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

MIRYAM MARCELA QUIROGA PINILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SISTEMAS
GIRARDOT (CUND.)
2021

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

MIRYAM MARCELA QUIROGA PINILLA

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

DIRECTOR:

ING. NANCY AMPARO GUACA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERIA DE SISTEMAS
GIRARDOT (CUND.)
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

GIRARDOT, 28 de noviembre 2021

AGRADECIMIENTO

Hoy quiero agradecer en primer lugar a Dios por darme la oportunidad de llegar hasta esta etapa de mi vida, siendo mi guía, dándome sabiduría y fortaleza para continuar y terminar mis estudios profesiones con éxito acompañado de familiares y amigos.

Agradezco a mis padres y hermanos por ser mi guía, darme animo con sus palabras para continuar en el diario vivir, brindándome su apoyo y su amor incondicional. Agradezco a mi esposo por ser ese acompañante en este camino; que me motivo a continuar y brindarme su compañía y amor, así como a mi hija por ser ese motor de arranque y motivación diaria, enseñándome a ser mejor persona y permitirme dejarle un mejor legado que nunca es tarde para continuar y ser profesional.

A la Universidad Nacional Abierta y a Distancia UNAD por permitirme formarme en su institución y brindarme los conocimientos necesarios para crecer como persona y crecer profesionalmente. A todos mis tutores que me brindaron sus conocimiento, apoyo, asesoramiento y amistad en este largo camino, a cada uno de ellos muchas gracias.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

SWITCH: Es un dispositivo que sirve para conectar varios elementos dentro de una red. Estos pueden ser un PC, una impresora, una televisión, una consola o cualquier aparato que posea una tarjeta Ethernet o Wifi. Los switches se utilizan tanto en casa como en cualquier oficina donde es común tener al menos un switch por planta y permitir así la interconexión de diferentes equipos.

TOPOLOGÍA DE RED: Una topología de red es la disposición de una red, incluyendo sus nodos y líneas de conexión. Hay dos formas de definir la geometría de la red: la topología física y la topología lógica (o de señal) Vlan: Es un método para crear redes lógicas independientes dentro de una misma red física.

VLAN: Pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local

INTERFACES: Dispositivo capaz de transformar las señales generadas por un aparato en señales comprensibles por otro Passwords: es una palabra procedente del inglés que puede traducirse al español como 'palabra clave'. En este sentido, es sinónimo de contraseña o clave. Una password o contraseña es un método de autentificación que se utiliza para controlar el acceso a información, espacios o recursos.

ROUTER: Un rúter, enrutador, (del inglés router) o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red.

RESUMEN

Con el propósito de identificar los protocolos de enrutamiento vistos durante el diplomado de CCNA, se procede a realizar la respectiva configuración de los dos escenarios correspondientes a la actividad, en el cual se hará uso de simulador del programa cisco packet tracer para realizar el respectivo montaje del escenario correspondiente, se realizará la respectiva proyección de redes conmutadas mediante routers y switches. Los diferentes dispositivos electrónicos permitirán evidenciar los conceptos y temáticas aprendidas realizando la respectiva identificación de comando básicos para la adecuada configuración de los escenarios detallando el paso a paso de las etapas realizadas durante el proceso.

El diplomado en profundización CISCO, permite desarrollar las habilidades prácticas en un ambiente simulado, orientando el conocimiento al procedimiento de diferentes escenarios que permiten la posibilidad de crear, diagnosticar, configurar y dar solución a problemas de redes.

Los escenarios propuestos plantean la configuración de diversos dispositivos que permiten la estructuración de la red, desde la configuración básica, los procesos de encapsulamiento de seguridad vlsm a la información, la creación de las redes Vlan, redes locales y virtuales, los protocolos DHCP Y NAT, la configuración de direccionamiento IP dentro del direccionamiento establecido previamente, validando la conexión exitosa de las configuraciones realizadas.

Palabras Clave: CISCO, CCNA, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In order to identify the routing protocols seen during the CCNA diploma, we proceed to perform the respective configuration of the two scenarios corresponding to the activity, in which the simulator of the cisco packet tracer program will be used to perform the respective assembly of the corresponding scenario, the respective projection of switched networks will be carried out through routers and switches. The different electronic devices will allow to evidence the concepts and themes learned by making the respective identification of basic command for the adequate configuration of the scenarios detailing the step by step of the stages carried out during the process.

The CISCO deepening diploma allows you to develop practical skills in a simulated environment, orienting knowledge to the procedure of different scenarios that allow the possibility of creating, diagnosing, configuring and solving network problems.

The proposed scenarios propose the configuration of various devices that allow the structuring of the network, from the basic configuration, the vlsm security encapsulation processes to the information, the creation of Vlan networks, local and virtual networks, the DHCP and NAT protocols, the configuration of IP addressing within the previously established addressing, validating the successful connection of the configurations made.

Keywords: CISCO, CCNA, Switching, Routing, Networking, Electronics.P, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

Existen diferentes necesidades, requerimientos y exigencias de las nuevas tecnologías de la información orientan indiscutiblemente al aprovechamiento de las herramientas que brindan comprensión, habilidades y capacidades para el manejo y uso de redes de datos.

Con el propósito de evidenciar los protocolos de enrutamiento propuestos por la academia CISCO los estudiantes del diplomado de profundización CISCO CCNA, busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se plantea crear dos escenarios en los cuales se debe evidenciar lo aprendido en el diplomado, el primer escenario se plantea implementar una red VLAN de IPv4 realizando la respectiva configuración de los dispositivos y equipos de manera que permita establecer la comunicación adecuada entre ellos y así permitir la adecuada transferencia de datos.

El trabajo se realiza mediante un proceso paso a paso de las configuraciones requeridas, necesarias para poder implementar la simulación del escenario 1, aplicando la configuración inicial, y el enrutamiento para el Router, donde se le asigna nombre y protocolo de comunicación. Se realizo la configuración del Router y Switch 1 en este proceso se tuvo en cuenta el direccionamiento IPV4 y para interconectar la PC -A y la PC- B, y se puedan realizar las validaciones mediante el uso del comando “ping”, a través de la creación de cuentas de usuarios y la asignación de contraseñas secretas para habilitar router, line de consola, línea terminal virtual.
En el escenario 2 se realizará la configuración de OPSF, para lo cual básicamente se deben primero inicializar los routers y los switches, posteriormente proceder a la configuración de los Routers siguiendo el paso a paso. Finalmente, se configuran los switches, realizando toda la conectividad del escenario en el simulador Packet Tracer. Se configurará la seguridad del switch, las VLAN y el routing entre VLAN de cada switch, así como también el protocolo de routing dinámico OSPF, se implementará DHCP y NAT para ipv4, mediante los comandos por el entorno de CLI adecuado y que se necesita para la práctica de cada una de las instrucciones y soluciones a desarrollar.

DESARROLLO

1. ESCENARIO 1

Figura 1. Topología escenario 1

Fuente: Propia.

En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos, diseñar el esquema de direccionamiento IPv4 para las LAN propuestas. El router y el switch también deben administrarse de forma segura.

Objetivos

Parte 1: Construir en el simulador la Red.

Parte 2: Desarrollar el esquema de direccionamiento IP para la LAN1 y la LAN2.

Parte 3: Configurar los aspectos básicos de los dispositivos de la Red propuesta.

Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 4: Configurar los hosts y verificar la conectividad entre los equipos

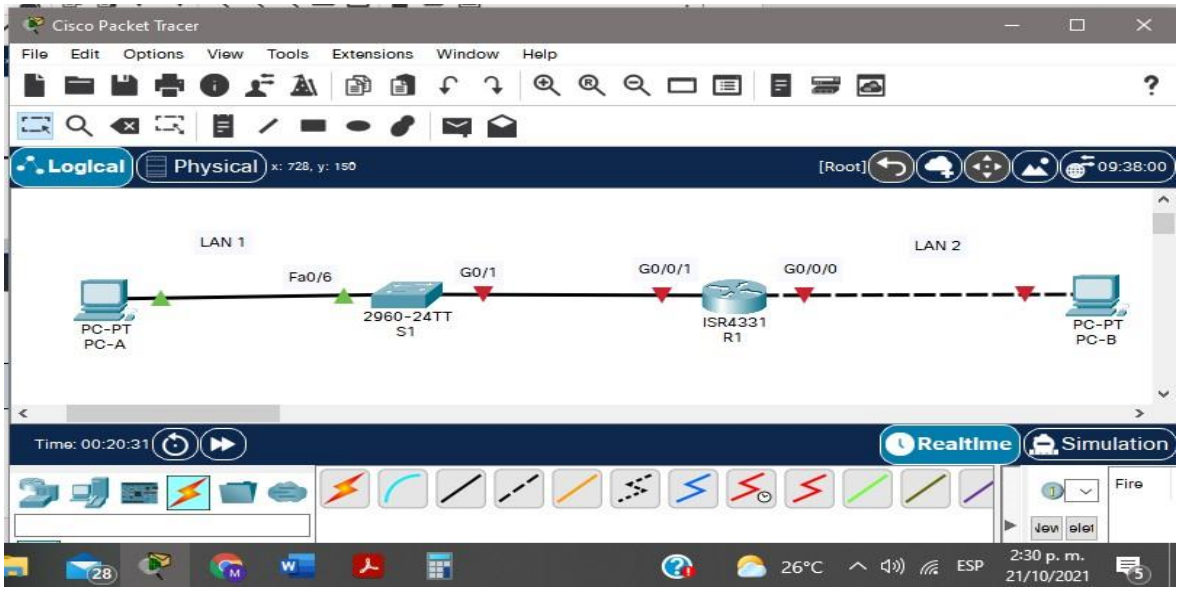
Aspectos básicos/situación

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

Parte 1: Construya la Red

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

Figura 2. Simulación de escenario 1



Fuente: Propia

Parte 2: Desarrolle el esquema de direccionamiento IP

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

Cada estudiante tomará el direccionamiento 192.168.57.0 donde X corresponde a los últimos dos dígitos de su cédula.

Se procede a realizar la subdivisión de la dirección IP dada.

192.168.57.0/24	Dirección IP de clase c, al ser de clase c el último octeto se toma para host.

