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

LEONARDO MARTINEZ AGUIRRE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA DE SISTEMAS
FLORENCIA
2022

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

LEONARDO MARTINEZ AGUIRRE

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 DECIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERIA DE SISTEMAS
FLORENCIA
2022

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

FLORENCIA, 26 de junio de 2022

## AGRADECIMIENTOS

Mis agradecimientos primero a dios por permite la oportunidad de culminar un proyecto de vida, de igual forma a mi familia especialmente a mi madre y padre que me han apoyado para culminar mi carrera.

## CONTENIDO

## LISTA DE TABLAS

## LISTA DE FIGURAS

## RESUMEN

Con el presente trabajo se busca generar una solución a los escenarios planteados para el trabajo de diplomado CISCO, dado como opción de grado para obtener el título de Ingeniero de Sistemas, implementando la estrategia de aprendizaje basada en escenarios mediante la utilización de la plataforma CISCO donde se desarrollaran los ejercicios generando el enrutamiento de las redes haciendo uso del simulador Packet Tracer mediante el empleo de comandos para realizar la respectiva configuración de las subredes e interfaz de los dispositivos a enlazar verificando la conmutación entre los host de extremo a extremo donde se evidencia de forma electrónica la interconexión de las subredes solicitadas en los dispositivos empleados.


Palabras clave: Broadcast, Swich, Networking, Hosts, Vlan.

## ABSTRACT

With the present work, we seek to generate a solution to the scenarios proposed for the CISCO diploma work, given as a degree option to obtain the title of Systems Engineer, implementing the learning strategy based on scenarios through the use of the CISCO platform where The exercises will be developed generating the routing of the networks using the Packet Tracer simulator by using commands to carry out the respective configuration of the subnets and interface of the devices to be linked, verifying the switching between the hosts from end to end where it is evidence of electronically the interconnection of the requested subnets in the devices used.


Keywords: Broadcast, Swich, Networking, Hosts, Vlan.

# INTRODUCCION

Con el pasar de los años la evolución de los sistemas de comunicación ha presentado pasos avanzados gracias al desarrollo e implementación de nuevos dispositivos e implantación de redes que han permitido la conexión en línea a grandes velocidades de transmisión dejando atrás las conexiones de baja calidad que se tenían algunos años para descargar un archivo o para iniciar una video llamada, más sin embrago es importante mencionar que todos estos recursos se dan gracias a la implementación de conexiones que permiten enlazar millones de host al mismo tiempo dado al orden y direccionamientos basados en protocolos de comunicación.

De acuerdo a lo anterior el presente trabajo pretende introducirse al ámbito de las comunicaciones con el fin analizar, conocer y desarrollar actividades colaborativas, individuales que permitirán afianzar cada día el conocimiento del estudiante mediante la metodología de aprendizaje en escenarios realizando el uso de herramientas de software que permitan interactuar de forma directa con equipos de comunicación y sus diferentes características de hardware.

Dentro de este orden de ideas podemos mencionar el análisis y solución de los escenarios uno y dos que se presentaran en el desarrollo del trabajo como opción de grado con el fin de aplicar los conocimientos adquiridos durante el desarrollo de los trabajos donde se empleara el direccionamiento de protocolo IP v 4, realizando el uso de subredes para la conexión de los diferentes dispositivos y el empleo de los comandos de configuración.

Finalmente es importante mencionar el complemento del trabajo dado a la formación académica generada por la plataforma de CISCO, para el proyecto de grado con los niveles de formación del curso CCNA1, que permitirán obtener conocimientos de Ethernet, redes, seguridad, capas de aplicación, protocolos y modelos como OIS y TCP /IP, a medida que avanza el curso.

## DESARROLLO

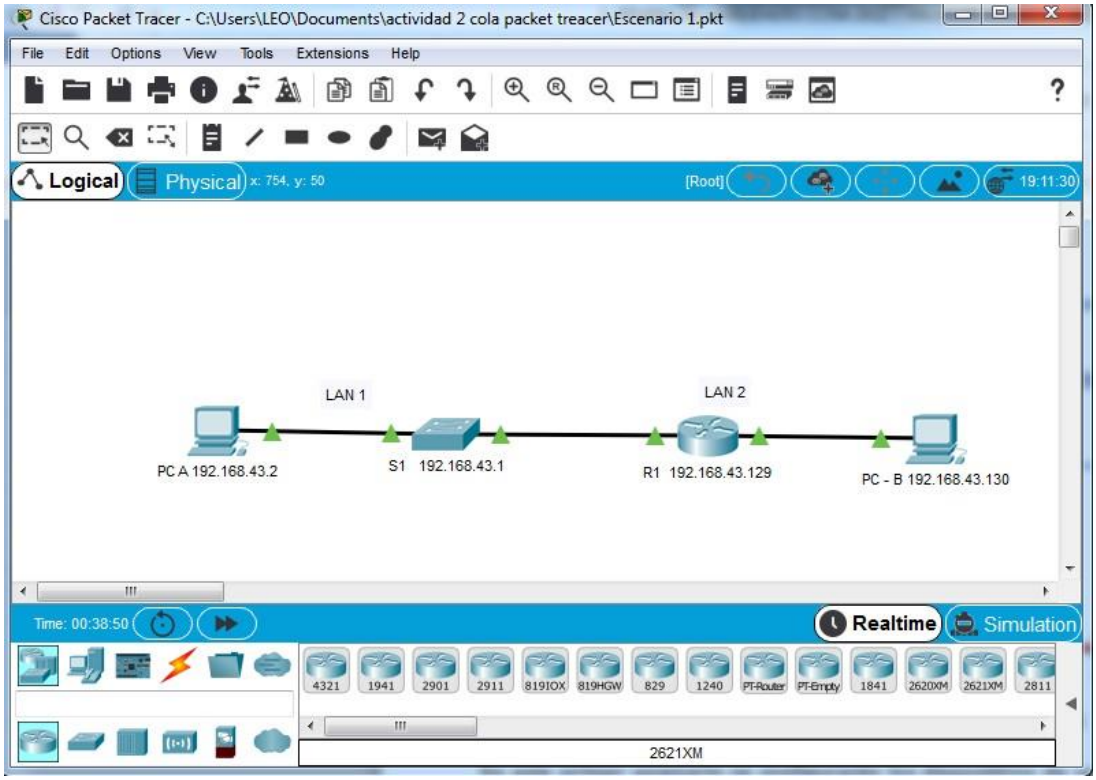
## 1. ESCENARIO 1

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

Figura 1. Topología Escenario




Fuente: Autoría propia en Packet Treacer

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

**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 tablade direccionamiento.

Cada estudiante tomará el direccionamiento 192.168.X.0 donde X corresponde a los últimos dos dígitos desu cédula.

Nota:

Para el desarrollo del direccionamiento ip según el requerimiento planteado tomamos la dirección IP 192.168.X.0 donde la x será reemplazada por los dos últimos dígitos de mi cedula quedando así: 192.168.43.0, siendo esta dirección clase TIPO C, según las dos subredes que nos están solicitando se toman dos bits más de la máscara de red es decir del ultimo octeto de toman estos dos prestados para asignarle los host de las subredes dado a esto la primera subred de 100 host seria 255.255.255.128 y para la segunda subred de 50 host seria 255.255.255.192.

Como se mencionaba en la nota anterior verificamos en una pequeña tabla la información solicitada.

Figura 2. Subredes Escenario 1

| Subred | Direcciones | Mascara | | 1ra, IP Subred LAN 1 Y LAN 2 | Ultima valida | Broadcast o Difusion | Host por red |
|---|---|---|---|---|---|---|---|
| 1 | 192.168.43.0 | 255.255.255.128 | /25 | 192.168.43.1 | 192.168.43.126 | 192.168.43.127 | 100 |
| 2 | 192.168.43.128 | 255.255.255.192 | /26 | 192.168.43.129 | 192.168.43.190 | 192.168.43.191 | 50 |

Tabla 1. Tabla de direccionamiento escenario 1.

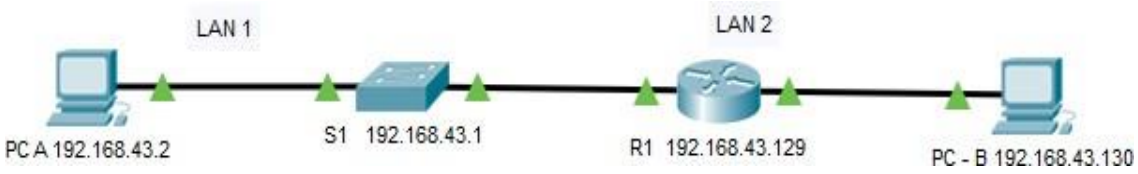
| **Item** | **Requerimiento** |
|---|---|
| Dirección de Red | 192.168.X.0 donde X corresponde a los últimos dosdígitos de mi cédula.<br>192.168.43.0 |
| Requerimiento de host Subred LAN1 | 100 |
| Requerimiento de host Subred LAN2 | 50 |
| R1 G0/0/1 | Primera dirección de host de la subred LAN1<br>192.168.43.1 |
| R1 G0/0/0 | Primera dirección de host de la subred LAN2<br>192.168.43.129 |
| S1 SVI | Segunda dirección de host de la subred LAN1<br>192.168.43.2 |
| PC-A | Última dirección de host de la subred LAN1<br>192.168.43.126 |
| PC-B | Última dirección de host de la subred LAN2<br>192.168.43.190 |

Fuente: Tabla tomada de PDF, **“**PRUEBA DE HABILIDADES CCNA 2022”.

## Parte 3: Configure aspectos básicos

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

Figura 3. Escenario de configuración 1.




Fuente: Autoría propia en Packet Treacer

Paso 1: configurar los ajustes básicos.

Tabla 2. Tabla de configuración para R1.

| **Tarea** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | |
| Nombre del router | R1 |
| Nombre de dominio | ccna-lab.com<br>R1(config)# ip domain-lookup<br>R1(config)# ip domain-name ccna-lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass |
| Establecer la longitud mínima para lascontraseñas | 10 caracteres |

| | |
|---|---|
| Crear un usuario administrativo en la base dedatos local | Nombre de usuario: **admin**<br>Password: **admin1pass** |
| Configurar el inicio de sesión en las líneas VTYpara que use la base de datos local | Línea vty 0 4 |
| Configurar VTY solo aceptando SSH | Line vty aceptando SSH |
| Cifrar las contraseñas de texto no cifrado | service password-encryption |
| Configure un MOTD Banner | Configurar mensaje de restricción al R1 |
| Configurar interfaz G0/0/0 | Establezca la descripción<br>Establece la dirección IPv4.<br>Activar la interfaz. |
| Configurar interfaz G0/0/1 | Establezca la descripción<br>Establece la dirección Ipv4.<br>Activar la interfaz. |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |

Fuente: Tabla tomada de PDF, “PRUEBA DE HABILIDADES CCNA 2022”.

Para la realización de las configuraciones anteriores se ingresa al R1, ejecutando el modo privilegiado.

Figura 4. Desactivar la búsqueda DNS del R1.

**Password**: ingresamos contraseña de acceso a consola

**R1>en**

**Password:** ingresamos contraseña de acceso EXECprivilegiado

**R1>en** ingresamos a modo privilegiado

**R1#conf t** ingresamos a modo configuración

**R1 (config) )# No ip domain-lookup** desactivamos búsqueda de DNS.

```
R1#nslookup
Translating "nslookup"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address

R1#capy
Translating "capy"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address
```

Figura 5. Asignación Nombre a Router 1.

**Password**: ingresamos contraseña de acceso a consola
**R1>en**
**Password:** ingresamos contraseña de acceso EXECprivilegiado
**R1>**
**R1>en** ingresamos a modo privilegiado
**R1#conf t** ingresamos a modo configuración

**R1(config)#hostname R1** Asignamos el nombre al router.

```
R1#show run
Building configuration...

Current configuration : 613 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
```

Fuente: Autoría propia en Packet Treacer

Figura 6. Asignación Nombre de dominio, ccna-lab.com.

**Password**: ingresamos contraseña de acceso a consola
**R1>en**
**Password:** ingresamos contraseña acceso EXECprivilegiado
**R1>**
**R1>en** ingresamos a modo privilegiado
**R1#conf t** ingresamos a modo configuración
**R1(config)# ip domain-lookup** **se genera comandos para**
**R1(config)# ip domain-name ccna-lab.com** **asignar el dominio**

```
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-lookup
R1(config)#ip domain-name ccna-lab.com
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show run
Building configuration...
!
ip domain-name ccna-lab.com
!
!
spanning-tree mode pvst
```

Figura 7. Contraseña cifrada para el modo EXECprivilegiado, “Ciscoenpass”.

**Password**: ingresamos contraseña de acceso a consola
**R1>en**
**Password:** ingresamos contraseña de acceso EXECprivilegiado
**R1>**
**R1>en** ingresamos a modo privilegiado
**R1#conf t** ingresamos a modo configuración
**R1 (config) )#enable password ciscoenpass** asignamos la contraseña
**R1 (config) )#service password-encryption** asignamos cifrado de claves

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#enable password ciscoenpass

Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#exit

!
enable password 7 0822455D0A160019020A1F17
!
!
```

Figura 8. Asignación de Contraseña de consola, " ciscoconpass".

**Password**: ingresamos contraseña de acceso a consola
**R1>en**
**Password:** ingresamos contraseña de acceso EXECprivilegiado
**R1>en** ingresamos a modo privilegiado
**R1#conf t** ingresamos a modo configuración
**Password**: ingresamos contraseña de acceso a consola
**R1>en**
**Password:** ingresamos contraseña acceso EXECprivilegiado
**R1> config t** ingresamos al modo configuración
**R1 (config) )#enable password ciscoconpass** configuramos contrase
**R1 (config) )#line console 0** asignamos la consola
**R1 (config-line )#password ciscoconpass** asignamos la contraseña
**R1 (config-line )#login**

```
!
!
line con 0
 password ciscoconpass
 login
!
```

Fuente: Autoría propia en Packet Treacer

Figura 9. Establecer la longitud mínima para las contraseñas, 10 caracteres.

**Password**: ingresamos contraseña de acceso a consola

**R1>en**

**Password:** ingresamos contraseña de acceso EXECprivilegiado

**R1>en** ingresamos a modo privilegiado

**R1#conf t** ingresamos a modo configuración

**R1(config)# security password min-length 10** se establece longitud

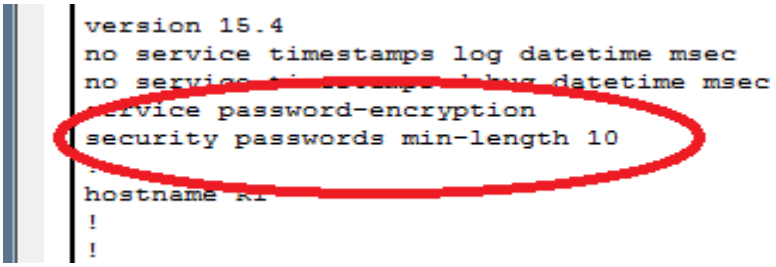



Figura 10. Crear un usuario administrativo en la base de datos local.

**Password: admin1pass, Nombre de usuario: admin**

**R1>en** **ingresamos contraseña de acceso EXECprivilegiado**

**Password:**

**R1#config t.** **ingresamos a modo configuración**

**R1(config)#security password min-length 10** **se realiza configuracion**

**R1(config)#**

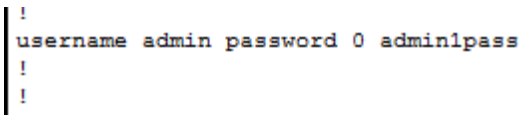


Figura 11. Configurar el inicio de sesión en las líneas VTYpara que use la basede datos local.

```
R1(config)#line vty 0 4
R1(config-line)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

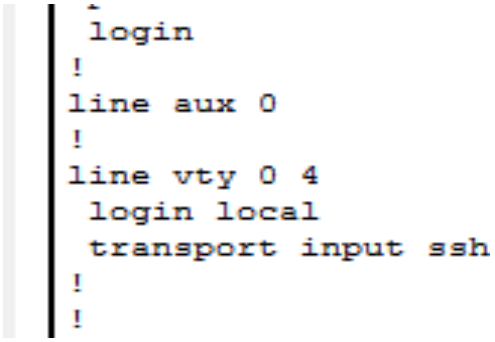



Figura 12. Configurar VTY solo aceptando SSH, se verifican cambios dentro de la configuración del R1.

```
R1(config-line)#transport input ssh
R1(config-line)#exit

R1(config)#
```

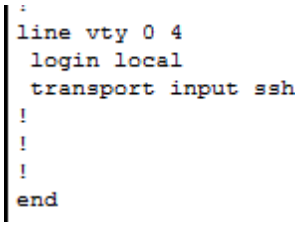


Figura 13. Cifrar las contraseñas de texto no cifrado.

**Se configura el comando** service password-encryption, para encriptar las claves configuradas en el dispositivo.

R1(config)#

R1(config)#service password-encryption

R1(config)#exit

R1#

```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service password-encryption
R1(config)#exit
```

Figura 14. Configure un MOTD Banner. Mensaje de ingreso no configurado.

