

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS  
CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

JULIAN ALEXANDER ANGEL LOPEZ

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

SOLUCION DE DOS ESCENARIOS PRESENTES EN ENTORNOS  
CORPORATIVOS BAJO EL USO DE TECNOLOGIA CISCO

JULIAN ALEXANDER ANGEL LOPEZ

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

DIRECTOR:  
MSc. HECTOR JULIAN PARRA MOGOLLON

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

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Facatativá Cundinamarca, 26 de Junio de 2022

## CONTENIDO

LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	8
RESUMEN .....	11
ABSTRACT .....	12
INTRODUCCIÓN .....	13
DESARROLLO .....	14
Escenario 1 .....	14
Aspectos básicos/situación.....	14
Parte 1: Construya la Red.....	14
Parte 2: Desarrolle el esquema de direccionamiento IP .....	15
Parte 3: Configure aspectos básicos .....	17
Paso 1: configurar los ajustes básicos.....	17
Paso 2. Configurar los equipos de la red LAN .....	23
Paso 3. Pruebas de Configuración .....	24
Escenario 2.....	25
Parte 1: Inicializar dispositivos.....	25
Paso 1: Inicializar y volver a cargar los routers y los switches.....	25
Parte 2: Configurar los parámetros básicos de los dispositivos.....	26
Paso 1: Configurar la computadora de Internet .....	26
Paso 3: Configurar Básica R2.....	27
Paso 4: Configuración Básica R3 .....	28
Paso 5: Configuración Básica S1 .....	29
Paso 6: Configuración Básica S3 .....	30
Paso 7: Verificar la conectividad de la red .....	30
Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN..	31
Paso 1: Configuración del Crear VLAN S1 .....	31
Paso 2: Configuración VLAN del S3.....	33

Paso 3: Configurar Subinterfaz R1 .....	33
Paso 4: Verificar la conectividad de la red .....	34
Parte 4: Configurar el protocolo de routing dinámico OSPF .....	35
Paso 1: Configurar OSPF en el R1 .....	35
Paso 2: Configurar OSPF en el R2.....	36
Paso 4: Verificar la información de OSPF .....	37
Parte 5: Implementar DHCP y NAT para IPv4 .....	37
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23.....	37
Paso 2: Configurar la NAT estática y dinámica en el R2 .....	38
Paso 3: Verificar el protocolo DHCP y la NAT estática .....	39
Parte 6: Configurar NTP .....	40
Parte 7: Configurar y verificar las listas de control de acceso (ACL) .....	40
Paso 1: Restringir el acceso a las líneas VTY en el R2 .....	40
Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente .....	41
CONCLUSIONES .....	42
BIBLIOGRAFIA.....	43

## LISTA DE TABLAS

Tabla 1. Direccionamiento General .....	15
Tabla 2. Direccionamiento Especifico .....	16
Tabla 3. Configuración SW .....	19
Tabla 4. Configuración PC-A .....	22
Tabla 5. Configuración PC-B. ....	22
Tabla 6. Eliminar configuración y volver a cargar.....	25
Tabla 7. Direccionamiento .....	26
Tabla 8. Configurar R1.....	26
Tabla 9. Configuración R2 .....	28
Tabla 10. Configuración R3 .....	28
Tabla 11. Configuración S1.....	29
Tabla 12. Configuración S3.....	30
Tabla 13. Respuesta Ping.....	31
Tabla 14. Configuración VLAN.....	33
Tabla 15. Verificación Conectividad .....	34
Tabla 16. Verificación Información de OSPF .....	35
Tabla 17. Configuración R1 Cómo servidor DHCP para las VLAN .....	35
Tabla 18. Verificación Protocolo DHCP y la NAT estática.....	39
Tabla 19. Configuración NTP .....	40
Tabla 20. Comando CLI .....	41

## LISTA DE FIGURAS

Figura 1. La topología de la red escenario 1 .....	13
Figura 2. Elaboración de la Red .....	14
Figura 3. Configuración Router.....	18
Figura 4. Configuración Direccionamiento IP .....	18
Figura 5. Configuración NVRAM.....	19
Figura 6. Configuración de SW .....	20
Figura 7. Configuración VTY.....	21
Figura 8. Configuración IP SW.....	21
Figura 9. Configuración PCS.....	23
Figura 10. Pruebas De Configuración.....	25
Figura 10. Solicitud De Topología.....	26
Figura 11. Carga De Dispositivos. ....	27
Figura 12. Pruebas De Ping R1 y R2.....	31
Figura 13. Pruebas De Ping Desde el Switch S1 y S3 .....	35
Figura 14. Protocolo DHCP.....	39
Figura 15. Configuración ACL.....	41

## GLOSARIO

**Cisco Packet Tracer:** es una herramienta de simulación, visualización, colaboración y evaluación para la enseñanza de redes. Permite que los estudiantes construyan su propio modelo o redes virtuales, obtengan acceso a representaciones gráficas importantes de esas redes, animen esas redes agregando sus propios paquetes de datos, hagan preguntas sobre esas redes y, por último, anoten y guarden sus creaciones.

**IPv4:** IPv4 (Protocolo de Internet versión 4 o en inglés: Internet Protocol version 4), es un protocolo de redes basados en Internet. Utiliza direcciones de **32 bits**, siendo el total de direcciones posibles de 4 294 967 296.

**LAN:** Es la abreviatura de Local Area Network. Denomina redes con extensión física limitada. La mayoría de las redes LAN se usan en hogares privados o en empresas, para instalar redes de hogar o de empresa. De este modo, distintos dispositivos pueden comunicarse entre ellos. De este modo, el intercambio de datos tiene lugar primero a nivel local.

Una red LAN consiste en un mínimo de dos dispositivos finales, pero puede conectar miles. Sin embargo, para las grandes distancias es más conveniente usar redes MAN y WAN. Una red de área local o Local Area Network puede conectar ordenadores, teléfonos inteligentes, impresoras, escáneres, dispositivos de almacenamiento, servidores y otros dispositivos de red entre sí y con Internet. Si, por ejemplo, una impresora está conectada a un ordenador a través de USB, normalmente solo este PC puede acceder a ella. Sin embargo, si la impresora está integrada en la red, varios dispositivos de la casa pueden imprimir a la vez.

**NAT:** A. La traducción de direcciones de red (NAT) está diseñada para conservar direcciones IP. Permite que se conecten a Internet las redes de IP privada que emplean direcciones IP no registradas. NAT opera en routers, que en general conectan dos redes, y convierte las direcciones privadas (no exclusivas globalmente) de la red interna en direcciones legales, antes de que se reenvíen los paquetes a otra red.

Se puede configurar NAT para que difunda al mundo exterior solo una dirección para toda la red. Esto brinda más seguridad, al ocultar de hecho detrás de esa dirección toda la red interna. NAT ofrece la doble función de seguridad y conservación de direcciones, y suele implementarse en entornos de acceso remoto.

**NTP:** son las siglas de **Network Time Protocol**. En español lo podemos traducir como 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. Estamos ante uno de los protocolos de red más antiguos y sigue siendo importante para mantener el funcionamiento correcto de las conexiones.

**OSPF:** organiza la información de la tipología de red utilizando lo que se llaman **LSA** y la base de datos de estado de enlace (**LSDB**). Cada LSA es una estructura de datos con alguna información específica sobre la tipología de red; el LSDB es simplemente la una base de datos con la colección de todos los LSA conocidos por un router.

**Red Hosts:** Un host no es más que un nodo, un ordenador o un conjunto de ellos, que ofrecen servicios, datos... al resto de ordenadores conectados a la red, sea esta local o global como internet. En el caso de redes locales, el host suele coincidir con el ordenador central que controla la red. Para hacernos una mejor idea, solo debemos pensar en las relaciones de parasitismo que estudiamos en la escuela. El parásito escoge un huésped, quien trabaja por los dos. Pues bien, la idea es similar. El PC huésped estará trabajando y ofreciendo servicios que recibirá el PC "parásito" o cliente. Evidentemente esto no es más que una simplificación, pero no deja de ser una buena aproximación al concepto.

**Router:** Un router recibe y envía datos en redes informáticas. Los routers a veces se confunden con los concentradores de red, los módems o los switch de red. No obstante, los routers pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales.