Figura 3. Análisis IP inicial

IP	MASCARA DE RED LAN 1	BITS A TRABAJAR
192.168.57.0/24	255.255.255.0	2^8
IP inicial dada	Máscara de red	Dos a la ocho por que solo se toma el cuarto octeto

Fuente: Propia

Se toma el último octeto y se puede observar que para la LAN 1 se usan 7 bits para host y 1 bits para subred en este caso en el prefijo de la IP dada /24 se le suma 1 bit de subred quedando la nueva red con prefijo /25 lo que quiere decir que la nueva mascara de red se sumas los 7 octetos de host el cual al realizar la operación da 128 quedando la LAN 1 así:

Figura 4. Direccionamiento LAN 1

	HOST	Dirección de red	Prefijo	Máscara de red
LAN 1	100	192.168.57.0	/25	255.255.255.128

Cuarto octeto							
0	0	0	0	0	0	0	0
1 bist para sub red	7 bist para host						

Fuente: Propia

Se toma el último octeto y se puede observar que para la LAN 2 se usan 6 bits para host y 2 bits para subred en este caso en el prefijo de la IP dada /24 se le suma 2 bit de subred quedando la nueva red con prefijo /26 lo que quiere decir que la nueva máscara red se sumas los 2^7=128 de la LAN 1 más 2^6= 64 de LAN 2 al realizar la suma da 192 quedando la LAN 2 así:

Figura 5. Direccionamiento LAN 2

	HOST	Dirección de red	Prefijo	Máscara de red
LAN 2	50	192.168.57.128	/26	255.255.255.192

Cuarto octeto							
0	0	0	0	0	0	0	0
2 bist para sub red	6 bist para host						

Fuente: Propia

Tabla 1. Subredes

LAN	CANTIDAD HOST	DIRECCIÓN DE RED	MASCARA DE RED	PRIMER IP	ULTIMA IP	BROADCAST
LAN 1	100	192.168.57.0	255.255.255.128	192.168.57.1	192.168.57.126	192.168.57.127
LAN 2	50	192.168.57.128	255.255.255.192	192.168.57.129	192.168.57.190	192.168.57.191
Posible ampliación de red futura		192.168.57.192				

Fuente: Propia

Tabla 2. Tabla de direccionamiento

ITEM	REQUERIMIENTO
Dirección de Red	192.168.57.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.57.1/25
R1 G0/0/0	192.168.57.129/26
S1 SVI	192.168.57.2/25
PC-A	192.168.57.126/25
PC-B	192.168.57.190/26

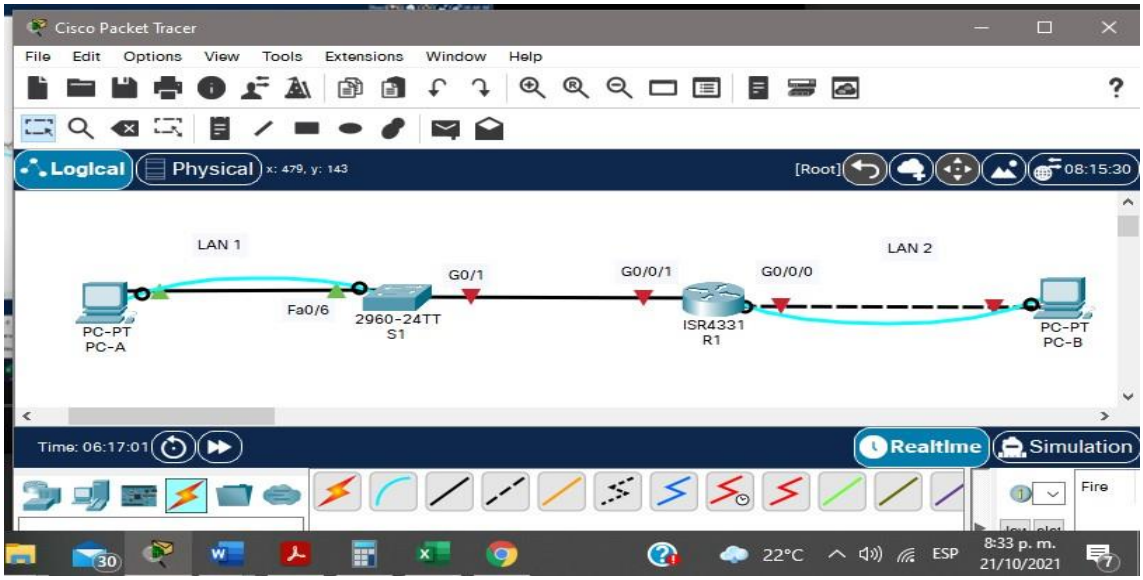
Fuente: Propia

Parte 3: Configure aspectos básicos

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

Se realiza la respectiva configuración agregando al escenario 1 el cable de consola a los diferentes dispositivos para poder realizar la adecuada conexión por medio de consola.

Figura 6. Simulación escenario 1 con cable de consola



Fuente: Propia

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Configuración Router R1

Tabla 3. Configuración R1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS	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
Establecer la longitud mínima para las contraseñas 10 caracteres	R1(config)#security password 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 4 R1(config-line)#password ciscopaso6 R1(config-line)#login local
Configurar VTY solo aceptando SSH	R1(config-line)#transport input SSH
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Configure un MOTD Banner	R1(config)#banner motd #Esta es una red privada, si usted continua tendrá acciones legales#
Configurar interfaz G0/0/0 Establezca la descripción Establece la dirección IPv4. Activar la interfaz	R1(config)#interface g0/0/0 R1(config-if)#ip address 192.168.57.129 255.255.255.192 R1(config-if)#description esta es la interfaz de la LAN 2 R1(config-if)#no shutdown
Configurar interfaz G0/0/1 Establezca la descripción Establece la dirección IPv4. Activar la interfaz.	R1(config)#interface g0/0/1 R1(config-if)#description esta es la interfaz de la LAN 1 R1(config-if)#ip address 192.168.57.1 255.255.255.128 R1(config-if)#no shutdown
Generar una clave de cifrado RSA Módulo de 1024 bits	R1(config)#ip domain name ccna-lab.com R1(config)#crypto key generate rsa The name for the keys will be: R1.ccna-lab.com Choose the size of the key modulus in the

	range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: 1024

Fuente: Propia.

Se procede a configurar el enrutador 1.

Se adjunta código.

Código de configuración Router R1

Router>enable	Ingreso a modo privilegiado.
Router#configure terminal	Ingreso a modo de configuración.
Enter configuration commands, one per line. End with CNTL/Z.	
Router(config)#no ip domain-lookup	Desactiva la búsqueda DNS.
Router(config)#hostname R1	Asignación nombre al router.
R1(config)#ip domain-name ccna-lab.com	Dominio del router.
R1(config)#enable secret ciscoenpass	Se encripta la contraseña para modo privilegiado.
R1(config)#line console 0	Se ingresa a la línea de la consola.
R1(config-line)#password ciscoconpass	Se asigna contraseña de acceso a la consola.
R1(config-line)#login	Se autentica la contraseña.
R1(config-line)#exit	Salir de línea de la consola.
R1(config)#security password min-length 10	Se establece la longitud mínima para las contraseñas de 10 caracteres.
R1(config)#username admin password admin1pass	Se crea un usuario administrativo en la base de datos local.
R1(config)#line vty 0 4	Se configura el inicio de sesión en las líneas VTY para que use la base de datos local.
R1(config-line)#password ciscopaso6	Se asigna una contraseña.

R1(config-line)#login local	Se asigna la base de datos local.
R1(config-line)#transport input SSH	Se configura para que la línea VTY solo acepte SSH.
R1(config-line)#exit	Se pide salir de línea de VTY
R1(config)#service password-encryption	Se cifran las contraseñas de texto no cifrado
R1(config)#banner motd #Esta es una red privada, si usted continua tendrá acciones legales#	Se configura un MOTD Banner
R1(config)#interface g0/0/0	Se llama la interfaz g0/0/0 para asignar IP
R1(config-if)#ip address 192.168.57.129 255.255.255.192	Se le asigna IPv4 a la interfaz g0/0/0 y mascara de red
R1(config-if)#description esta es la interfaz de la LAN 2	Se le da una descripción a la interfaz g0/0/0
R1(config-if)#no shutdown	Se guarda y se activa la configuración
R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up	
R1(config-if)#exit	Salir de la configuración de la interfaz g0/0/0
R1(config)#interface g0/0/1	Se llama la interfaz g0/0/1 para asignar IP
R1(config-if)#description esta es la interfaz de la LAN 1	Se le da una descripción a la interfaz g0/0/1
R1(config-if)#ip address 192.168.57.1 255.255.255.128	Se le asigna IPv4 a la interfaz g0/0/1 y mascara de red
R1(config-if)#no shutdown	Se guarda y se activa la configuración
R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up	

R1(config-if)#exit	Salir de la configuración de la interfaz g0/0/1
R1(config)#ip domain name ccna-lab.com	Se llama el dominio
R1(config)#crypto key generate rsa	Se llama el cifrado para 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	Se ingresa el Módulo de 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]	
R1(config)#exit	Salir de la configuración rsa
*Mar 1 0:51:21.948: %SSH-5-ENABLED: SSH 1.99 has been enabled R1# %SYS-5-CONFIG_I: Configured from console by console	
R1#wr Building configuration...	Guardar la configuración

Las tareas de configuración de S1 incluyen lo siguiente:

Configuración switch S1

Tabla 4. Configuración S1

TAREA	ESPECIFICACIÓN
Desactivar la búsqueda DNS.	Switch(config)#no ip domain-lookup
Nombre del switch S1	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)#password ciscopaso6 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 #Este es un swicht privado absténgase en continuar#
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#ip domain name ccna-lab.com S1(config)#crypto key generate rsa 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 conforme la tabla de direccionamiento.	S1(config)#interface vlan 1 *Mar 1 3:28:28.545: %SSH-5-ENABLED: SSH 1.99 has been enabled S1(config-if)#ip address 192.168.57.2 255.255.255.128 S1(config-if)#no shutdown S1(config-if)#exit
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.	ip default-gateway 192.168.57.1

Fuente: Propia.

Se procede a configurar el Switch 1.