R1#
R1#config t ingresamos a modo configuración
R1(config)#banner motd "El acceso a R1 esta restringido. Solo personal autorizado"
R1(config)#exit

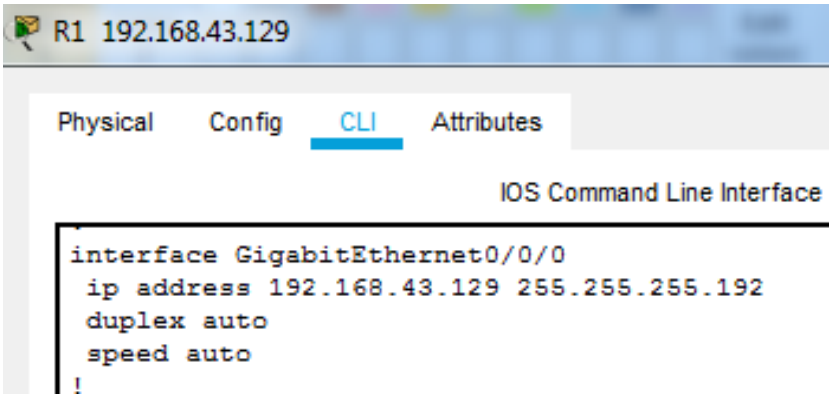
```
ip flow-export version 9
!
!
!
banner motd ^CEl acceso a R1 esta restringido. Solo personal
autorizado^C
!
!
```

Fuente: Autoría propia en Packet Treacer

Figura 15. Configurar interfaz G0/0/0

Se realiza la configuración de la interfaz GibabitEthernet 0/0/0, mediante los comandos en consola, verificando que la información fue registrada.

```
R1>en
Password:
R1#config t
R1(config)#Interface GigabitEthernet0/0/0
R1(config-if)#ip address 192.168.43.129 255.255.255.192
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#exit
R1#
```




Fuente: Autoría propia en Packet Treacer

Figura 16. Configurar interfaz G0/0/1

se realiza la configuración de la interfaz GibabitEthernet 0/0/1, mediante los comandos en consola, verificando que la información fue registrada.

```
R1#config t
R1(config)#Interface GigabitEthernet0/0/1
R1(config-if)#ip address 192.168.43.1 255.255.255.128
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#exit
R1#
```

```
 speed auto
!
interface GigabitEthernet0/0/1
 ip address 192.168.43.1 255.255.255.128
 duplex auto
 speed auto
!
```

Figura 17. Generar una clave de cifrado RSA, Módulo de 1024 bits.

R1(config)#

R1(config)#crypto key generate rsa

% You already have RSA keys defined named R1.ccna-lab.com .

% Do you really want to replace them? [yes/no]: yes

The name for the keys will be: R1.ccna-lab.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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.
-
  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]
```

**Las tareas de configuración de S1 incluyen lo siguiente:**

Tabla 3. Configuración de S1.

| Tarea | Especificación |
|---|---|
| Desactivar la búsqueda DNS. | |
| Nombre del switch | S1>en<br>S1#config t<br>S1(config)#hostname S1 |
| Nombre de dominio | ccna-lab.com<br><br>S1(config)#ip domain-lookup<br>S1(config)#ip domain-name ccna- lab.com |
| Contraseña cifrada para el modo EXEC privilegiado | ciscoenpass |
| Contraseña de acceso a la consola | ciscoconpass |
| Crear un usuario administrativo en la base de datos local | Nombre de usuario: admin<br><br>Password: admin1pass |
| Configurar el inicio de sesión en las líneas VTY para queuse la base de datos local | |
| Configurar las líneas VTY para que acepten únicamentelas conexiones SSH | |
| Cifrar las contraseñas de texto no cifrado | |
| Configurar un MOTD Banner | |
| Generar una clave de cifrado RSA | Módulo de 1024 bits |

| | |
|---|---|
| Configurar la interfaz de administración (SVI) | Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento |
| Configuración del gateway predeterminado | .<br><br>Se configura dirección Gateway 192.168.43.127 |

Fuente: Tabla tomada de PDF, “PRUEBA DE HABILIDADES CCNA 2022”.

De acuerdo a la tabla anterior se realizara la configuración para **S1**.

Figura 18. Desactivar la búsqueda DNS.

```
S1>en
S1#config t
S1(config)#no ip domain-lookup
```

```
S1>
S1>en
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#
S1(config)#
```

Fuente: Autoría propia en Packet Treacer

Figura 19. Nombre del switch y nombre de  dominio ccna-lab.com.

```
S1>en
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#hostname S1
S1(config)#ip domain-lookup
S1(config)#ip domain-name ccna-lab.com
```

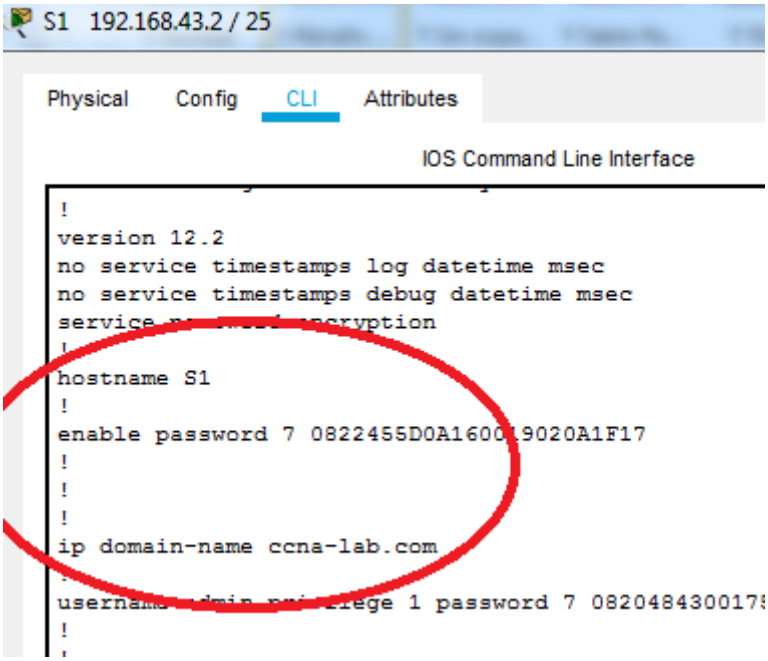
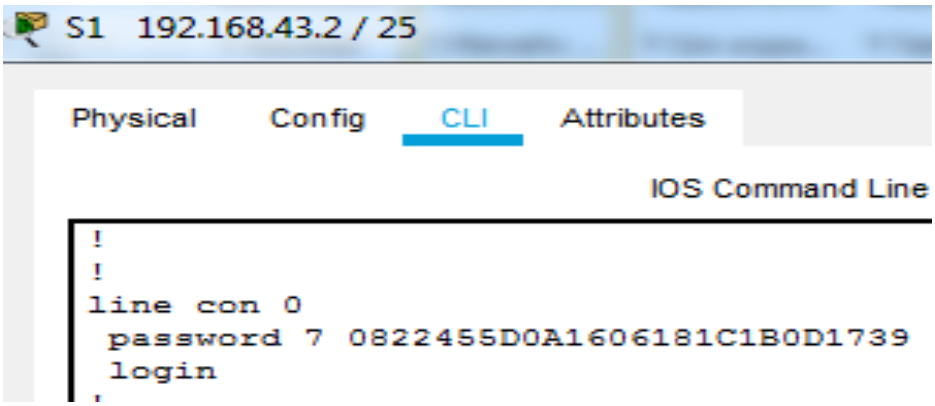



Figura 20. Contraseña de acceso a la consola

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
```




Fuente: Autoría propia en Packet Treacer

Figura 21. Contraseña cifrada para el modo EXEC privilegiado.

Se establece mediante configuración la contraseña de ingreso a modo privilegiado y la configuración para encriptar la misma.

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable password ciscoenpass
S1(config)#service password-encryption
```

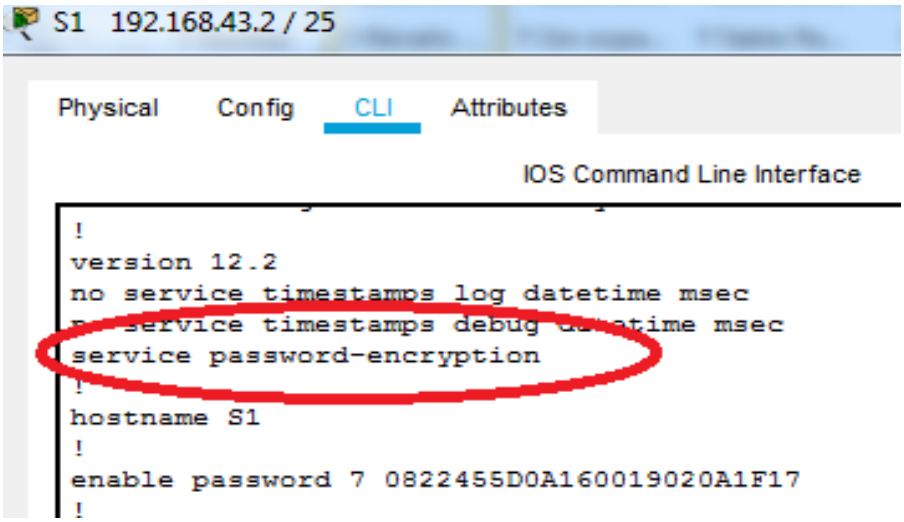
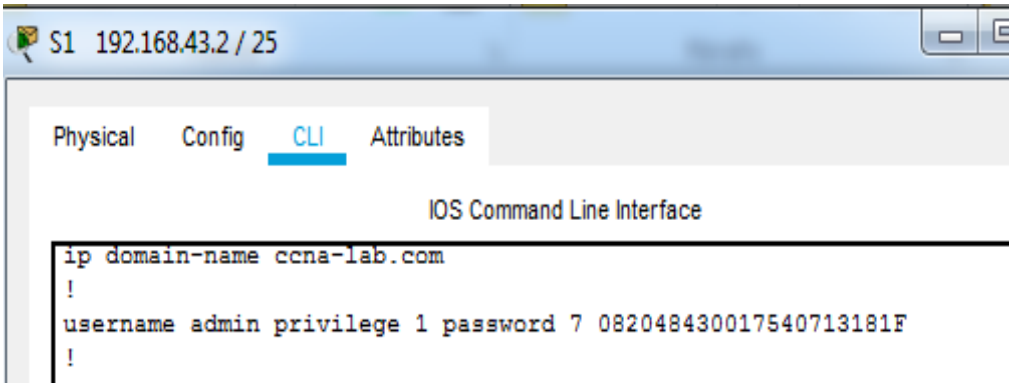


Figura 22. Crear un usuario administrativo en la base dedatos local.

**Password: admin1pass,  Nombre de usuario: admin**

```
S1#config t
S1(config)#
S1(config)#username admin password admin1pass
```




Fuente: Autoría propia en Packet Treacer

Figura 23. Configurar el inicio de sesión en las líneas VTYpara B.D  local.

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line vty 0 4
S1(config-line)#line vty 0 4
S1(config-line)#login local
S1(config-line)#exit
```

```
 password 7 0822455D0A1606181C1B0D1739
 login
!
line vty 0 4
 login local
 transport input ssh
```

Figura 24. Configurar VTY solo aceptando SSH en S1, se verifican cambios enla configuracion.

```
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#
```

```
 password 7 0822455D0A1606181C1B0D1739
 login
!
line vty 0 4
 login local
 transport input ssh
```

Figura 25. Cifrar las contraseñas de texto no cifrado.

```
S1(config)#
S1(config)#service password-encryption
S1(config)#exit
S1#
```

```
S1(config)#service password-encryption
S1(config)#exit
S1#
```

Figura 26. Configure un MOTD Banner. Mensaje de ingreso no configurado.

```
S1#en
S1#config t
S1(config)#banner motd "El acceso a S1 esta restringido a  personal no  autorizado"
S1(config)#exit
```

```
!
banner motd ^CEl acceso a S1 esta restringido.Ingreso solo a personal
autorizado^C
!
!
!
line con 0
 password 7 0822455D0A1606181C1B0D1739
 login
!
```

Figura 27. Generar una clave de cifrado RSA, Módulo de 1024 bits.

S1(config)#

S1(config)#crypto key generate rsa

% You already have RSA keys defined named R1.ccna-lab.com .

% Do you really want to replace them? [yes/no]: yes

The name for the keys will be: R1.ccna-lab.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

```
S1#
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#crypto key generate rsa
The name for the keys will be: S1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Figura 28. Configurar la interfaz de administración (SVI).

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.43.2 255.255.255.128
S1(config-if)#no shut
S1(config-if)#exit
```

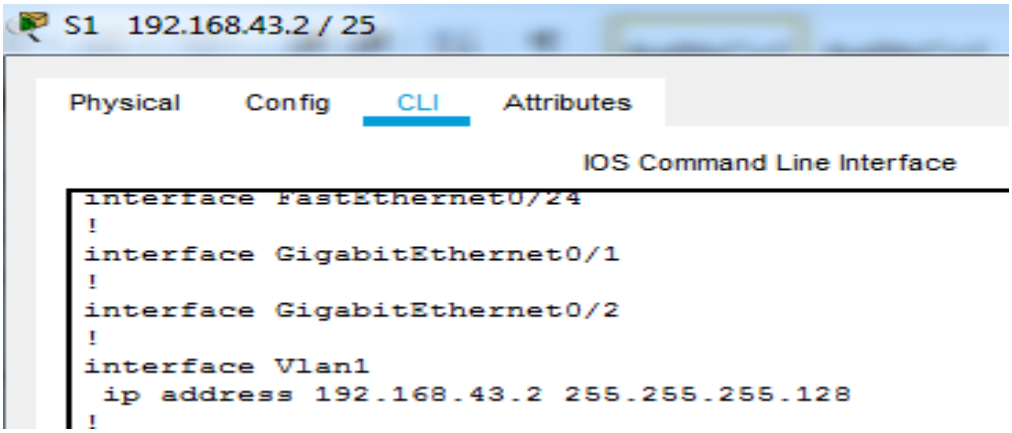
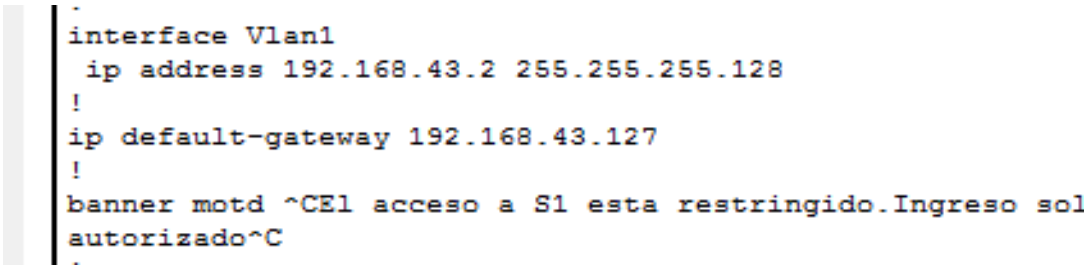



Figura 29. Configuración del gateway predeterminado.

