DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN
“SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO”

MARTHA LUCIA PARADA PELAEZ

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

DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN
“SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO”

MARTHA LUCIA PARADA PELAEZ

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

DIRECTOR:

MSc. JUAN CARLOS VESGA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

4 de Marzo del 2022

AGRADECIMIENTOS

Quiero agradecerle principalmente a Dios por bendecirme todos los días y darme vida y salud para seguir adelante. Agradecerles a mis padres por guiarme en el camino correcto y cuidarme durante todo mi tiempo de vida estudiantil, por ser mi apoyo y fortaleza.

Agradecerle a la Universidad Nacional Abierta y a Distancia (UNAD), a sus docentes en especial a los docentes del programa de ingeniería de sistemas por haber compartido sus conocimientos a lo largo de mi formación como profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ACL (Lista de Control de Accesos): Es una serie de instrucciones que controlan que en un Router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

BÚSQUEDA DE DNS (Sistema de nombres de dominio): Es el proceso involucrado en la obtención de una dirección de Protocolo de Internet (IP) cuando se realiza una solicitud de resolución de DNS. El sistema DNS es una red interconectada de servidores informáticos dispuestos en una jerarquía de dominios y subdominios. Dependiendo de la naturaleza de la resolución DNS y de la información DNS que los servidores DNS almacenan en caché, una búsqueda DNS puede viajar lateralmente a través del sistema DNS o reenviarse a servidores ascendentes o raíz.

DHCP (Protocolo de configuración dinámica de host): Es un protocolo de red que utiliza una arquitectura cliente-servidor. Este se encarga de asignar de manera dinámica y automática una dirección IP, ya sea una dirección IP privada desde el router hacia los equipos de la red local, o también una IP pública por parte de un operador que utilice este tipo de protocolo para el establecimiento de la conexión.

DTP (Dynamic Trunking Protocol): Es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

ETHERCHANNEL: Es una tecnología de Cisco construida de acuerdo con los estándares 802.3 full-duplex Fast Ethernet. Permite la agrupación lógica de varios enlaces físicos Ethernet, esta agrupación es tratada como un único enlace y permite sumar la velocidad nominal de cada puerto físico Ethernet usado y así obtener un enlace troncal de alta velocidad. Los puertos usados deben tener las mismas características y configuración.

LÍNEAS VTY: permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15. El número de líneas vty que admite un router Cisco varía según el tipo de router y la versión de IOS.

NAT (Network Address Translator): Su función es traducir las direcciones para que sean posibles las conexiones, es una parte fundamental entre nuestros dispositivos e Internet. Forma parte del router, módem o el equipo que utilicemos para conectarnos a la red.

NTP (Network Time Protocol): Protocolo de tiempo de red, su función principal es la de sincronizar los relojes de los sistemas informáticos. Para ello utiliza el enrutamiento de paquetes en redes con latencia variable.

OSPF (Open Shortest Path First): Es un protocolo de enrutamiento dinámico interior (IGP – Internal Gateway Protocol -). Usa un algoritmo de tipo Estado de Enlace.

RSA: Criptosistemas de clave pública, se suele usar para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

VLAN (Virtual LAN): Redes de área local virtuales, es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente.

RESUMEN

El desarrollo del presente informe consiste en la configuración de dos redes de comunicación utilizando el software de simulación Cisco Packet Tracer. Primeramente, se realiza la topología, seguidamente se realizan las configuraciones básicas para cada uno de los dispositivos involucrados en cada una de las redes; y se continúa con las configuraciones para que permitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. Posteriormente en la primera red se configura el enrutamiento entre VLAN, el protocolo de configuración de hosts dinámicos DHCP, Etherchannel y port-security, mientras en la segunda red se configura además el protocolo de routing dinámico OSPF, 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, teniendo en cuenta el uso de comandos ping, traceroute, show ip route, entre otros para la realización de la verificación de conectividad. De esta manera se hace posible ejecutar las configuraciones para la administración de redes más seguras.

Palabras clave: CCNA, Cisco, Enrutamiento, Protocolo, Redes de telecomunicación, Seguridad.

ABSTRACT

The development of this report consists of the configuration of two communication networks using the Cisco Packet Tracer simulation software. First, the topology is made, then the basic configurations are made for each of the devices involved in each of the networks; and configurations continue to allow both IPv4 and IPv6 connectivity for supported hosts. Subsequently, in the first network, routing between VLANs, the DHCP dynamic host configuration protocol, Etherchannel, and port-security are configured, while in the second network, the OSPF dynamic routing protocol, dynamic network address translation, and static (NAT), access control lists (ACL) and the server/client network time protocol (NTP), taking into account the use of ping, traceroute, show ip route commands, among others, to carry out the verification of connectivity. In this way it is possible to execute the configurations for the administration of more secure networks.

Keywords: CCNA, Cisco, Routing, Protocol, Telecommunication networks, Security.

INTRODUCCIÓN

El presente informe está basado en la configuración de dos redes de comunicación utilizando el software de simulación Cisco Packet Tracer, para la identificación del grado de desarrollo de competencias y habilidades que fueron adquiridas en la solución de problemas relacionados con diversos aspectos de Networking.

La particularidad de estas redes es el uso de comandos especializados y diversos protocolos junto con métricas de enrutamiento., lo que facilita la tarea de administración de una red con acceso seguro y buena interoperabilidad.

Debido a que las redes LAN, están construidas mediante la interconexión de nodos mediante cables o medios inalámbricos, el ámbito de conexión está limitado ya sea por un edificio o nuestra propia habitación, casi sin posibilidad de acceso externo es importante asegurar buenas configuraciones internas.

DESARROLLO

1. ESCENARIO No.1

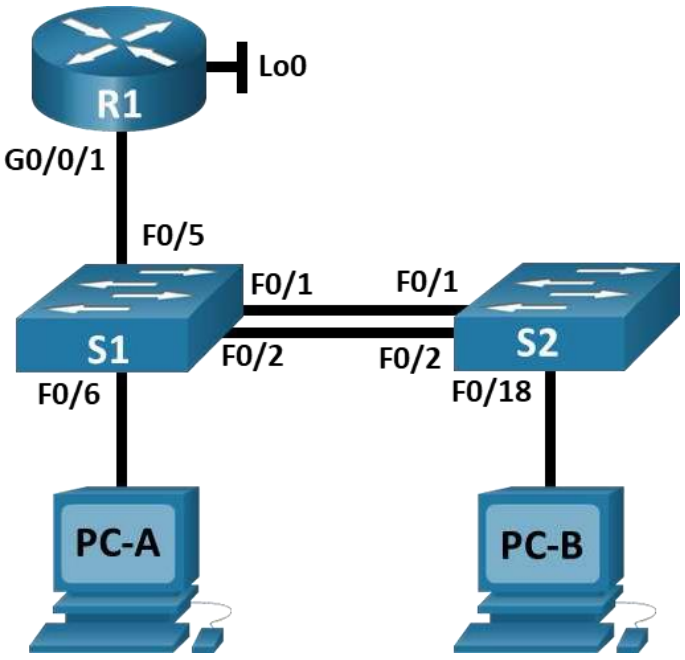
Este primer escenario tiene como objetivo configurar los dispositivos de la red para que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados, teniendo en cuenta que el Router y el Switch también deben administrarse de forma segura, además configurar el enrutamiento entre VLAN, DHCP, Etherchannel y port-security. Inicialmente se identificaran los dispositivos, seguidamente se realizara la topología, se procederá a realizar las respectivas configuraciones en el Router, los Switch y los equipos de cómputo, y por último se realizaran las verificaciones de conectividad de toda la red.

1.1 Topología

Los dispositivos que conforman la red son:

- Un Router Cisco ISR4331
- Dos Switch Cisco WS-C3560-24PS
- Dos equipos de cómputo de escritorio

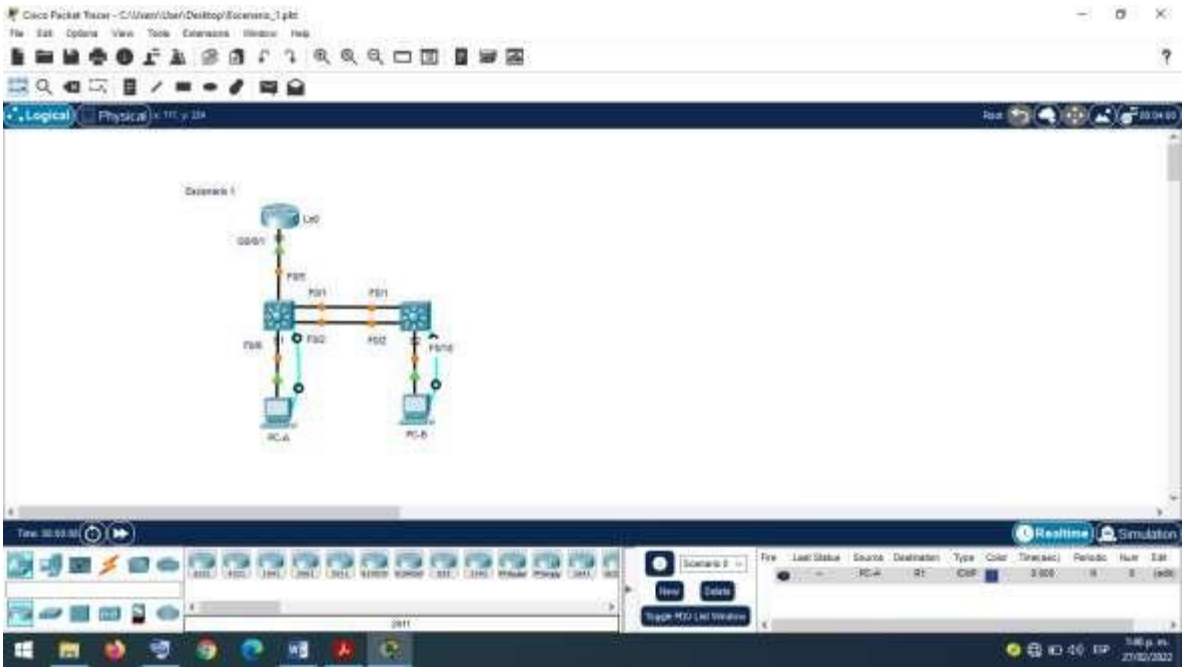
Figura 1 Topología de la red del escenario No. 1



Fuente: Guía Prueba de habilidades prácticas CCNA.

Se adicionan a la pantalla principal del software Cisco Packet Tracer los dispositivos, luego se conectan por medio del cable de cobre directo según corresponda el puerto FastEthernet como se muestra en la topología.

Figura 2 Realización del escenario No. 1 en el software.



Fuente: Propia.

Las VLAN a crear en el Switch S2 son:

Tabla 1 VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Fuente: Guía Prueba de habilidades prácticas CCNA.

Las direcciones IPv4 e IPv6 que se le asignan a cada dispositivo dentro de la red son:

Tabla 2 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:db5: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	DHCP para puerta de enlace predeterminada IPv4
	2001:db5:acad:b: :50 /64	fe80::1

Fuente: Guía Prueba de habilidades prácticas CCNA.

1.2 Procedimiento

Las configuraciones a realizar se deben realizar en orden secuencial, es por ello que se seguirá el siguiente procedimiento:

1.2.1 Parte 1: Inicializar y recargar y configurar aspectos básicos de los dispositivos

Esta primera parte está compuesta por los pasos descritos a continuación:

Paso 1: Inicializar y volver a cargar el router y el switch

Se introducen los siguientes comandos según corresponda a cada dispositivo, a través de la ventana CLI del mismo. En esta parte es importante tener presente que

en cada dispositivo primero se ingresa al modo EXEC-privilegiado por medio del comando **enable**.

Router (R1)

Router>enable

Router#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Router#show startup-config

Startup-config is not present

Router#reload

Proceed with reload? [confirm]

Switch (S1) y (S2)

Switch>enable

Switch#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

Erase of nvram: complete

Switch# show startup-config

Startup-config is not present

Switch#reload

Proceed with reload? [confirm]

Después de seguir las instrucciones anteriores, se realiza la activación de la plantilla SDM en los Switch por medio del comando, sdm prefer dual-ipv4-and-ipv6 default para que estos admitan el direccionamiento IPv4 e IPv6. En esta parte es importante tener presente que en cada dispositivo primero se ingresa al modo EXEC-privilegiado por medio del comando enable y seguidamente se coloca el comando configure terminal para ingresar en el modo EXEC-configuración. Al finalizar se

coloca el comando reload que permite activar la nueva configuración que se estableció en los Switch.

Switch (S1) y (S2)

Switch>enable

Switch#configure terminal

Switch(config)# sdm prefer dual-ipv4-and-ipv6 default

Switch(config)#exit

Switch#reload

System configuration has been modified. Save? [yes/no]: yes

Paso 2: Configurar R1

Esta configuración está compuesta por los parámetros básicos que deben llevar todos los dispositivos como desactivar la búsqueda DNS, nombre, contraseñas, mensaje de advertencia y su vez para este caso se crea un usuario administrativo, se habilita el routing Iv6 y se configuran las interfaces del Router con su respectiva dirección IP.

Tabla 3 Tareas de configuración para R1

Tarea	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router	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	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 privilege 15 secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#exit
Configurar VTY solo aceptando SSH	R1(config)#line vty 0 15 R1(config-line)#transport input ssh R1(config-line)#login local R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #El acceso no autorizado está prohibido#
Habilitar el routing IPv6	R1(config)#ipv6 unicast-routing
Configurar interfaz G0/0/1 y subinterfaces, para esto: • 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 gi0/1.2 R1(config-subif)#encapsulation dot1q 2 R1(config-subif)#description LAN to VLAN2 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)#exit
	R1(config)#interface gi0/1.3 R1(config-subif)#encapsulation dot1q 3 R1(config-subif)#description LAN to VLAN3 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)#exit
	R1(config)#interface gi0/1.4 R1(config-subif)#encapsulation dot1q 4 R1(config-subif)#description LAN to VLAN4 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 R1(config-subif)#exit
	R1(config)#interface gi0/1.6 R1(config-subif)#encapsulation dot1q 6 R1(config-subif)#description VLAN6 Native R1(config-subif)#ipv6 address fe80::1 link-local R1(config-subif)#no shutdown R1(config-subif)#exit
Configure el Loopback0 interface, para esto: • Establezca la descripción • Establece la dirección IPv4. • Establece la dirección IPv6. • Establezca la dirección local de enlace IPv6 como fe80::1	R1(config)#interface loopback0 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)#no shutdown R1(config-if)#exit
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#crypto key generate rsa 1024 R1(config)#do write R1(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar Switches S1 y S2

Esta configuración está compuesta por los parámetros básicos que deben llevar todos los dispositivos como desactivar la búsqueda DNS, nombre, contraseñas, configuración del inicio de sesión en las líneas VTY para que use la base de datos local, crear el mensaje de advertencia, configurar VTY solo aceptando SSH, generar una clave de cifrado RSA por medio del crypto key generate rsa 1024 y su vez para este caso además se configurar la interfaz de administración (SVI).

Tabla 4 Tareas de configuración para S1.

Tarea	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain lookup
Nombre del Switch	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 S1(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config)#line vty 0 15 S1(config-line)#transport input ssh S1(config-line)#login local S1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configure un MOTD Banner	S1(config)# banner motd #El acceso no autorizado está prohibido#
Generar una clave de cifrado RSA y asignarle el Módulo de 1024 bits	S1(config)#crypto key generate rsa 1024
Configurar interfaz de administración (SVI) para esto hay que: • 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 Vlan4 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 Vlan4 Management S1(config-if)#no shutdown

	S1(config-if)#exit
Configuración del gateway predeterminado, para esto hay que: • Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S1(config)#ip default-gateway 10.21.5.97 S1(config)#do write Building configuration... [OK]

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

En este paso, se repiten las mismas tareas que se configuraron previamente en S1.

Tabla 5 Tareas de configuración para S2.

Tarea	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Switch(config)#no ip domain lookup
Nombre del Switch	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 S2(config-line)#exit
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S2(config)#line vty 0 15 S2(config-line)#transport input ssh S2(config-line)#login local S2(config-line)#exit

Cifrar las contraseñas de texto no cifrado	S2(config)#service password-encryption
Configure un MOTD Banner	S2(config)# banner motd #El acceso no autorizado está prohibido#
Generar una clave de cifrado RSA y asignarle el Módulo de 1024 bits	S2(config)#crypto key generate rsa 1024
Configurar interfaz de administración (SVI) para esto hay que: • 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 Vlan4 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::98 link-local S2(config-if)#description Vlan4 Management S2(config-if)#no shutdown S2(config-if)#exit
Configuración del gateway predeterminado, para esto hay que: • Configure la puerta de enlace predeterminada como 10.21.5.97 para IPv4	S2(config)#ip default-gateway 10.21.5.97 S2(config)#do write Building configuration... [OK]

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

1.2.2 Parte 2: Configuración de la infraestructura de red (VLAN, trunking, etherchannel)

Esta parte de configuración troncal, le proporciona a la red la facilidad de utilizar solo una interfaz para enrutar los paquetes de varias VLANs que viajan a través de los Switches.

Paso 1: Configurar S1

Iniciamos creando las VLAN para así crear enlaces troncales 802.1Q en las interfaces F0/1, F0/2 y F0/5, esto para permitir el paso del tráfico de las distintas VLANs creadas, Seguidamente se crea un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2 por medio del comando channel-group number mode on para agregar la interfaz física al channel. Además se usa el protocolo LACP ((Link Aggregation Control Protocol o protocolo de control de agregación de enlaces) para la negociación formando un único canal lógico, por último se configura la seguridad del puerto en los puertos de acceso para solo tres direcciones.

Tabla 6 Configuración de la infraestructura de red en 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(config)#vlan 2 S1(config-vlan)#name Bikes S1(config-vlan)#exit S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config-vlan)#exit S1(config)#vlan 4 S1(config-vlan)#name Management S1(config-vlan)#exit S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config-vlan)#exit S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit
Crear troncales 802.1Q que utilicen la VLAN 6 nativa en las interfaces F0/1, F0/2 y F0/5	S1(config)#interface fa0/5 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk allowed vlan 2,3,4,6 S1(config-if)#exit
	S1(config)#interface range fastEthernet 0/1-2 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)#switchport trunk allowed vlan 2,3,4,6 S1(config-if-range)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, para ello usar el protocolo LACP para la negociación.	S1(config)#interface range fastEthernet 0/1-2 S1(config-if-range)#channel-group 1 mode active S1(config-if-range)#channel-protocol lacp

	S1(config-if-range)#interface Port-channel 1 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trun k S1(config-if)#switchport trunk native vlan 6 S1(config-if)#exit
Configurar el puerto de acceso de host para VLAN 2 en la Interface F0/6	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#exit
Configure port-security en los access ports, para que permita 3 direcciones MAC.	S1(config)#interface fastEthernet 0/6 S1(config-if)#switchport port-security maximum 3 S1(config-if)#exit
Proteja todas las interfaces no utilizadas, para esto hay que: • Asignar a VLAN 5. • Establecer en modo de acceso, agregar una descripción y apagar	S1(config)#interface range fa0/3-4, fa0/7-24, gig0/1-2 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#description *** Puertos sin utilizar *** S1(config-if-range)#shutdown S1(config-if-range)#exit S1(config)#do write Building configuration... [OK]

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar S2

En este paso, se repiten las mismas tareas que se configuraron previamente en S1.

Tabla 7 Configuración de la infraestructura de red en S2

Tarea	Especificación
Crear VLAN, estas son: • VLAN 2, nombre Bikes • VLAN 3, nombre Trikes	S2(config)# S2(config)#vlan 2 S2(config-vlan)#name Bikes

• VLAN 4, name Management • VLAN 5, nombre Parking • VLAN 6, nombre Native	S2(config-vlan)#vlan 3 S2(config-vlan)#name Trikes S2(config-vlan)#vlan 4 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)#do wr Building configuration... [OK]
Crear troncales 802.1Q que utilicen la VLAN 6 nativa en las interfaces F0/1 y F0/2	S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)# shutdown S2(config-if-range)#switchport trunk encapsulation dot1q S2(config-if-range)#switchport mode trunk S2(config-if-range)#switchport trunk native vlan 6 S2(config-if-range)#switchport trunk allowed vlan 2,3,4,6 S2(config-if-range)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2, para ello usar el protocolo LACP para la negociación.	S2(config)#interface range fastEthernet 0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#interface Port-channel 1 S2(config-if-range)#channel-protocol lacp S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport trunk native vlan 6 S2(config-if)#exit
Configurar el puerto de acceso de host para VLAN 3 en la Interface F0/18	S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports, para que permita 3 direcciones MAC.	S2(config)#interface fastEthernet 0/18 S2(config-if)#switchport mode access

	S2(config-if)#switchport port-security maximum 3 S2(config-if)#do write Building configuration... [OK]
Proteja todas las interfaces no utilizadas, para esto hay que: • Asignar a VLAN 5. • Establecer en modo de acceso, agregar una descripción y apagar	S2(config)#interface range fa0/3-17, fa0/19-24, gig0/1-2 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport access vlan 5 S2(config-if-range)# switchport port-security S2(config-if-range)# switchport port-security violation shutdown S2(config-if-range)#description ***Puertos sin utilizar *** S2(config-if-range)#shutdown S2(config-if)#do write Building configuration... [OK]

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

1.2.3 Parte 3: Configurar soporte de host

Para esta parte se utiliza el protocolo de configuración dinámica de host (también conocido por sus siglas de DHCP), este asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo de forma automática.

Paso 1: Configure R1

Esta configuración se realiza en R1 solamente, para ello se crear una ruta predeterminada para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0, y seguidamente se configura IPv4 DHCP para VLAN 2 y para la VLAN 3.

Tabla 8 Configuración del soporte de host en R1

Tarea	Especificación
Configure Default Routing, para esto hay que:	R1>enable R1#configure terminal

• Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0	R1(config)# ip route 0.0.0.0 0.0.0.0 loopback 0 R1(config)# ipv6 route ::/0 loopback 0
Configurar IPv4 DHCP para VLAN 2, para esto hay que: • 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 10.21.5.2 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, para esto hay que: • 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(config)#do write

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Configurar los servidores

Esta configuración está compuesta por la dirección física, IP, que siempre va acompañada de la máscara de subred, y el Gateway tanto para IPv4 como para IPv6 que es la puerta de enlace o pasarela, que permite a través de sí mismo, acceder a otra red. Después de configurar cada servidor, se registran las configuraciones de red del host utilizando el comando ipconfig /all, en la ventana Command Prompt del equipo.

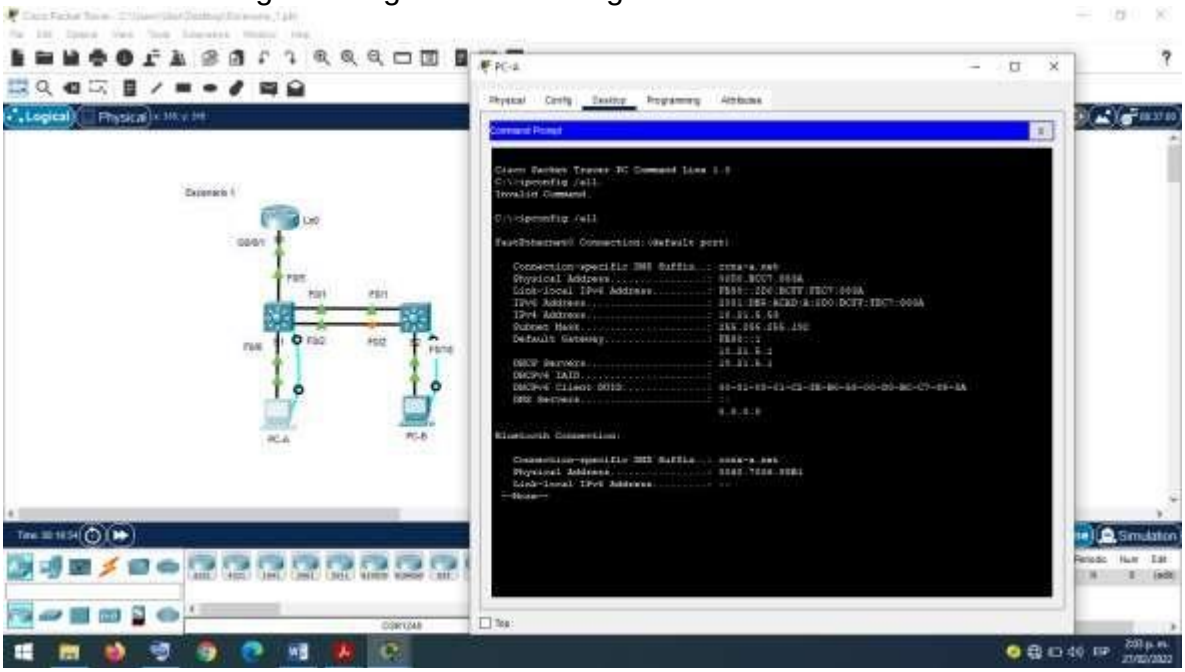
Tabla 9 Configuración de red del PC-A

Configuración de red de PC-A

Descripción	PC-A
Dirección física	00D0.BCC7.883A
Dirección IP	10.21.5.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.21.5.1
Gateway predeterminado IPv6	FE80::1

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 3 Registro de las configuraciones de red en PC-A



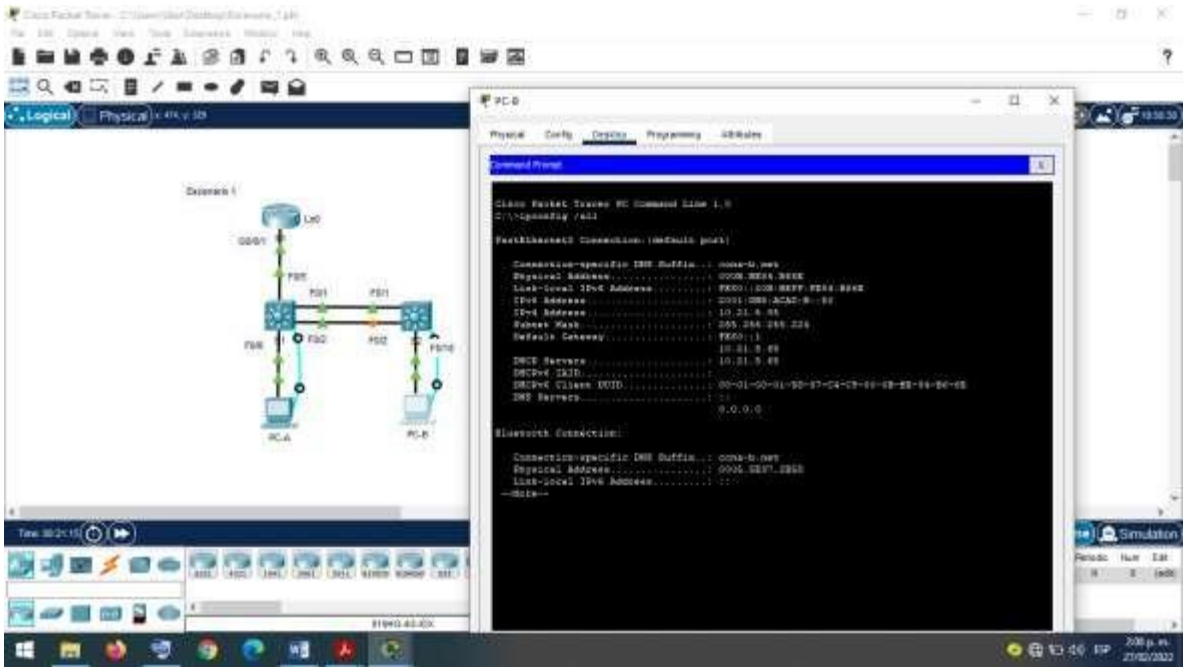
Fuente: Propia.

Tabla 10 Configuración de red del PC-B

Configuración de red de PC-B	
Descripción	PC-B
Dirección física	000B.BE84.B66E
Dirección IP	10.21.5.85
Máscara de subred	255.255.255.224
Gateway predeterminado	10.21.5.65
Gateway predeterminado IPv6	FE80::1

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 4 Registro de las configuraciones de red en PC-B



Fuente: Propia.

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

La parte de la verificación de conectividad se realiza desde un equipo a otro, para ello se abre la consola de comandos y se escribe el comando ping seguido de la dirección IP del host.

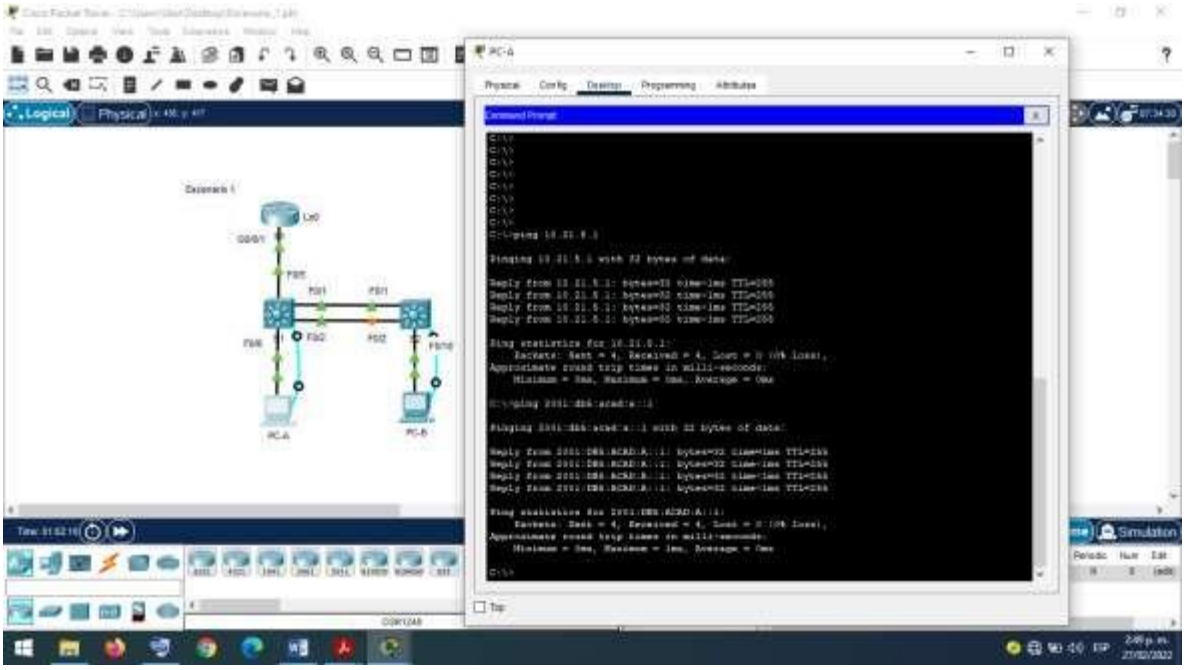
Tabla 11 Prueba de conectividad de red

Desde	A	de Internet	Dirección IP	Resultados de PING
PC-A	R1, G0/0/1.2	Dirección	10.21.5.1	Exitoso (Figura 5)
		IPv6	2001:db5:acad:a::1	Exitoso (Figura 5)
	R1, G0/0/1.3	Dirección	10.21.5.65	Exitoso (Figura 6)
		IPv6	2001:db5:acad:b::1	Exitoso (Figura 6)
	R1, G0/0/1.4	Dirección	10.21.5.97	Exitoso (Figura 7)

		IPv6	2001:db5:acad:c::1	Exitoso (Figura 7)
	S1, VLAN 4	Dirección	10.21.5.98	Exitoso (Figura 8)
		IPv6	2001:db5:acad:c::98	Exitoso (Figura 8)
	S2, VLAN 4	Dirección	10.21.5.99	Exitoso (Figura 9)
		IPv6	2001:db5:acad:c::99	Exitoso (Figura 9)
	PC-B	Dirección	10.21.5.85	Exitoso (Figura 10)
		IPv6	2001:DB5:ACAD:B:20B:BEFF:FE84:B66E	Exitoso (Figura 10)
	R1 Bucle 0	Dirección	209.165.201.1	Exitoso (Figura 11)
		IPv6	2001:db5:acad:209::1	Exitoso (Figura 11)
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Exitoso (Figura 12)
		IPv6	2001:db5:acad:209::1	Exitoso (Figura 12)
	R1, G0/0/1.2	Dirección	10.21.5.1	Exitoso (Figura 13)
		IPv6	2001:db5:acad:a::1	Exitoso (Figura 13)
	R1, G0/0/1.3	Dirección	10.21.5.65	Exitoso (Figura 14)
		IPv6	2001:db5:acad:b::1	Exitoso (Figura 14)
	R1, G0/0/1.4	Dirección	10.21.5.97	Exitoso (Figura 15)
		IPv6	2001:db5:acad:c::1	Exitoso (Figura 15)
	S1, VLAN 4	Dirección	10.21.5.98	Exitoso (Figura 16)
		IPv6	2001:db5:acad:c::98	Exitoso (Figura 16)
	S2, VLAN 4	Dirección	10.21.5.99	Exitoso (Figura 17)
		IPv6	2001:db5:acad:c: :99	Exitoso (Figura 17)

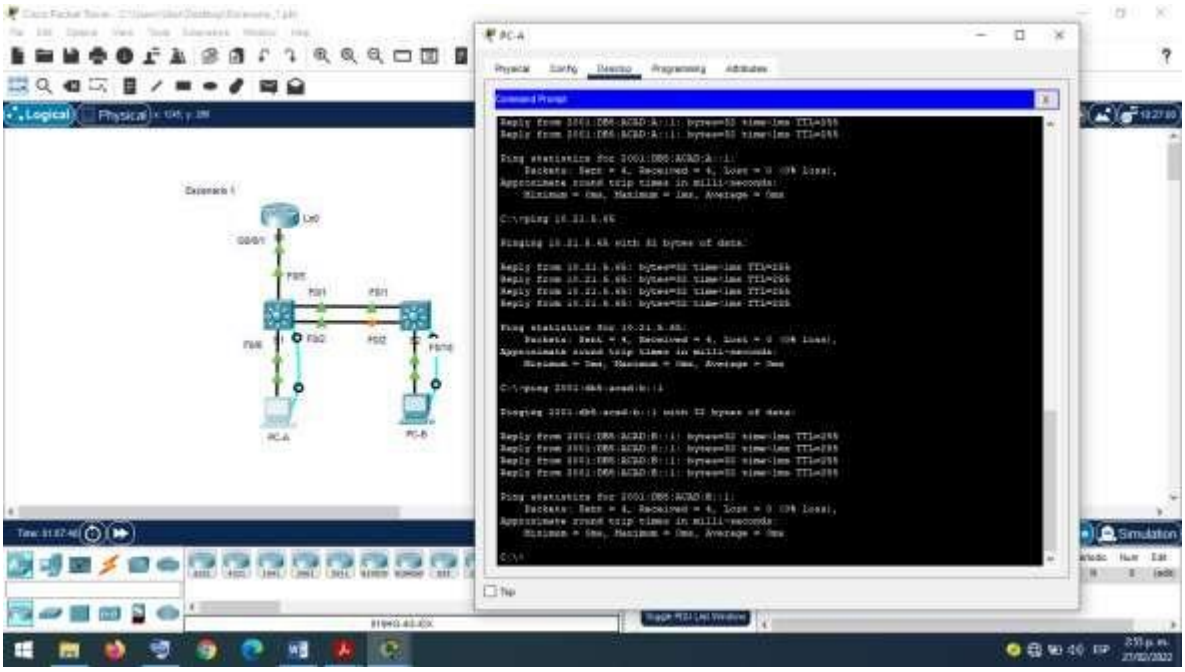
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 5 Prueba de conectividad desde PC-A a R1 (G0/0/1.2)



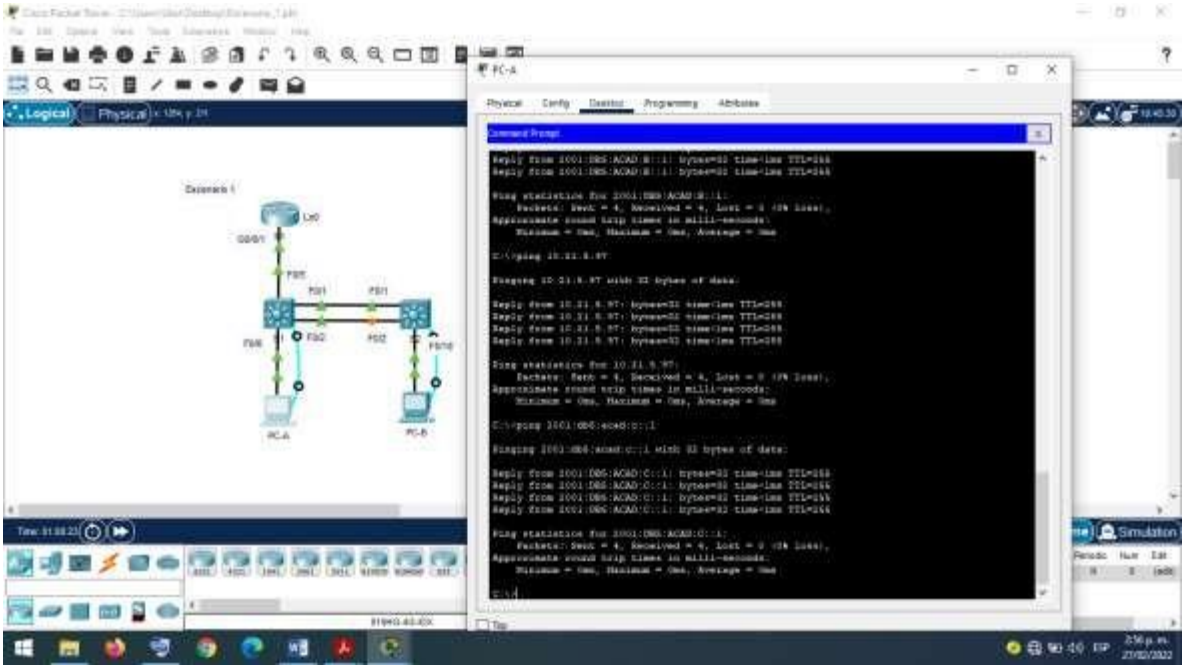
Fuente: Propia

Figura 6 Prueba de conectividad desde PC-A a R1 (G0/0/1.3)



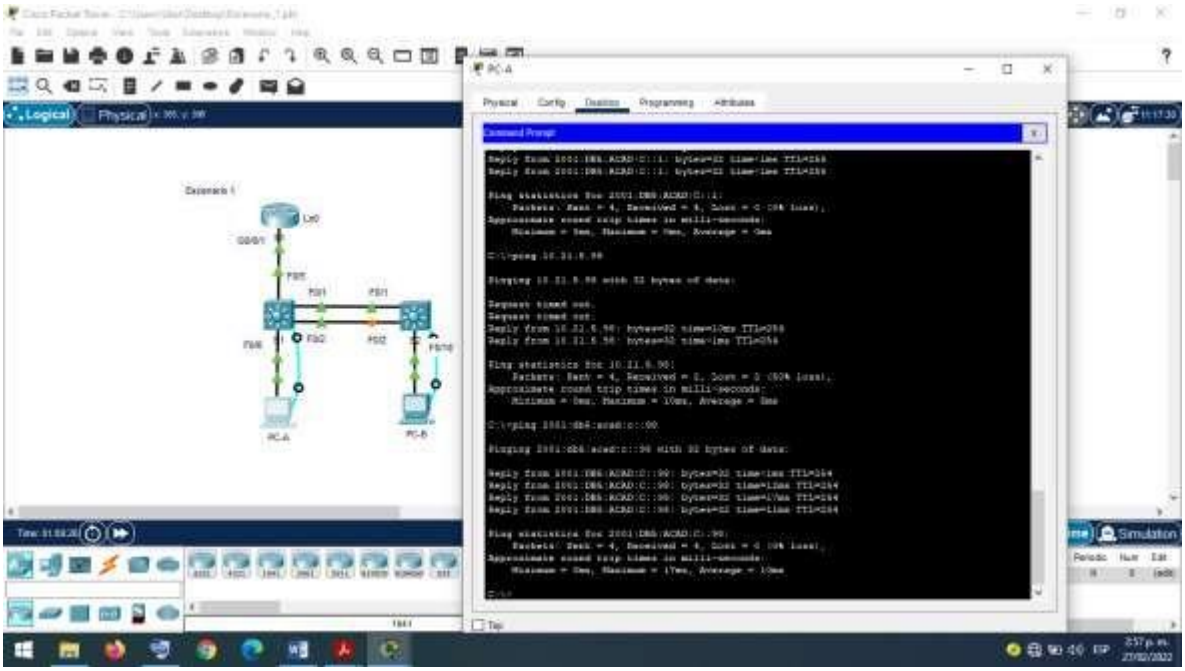
Fuente: Propia

Figura 7 Prueba de conectividad desde PC-A a R1 (G0/0/1.4)



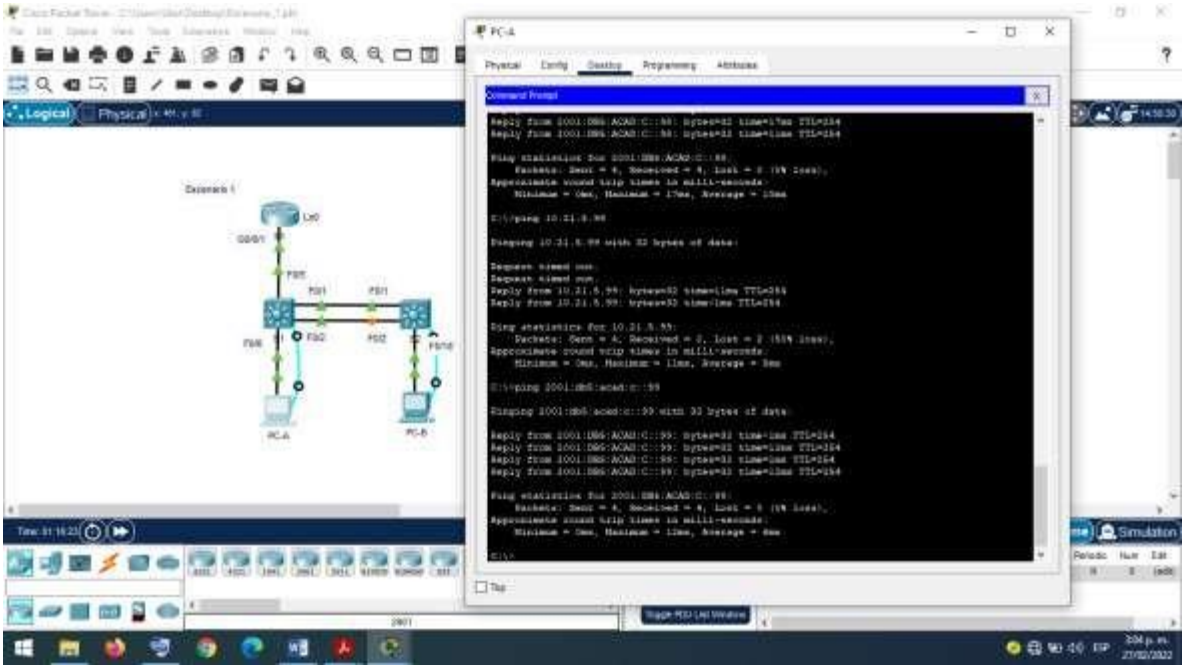
Fuente: Propia

Figura 8 Prueba de conectividad desde PC-A a S1 (VLAN 4)



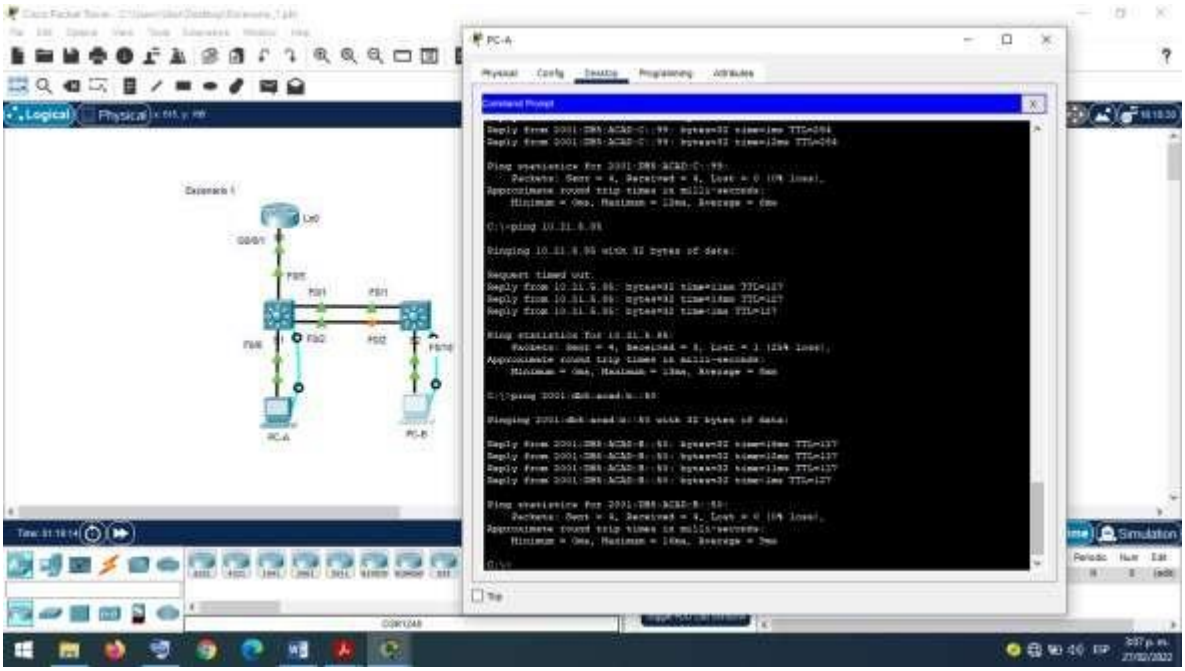
Fuente: Propia

Figura 9 Prueba de conectividad desde PC-A a S2 (VLAN 4)



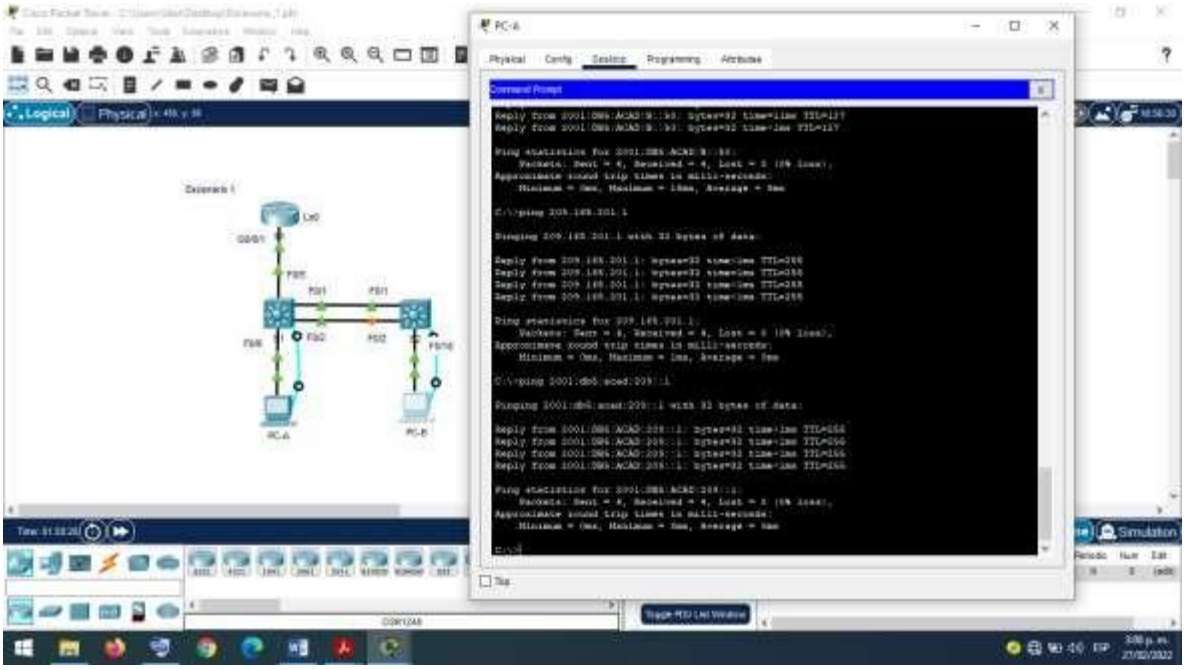
Fuente: Propia

Figura 10 Prueba de conectividad desde PC-A a PC-B



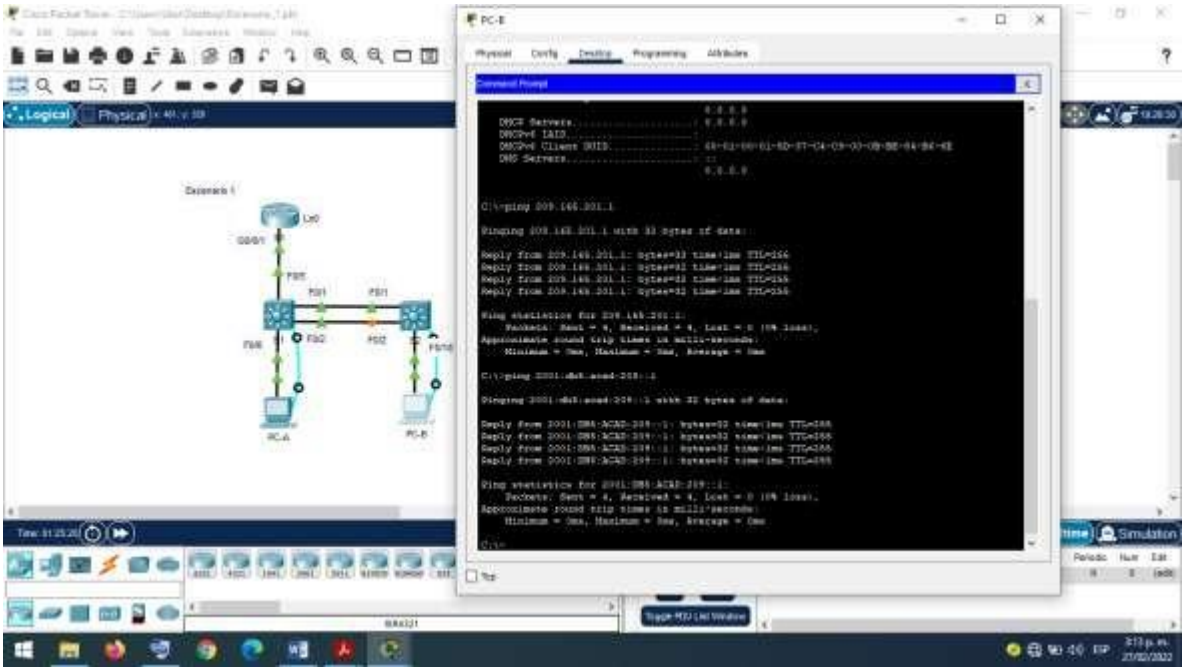
Fuente: Propia

Figura 11 Prueba de conectividad desde PC-A a R1 (Bluce 0)



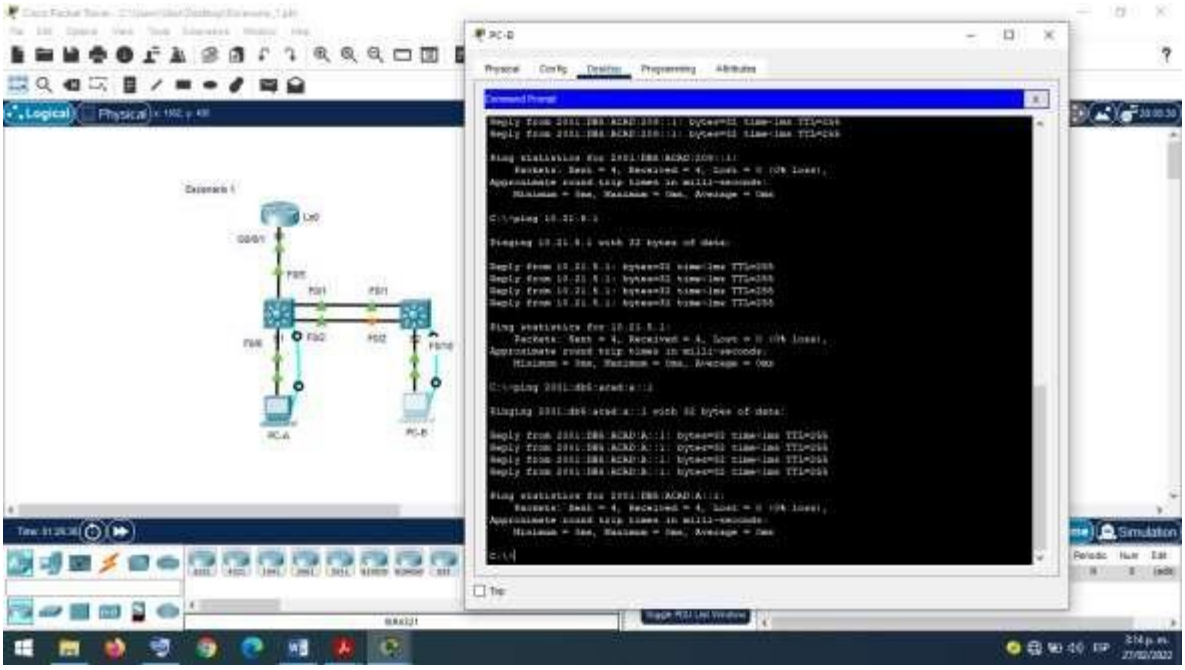
Fuente: Propia

Figura 12 Prueba de conectividad desde PC-B a R1 (Bluce 0)