**Subnetting:** Definido de la forma más simple, el término subnetting hace referencia a la subdivisión de una red en varias subredes. El subneteo permite a los administradores de red, por ejemplo, dividir una red empresarial en varias subredes sin hacerlo público en Internet. Esto se traduce en que el router que establece la conexión entre la red e Internet se especifica como dirección única, aunque puede que haya varios hosts ocultos. Así, el número de hosts que están a disposición del administrador aumenta considerablemente.

Con la aparición de IPv6, que abarca 128 bits y reemplazará a la versión IPv4 en los próximos años, las direcciones IP ausentes ya no tendrán un papel principal para la creación de subredes.

**Switch:** Los switches son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí.

## RESUMEN

En este documento se presentan los Escenarios 1 y 2 del desarrollo de una Red propuesta mediante la información básica de algunos escenarios, para lo cual se utiliza la herramienta de simulación desarrollada por Cisco Packet Tracer, esta herramienta hace posible la simulación del enrutamiento a través de la creación de redes, utilizando equipos de networking para el bosquejo de la presentación final. Se crean topologías utilizando equipos electrónicos de telecomunicaciones, y se configuran dichos dispositivos para el desarrollo puntual de la actividad. Para ello se hace uso del conocimiento en diseño de redes, dando solución a los requerimientos solicitados y se describe el paso a paso de la configuración de los diferentes elementos. La herramienta de simulación utilizada permite sacar el máximo beneficio de la red propuesta realizando subnetting y encriptación de redes LAN facilitando la aproximación a un conocimiento experto para lograr una certificación CCNP. Y finalmente, en el segundo escenario mediante el uso de conexiones IPv4 e IPv6 donde se realiza la configuración de estos equipos mediante comandos para el uso de protocolos, seguridad, direcciones dinámicas entre otros.

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

## **ABSTRACT**

This document presents Scenarios 1 and 2 of the development of a Network through the basic information of some scenarios, for which the simulation tool developed by Cisco Packet Tracer is used, this tool makes it possible to simulate routing through the creation networking, using networking equipment for the final presentation outline. Topologies are created using electronic telecommunications equipment, and these devices are configured for the specific development of the activity. For this, knowledge in network design is used, providing a solution to the requested requirements and the step-by-step configuration of the different elements is described. The simulation tool used allows getting the most out of the proposed network by performing subnetting and encryption of LAN networks, facilitating the approximation to expert knowledge to achieve a CCNP certification. And finally, in the second scenario through the use of IPv4 and IPv6 connections where the configuration of these devices is carried out through commands for the use of protocols, security, dynamic addresses, among others.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

## INTRODUCCIÓN

El siguiente trabajo se realiza bajo la simulación del software de Cisco Packet Tracer, donde se implementan dos tipos de topologías, una de ellas se encuentra conformada por dos equipos de cómputo, un switch y un router, en el cual se realiza un análisis sobre el comportamiento de diversos protocolos; la configuración se realiza por medio de subnetting a la dirección ip 192.168.57.0 donde los dos penúltimos dígitos corresponden al número de mi documento de identidad.

De esta manera se procede a la configuración de cada uno de los dispositivos, donde se toma nota del paso a paso de cada proceso y se registran los comandos necesarios para realizar las diferentes configuraciones básicas de seguridad de los hosts indicadas para el desarrollo de la actividad. Así mismo se verifica la conectividad entre los equipos, los cuales se registran y se toman como evidencias pantallazos del resultado final.

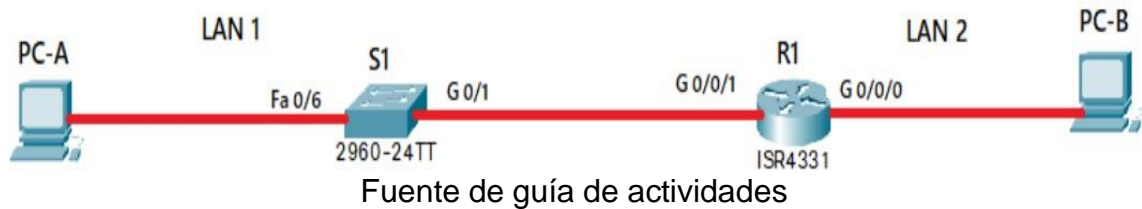
En el segundo escenario, se realizan temáticas como el protocolo OSPF que nos permite compartir y actualizar las tablas de ruteo, también, los ACL, NAT y el protocolo NTP utilizado para sincronizar los relojes u horas de los dispositivos que componen la red.

## DESARROLLO

### Escenario 1

Figura 1. La topología de la red escenario 1

#### Topología



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.

#### 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 switch 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. Elaboración de la Red



Fuente Autor

## 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.X.0 donde X corresponde a los últimos dos dígitos de su cédula.

Tabla 1 Direccionamiento General

Item	Requerimiento
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1
R1 G0/0/0	Primera dirección de host de la subred LAN2
S1 SVI	Segunda dirección de host de la subred LAN1
PC-A	Última dirección de host de la subred LAN1
PC-B	Última dirección de host de la subred LAN2

Fuente Guía de Actividades.

Tabla 2 Direccionamiento Especifico

<b>Item</b>	<b>Requerimiento</b>
Dirección de Red 192.168.X.0 donde X corresponde a los últimos dos dígitos de su cédula.	192.168.57.0 / 24
Requerimiento de host Subred LAN1 100	Dirección de red: 192.168.57.0/25 Cantidad de direcciones: 128 Cantidad de direcciones útiles: 126 Primera dirección valida: 192.168.57.1 Ultima dirección valida: 192.168.57.126 Broadcast: 192.168.57.127 Mascara decimal 255.255.255.128
Requerimiento de host Subred LAN2 50	Dirección de red: 192.168.57.128/26 Cantidad de direcciones: 64 Cantidad de direcciones útiles: 62 Primera dirección valida: 192.168.57.129 Ultima dirección valida: 192.168.57.190 Broadcast: 192.168.57.191 Mascara decimal 255.255.255.192
R1 G0/0/1 Primera dirección de host de la subred LAN1	192.168.57.1 /25
R1 G0/0/0 Primera dirección de host de la subred LAN2	192.168.57.129 /26
S1 SVI Segunda dirección de host de la subred LAN1	192.168.57.2
PC-A Última dirección de host de la subred LAN1	192.168.57.126 /25
PC-B Última dirección de host de la subred LAN1	192.168.57.190 /26

Fuente Autor



### Parte 3: Configure aspectos básicos

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

#### Paso 1: configurar los ajustes básicos.

- A.** Desactivar la búsqueda DNS  
Router>enable --- Inicio modo privilegiado  
Router#config t --- Ingreso Modo configuración  
Router(config)#no ip domain-lookup --- Desactivar búsqueda DNS
  
- B.** Establecer R1 Nombre del router  
Router#config t --- Ingreso Modo configuración  
Router(config)#hostname R1 --- Nombrar Router  
R1(config)#
  
- C.** Nombre de dominio ccna-lab.com  
R1(config)#ip domain-name ccna-lab.com --- Establecer el nombre de dominio  
R1(config)#
  
- D.** Contraseña cifrada para el modo EXEC privilegiado ciscoenpass  
R1(config)# enable password ciscoenpass ---Establece contraseña para modo privilegiad  
R1(config)#
  
- E.** Contraseña de acceso a la consola ciscoconpass  
R1(config)#line console 0 --- Modo de configuracion linea de consola 0  
R1(config-line)# password ciscoconpass--- Se establece la contraseña de inicio de consola R1(config-line) #login --- activar autenticación al iniciar dispositivo  
R1(config-line) #exit
  
- F.** Establecer la longitud mínima para las contraseñas 10 caracteres  
R1(config)# security passwords min-length 10--- Establece mínimo de 10 caracteres para la contraseña  
R1(config)#
  
- G.** Crear un usuario administrativo en la base de datos local Usuario admin y password admin1pass  
R1(config)# username admin secret admin1pass--- crear usuario para ingreso al dispositivo con contraseña