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.43.2 255.255.255.128
S1(config-if)#no shut
S1(config-if)#ip default-gateway 192.168.43.127
S1(config)#no shut
```



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

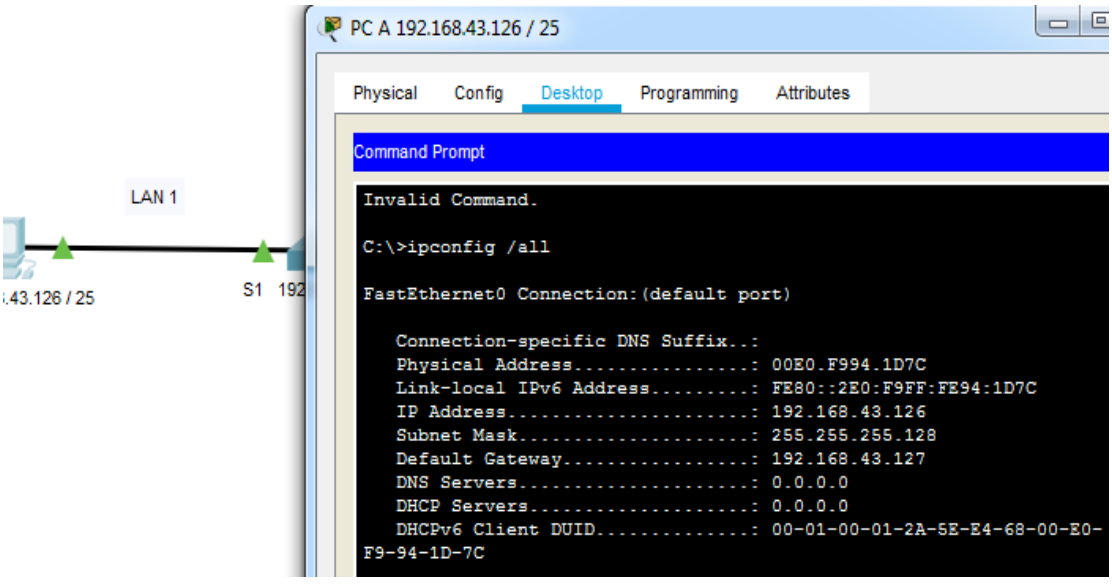
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 4. PC-A Network Configuration

| **PC-A Network Configuration** | |
|---|---|
| **Descripción** | FastEthernet0 |
| **Dirección Física** | 00E0.F994.1D7C |
| **Dirección IP** | 192.168.43.126 |
| **Mascara de Subred** | 255.255.255.128 |
| **Gateway predeterminado** | 192.168.43.127 |

**Fuente: Tabla tomada de PDF, "**PRUEBA DE HABILIDADES CCNA 2022".

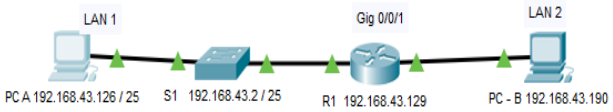
Figura 30. Configuración IP PC A.




Fuente: Autoría propia en Packet Treacer

Figura 31. Se anexa evidencia de conectividad de PC A a P CB.

Se realiza ping desde la PC A a la PC B, es decir de la LAN 1 a la LAN 2.



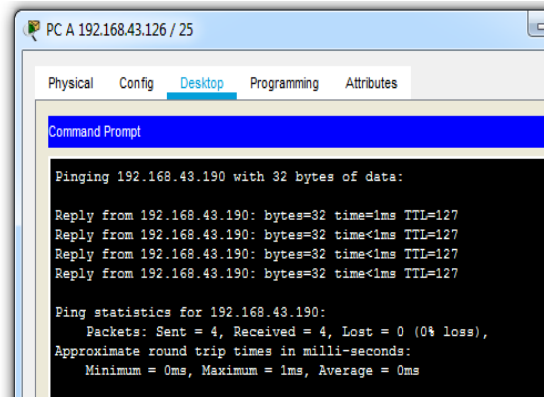




Tabla 5. PC-B Network Configuration

| **PC-B Network Configuration** | |
|---|---|
| **Descripción** | FastEthernet0 |
| **Dirección Física** | 0040.0B92.87AD |
| **Dirección IP** | 192.168.43.190 |
| **Mascara de Subred** | 255.255.255.192 |
| **Gateway predeterminado** | 192.168.43.191 |

Fuente: Tabla tomada de PDF, **“**PRUEBA DE HABILIDADES CCNA 2022”.

Figura 32. Configuración IP  PC B.

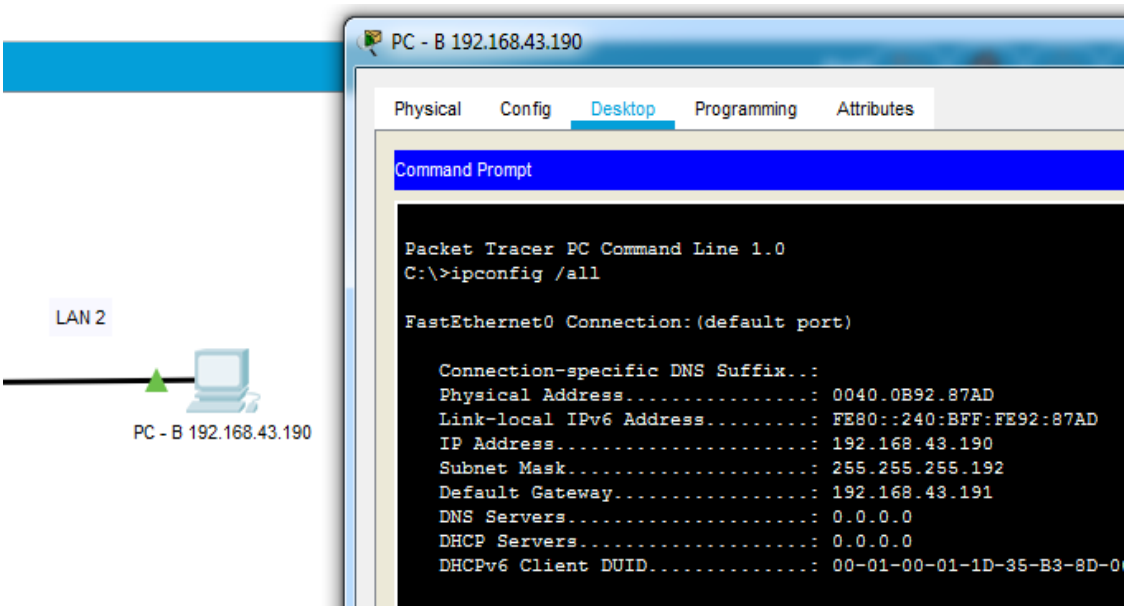
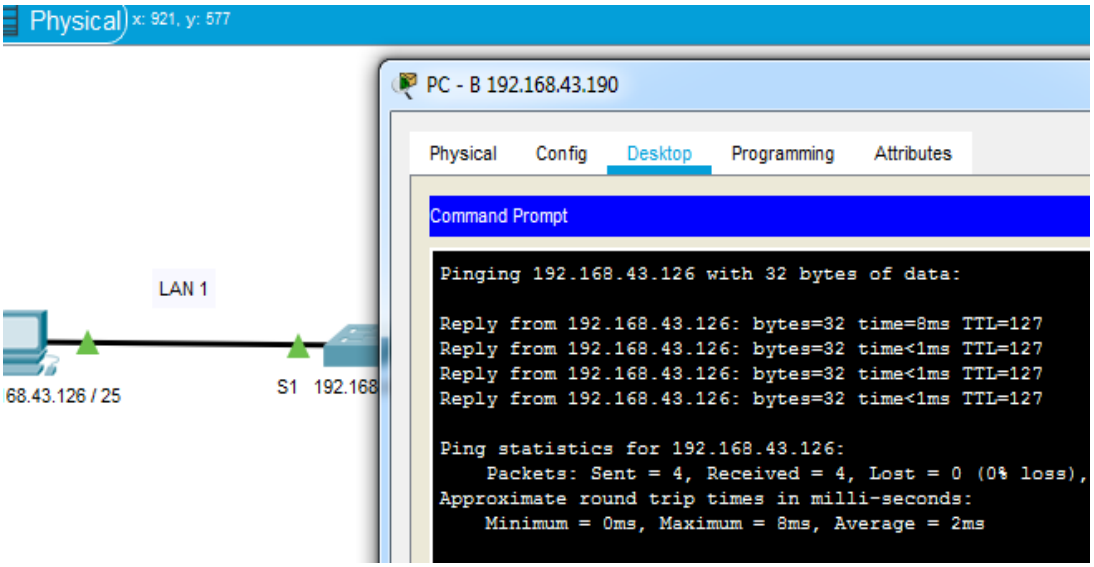



Figura 33. Se anexa evidencia de conectividad de PC A a P CB.

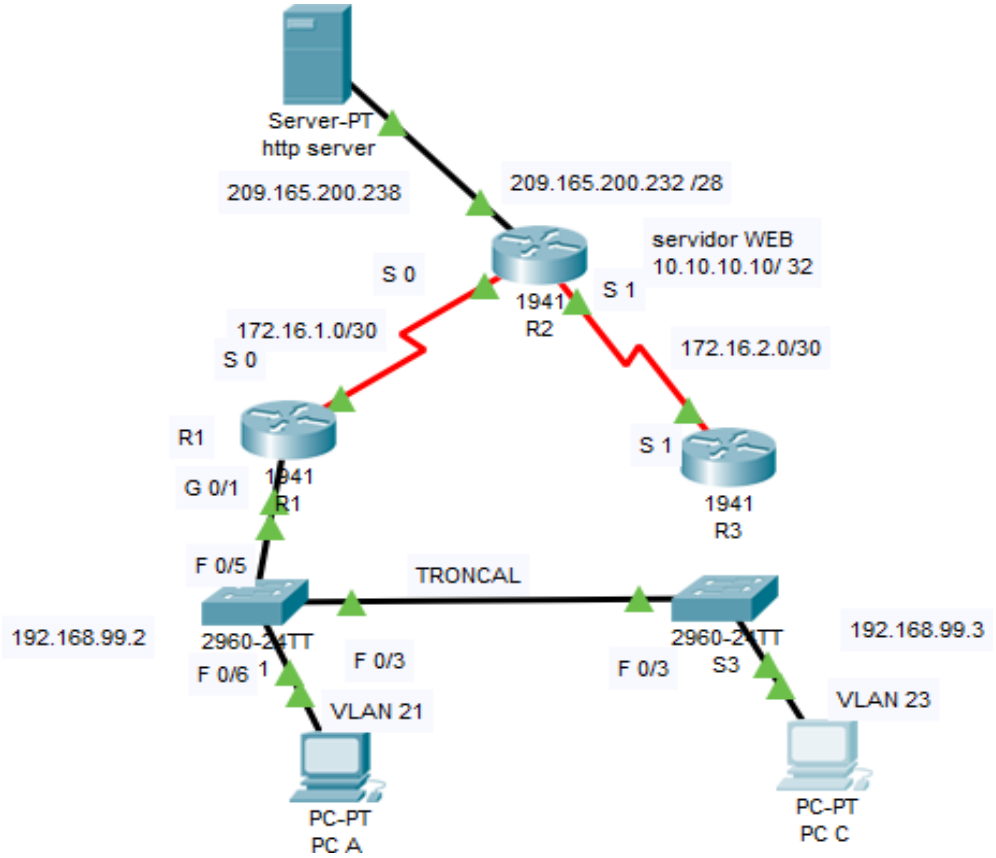
Se realiza ping desde la PC B a la PC A, es decir de la LAN 2 a la LAN 1.



## 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 34. Topología escenario 2.



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

### Parte 1: Inicializar dispositivos

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. Inicialización y cargar de Routers y Switches.

| **Tarea** | **Comando de IOS** |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Router > enable<br>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<br>switch#delete vlan.dat<br>switch#erase startup-config |
| Volver a cargar ambos switches | swicht#reload |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | switch#show flash |

**Fuente: Tabla tomada de PDF, "**PRUEBA DE HABILIDADES CCNA 2022".

Figura 35. Inicialización y recarga del R1

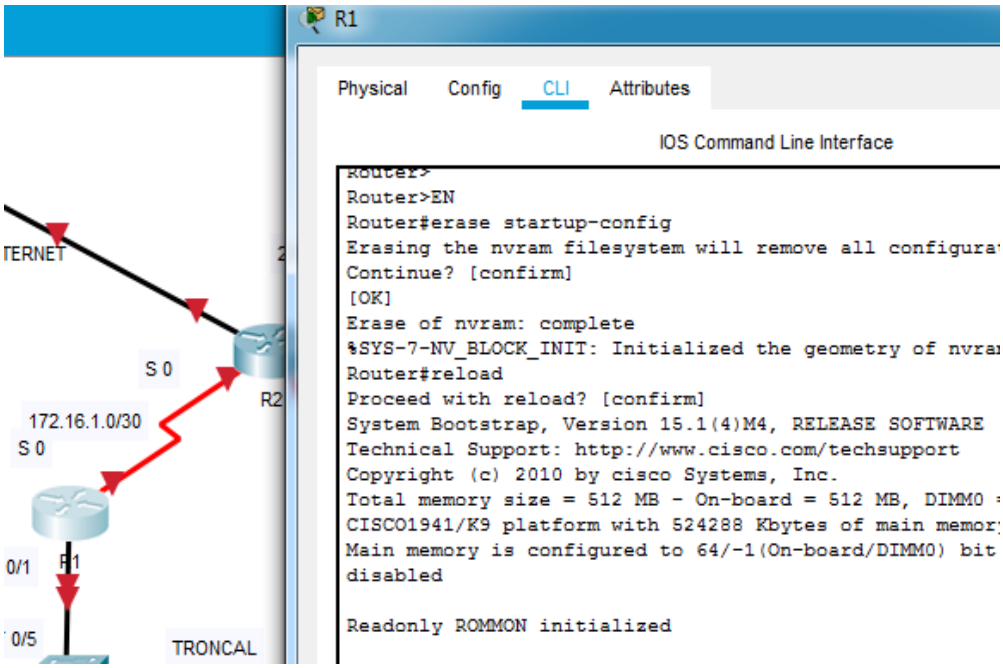



Figura 36. Inicialización y recarga del R2

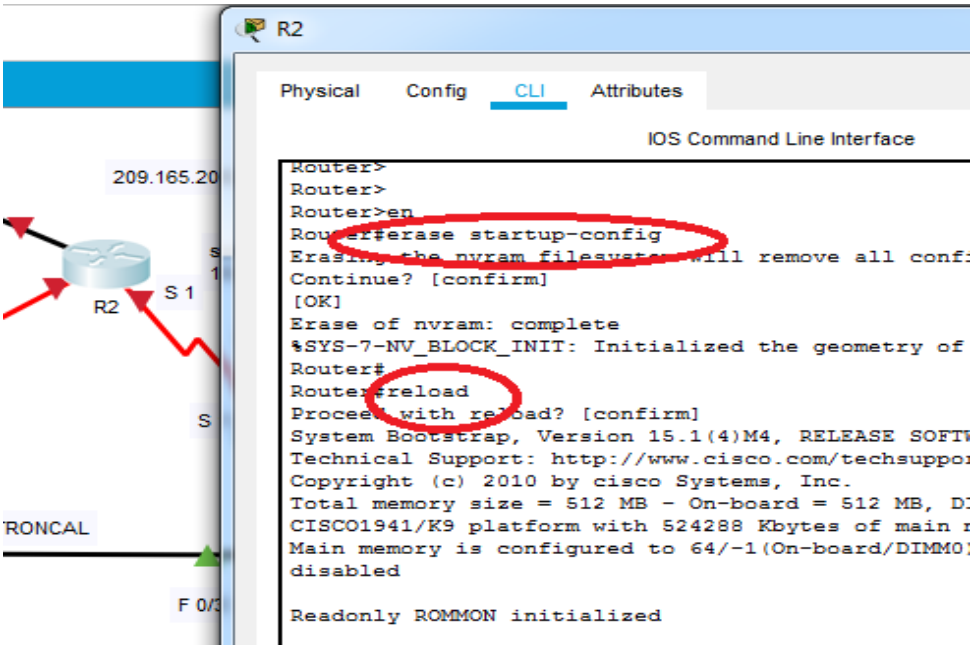


Figura 37. Inicialización y recarga del R3.

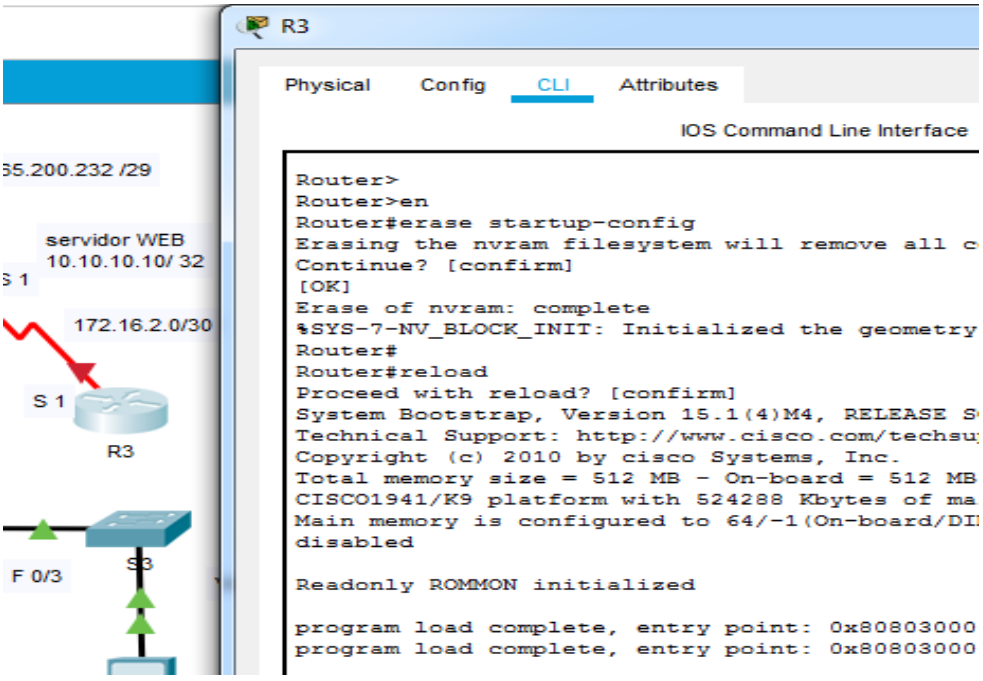
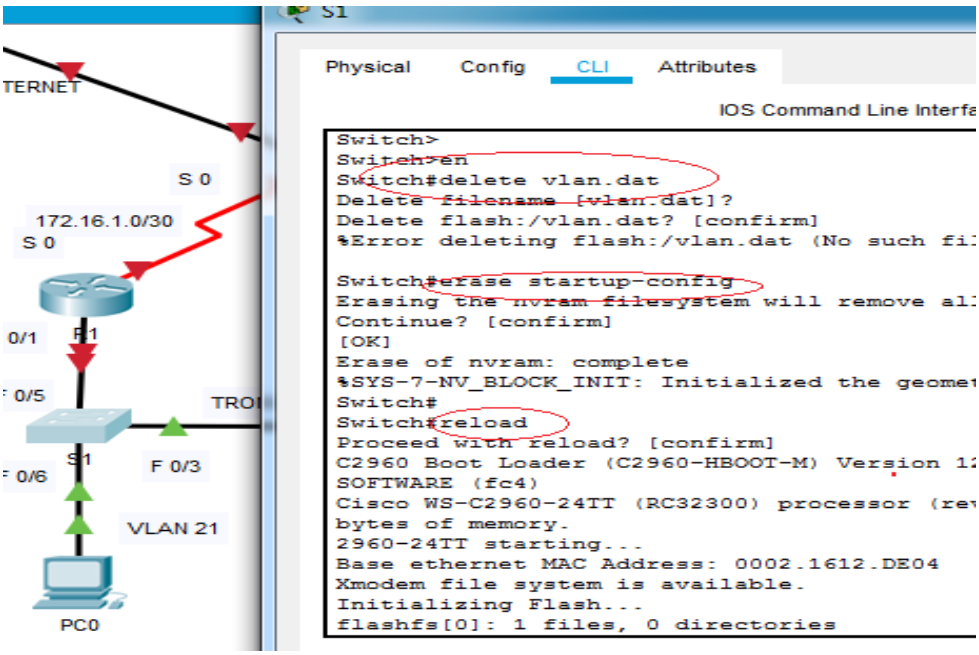



Figura 38. Inicialización y recarga del S1.




Fuente: Autoría propia en Packet Treacer

Figura 39. Revisión de memoria flash en S1.

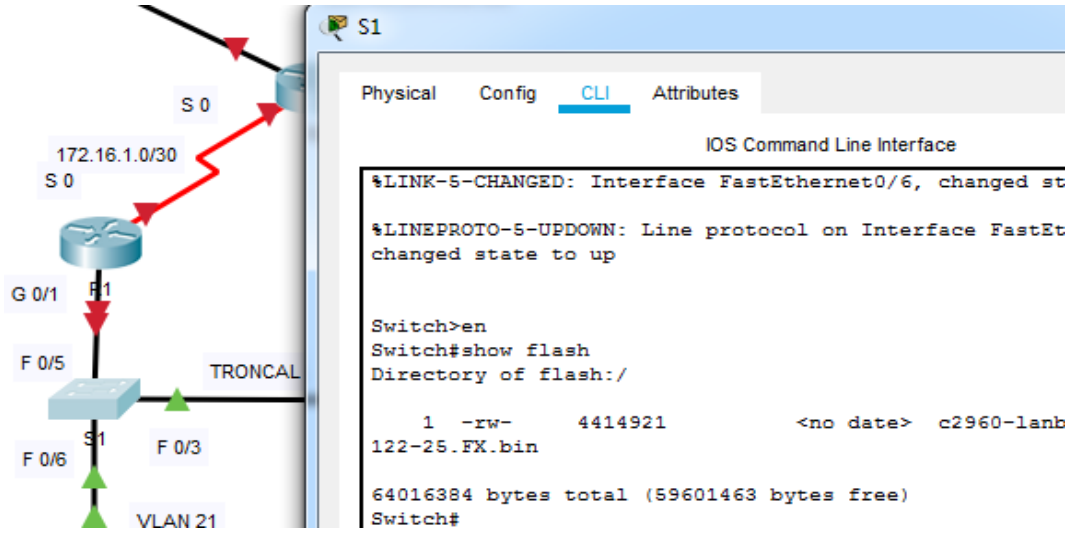
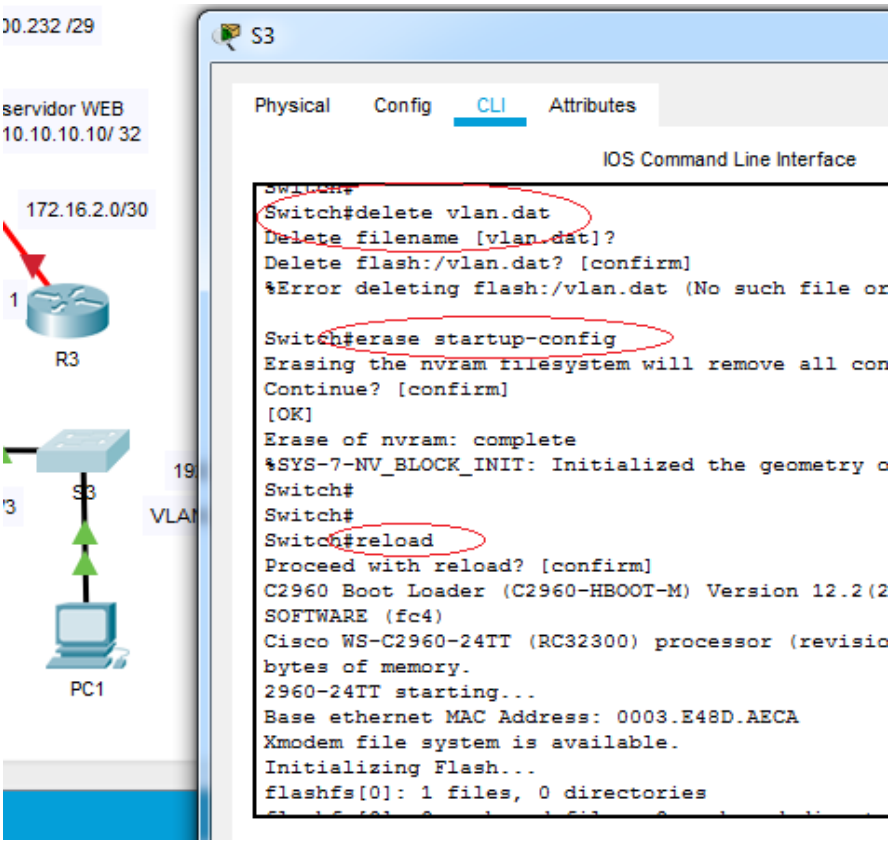
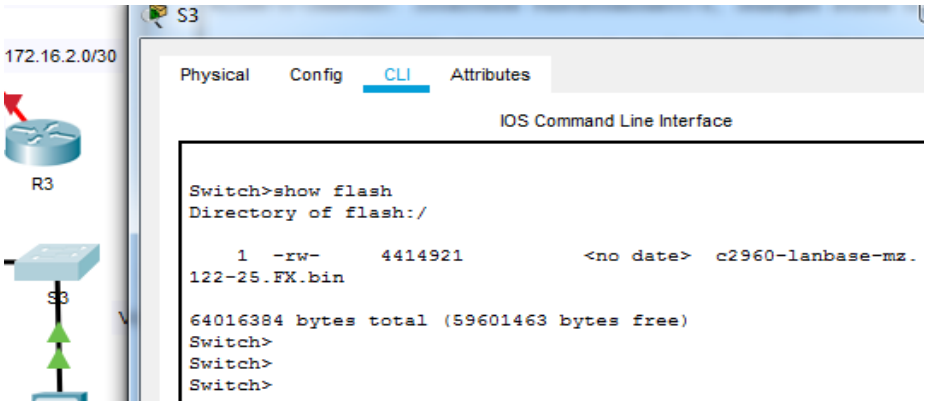



Figura 40. Inicialización y recarga del S3.




Fuente: Autoría propia en Packet Treacer

Figura 41. Revisión de memoria flash en S3.




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

**Paso 1: Configurar la computadora de Internet**

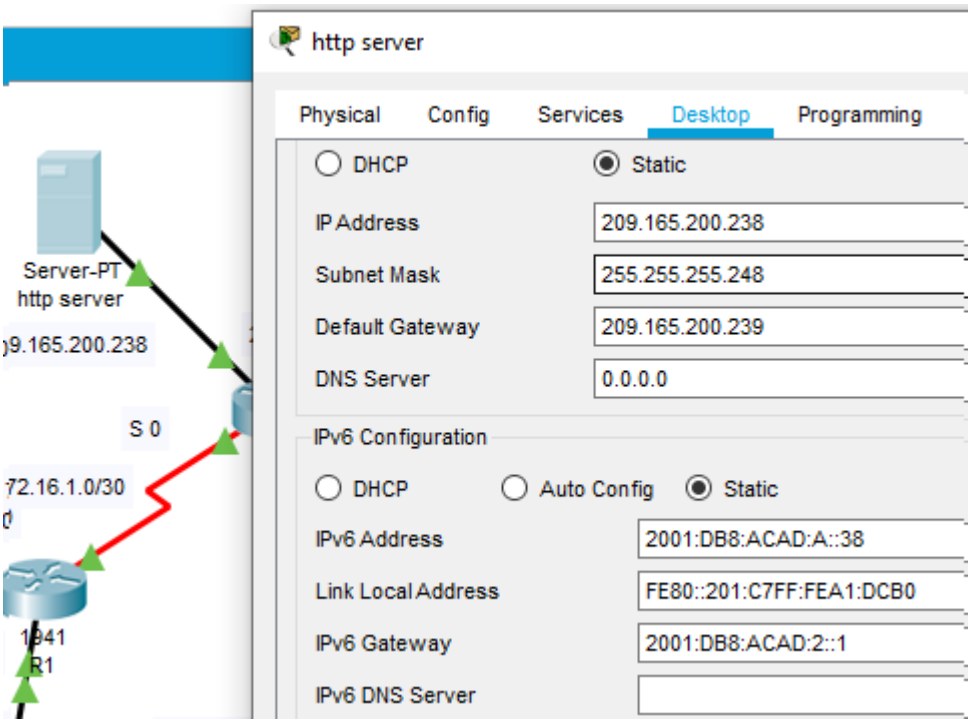
**Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):**

Tabla 7. Direcciones para configurar Servidor WEB.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Dirección IPv4 | **209.165.200.238** |
| Máscara de subred para IPv4 | **255.255.255.248** |
| Gateway predeterminado | **209.165.200.239** |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::2/64 |
| Gateway predeterminado IPv6 | **2001:DB8:ACAD:2::1** |

**Fuente: Tabla tomada de PDF, "**PRUEBA DE HABILIDADES CCNA 2022".

Figura 42. Configuración de servidor WEB.




Fuente: Autoría propia en Packet Treacer

## Paso 2: Configurar R1

**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.

**Las tareas de configuración para R1 incluyen las siguientes:**

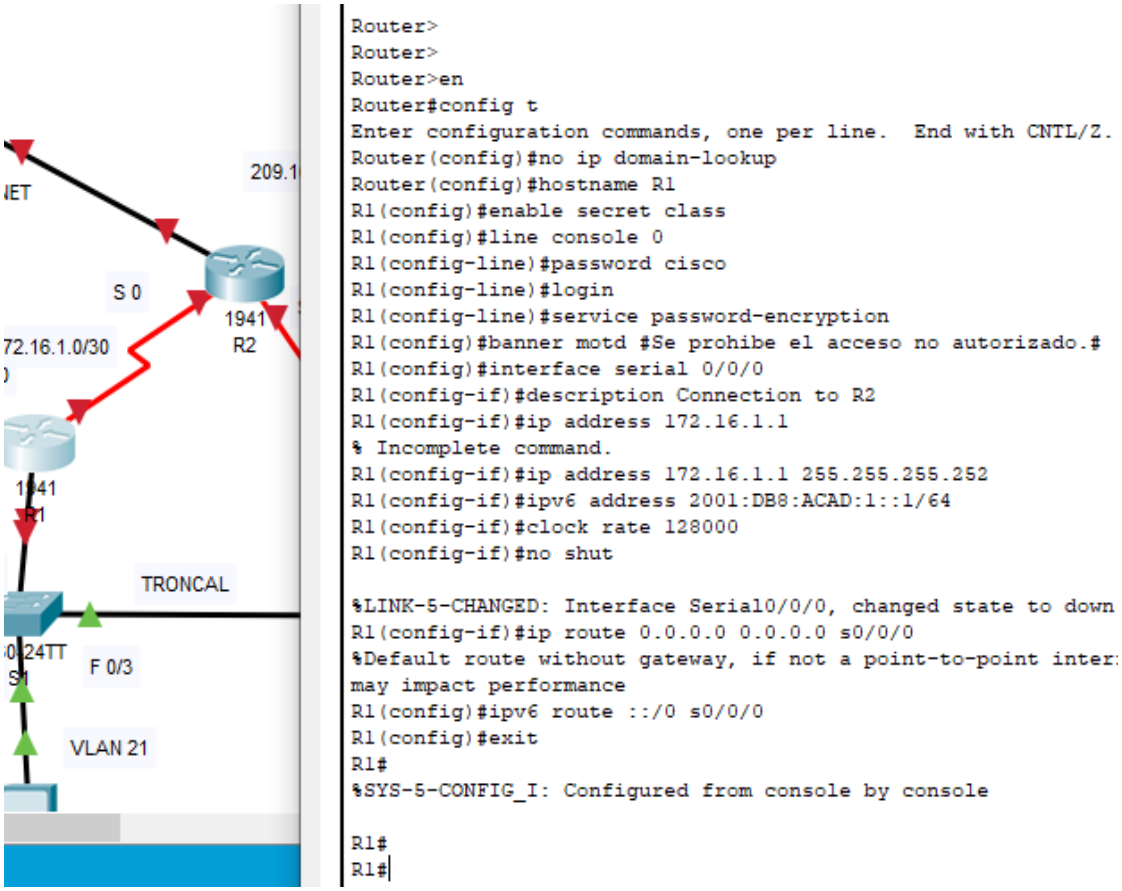
Tabla 8. Configuración de tareas R1.

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | 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<br>R1(config-line)#password cisco<br>R1(config-line)#login |
| Contraseña de acceso Telnet | R1(config-line)#line vty 0 4<br>R1(config-line)#password cisco<br>R1(config-line)#login |
| 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 S0/0/0 | R1(config)# interface serial 0/0/0<br>R1(config-if)#description Connection to R2<br>R1(config-if)#ip address 172.16.1.1 255.255.255.252<br>R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64<br>R1(config-if)#clock rate 128000 |

| | |
|---|---|
| | R1(config-if)#no shutdown |
