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

DIANA ANDREA CASTILLO SÁENZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
VÉLEZ, SANTANDER
2021

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

DIANA ANDREA CASTILLO SÁENZ

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

TUTOR:
INGENIERO RAUL BAREÑO GUTIERREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
VÉLEZ, SANTANDER
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Vélez (21, noviembre, 2021)

AGRADECIMIENTOS

Debo agradecer de manera especial y sincera al ingeniero Raul Bareño Gutiérrez por su apoyo, orientación y constante ánimo en el desarrollo de mi trabajo, además de ser una guía en mi proceso de aprendizaje. Le agradezco también el haberme facilitado los medios para llevar a cabo el desarrollo de las actividades propuestas en el curso. Muchas Gracias ingeniero por su apoyo y confianza, eres un excelente profesional y ser humano.

Quiero expresar también mi agradecimiento a la ingeniera Nancy Amparo Guaca por su orientación constante en el desarrollo de las actividades, por preocuparse por el aprendizaje de cada uno de nosotros, fue de gran ayuda para el desarrollo de las actividades propuestas en el diplomado. Muchas gracias ingeniera.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág.

GLOSARIO

ACL: Una lista de control de accesos es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos

CCNA: Cisco Certified Network Associated.

DHCP: El protocolo DHCP es un protocolo de red que utiliza una arquitectura cliente/servidor; este protocolo se encarga de asignar de manera dinámica y automática una dirección IP, bien sea privada o pública.

DIRECCIÓN IP: Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP.

DIRECCIONAMIENTO IP: Son los equipos y redes que funcionan mediante el protocolo TCP/IP Protocolo de control de transmisión/ Protocolo de internet.

NAT: Significa Network Address Translation o Traducción de direcciones de red. Se trata de un sistema que se utiliza en las redes bajo el protocolo IP y que permite el intercambio de paquetes entre dos redes que tienen asignadas mutuamente direcciones IP incompatibles.

OSPF: Es un protocolo de enrutamiento dinámico interior IGP, usa un algoritmo de tipo estado de enlace.

DNS: (Domain Name System). Es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados.

ROUTER: Es un dispositivo que recibe y envía datos en redes informáticas; un router permite la interconexión de computadoras en red.

SSH: Es un protocolo de red y de administración remota, diseñado originalmente para reemplazar a Telnet y otros protocolos no seguros como RSH; la conexión SSH está cifrada de extremo a extremo además de necesitar una autenticación para poder conectar al servidor.

SUBRED: Es una pequeña red dentro de una más grande.

SWITCH: Es un dispositivo que se utiliza para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina.

RESUMEN

En esta evaluación de prueba de habilidades se realiza análisis de dos escenarios en los cuales se identifican las competencias y habilidades adquiridas en el trascurso del diplomado de profundización de cisco CCNA. El primer escenario consta de una red pequeña en la que se debe realizar la configuración de routers, switches y PCs; dicha configuración consta de configuración básica en los dispositivos, empleando comandos que ayudan a cifrar las contraseñas insertadas en los routers y switches con el fin de mejorar la seguridad de los mismos para que se puedan administrar de forma segura.

En el segundo escenario se realiza la configuración de una red pequeña con conectividad IPv4 e IPv6 en donde se efectúan configuraciones como el protocolo de routing dinámico OSPF, el protocolo DHCP la traducción de direcciones de red dinámicas y estáticas NAT, protocolo NTP, la seguridad entre swiches y el routing entre vlan; en cada configuración se realizan verificaciones de funcionamiento y análisis de los mismos.

PALABRAS CLAVE: Packet tracer, Subredes, Direccionamiento IP, Router, Switch, SSH, DHCP, NAT, OSPF, NTP, Seguridad.

ABSTRACT

In this skills test evaluation, an analysis of two scenarios is carried out in which the competencies and skills acquired in the course of the Cisco CCNA deepening diploma are identified. The first scenario consists of a small network in which the configuration of routers, switches and PCs must be carried out; This configuration consists of basic configuration in the devices, using commands that help to encrypt the passwords inserted in the routers and switches in order to improve their security so that they can be managed safely.

In the second scenario, the configuration of a small network with IPv4 and IPv6 connectivity is carried out, where configurations such as the dynamic routing protocol OSPF, the DHCP protocol, the translation of dynamic and static network addresses

NAT, NTP protocol, security between swiches and routing between vlan; operation checks and analyzes are carried out in each configuration.