Código de configuración Switch S1

Switch>enable	Ingreso a modo privilegiado.
Switch#configure terminal	Ingreso a modo de configuración.
Enter configuration commands, one per line. End with CNTL/Z.	
Switch(config)#no ip domain-lookup	Desactiva la búsqueda DNS.
Switch(config)#hostname S1	Asignación nombre al switch.
S1(config)#ip domain-name ccna-lab.com	Dominio del switch.
S1(config)#enable secret ciscoenpass	Se encripta la contraseña para modo privilegiado.
S1(config)#line console 0	Se ingresa a la línea de la consola.
S1(config-line)#password ciscoconpass	Se asigna contraseña de acceso a la consola.
S1(config-line)#login	Se autentica la contraseña**.**

S1(config-line)#exit	Salir de línea de la consola**.**
S1(config)#username admin password admin1pass	Se crea un usuario administrativo en la base de datos local**.**
S1(config)#line vty 0 15	Se configura el inicio de sesión en las líneas VTY para que use la base de datos local**.**
S1(config-line)#password ciscopaso6	Se asigna una contraseña**.**
S1(config-line)#login local	Se asigna la base de datos local**.**
S1(config-line)#transport input SSH	Se configura para que la línea VTY solo acepte SSH**.**
S1(config-line)#exit	Se pide salir de línea de VTY.
S1(config)#service password-encryption	Se cifran las contraseñas de texto no cifrado.
S1(config)#banner motd #Este es un swicht privado absténgase en continuar#	Se configura un MOTD Banner.
S1(config)#ip domain name ccna-lab.com	Se llama el dominio.
S1(config)#crypto key generate rsa	Se llama el cifrado para 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]	Se ingresa el Módulo de 1024 bits.
S1(config)#interface vlan 1	Se llama la interfaz vlan 1 para la asignación de la IP.
*Mar 1 3:28:28.545: %SSH-5-ENABLED: SSH 1.99 has been enabled	
S1(config-if)#ip address 192.168.57.2 255.255.255.128	Se le asigna la IPv4 a la interfaz vlan 1 y la máscara de red.
S1(config-if)#no shutdown	Se guarda la configuración.

S1(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up	
S1(config-if)#exit	Salir de la configuración vlan 1.
S1(config)#ip default-gateway 192.168.57.1	Se configura la puerta de enlace predeterminada del Gateway.

Paso 2. Configurar los equipos

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

Tabla 5. PC-A Network Configuration

PC-A Network Configuration	
Descripción	Este es el PC -A
Dirección física	000B.BEAA.94B2
Dirección IP	192.168.57.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.57.1

Fuente: Propia.

Se ingresa al PC-A y en desktop se da clic en IP configuration allí se ingresa en los espacios correspondientes la dirección IPv4, la máscara de red y el Gateway.

Se ingresa a la PC-A en desktop y en command prompt se ingresa en comando ipconfig /all, este permitirá ver la información de configuración del PC-A y su dirección física**.**

Tabla 6. PC-B Network Configuration

PC-B Network Configuration	
Descripción	Esta es la PC-B
Dirección física	0005.5EAE.7349
Dirección IP	192.168.57.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.57.1

Fuente: Propia.

Se ingresa al PC-B y en desktop se da clic en IP configuration allí se ingresa en los espacios correspondientes la dirección IPv4, la máscara de red y el Gateway. Se ingresa a la PC-B en desktop y en command prompt se ingresa en comando ipconfig /all, este permitirá ver la información de configuración del PC-B y su dirección física**.**

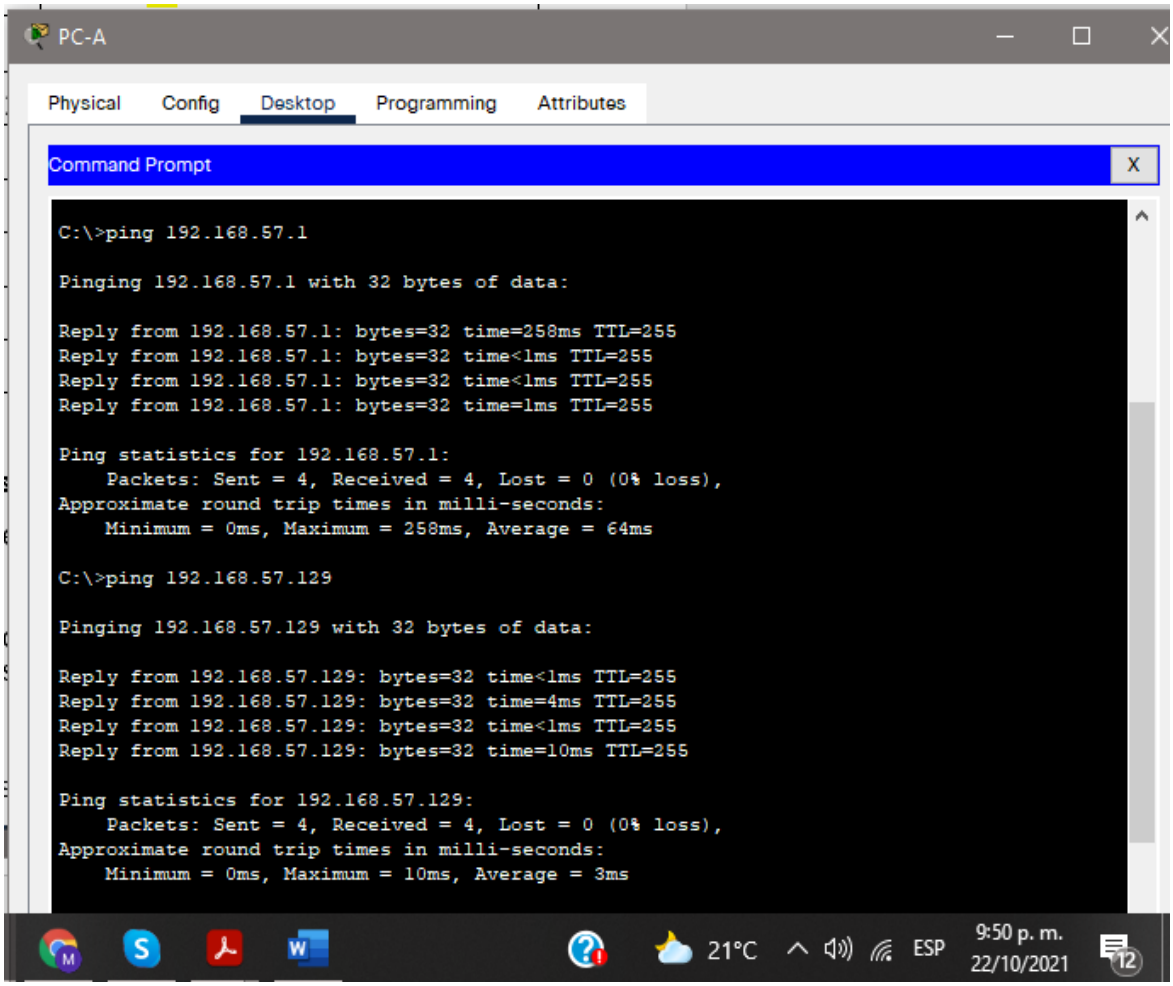
Pruebas de conectividad

Se ingresan el comando ping y la dirección IP del equipo que se desea verificar la conectividad.
Código:

C:\>ping 192.168.57.1 Prueba de conectividad de PC-A a interfaz g0/0/1

C:\>ping 192.168.57.129 Prueba de conectividad de PC-A a interfaz g0/0/0

Figura 7. Pruebas de conectividad de PC-A a interfaz g0/0/0 e interfaz g0/0/1



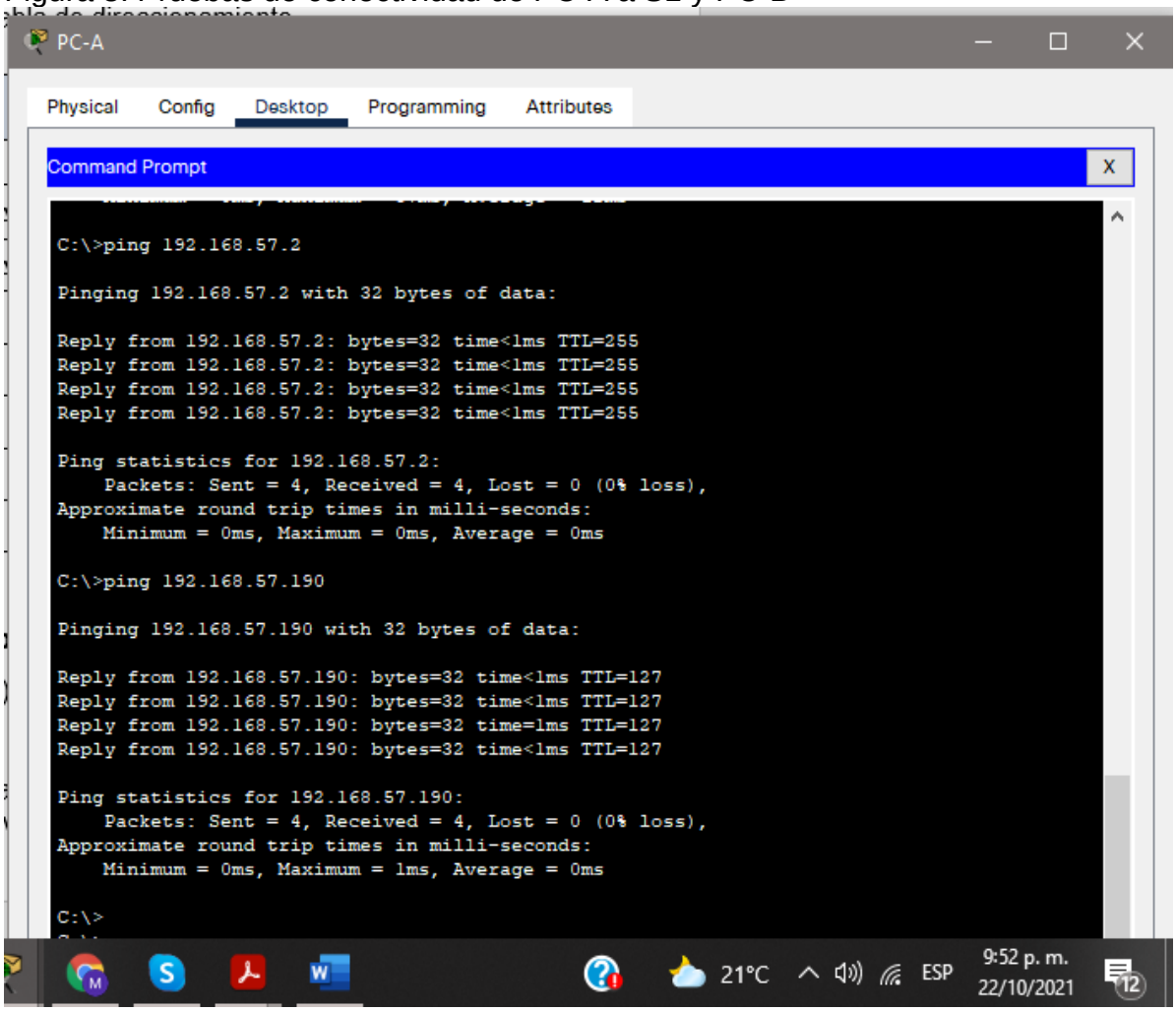
Fuente: propia

Código:

C:\>ping 192.168.57.2 Prueba de conectividad de PC-A a Switch

C:\>ping 192.168.57.190 Prueba de conectividad de PC-A a PC-B

Figura 8. Pruebas de conectividad de PC-A a S1 y PC-B



Fuente: propia

Prueba de acceso con SSH

Para realizar la prueba de acceso a ssh se ingresa el comando ssh -l usuario dirección IP en este caso será así: ssh -l admin 192.168.57.2, la dirección IP ingresada corresponde a la del switch, en seguida pedirá que se ingrese el password que es admin1pass, mostrará el mensaje que se configuro en el banner motd. Para ver la respectiva configuración que se realizó se ingresa el comando sh run.

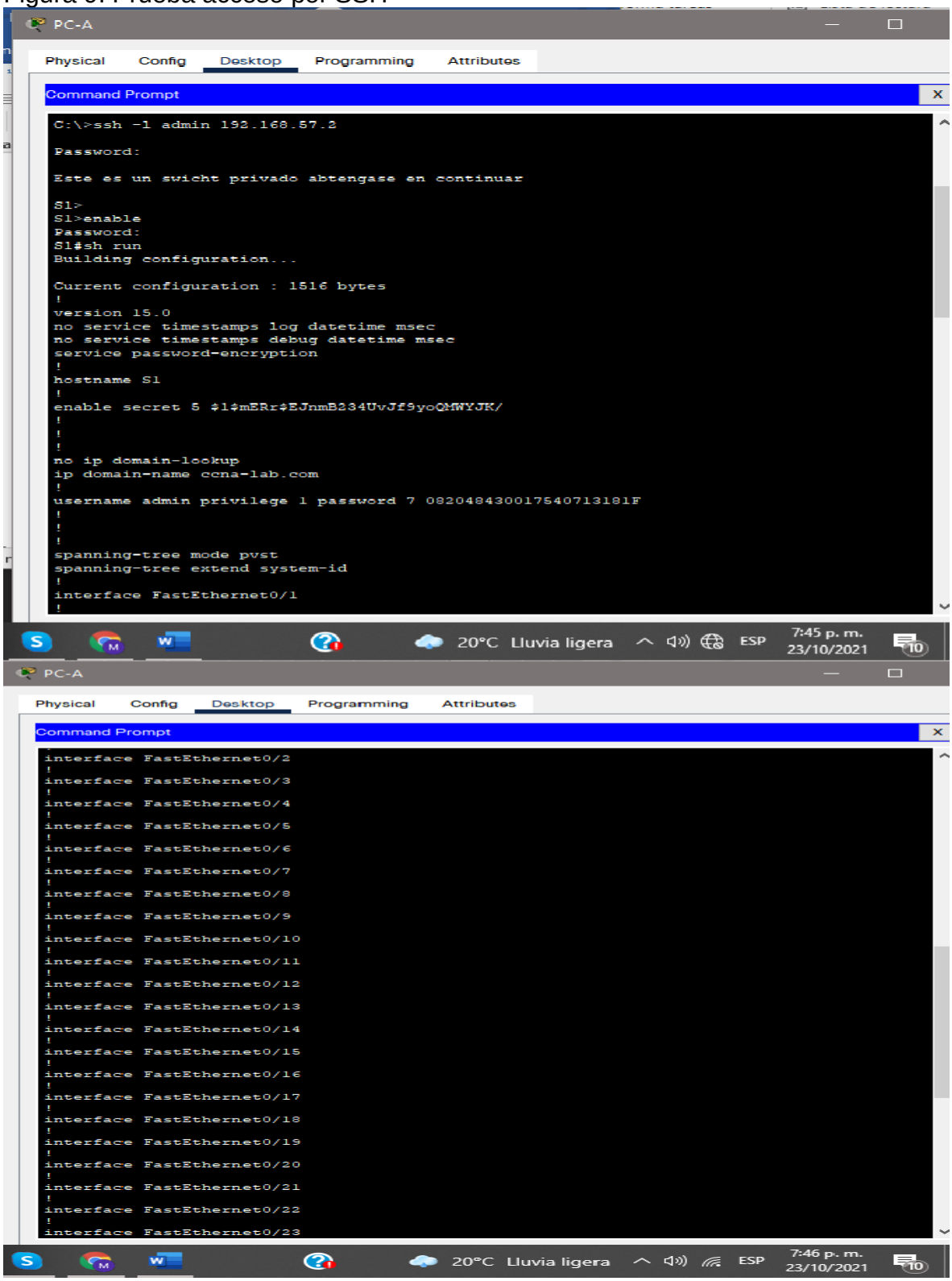
Código de prueba de acceso con ssh y resultados de configuración realizadas.

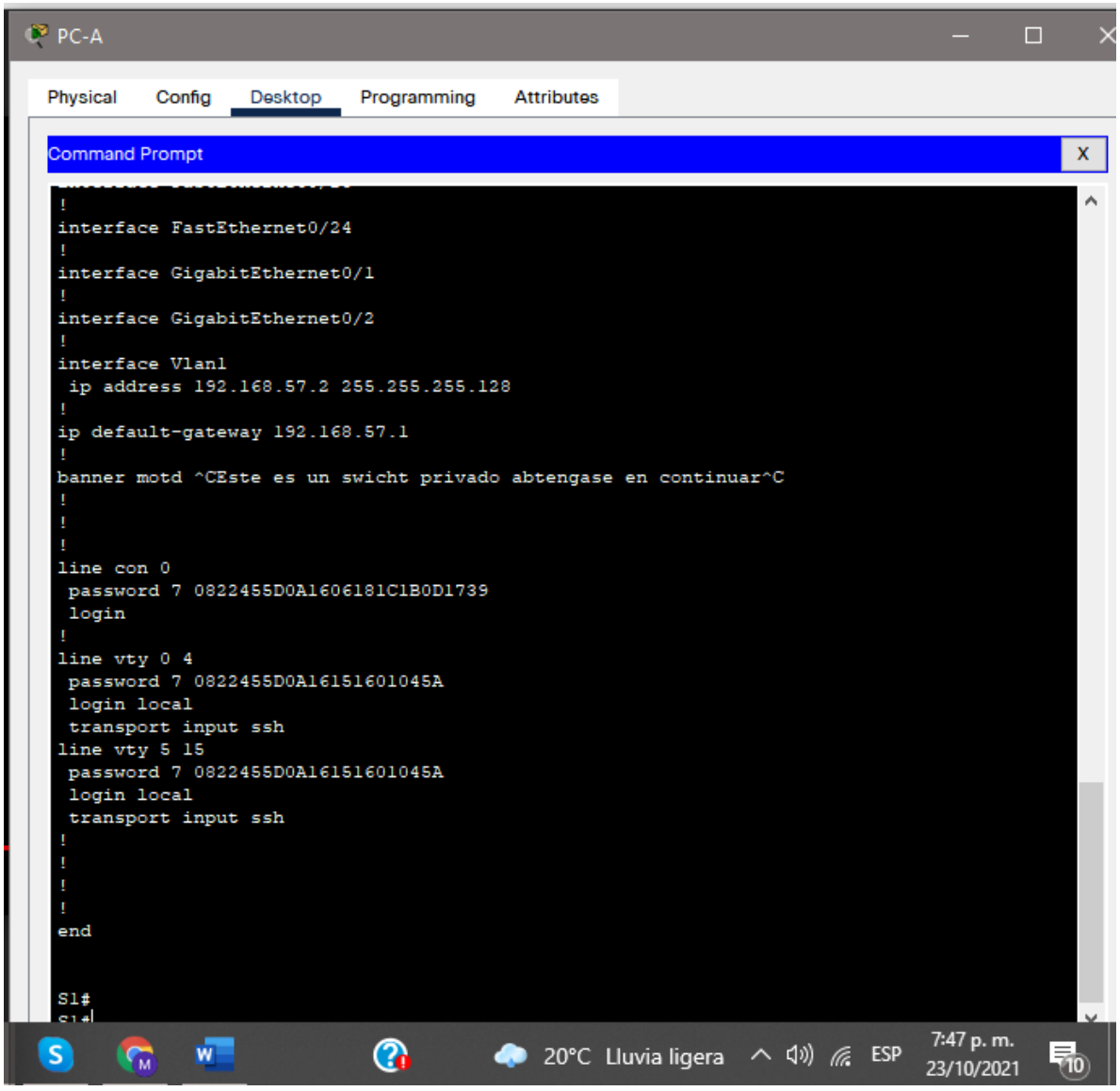
C:\>ssh -l admin 192.168.57.2	Ingreso al administrador por ssh
Password:	Ingreso de contraseña de administrador
Este es un switch privado absténgase en continuar S1>	Mensaje creado en banner motd
S1>enable	Ingreso al modo privilegiado
Password:	Ingreso de contraseña creada para modo privilegiado
S1#sh run	Ingreso a información de configuración del equipo
Building configuration... Current configuration : 1516 bytes ! version 15.0 no service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption !	
hostname S1 !	Nombre asignado al Switch
enable secret 5 1mERr$EJnmB234UvJf9yoQMWYJK/ ! !	Contraseña cifrada de acceso a consola
no ip domain-lookup ip domain-name ccna-lab.com !	Dominio asignado
username admin privilege 1 password 7 08204843001754071 3181F ! !	Usuario administrativo de base local y contraseña cifrada
spanning-tree mode pvst spanning-tree extend system-id !	
interface FastEthernet0/1 !	Interfaces

```
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
```

interface FastEthernet0/24 ! interface GigabitEthernet0/1 ! interface GigabitEthernet0/2 !	
interface Vlan1 ip address 192.168.57.2 255.255.255.128	Dirección IP asignada a la vlan 1
! ip default-gateway 192.168.57.1	Dirección IP asignada al Gateway
! banner motd ^CEste es un swicht privado absténgase en continuar^C	Banner motd creado
! ! line con 0 password 7 0822455D0A1606181C1B0D1739 login	Contraseña de acceso a consola cifrada
! line vty 0 4 password 7 0822455D0A16151601045A login local	Ingreso a línea vty de router y contraseña de acceso para vty cifrada
transport input ssh	Especifica que se está trabajando en ssh
line vty 5 15 password 7 0822455D0A16151601045A login local	Ingreso a línea vty de switch y contraseña de acceso para vty cifrada
transport input ssh ! ! ! end S1#	Especifica que se está trabajando en ssh

Figura 9. Prueba acceso por SSH



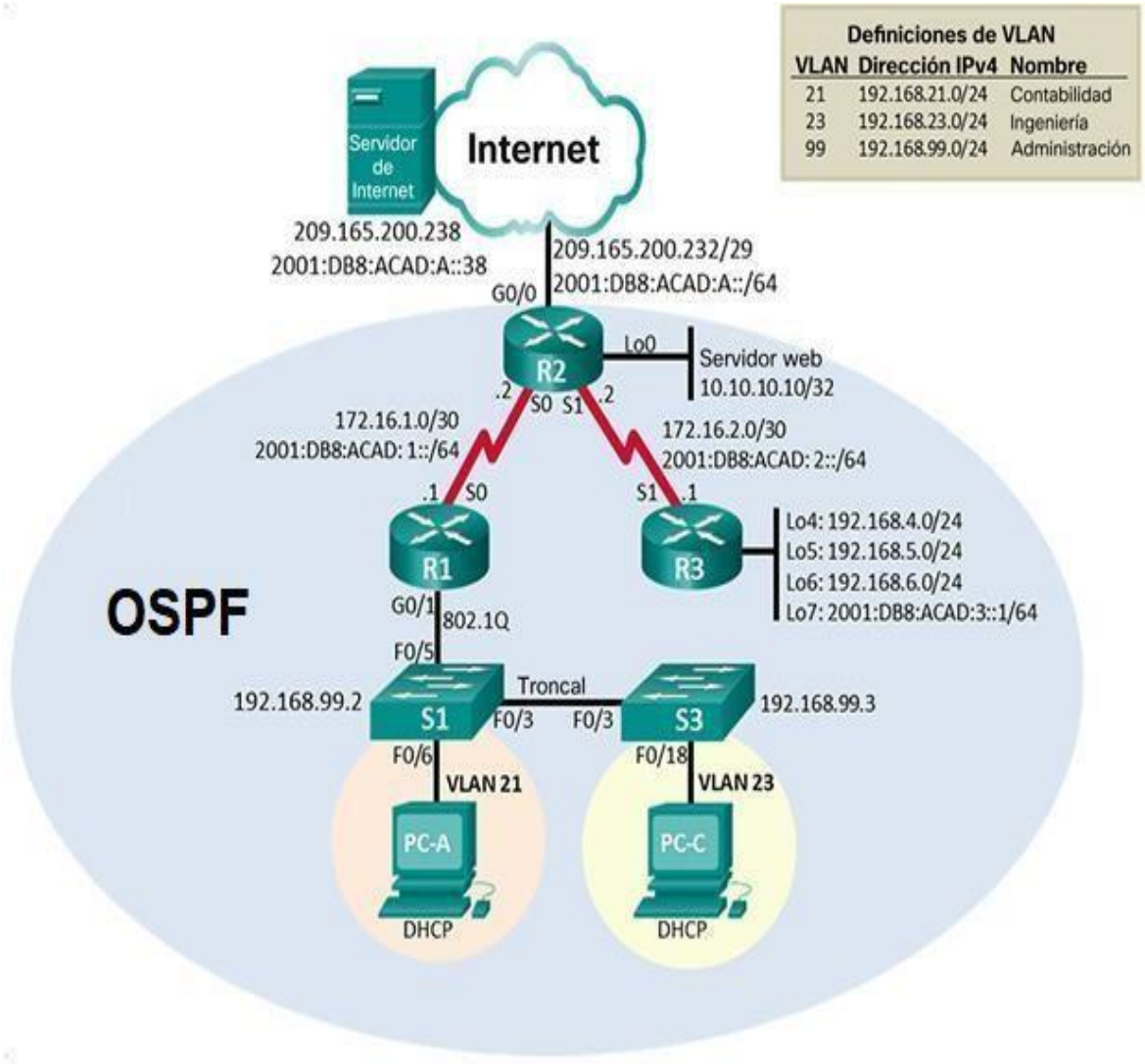


Fuente: propia

2. ESCENARIO 2

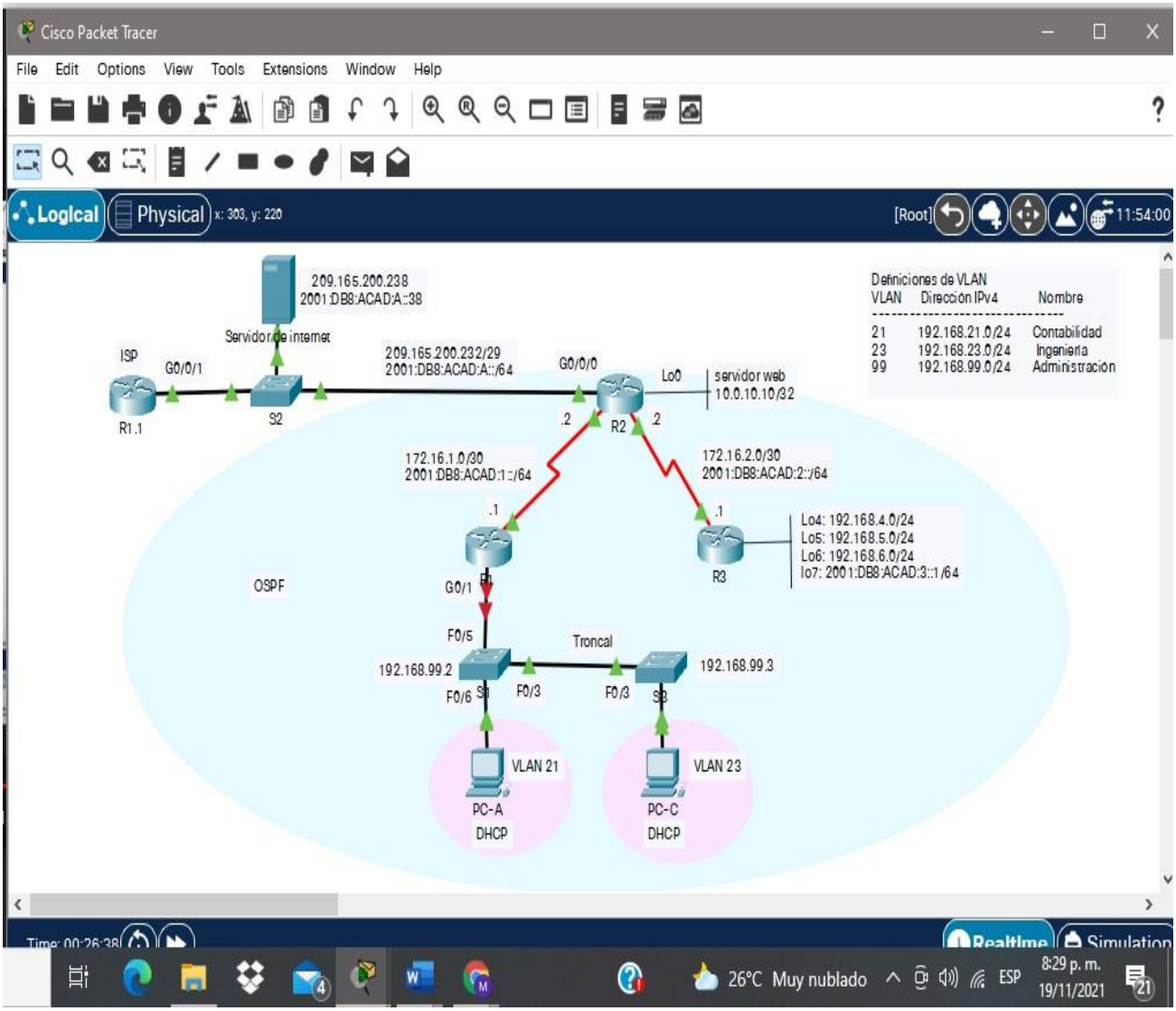
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de 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.

Figura 10. Topología escenario 2



Fuente: Propia.

Figura 11. Topología escenario 2 en simulador packet Tracer



Fuente: propia

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.

Tabla 7. Inicialización y recarga de R1, R2, R3, S1 y S3.

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

Fuente: Propia.

Figura 12. verifique la inicialización de los dispositivos.

Fuente: Propia.

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 8. Configuración de la computadora de internet

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

Fuente: Propia.

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.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9. Configuración R1

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

Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Contraseña de acceso Telnet	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	R1(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/1/0	R1(config)#ipv6 unicast-routing R1(config)#interface serial 0/1/0 R1(config-if)#description R1 a R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no shutdown %LINK-5-CHANGED: Interface Serial0/1/0, changed state to down R1(config-if)#exit
Rutas predeterminadas	R1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0 %Default route without gateway, if not a point-to-point interface, may impact performance R1(config)#ipv6 route ::/0 s0/1/0 R1(config)#exit R1# %SYS-5-CONFIG_I: Configured from console by console

Fuente: Propia.