| Rutas predeterminadas | R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0<br>R1(config)#ipv6 route ::/0 s0/0/0<br>R1(config)#ipv6 unicas<br>R1(config)#ipv6 unicast-routing |

Fuente: Tabla tomada de PDF, “PRUEBA DE HABILIDADES CCNA 2022”.

Figura 43. Configuración R1.




Fuente: Autoría propia en Packet Treacer

## Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

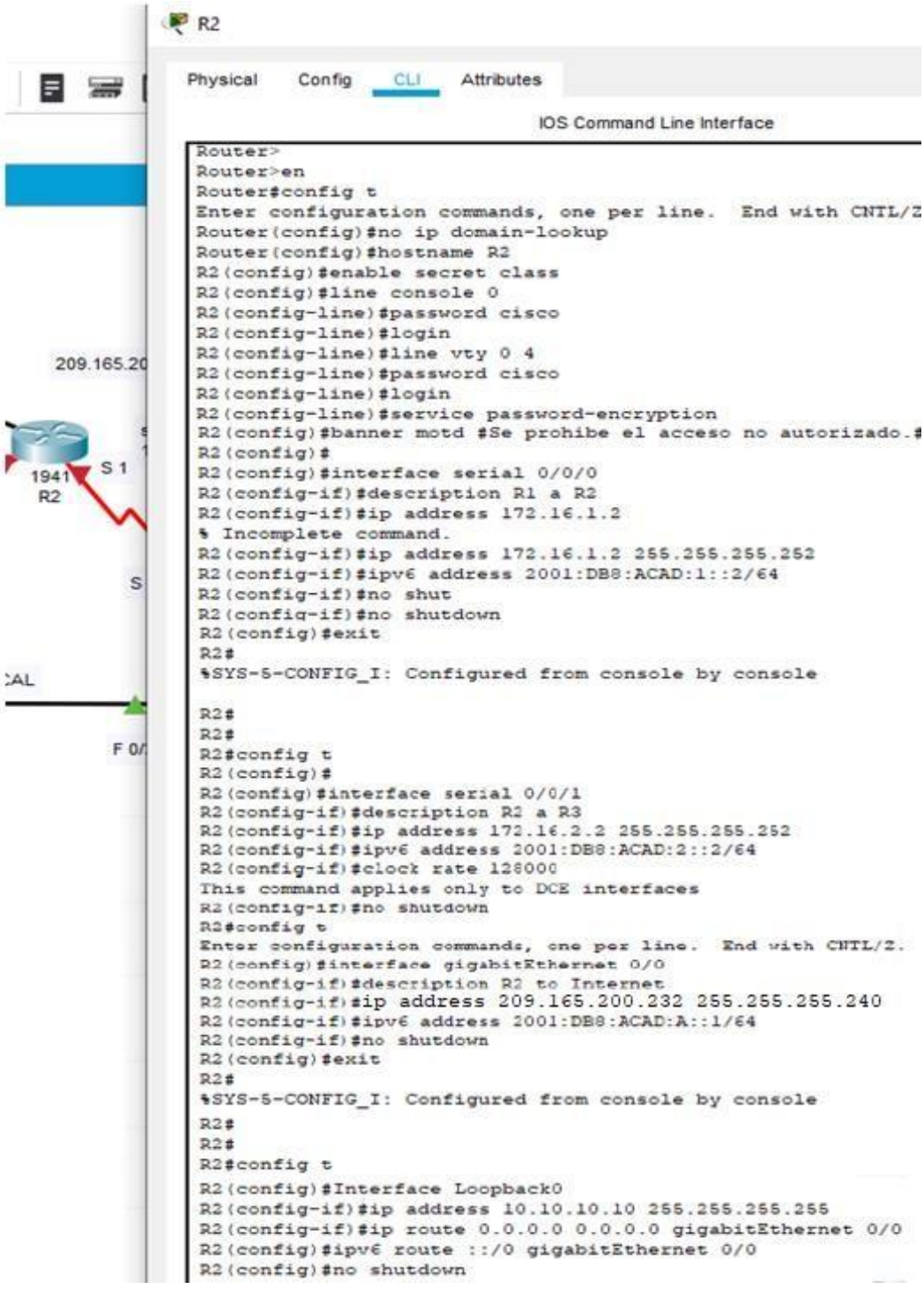
Tabla 9. Configuración de tareas R2.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | 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<br>R2(config-line)#password cisco<br>R2(config-line)#login |
| Contraseña de acceso Telnet | R2(config-line)#line vty 0 4<br>R2(config-line)#password cisco<br>R2(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R2(config)#service password-encryption |
| Habilitar el servidor HTTP | R2(config)#ip http server |
| Mensaje MOTD | R2(config)#banner motd #Se prohibe el acceso no autorizado.# |
| Interfaz S0/0/0 | R2(config)#interface serial 0/0/0<br>R2(config-if)#description R1 a R2<br>R2(config-if)#ip address 172.16.1.2 255.255.255.252<br>R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64<br>R2(config-if)#no shutdown |
| Interfaz S0/0/1 | R2(config)#interface serial 0/0/1<br>R2(config-if)#description R2 a R3<br>R2(config-if)#ip address 172.16.2.2 255.255.255.252<br>R2(config-if)#ipv6 address |

| | |
|---|---|
| | 2001:DB8:ACAD:2::2/64<br>R2(config-if)#clock rate 128000<br>R2(config-if)#no shutdown |
| Interfaz G0/0 (**simulación** de Internet) | R2(config)#interface gigabitEthernet 0/0<br>R2(config-if)#description R2 to Internet<br>R2(config-if)# ip address<br>209.165.200.232<br>255.255.255.240<br>R2(config-if)# ipv6 address<br>2001:DB8:ACAD:A::1/64<br>R2(config-if)#no shutdown<br>R2(config-if)#exit |
| Interfaz loopback 0 (servidor web simulado) | R2(config-if)# Interface Loopback0<br>R2(config-if)#ip address 10.10.10.10<br>255.255.255.255 |
| Ruta predeterminada | R2(config)# ip route 0.0.0.0 0.0.0.0<br>gigabitEthernet 0/0<br>R2(config)#ipv6 route ::/0<br>gigabitEthernet 0/0 |

Fuente: Tabla tomada de PDF**, "**PRUEBA DE HABILIDADES CCNA 2022".

Figura 44. Configuración R2.




Fuente: Autoría propia en Packet Treacer

### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

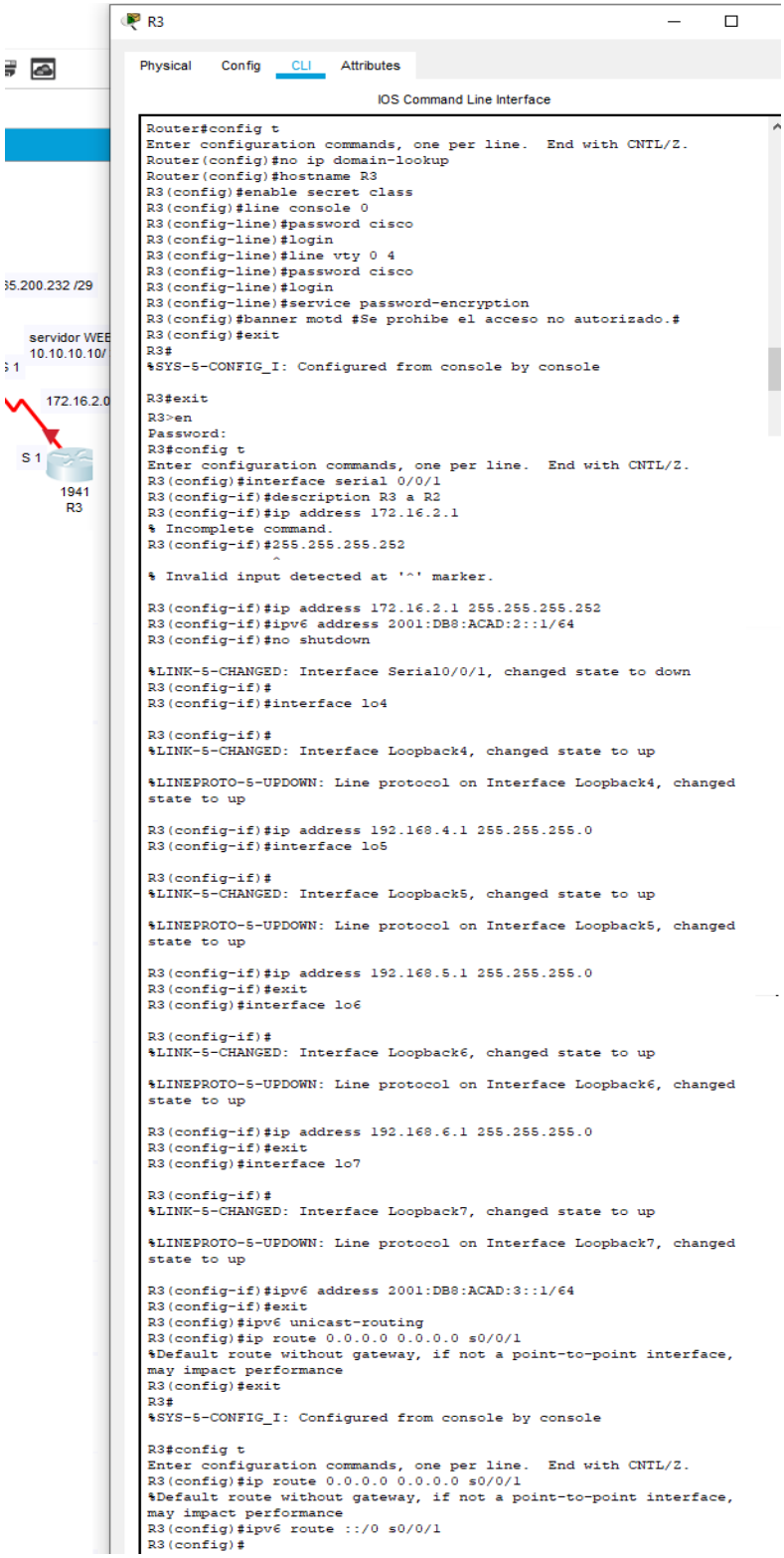
Tabla 10. Configuración de tareas R3.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | 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<br>R3(config-line)#password cisco<br>R3(config-line)#login |
| Contraseña de acceso Telnet | R3(config-line)#line vty 0 4<br>R3(config-line)#password cisco<br>R3(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | R3(config)#service password-encryption |
| Mensaje MOTD | R3(config)#banner motd #Se prohibe el acceso no autorizado.# |
| Interfaz S0/0/1 | R3(config)#interface serial 0/0/1<br>R3(config-if)#description R3 a R2<br>R3(config-if)#ip address 172.16.2.1 255.255.255.252<br>R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64<br>R3(config-if)#no shutdown |
| Interfaz loopback 4 | R3(config)#interface lo4<br>R3(config-if)#ip address 192.168.4.1 255.255.255.0 |
| Interfaz loopback 5 | R3(config)#interface lo5<br>R3(config-if)#ip address 192.168.5.1 |

| | |
|---|---|
| | 255.255.255.0 |
| Interfaz loopback 6 | R3(config)#interface lo6<br>R3(config-if)#ip address 192.168.6.1 255.255.255.0 |
| Interfaz loopback 7 | R3(config)#interface lo7<br>R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64<br>R3(config-if)#exit<br><br>R3(config)#ipv6 unicast-routing |
| Rutas Predeterminadas | R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1<br>R3(config)#ipv6 route ::/0 s0/0/1 |

Fuente: Tabla tomada de PDF**, "**PRUEBA DE HABILIDADES CCNA 2022".

Figura 45. Configuración R3.




Fuente: Autoría propia en Packet Treacer

Nota: Después de inicializar los dispositivos pertenecientes al escenario 2, se lleva acabo el cargue de los parámetros solicitados y con ello la configuración de las interfaces seriales y de gigabitEthernet con protocolos IPv4 e IPv6 con el fin de crear la conexión delas diferentes subredes dentro de la red, adicional se crean las interfaces loopback en R3, con el fin de crear las interfaces virtuales, dado que estas no se asignan a un puerto físico en específico.

**Paso 5: Configurar S1**

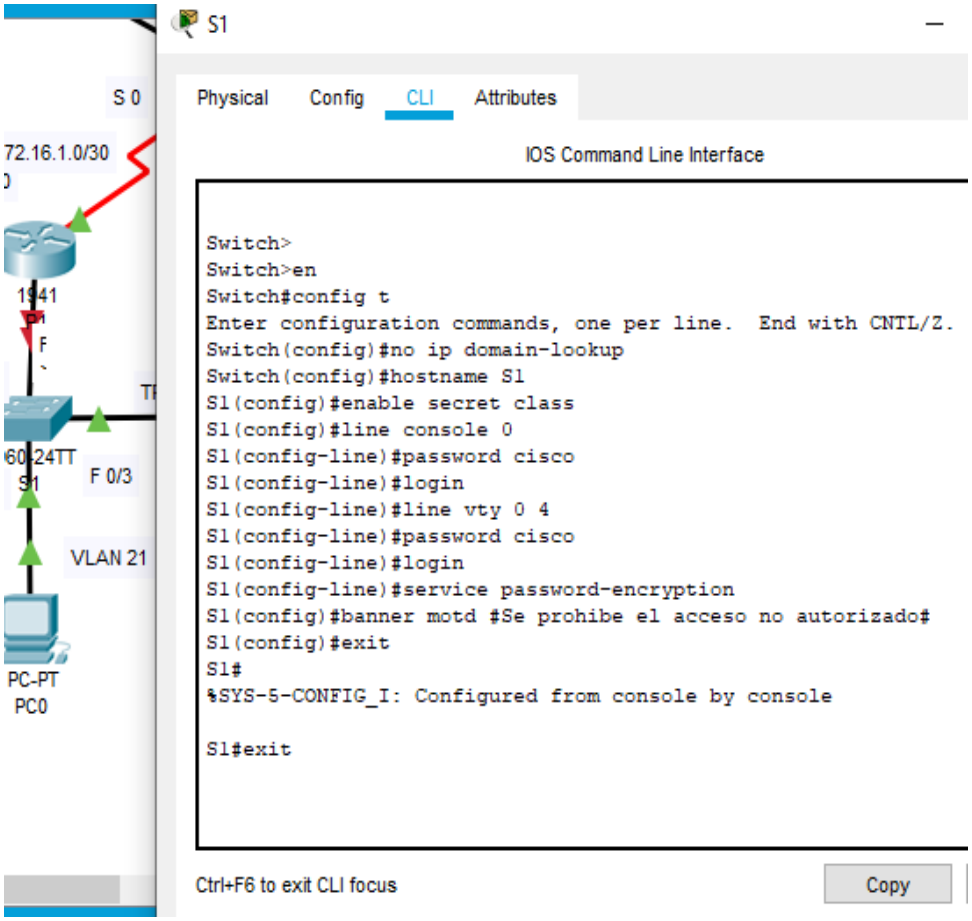
**La configuración del S1 incluye las siguientes tareas:**

Tabla 11. Configuración de tareas S1.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | 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<br>S1(config-line)#password cisco<br>S1(config-line)#login |
| Contraseña de acceso Telnet | S1(config-line)#line vty 0 4<br>S1(config-line)#password cisco<br>S1(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | S1(config-line)#service password-encryption |