- H.** Configurar el inicio de sesión en las líneas VTY para que use la base de datos local

```
R1(config)#line vty 0 15-- Ingreso a la configuración en las líneas VTY
R1(config-line)#login local ---Establece el usuario creado para iniciar el
dispositivo
R1(config-line)# transport input ssh--- Activar la autenticación de inicio a la
base de datos local
R1(config-line)#exit--- Salir
```

- I.** Configurar VTY solo aceptando SSH
- ```
R1(config-line)#transport input ssh --- Establece que solo acepten conexión
SSH dentro de las líneas vty
R1(config-line)#
```

- J.** Cifrar las contraseñas de texto no cifrado
- ```
R1(config)#Service password-encryption---Cifra las contraseñas de texto
R1(config)#
```

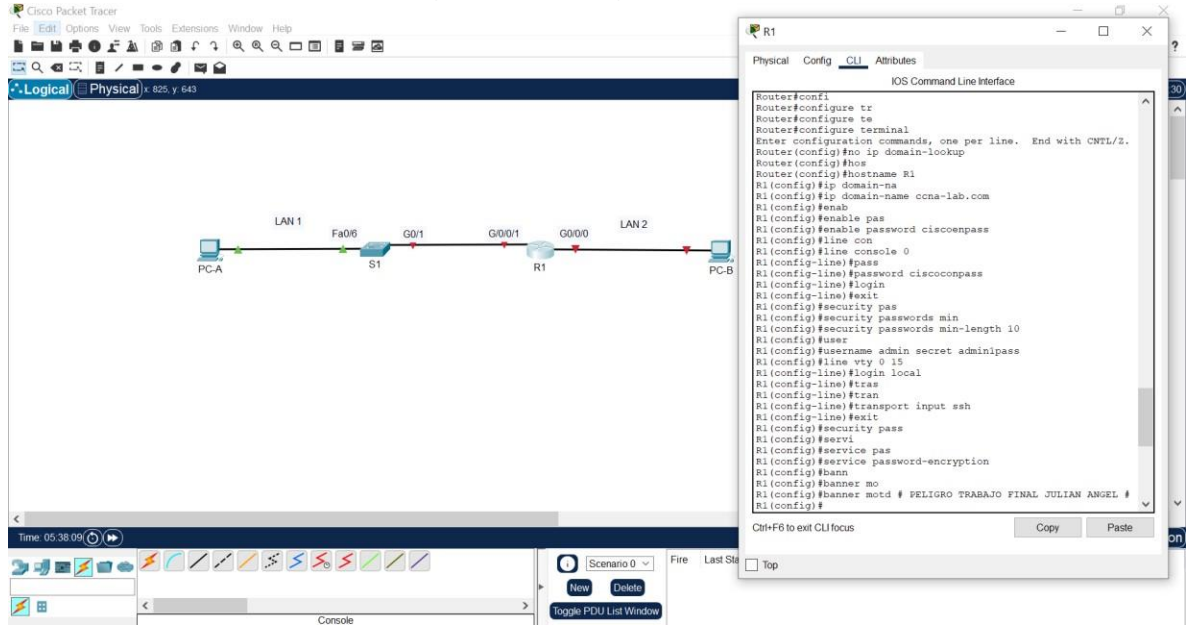
- K.** Configure un MOTD Banner
- ```
R1(config)#banner motd #Colocar mensaje# ---Mensaje de alerta al iniciar el
equipo
R1(config)#
```

- L.** Configurar interfaz G0/0/0 establecer la dirección IPv4 y activar la interfaz
- ```
R1(config)#interface g0/0/0 ---Ingreso a la interface
R1(config-if)#ip address 192.168.57.129 255.255.255.192 --- Configuración
de direccionamiento sobre la interface
R1(config-if)#no shutdown --- Activar la interface
```

- M.** Configurar interfaz G0/0/1 establecer la dirección IPv4 y activar la interfaz
- ```
R1(config-if)#interface g0/0/1 --- Ingreso a la interface
R1(config-if)#ip address 192.168.57.1 255.255.255.128 --- Configuración de
direccionamiento sobre la interface
R1(config-if)#no shutdown --- Activar la interface
```

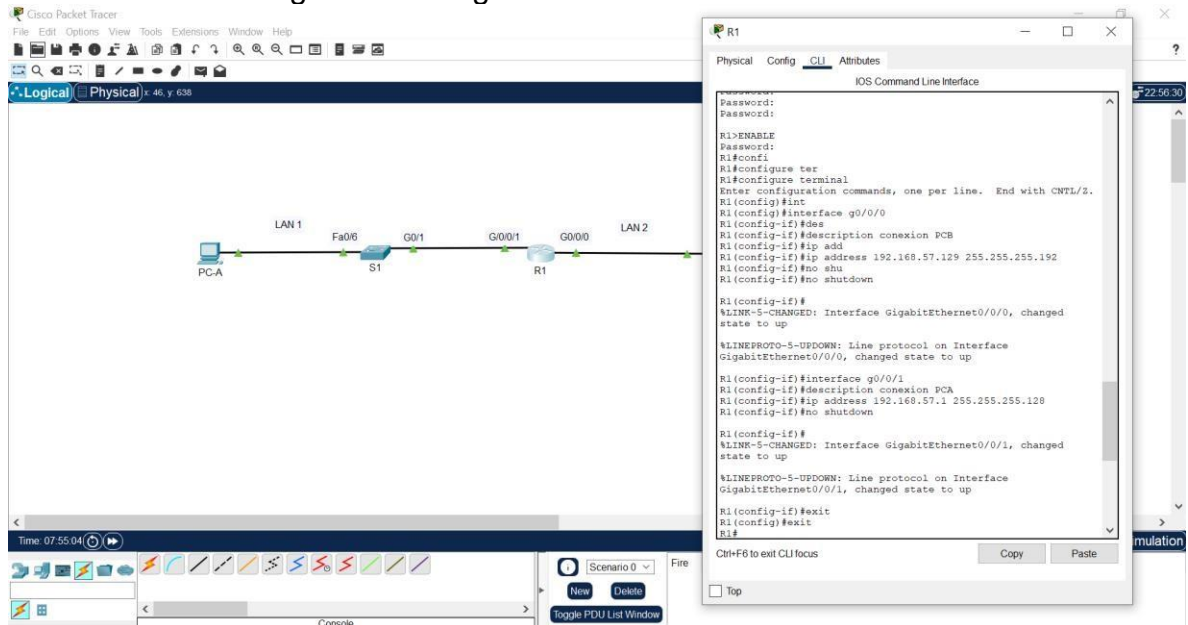
- N.** Generar una clave de cifrado RSA Modulo de 1024 bits Se establece en 1024 bits en el módulo de cifrado
- ```
R1(config)#ip domain-name ccna-lab.com ---Establecer Nombre de Dominio
R1(config)#crypto key generate rsa --- Crear clave de encryption RSA [512]:
1024 --- Establecer el tamaño del modulo en 1024
```

Figura 3. Configuración del Router



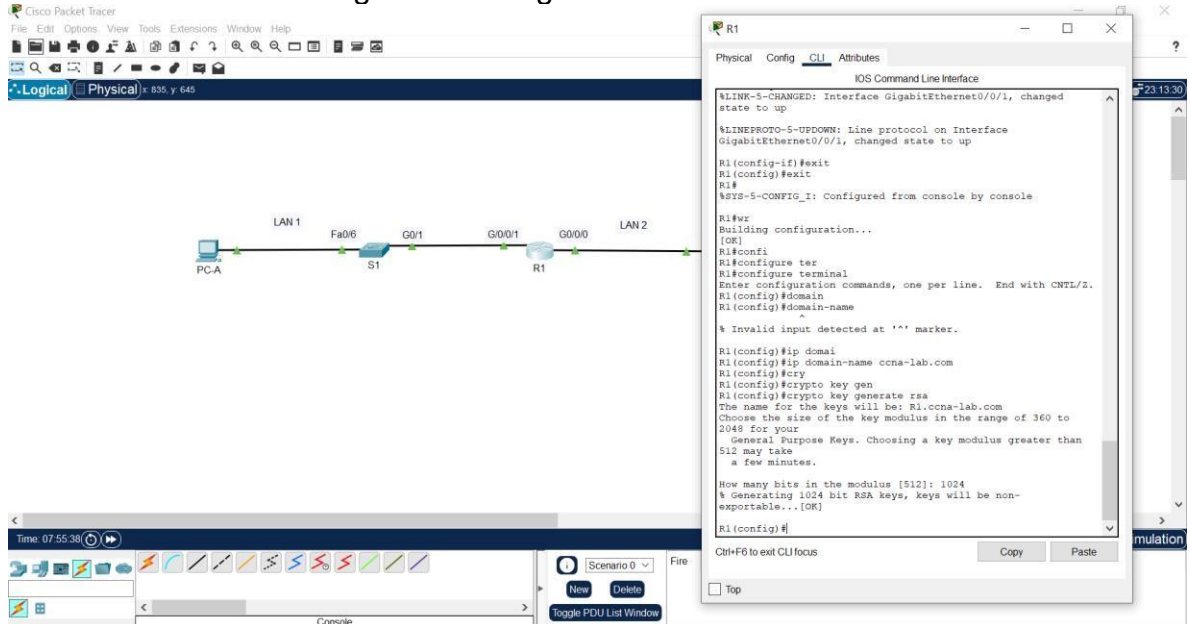
Fuente Autor.

