

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 DE CIENCIAS 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 DE CIENCIAS 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

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
RESUMEN Y PALABRAS CLAVES.....	9
ABSTRACT AND KEYWORDS.....	10
INTRODUCCIÓN.....	11
DESARROLLO.....	12
Escenario 1.....	12
Escenario 2.....	36
CONCLUSIONES.....	82
BIBLIOGRAFÍA.....	83

LISTA DE TABLAS

Tabla 1. Tabla de direccionamiento escenario 1.....	14
Tabla 2. Tabla de configuración para R1... ..	15
Tabla 3. Configuración S1	25
Tabla 4. PC-A Network Configuration.....	33
Tabla 5. PC-B Network Configuration.....	34
Tabla 6. Inicialización y cargar de Routers y Switches	37
Tabla 7. Direcciones para configurar Servidor WEB	41
Tabla 8. Configuración de tareas R1... ..	43
Tabla 9. Configuración de tareas R2... ..	45
Tabla 10. Configuración de tareas R3... ..	48
Tabla 11. Configuración de tareas S1... ..	51
Tabla 12. Configuración de tareas S3... ..	53
Tabla 13. Verificación de conectividad... ..	55
Tabla 14. Configuración VLAN en S1... ..	56
Tabla 15. Configuración VLAN Y Mode Trunk en S3... ..	59
Tabla 15. Configuración Vlan IPv4 en R1... ..	61
Tabla 16. Pruebas de comunicaciones entre S1 y S3 por VLAN	63
Tabla 17. Configuración de OSPF en R1	64
Tabla 18. Configuración de OSPF en R2.....	66
Tabla 19. Configuración de OSPF en R3.....	67
Tabla 20. Verificación de comandos CLI.....	69
Tabla 21. Configuración R1, Servidor de DHCP	71
Tabla 22. Configuración NAT estática y dinámica en R2... ..	73
Tabla 23. Configuración NTP	77
Tabla 24. Configuración de listas de acceso R2... ..	79
Tabla 25. Verificación de comandos listas de accesos.....	80

LISTA DE FIGURAS

Figura 1. Topología Escenario 1	12
Figura 2. Subredes de escenario 1	14
Figura 3. Escenario de configuración 1	15
Figura 4. Desactivar la búsqueda DNS del R1	16
Figura 5. Asignación Nombre a Router 1	17
Figura 6. Asignación Nombre de dominio	18
Figura 7. Contraseña cifrada modo EXEC privilegiado	18
Figura 8. Asignación de Contraseña de consola	19
Figura 9. Establecer la longitud mínima para la Contraseña	20
Figura 10. Crear un usuario administrativo en la base de datos local	20
Figura 11. Configurar el inicio de sesión en las líneas VTY	21
Figura 12. Configurar VTY solo aceptando SSH	21
Figura 13. Cifrar las contraseñas de texto no cifrado	22
Figura 14. Configure un MOTD Banner	22
Figura 15. Configurar interfaz G0/0/0	23
Figura 16. Configurar interfaz G0/0/1	23
Figura 17. Generar una clave de cifrado RSA, Módulo de 1024 bits	24
Figura 18. Desactivar la búsqueda DNS	26
Figura 19. Nombre del Switch y nombre de dominio	27
Figura 20. Contraseña de acceso a la consola	27
Figura 21. Contraseña cifrada para el modo EXEC privilegiado	28
Figura 22. Crear un usuario administrativo en la base de datos local	29
Figura 23. Configurar el inicio de sesión en las líneas VTY para B.D local	29
Figura 24. Configurar VTY solo aceptando SSH en S1	30
Figura 25. Cifrar las contraseñas de texto no cifrado	30
Figura 26. Configure un MOTD Banner. Mensaje de ingreso no configurado	30
Figura 27. Generar una clave de cifrado RSA, Módulo de 1024 bits	31
Figura 28. Configurar la interfaz de administración (SVI)	32

Figura 29. Configuración del Gateway predeterminado	32
Figura 30. Configuración IP PC A	33
Figura 31. Se anexa evidencia de conectividad de PC A a P CB	34
Figura 32. Configuración IP PC B	35
Figura 33. Se anexa evidencia de conectividad de PC A a P CB	35
Figura 34. Topología escenario 2	36
Figura 35. Inicialización y recarga del R1	38
Figura 36. Inicialización y recarga del R2	38
Figura 37. Inicialización y recarga del R3	39
Figura 38. Inicialización y recarga del S1	39
Figura 39. Revisión de memoria flash en S1	40
Figura 40. Inicialización y recarga del S3	40
Figura 41. Revisión de memoria flash en S3	41
Figura 42. Configuración de servidor WEB	42
Figura 43. Configuración R1	44
Figura 44. Configuración R2	47
Figura 45. Configuración R3	50
Figura 46. Configuración S1	52
Figura 47. Configuración S3	54
Figura 48. Configuración VLAN S1	58
Figura 49. Configuración VLAN y Mode Trunk S3	60
Figura 50. Configuración VLAN IPv4 en R1	62
Figura 51. Configuración del Protocolo dinámico OSPF R1	65
Figura 52. Configuración del Protocolo dinámico OSPF R2	67
Figura 53. Configuración del Protocolo dinámico OSPF R3	68
Figura 54. Revisión información de comandos CLI	70
Figura 55. Configuración de R1 como servidor de DHCP	72
Figura 56. Configuración NAT estática y dinámica en el R2	74
Figura 57. Configuración NAT y calendario R1 y R2	78
Figura 58. Listas de control de acceso (ACL), en R2	80

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 embargo 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

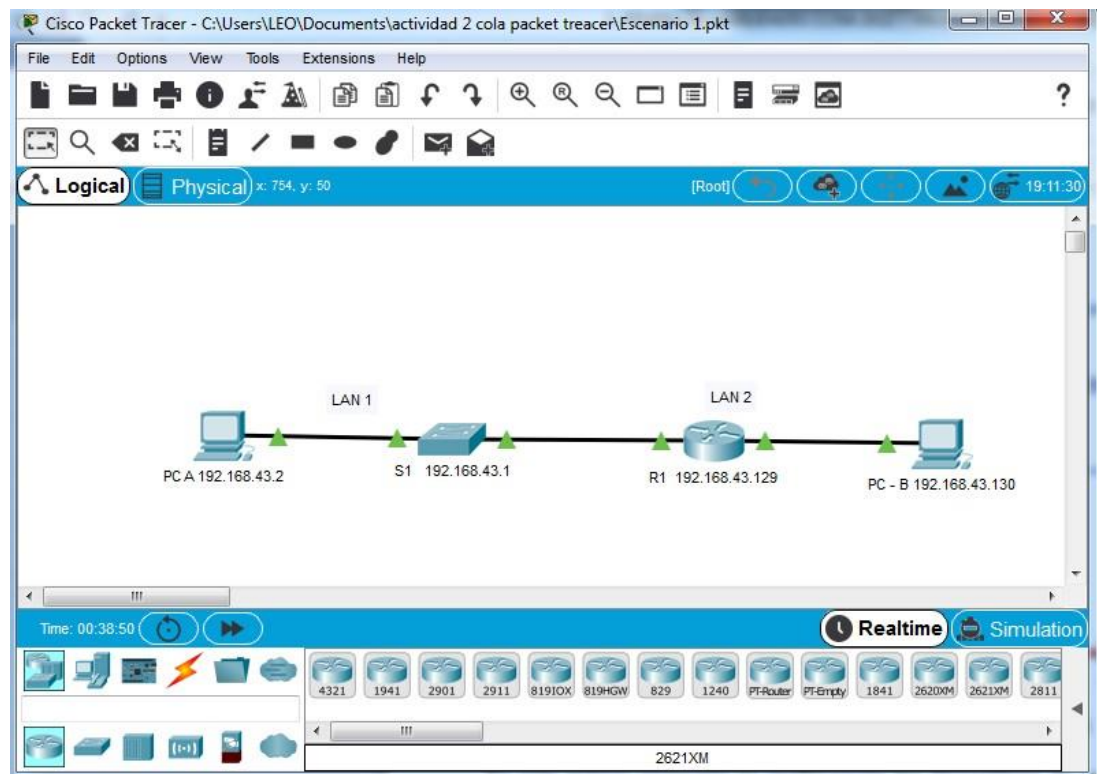
1. ESCENARIO 1

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 Tracer

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.

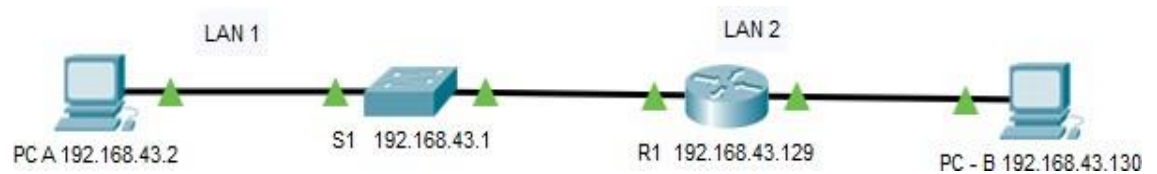
Item	Requerimiento
Dirección de Red	192.168.X.0 donde X corresponde a los últimos dos dígitos de mi cédula. 192.168.43.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	Primera dirección de host de la subred LAN1 192.168.43.1
R1 G0/0/0	Primera dirección de host de la subred LAN2 192.168.43.129
S1 SVI	Segunda dirección de host de la subred LAN1 192.168.43.2
PC-A	Última dirección de host de la subred LAN1 192.168.43.126
PC-B	Última dirección de host de la subred LAN2 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 R1(config)# ip domain-lookup 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 las contraseñas	10 caracteres

Crear un usuario administrativo en la base de datos local	Nombre de usuario: admin Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para 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 Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección Ipv4. 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#copy
Translating "copy"...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 Tracer

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 Tracer

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

```
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R1
!
```

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)#

```
!
username admin password 0 admin1pass
!
```

Figura 11. Configurar el inicio de sesión en las líneas VTY para que use la base de datos local.