| Mensaje MOTD | S1(config)#banner motd #Se prohibe el acceso no autorizado# |

**Fuente: Tabla tomada de PDF, "**PRUEBA DE HABILIDADES CCNA 2022".

Figura 46. Configuración S1.




Fuente: Autoría propia en Packet Treacer

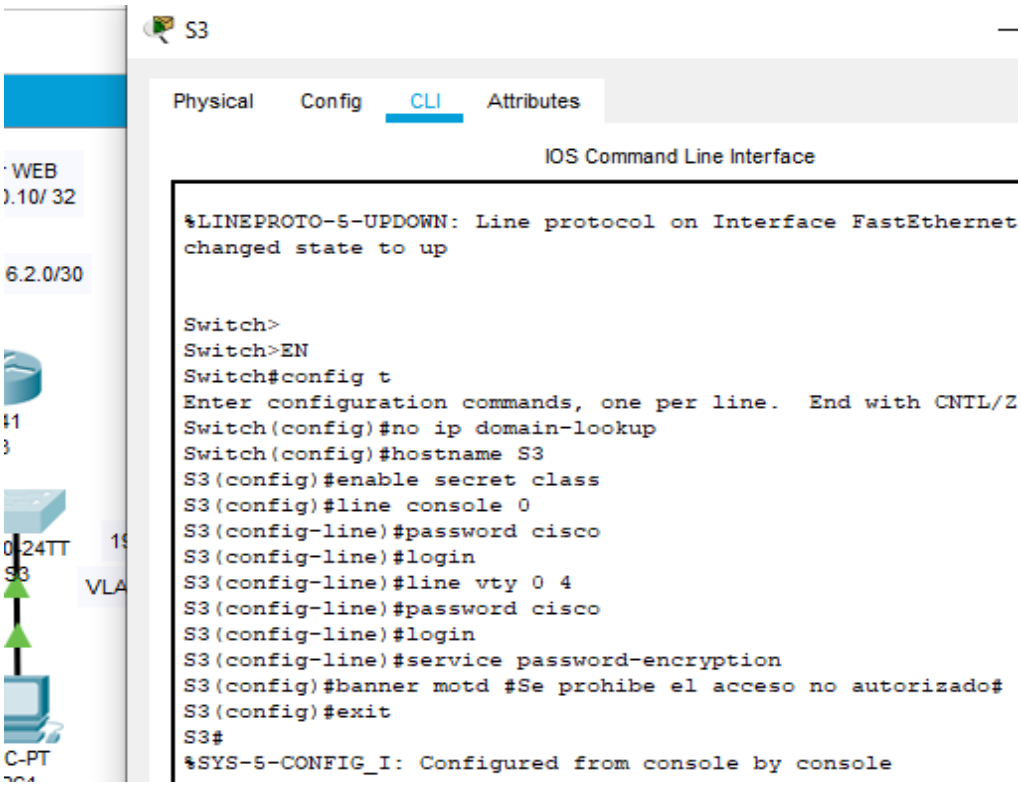
**Paso 6: Configurar el S3. La configuración del S3 incluye las siguientes tareas:**

Tabla 12. Configuración de tareas S3.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | Switch(config)#no ip domain-lookup |
| Nombre del switch | Switch(config)#hostname S1 |
| Contraseña de exec privilegiado cifrada | S3(config)#enable secret class |
| Contraseña de acceso a la consola | S3(config)#line console 0<br>S3(config-line)#password cisco<br>S3(config-line)#login |
| Contraseña de acceso Telnet | S3(config-line)#line vty 0 4<br>S3(config-line)#password cisco<br>S3(config-line)#login |
| Cifrar las contraseñas de texto no cifrado | S3(config-line)#service password-encryption |
| Mensaje MOTD | S3(config)#banner motd #Se prohibe el acceso no autorizado# |

Fuente: Tabla tomada de PDF, **"**PRUEBA DE HABILIDADES CCNA 2022".

Figura 47. Configuración S3.




Fuente: Autoría propia en Packet Treacer

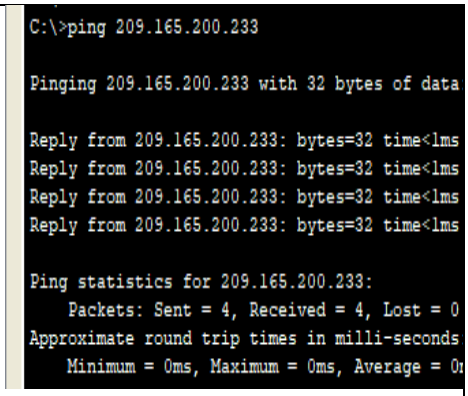
**Paso 7: Verificar la conectividad de la red.**

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. Verificación de conectividad.

| **Desde** | **A** | **Dirección IP** | **Resultados de ping.** |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | R1#ping 172.16.1.2<br><br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 172.16.1.2,<br>!!!!!<br>Success rate is 100 percent (5/5), round-trip<br><br>R1# |
| R2 | R3, S0/0/1 | 172.16.2.1 | R2#ping 172.16.2.1<br><br>Type escape sequence to abort.<br>Sending 5, 100-byte ICMP Echos to 172.16<br>!!!!!<br>Success rate is 100 percent (5/5), round<br><br>R2# |

| | | | |
|---|---|---|---|
| PC de Internet | Gateway predeterminado | 209.165.200.233 |  |

Fuente: Tabla tomada de PDF**, "**PRUEBA DE HABILIDADES CCNA 2022".

**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 14. Configuración VLAN en S1.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Crear la base de datos de VLAN | S1(config)#vlan 21<br>S1(config-vlan)#name Contabilidad<br>S1(config-vlan)#vlan 23<br>S1(config-vlan)#name Ingenieria<br>S1(config-vlan)#vlan 99<br>S1(config-vlan)#name Administracion |
| Asignar la dirección IP de administración. | S1(config)#interface vlan 99<br>S1(config-if)#ip address 192.168.99.2 255.255.255.0 |
| 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 fastEthernet 0/3<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 1 |

| | |
|---|---|
| Forzar el enlace troncal en la interfaz F0/5 | S1(config)#interface fastEthernet 0/5<br>S1(config-if)#switchport mode trunk<br>S1(config-if)#switchport trunk native vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S1(config)#interface range fa0/1-2, fa0/4, fa0/6-24<br>S1(config-if-range)#switchport mode access |
| Asignar F0/6 a la VLAN 21 | S1(config)#interface range fa0/6<br>S1(config-if-range)#switchport access vlan 21 |
| Apagar todos los puertos sin usar | S1(config)#interface range fa0/1-2,fa0/4,fa0/7- 24,gi0/1-2<br>S1(config-if-range)#shutdown |

Fuente: Tabla tomada de PDF, “PRUEBA DE HABILIDADES CCNA 2022”.

Figura 48. Configuración VLAN S1.


Fuente: Autoría propia en Packet Treacer

## Paso 2: Configurar el S3

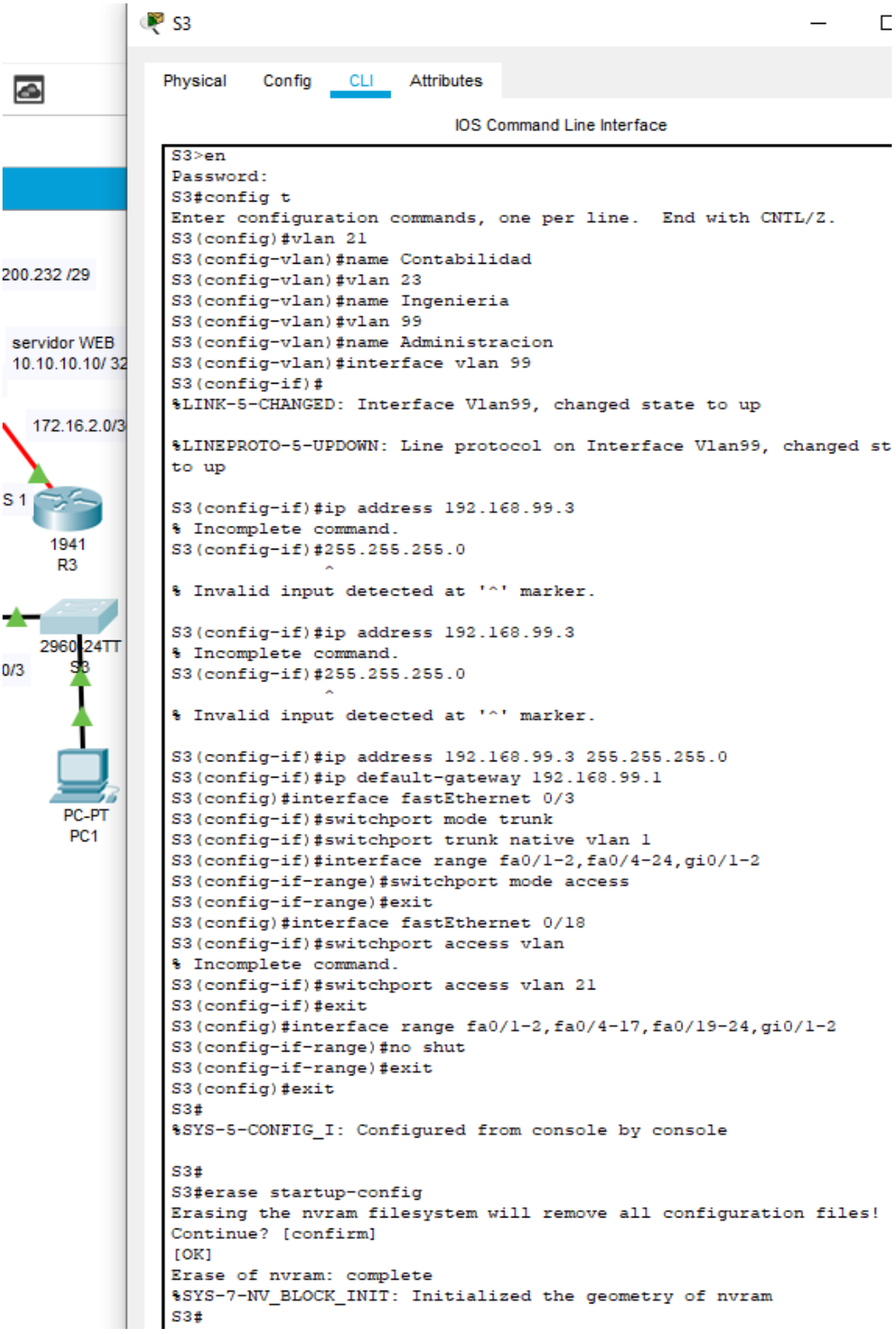
La configuración del S3 incluye las siguientes tareas:

Tabla 15. Configuración VLAN Y Mode Trunk en S3.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Crear la base de datos de VLAN | S3(config)#vlan 21<br>S3(config-vlan)#name Contabilidad<br>S3(config-vlan)#vlan 23<br>S3(config-vlan)#name Ingenieria<br>S3(config-vlan)#vlan 99<br>S3(config-vlan)#name Administracion |
| Asignar la dirección IP de administración. | S3(config)#interface vlan 99<br>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 fastEthernet 0/3<br>S3(config-if)#switchport mode trunk<br>S3(config-if)#switchport trunk native<br>vlan 1 |
| Configurar el resto de los puertos como puertos de acceso | S3(config)#interface range fa0/1-2,fa0/4-24,gi0/1-2<br>S3(config-if-range)#switchport mode access<br>S3(config-if-range)#exit |
| Asignar F0/18 a la VLAN 21 | S3(config)#interface fastEthernet 0/18<br>S3(config-if)#switchport access vlan<br>21<br>S3(config-if)#exit |
| Apagar todos los puertos sin usar | S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2<br>S3(config-if-range)#shutdown<br>S3(config-if-range)#exit |

Fuente: Tabla tomada de PDF, “PRUEBA DE HABILIDADES CCNA 2022”.

Figura 49. Configuración VLAN y Mode Trunk S3.




S3

Physical Config CLI Attributes

IOS Command Line Interface