Figura 4. Configuración de Direccinamiento IP



Fuente Autor

Figura 5. Configuración en la NVRAM.



Fuente Autor

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 3. Configuración SW

Tarea	Especificación
Inicio modo privilegiado	Switch>enable
Ingreso Modo configuración	Switch#config t
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
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	S1(config)#line console 0 S1(config-line)#login local

use la base de datos local	S1(config-line)#exit S1(config)#line vty 0 4 S1(config)#line vty 0 15 S1(config-line)#login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	S1(config) line vty 0 4 S1(config-line)#transport input ssh
Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption
Configurar un MOTD Banner	S1(config)#banner motd #colocar el aviso #
Generar una clave de cifrado RSA Módulo de 1024 bits	S1(config)#ip domain-name ccna-lab.com S1(config)#crypto key generate rsa 1024 ok
Configurar la interfaz de administración (SVI) Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento	S1(config)#interface vlan 1 S1(config-if)#ip address 192.168.57.2 255.255.255.128
Configuración del gateway predeterminado Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.	S1(config)#ip default-gateway 192.168.57.1

Fuente Autor

Figura 6 Configuración del SW

The screenshot displays the Cisco Packet Tracer interface. On the left, a network diagram shows a PC (PCA) connected to a switch (S1) via LAN 1. The switch (S1) is connected to a router (R1) via its Fa0/6 interface and the router's G0/0/1 interface. The router (R1) has its G0/0/0 interface connected to the switch's G0/0/0 interface. On the right, the CLI window for switch S1 is open, showing the following configuration commands:

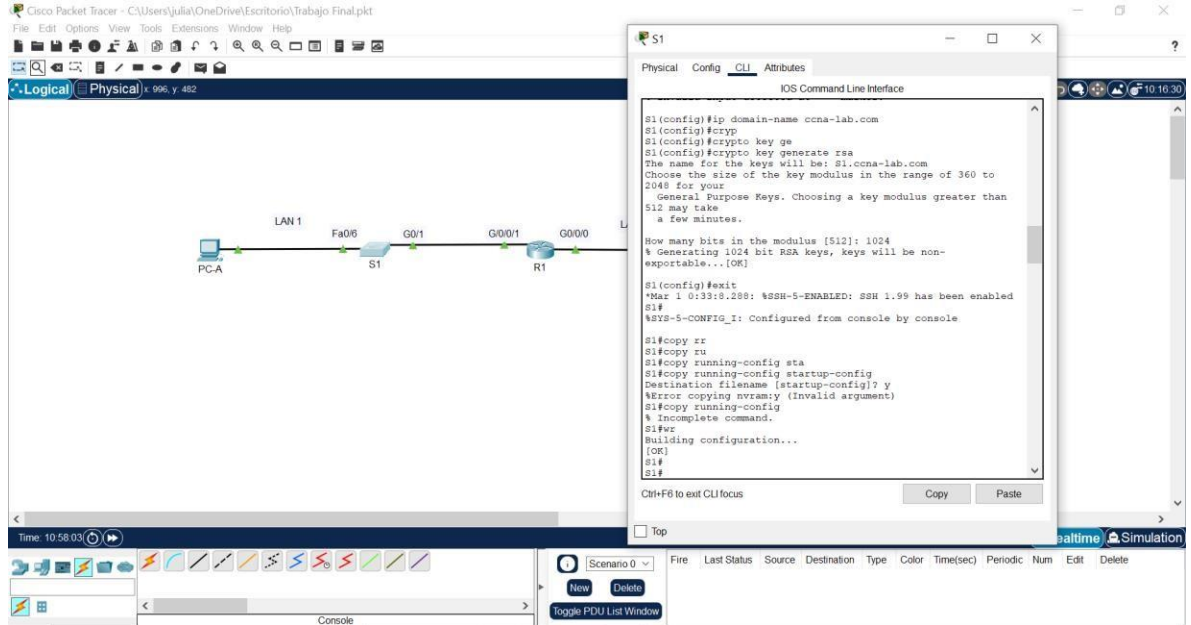
```

S1>conf t
Switch#configure termi
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip doma
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable passw
S1(config)#enable secret ciscoenpass
S1(config)#enable se
S1(config)#enable secret ciscoenpass
S1(config)#line con
S1(config)#line console 0
S1(config-line)#pas
S1(config-line)#password ciscoenpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#user
S1(config)#username admin pas
S1(config)#username admin password adminpass
S1(config)#line console 0
S1(config-line)#login local
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#ser
S1(config)#service pas
S1(config)#service password-encryption
S1(config)#banner mo
S1(config)#banner motd # PELIGRO TRABAJO FINAL JULIAN ANGEL #

```

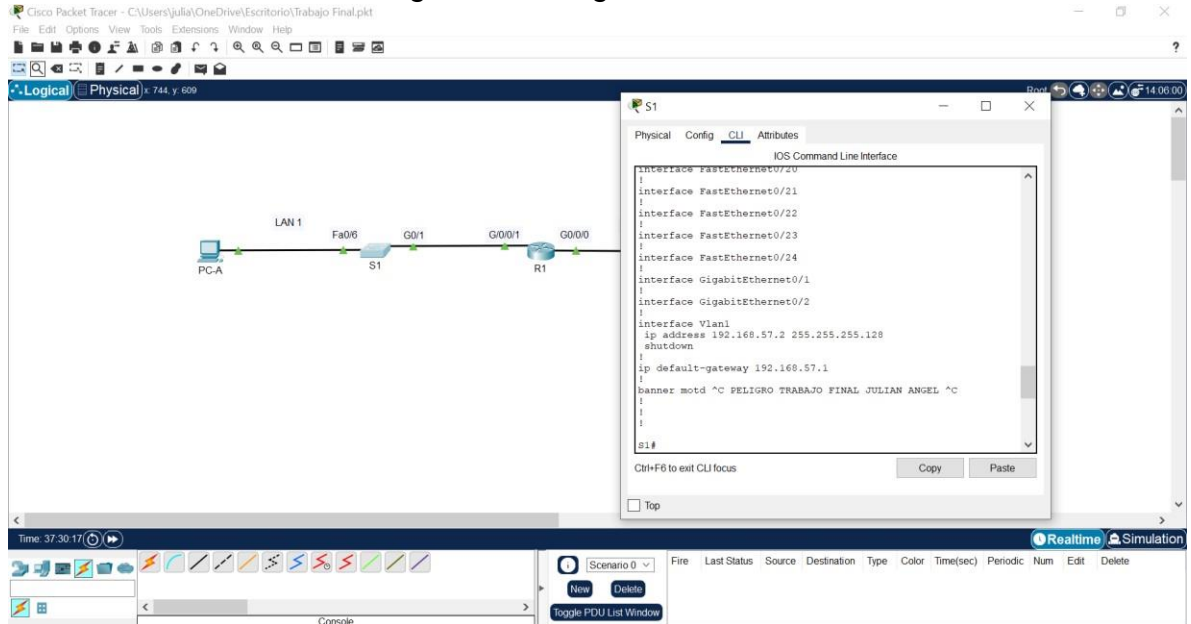
Fuente Autor

Figura 7. Configuración VTY



Fuente Autor

Figura 8. Configuración IP SW



Fuente Autor

## Paso 2. Configurar los equipos de la red LAN

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

Tabla 4. Configuración PC-A

PC-A Network Configuración	
Descripción	FastEthernet 0
Dirección física	0009.7C67.5B20
Dirección IP	192.168.57.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.57.1