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

```
^
login
!
line aux 0
!
line vty 0 4
  login local
  transport input ssh
!
!
```

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)#
```

```
:
line vty 0 4
  login local
  transport input ssh
!
!
!
end
```

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
```

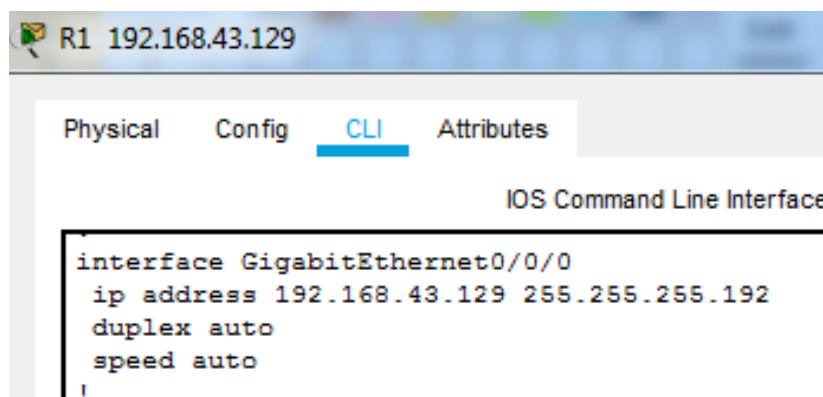
```
| ip flow-export version 9  
|  
|  
|  
| banner motd ^CEl acceso a R1 esta restringido. Solo personal  
| autorizado^C  
|  
|
```

Fuente: Autoría propia en Packet Tracer

Figura 15. Configurar interfaz G0/0/0

Se realiza la configuración de la interfaz GigabitEthernet 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 Tracer

Figura 16. Configurar interfaz G0/0/1

se realiza la configuración de la interfaz GigabitEthernet 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 S1#config t S1(config)#hostname S1
Nombre de dominio	ccna-lab.com S1(config)#ip domain-lookup 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 Password: admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	
Configurar las líneas VTY para que acepten únicamente las 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	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 Tracer

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
```

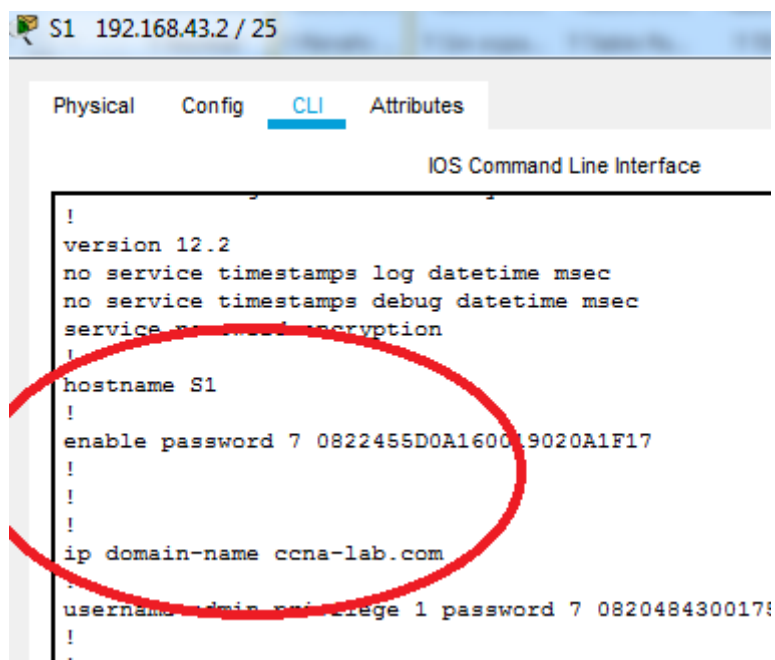


Figura 20. Contraseña de acceso a la consola

```
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
```

```
S1 192.168.43.2 / 25
Physical Config CLI Attributes
IOS Command Line
!
!
line con 0
 password 7 0822455D0A1606181C1B0D1739
 login
!
```

Fuente: Autoría propia en Packet Tracer

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
```

```
S1 192.168.43.2 / 25
Physical Config CLI Attributes
IOS Command Line Interface
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable password 7 0822455D0A160019020A1F17
!
```

Figura 22. Crear un usuario administrativo en la base de datos local.

Password: admin1pass, Nombre de usuario: admin

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



Fuente: Autoría propia en Packet Tracer

Figura 23. Configurar el inicio de sesión en las líneas VTY para 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 en la configuración.

```
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
```

```

!
!
!
!
!
!
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]

```

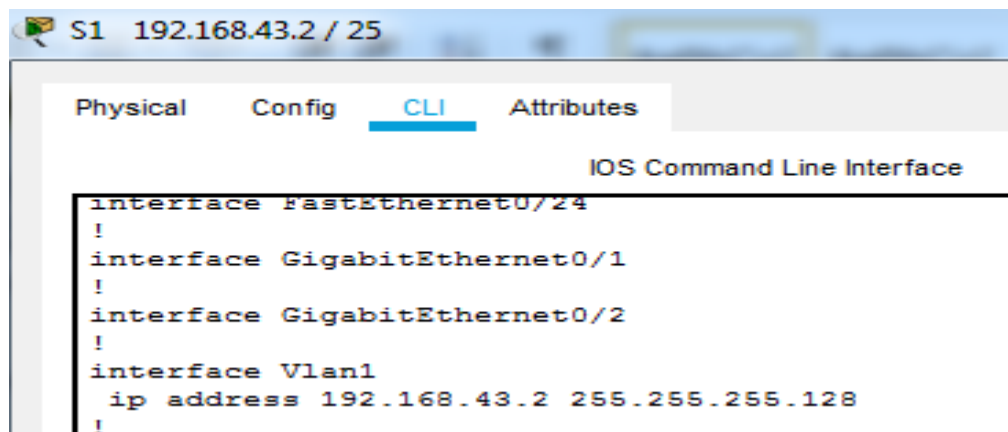
```

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
```

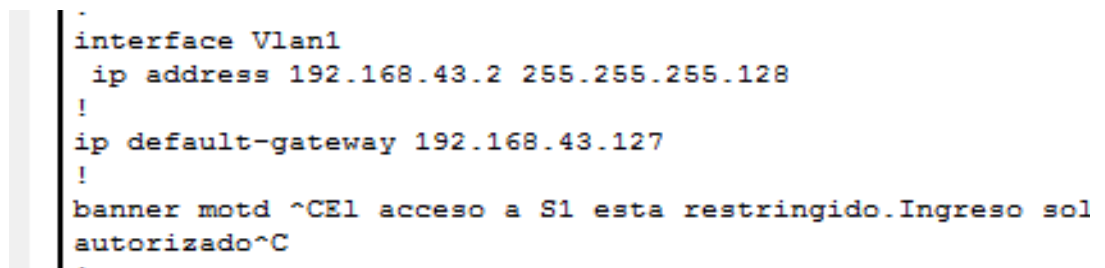


The screenshot shows a network device's CLI interface. The title bar indicates the device is S1 with IP 192.168.43.2 / 25. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The main window displays the following configuration commands:

```
IOS Command Line Interface
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.43.2 255.255.255.128
!
```

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
```



The screenshot shows a network device's CLI interface with the following configuration commands:

```
interface Vlan1
 ip address 192.168.43.2 255.255.255.128
!
 ip default-gateway 192.168.43.127
!
 banner motd ^CEl acceso a S1 esta restringido.Ingreso sol
 autorizado^C
.
```


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

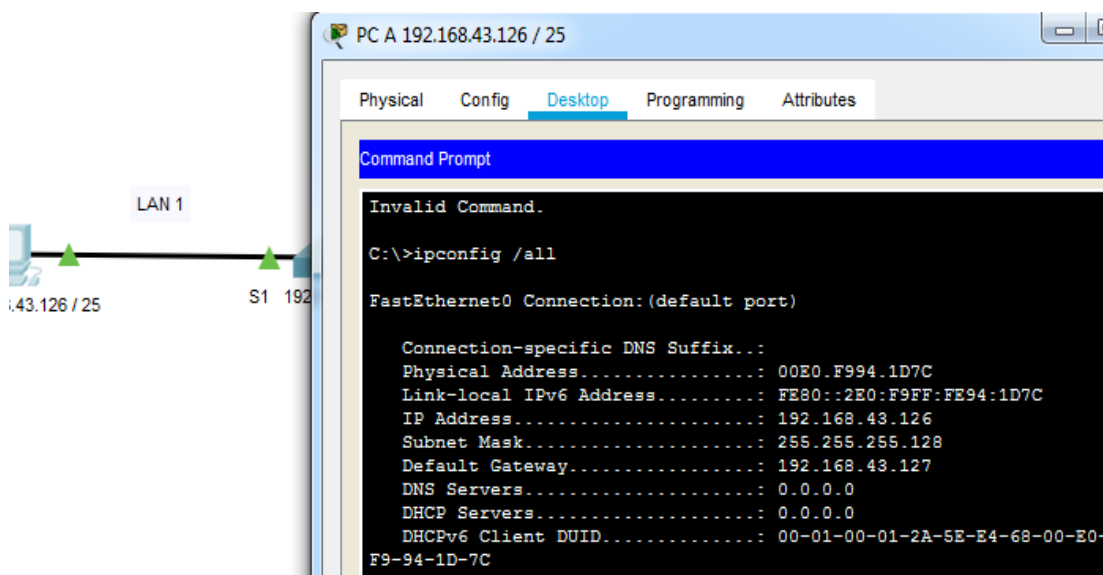
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

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 Tracer

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.

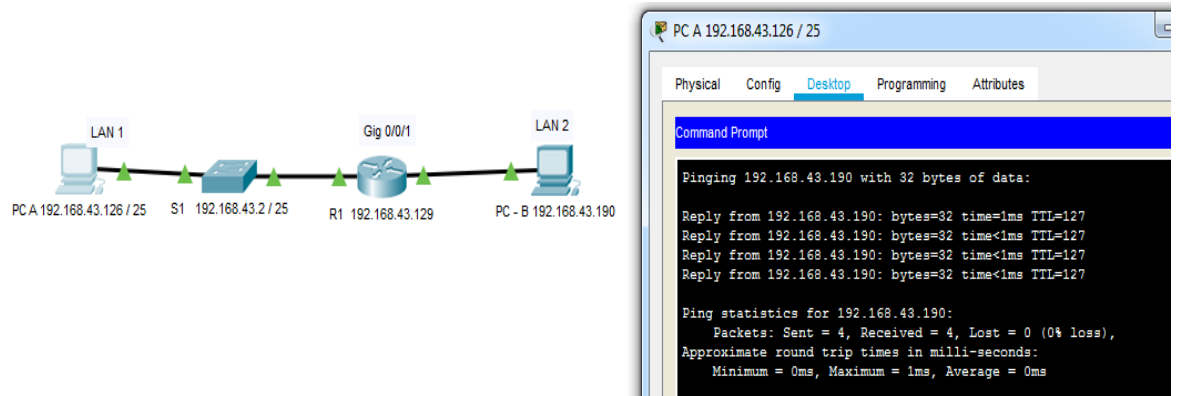


Tabla 5. PC-B Network Configuration

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.

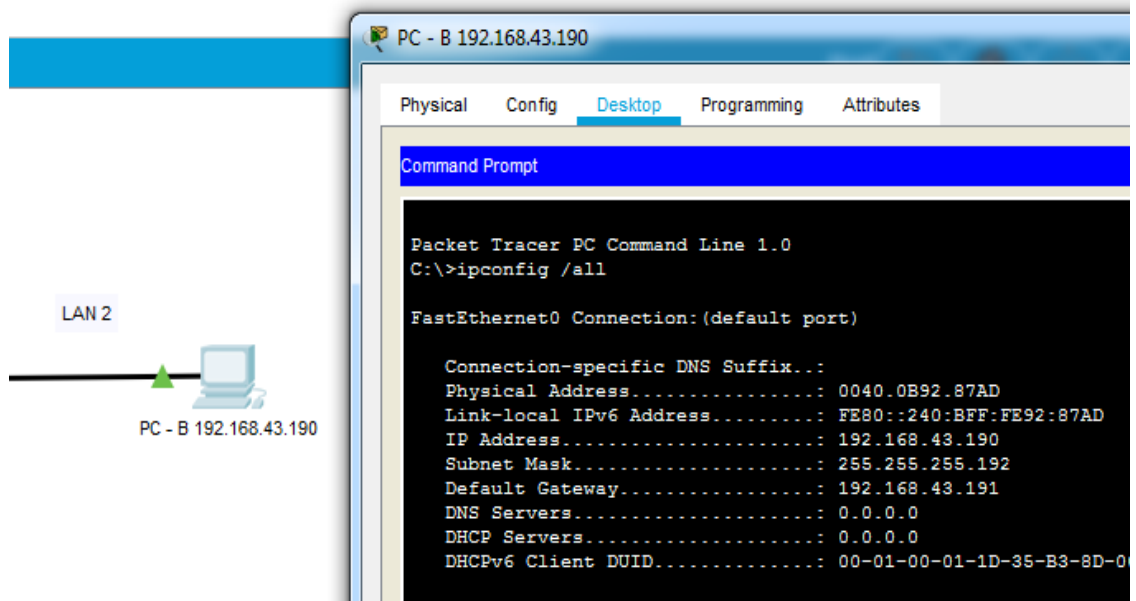
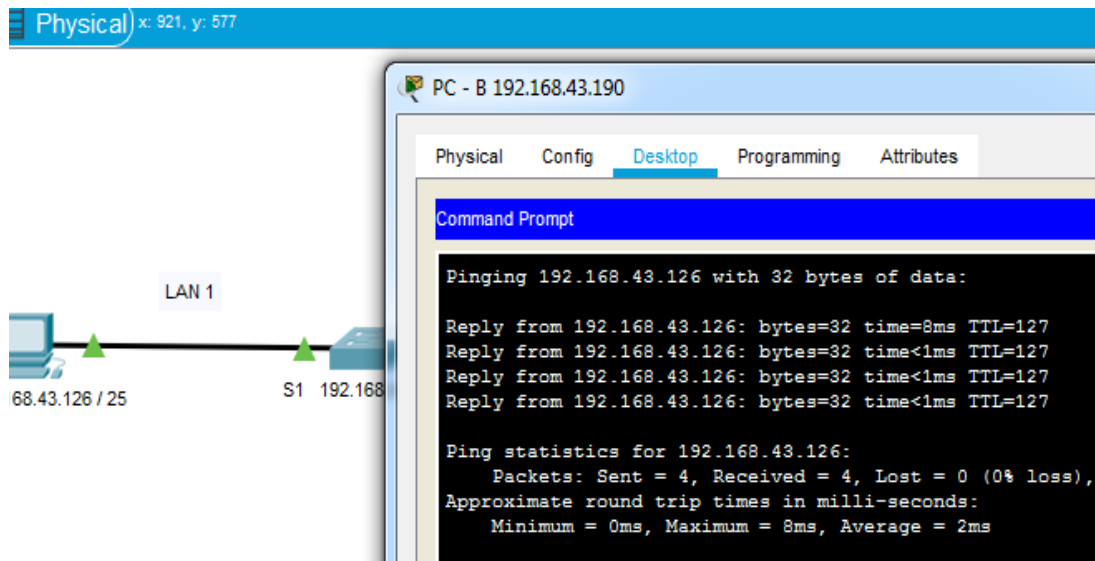


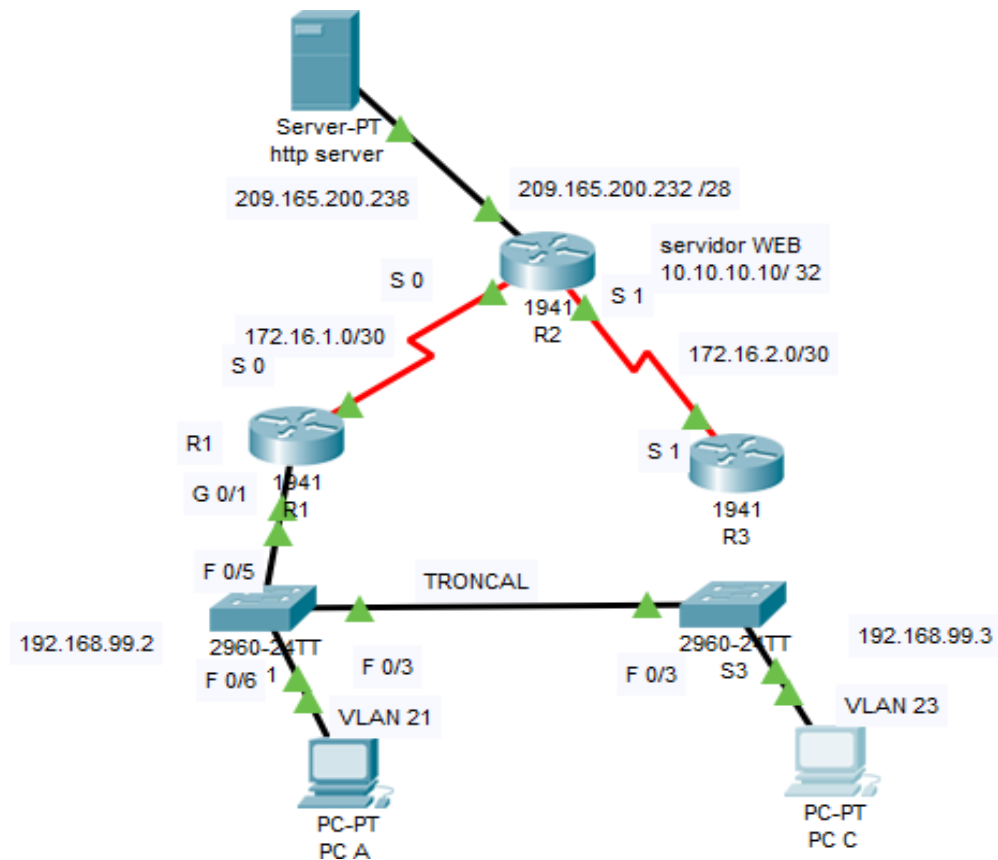
Figura 33. Se anexa evidencia de conectividad de PC A a P CB.
Se realiza ping desde la PC B a la PC A, es decir de la LAN 2 a la LAN 1.



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 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#delete vlan.dat 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

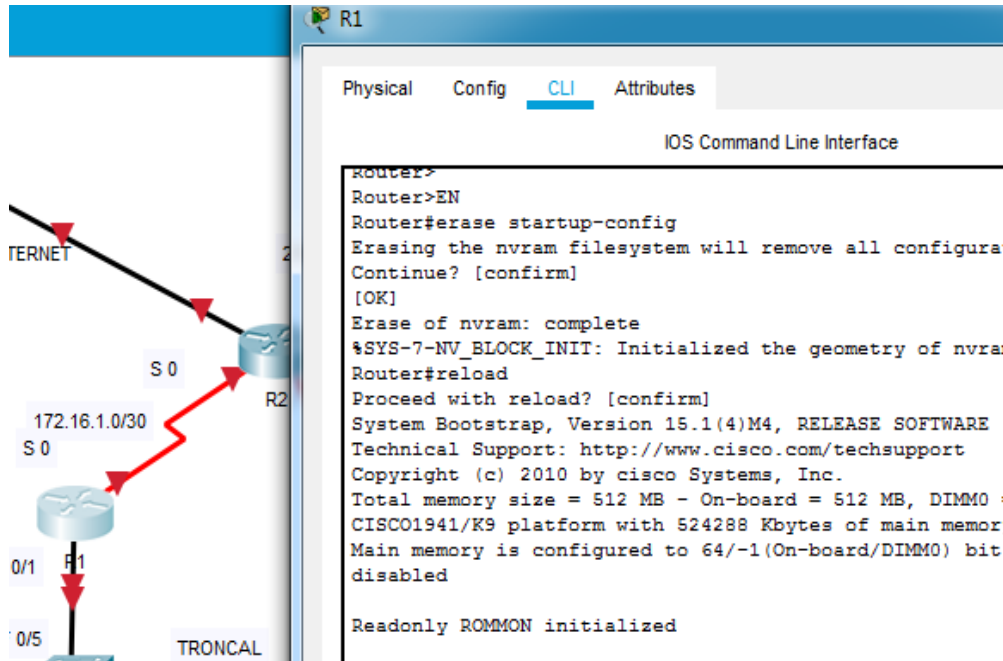


Figura 36. Inicialización y recarga del R2

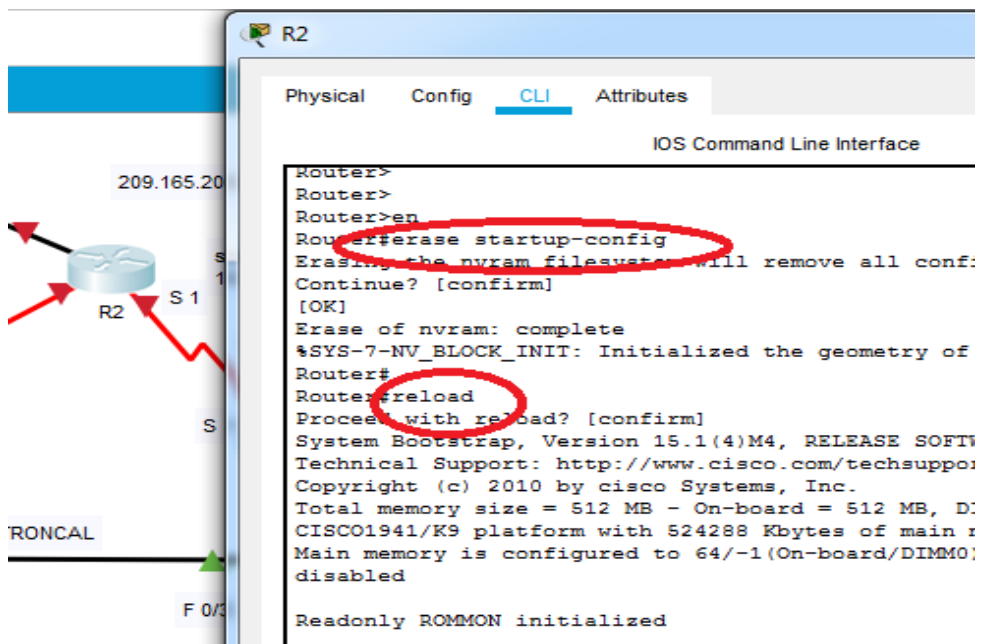


Figura 37. Inicialización y recarga del R3.

The screenshot shows a network diagram on the left and the CLI interface for router R3 on the right. In the diagram, R3 is connected to a switch S3 at interface F0/3. A server labeled 'servidor WEB' is connected to R3 at interface S1 with IP 10.10.10.10/32. Another server is connected to R3 at interface S1 with IP 172.16.2.0/30. The CLI window shows the following commands and output:

```

Router>
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all c
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry
Router#
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE S
Technical Support: http://www.cisco.com/techsu
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB
CISCO1941/K9 platform with 524288 Kbytes of ma
Main memory is configured to 64/-1(On-board/DI
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000
program load complete, entry point: 0x80803000
    
```

Figura 38. Inicialización y recarga del S1.

The screenshot shows a network diagram on the left and the CLI interface for switch S1 on the right. In the diagram, S1 is connected to a router R0 at interface F1/0/5. A PC is connected to S1 at interface F0/6 in VLAN 21. The CLI window shows the following commands and output:

```

Switch>
Switch>en
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such fi:

Switch#erase startup-config
Erasing the nvram filesystem will remove all:
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geomet
Switch#
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 1:
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (rev
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0002.1612.DE04
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
    
```

Fuente: Autoría propia en Packet Tracer

Figura 39. Revisión de memoria flash en S1.

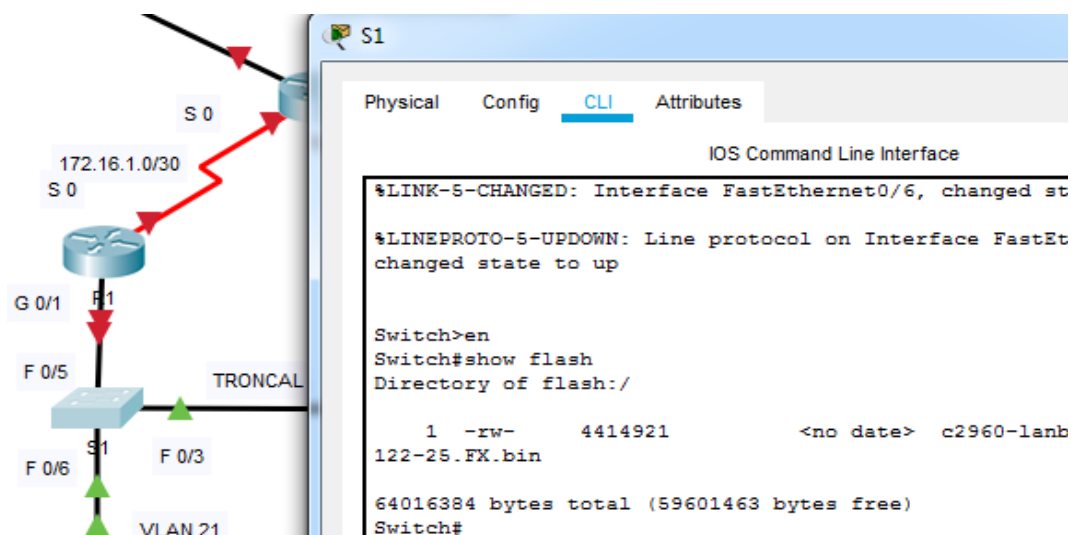
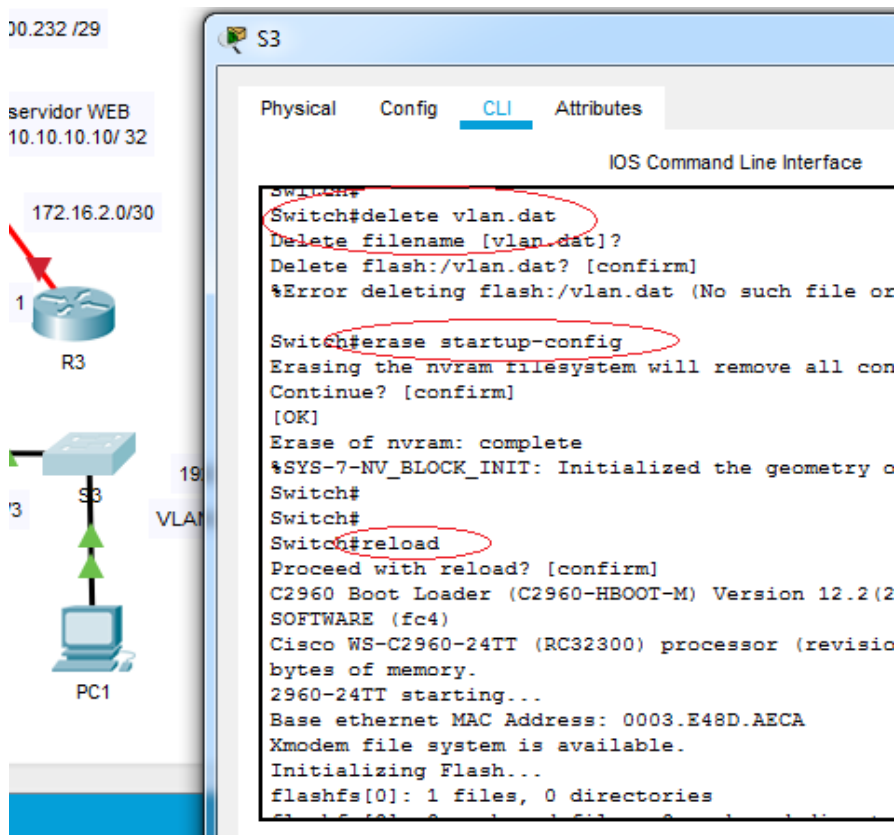
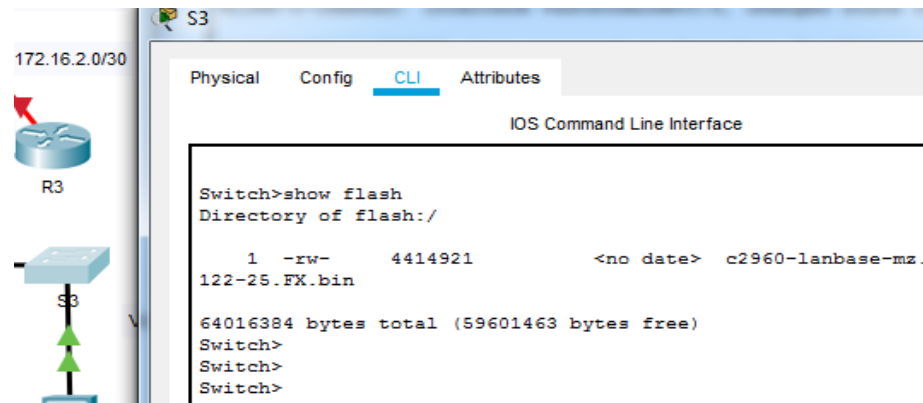


Figura 40. Inicialización y recarga del S3.



Fuente: Autoría propia en Packet Tracer

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.

The image shows a Packet Tracer configuration for an http server. On the left, a server icon labeled 'Server-PT http server' is connected to a router icon labeled 'R1' via a serial link labeled 'S0'. The server's IP address is shown as '209.165.200.238'. The router's interface is labeled 'S0' and has an IPv4 address of '172.16.1.0/30'. The configuration window for the http server is open, showing the following settings:

Category	Option	Value
IPv4 Configuration	<input type="radio"/> DHCP	
	<input checked="" type="radio"/> Static	
	IP Address	209.165.200.238
	Subnet Mask	255.255.255.248
Default Gateway	209.165.200.239	
DNS Server	0.0.0.0	
IPv6 Configuration	<input type="radio"/> DHCP	
	<input type="radio"/> Auto Config	
	<input checked="" type="radio"/> Static	
	IPv6 Address	2001:DB8:ACAD:A::38
	Link Local Address	FE80::201:C7FF:FEA1:DCB0
IPv6 Gateway	2001:DB8:ACAD:2::1	
IPv6 DNS Server		

Fuente: Autoría propia en Packet Tracer

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:

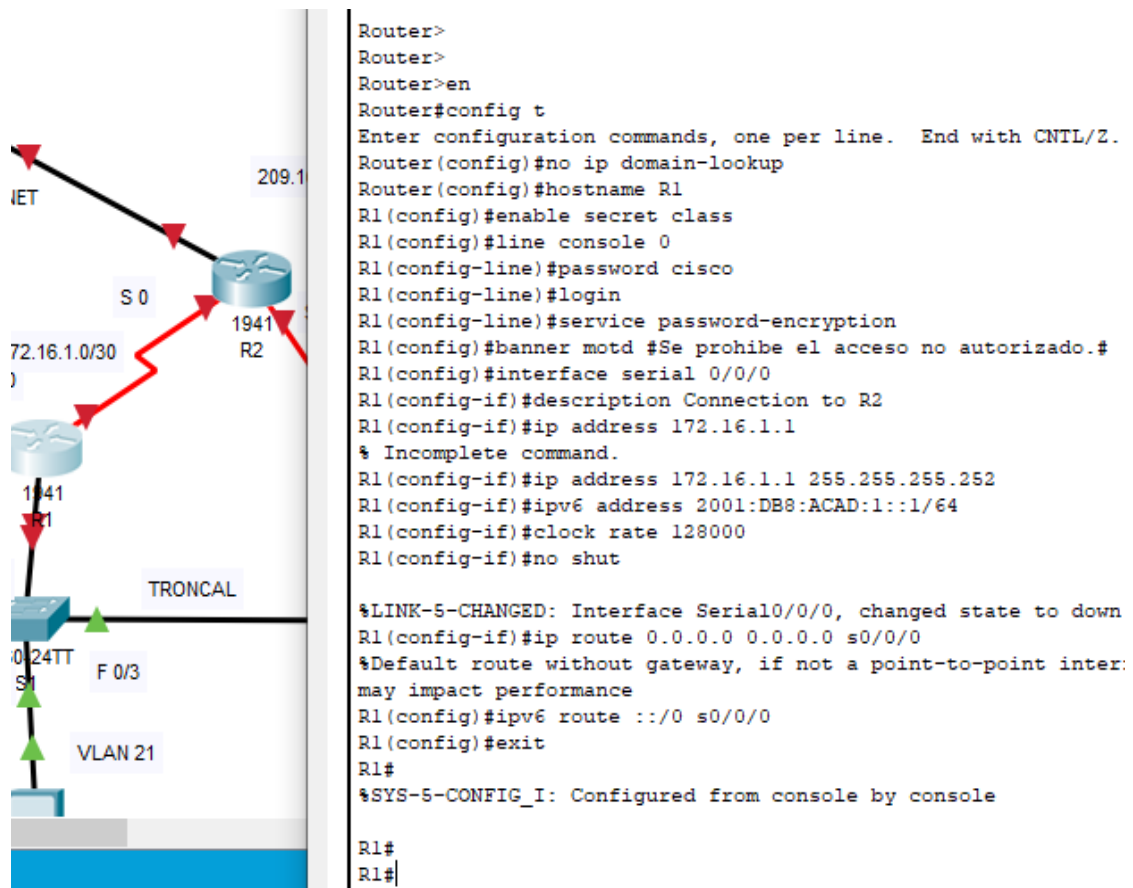
Tabla 8. Configuración de tareas R1.

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 R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config-line)#line vty 0 4 R1(config-line)#password cisco 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 R1(config-if)#description Connection to R2 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000

	R1(config-if)#no shutdown
Rutas predeterminadas	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)#ipv6 unicast 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:

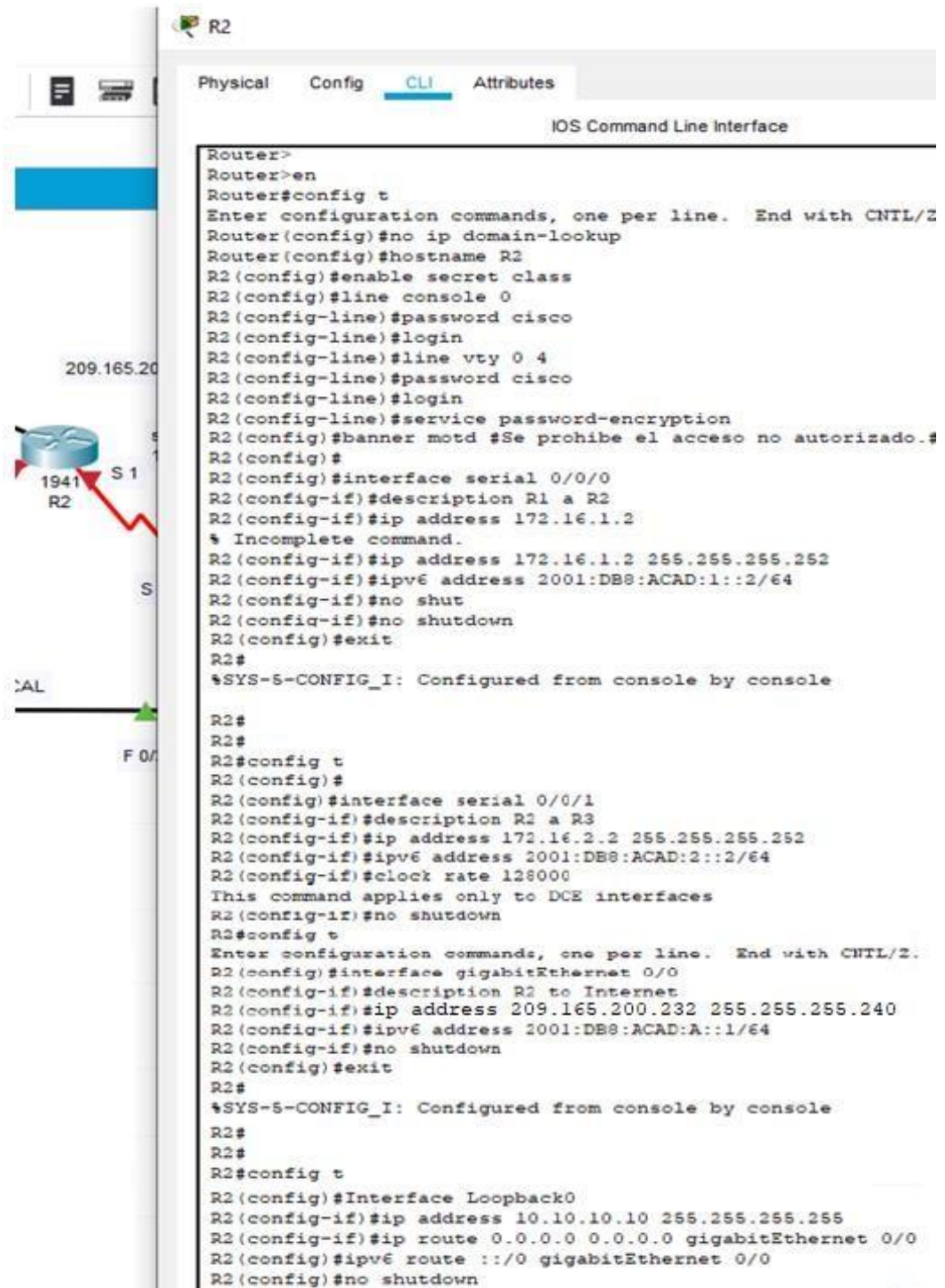
Tabla 9. Configuración de tareas R2.

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 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server
Mensaje MOTD	R2(config)#banner motd #Se prohíbe el acceso no autorizado.#
Interfaz S0/0/0	R2(config)#interface serial 0/0/0 R2(config-if)#description R1 a R2 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 serial 0/0/1 R2(config-if)#description R2 a R3 R2(config-if)#ip address 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 address

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

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

Figura 44. Configuración R2.



The screenshot displays the configuration of Router R2 in Packet Tracer. The interface shows the CLI with the following commands and output:

```

Router>
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#banner motd #Se prohíbe el acceso no autorizado.#
R2(config)#
R2(config)#interface serial 0/0/0
R2(config-if)#description R1 a R2
R2(config-if)#ip address 172.16.1.2
% Incomplete command.
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 shut
R2(config-if)#no shutdown
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R2#
R2#config t
R2(config)#
R2(config)#interface serial 0/0/1
R2(config-if)#description R2 a 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
This command applies only to DCE interfaces
R2(config-if)#no shutdown
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#description R2 to Internet
R2(config-if)#ip address 209.165.200.232 255.255.255.240
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#
R2#
R2#config t
R2(config)#Interface Loopback0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0
R2(config)#ipv6 route ::/0 gigabitEthernet 0/0
R2(config)#no shutdown

```

Fuente: Autoría propia en Packet Tracer

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 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado.#
Interfaz S0/0/1	R3(config)#interface serial 0/0/1 R3(config-if)#description R3 a 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 lo4 R3(config-if)#ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config)#interface lo5 R3(config-if)#ip address 192.168.5.1

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

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

Figura 45. Configuración R3.

```

R3
Physical Config CLI Attributes
IOS Command Line Interface

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#service password-encryption
R3(config)#banner motd #Se prohíbe el acceso no autorizado.#
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#exit
R3>en
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface serial 0/0/1
R3(config-if)#description R3 a R2
R3(config-if)#ip address 172.16.2.1
% Incomplete command.
R3(config-if)#255.255.255.252
^
% Invalid input detected at '^' marker.
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

%LINK-S-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#
R3(config-if)#interface lo4

R3(config-if)#
%LINK-S-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Loopback4, changed
state to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#interface lo5

R3(config-if)#
%LINK-S-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Loopback5, changed
state to up
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface lo6

R3(config-if)#
%LINK-S-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Loopback6, changed
state to up
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#interface lo7

R3(config-if)#
%LINK-S-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface Loopback7, changed
state to up
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#ipv6 unicast-routing
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface,
may impact performance
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface,
may impact performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#
  
```

Fuente: Autoría propia en Packet Tracer

Nota: Después de inicializar los dispositivos pertenecientes al escenario 2, se lleva a cabo 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 de las 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

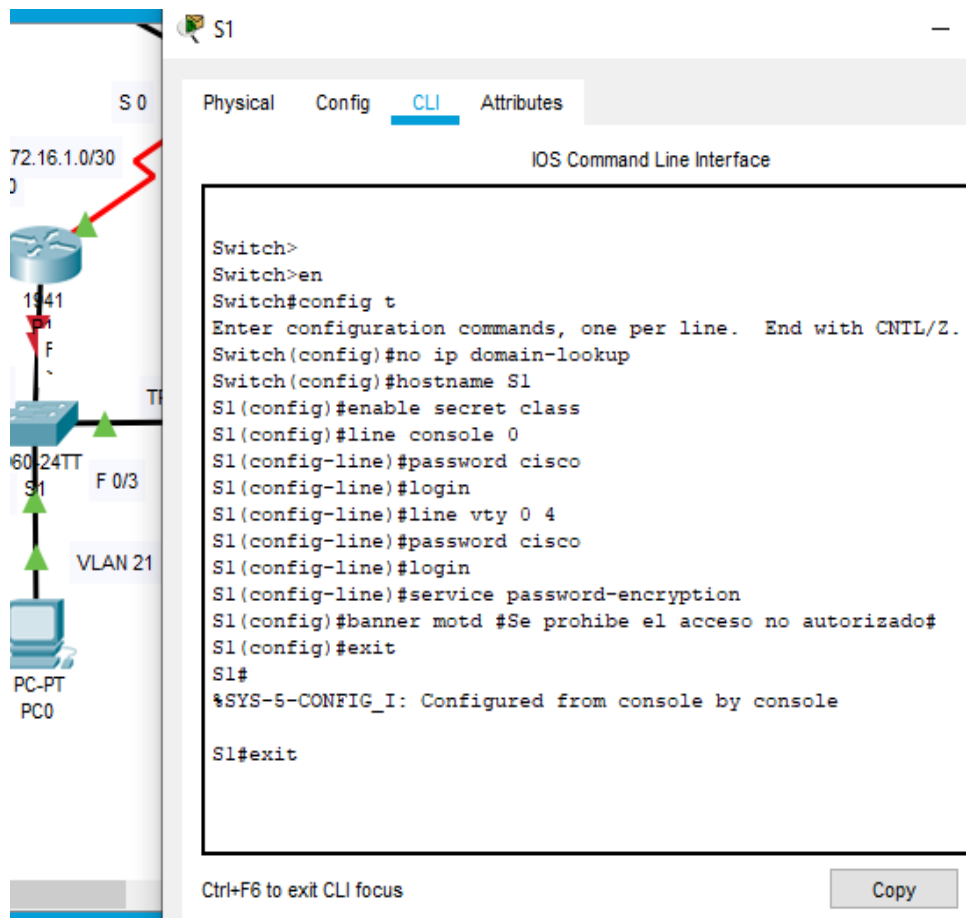
La configuración del S1 incluye las siguientes tareas:

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 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config-line)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login
Cifrar las contraseñas de texto no cifrado	S1(config-line)#service password-encryption
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

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

Figura 46. Configuración S1.



The screenshot shows the configuration of switch S1 in Packet Tracer. The network diagram on the left shows S1 connected to a router (S0) and a PC (PC0). The CLI window on the right displays the configuration commands for S1.