```
S3>en
Password:
S3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#interface vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed st
to up

S3(config-if)#ip address 192.168.99.3
% Incomplete command.
S3(config-if)#255.255.255.0
                ^
% Invalid input detected at '^' marker.

S3(config-if)#ip address 192.168.99.3
% Incomplete command.
S3(config-if)#255.255.255.0
                ^
% Invalid input detected at '^' marker.

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#interface fastEthernet 0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#interface range fa0/1-2,fa0/4-24,gi0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#interface fastEthernet 0/18
S3(config-if)#switchport access vlan
% Incomplete command.
S3(config-if)#switchport access vlan 21
S3(config-if)#exit
S3(config)#interface range fa0/1-2,fa0/4-17,fa0/19-24,gi0/1-2
S3(config-if-range)#no shut
S3(config-if-range)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
S3#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
S3#
```

## Paso 3: Configurar R1

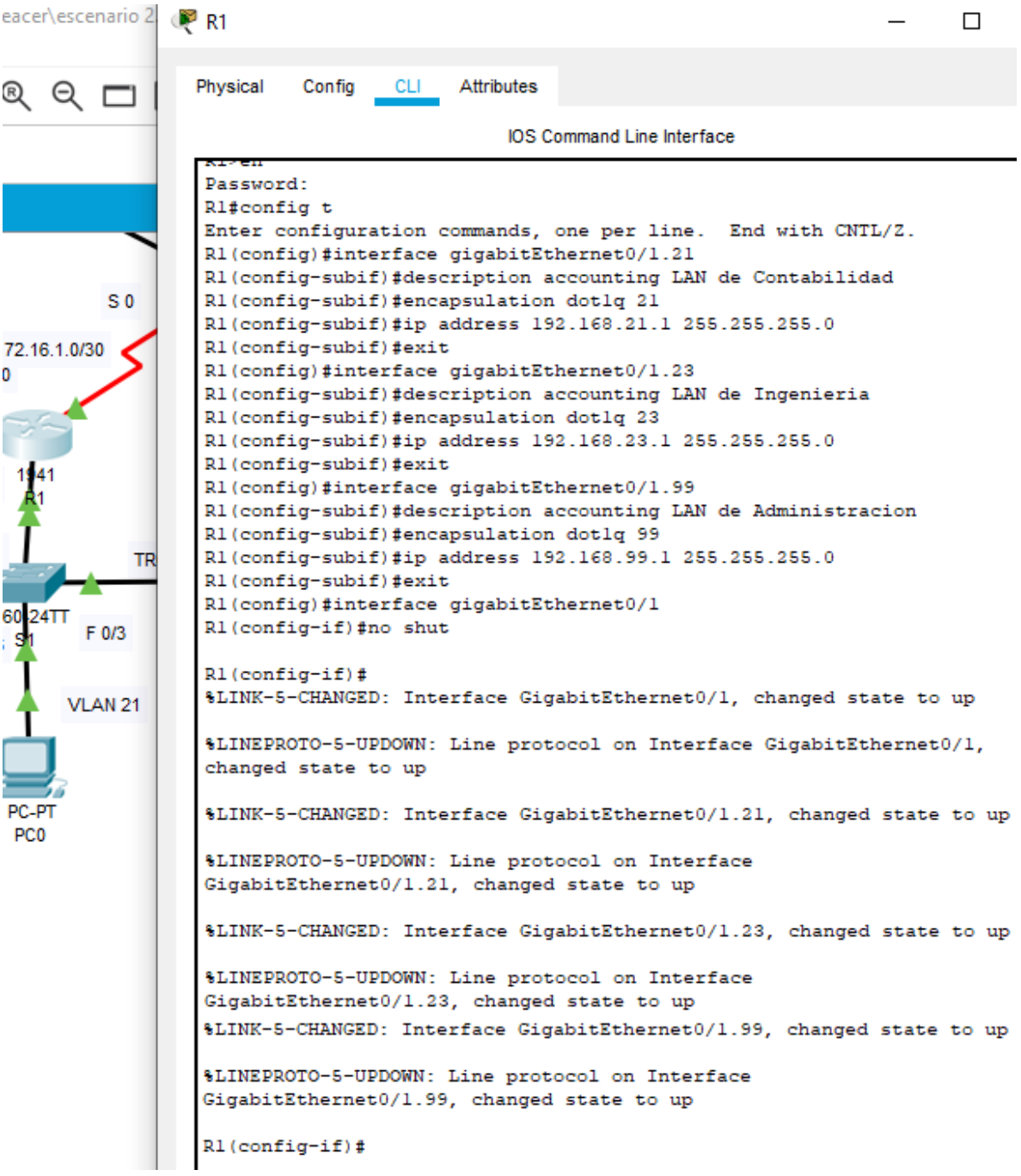
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 15. Configuración Vlan IPv4 en R1.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | Descripción: LAN de Contabilidad<br>Asignar la VLAN 21<br>Asignar la primera dirección disponible a esta interfaz:<br>R1(config)#interface gigabitEthernet 0/1.21<br>R1(config-subif)#description accounting LAN de Contabilidad<br>R1(config-subif)#encapsulation dot1q 21<br>R1(config-subif)#ip address 192.168.21.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | Descripción: LAN de Ingeniería<br>Asignar la VLAN 23<br>Asignar la primera dirección disponible a esta interfaz:<br>R1(config)#interface gigabitEthernet 0/1.23<br>R1(config-subif)#description accounting LAN de Ingenieria<br>R1(config-subif)#encapsulation dot1q 23<br>R1(config-subif)#ip address 192.168.23.1 255.255.255.0 |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | Descripción: LAN de Administración<br>Asignar la VLAN 99<br>Asignar la primera dirección disponible a esta interfaz:<br>R1(config)#interface gigabitEthernet 0/1.99<br>R1(config-subif)#description accounting LAN de Administracion<br>R1(config-subif)#encapsulation dot1q 99<br>R1(config-subif)#ip address 192.168.99.1 255.255.255.0 |
| Activar la interfaz G0/1 | R1(config)#interface gigabitEthernet 0/1<br>R1(config-if)#no shutdown |

Fuente: Tabla tomada de PDF, **"**PRUEBA DE HABILIDADES CCNA 2022".

Figura 50. Configuración VLAN IPv4 en  R1.




Fuente: Autoría propia en Packet Treacer

### 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 16. Pruebas de comunicaciones entre S1 y S3 por VLAN.

| **Desde** | **A** | **Dirección IP** | **Resultados de ping** |
|---|---|---|---|
| **S1** | R1, dirección VLAN 99 | 192.168.99.1 | `S1#ping 192.168.99.1`<br><br>`Type escape sequence to abort.`<br>`Sending 5, 100-byte ICMP Echos to 192.`<br>`!!!!!`<br>`Success rate is 100 percent (5/5), rou` |
| **S3** | R1, dirección VLAN 99 | 192.168.99.1 | `S3#ping 192.168.99.1`<br><br>`Type escape sequence to abort.`<br>`Sending 5, 100-byte ICMP Echos to 192.1`<br>`!!!!!`<br>`Success rate is 100 percent (5/5), rour` |
| **S1** | R1, dirección VLAN 21 | 192.168.21.1 | `S1#ping 192.168.21.1`<br><br>`Type escape sequence to abort.`<br>`Sending 5, 100-byte ICMP Echos to 192.16`<br>`!!!!!`<br>`Success rate is 100 percent (5/5), rounc` |
| **S3** | R1, dirección VLAN 23 | 192.168.23.1 | `S3#ping 192.168.23.1`<br><br>`Type escape sequence to abort.`<br>`Sending 5, 100-byte ICMP Echos to 192.`<br>`!!!!!`<br>`Success rate is 100 percent (5/5), rou` |

**Fuente: Tabla tomada de PDF, "**PRUEBA DE HABILIDADES CCNA 2022".

NOTA: De acuerdo a las pruebas anteriores se llevó a cabo la configuración de las VLAN entre los dispositivos S1 y S3, utilizando protocolo IPv4, con ello se empleó la creación de las redes lógicas independientes que permiten segmentar la red en este caso las VLAN virtuales con el fin permitir el acceso a cada subred y poder usarla para un fin en específico, donde se empleó el uso de un enlace troncal que permitirá la conexión entre los Switches S1, S3 y el Router en este caso R1, de igual forma se configura el acceso estatico asignados a los puertos de los dispositivos y el modo Access para que cada puerto sea específicamente asignado a la VLAN en especifico.

## 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:

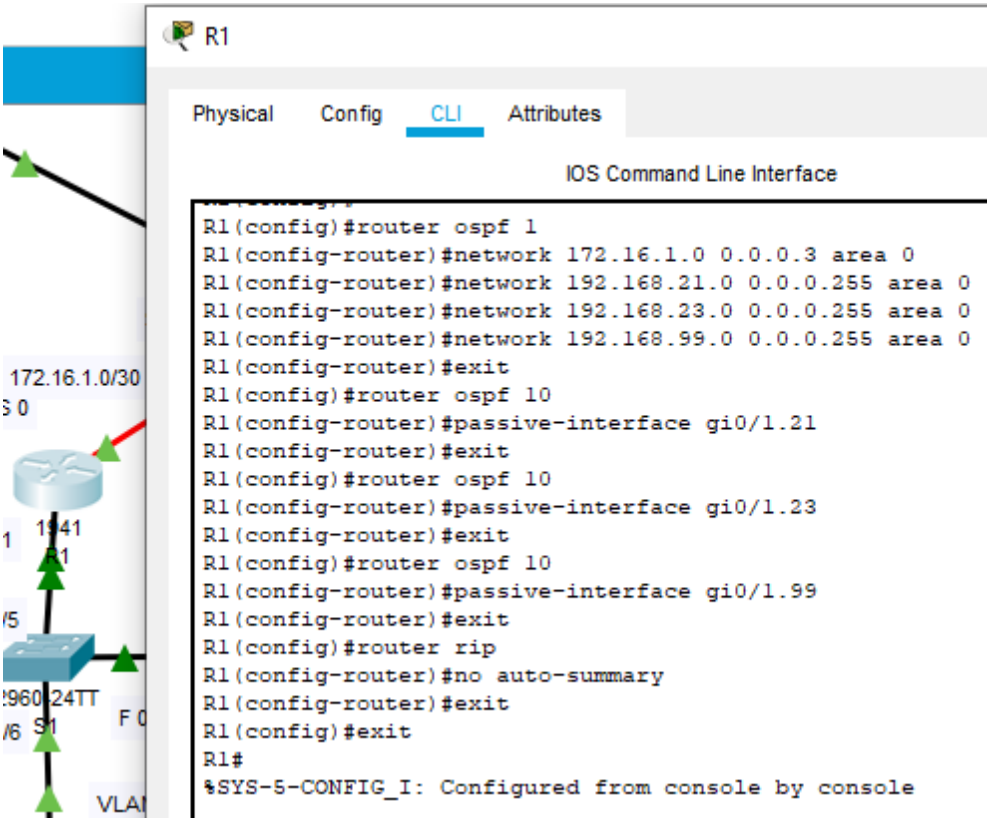
Tabla 17. Configuración de OSPF en R1.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Configurar OSPF área 0 | R1(config)#router ospf 1 |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente.<br><br>R1(config-router)#network 172.16.1.0 0.0.0.3 area 0<br>R1(config-router)#network 192.168.21.0 0.0.0.255 area 0<br>R1(config-router)#network 192.168.23.0 0.0.0.255 area 0<br>R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 |
| Establecer todas las interfaces LAN como pasivas | R1(config)#router ospf 10<br>R1(config-router)#passive-interface |

| | |
|---|---|
| | gi0/1.21<br>R1(config)#router ospf 10<br>R1(config-router)#passive-interface<br>gi0/1.23<br>R1(config)#router ospf 10<br>R1(config-router)#passive-interface<br>gi0/1.99 |
| Desactive la sumarización automática | R1(config)#router rip<br>R1(config-router)#no auto-summary |

Fuente: Tabla tomada de PDF, **“**PRUEBA DE HABILIDADES CCNA 2022”.

Figura 51. Configuración del Protocolo dinámico OSPF R1.




Fuente: Autoría propia en Packet Treacer

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

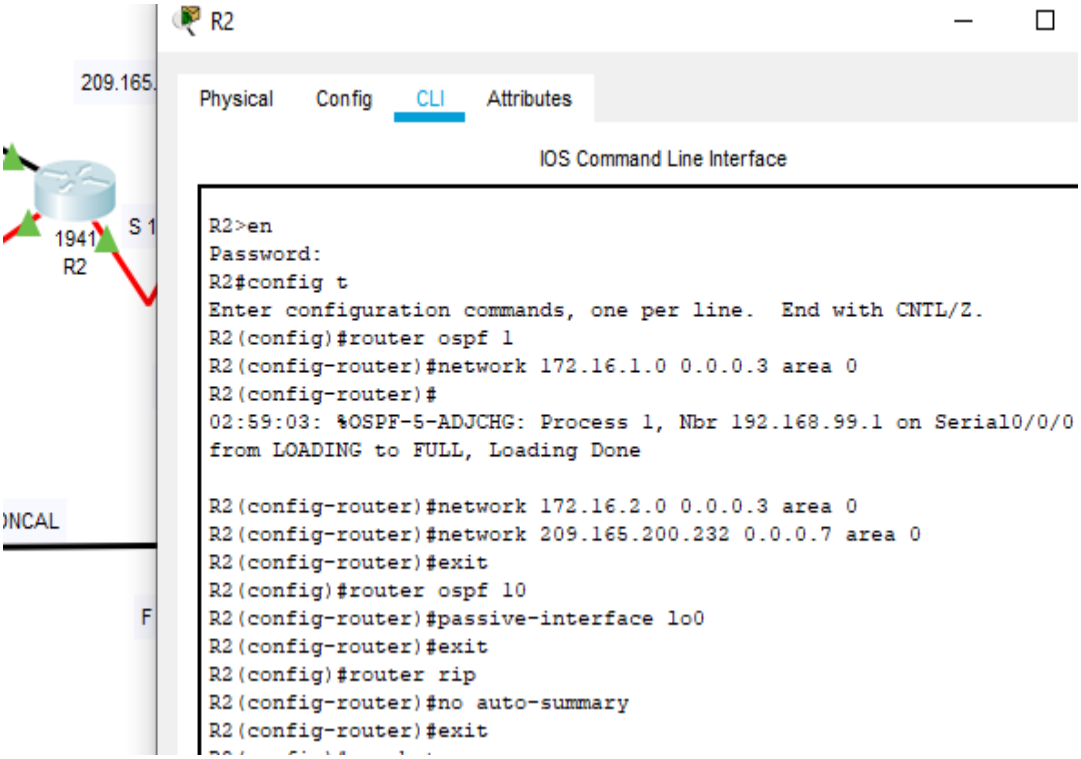