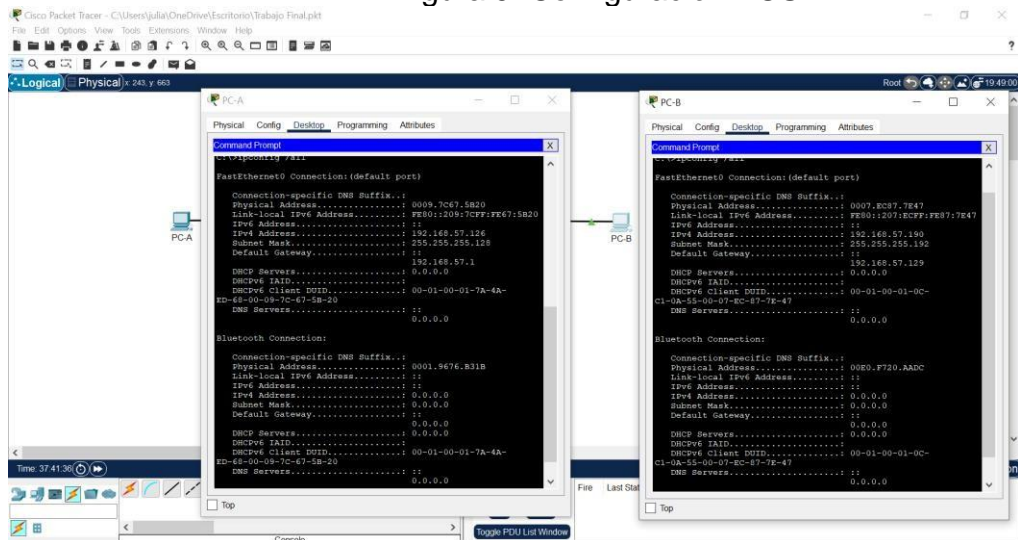
Fuente Autor

Tabla 5. Configuración PC-B

PC-B Network Configuración	
Descripción	FastEthernet 0
Dirección física	0007.EC87.7E47
Dirección IP	192.168.57.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.57.129

Fuente Autor

Figura 9. Configuración PCS



Fuente Autor



### Paso 3. Pruebas de Configuración

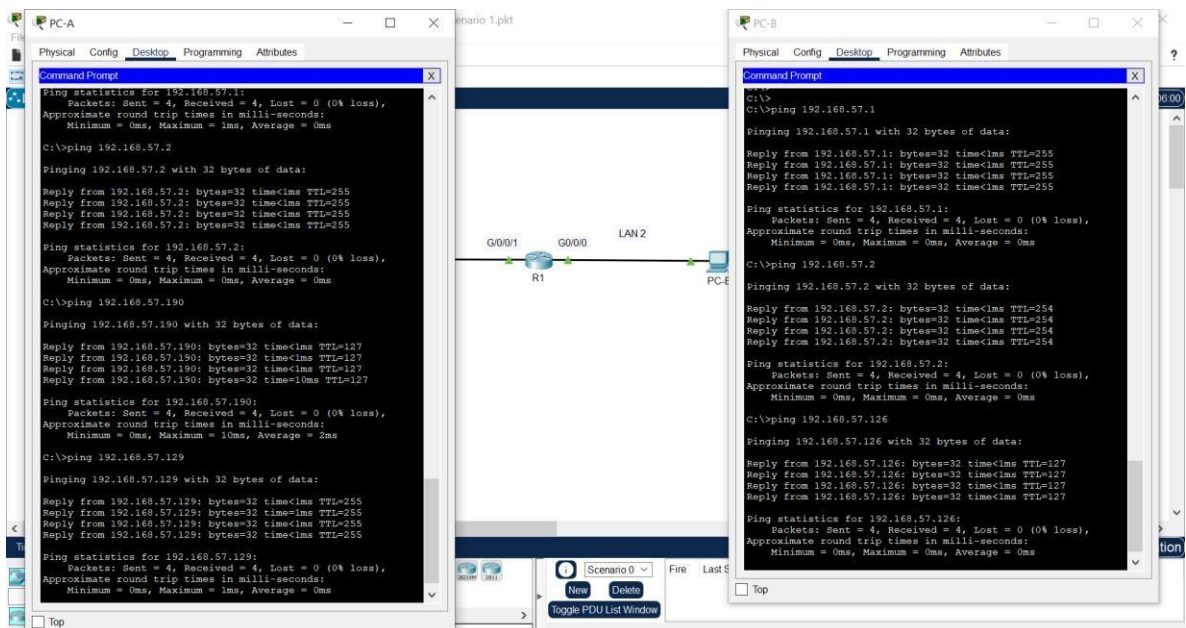
#### A. Prueba de conexión PC-A

```
Ping 192.168.57.1  
Ping 192.168.57.2  
Ping 192.168.57.190  
Ping 192.168.57.129
```

#### B. Prueba de conexión PC-B

```
Ping 192.168.57.1  
Ping 192.168.57.2  
Ping 192.168.57.126
```

Figura 10. Pruebas De Conectividad



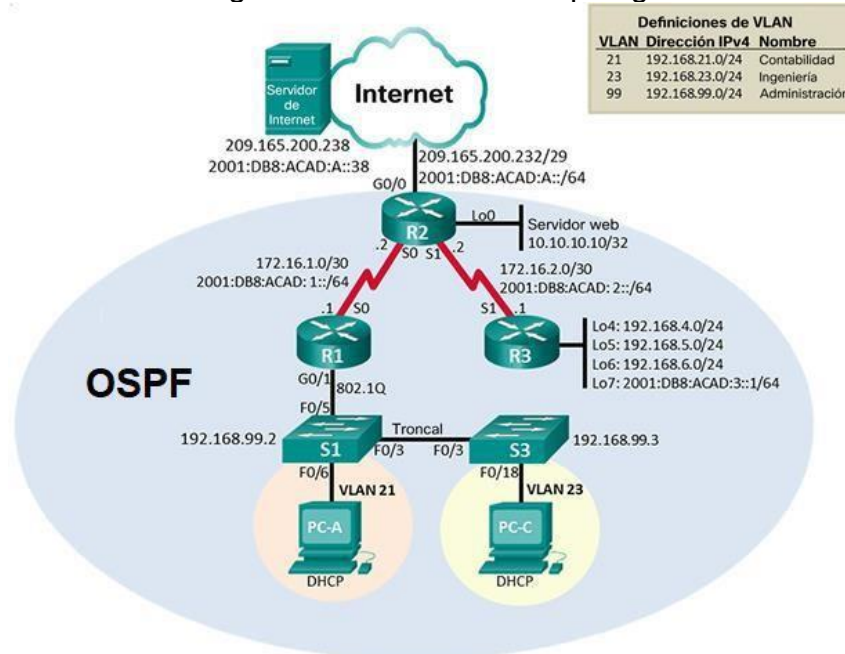
Fuente Autor



## Escenario 2

Escenario: 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 11. Solicitud De Topología



Fuente de guía de actividades

### 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 6 Eliminar Configuración y volver a cargar

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config

Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch#erase startup-config
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch#show flash

Fuente Autor

## Parte 2: Configurar los parámetros básicos de los dispositivos

### Paso 1: Configurar la computadora de Internet

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

Tabla 7 Direccionamiento

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente Autor

**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.

Tabla 8 Configurar R1

Elemento O Tarea De Configuración	Especificación
Desactivar la búsqueda DNS	no ip domain lookup
Nombre del router	R1
Contraseña de exec privilegiado cifrada	enable secret class
Contraseña de acceso a la consola	line console 0 password cisco
Contraseña de acceso Telnet	line vty 0 15 password cisco
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interface Serial S0/0/0	<pre>R1(config)#inter s0/0/0 R1(config-if)#description Conexion hacia el 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 shut</pre>
Rutas predeterminadas	<pre>R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0 R1(config)#</pre>