```
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #Se prohíbe el acceso no autorizado#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#exit
```

Fuente: Autoría propia en Packet Tracer

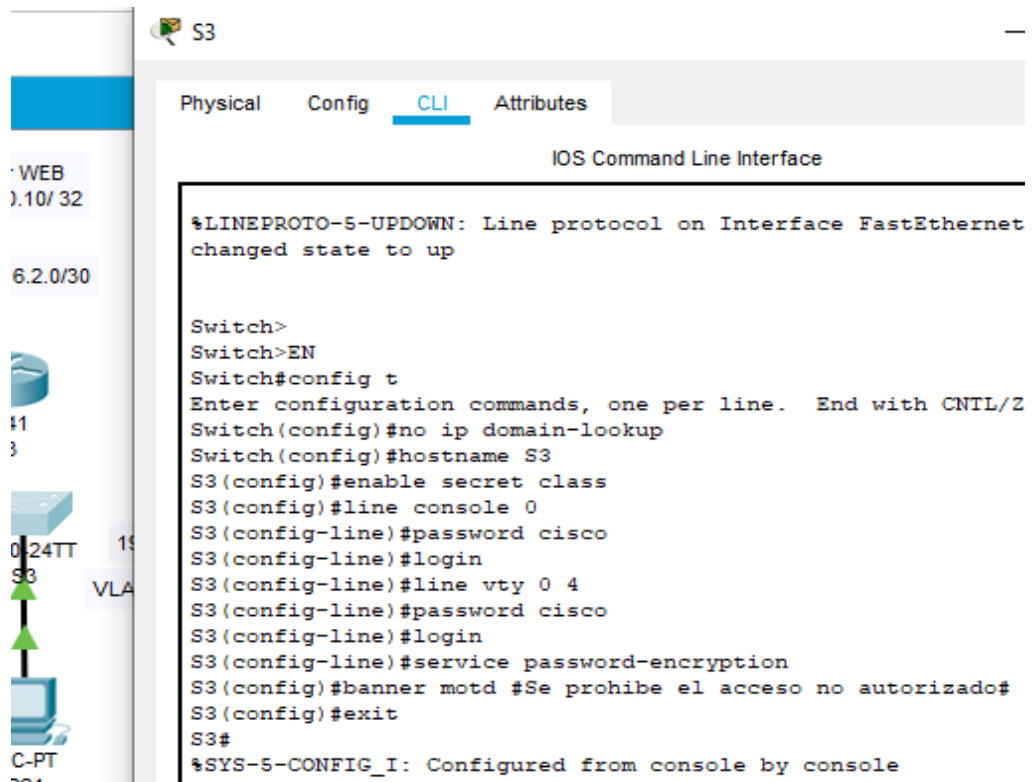
Paso 6: Configurar el S3. La configuración del S3 incluye las siguientes tareas:

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 S3(config-line)#password cisco S3(config-line)#login
Contraseña de acceso Telnet	S3(config-line)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login
Cifrar las contraseñas de texto no cifrado	S3(config-line)#service password-encryption
Mensaje MOTD	S3(config)#banner motd #Se prohíbe el acceso no autorizado#

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

Figura 47. Configuración S3.



```
Switch>
Switch>EN
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #Se prohíbe el acceso no autorizado#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Fuente: Autoría propia en Packet Tracer

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	<pre>R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, !!!! Success rate is 100 percent (5/5), round-trip R1#</pre>
R2	R3, S0/0/1	172.16.2.1	<pre>R2#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, !!!! Success rate is 100 percent (5/5), round-trip R2#</pre>

PC de Internet	Gateway predeterminado	209.165.200.233	<pre>C:\>ping 209.165.200.233 Pinging 209.165.200.233 with 32 bytes of data: Reply from 209.165.200.233: bytes=32 time<1ms Reply from 209.165.200.233: bytes=32 time<1ms Reply from 209.165.200.233: bytes=32 time<1ms Reply from 209.165.200.233: bytes=32 time<1ms Ping statistics for 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
----------------	------------------------	-----------------	---

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 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion
Asignar la dirección IP de administración.	S1(config)#interface vlan 99 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 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	S1(config)#interface fastEthernet 0/5 S1(config-if)#switchport mode trunk 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 S1(config-if-range)#switchport mode access
Asignar F0/6 a la VLAN 21	S1(config)#interface range fa0/6 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 S1(config-if-range)#shutdown

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

Figura 48. Configuración VLAN S1.



```

cer/escenario 2.pkt S1
Physical Config CLI Attributes
IOS Command Line Interface
Password:
S1>en
Password:
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#interface vlan 99
S1(config-if)#
*LINK-S-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2
* Incomplete command.
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
*LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
*LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
*LINEPROTO-S-UPDOWN: Line protocol on Interface Vlan99, changed stat
to up
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#interface fastEthernet 0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface range fa0/1-2, fa0/4, fa0/6-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#interface range fa0/6
S1(config-if-range)#exit
S1(config)#interface range fa0/6
S1(config-if-range)#switchport access vlan 21
S1(config-if-range)#interface range fa0/1-2, fa0/4, fa0/7-24, gi0/
S1(config-if-range)#shutdown
*LINK-S-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/2, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/4, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/7, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/8, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/9, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/10, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/11, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/12, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/13, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/14, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/15, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/16, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/17, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/19, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/20, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/21, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/22, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/23, changed state to
administratively down
*LINK-S-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
*LINK-S-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
*LINK-S-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
S1(config-if-range)#exit
S1(config)#shutdown
* Invalid input detected at '^' marker.
S1(config)#exit
S1#
*SYS-S-CONFIG_I: Configured from console by console
S1#shutdown
Translating "shutdown"
* Unknown command or computer name, or unable to find computer
address
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Fuente: Autoría propia en Packet Tracer

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	<pre>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</pre>
Asignar la dirección IP de administración.	<pre>S3(config)#interface vlan 99 S3(config-if)#ip address 192.168.99.3 255.255.255.0</pre>
Asignar el gateway predeterminado	<pre>S3(config)#ip default-gateway 192.168.99.1</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S3(config)#interface fastEthernet 0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S3(config)#interface range fa0/1- 2,fa0/4-24,gi0/1-2 S3(config-if-range)#switchport mode access S3(config-if-range)#exit</pre>
Asignar F0/18 a la VLAN 21	<pre>S3(config)#interface fastEthernet 0/18 S3(config-if)#switchport access vlan 21 S3(config-if)#exit</pre>
Apagar todos los puertos sin usar	<pre>S3(config)#interface range fa0/1- 2,fa0/4-17,fa0/19-24,gi0/1-2 S3(config-if-range)#shutdown S3(config-if-range)#exit</pre>

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

Figura 49. Configuración VLAN y Mode Trunk 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 Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz: R1(config)#interface gigabitEthernet 0/1.21 R1(config-subif)#description accounting LAN de Contabilidad R1(config-subif)#encapsulation dot1q 21 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 Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz: R1(config)#interface gigabitEthernet 0/1.23 R1(config-subif)#description accounting LAN de Ingenieria R1(config-subif)#encapsulation dot1q 23 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 Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz: R1(config)#interface gigabitEthernet 0/1.99 R1(config-subif)#description accounting LAN de Administracion R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	R1(config)#interface gigabitEthernet 0/1 R1(config-if)#no shutdown

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

Figura 50. Configuración VLAN IPv4 en R1.

The screenshot displays the configuration of R1 in Packet Tracer. The network diagram on the left shows R1 connected to S0 (72.16.1.0/30), TR, and S1 (60/24TT). S1 is connected to PC0 (VLAN 21). The CLI on the right shows the configuration of interfaces gigabitEthernet0/1.21, 0/1.23, and 0/1.99 with descriptions and IP addresses.

```

R1>en
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gigabitEthernet0/1.21
R1(config-subif)#description accounting LAN de Contabilidad
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet0/1.23
R1(config-subif)#description accounting LAN de Ingenieria
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet0/1.99
R1(config-subif)#description accounting LAN de Administracion
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface gigabitEthernet0/1
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.23, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.99, changed state to up

R1(config-if)#
  
```

Fuente: Autoría propia en Packet Tracer

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	<pre>S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1: !!!!!! Success rate is 100 percent (5/5), round trip time = 0.000 msec</pre>
S3	R1, dirección VLAN 99	192.168.99.1	<pre>S3#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1: !!!!!! Success rate is 100 percent (5/5), round trip time = 0.000 msec</pre>
S1	R1, dirección VLAN 21	192.168.21.1	<pre>S1#ping 192.168.21.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1: !!!!!! Success rate is 100 percent (5/5), round trip time = 0.000 msec</pre>
S3	R1, dirección VLAN 23	192.168.23.1	<pre>S3#ping 192.168.23.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.1: !!!!!! Success rate is 100 percent (5/5), round trip time = 0.000 msec</pre>

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 específico.

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. R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	R1(config)#router ospf 10 R1(config-router)#passive-interface

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

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

Figura 51. Configuración del Protocolo dinámico OSPF R1.

The screenshot displays the configuration of router R1 in Packet Tracer. On the left, a network diagram shows router R1 (IP 1941) connected to a switch (IP 1960) via a serial link (S1). The switch has a VLAN configuration. On the right, the CLI window shows the following configuration:

```

R1
  Physical Config CLI Attributes
  IOS Command Line Interface
  R1(config)#router ospf 1
  R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
  R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
  R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
  R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
  R1(config-router)#exit
  R1(config)#router ospf 10
  R1(config-router)#passive-interface gi0/1.21
  R1(config-router)#exit
  R1(config)#router ospf 10
  R1(config-router)#passive-interface gi0/1.23
  R1(config-router)#exit
  R1(config)#router ospf 10
  R1(config-router)#passive-interface gi0/1.99
  R1(config-router)#exit
  R1(config)#router rip
  R1(config-router)#no auto-summary
  R1(config-router)#exit
  R1(config)#exit
  R1#
  %SYS-5-CONFIG_I: Configured from console by console

```

Fuente: Autoría propia en Packet Tracer

Paso 2: Configurar OSPF en el R2

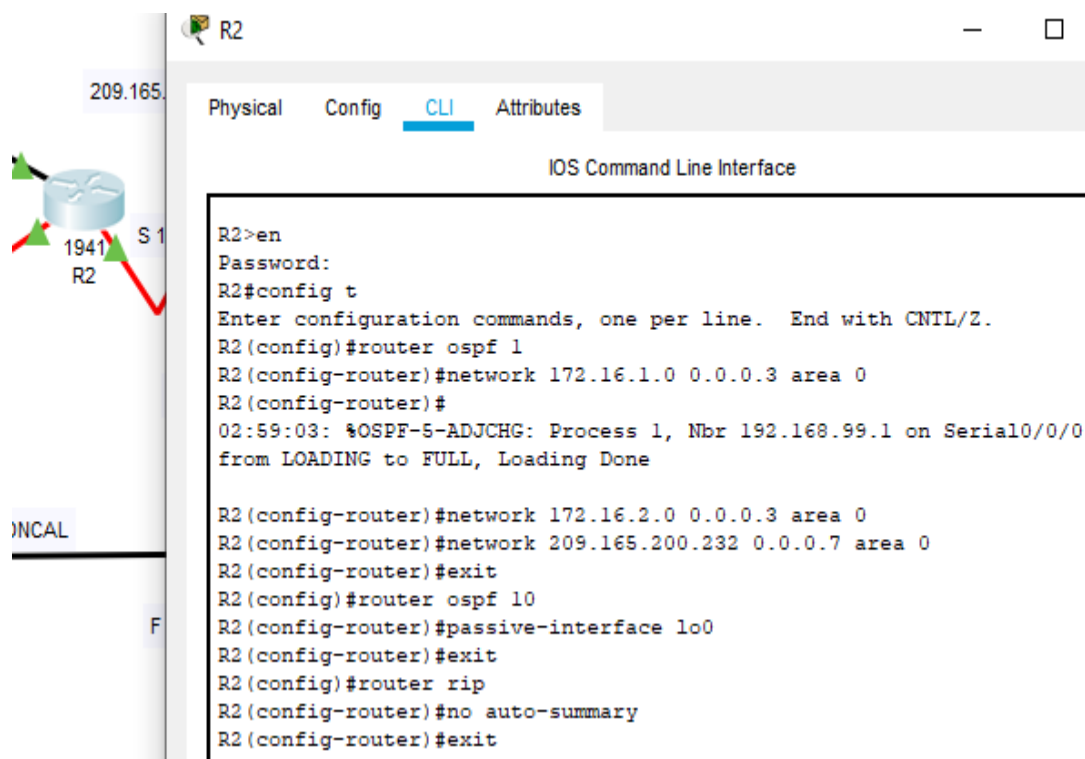
La configuración del R2 incluye las siguientes tareas:

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. 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 209.165.200.232 0.0.0.7 area 0
Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 10 R2(config-router)# passive-interface lo0
Desactive la sumarización automática.	R2(config)#router rip 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 R3(config-router)#network 192.168.4.0 0.0.0.255 area 0 R3(config-router)#network 192.168.5.0 0.0.0.255 area 0

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

Figura 53. Configuración del Protocolo dinámico OSPF R3.

The screenshot displays the configuration of router R3 in Packet Tracer. On the left, a network diagram shows a server (S1) with IP 10.10.10.10/32 connected to R3 (1941) via a switch (S1) at 172.16.2.0/30. R3 is also connected to a switch (S2) at 2960/24TT via interface F 0/3. The right pane shows the CLI configuration for R3:

```

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
03:15:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.10 on Serial0/0/1
from LOADING to FULL, Loading Done

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)#router ospf 10
R3(config-router)#exit
R3(config)#router ospf 10
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#router rip
R3(config-router)#no auto-summary
R3(config-router)#exit
R3(config)#exit

```

Fuente: Autoría propia en Packet Tracer

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

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Password:
R2#Show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.10.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    209.165.200.232 0.0.0.7 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10      110          00:18:20
    192.168.6.1      110          00:16:46
    192.168.99.1     110          00:22:50
  Distance: (default is 110)

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.165.200.233
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: (default is 110)

R2#
R2#Show ip route ospf
  192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/65] via 172.16.2.1, 00:18:48, Serial10/0/1
  192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/65] via 172.16.2.1, 00:17:53, Serial10/0/1
  192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/65] via 172.16.2.1, 00:17:39, Serial10/0/1
O       192.168.21.0 [110/65] via 172.16.1.1, 00:23:46, Serial10/0/0
O       192.168.23.0 [110/65] via 172.16.1.1, 00:23:46, Serial10/0/0
O       192.168.99.0 [110/65] via 172.16.1.1, 00:23:46, Serial10/0/0

R2#Show ip ospf database
      OSPF Router with ID (10.10.10.10) (Process ID 1)

          Router Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum Link
count
192.168.99.1   192.168.99.1  1438         0x80000005    0x00b2d3 5
10.10.10.10    10.10.10.10  1168         0x80000005    0x001f4c 5
192.168.6.1    192.168.6.1  1074         0x80000005    0x00c5f6 5
  
```

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 Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
Crear un pool de DHCP para la VLAN 23	Nombre: ENGR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

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

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

Figura 55. Configuración de R1 como servidor de DHCP.

The screenshot displays the configuration of router R1 in Packet Tracer. On the left, a network diagram shows a switch (S0) connected to router R1. The switch has a 24TT port connected to R1's Fa0/3. The network 172.16.1.0/30 is associated with S0. On the right, the CLI shows the following configuration:

```

R1>en
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.30
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.30
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

```

Fuente: Autoría propia en Packet Tracer

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

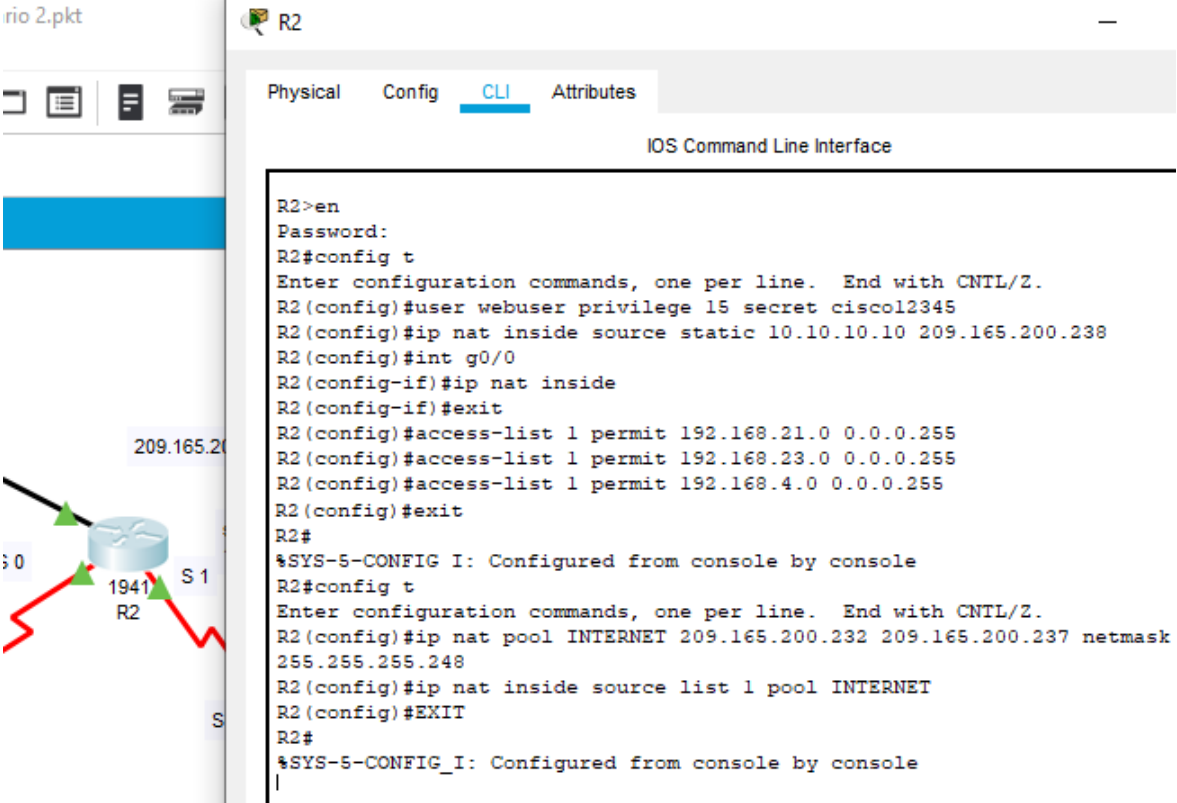
La configuración del R2 incluye las siguientes tareas:

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 Contraseña: cisco12345 Nivel de privilegio: 15 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 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 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
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 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



The image shows a Packet Tracer interface with a router R2 and its CLI configuration window. The router is connected to a switch S1 and has interfaces g0/0 and S1. The CLI window shows the following configuration steps:

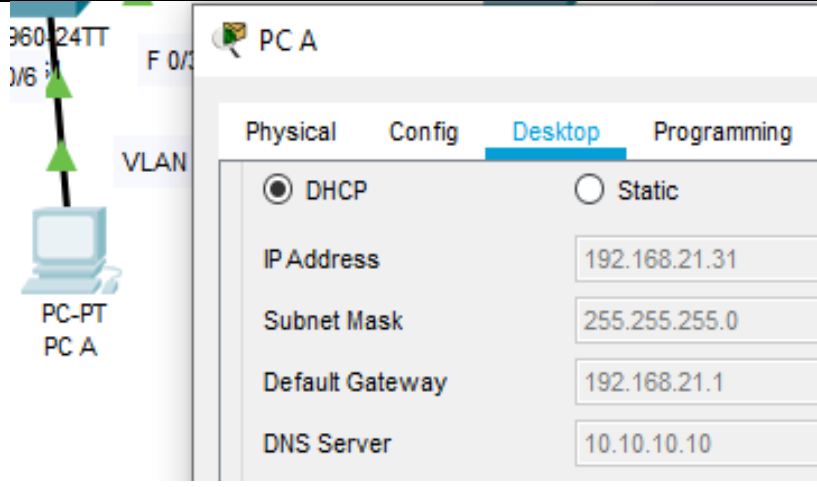
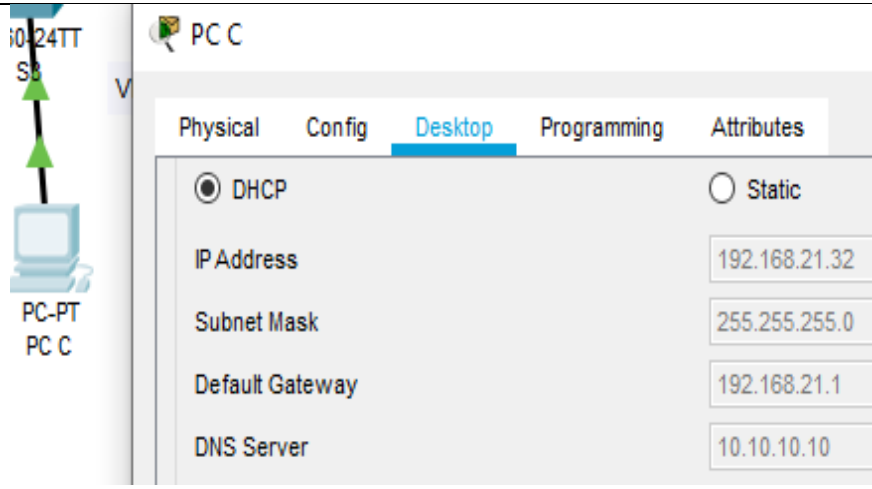
```
R2>en
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.238
R2(config)#int g0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.0.255
R2(config)#exit
R2#
%SYS-5-CONFIG I: Configured from console by console
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat pool INTERNET 209.165.200.232 209.165.200.237 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#EXIT
R2#
%SYS-5-CONFIG_I: Configured from console by console
|
```

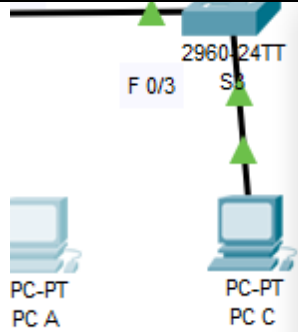
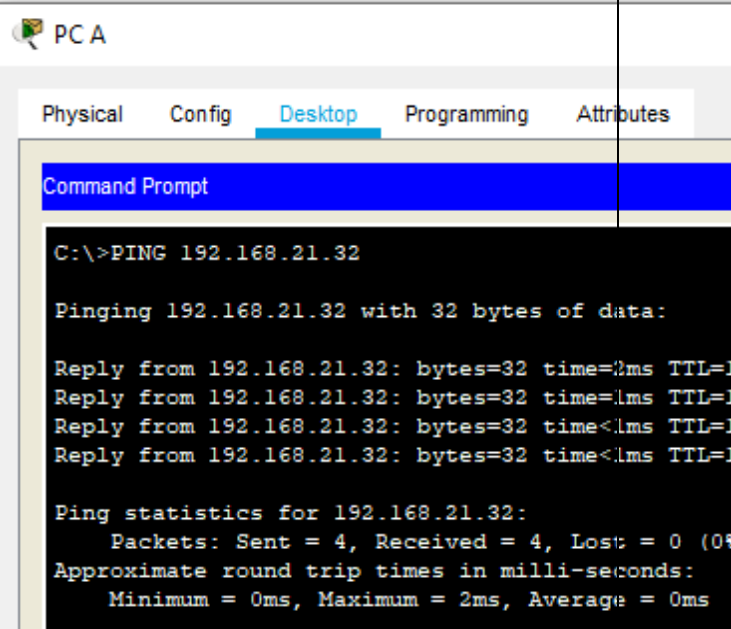
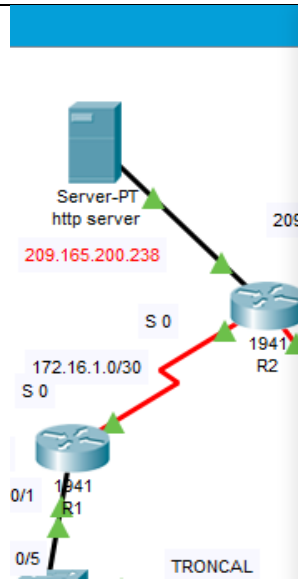
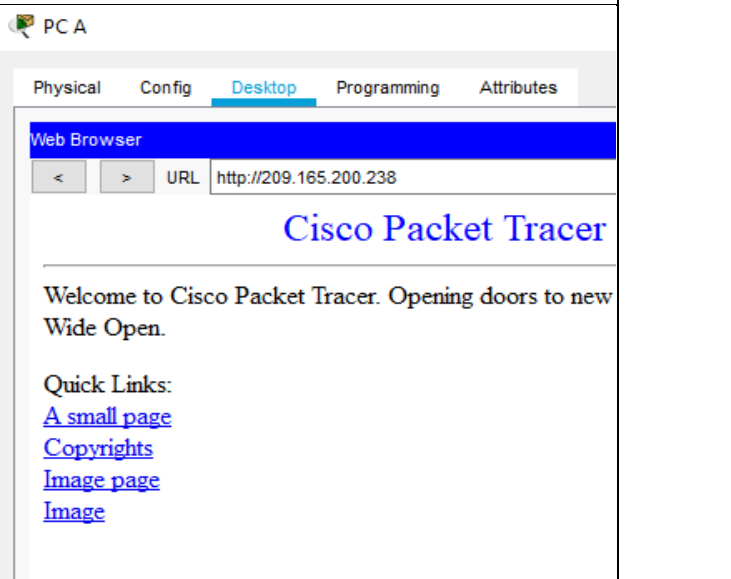
Fuente: Autoría propia en Packet Tracer

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	
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	 <p>The screenshot shows the configuration for PC A. The 'Desktop' tab is active, and the 'DHCP' radio button is selected. The IP Address is set to 192.168.21.31, the Subnet Mask is 255.255.255.0, the Default Gateway is 192.168.21.1, and the DNS Server is 10.10.10.10.</p>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <p>The screenshot shows the configuration for PC C. The 'Desktop' tab is active, and the 'DHCP' radio button is selected. The IP Address is set to 192.168.21.32, the Subnet Mask is 255.255.255.0, the Default Gateway is 192.168.21.1, and the DNS Server is 10.10.10.10.</p>

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

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

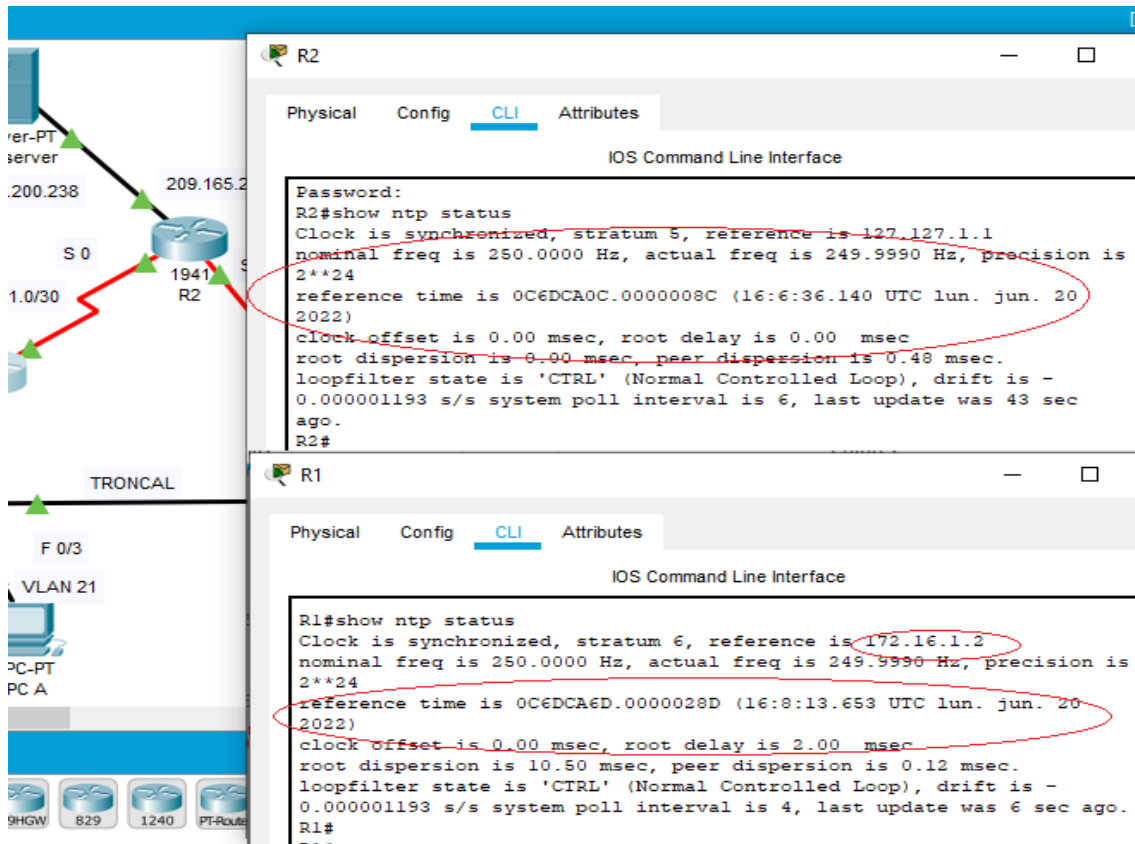
Nota: Con la configuración de los protocolos DHCP y NAT, en los dispositivos R1 Y R2 se logró generar la conexión de los host con enrutamiento dinámico y configuración de las Vlan 21 y 23, sobre R1 dejando este como servidor DHCP y en R2, se configura el protocolo NAT, con el fin de crear rutas estáticas 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)

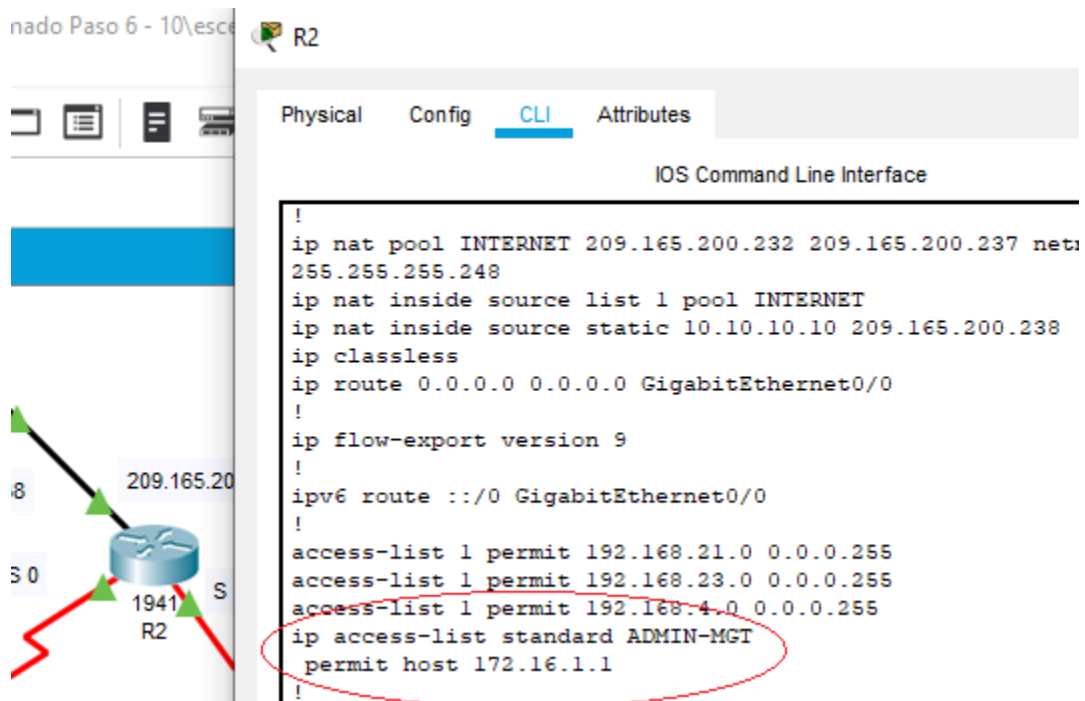
Paso 1: Restringir el acceso a las líneas VTY en el R2

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 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 R2(config-std-nacl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config-stdnacl)#permit host 172.16.1.1 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".

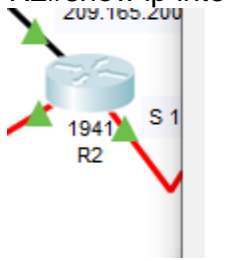
Figura 58. Listas de control de acceso (ACL), en R2.



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	<p>R2#show ip access-lists</p> <pre> R2>en Password: R2#show ip access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.0.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 </pre>

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

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 protocolos 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!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

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>