La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuración de OSPF en 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.<br><br>R2(config-router)#network 172.16.1.0 0.0.0.3 area 0<br>R2(config-router)#network 172.16.2.0 0.0.0.3 area 0<br>R2(config-router)#network<br>209.165.200.232 0.0.0.7 area 0 |
| Establecer la interfaz LAN (loopback) como pasiva | R2(config)#router ospf 10<br>R2(config-router)# passive-interface<br>lo0 |
| Desactive la sumarización automática. | R2(config)#router rip<br>R2(config-router)#no auto-summary |

Fuente: Tabla tomada de PDF, **"**PRUEBA DE HABILIDADES CCNA 2022".

Figura 52. Configuración del Protocolo dinámico OSPF R2.




## Paso 3: Configurar OSPFv3 en el R3

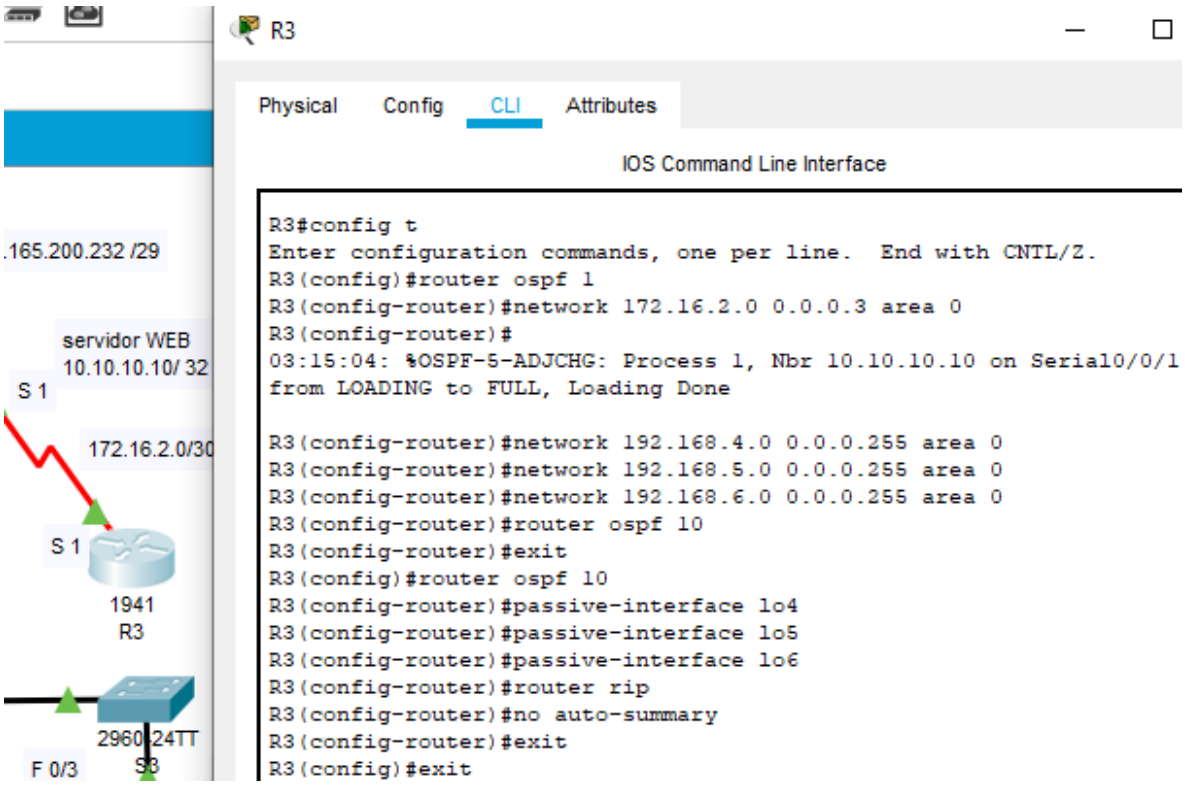
La configuración del R3 incluye las siguientes tareas:

Tabla 19. Configuración de OSPF en R3.

| **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<br>R3(config-router)#network 192.168.4.0 0.0.0.255 area 0<br>R3(config-router)#network 192.168.5.0 0.0.0.255 area 0 |

| | |
|---|---|
| | R3(config-router)#network 192.168.6.0<br>0.0.0.255 area 0 |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | R3(config)#router ospf 10<br>R3(config-router)# passive-interface lo4<br>R3(config-router)# passive-interface lo5<br>R3(config-router)# passive-interface lo6 |
| Desactive la sumarización automática. | R3(config)#router rip<br>R3(config-router)#no auto-summary |

Figura 53. Configuración del Protocolo dinámico OSPF R3.




Fuente: Autoría propia en Packet Treacer

**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:

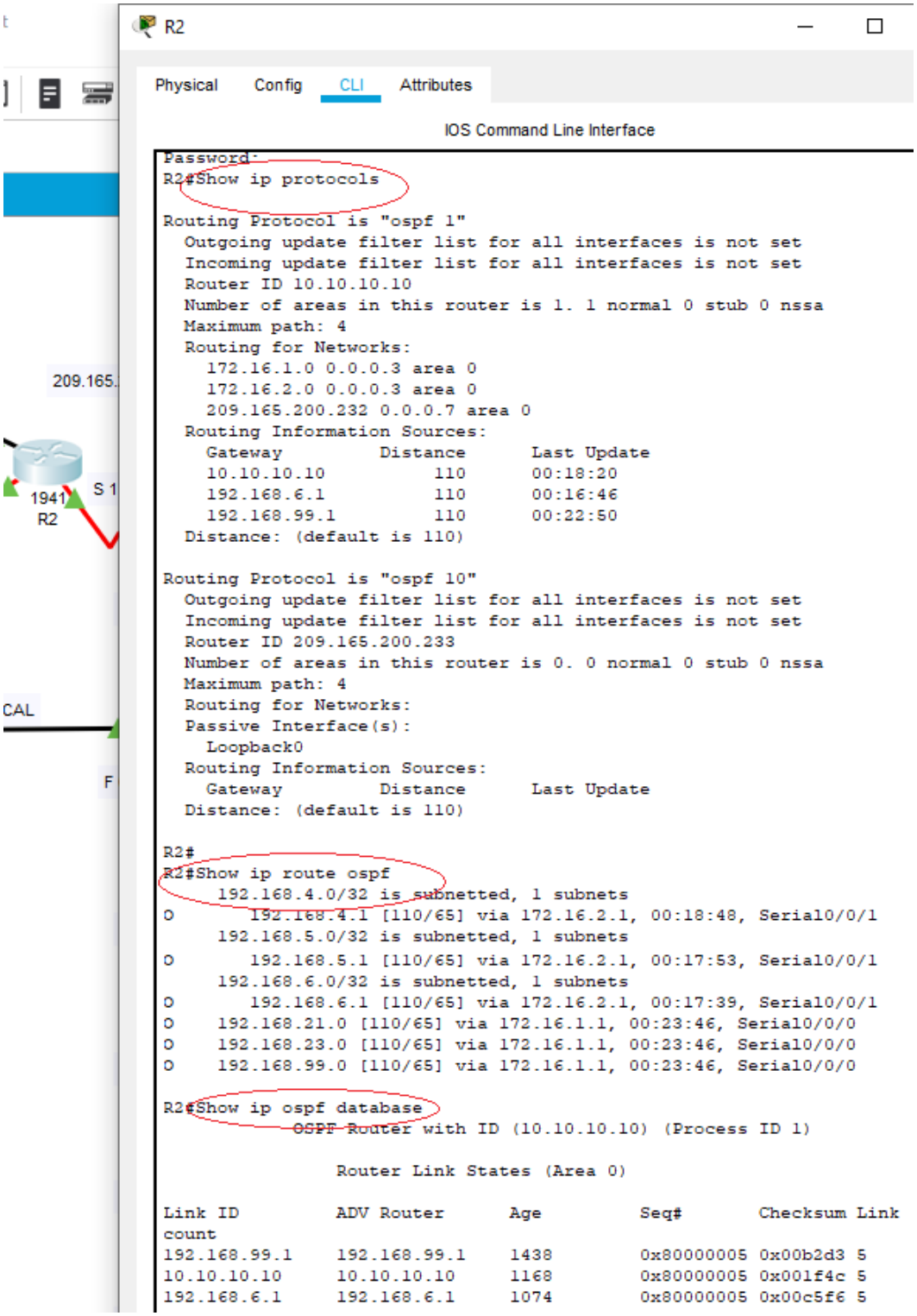
Tabla 20. Verificación de comandos CLI.

| 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? | Se emplea el comando:<br>Show ip protocols |
| ¿Qué comando muestra solo las rutas OSPF? | Se emplea el comando:<br>Show ip route ospf |
| ¿Qué comando muestra la sección de OSPF de la configuración en ejecución? | Se emplea el comando:<br>Show ip ospf database |

Fuente: Tabla tomada de PDF, “PRUEBA DE HABILIDADES CCNA 2022”.

Nota: De acuerdo a las configuraciones anteriores se realiza la asignación de las áreas dado al protocolo OSPF, con el fin de crear las rutas más cortas entre los Router de la red que estén configurados bajo este protocolo, con ello se genera la adyacencia entre vecinos donde por medio de una base de datos que emplea OSPF, determina cual es la mejor ruta para enviar el tráfico de la red entre los dispositivos de esta, mediante el uso de un algoritmo.

Figura 54. Revisión información de comandos CLI.



## 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:

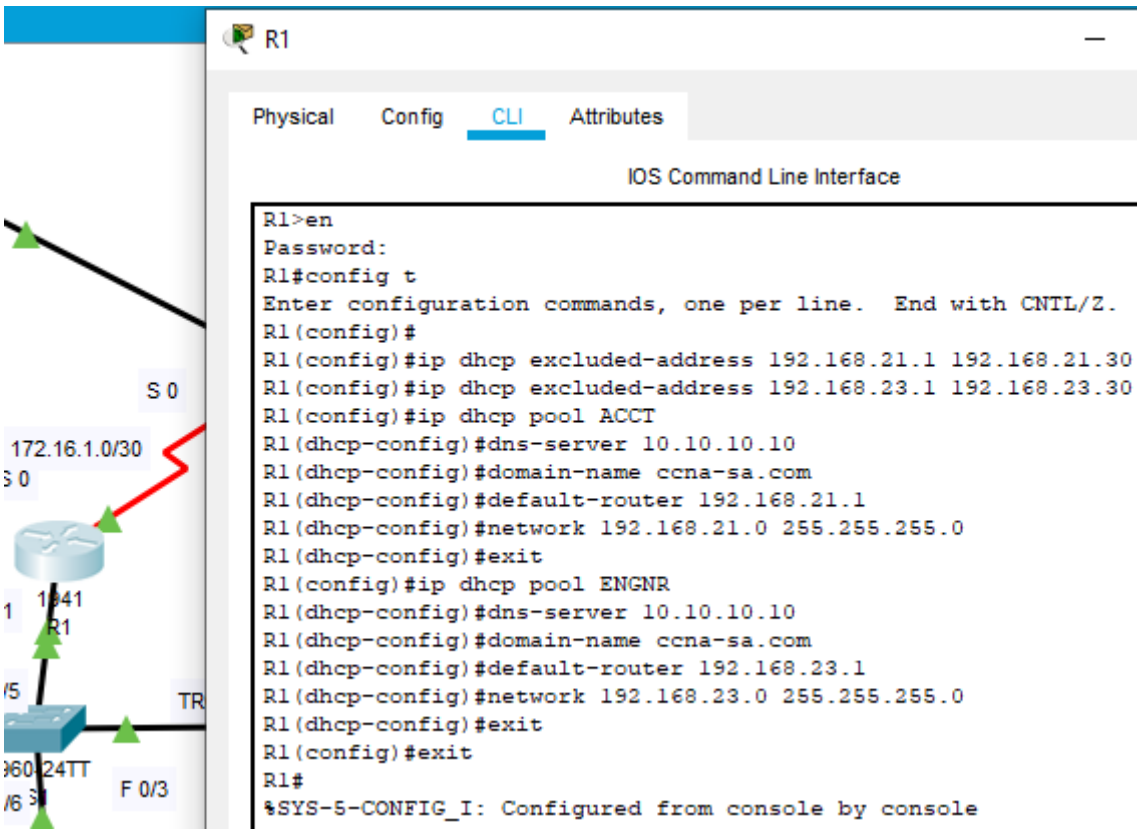
Tabla 21. Configuración R1, Servidor de DHCP

| **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 192.168.21.1 192.168.21.30 |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30 |
| Crear un pool de DHCP para la VLAN 21. | Nombre: ACCT<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado<br><br>R1(config)#ip dhcp pool ACCT<br>R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-sa.com<br>R1(dhcp-config)#default-router 192.168.21.1<br>R1(dhcp-config)#network 192.168.21.0 255.255.255.0<br>R1(dhcp-config)#exit |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado |

| | |
|---|---|
| | R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10<br>R1(dhcp-config)#domain-name ccna-<br>sa.com<br>R1(dhcp-config)#default-router 192.168.23.1<br>R1(dhcp-config)#network 192.168.23.0 255.255.255.0 |

Fuente: Tabla tomada de PDF, **“**PRUEBA DE HABILIDADES CCNA 2022”.

Figura 55. Configuración de R1 como servidor de DHCP.




Fuente: Autoría propia en Packet Treacer

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

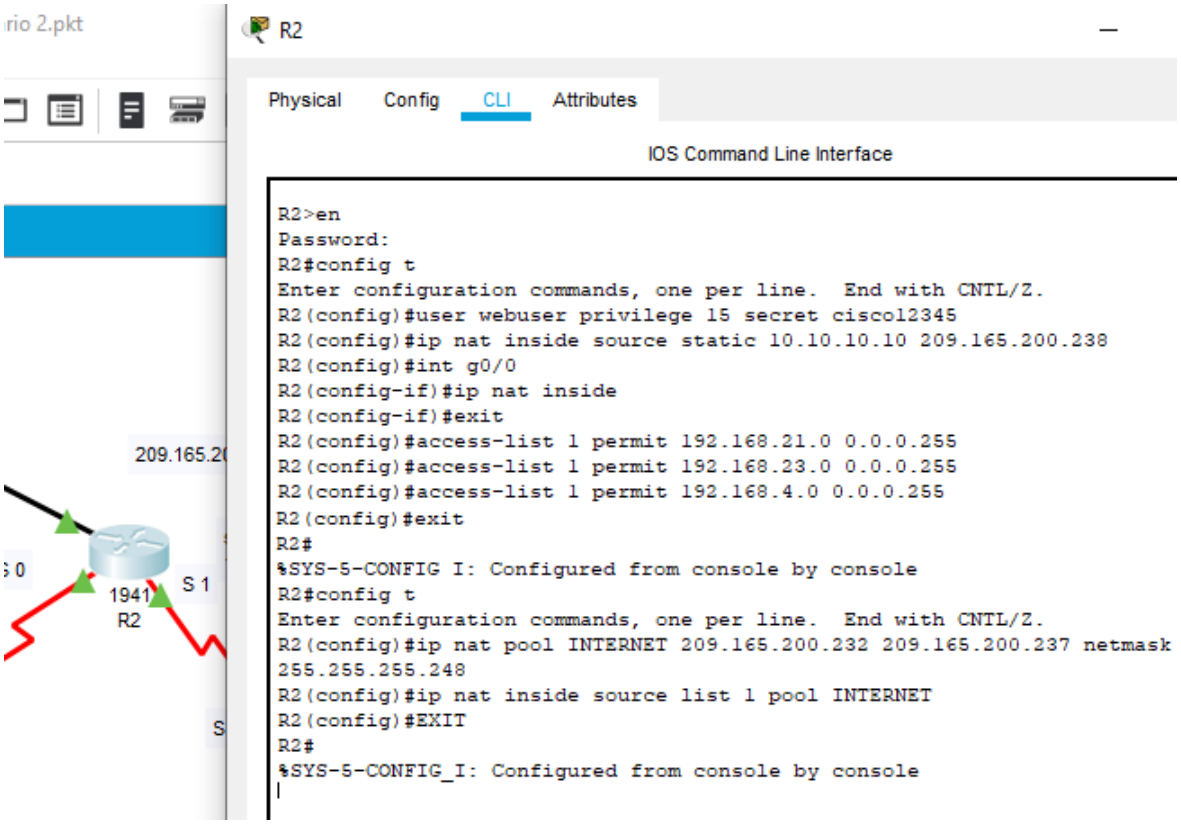
La configuración del R2 incluye las siguientes tareas:

Tabla 22. Configuración NAT estática y dinámica en R2.

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Crear una base de datos local con una cuenta de usuario | Nombre de usuario: **webuser**<br>Contraseña: **cisco12345**<br>Nivel de privilegio: 15<br>R2(config)#user webuser privilege 15 secret cisco12345 |
| Habilitar el servicio del servidor HTTP | No se realiza configuración. |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | No se realiza configuración. |
| Crear una NAT estática al servidor web. | R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238 |
| Asignar la interfaz interna y externa para la NAT estática | R2(config)#int g0/0<br>R2(config-if)#ip nat inside |
| Configurar la NAT dinámica dentro de una ACL privada | R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255<br>R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255 |
| Defina el pool de direcciones IP públicas utilizables. | Nombre del conjunto: **INTERNET**<br>El conjunto de direcciones incluye:<br>R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask 255.255.255.248 |
| Definir la traducción de NAT dinámica | R2(config)#ip nat inside source list 1 pool INTERNET |

Fuente: Tabla tomada de PDF, **"**PRUEBA DE HABILIDADES CCNA 2022".

Figura 56. Configuración NAT estática y dinámica en el R2

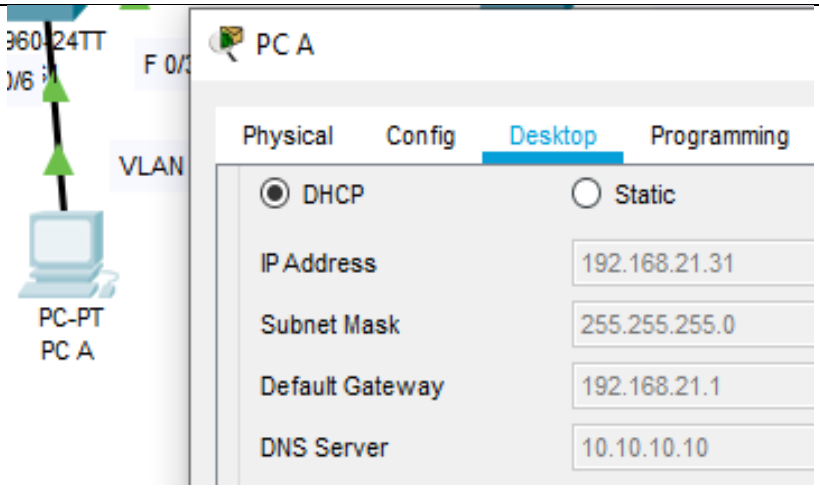
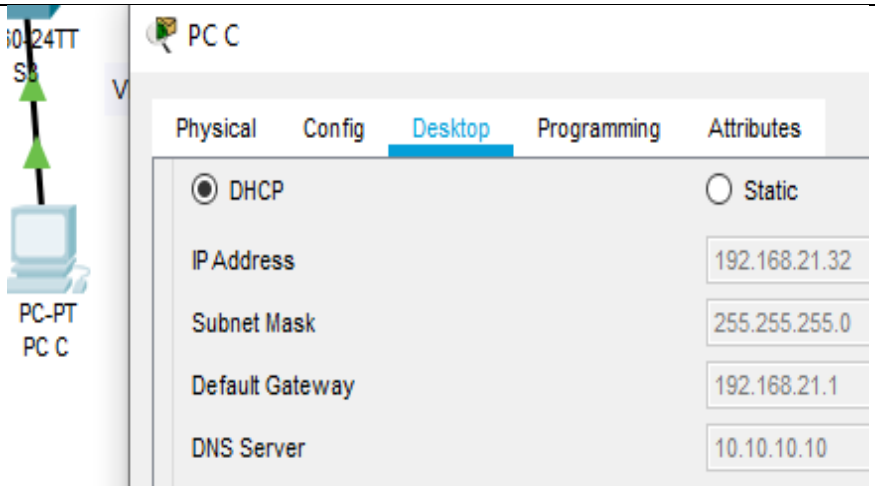


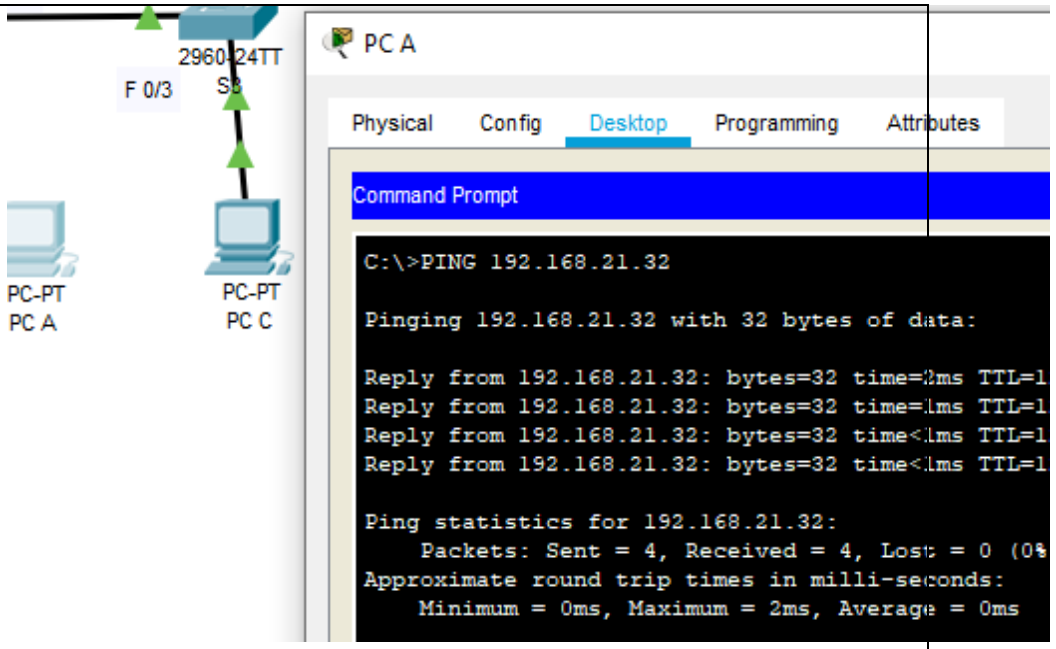
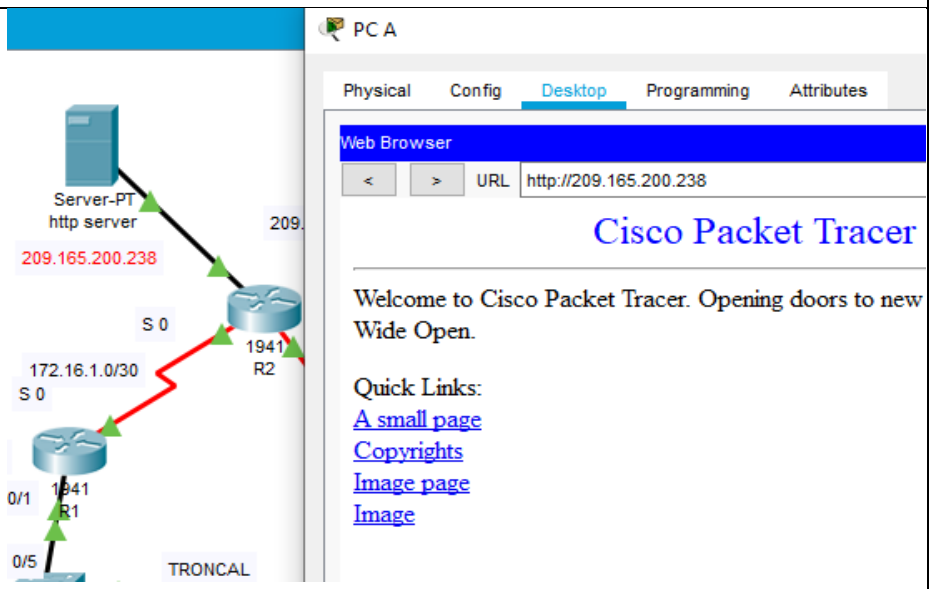

Fuente: Autoría propia en Packet Treacer

**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 22. Pruebas de verificación DHCP y NAT estatica.

| **Prueba** | |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP |  |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP |  |

| | |
|---|---|
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. |  |