Fuente Autor

**Nota:** Todavía no configure G0/1.

### Paso 3: Configurar Básica R2

La configuración del R2 incluye las siguientes tareas:

Tabla 9. Configuración R2

Elemento O Tarea De Configuración	Especificación
Desactivar la búsqueda DNS	<pre>Router&gt;enable Router#config t Router(config)#no ip domain-lookup</pre>
Nombre del router	<pre>Router(config)#hostname R2</pre>
Contraseña de exec privilegiado cifrada	<pre>R2(config)#enable secret class</pre>
Contraseña de acceso a la consola	<pre>R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit</pre>
Contraseña de acceso Telnet	<pre>R2(config)#line vty 0 15 R2(config-line)#password cisco R2(config-line)#login R2(config-line)#</pre>
Cifrar las contraseñas de texto no cifrado	<pre>service password-encryption</pre>
Habilitar el servidor HTTP	Comando no soportado por Packet Tracer
Mensaje MOTD	<pre>#banner motd #Se prohíbe el acceso no autorizado! #</pre>
Interfaz S0/0/0	<pre>R2(config)#inter s0/0/0 R2(config-if)#description Conexion hacia el R1</pre>

	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 S0/0/1	R2(config)#interface s0/0/1 R2(config-if)#description Conexion Hacia R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shutdown R2(config-if)#
Interfaz G0/0 (simulación de Internet)	R2#config t R2(config)#interface g0/0 R2(config-if)#description Conexion Hacia 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)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Simulacion de servidor WEB R2(config-if)#
Ruta predeterminada	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0 R2(config)#

Fuente Autor

#### Paso 4: Configuración Básica R3

La configuración del R3 incluye las siguientes tareas:

Tabla 10. Configuración R3

Elemento O Tarea De Configuración	Especificación
Desactivar la búsqueda DNS	Router#config t 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 vty 0 15 R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado!#
Interfaz S0/0/1	R3(config)#interface s0/0/1 R3(config-if)#description Conexion Hacia R2 R3(config-if)#ip address 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no shutdown
Interfaz loopback 4	R3(config)#interface loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#interface loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0
Interfaz loopback 6	R3(config)#interface loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config)#interface loopback 7 R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 serial0/0/1 R3(config)#ipv6 route ::/0 serial0/0/1

Fuente Autor

### Paso 5: Configuración Básica S1

La configuración del S1 incluye las siguientes tareas:

Tabla 11. Configuración S1

Elemento O Tarea De Configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t 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 vty 0 15 S1(config-line)#password cisco S1(config-line)#login
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 Autor

### Paso 6: Configuración Básica S3

La configuración del S3 incluye las siguientes tareas:

Tabla 12. Configuración S3

Elemento O Tarea De Configuración	Especificación
Desactivar la búsqueda DNS	Switch>enable Switch#config t 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 vty 0 15 S3(config-line)#password cisco S3(config-line)#login
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 Autor

### 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.

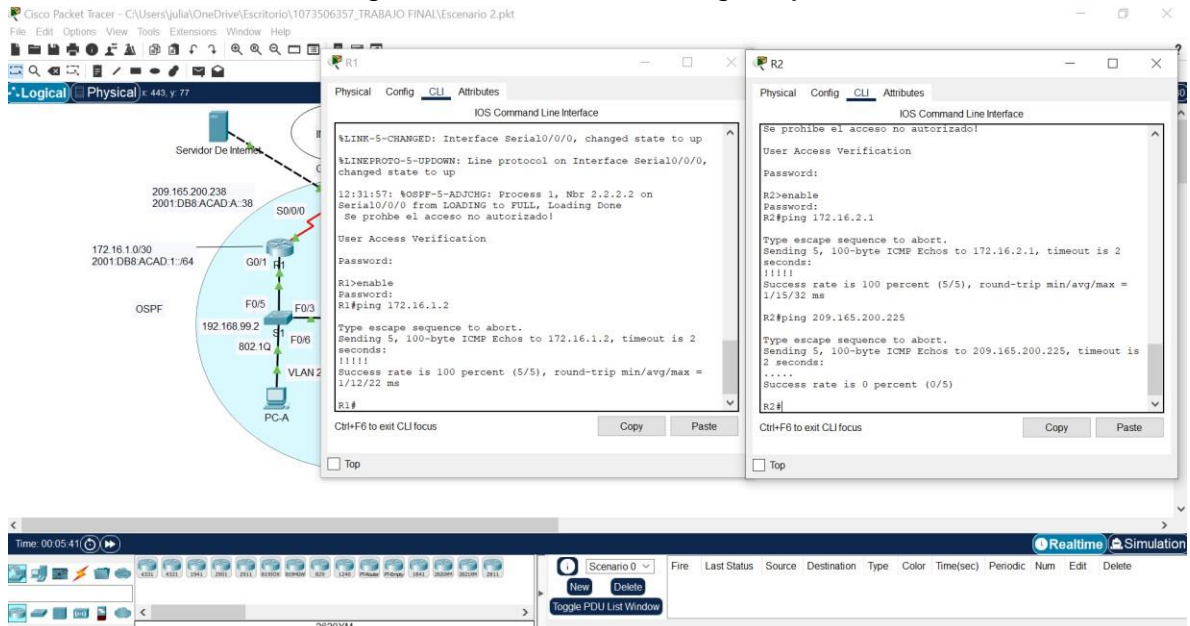
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 13. Respuestas a Ping

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Se Pudo
R2	R3, S0/0/1	172.16.2.1	Se Pudo
PC de Internet	Gateway predeterminado	209.165.200.225	No Pudo

Fuente Autor

Figura 12. Pruebas De Ping R1 y R2



Fuente Autor

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

#### Paso 1: Configuración del Crear VLAN S1

La configuración del S1 incluye las siguientes tareas:

##### A. Crear La Base De Datos De Vlan

S1#config t --- Ingreso Modo configuración

S1(config)#vlan 21 --- Ingreso modo configuracion VLAN 21

S1(config-vlan)#name Contabilidad --- Nombrar Vlan

S1(config-vlan)#vlan 23 --- Ingreso modo configuracion VLAN 26

S1(config-vlan)#name Ingenieria --- Nombrar Vlan

S1(config-vlan)#vlan 99 --- Ingreso modo configuracion VLAN 99

S1(config-vlan)#name administración --- Nombrar Vlan

### **B. Asignar La Dirección Ip De Administración.**

S1(config)#interface vlan 99 --- Ingreso modo configuración VLAN 99  
S1(config-if)#ip address 192.168.99.2 255.255.255.0 --- Configuración de direccionamiento sobre la vlan  
S1(config-if)#no shut --- Activar la interface

### **C. Asignar El Gateway Predeterminado**

S1(config)#ip default-gateway 192.168.99.1 --- establece un Gateway predeterminado en el dispositivo

### **D. Forzar El Enlace Troncal En La Interfaz F0/3**

S1(config)#interface f0/3 --- Ingreso a la interface  
S1(config-if)#switchport mode trunk --- Establecer la interface en modo troncal  
S1(config-if)#switchport trunk native vlan 1 --- Especifica la vlan nativa para enlaces troncales

### **E. Forzar El Enlace Troncal En La Interfaz F0/5**

S1(config)#interface f0/5 --- Ingreso a la interface  
S1(config-if)#switchport mode trunk --- Establecer la interface en modo troncal  
S1(config-if)#switchport trunk native vlan 1 --- Especifica la vlan nativa para enlaces troncales

### **F. Configurar El Resto De Los Puertos Compuertos De Acceso**

S1(config)#interface range f0/1-2,f0/4,f0/6-24,g0/1-2 --- Selecciona las interfaces a la vez en rango que se requiera  
S1(config-if-range)#switchport mode Access --- se establece el modo acceso en las interfaces seleccionadas

### **G. Asignar F0/6 A La Vlan 21**

S1(config)#interface f0/6 --- Ingreso a la interface  
S1(config-if)#switchport access vlan 21 --- se asigna la interface a la vlan

### **H. Apagar Todos Los Puertos Sin Usar**

S1(config)#interface range f0/1-2,f0/4,f0/7-24,g0/1-2 --- Selecciona las interfaces a la vez en rango que se requiera  
S1(config-if-range)#shutdown --- se apagan las interfaces seleccionadas



## Paso 2: Configuración VLAN del S3

La configuración del S3 incluye las siguientes tareas:

Tabla 14. Configuración VLAN

Elemento O Tarea De Configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan 21 S3(config-vlan)#name Contabilidad --- Nombrar Vlan S3(config-vlan)#vlan 23 S3(config-vlan)#name Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administración
Asignar la dirección IP de administración	S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0
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
Configurar el resto de los puertos como puertos de acceso	S3(config-if)#interface range f0/1-2,f0/4- 24,g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21	S3(config)#interface f0/18 S3(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	S3(config)#interface range f0/1-2,f0/4- 17,f0/19-24,g0/1-2 S3(config-if-range)#shutdown

Fuente Autor

## Paso 3: Configurar Subinterfaz R1

Las tareas de configuración para R1 incluyen las siguientes:

### A. Configurar La Subinterfaz 802.1q .21 Eng0/1

R1(config)#interface g0/1.21 --- Ingresar al modo de configuración de interface virtual

R1(config-subif)#description LAN Contabilidad --- Se añade una etiqueta a la interface

R1(config-subif)#encapsulation dot1q 21 --- habilita 802.1Q y asocia una VLAN específica a la subinterfaz.

R1(config-subif)#ip address 192.168.21.1 255.255.255.0 --- Configuración de direccionamiento sobre la interface

### **B. Configurar La Subinterfaz 802.1q .23 Eng0/1**

R1(config)#interface g0/1.23 --- Ingresar al modo de configuración de interface virtual

R1(config-subif)#description LAN Ingenieria --- Se añade una descripción o etiqueta a la interface

R1(config-subif)#encapsulation dot1q 23--- habilita 802.1Q y asocia una VLAN específica a la subinterfaz.

R1(config-subif)#ip address 192.168.23.1 255.255.255.0 --- Configuración de direccionamiento sobre la interface

### **C. Configurar La Subinterfaz 802.1q .99 Eng0/1**

R1(config-subif)#interface g0/1.99 --- Ingresar al modo de configuración de interface virtual

R1(config-subif)#description LAN Administración --- Se añade una descripción o etiqueta a la interface

R1(config-subif)#encapsulation dot1q 99 --- habilita 802.1Q y asocia una VLAN específica a la subinterfaz.

R1(config-subif)#ip address 192.168.99.1 255.255.255.0 --- Configuración de direccionamiento sobre la interface

### **d. Activar la interfaz G0/1**

R1(config-subif)#interface g0/1 --- Ingresar al modo de configuración de interface

R1(config-if)#no shutdown --- Activar la interface

### **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.

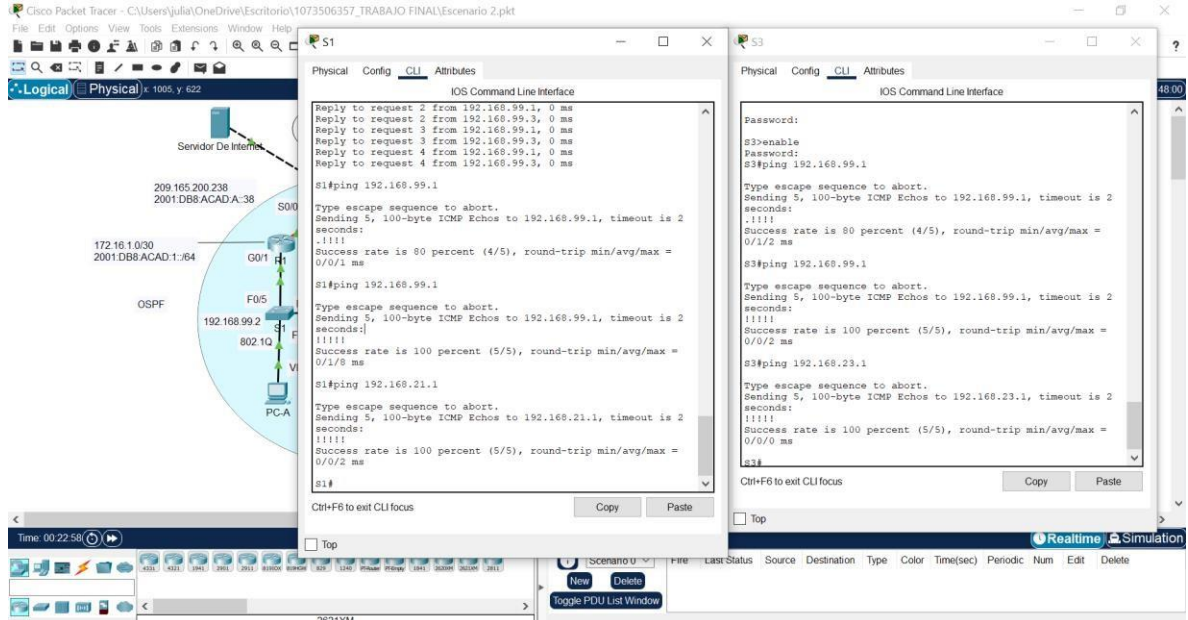
Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 15. Verificación de Conectividad

<b>Desde</b>	<b>A</b>	<b>Dirección IP</b>	<b>Resultados de ping</b>
S1	R1, dirección VLAN 99	192.168.99.1	RESPONDE
S3	R1, dirección VLAN 99	192.168.99.1	RESPONDE
S1	R1, dirección VLAN 21	192.168.21.1	RESPONDE
S3	R1, dirección VLAN 23	192.168.23.0	RESPONDE

Fuente Autor

Figura 13. Pruebas De Ping Desde el Switch S1 y S3



Fuente Autor

## Parte 4: Configurar el protocolo de routing dinámico OSPF

### Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente
- Establecer todas las interfaces LAN como pasivas
- Desactive la sumarización automática

R1(config)#router ospf 1 --- Habilitar enrutamiento OSPF en el router

R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 --- habilitar el OSPF en las redes

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 192.168.24.0 0.0.0.255 area 0

R1(config-router)#passive-interface g0/1.21 --- Evita la transmisión de mensajes de routing a través de la interface seleccionada

R1(config-router)#passive-interface g0/1.23

R1(config-router)#passive-interface g0/1.99

El Comando auto summary no puede ser soportado para OSPF

### **Paso 2: Configurar OSPF en el R2**

La configuración del R2 incluye las siguientes tareas:

- a. Configurar OSPF área 0**
- b. Anunciar las redes conectadas directamente**
- c. Establecer todas las interfaces LAN (loopback) como pasivas**
- d. Desactive la sumarización automática**

R2(config)#router ospf 1 --- Habilitar enrutamiento OSPF en el router

R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 --- Habilitar el OSPF en las redes

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

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0

R2(config-router)#network 10.10.10.10 0.0.0.0 area 0

R2(config-router)#passive-interface loopback 0 --- Evita la transmisión de mensajes de routing a través de la interface seleccionada

El Comando auto summary no puede ser soportado para OSPF

### **Paso 3: Configurar OSPFv3 en el R2**

La configuración del R3 incluye las siguientes tareas:

- a. Configurar OSPF área 0**
- b. Anunciar las redes IPv4 conectadas directamente**
- c. Establecer todas las interfaces LAN IPv4 (loopback) como pasivas**
- d. Desactive la sumarización automática**

R3(config)#router ospf 1 --- Habilitar enrutamiento OSPF en el router

R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 --- Habilitar el OSPF en las redes

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

R3(config-router)#passive-interface loopback 4 --- Evita la transmisión de mensajes de routing a través de la interface seleccionada

R3(config-router)#passive-interface loopback 5

R3(config-router)#passive-interface loopback 6

R3(config-router)#

#### 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 16. Verificación 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?	R1#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R1#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R1#show run   section ospf router ospf 1

Fuente Autor

#### Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración el R1 como servidor de DHCP para las VLAN

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.	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com

Fuente Autor

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

La configuración del R2 incluye las siguientes tareas:

### **A. Crear Una Base De Datos Local Con Unacuenta De Usuario**

R2(config)#username webuser privilege 15 secret cisco12345 --- Indica el nombre del usuario, el nivel de privilegio del usuario y una clave secreta encriptada.