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Configuración R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router#enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiado cifrada	R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Contraseña de acceso Telnet	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	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 R2#
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado#

Interfaz S0/1/0	R2(config)#interface s0/1/0 R2(config-if)#description conexion a R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 R2(config-if)#no shutdown
Interfaz S0/1/1	R2(config-if)#interface s0/1/1 R2(config-if)#description conexion a R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown
Interfaz G0/0/0 (simulación de Internet)	R2(config-if)#interface g0/0/0 R2(config-if)#description conexion servidor R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#no shutdown
Interfaz loopback 0 (servidor web simulado)	R2(config-if)#interface lo0 R2(config-if)#description servidor web R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#no shutdown
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0/0 %Default route without gateway, if not a point-to-point interface, may impact performance R2(config)#ipv6 route ::/0 gigabitEthernet 0/0/0 R2(config)# R2# %SYS-5-CONFIG_I: Configured from console by console

Fuente: Propia.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11. Configuración R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>enable Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config-line)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado#
Interfaz S0/1/1	R3(config)#ipv6 unicast-routing R3(config)#interface s0/1/1 R3(config-if)#description conexion a R2 R3(config-if)#ip address 172.168.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface lo4 R3(config-if)#description interfaz loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0

	R3(config-if)#exit
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)#description interfaz loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 6	R3(config)#interface lo6 R3(config-if)#description interfaz loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#interface lo7 R3(config-if)#description interfaz loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#no shutdown
Rutas predeterminadas	R3(config-if)#ip route 0.0.0.0 0.0.0.0 s0/1/1 %Default route without gateway, if not a point-to-point interface, may impact performance R3(config)#ipv6 route ::/0 s0/1/1 R3(config)# R3# %SYS-5-CONFIG_I: Configured from console by console

Fuente: Propia.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12. Configuración S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S1
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#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	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Fuente: Propia.

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiado cifrada	S3(config)#enable secret class

Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#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	S3(config)#banner motd # Se prohíbe el acceso no autorizado#

Fuente: Propia.

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 14. Verificación de conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/1/0	172.16.1.2	Ping exitoso
R2	R3, S0/1/1	172.16.2.1	Ping exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Ping exitoso

Fuente: Propia.

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

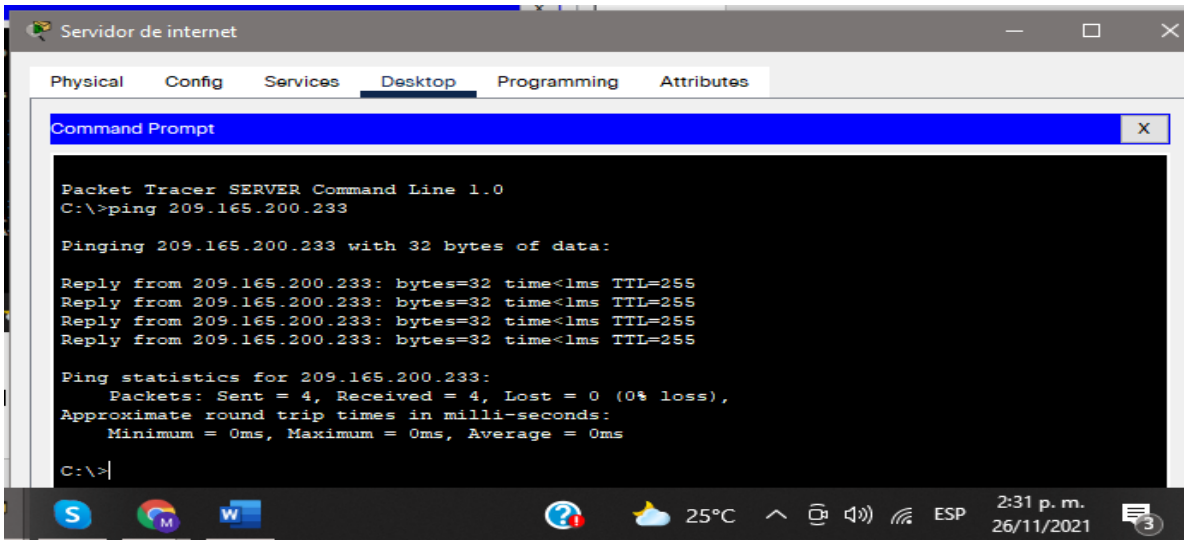
Figura 13. Ping de R1 a R2 s0/1/0

Fuente: Propia

Figura 14. Ping de R2 a R3 s0/1/1

Fuente: Propia

Figura 15. Ping Pc de internet a Gateway predeterminado



Fuente: Propia.

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 15. Configuración de la seguridad del Switch, S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan 21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion S1(config-vlan)#exit
Asignar la dirección IP de administración.	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	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#interface f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Forzar el enlace troncal en la interfaz F0/5	S1(config-if)#interface f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#no shutdown
Configurar el resto de los puertos como puertos de acceso	S1(config-if)#interface range f0/1-2, f0/4, f0/7-24 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#exit

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

Fuente: Propia.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16. Configuración de la seguridad del Switch, S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0 S3(onfig-if)no shutdown S3(config-if)#exit
Asignar el gateway predeterminado.	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	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	S3(config)#interface range f0/1 - f0/2 S3(config-if-range)#switchport mode access S3(config)#interface range f0/7 - f0/24 S3(config-if-range)#switchport mode access S3(config-if-range)#exit

Asignar F0/18 a la VLAN 21	S3(config)#interface f0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit
Apagar todos los puertos sin usar	S3(config)#interface range f0/7 - f0/17 S3(config-if-range)#shutdown S3(config)#interface range f0/19 - f0/24 S3(config-if-range)#shutdown S3(config-if)#exit

Fuente: Propia.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración de la seguridad del Router, R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#interface g0/0/1 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#interface g0/0/1.21 R1(config-subif)# R1(config-subif)#description LAN de contabilidad VLAN 21 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	R1(config)#interface g0/0/1.23 R1(config-subif)#description LAN de ingenieria VLAN 23 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	R1(config)#interface g0/0/1.99 R1(config-subif)#description LAN de administracion VLAN 99 R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit R1(config)#
Activar la interfaz G0/1	R1(config)#interface g0/0/1 R1(config-if)#no shutdown R1(config-subif)#exit

Fuente: Propia.

Paso 4: Verificar la conectividad de la red

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

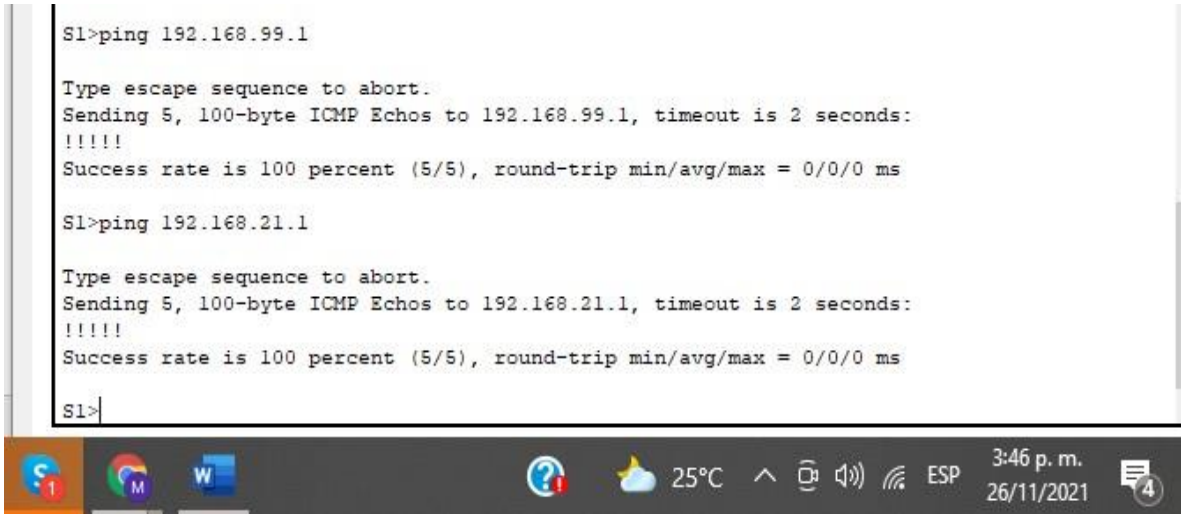
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 18. Verificación de conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Si hubo conexión
S3	R1, dirección VLAN 99	192.168.99.1	Si hubo conexión
S1	R1, dirección VLAN 21	192.168.21.1	Si hubo conexión
S3	R1, dirección VLAN 23	192.168.23.1	Si hubo conexión

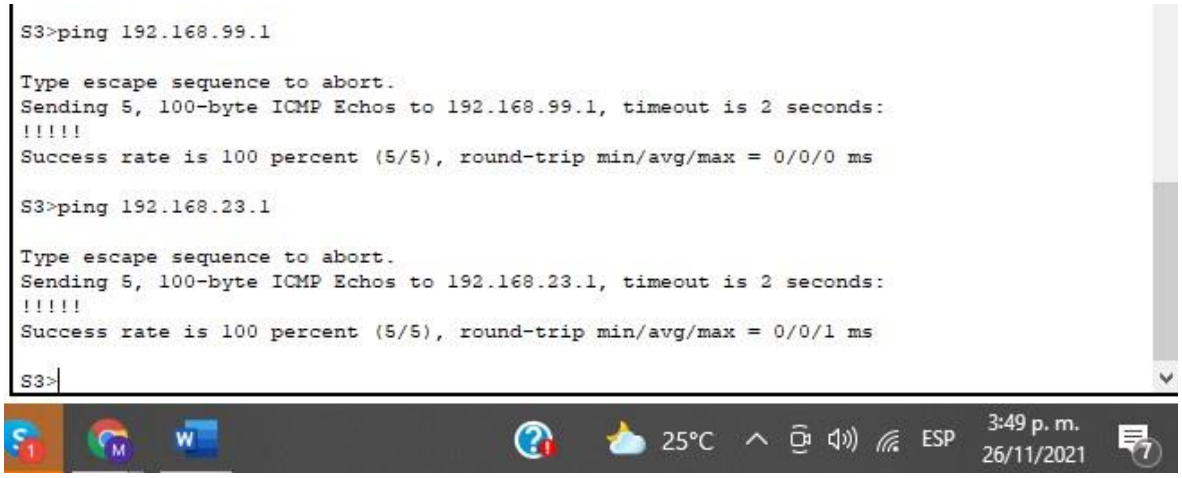
Fuente: Propia.