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) |  |

Fuente: Tabla tomada de PDF, **“**PRUEBA DE HABILIDADES CCNA 2022”.

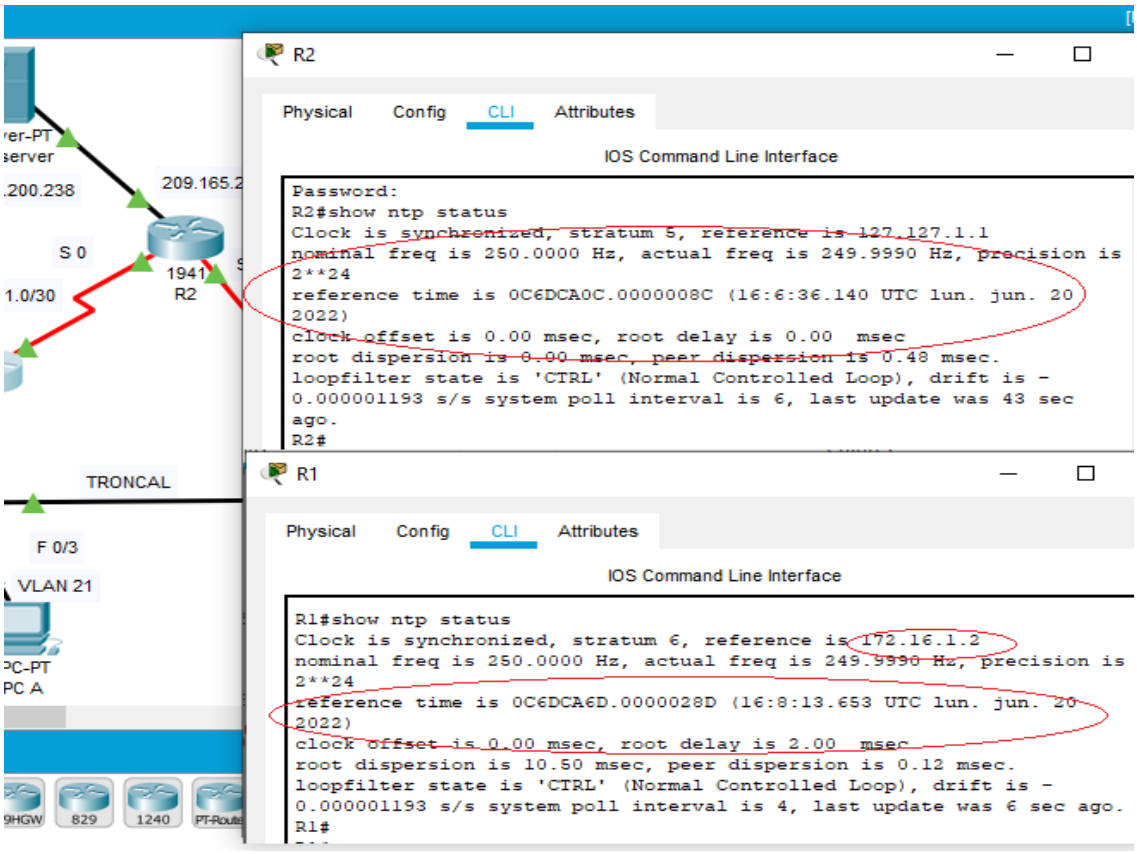
Nota: Con la configuración de los protocolos DHCP y NAT, en los dispositivos R1 Y R2 se logró generar la conexión de los host con enrutamiento dinámico y configuración de las Vlan 21 y 23, sobre R1 dejando este como servidor DHCP y en R2, se configura el protocolo NAT, con el fin de crear rutas estáticas y dinámicas es decir que estas se puedan comunicar o acceder desde la red interna o desde la red externa mediante una lista de direcciones IP de las mismas subredes configuradas.

## Parte 6: Configurar NTP

Tabla 23. Configuración NTP

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | R2#clock set 15:54:10 19 JUN 2022 |
| 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 status |

Figura 57. Configuración NAT y calendario R1 y R2




Nota: De acuerdo a la gráfica anterior se realiza la configuración del protocolo NTP, con el fin de llevar a cabo la sincronización de los relojes de los Router que se encuentran en la misma red.

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

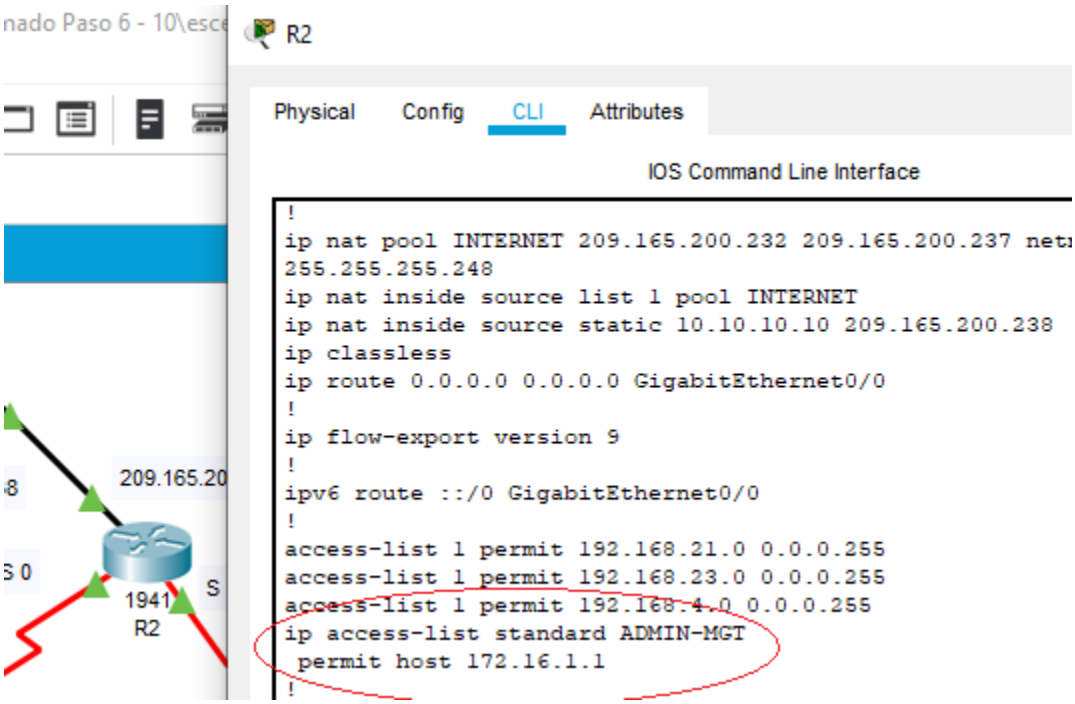
### Paso 1: Restringir el acceso a las líneas VTY en el R2

Tabla 24. Configuración de listas de acceso 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**<br><br>R2(config)#ip access-list standard ADMIN-MGT |
| Aplicar la ACL con nombre a las líneas VTY | R2(config-stdnacl)#permit host 172.16.1.1<br>R2(config-std-nacl)#exit |
| Permitir acceso por Telnet a las líneas de VTY | R2(config-stdnacl)#permit host 172.16.1.1<br>R2(config-std-nacl)#exit |
| Verificar que la ACL funcione como se espera | R2#show run |

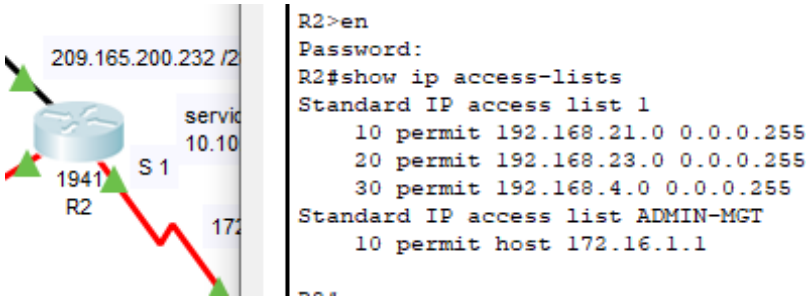
Fuente: Tabla tomada de PDF**, "**PRUEBA DE HABILIDADES CCNA 2022".

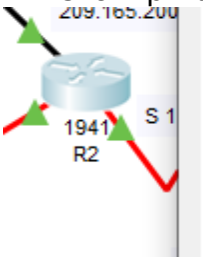
Figura 58. Listas de control de acceso (ACL),  en R2.




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

Tabla 25. Verificación de comandos listas de accesos.

| **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 ip access-lists<br>  |

| | |
|---|---|
| Restablecer los contadores de una lista de acceso | R2#clear access-list counters ip |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | R2#show ip interface<br>  <br>`R2#show ip interface`<br>`GigabitEthernet0/0 is up, line protocol is up`<br>`  Internet address is 209.165.200.232/28`<br>`  Broadcast address is 255.255.255.255`<br>`  Address determined by setup command`<br>`  MTU is 1500 bytes`<br>`  Helper address is not set`<br>`  Directed broadcast forwarding is disabled` |
| ¿Con qué comando se muestran las traducciones NAT? | R2#show ip nat translations<br>`R2#`<br>`R2#`<br>`R2#show ip nat translations`<br>`Pro  Inside global     Inside local       Outside local`<br>`global`<br>`---  209.165.200.238   10.10.10.10        ---` |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | R2#clear ip nat translation |

Fuente: Tabla tomada de PDF, **“**PRUEBA DE HABILIDADES CCNA 2022”.

# CONCLUSIONES

De acuerdo a las actividades anteriores se realiza el análisis y desarrollo del direccionamiento IP, con el fin de conectar las subredes de los dispositivos implementados con el protocolo IP v4, donde se llevan a cabo el enrutamiento solicitado de acuerdo a las dos subredes.

En segundo lugar se logra generar la solución de los escenarios planteados, realizando la implementación de las configuraciones bajo la herramienta de trabajo Packet Tracer, que nos permito afianzar los protocolos de seguridad de consola, configuración de las interfaces, dominios y Vlan de acuerdo a lo solicitado por los requerimientos.

Así mismo de acuerdo a los escenarios, se diseñó el direccionamiento IPv4, de acuerdo a los solicitado en el desarrollo de la practica donde se generaron direcciones IP para la subred de 100 host y 50 host y una Vlan y se configuraron sobre la interfaz de los dispositivos, según los requerimientos del primer escenario y para el segundo escenario se lograron configurar las interfaces Seriales, Gigabit, FastEthernet de los Router y Switches, donde se emplearon protocoles de enrutamiento DHCP, OSPF, ACL, IPv4, IPv6, VLAN y demás configuración para poder conectar el acceso acceso desde el Host hasta el servidor WEB, conectado las diferentes subredes entre cada dispositivo.

## BIBLIOGRAFIA


Ariganello, E. (s. f.). Técnicas de Configuración de Routers CISCO. Grupo Editorial RA-MA.

Cardona, B., & Elvira, M. (2015). El direccionamiento IP. https://riunet.upv.es/handle/10251/47138

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Enredando con redes ...ACLs, Listas de Control de Acceso. (2015, enero 8). Enredando con redes ... https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

López Bulla, R. (2018). Enrutamiento y configuración de redes. Fundación Universitaria del Área Andina. https://doi.org/10.33132/9789585462809

MONOGRÁFICO: Listas de control de acceso (ACL)—Introducción | Observatorio Tecnológico. (s. f.). Recuperado 26 de junio de 2022, de http://recursostic.educacion.es/observatorio/web/gl/software/servidores/1065-listas-de-control-de-acceso-acl?start=1

OSPF Protocol | Open Shortest Path First Protocol—Javatpoint. (s. f.). www.javatpoint.com. Recuperado 26 de junio de 2022, de https://www.javatpoint.com/ospf-protocol

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

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

Qué es un Servidor DHCP. (2019, noviembre 15). OpenWebinars.net. https://openwebinars.net/blog/que-es-un-servidor-dhcp/

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx