Configuración de host PC-A

Configuración de red de PC-A	
Descripción	PC-A
Dirección física	000A.4140.AC28
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

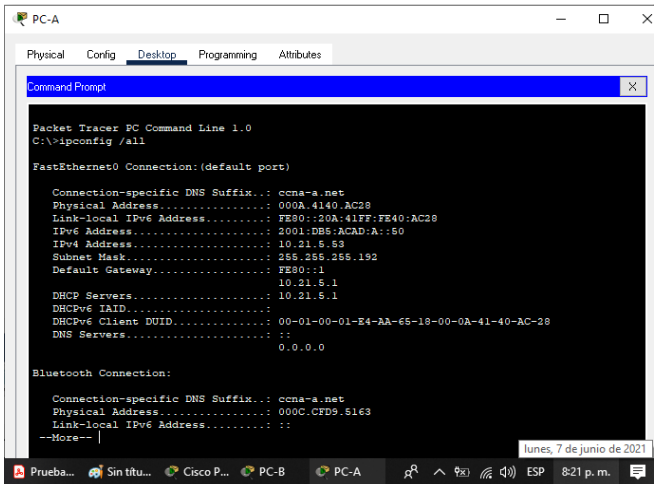


Fig. 4. Configuración parámetros de red PC-A

Tabla 8. Configuración de host PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000A.41EB.E93E
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

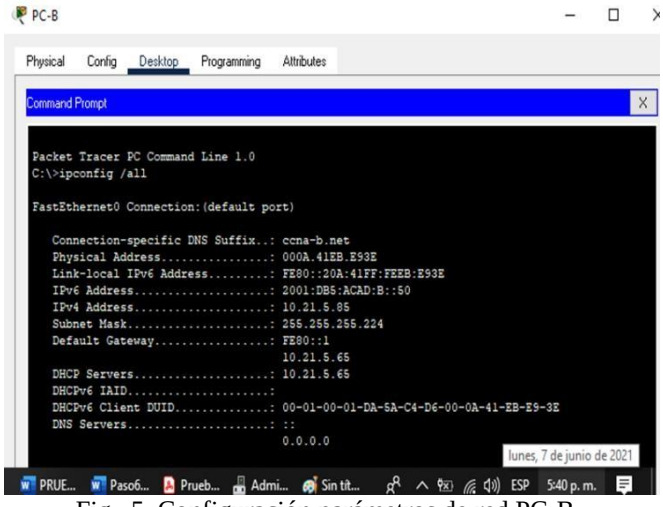


Fig. 5. Configuración parámetros de red PC-B

E. 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.

Tabla 9. Conectividad IPv4 e IPv6 entre dispositivos de la red.

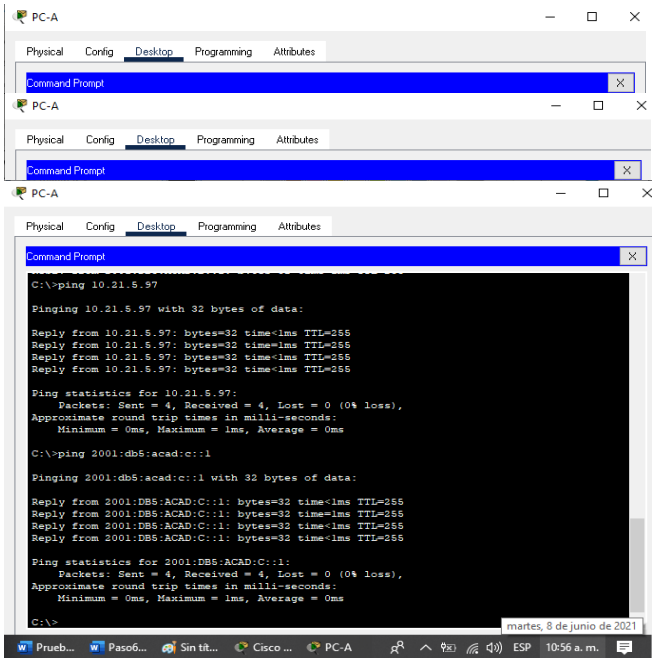
Desde	A	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	10.21.5.1	**Satisfactorio**
		2001:db5:acad:a: :1	**Satisfactorio**
	R1, G0/0/1.3	10.21.5.65	**Satisfactorio**
		2001:db5:acad:b: :1	**Satisfactorio**
	R1, G0/0/1.4	10.21.5.97	**Satisfactorio**
		2001:db5:acad:c: :1	**Satisfactorio**
	S1, VLAN 4	10.21.5.98	**Satisfactorio**
		2001:db5:acad:c: :98	**Satisfactorio**
	S2, VLAN 4	10.21.5.99.	**Satisfactorio**
		2001:db5:acad:c: :99	**Satisfactorio**
	PC-B	IP address will vary.	**Satisfactorio**
		2001:db5:acad:b: :50	**Satisfactorio**
	R1 Bucle 0	209.165.201.1	**Satisfactorio**
PC-B	R1 Bucle 0 *R1 Bucle 0*	209.165.201.1	**Satisfactorio**
		2001:db5:acad:209: :1	**Satisfactorio**
	R1, G0/0/1.2	10.21.5.1	**Satisfactorio**
		2001:db5:acad:a: :1	**Satisfactorio**
	R1, G0/0/1.3	10.21.5.65	**Satisfactorio**
		2001:db5:acad:b: :1	**Satisfactorio**
	R1, G0/0/1.4	10.21.5.97	**Satisfactorio**
		2001:db5:acad:c: :1	**Satisfactorio**
	S1, VLAN 4	10.21.5.98	**Satisfactorio**
		2001:db5:acad:c: :98	**Satisfactorio**
	S2, VLAN 4	10.21.5.99.	**Satisfactorio**
		2001:db5:acad:c: :99	**Satisfactorio**

1) Pruebas de conectividad:

Fig. 6. Prueba de conectividad Ping del PC-A a R1,G0/0/1.2.

Fig. 7. Prueba de conectividad Ping del PC-A a R1,G0/0/1.3.

Fig. 8. Prueba de conectividad Ping del PC-A a R1,G0/0/1.4.



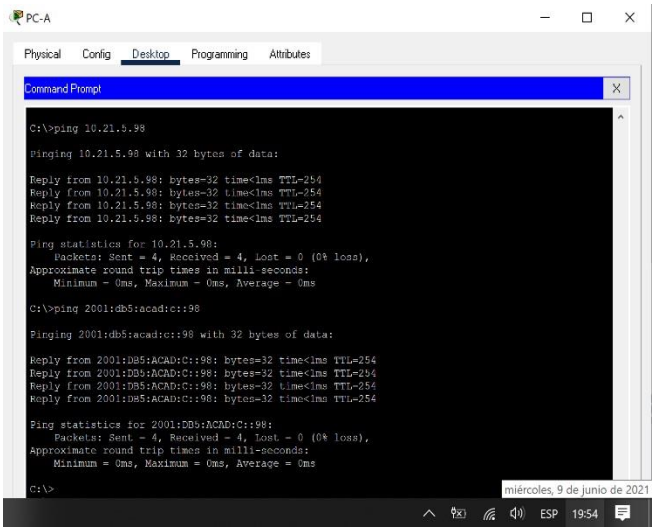


Fig. 9. Prueba de conectividad Ping del PC-A a S1, VLAN 4.

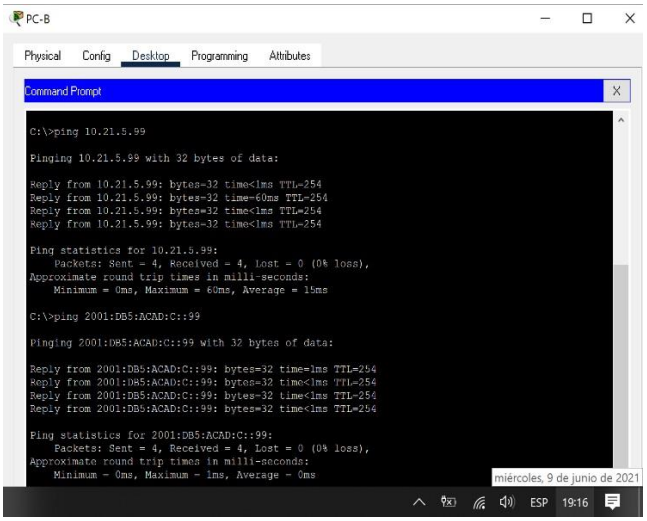


Fig. 10. Prueba de conectividad Ping del PC-A a S2, VLAN 4

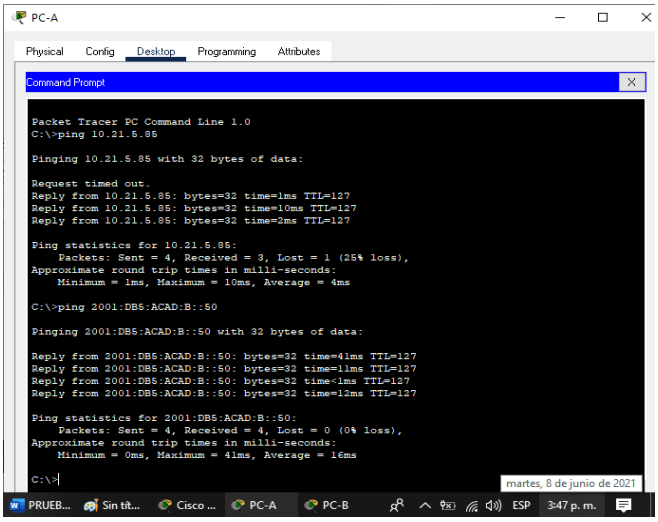


Fig. 11. Prueba de conectividad Ping del PC-A a PC-B

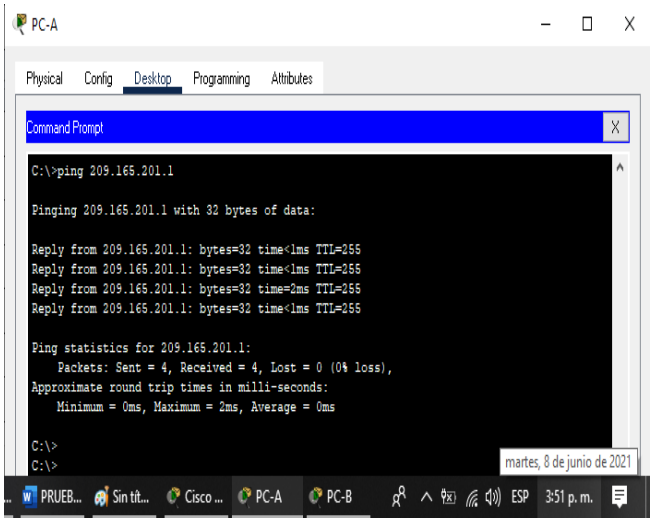


Fig. 12. Prueba de conectividad Ping del PC-A a R1 Loopback 0.

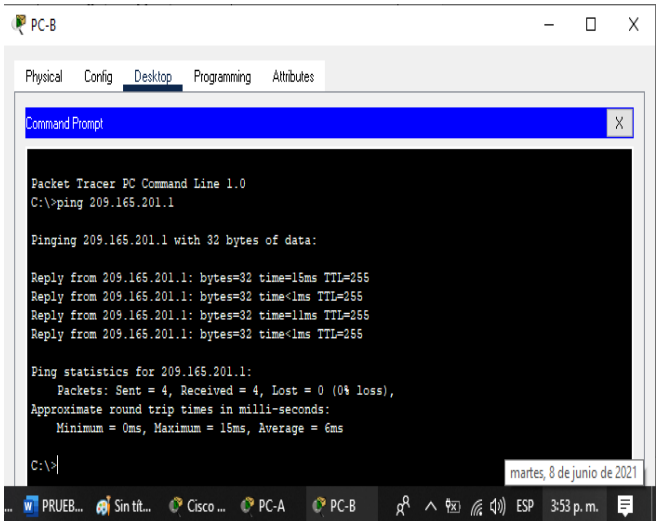


Fig. 13. Prueba de conectividad Ping del PC-B a R1 Loopback 0.

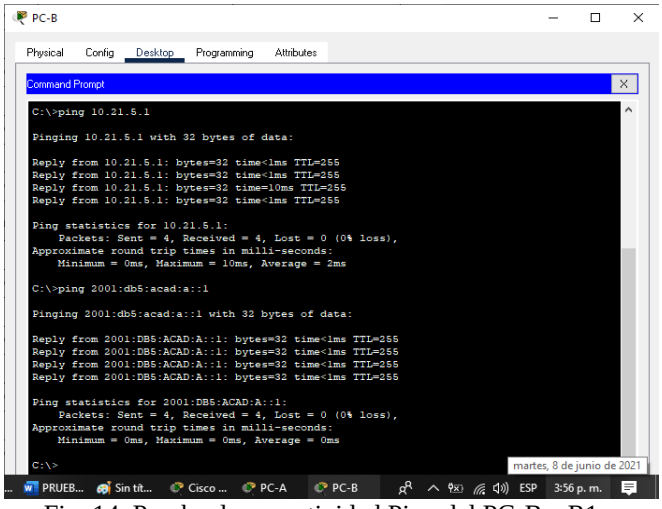


Fig. 14. Prueba de conectividad Ping del PC-B a R1, G0/0/1.2

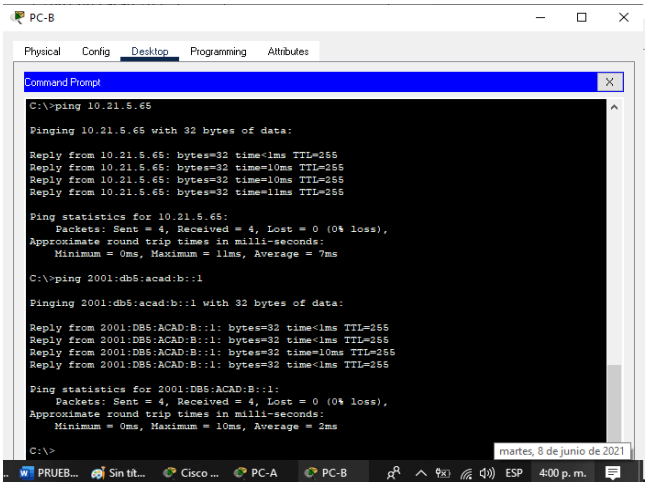


Fig. 15. Prueba de conectividad Ping del PC-B a R1, G0/0/1.3

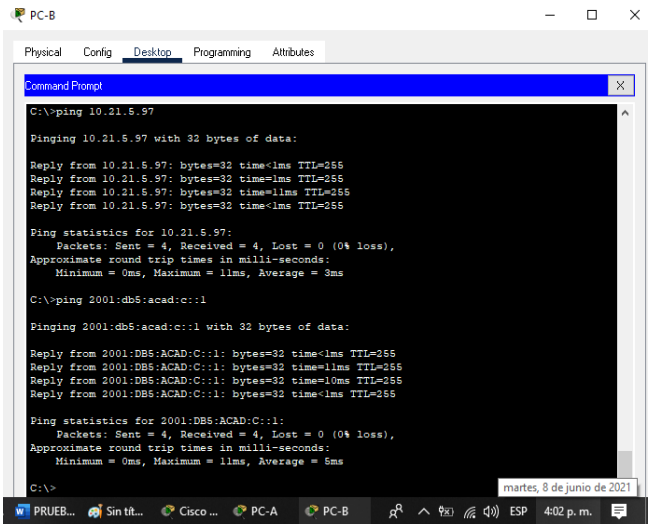


Fig. 16. Prueba de conectividad Ping del PC-B a R1, G0/0/1.4

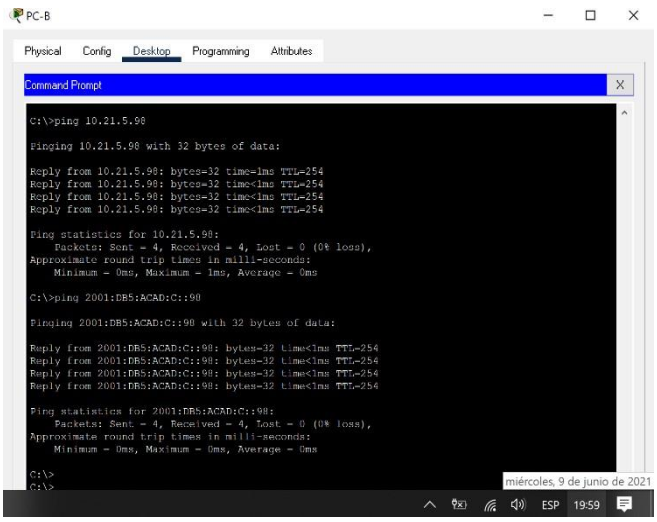


Fig. 17. Prueba de conectividad Ping del PC-B a S1, VLAN 4

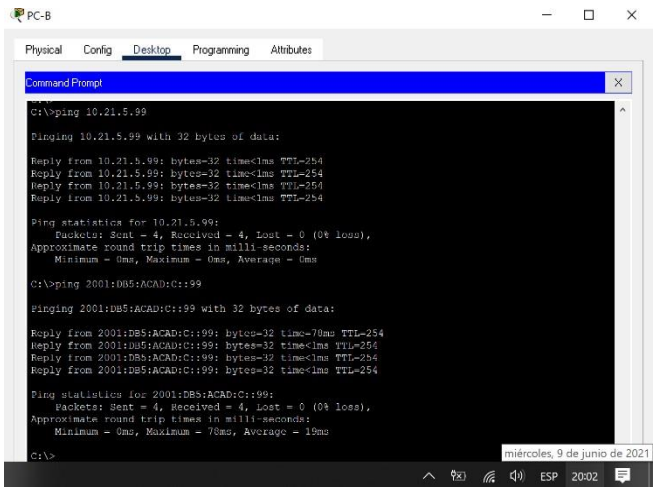


Fig. 18. Prueba de conectividad Ping del PC-B a S2, VLAN 4

IV. CONCLUSIÓN

Es importante al iniciar la configuración de cualquier equipo realizar una carga de las configuraciones iniciales y/o volver a configurar con el diseño o configuración deseado o con una copia de seguridad que se tenga de los parámetros del equipo operando satisfactoriamente.

Gracias a los conocimientos adquiridos en los laboratorio y trabajos colaborativos realizados a lo largo del curso de Diplomado, y con la ayuda del software Packet Tracer de CISCO para el montaje y simulación de la red a analizar; se logró la correcta y satisfactoria configuración de los escenarios propuestos como prueba de habilidades.

Es importante implementar correctamente las diferentes rutinas y comando aprendidos en el transcurso del Diplomado para que de una maneja eficaz y ágil los escenarios funcione sin mayores complicaciones.

REFERENCES

[1] CISCO. (2019). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4

[2] CISCO. (2019). Capa de aplicación. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10.

[3] CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

[4] CISCO. (2019). Capa de transporte. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9

[5]CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2

[6] CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

[7] CISCO. (2019). Configuración del Switch. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

[8] CISCO. (2019). Detección, Administración y Mantenimiento de Dispositivos. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#10

[9] CISCO. (2019). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

[10] CISCO. (2019). Direccionamiento IP. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

V. BIOGRAFIA

Abel Antonio Algarra, nacido el 12 de julio de 1974 en Bogotá (Colombia), se graduó como bachiller académico en 1992 en el Colegio Claretiano de Bogota, es candidato para obtener el título de Ingeniero en telecomunicaciones de la Universidad Nacional Abierta y a Distancia (UNAD). Es Tecnico en electrónica Industrial del SENA. Actualmente se desempeña como Tecnico Electrónico senior en Caracol Televisión.