Figura 16. Prueba de conectividad desde S1 a R1, Vlan 99 y Vlan 21



Fuente: propia

Figura 17. Prueba de conectividad desde S3 a R1, Vlan 23 y Vlan 99



Fuente: propia.

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 19. Configurar OSPF en el R1

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#route ospf 1
Anunciar 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 R1(config-router)#exit
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive-interface g0/0/1 R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99 R1(config-router)#exit
Desactive la sumarización automática	No aplica (El escenario simulado en Packet Tracer no permite la inserción del comando no autosummary). R1(config)#router ospf 1 R1(config-router)#no auto-summary ^ % Invalid input detected at '^' marker. R1(config-router)#exit

Fuente: Propia.

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuración protocolo de enrutamiento OSPF en el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2(config)#router ospf 1

Anunciar las redes conectadas directamente Nota: Omitir la red G0/0.	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 loopback 0
Desactive la sumarización automática.	No aplica (El escenario simulado en Packet Tracer no permite la inserción del comando no auto- 78 summary). R2(config)#router ospf 1 R2(config-router)#no auto-summary ^ % Invalid input detected at '^' marker. R2(config-router)#exit

Fuente: Propia.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

Tabla 21. Configurar OSPFv3 en el R*3*

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3(config)#router 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 loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#exit
Desactive la sumarización	No aplica

automática.	(El escenario simulado en Packet Tracer no permite la inserción del comando no auto-summary). R3(config)#no auto-summary ^ % Invalid input detected at '^' marker.

Fuente: Propia.

Paso 4: Verificar la información de OSPF

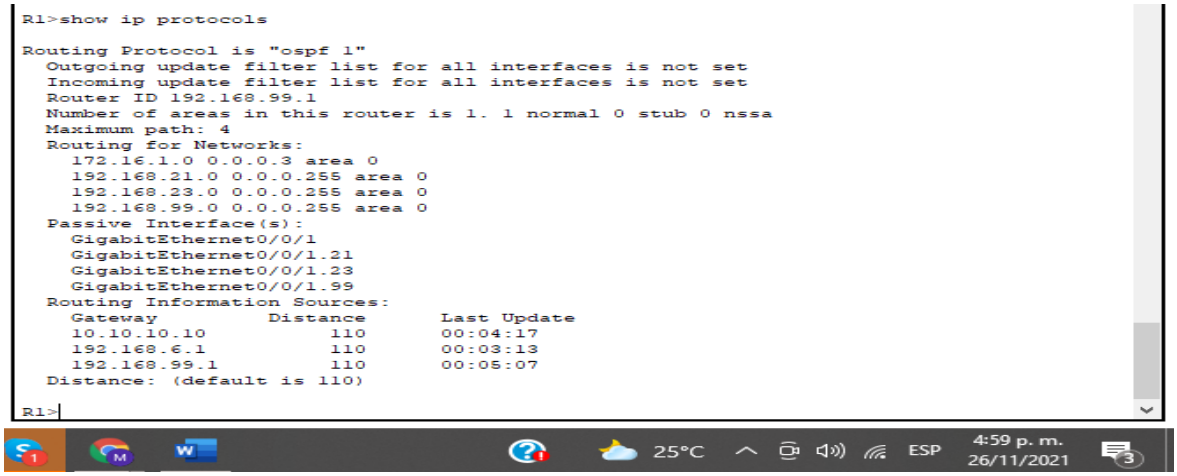
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 22. Verificar la información 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 ip ospf database

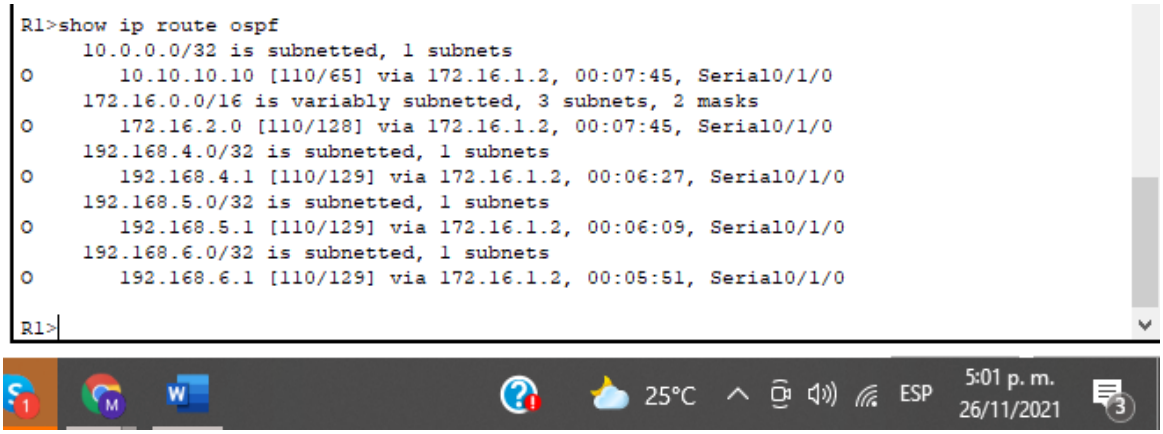
Fuente: Propia.

Figura 18. Comando Show Ip Protocols desde R1



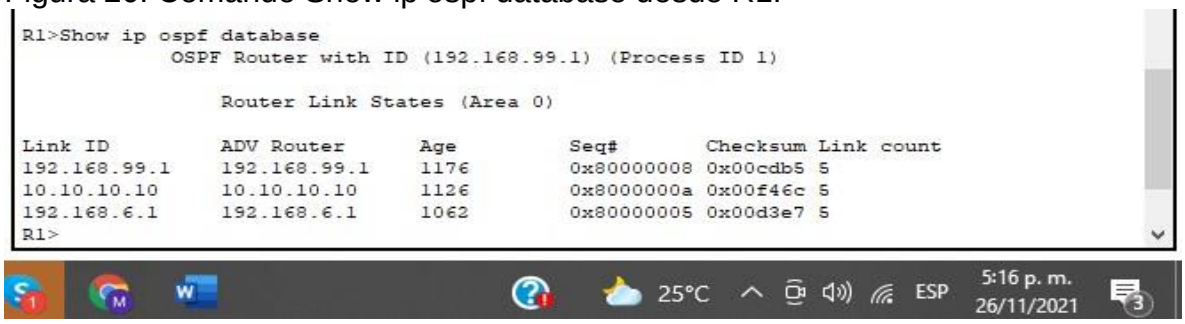
Fuente: propia.

Figura 19. Comando Show Ip route Ospf desde R1



Fuente: propia.

Figura 20. Comando Show ip ospf database desde R1.



Fuente: propia.

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

Elemento o tarea de configuración	Especificación
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 dominio: ccna-sa.com Establecer el gateway predeterminado	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-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(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#exit

Fuente: Propia.

Paso 2: Configuración NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configuración NAT estática y dinámica en el 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(config)#user webuser privilege 15 secret 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.
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.
Crear una NAT estática al servidor web.	R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233
Asignar la interfaz interna y externa para la NAT estática	R2(config)#interface g0/0/0 R2(config-if)#ip nat outside R2(config-if)#interface s0/1/0 R2(config-if)#ip nat inside R2(config-if)#interface s0/1/1 R2(config-if)#ip nat inside R2(config-if)#interface lo0 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 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 192.168.0.0 0.0.3.255

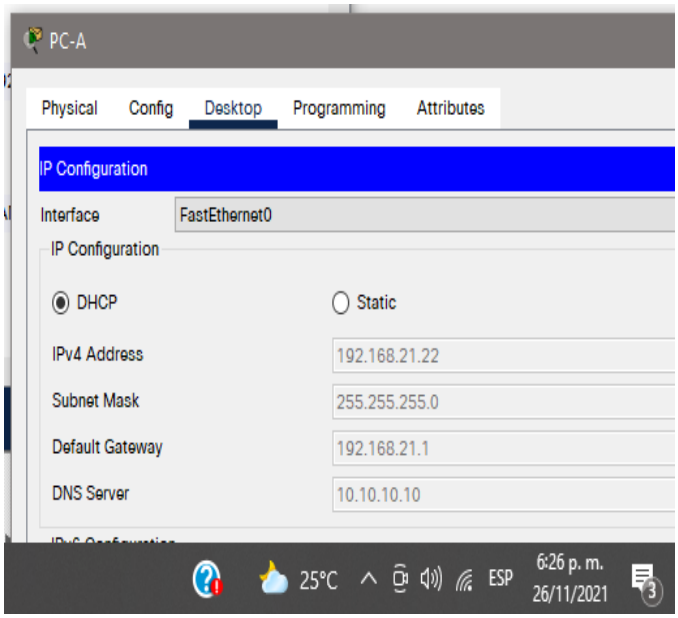
Defina el pool de direcciones IP públicas utilizables. Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228	R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#ip nat inside source list 1 pool INTERNET

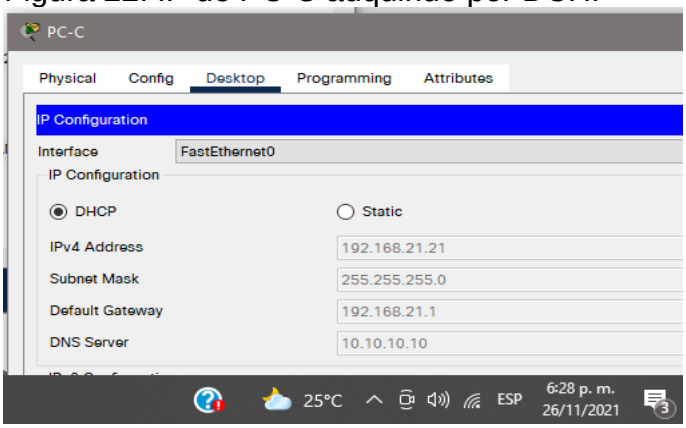
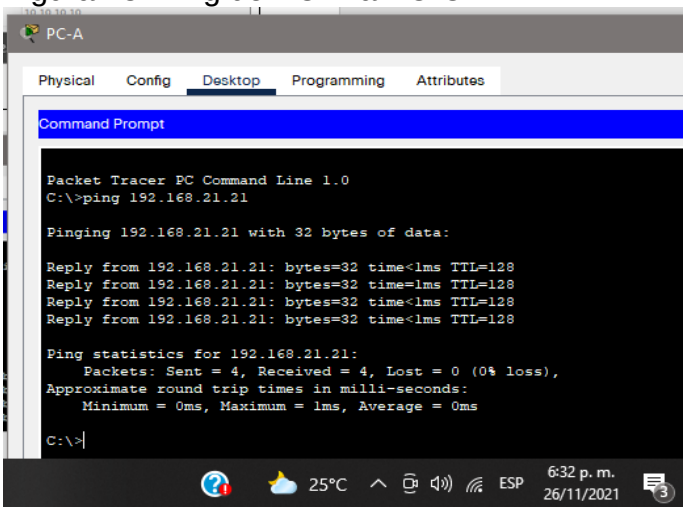
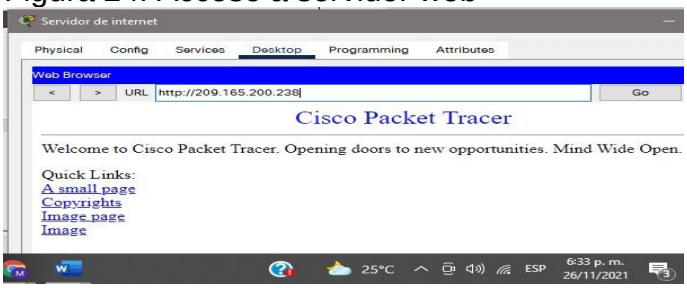
Fuente: Propia.

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 25. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 21. IP de PC-A adquirido por DCHP  Fuente: propia

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 22. IP de PC-C adquirido por DCHP  Fuente: propia
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Figura 23. Ping de PC-A a PC-C  Fuente: Propia.
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	Figura 24. Acceso a servidor web  Fuente: Propia.

	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. Se emplea 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

Fuente: Propia.

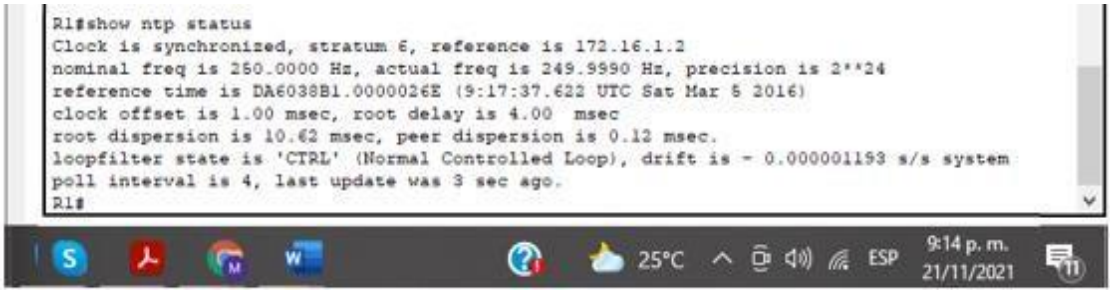
Parte 6: Configurar NTP

Tabla 26. Configurar NTP en R1 y R2

Elemento o tarea de configuración	Especificación
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 R2(config)#exit
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#show ntp status

Fuente: propia

Figura 25. Verificación de configurar NTP en R1



Fuente: Propia.

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

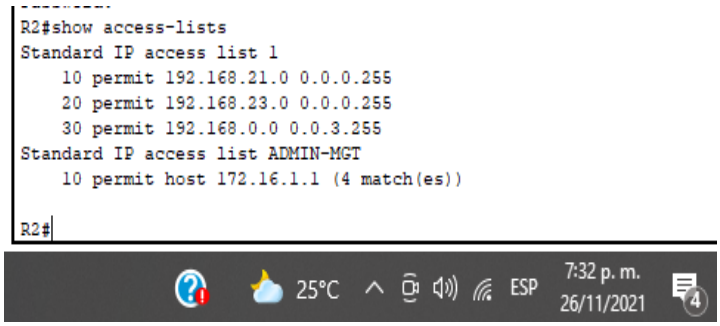
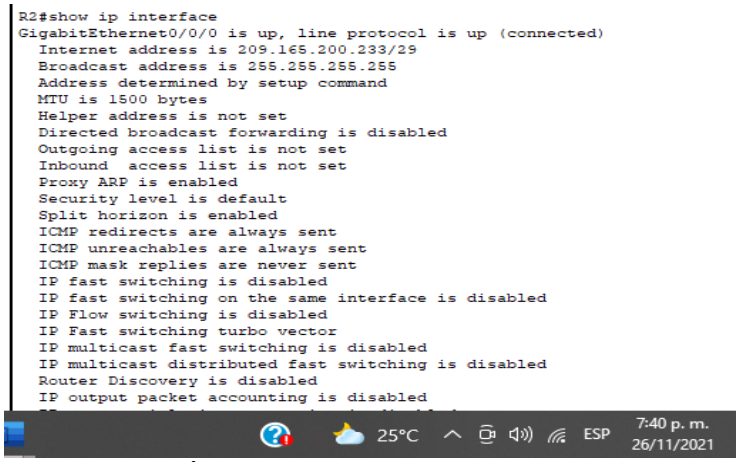
Paso 1: Restringir el acceso a las líneas VTY en el R2

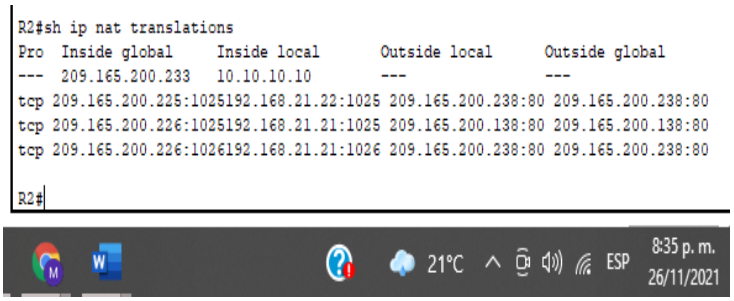
Tabla 27. Restringir el acceso a las líneas VTY en el R2

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-lis 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 15 R2(config-line)#access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	R2(config-line)#transport input telnet R2(config-line)#exit
Verificar que la ACL funcione como se espera	Figura 26. Verificación y conexión Telnet desde R1 a R2  Fuente: propia.

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

Tabla 28. 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 27: comando show acces-lists  Fuente: Propia.
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 | include access R2#show running-config | include access Figura 28. Comando show ip interface  Fuente: Propia.

¿Con qué comando se muestran las traducciones NAT? 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.	R2#show ip nat translations Figura 29. Comando show ip nat translations  Fuente. Propia.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	R2#clear ip nat translation

Fuente. Propia.

CONCLUSIONES

Se identificaron lo diferentes comandos a utilizar para realizar la adecuada configuración de los equipos que se manejaron en el escenario 1, se identificó el adecuado enrutamiento de los equipos evidenciando por medio de comando ping que la conectividad fue exitoso en los diferentes equipos; por medio de la prueba de acceso por SSH se identificó la adecuada configuración de los diferentes dispositivos y el adecuado cifrado de las contraseñas de acceso.

Gracias a la máscara de red se permite delimitar el ámbito de la red de ordenadores. Así la máscara de red permite al usuario identificar e indicar a todos los dispositivos que parte de la dirección IP es la correspondiente al número de la red, la nueva máscara de subred y la cantidad de host que le corresponde.

El desarrollo de la actividad permitió comprender que el servicio DHCP se puede encontrar activo en un servidor donde se centraliza la administración de las direcciones IP de la red, que los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser dividido en su área.

Las listas de control de acceso desempeñan un gran papel como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema, para poder aplicar los conocimientos adquiridos a lo largo del curso de profundización Cisco y sobre todo relacionados con el protocolo de enrutamiento denominado OSPF, aplicando su configuración básica a los dispositivos de red, configurando una prioridad de routers, desactivando las actualizaciones de enrutamiento en las interfaces adecuadas y verificando la conectividad entre los dispositivos de la topología**.**

Para realizar un buen direccionamiento es de suma importancia realizar correctamente la tabla de subredes para así facilitar el proceso de asignación y configuración de subredes en los equipos. Si todos los equipos pertenecen a una misma subred es posible la conexión entre los diferentes equipos que conforman la red y cuando los equipos se encuentran dentro de la misma subred los datos pueden ser enviados directamente sin necesidad de desvíos de comunicación.

BIBLIOGRÁFIA

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

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

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

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre IPv6. *Inge Cuc*, *12*(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, *14*(1), 127-138.

BAREÑO, Gutiérrez, R., Sevillano, A. M. L., Díaz-Piraquive, F. N., & González-Crespo, R. (2021, July). Analysis of WEB Browsers of HSTS Security Under the MITM Management Environment. In *International Conference on Knowledge Management in Organizations* (pp. 331-344). Springer, Cham.

BAREÑO, Gutiérrez, R., Cardenas-Urrea, S. E., Navarro-Nuñez, W., Sarmiento-Osorio, H., & Forero-Paez, N. (2017). Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia. *Revista UIS Ingenierías*, *16*(1), 75-84.

BAREÑO Gutiérrez, R. (2013). Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.

BAREÑO Raúl, G., & Sevillano, A. M. L. (2017, October). Services cloud under HSTS, Strengths and weakness before an attack of man in the middle MITM. In *2017 Congreso Internacional de Innovacion y Tendencias en Ingenieria (CONIITI)* (pp. 1-5). IEEE.

GUTIERREZ, R. B., Núñez, W. N., Urrea, S. C., Osorio, H. S., & Acosta, N. D. (2016). Revisión de la seguridad en la implementación de servicios sobre

IPv6. *Inge Cuc*, *12*(1), 86-93.

GUTIERREZ, R. B., Urrea, S. C., Núñez, W. N., Sarmiento, H., Acosta, N. D., & Sánchez, G. G. V. (2015). Análisis de la seguridad en la implementación de servicios corporativos sobre el protocolo IPV. *Revista de Tecnología*, *14*(1), 127-138.

MOJICA S. Felipe, Andrés, L. V. S., & Raúl, B. G. (2019, October). Risks Found in Electronic Payment Cards on Integrated Public Transport System Applying the ISO 27005 Standard. Case Study Sitp DC Colombia. In *2019 Congreso Internacional de Innovación y Tendencias en Ingenieria (CONIITI)* (pp. 1-6). IEEE.

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

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

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

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