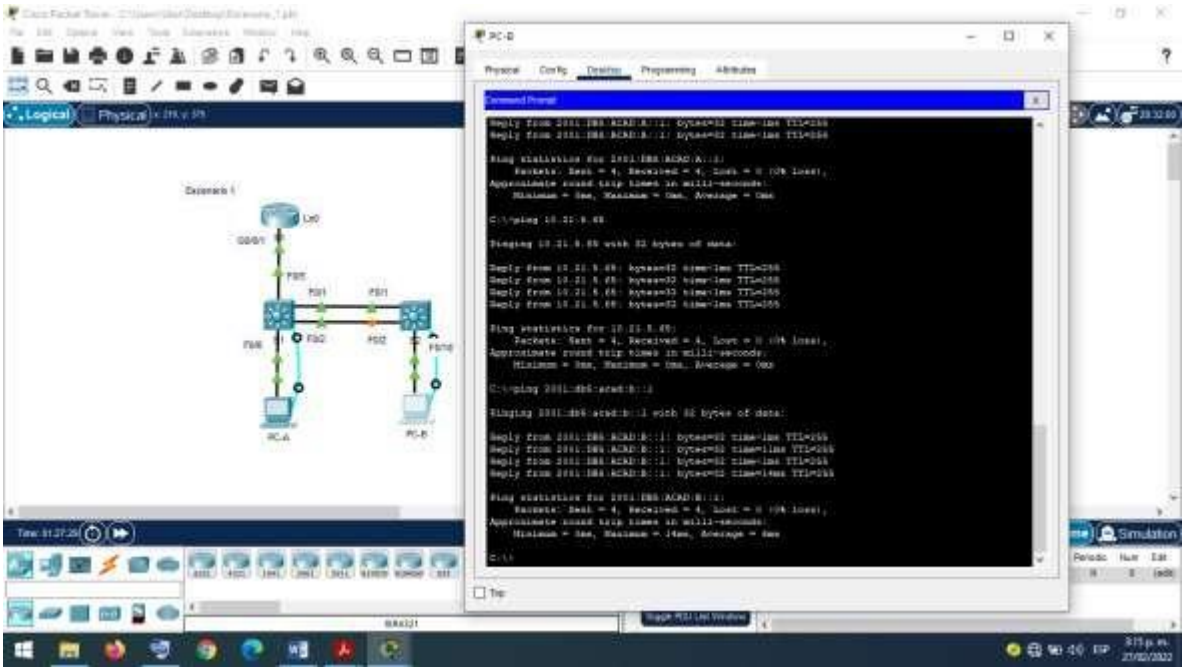
Fuente: Propia

Figura 13 Prueba de conectividad desde PC-B a R1(G0/0/1.2)



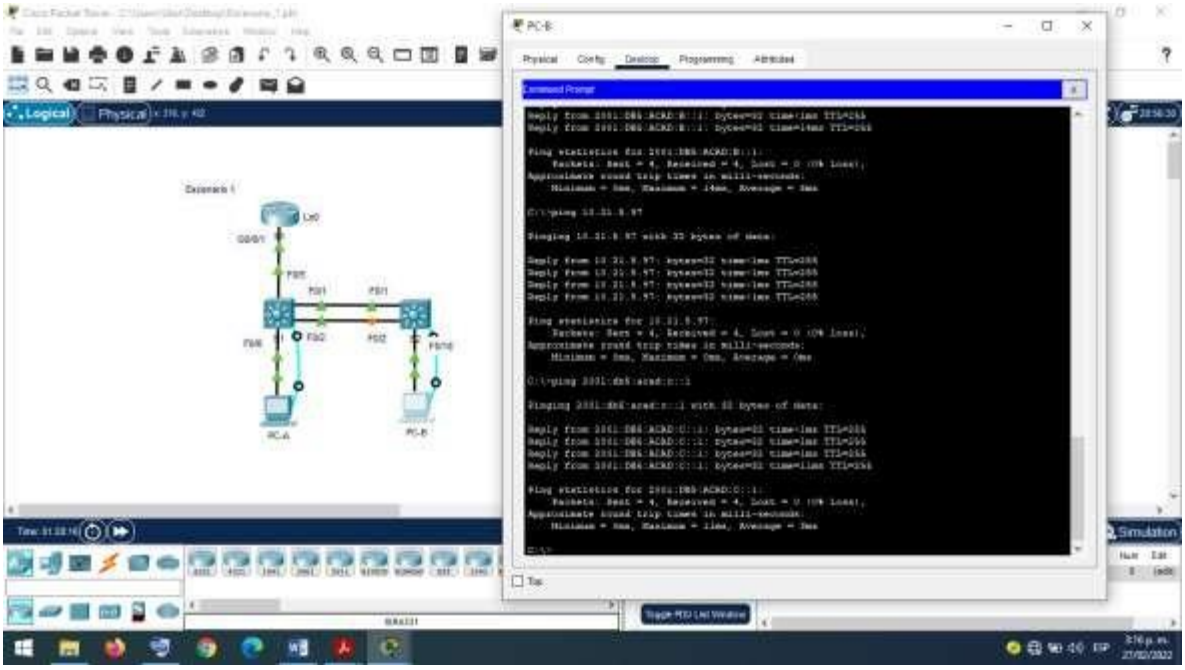
Fuente: Propia

Figura 14 Prueba de conectividad desde PC-B a R1(G0/0/1.3)



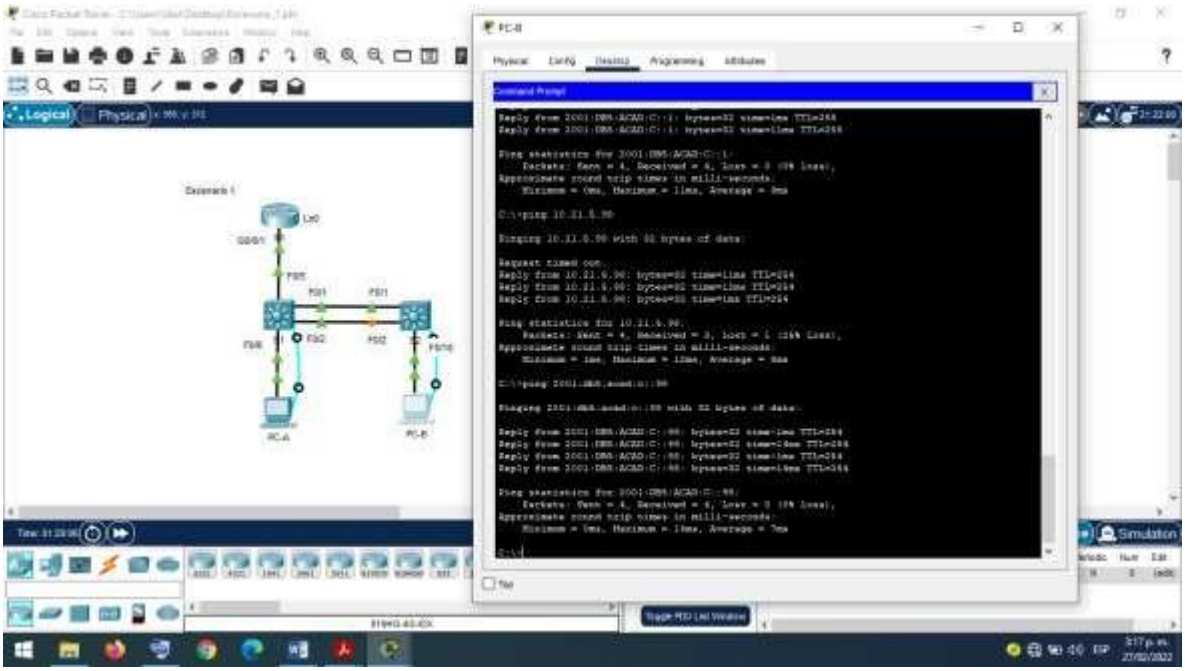
Fuente: Propia

Figura 15 Prueba de conectividad desde PC-B a R1(G0/0/1.4)



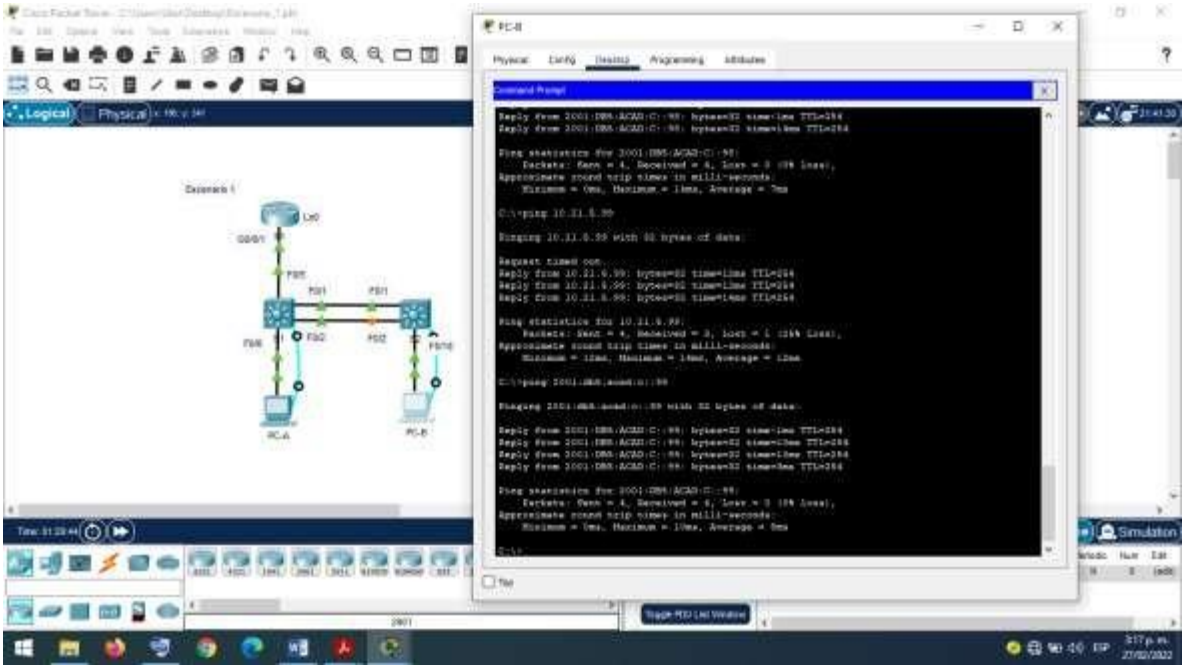
Fuente: Propia

Figura 16 Prueba de conectividad desde PC-B a S1 (VLAN 4)



Fuente: Propia

Figura 17 Prueba de conectividad desde PC-B a S2 (VLAN 4)



Fuente: Propia

A través de las imágenes anteriores se muestra el registro de conectividad desde un equipo a otro, para ello se abre la consola de comandos y se escribe el comando ping seguido de la dirección IP del host según corresponda (Ver Tabla 11).

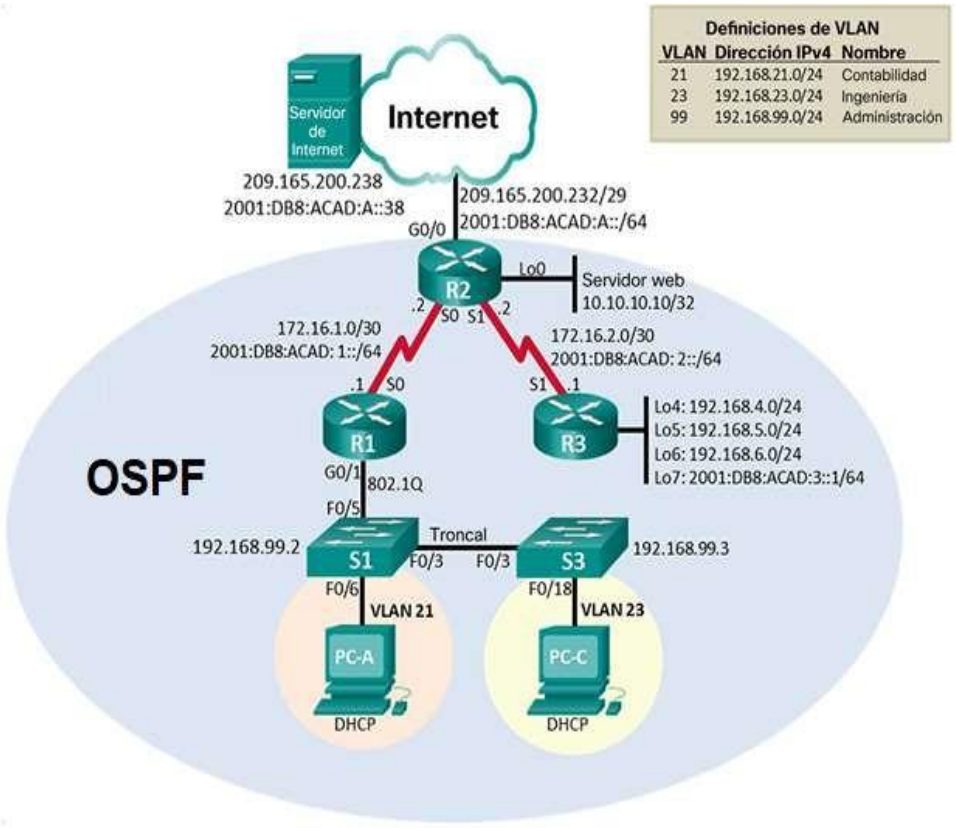
Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

2. ESCENARIO No.2

Este segundo escenario tiene como objetivo configurar los dispositivos de la red para que admitan tanto la conectividad IPv4 como IPv6, configurar la 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. Inicialmente se identificaran los dispositivos, seguidamente se realizara la topología, se procederá a realizar las respectivas configuraciones en el Router, los Switch y los equipos de cómputo, y por último se realizaran las verificaciones de conectividad de toda la red.

2.1 Topología

Figura 18 Topología de la red del escenario No. 2



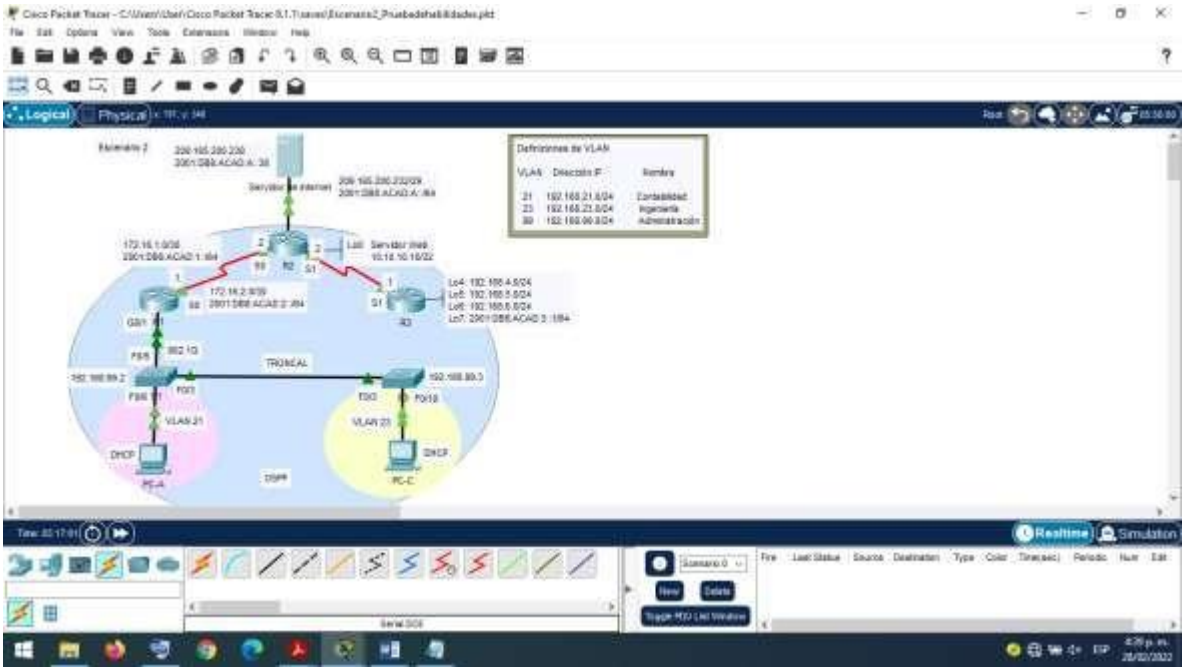
Fuente: Guía Prueba de habilidades prácticas CCNA.

Los dispositivos que conforman la red son:

- Tres Router Cisco 1941
- Dos Switch Cisco 2960-24TT
- Un Server-PT
- Dos equipos de cómputo de escritorio

Se adicionan a la pantalla principal del software Cisco Packet Tracer los dispositivos, luego se conectan por medio del cable de cobre directo según corresponda el puerto FastEthernet como se muestra en la topología.

Figura 19 Realización del escenario No. 2.



Fuente: Propia.

2.2 Procedimiento

Las configuraciones a realizar se deben realizar en orden secuencial, es por ello que se seguirá el siguiente procedimiento:

2.2.1 Parte 1: Inicializar y recargar y configurar aspectos básicos de los dispositivos

Esta primera parte está compuesta por los pasos descritos a continuación:

Paso 1: Inicializar y volver a cargar los Routers y los Switches

Se introducen los siguientes comandos según corresponda a cada dispositivo, a través de la ventana CLI del mismo. En esta parte es importante tener presente que en cada dispositivo primero se ingresa al modo EXEC-privilegiado por medio del comando enable.

Tabla 12 Inicialización de los routers y switchs

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router# erase startup-config Continue? [confirm] [Enter] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Router# reload Proceed with reload? [confirm] [Enter]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [Enter] [OK] Erase of nvram: complete
Volver a cargar ambos switches	Switch# reload Proceed with reload? [confirm] [Enter]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show vlan brief

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

2.2.2 Parte 2: Configurar los parámetros básicos de los dispositivos.

Esta parte está compuesta por los parámetros básicos que deben llevar todos los dispositivos

Paso 1: Configurar la computadora de Internet.

Esta configuración está compuesta por la dirección física, IP, que siempre va acompañada de la máscara de subred, y el Gateway tanto para IPv4 como para

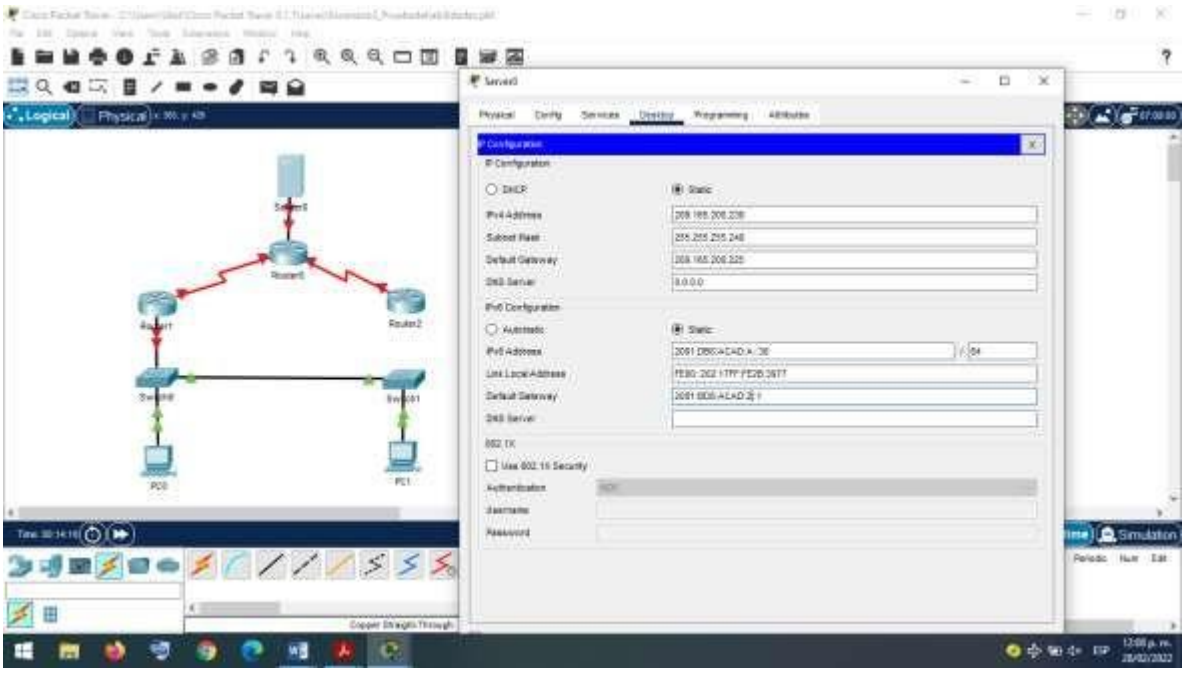
IPv6 que es la puerta de enlace o pasarela, que permite a través de sí mismo, acceder a otra red.

Tabla 13 Direcciones IPv4 e IPv6 para configurar en la computadora

Tarea	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:BD8:ACAD:A::25

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 20 Verificación de la configuración en computadora



Fuente: Propia.

Paso 2: Configurar R1.

Esta configuración está compuesta por los parámetros básicos que deben llevar todos los dispositivos como desactivar la búsqueda DNS, nombre, contraseña de exec, de acceso a la consola, de acceso a Telnet, mensaje de advertencia y su vez

para este caso se establecen las direcciones IPv4 e IPv6 y rutas predeterminadas para la interfaz S0/0/0.

Tabla 14 Configuración R1

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Router(config)#no ip domain-lookup
Nombre del router “R1”	Router>enable Router# configure terminal Router(config)#hostname R1
Contraseña de exec privilegiado cifrada • class	R1(config)# enable secret class
Contraseña de acceso a la consola • cisco	R1(config)# line console 0 R1(config-line)# password cisco R1(config-line)# login R1(config-line)# exit
Contraseña de acceso Telnet • 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 #El acceso no autorizado está prohibido#
Interfaz S0/0/0 para esto: • Establezca la descripción • Establecer la dirección IPv4 (Consultar el diagrama de topología para conocer la información de direcciones) • Establecer la dirección IPv6 (Consultar el diagrama de topología para conocer la información de direcciones) • Establecer la frecuencia de reloj en 128000 • Activar la interfaz	R1(config)#interface serial 0/0/0 R1(config)#description Conexion a R2 R1(config)#ip address 172.16.1.1 255.255.255.252 R1(config)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config)#clock rate 128000 R1(config)#no shutdown
Rutas predeterminadas • Configurar una ruta IPv4 predeterminada de S0/0/0	R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2

• Configurar una ruta IPv6 predeterminada de S0/0/0	

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar R2.

Esta configuración está compuesta por los parámetros básicos que deben llevar todos los dispositivos como desactivar la búsqueda DNS, nombre, contraseña de exec, de acceso a la consola, de acceso a Telnet, mensaje de advertencia y su vez se establecen las direcciones IPv4 e IPv6 para la interfaz S0/0/0, S0/0/1, G0/0 y loopback 0(Servidor web). Las direcciones se establecen según correspondan.

Tabla 15 Configuración R2

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Router>enable Router#configure terminal 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 console 0 R2(config-line)# password cisco R2(config-line)# login
Contraseña de acceso Telnet • cisco	R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)# login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption R2(config)#exit
Habilitar el servidor HTTP	No aplica (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)# R2(config)#ip http server ^ % Invalid input detected at '^' marker. R2(config)#exit

Mensaje MOTD “Se prohíbe el acceso no autorizado.”	R2(config)# banner motd #El acceso no autorizado está prohibido#
Interfaz S0/0/0 para esto: • Establezca la descripción • Establecer la dirección IPv4 (Utilizar la siguiente dirección disponible en la subred) • Establecer la dirección IPv6 (Consultar el diagrama de topología para conocer la información de direcciones) • Activar la interfaz	R2(config)# interface serial 0/0/0 R2(config)# description Conexion a R1 R2(config)# ip address 172.16.1.2 255.255.255.252 R2(config)# ipv6 address 2001:DB8:ACAD:1::2/64 R2(config)# no shutdown R2(config)# exit
Interfaz S0/0/1, para esto: • Establezca la descripción • Establecer la dirección IPv4 (Utilizar la primera dirección disponible en la subred) • Establecer la dirección IPv6 (Consultar el diagrama de topología para conocer la información de direcciones). • Establecer la frecuencia de reloj en 128000 • Activar la interfaz	R2(config)# interface serial 0/0/1 R2(config)# description Conexion a R3 R2(config)# ip address 172.16.2.2 255.255.255.252 R2(config)# ipv6 address 2001:DB8:ACAD:2::2/64 R2(config)# clock rate 128000 R2(config)# no shutdown R2(config)# exit
Interfaz G0/0 (simulación de Internet), para esto: • Establezca la descripción • Establecer la dirección IPv4 (Utilizar la primera dirección disponible en la subred) • Establecer la dirección IPv6 (Utilizar la primera dirección disponible en la subred) • Activar la interfaz	R2(config)# interface gigabitEthernet 0/0 R2(config)# description Conexion Servidor R2(config)# ip address 209.165.200.225 255.255.255.248 R2(config)# ipv6 address 2001:DB8:ACAD:A::25/64 R2(config)# no shutdown R2(config)# exit
Interfaz loopback 0 (servidor web simulado), para esto: • Establezca la descripción. • Establecer la dirección IPv4	R2(config)# interface loopback 0 R2(config)# description Conexion Servidor Web simulado R2(config)# ip address 10.10.10.10 255.255.255.255 R2(config)# exit
Ruta predeterminada, para esto:	R2(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1

• Configure la ruta IPv4 predeterminada de G0/0. • Configure la ruta IPv6 predeterminada de G0/0.	R2(config)# ipv6 route ::/0 2001:DB8:ACAD:1::1 R2(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.1 R2(config)# ipv6 route ::/0 2001:DB8:ACAD:2::1 R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.238 R2(config)# ipv6 route ::/0 2001:BD8:ACAD:A::38 R2(config)# exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Configurar R3.

Esta configuración está compuesta por los parámetros básicos que deben llevar todos los dispositivos como desactivar la búsqueda DNS, nombre, contraseña de exec, de acceso a la consola, de acceso a Telnet, mensaje de advertencia y su vez se establecen las direcciones IPv4 e IPv6 para la interfaz S0/0/1, loopback 4,5,6,7. Las direcciones se establecen según correspondan.

Tabla 16 Configuración R3.

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Router>enable Router#configure terminal 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)# 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 #El acceso no autorizado está prohibido#
Interfaz S0/0/1, para esto: • Establezca la descripción • Establecer la dirección IPv4 (Utilizar la siguiente dirección disponible en la subred) • Establecer la dirección IPv6 (Consultar el diagrama de topología para conocer la información de direcciones) • Activar la interfaz	R3(config)# interface serial 0/0/1 R3(config)# description Conexion a R2 R3(config)# ip address 172.16.2.1 255.255.255.252 R3(config)# ipv6 address 2001:DB8:ACAD:2::1/64 R3(config)# no shutdown

Interfaz loopback 4, para esto:
• Establecer la dirección IPv4 (Utilizar la primera dirección disponible en la subred)
	R3(config)#interface loopback 4
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 4)
	R3(config)# ip address 192.168.4.1 255.255.255.0
	R3(config)# exit

Interfaz loopback 5, para esto:
• Establecer la dirección IPv4 (Utilizar la primera dirección disponible en la subred)
	R3(config)# interface loopback 5
	R3(config)# description Interfaz virtual (para pruebas, en este caso el 5)
	R3(config)# ip address 192.168.5.1 255.255.255.0
	R3(config)#exit

Interfaz loopback 6, para esto:
• Establecer la dirección IPv4 (Utilizar la primera dirección disponible en la subred)
	R3(config)#interface loopback 6
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 6)
	R3(config)#ip address 192.168.6.1 255.255.255.0
	R3(config)#exit

Interfaz loopback 7, para esto:
• Establecer la dirección IPv6 (Consultar el diagrama de topología para conocer la información de direcciones)
	R3(config)#interface loopback 7
	R3(config)#description Interfaz virtual (para pruebas, en este caso el 7)
	R3(config)#ipv6 address 2001:db8:acad:3::1/64
	R3(config)#exit

Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)#ipv6 route ::/0 2001:DB8:ACAD:2::2 R3(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 5: Configurar S1.

Se configuran los parámetros básicos como desactivar la búsqueda DNS, nombre, contraseña de exec, de acceso a la consola, de acceso a Telnet, cifrada de contraseñas y el mensaje de advertencia, es importante tener en cuenta cómo funciona el comando login, este configura el Switch para que requiera autenticación al iniciar sesión.

Cuando se habilita el inicio de sesión y se establece una contraseña, se solicita al usuario de la consola que introduzca una contraseña antes de darle acceso a la CLI.

Tabla 17 Configuración S1.

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Switch#configure terminal Switch(config)#no ip
Nombre del switch “S1”	switch(config)#hostname S1 S1(config)#exit
Contraseña de exec privilegiado cifrada “class”	S1(config)# enable secret class
Contraseña de acceso a la consola “cisco”	S1(config)# line console 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# exit
Contraseña de acceso Telnet “cisco”	S1(config)#line vty 0 4 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 #El acceso no autorizado está prohibido#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 6: Configurar S3.

En este paso, se repiten las mismas tareas que se configuraron previamente en S1.

Tabla 18 Configuración S3.

Tarea	Comando de IOS
Desactivar la búsqueda DNS	Switch#configure terminal Switch(config)#no ip domain-lookup Switch(config)#exit
Nombre del switch “S3”	switch(config)#hostname S3
Contraseña de exec privilegiado cifrada • class	S3(config)# enable secret class
Contraseña de acceso a la consola • cisco	S3(config)# line console 0 S3(config-line)# password cisco S3(config-line)# login
Contraseña de acceso Telnet • cisco	S3(config)#line vty 0 4 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 #El acceso no autorizado está prohibido#

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 7: Verificar la conectividad de la red.

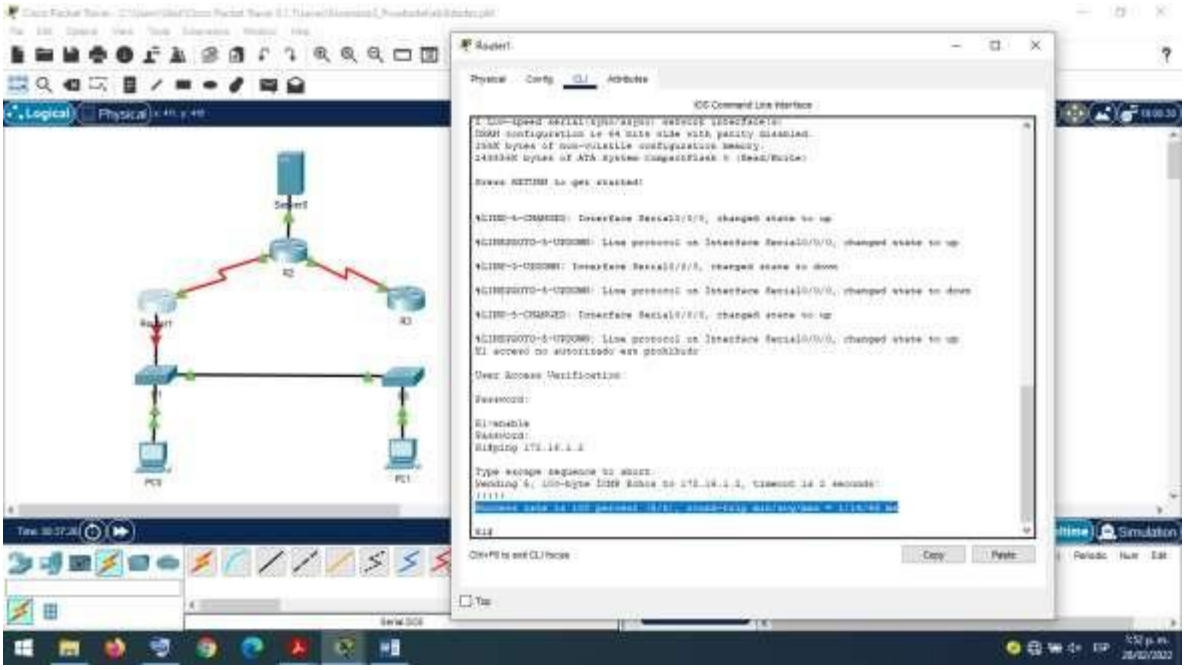
La verificación de conectividad se realiza desde un equipo a otro, para ello se abre la consola de comandos y se escribe el comando ping seguido de la dirección IP del host, que se encuentra en la tabla 19.

Tabla 19 Verificación de conectividad para Router y PC.

Desde	A	Dirección IP	Resultados de PING
R1	R2, S0/0/0	172.16.1.2	Exitoso (Figura 21)
R2	R3, S0/0/1	172.16.2.1	Exitoso (Figura 22)
PC de Internet	Gateway predeterminado	209.165.200.225	Exitoso (Figura 23)

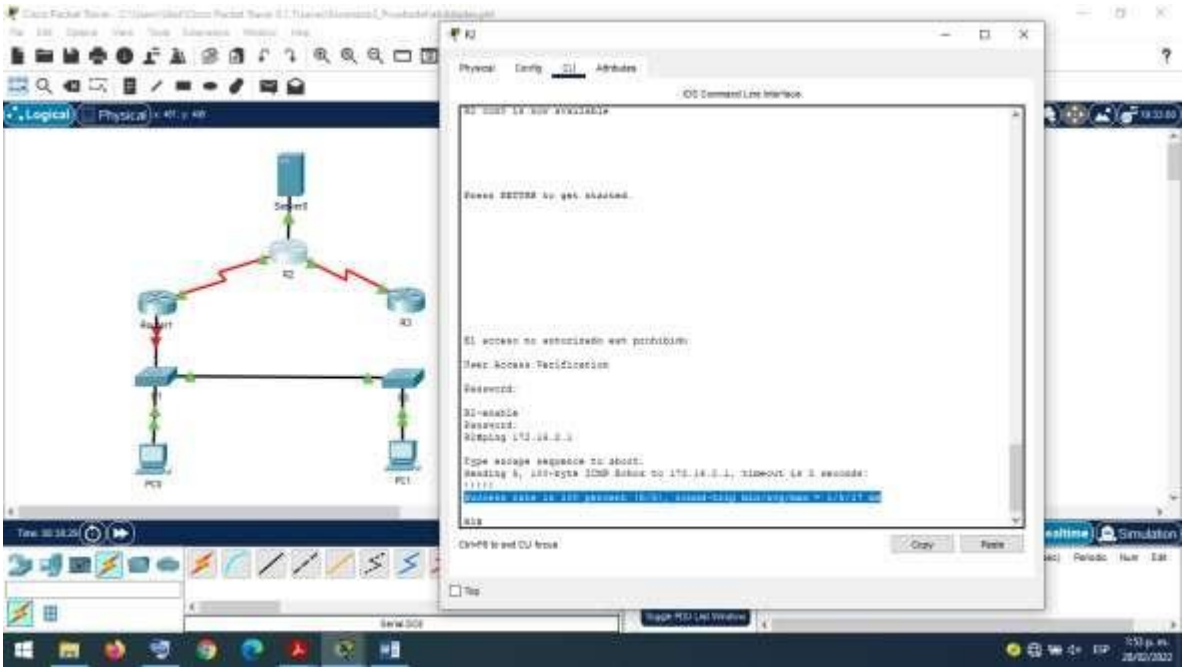
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 22 Prueba de conectividad desde R1 a R2



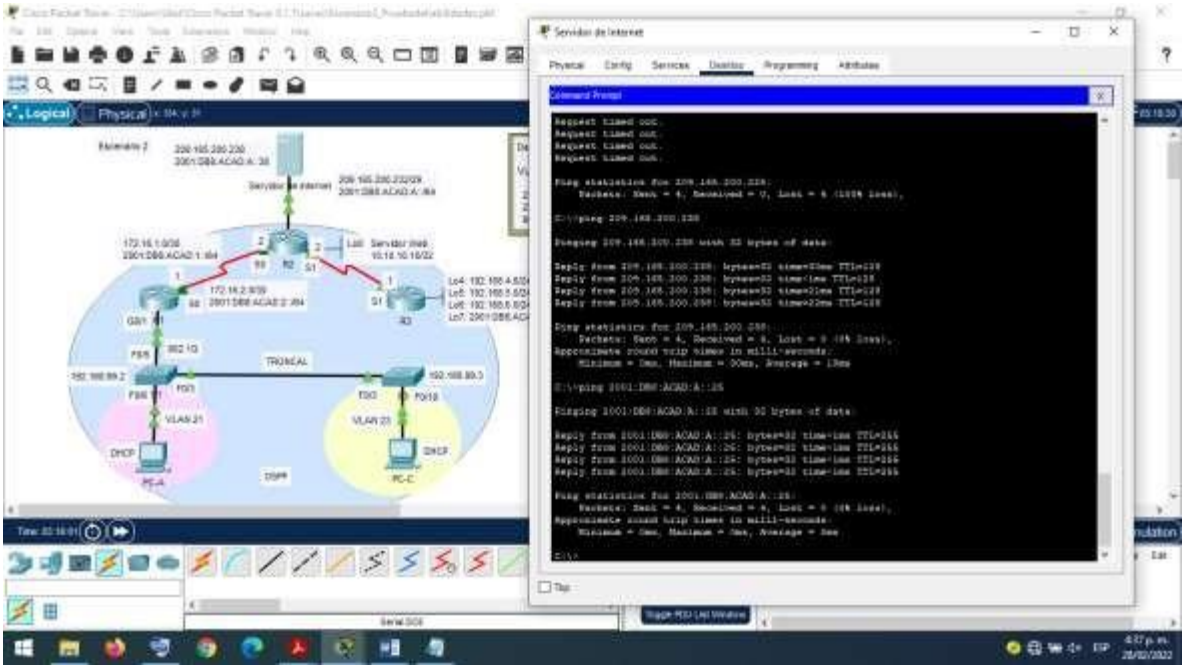
Fuente: Propia

Figura 23 Prueba de conectividad desde R2 a R3



Fuente: Propia

Figura 24 Prueba de conectividad desde el PC de internet al Gateway



Fuente: Propia

2.2.3 Parte 3: Configurar la seguridad del Switch, las VLAN y el routing entre VLAN.

En esta parte se crean las VLAN, donde estas son redes de área local virtual, al configurar el enlace troncal o trunk, este permitirá que se conecte S1 con S3 y llevar las VLANs que se configuran de una vez forma segura.

Paso 1: Configurar S1.

Iniciamos creando las VLAN, luego se le asigna la dirección IPv4 a la VLAN 99 que es la de administración con una puerta de enlace, para así forzar el enlace troncal en las interfaces F0/3 y F0/5, seguidamente se configuran el resto de los puertos como puertos de acceso, se asigna a la interfaz F0/6 la VLAN 21 y al final se apagan los puertos sin usar.

Tabla 20 Configuración Switch S1.

Tarea	Comando de IOS
Crear la base de datos de VLAN, hay que:	S1#config terminal S1(config)#vlan 21

• Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican	S1(config)#name Contabilidad S1(config)#vlan 23 S1(config)#name Ingenieria S1(config)#vlan 99 S1(config)#name Administracion S1(config)#exit
Asignar la dirección IP de administración, para esto hay que: • 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)#ip address 192.168.99.2 255.255.255.0 S1(config)#exit
Asignar el Gateway predeterminado, para esto hay que: • 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 fastEthernet 0/3 S1(config)#switchport mode trunk S1(config)#switchport trunk native vlan 1 S1(config)#exit
Forzar el enlace troncal en la interfaz F0/5 • Utilizar la red VLAN 1 como VLAN nativa	S1(config)#interface fastEthernet 0/5 S1(config)#switchport mode trunk S1(config)#switchport trunk native vlan 1 S1(config)#exit
Configurar el resto de los puertos como puertos de acceso • Utilizar el comando interface range	S1(config)#interface range fastEthernet 0/1-2, f0/4, f0/6-24, g0/1-2 S1(config)#switchport mode access S1(config)#exit
Asignar F0/6 a la VLAN 21	S1(config)#interface fastEthernet 0/6 S1(config)#switchport access vlan 21 S1(config)#exit
Apagar todos los puertos sin usar	S1(config)#interface range fastEthernet 0/1-2, f0/4, f0/7-24, g0/1-2 S1(config)#shutdown S1(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar S3.

En este paso, se repiten las mismas tareas que se configuraron previamente en S1.

Tabla 21 Configuración Switch S3.

Tarea	Comando de IOS
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	S3(config)#vlan 21 S3(config)#name Contabilidad S3(config)#vlan 23 S3(config)#name Ingenieria S3(config)#vlan 99 S3(config)#name Administracion S3(config)#exit
Asignar la dirección IP de administración, para esto hay que: • 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)#ip address 192.168.99.3 255.255.255.0
Asignar el Gateway predeterminado, para esto hay que: • Asigne la primera dirección IPv4 de la subred como el Gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3, para esto hay que: • Utilizar la red VLAN 1 como VLAN nativa	S3(config)#interface fastEthernet 0/3 S3(config)#switchport mode trunk S3(config)#switchport trunk native vlan 1 S1(config)#exit
Configurar el resto de los puertos como puertos de acceso, para ello hay que: • Utilizar el comando interface range	S3(config)#interface range fastEthernet 0/1- 2, f0/4-24, g0/1-2 S3(config)#switchport mode access
Asignar F0/18 a la VLAN 23	S3(config)#interface fastEthernet 0/18 S3(config)#switchport access vlan 23
Apagar todos los puertos sin usar	S3(config)#interface range fastEthernet 0/1-2, f0/4-17, f0/19-24, g0/1-2 S3(config)#shutdown S3(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas.

Paso 3: Configurar R1.

Este paso se utiliza el protocolo IEEE 802.1Q que permite a la red compartir el mismo medio físico sin interferencia, además en este paso ahora si se activa la interfaz G0/1.

Tabla 22 Configuración Router R1.

Tarea	Comando de IOS
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 gigabitEthernet 0/1.21 R1(config)#encapsulation dot1Q 21 R1(config)#ip address 192.168.21.1 255.255.255.0 R1(config)#description LAN de contabilidad VLAN 21 R1(config)#no shutdown R1(config)#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 gigabitEthernet 0/1.23 R1(config)#encapsulation dot1Q 23 R1(config)#ip address 192.168.23.1 255.255.255.0 R1(config)#description LAN de Ingenieria VLAN 23 R1(config)#no shutdown R1(config)#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 gigabitEthernet 0/1.99 R1(config)#encapsulation dot1Q 99 R1(config)#ip address 192.168.99.1 255.255.255.0 R1(config)#description LAN de Administracion VLAN 99 R1(config)#no shutdown R1(config)#exit
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config)#no shutdown R1(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Verificar la conectividad de la red.

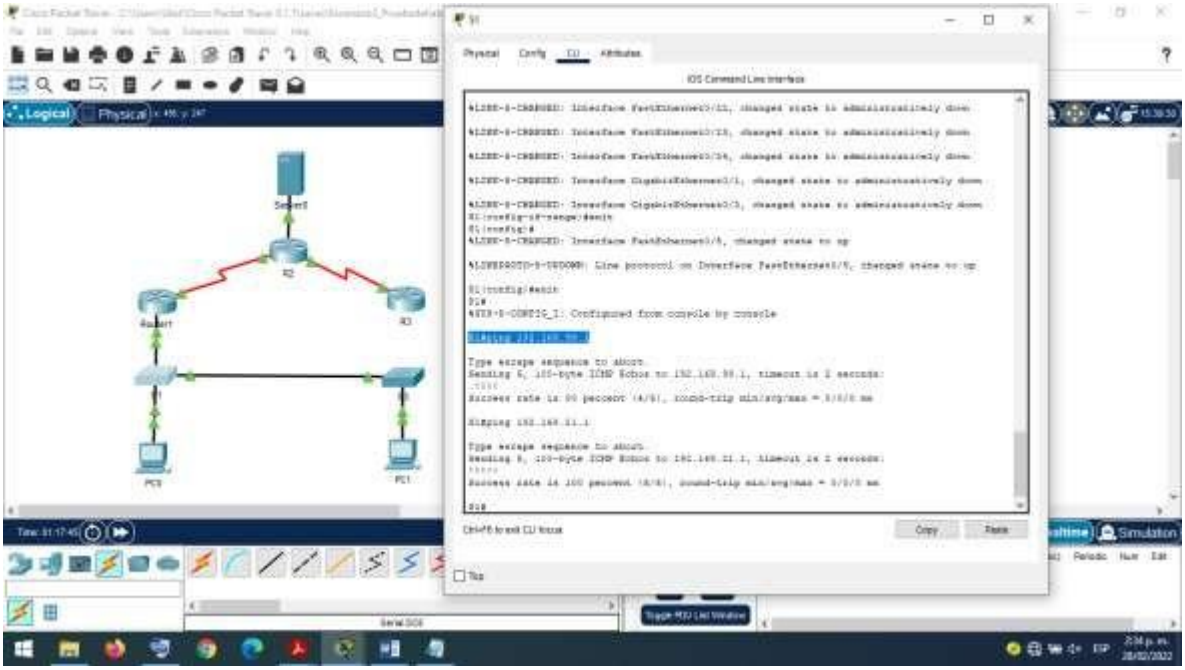
A medida que se avanza en la configuración es importante ir haciendo verificaciones de conectividad, esta se realiza desde un equipo a otro, para ello se abre la consola de comandos y se escribe el comando ping seguido de la dirección IP del host.

Tabla 23 Prueba de conectividad de red

Desde	A	Dirección IP	Resultados de PING
S1	R1, dirección de VLAN 99	192.168.99.1	Exitoso (Figura 25)
S3	R1, dirección de VLAN 99	192.168.99.1	Exitoso (Figura 25)
S1	R1, dirección de VLAN 21	192.168.21.1	Exitoso (Figura 26)
S3	R1, dirección de VLAN 23	192.168.23.1	Exitoso (Figura 25)

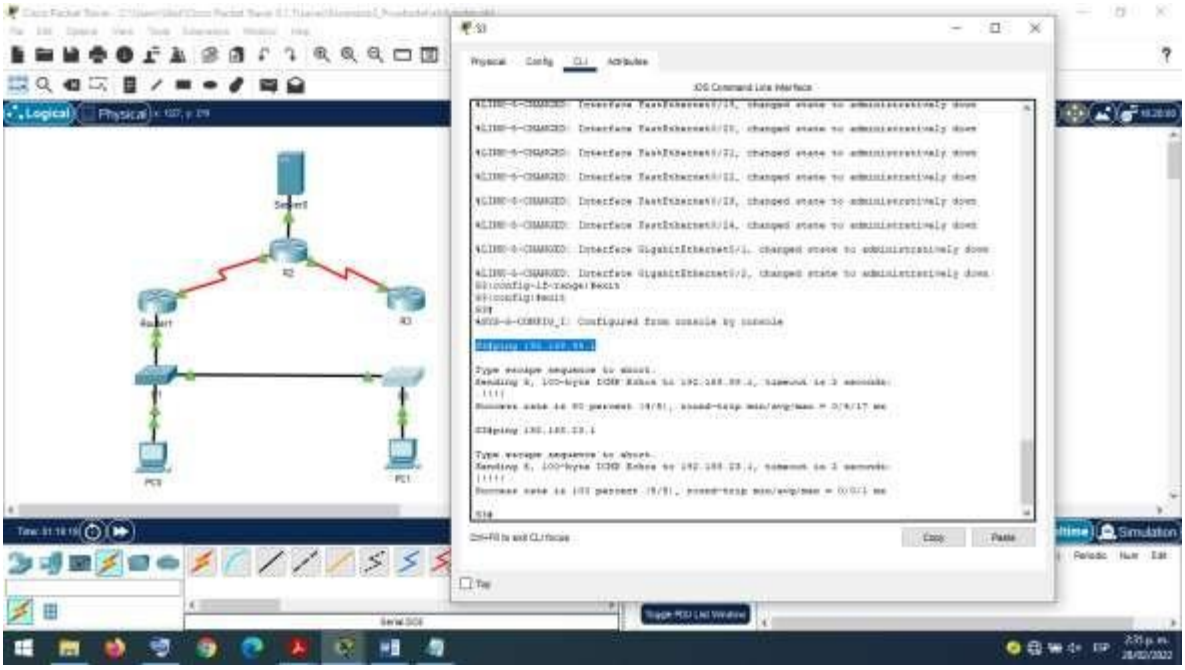
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 27 Prueba de conectividad desde S1 a la VLAN 99 y 21



Fuente: Propia

Figura 28 Prueba de conectividad desde S3 a la VLAN 99 y 23



Fuente: Propia

Paso 5: Habilitar el envío de tráfico IPv6 en R1, R2 y R3.

En este paso para activar el trafico IPv6 que esta deshabilitado, se utiliza el comando ipv6-unicast-routing.

Tabla 24 Habilitación tráfico IPv6 en R1, R2 y R3.

Tarea	Comando de IOS
• Habilitar el routing de unidifusión IPv6 en R1, R2 y R3. • (El comando de configuración global ipv6 unicast-routing debe configurarse para que habilite al router el reenvío de paquetes IPv6) • (Permite enrutar paquetes IPv6 entre las distintas interfaces del router)	R1(config)#ipv6 unicast-routing R2(config)#ipv6 unicast-routing R3(config)#ipv6 unicast-routing

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

2.2.4 Parte 4: Configurar el protocolo de routing dinámico OSPF.

Esta parte involucra el protocolo OSPF, este es un protocolo de direccionamiento de tipo enlace-estado que calculara la ruta más corta para enviar la información de allí su importancia.

Paso 1: Configurar OSPF en el R1.

Primero se anuncia el protocolo por medio del comando router ospf, configurado en área 0, seguidamente se anuncian las redes que estarán conectadas directamente a R1 por medio del comando network la dirección IP y el área, inmediatamente se establecerán la interfaces loopback como pasivas con el comando passive-interface seguido del nombre de la interfaz, al final se desactiva la somatización automática por medio del comando no auto-summary.

Tabla 25 Configuración protocolo de enrutamiento OSPF en el R1.

Tarea	Comando de IOS
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config)#router-id 1.1.1.1
Anunciar las redes conectadas directamente • Asigne todas las redes conectadas directamente.	R1(config)#network 172.16.1.0 0.0.0.3 area 0 R1(config)#network 192.168.21.0 0.0.0.255 area 0 R1(config)#network 192.168.23.0 0.0.0.255 area 0 R1(config)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config)#passive-interface gigabitEthernet 0/1.21 R1(config)#passive-interface gigabitEthernet 0/1.23 R1(config)#passive-interface gigabitEthernet 0/1.99 R1(config)#exit
Desactive la sumarización automática	R1(config)#router ospf 1 R1(config-router)#no auto-summary R1(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 2: Configurar OSPF en el R2.

En este paso, se repiten las mismas tareas que se configuraron previamente en R1, excepto que la red G0/0 no se anunciara y solo la interface loopback 0 se establecerá como pasiva.

Tabla 26 Configuración protocolo de enrutamiento OSPF en el R2.

Tarea	Comando de IOS
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config)#router-id 2.2.2.2
Anunciar las redes conectadas directamente Nota: Omitir la red G0/0.	R2(config)#network 10.10.10.10 0.0.0.0 area 0 R2(config)#network 172.16.1.0 0.0.0.3 area 0 R2(config)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#passive-interface loopback 0 R2(config)#exit
Desactive la sumarización automática	R2(config)#router ospf 1 R2(config-router)#no auto-summary

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar OSPFv3 en el R2.

En este paso, se repiten las mismas tareas que se configuraron previamente en los Routers anteriores.

Tabla 27 Configuración protocolo de enrutamiento OSPFv3 en el R2.

Tarea	Comando de IOS
Configurar OSPF área 0	R2(config)#router ospf 1 R2(config)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	R2(config-router)#network 172.16.1.0 0.0.0.255 area 0 R2(config-router)#network 172.16.2.0 0.0.0.255 area 0 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#network 192.168.4.0 0.0.0.255 area 0

	R2(config-router)#network 192.168.5.0 0.0.0.255 area 0 R2(config-router)#network 192.168.6.0 0.0.0.255 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface lo4 R2(config-router)#passive-interface lo5 R2(config-router)#passive-interface lo6
Desactive la sumarización automática.	R2(config-router)#no auto-summary

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Configurar OSPFv3 en el R3

En este paso, se repiten las mismas tareas que se configuraron previamente en los Routers anteriores.

Tabla 28 Configuración OSPF en el R3

Tarea	Comando de IOS
Configurar OSPF area 0	R3(config)#router ospf 1 R3(config)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.2.0 0.0.0.255 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 R3(config-router)#passive-interface lo7
Desactive la sumarización automática.	R3(config-router)#no auto-summary

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 4: Verificar la información de OSPF.

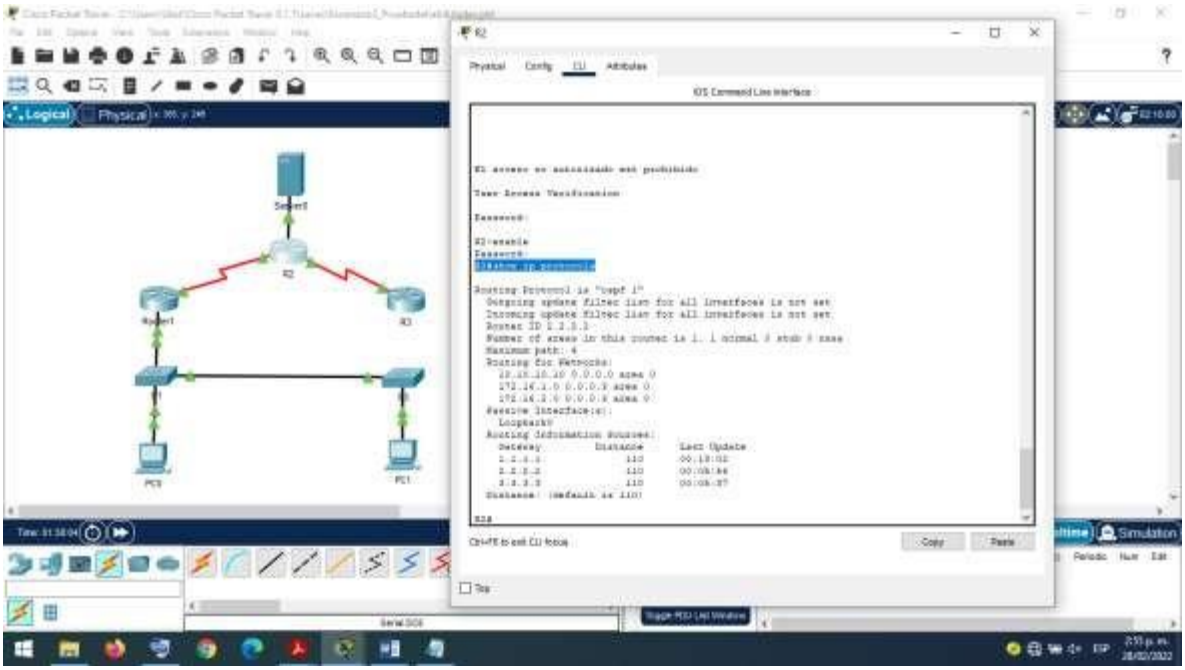
Esta verificación de configuración del protocolo OSPF se realiza en la ventana CLI colocando el comando adecuado.

Tabla 29 Verificación información 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?	R1#Show ip protocols R2#Show ip protocols R3#Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#Show ip route ospf R2#Show ip route ospf R3#Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#Show running-config | section router ospf R2# Show running-config | section router ospf R3# Show running-config | section router ospf

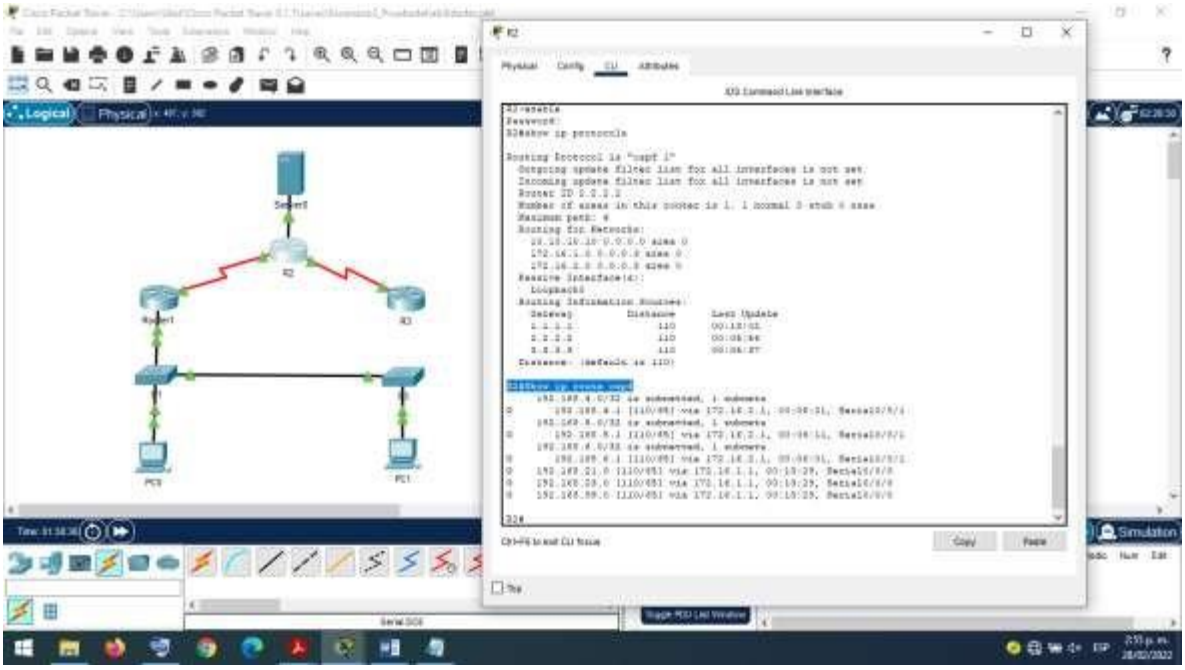
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 29 Uso del comando que muestra la ID del protocolo OSPF en R2



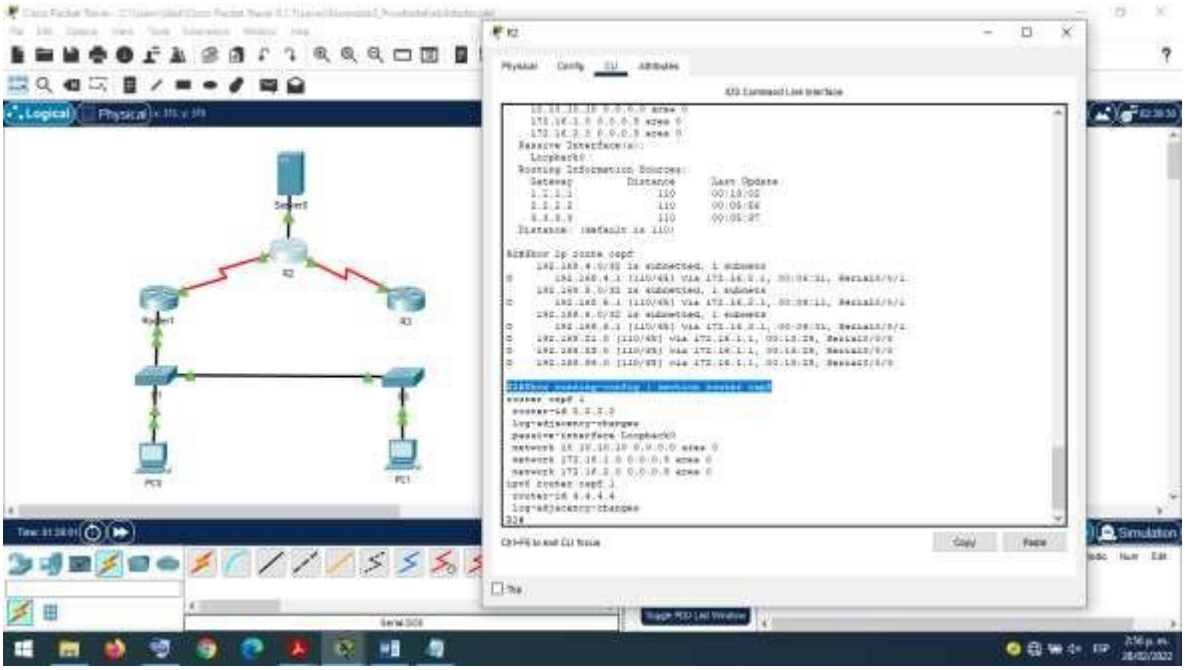
Fuente: Propia

Figura 30 Uso del comando que muestra solo las rutas OSPF en R2



Fuente: Propia

Figura 31 Uso del comando que muestra la configuración OSPF en R2



Fuente: Propia

2.2.5 Parte 5: Implementar DHCP y NAT para IPv4.

Para esta parte se utiliza el protocolo de configuración dinámica de host (también conocido por sus siglas de DHCP), este asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo de forma automática, también se utiliza el protocolo NAT que es la traducción de direcciones de red que utilizaran los Routers para cambiar información entre las dos red a las cuales se les asigno direcciones diferentes.

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

Se reservan las primeras 20 direcciones para la VLAN 21, las siguientes para la VLAN 23 y asi mismo se establece un rango de IP's excluidas del conjunto pool de direcciones.

Tabla 30 Configuración e implementación DHCP y NAT para IPv4.

Tarea	Comando de IOS
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21. • Nombre: ACCT • Servidor DNS: 10.10.10.10 • Nombre de dominio: ccna-sa.com • Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(config)#network 192.168.21.0 255.255.255.0 R1(config)#default-router 192.168.21.1 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#exit
Crear un pool de DHCP para la VLAN 23. • Nombre: ENGNR • Servidor DNS: 10.10.10.10 • Nombre de dominio: ccna-sa.com • Establecer el gateway predeterminado	R1(config)#ip dhcp pool ENGNR R1(config)#network 192.168.23.0 255.255.255.0 R1(config)#default-router 192.168.23.1 R1(config)#dns-server 10.10.10.10 R1(config)#domain-name ccna-sa.com R1(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

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

Primero se crea una base de datos local con la cuenta de usuario que nos dan, luego se crea una NAT estática al servidor web, se asigna la interfaz interna y externa para la NAT estática, para así luego configurar la NAT dinámica dentro de una ACL privada, donde esta NAT dinámica es una única dirección interna que se traduce a una única dirección externa por ello al final se define esta.

Tabla 31 Configuración de NAT estática y dinámica en el R2.

Tarea	Comando de IOS
Crear una base de datos local con una cuenta de usuario. • Nombre de usuario: webuser • Contraseña: cisco12345 • Nivel de privilegio: 15	R2(config)#username webuser privilege 15 R2(config)#password cisco12345
Habilitar el servicio del servidor HTTP	No aplica (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2 (config)#ip http server ^ % Invalid input detected at '^' marker. R2(config)#exit
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	No aplica (El escenario simulado en Packet Tracer no permite la inserción del protocolo HTTP). R2(config)#ip http authentication local ^ % Invalid input detected at '^' marker. R2(config)#exit
Crear una NAT estática al servidor web. • Dirección global interna: 209.165.200.229	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 R2(config)#exit
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface gigabitEthernet 0/0 R2(config)#ip nat outside R2(config)#exit R2(config)#interface loopback 0 R2(config)#ip nat inside R2(config)#exit

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 • Permitir la traducción de un resumen de las redes LAN • (loopback) en el R3	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 R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255 R2(config)#exit
Defina el pool de direcciones IP públicas utilizables. • Nombre del conjunto: INTERNET • El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#exit

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Paso 3: Verificar el protocolo DHCP y la NAT estática.

Esta verificación de configuración del protocolo DHCP se realiza en la ventana Desktop seguida de la pestaña IP configuration de cada equipo de cómputo, se selecciona la opción DHCP y si quedo bien configurado saldrá el mensaje DHCP request successful.

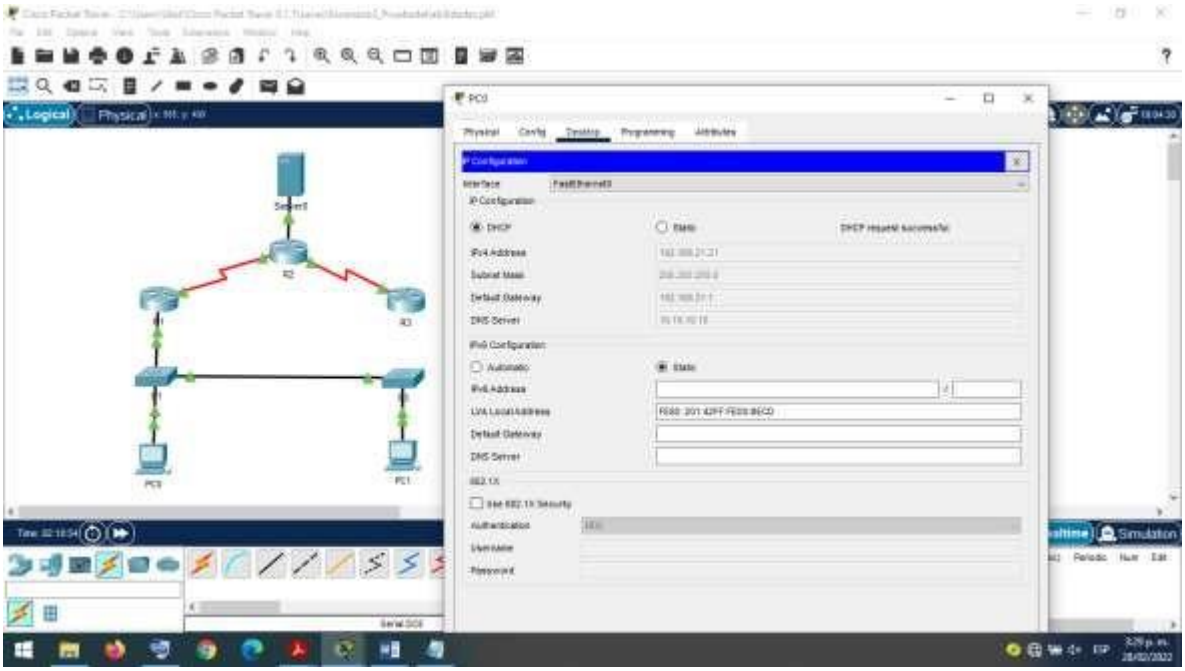
Tabla 32 Verificación de protocolo DHCP y NAT estática.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso (Figura 29)
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Exitoso (Figura 30)
Verificar que la PC-A pueda hacer ping a la PC-C	Exitoso (Figura 31)

Nota: Quizá sea necesario deshabilitar el firewall de la PC.	
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	Para este caso, al insertar la IP 209.165.200.229 no tiene acceso ya que en el ambiente de simulación el router no permite la habilitación del protocolo HTTP. Sin embargo, se aplica en el navegador la IP configurada en el servidor que es: 209.165.200.238 y se visualiza la información configurada en el archivo index.html del servidor. (Figura 32)

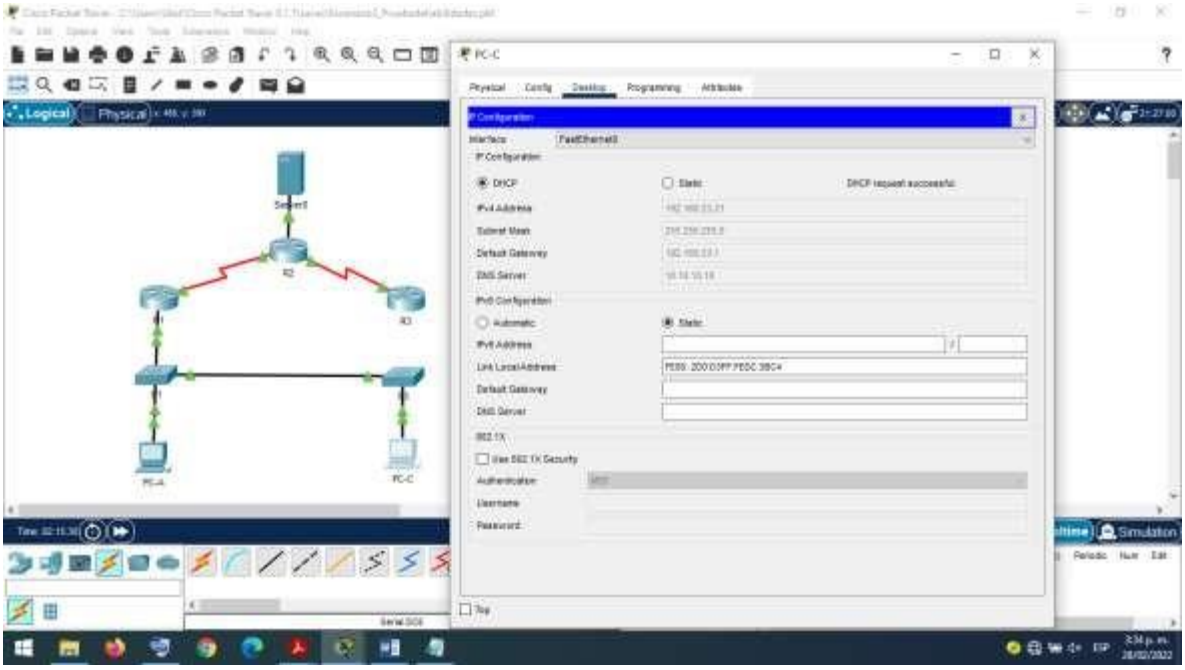
Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 32 Verificación de DHCP en PC-A.



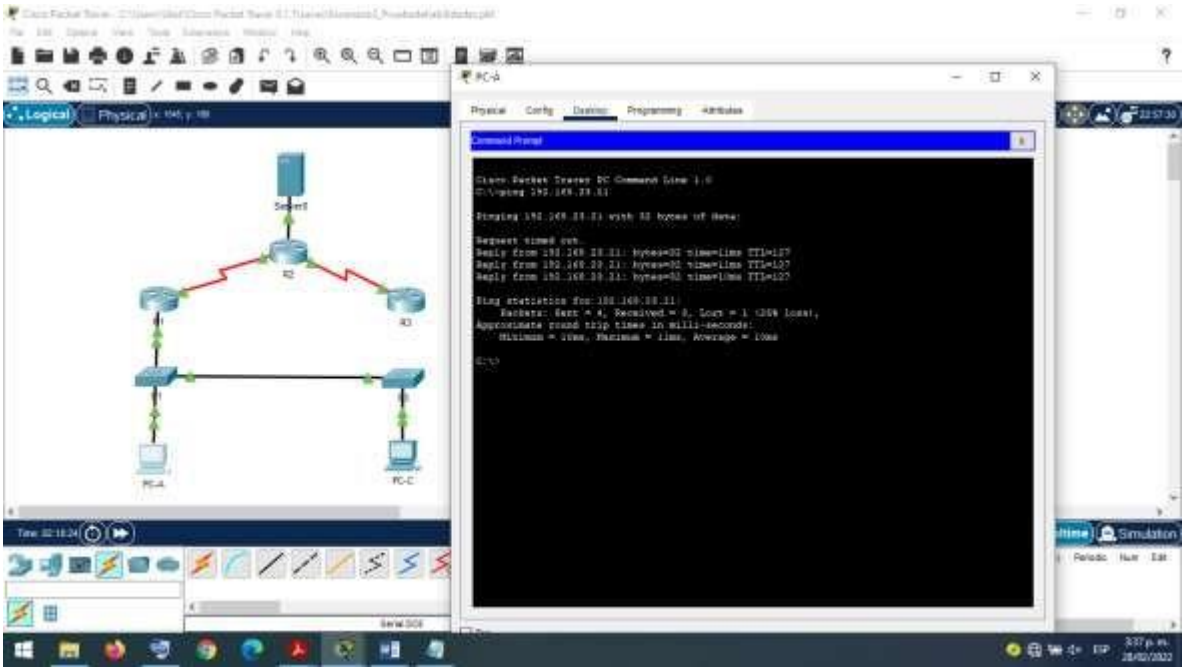
Fuente: Propia

Figura 33 Verificación de DHCP en PC-C



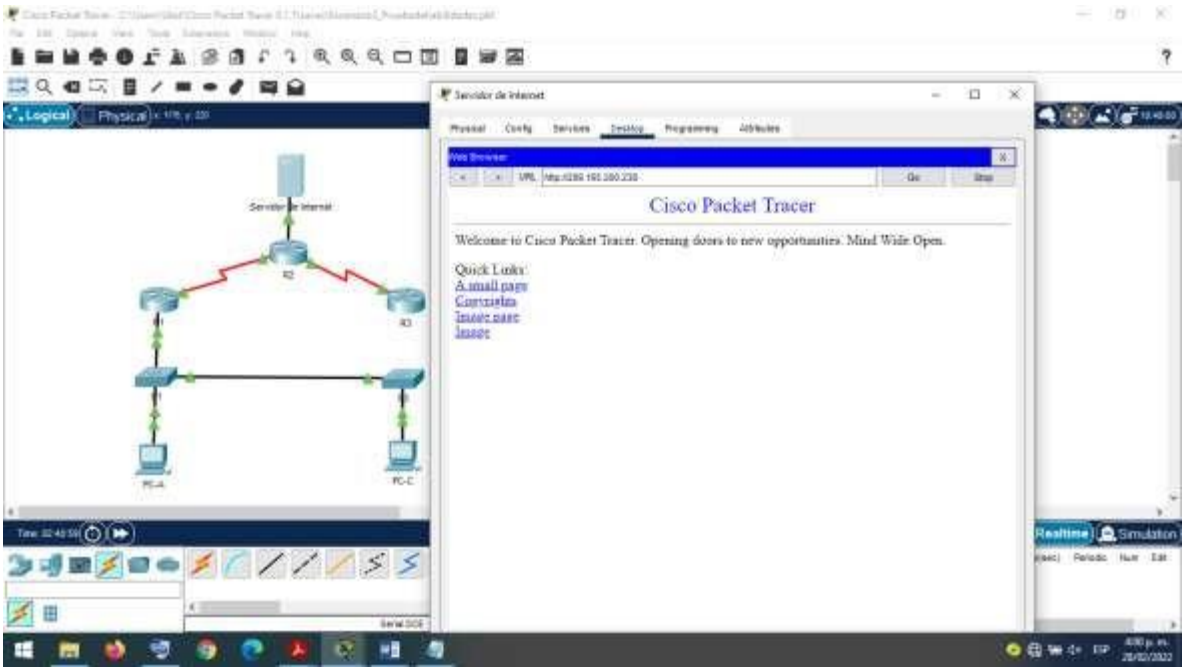
Fuente: Propia

Figura 34 Verificación de conexión entre PC-A y PC-C



Fuente: Propia

Figura 35 Verificación de acceso al Servidor web



Fuente: Propia

2.2.6 Parte 6: Configurar NTP.

En esta parte se configura el protocolo NTP (Network Time Protocol), la función principal de este es sincronizar el reloj de un sistema, para ello primero se ajusta la fecha en el Router R2 y al mismo tiempo se configura como maestro NTP y R1 como cliente.

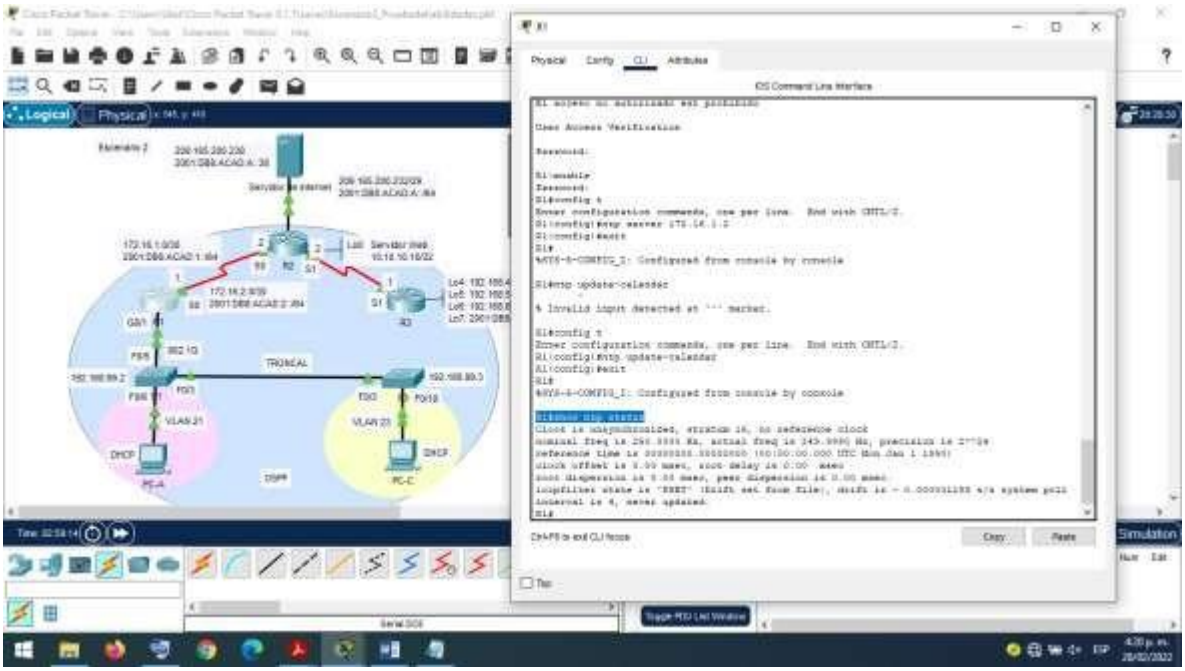
Tabla 33 Configuración NTP.

Tarea	Comando de IOS
Ajuste la fecha y hora en R2 • 5 de marzo de 2016, 9 a. m.	R2#clock set 09:00:00 05 March 2016
Configure R2 como un maestro NTP. • Nivel de estrato: 5	R2(config)#ntp master 5
Configure 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 • Se aplica el comando show ntp status en R1 y R2.	R1#show ntp status R2#show ntp status

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 36 Verificación de la configuración NTP en R1



Fuente: Propia

2.2.7 Parte 7: Configurar y verificar las listas de control de acceso (ACL).

El objetivo de configurar las ACL es filtrar el tráfico de la lisa de redes y acciones proporcionando mayor seguridad al acceder a la red.

Paso 1: Restringir el acceso a las líneas VTY en R2.

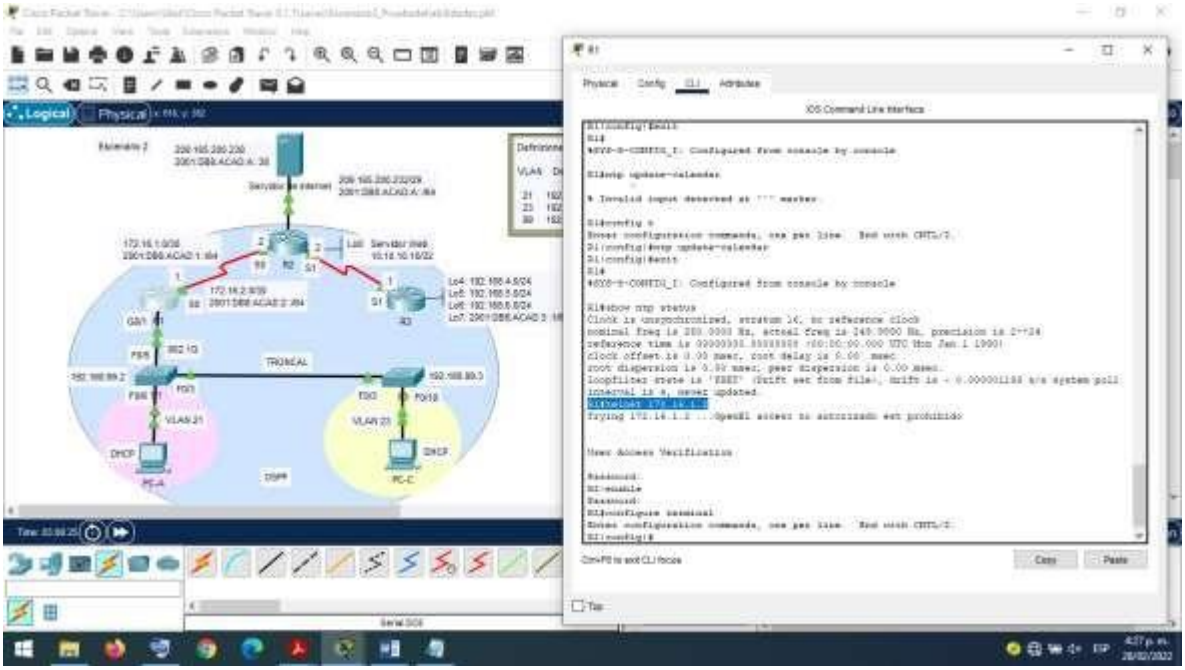
En este paso se configura una ACL, para ello se le asigna nombre para que solo R1 establezca una conexión Telnet con R2. Y esto se realiza por medio de las líneas VTY.

Tabla 34 Restricción de acceso a las líneas VTY en R2.

Tarea	Comando de IOS
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)#permit host 172.16.1.1
Aplicar la ACL con nombre a las líneas VTY	R2(config)#line vty 0 4 R2(config)#access-class ADMIN-MGT in R2(config)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config)#transport input telnet R2(config)#exit
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 (Figura 34)

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 37 Verificación de la ACL



Fuente: Propia

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

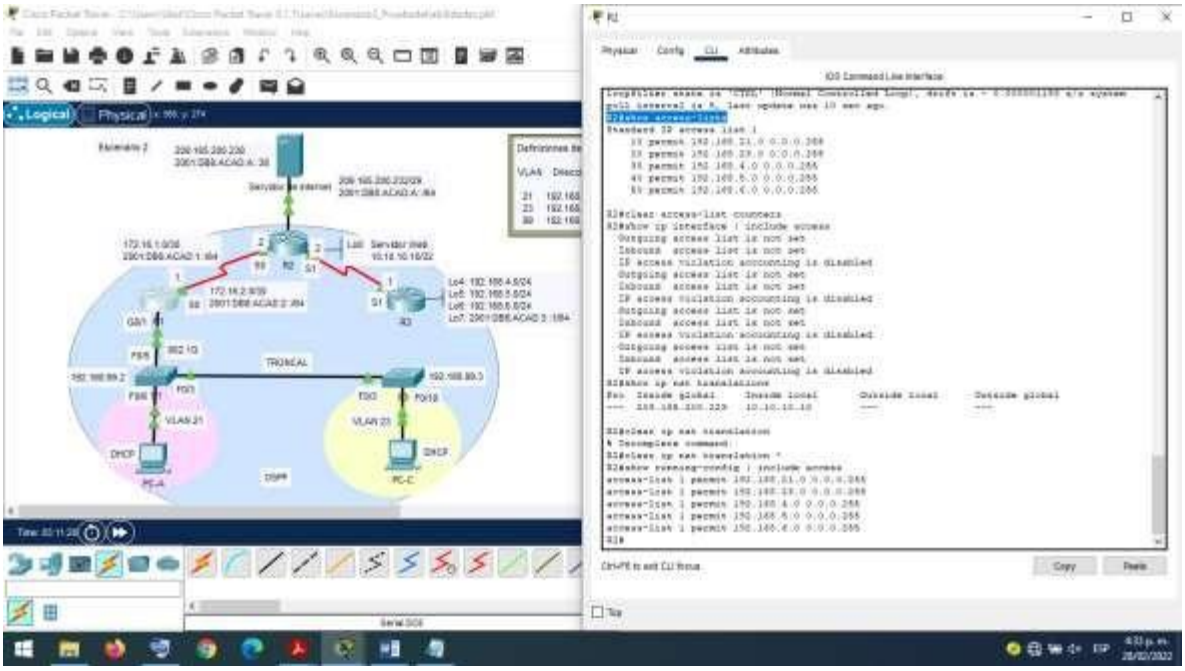
Los comandos que están en la tabla, se colocan en el modo de administrador de la ventana CLI y estos permiten ver o cambiar la configuración del router. Para acceder a este modo desde el modo de usuario hay que ejecutar el comando enable y luego si el comando que sea adecuado.

Tabla 35 Líneas de comando aplicadas a listas de acceso.

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists (Figura 35)
Restablecer los contadores de una lista de acceso	R2#clear access-list counters (Figura 35)
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface | include Access R2#show running-config | include Access (Figura 35)
¿Con qué comando se muestran las traducciones NAT? • 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.	R2#show ip nat translations (Figura 35)
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation * (Figura 35)

Fuente: Propia, tomando como referencia la Guía Prueba de habilidades prácticas CCNA.

Figura 38 Líneas de comando aplicadas a listas de acceso



Fuente: Propia

CONCLUSIONES

La consolidación de este trabajo consistió en organizar la adquisición de conocimientos, habilidades y destrezas en el diseño e implementación de redes informáticas que permiten el procesamiento, interoperabilidad, acceso seguro, control y gestión de la información en las redes de telecomunicaciones a través de los distintos protocolos de enrutamiento utilizados.

El proceso de configuración de los dispositivos en un principio parece ser algo demasiado difícil pero una vez, tenemos claro cómo funciona la sintaxis de cada comando se vuelve más fácil de comprender y configurar e integrar de manera correcta una red.

Se configuraron y crearon VLAN logrando observar y verificar cómo funcionan, se creó además un enlace troncal entre los Switches para permitir que los PC’s se comuniquen entre sí, esto a su vez posibilita la función de transferir el tráfico de varias VLAN a través de un único enlace y conservar intactas la segmentación y la identificación de VLAN.

Luego de realizar las respectivas configuraciones para activar el protocolo DHCP para direccionamiento IPv4 e IPv6, se concluye que es indicado para la administración de direcciones por su facilidad. Por otra parte, fue indispensable manejar los fundamentos principales de los protocolos que existen actualmente para las redes, estos permiten acceder y/o transferir información a todos los dispositivos de forma segura y que admitan conectividad por cable o inalámbrica a una red desde casi cualquier lugar.

Verificar y detectar errores a tiempo es importante en una red. Es por eso que resulta fundamental tener en cuenta el uso de comandos como ipconfig, ipv6config, nslookup, Tracer, ping, show entre otros. Para ir examinando con detalle las configuraciones a medida que se van realizando.

En conclusión, podemos advertir que las redes de telecomunicaciones han aumentado considerablemente y que eso se debe a la expansión tecnológica que nos requiere a todos conectados. Es fundamental continuar por este camino actualizándonos y profundizando podemos tener mejores resultados.

REFERENCIAS

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

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. (2019). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

Vesga, J. (2017). Ping y Tracer como estrategia en los procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

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

CISCO. (2019). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

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

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

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2019). Routing Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#3

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

CISCO. (2019). VLAN. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. (2019). Listas de Control de Acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

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

CISCO. (2019). NAT para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

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

¿Qué es una búsqueda de DNS? (s. f.). Recuperado 1 de marzo de 2022, de https://www.netinbag.com/es/internet/what-is-a-dns-search.html

RSA. (s. f.). Recuperado 1 de marzo de 2022, de https://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/rsa.html

ACL: Lista de Control de Accesos. (s. f.). Recuperado 1 de marzo de 2022, de https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html

Protocolo DHCP: Qué es, funcionamiento y ejemplos para configurarlo. (s. f.). RedesZone. Recuperado 1 de marzo de 2022, de https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/

TODO SOBRE REDES: ETHERCHANNEL. (s. f.). TODO SOBRE REDES. Recuperado 1 de marzo de 2022, de http://todosobreredesdedatos.blogspot.com/p/etherchannel.html

2.2.2.3 Protección del acceso a EXEC del usuario. (s. f.). Recuperado 1 de marzo de 2022, de http://itroque.edu.mx/cisco/cisco1/course/module2/2.2.2.3/2.2.2.3.html

TODO SOBRE REDES: VTY. (s. f.). TODO SOBRE REDES. Recuperado 1 de marzo de 2022, de http://todosobreredesdedatos.blogspot.com/p/vty.html

Dynamic Trunking Protocol. (2020). En Wikipedia, la enciclopedia libre. https://es.wikipedia.org/w/index.php?title=Dynamic_Trunking_Protocol&oldid=131513222

OSPF Design Guide. (s. f.). Cisco. Recuperado 1 de marzo de 2022, de https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Qué es OSPF y Cómo Funciona OSPF. (2020, agosto 10). CCNA Desde Cero. https://ccnadesdecero.com/curso/ospf/

Protocolo de red NTP: Cómo funciona y para qué se utiliza en los equipos. (s. f.). RedesZone. Recuperado 1 de marzo de 2022, de https://www.redeszone.net/tutoriales/internet/que-es-protocolo-ntp/

Qué significa NAT y cómo actúa en la red. (s. f.). RedesZone. Recuperado 1 de marzo de 2022, de https://www.redeszone.net/tutoriales/redes-cable/que-es-nat-red/

Qué son las VLAN, para qué sirven y cómo funcionan con ejemplos de uso. (s. f.). RedesZone. Recuperado 1 de marzo de 2022, de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Redes e Internet – Todo lo que debes saber (s. f.). Profesional Review. Recuperado 1 de marzo de 2022, de https://www.profesionalreview.com/redes/

Comandos básicos para trabajar con Packet Tracer. (2015, julio 29). EL portafolio de las redes. https://elportafoliodelasredes.wordpress.com/2015/07/29/comandos-basicos-para-trabajar-con-packet-tracer/

ANEXO

VIDEO DE ACTIVDAD
https://drive.google.com/file/d/1fcsMNmvb8UNwDJWS4ItvoISlrgL-k6b-/view?usp=sharing