### **B. Habilitar El Servicio Del Servidor Http**

Comando no soportado

### **C. Configurar El Servidor Http Para Utilizar La Base De Datos Local Para La Autenticación**

Comando no soportado

### **D. Crear Una Nat Estática Al Servidor Web.**

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237 --- Establece la traducción estática entre una dirección local interna y una dirección global interna.

### **E. Asignar La Interfaz Interna Y Externa Para La Nat Estática**

R2(config)#interface g0/0 --- Ingreso a la interface

R2(config-if)#ip nat outside --- Identificar la interfaz como externa.

R2(config-if)#interface s0/0/0 --- Ingreso a la interface

R2(config-if)#ip nat inside --- Identificar la interfaz como interna

R2(config-if)#interface s0/0/1

R2(config-if)#ip nat inside

### **F. Configurar La Nat Dinámica Dentro De Unaacl 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

R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 --- se crea la lista y posteriormente se asocia a una interfaz entrante o saliente.

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

### G. Defina El Pool De Direcciones Ip Públicasutilizables.

R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248 --- Definir el conjunto de direcciones globales que se debe usar para la traducción.

### H. Definir La Traducción De Nat Dinámica

R2(config)#ip nat inside source list 1 pool INTERNET --- Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción dinámica de origen.

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

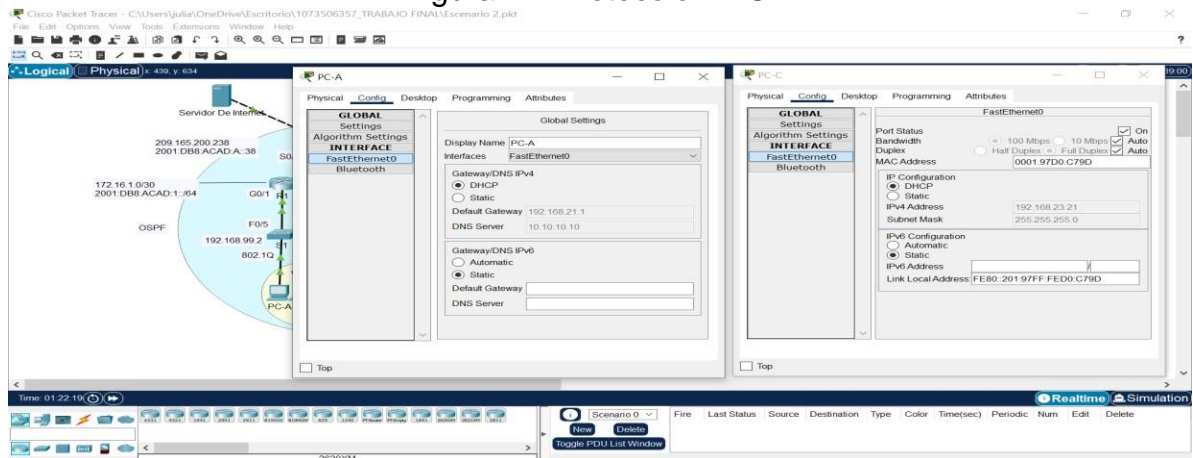
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 18. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Si se pudo
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Si se pudo
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	No se pudo
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	No se pudo

Fuente Autor

Figura 14. Protocolo DHCP



Fuente Autor

## Parte 6: Configurar NTP

Tabla 19. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	R2#clock set 9:00:00 5 march 2016
Configure R2 como un maestro NTP.	R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	R1(config)#ntp server 172.16.1.2
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1(config)#ntp update-calendar
Verifique la configuración de NTP en R1.	R1#show ntp associations

Fuente Autor

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

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

#### A. 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 --- se asigna el nombre a la ACL standar

R2(config-std-nacl)#permit host 172.16.1.1 --- Se establece la dirección R1 permitir conexión Telnet a R2

#### B. Aplicar La Acl Con Nombre A Las Líneas Vty

R2(config)#line vty 0 15

R2(config-line)#access-class ADMIN-MGT in

#### C. Permitir Acceso Por Telnet A Las Líneas De Vty

R2(config-line)#transport input telnet --- Permite las conexiones Telnet en las líneas vty

#### D. Verificar Que La Acl Funcione Como Se Espera

Prueba de conexión desde r1 a r2 via telnet

Se intenta realizar conexión desde el R3 pero es rechazada por la lista de Acceso





## CONCLUSIONES

En esta actividad se describe la configuración básica de una red de telecomunicaciones en el entorno virtual de la plataforma cisco Packet Tracer, herramienta funcional para el diseño y configuración de Redes, la cual permite simular, visualizar y evaluar modelos de redes virtuales y realizar la configuración de los diferentes dispositivos que intervienen en una Red.

En el primer escenario se trabajó en el diseño de una red pequeña, que consta de un Router, un Switch y dos equipos de cómputo, donde el objetivo fue establecer un escenario LAN para realizar el análisis del comportamiento de diferentes protocolos y métricas de enrutamiento entre los dispositivos, así como brindar direccionamiento y servicios de seguridad básicos para el funcionamiento óptimo de todos los equipos. En el escenario número 2 se elabora un enrutamiento OSPF, donde se le da una solución a un diseño propuesto, se realiza la topología solicitada y se arma una troncal entre los switches, se interconectan tres routers y se realiza la protección de cada dispositivo, se habilitan interfaces aumentando la seguridad de los dispositivos y finalmente se realiza configuración y prueba de las ACL.

## BIBLIOGRAFIA

Teaching with Packet Tracer. (2020, 8 mayo). Networking Academy. Recuperado 5 de julio de 2022, de <https://www.netacad.com/es/courses/packet-tracer/teaching>

Marcelo. (2020, 4 julio). IPv4. CCNA Desde Cero. Recuperado 5 de julio de 2022, de <https://ccnadesdecero.com/curso/ipv4/>

LAN — Red de área local: la tecnología de un vistazo. (2020, 2 marzo). IONOS Digitalguide. Recuperado 5 de julio de 2022, de <https://www.ionos.es/digitalguide/servidores/know-how/lan/>

Preguntas frecuentes sobre la traducción de direcciones de red (NAT). (2022, 16 marzo). Cisco. Recuperado 15 de mayo de 2022, de [https://www.cisco.com/c/es\\_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html?dtid=osscdc000283](https://www.cisco.com/c/es_mx/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html?dtid=osscdc000283)

Jiménez, J. (2021, 25 septiembre). NTP: en qué consiste este protocolo de red. RedesZone. Recuperado 5 de julio de 2022, de <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-ntp/>

Marcelo. (2020, 10 agosto). Introducción a OSPF. CCNA Desde Cero. Recuperado 5 de julio de 2022, de <https://ccnadesdecero.com/curso/ospf/>

Host. (s. f.). Sistemas Master. Recuperado 15 de mayo de 2022, de <https://sistemas.com/host.php>

¿Qué es un router? - Definición y usos. (2021, 18 octubre). Cisco. Recuperado 5 de julio de 2022, de [https://www.cisco.com/c/es\\_mx/solutions/small-business/resource-center/networking/what-is-a-router.html](https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-a-router.html)

El Subnetting para sacar el máximo partido a tu red. (2019, 16 agosto). IONOS Digitalguide. Recuperado 15 de mayo de 2022, de <https://www.ionos.es/digitalguide/servidores/know-how/subnetting-como-funcionan-las-subredes/#:%7E:text=ya%20en%201985.-,%C2%BFQu%C3%A9%20es%20el%20subnetting%3F,sin%20hacerlo%20p%C3%BAblico%20en%20Internet.>

¿Cómo funciona un switch? (2021, 22 septiembre). Cisco. Recuperado 15 de mayo de 2022, de [https://www.cisco.com/c/es\\_mx/solutions/small-business/resource-center/networking/network-switch-how.html?dtid=osscdc000283](https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/network-switch-how.html?dtid=osscdc000283)