KEYWORDS: Packet tracer, Subnet, IP addressing, Router, Switch, SSH, DHCP, NAT, OSPF, NTP, Security

INTRODUCCIÓN

El presente trabajo evidencia la solución de dos escenarios propuestos en donde se implementan todos los conocimientos y habilidades adquiridas a través del desarrollo del curso en CISCO CCNA, además del manejo y configuración del programa packet tracer.

En el primer escenario se realizan las configuraciones de interfaces y de seguridad a los routers y switches implementados para su correcto funcionamiento, adicionalmente se realiza un análisis y cálculo de direccionamiento IP con dos subredes para su comunicación.

En el segundo escenario se realizan configuraciones de direccionamiento IPv4 e IPv6 en los routers y switches, a su vez routing entre Vlan, protocolo OSPF, protocolo dinámico DHCP, traducción de direcciones de red dinámicas y estáticas NAT, listas de control de acceso ACL y protocolo de tiempo de red NTP servidor/cliente, las cuales se implementan para el correcto funcionamiento del escenario.

La solución de los dos escenarios cuenta con la documentación completa de comandos y con la verificación y funcionamiento.

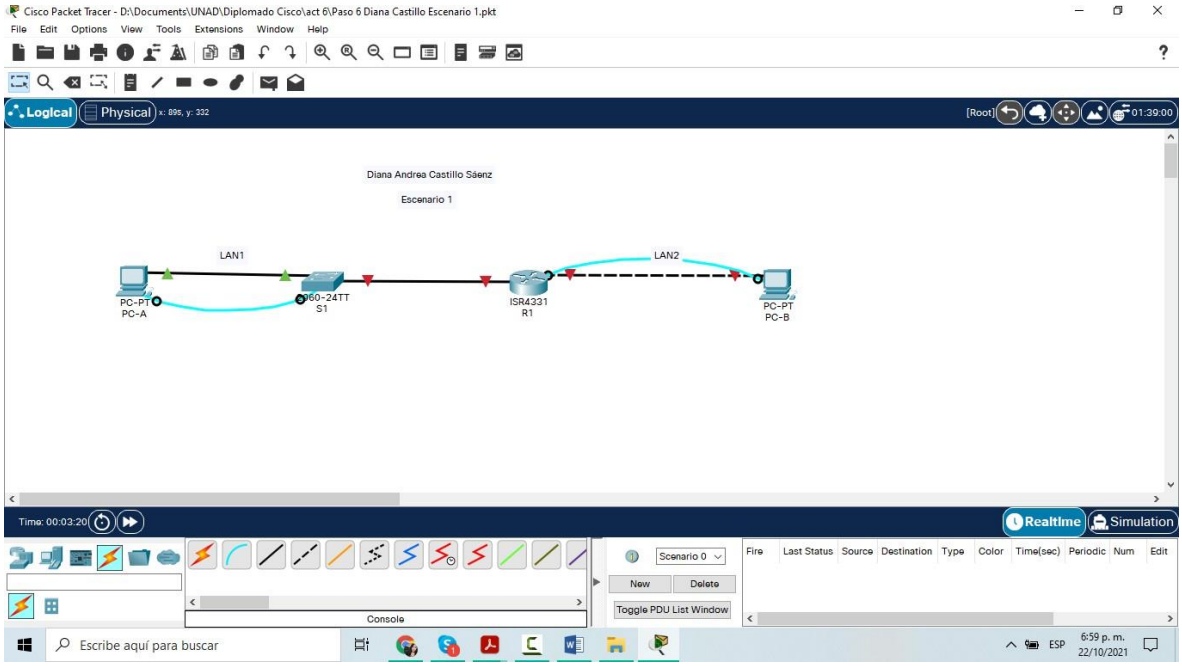
DESARROLLO

1. ESCENARIO 1

1.1. Construya la Red

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

Figura 1. Topología escenario 1.



Fuente: Autor

1.2. Desarrolle el esquema de direccionamiento IP

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

Tabla 1. Tabla de direccionamiento

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

Fuente: Autor

Para desarrollar este esquema propuesto se tiene en cuenta que los dos últimos dígitos de la cédula son 30, por lo consiguiente quedaría la dirección de red de la siguiente manera:

192 . 168 . 30 . 0 /24

Para la LAN 1 se tiene en cuenta 100 host por lo tanto para satisfacer los 100 host se tiene en cuenta lo siguiente:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Por lo anterior se tiene en cuenta $2^7 - 2 = 126$ host

0	0 0 0 0 0 0 0
Subred	7 host

Debido a esto la nueva máscara de subred es la siguiente:

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 0 0 0 0 0 0 0
255 . 255 . 255 . 128

Por lo tanto la dirección de red es la siguiente:

192 . 168 . 30 . 0 /25

Entonces para la LAN 1 de 100 host la dirección es 192.168.30.0, y para la LAN 2 de 50 host la dirección de red es 192.168.30.128, puesto que se toma 256-128=128 la cual es el índice de incremento para la siguiente subred.

Para la LAN 2 de 50 host se tiene en cuenta la dirección de red 192.168.30.128, como se debe satisfacer los 50 host se tiene lo siguiente:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Por lo anterior se tiene en cuenta $2^6 - 2 = 126$ host

0	0	0	0	0	0	0	0
Subred		6 host					

Debido a esto la nueva máscara de subred es la siguiente:

1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 0 0 0 0 0 0
255 . 255 . 255 . 192

Por lo tanto la dirección de red es la siguiente:

192 . 168 . 30 . 128 /25

Para el cálculo de las direcciones IP disponibles se debe tener en cuenta lo siguiente:

Tabla 2. Cálculo direcciones IP disponibles.

Host	Dirección de red	Mascara	Primer IP disponible	Último IP disponible	Broadcast	
100	192.168.30.0	255.255.255.128	192.168.30.1	192.168.30.126	192.168.30.127	128
50	192.168.30.128	255.255.255.192	192.168.30.129	192.168.30.190	192.168.20.191	64
	192.168.30.192					

Fuente: Autor

De acuerdo a la tabla anterior se puede llenar la tabla de direccionamiento propuesta al inicio quedando de la siguiente forma:

Tabla 3. Tabla de direccionamiento resuelta.

ITEM	REQUERIMIENTO
Dirección de Red	192.168.30.0
Requerimiento de host Subred LAN1	100
Requerimiento de host Subred LAN2	50
R1 G0/0/1	192.168.30.1
R1 G0/0/0	192.168.30.129
S1 SVI	192.168.30.2
PC-A	192.168.30.126
PC-B	192.168.30.190

Fuente: Autor

1.3. Configure aspectos básicos

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

Se tiene en cuenta que en la topología se debe anexar el cable de consola para proceder a configurar el router y el switch respectivamente.

1.3.1. Configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

- Desactivar la búsqueda DNS
- Nombre del router: R1
- Nombre de dominio: 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
- Configurar VTY solo aceptando SSH
- Cifrar las contraseñas de texto no cifrado
- Configure un MOTD Banner
- Configurar interfaz G0/0/0:
  Establezca la descripción
  Establezca la dirección IPv4
  Activar la interfaz
- Configurar interfaz g0/0/1:
  Establezca la descripción
  Establezca la dirección IPv4
  Activar la interfaz
- Generar una clave de cifrado RSA: módulo de 1024 bits.

A continuación se anexa el código de configuración de R1:

```
Router>enable                                   Se ingresa al modo EXEC privilegiado
Router#configure terminal                       Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup              Se desactiva la búsqueda por DNS
Router(config)#hostname R1                      Se asigna nombre al Router
R1(config)#ip domain-name ccna-lab.com          Se ingresa nombre de dominio
R1(config)#enable secret ciscoenpass            Se pone contraseña de acceso al modo privilegiado
```

R1(config)#line console 0 Se ingresa al modo de configuración de línea de la consola
R1(config-line)#password ciscoconpass Se ingresa la contraseña para la línea de consola
R1(config-line)#login Se utiliza para que el router requiera autenticación al iniciar sesión.
R1(config-line)#exit Se sale de la configuración de línea de la consola
R1(config)#security passwords min-length 10 Se establece longitud mínima para las contraseñas en este caso de 10
R1(config)#username admin password admin1pass Se crea un usuario administrativo y contraseña en la base de datos local
R1(config)#line vty 0 4 Se ingresa a la configuración de la línea VTY del router
R1(config-line)#password dianacisco Se pone contraseña a esa línea VTY
R1(config-line)#login local Se habilita la base de datos local para la autenticación
R1(config-line)#transport input SSH Se configura VTY para que solo acepte SSH
R1(config-line)#exit Se sale de la configuración de línea VTY
R1(config)#service password-encryption Se cifran las contraseñas de texto no cifrado
R1(config)#banner motd #Acceso no autorizado para personal ajeno a la UNAD.# Se ingresa un mensaje de aviso
R1(config)#int g0/0/0 Se ingresa a la interfaz gigabitEthernet 0/0/0
R1(config-if)#description Esta es la interfaz de la LAN 2 Se realiza descripción de la interfaz
R1(config-if)#ip add 192.168.30.129 255.255.255.192 Se ingresa la dirección IP y la máscara de red para la interfaz
R1(config-if)#no shutdown Se activa la interfaz
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
R1(config-if)#int g0/0/1 Se ingresa a la interfaz gigabitEthernet 0/0/1
R1(config-if)#description Esta es la interfaz de la LAN 1 Se realiza descripción de la interfaz
R1(config-if)#ip add 192.168.30.1 255.255.255.128 Se ingresa la dirección IP y la máscara de red para la interfaz
R1(config-if)#no shutdown Se activa la interfaz

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/1, changed state to up
R1(config-if)#ip domain name ccna-lab.com
R1(config)#crypto key generate rsa    Se genera clave de cifrado RSA
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than 512
may take a few minutes.
How many bits in the modulus [512]: 1024    Se ingresa el modulo de 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#exit                          Se sale del modo de configuración
*Mar 1 0:9:36.705: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#wr                                    Se guarda la configuración
Building configuration...
[OK]
```

Las tareas de configuración de S1 incluyen lo siguiente:

- Desactivar la búsqueda DNS
- Nombre del router: S1
- Nombre de dominio: 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
- Configurar VTY solo aceptando SSH
- Cifrar las contraseñas de texto no cifrado
- Configure 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: Configure la puerta de enlace predeterminada conforme a la tabla de direccionamiento.

A continuación se anexa el código de configuración de S1:

```
Switch>enable                                   Se ingresa al modo EXEC privilegiado
Switch#configure terminal                       Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup              Se desactiva la búsqueda por DNS
Switch(config)#hostname S1                      Se asigna nombre al Switch
S1(config)#ip domain-name ccna-lab.com          Se ingresa nombre de dominio
S1(config)#enable secret ciscoenpass            Se pone contraseña de acceso al modo privilegiado
S1(config)#line console 0                       Se ingresa al modo de configuración de línea de la consola
S1(config-line)#password ciscoconpass           Se ingresa la contraseña para la línea de  consola
S1(config-line)#login                           Se utiliza para que el switch requiera autenticación al iniciar sesión.
S1(config-line)#exit                            Se sale de la configuración de línea de la consola
S1(config)#username admin password admin1pass   Se crea un usuario administrativo y contraseña en la base de datos local
S1(config)#line vty 0 15                        Se ingresa a la configuración de la línea VTY del switch
S1(config-line)#password dianacisco             Se pone contraseña a esa línea VTY
S1(config-line)#login local                     Se habilita la base de datos local para la autenticación
S1(config-line)#transport input SSH             Se configura VTY para que solo acepte SSH
S1(config-line)#exit                            Se sale de la configuración de línea VTY
S1(config)#service password-encryption          Se cifran las contraseñas de texto no cifrado
S1(config)#banner motd #Acceso no autorizado para personal ajeno a la UNAD.#
                                                Se ingresa un mensaje de aviso
S1(config)#ip domain name ccna-lab.com
S1(config)#crypto key generate rsa              Se genera clave de cifrado 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]
S1(config)#int vlan 1                    Se ingresa a la interfaz vlan 1
*Mar 1 0:3:26.164: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-if)#ip add 192.168.30.2 255.255.255.128      Se ingresa la
dirección IP y la máscara de red para la interfaz
S1(config-if)#no shutdown                Se activa la interfaz
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up
S1(config-if)#ip default-gateway 192.168.30.1          Se configura la
puerta de enlace predeterminado
S1(config)#exit                          Se sale del modo de configuración
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#wr                                    Se guarda la configuración
Building configuration...
[OK]
```

1.3.2. Configurar los equipos

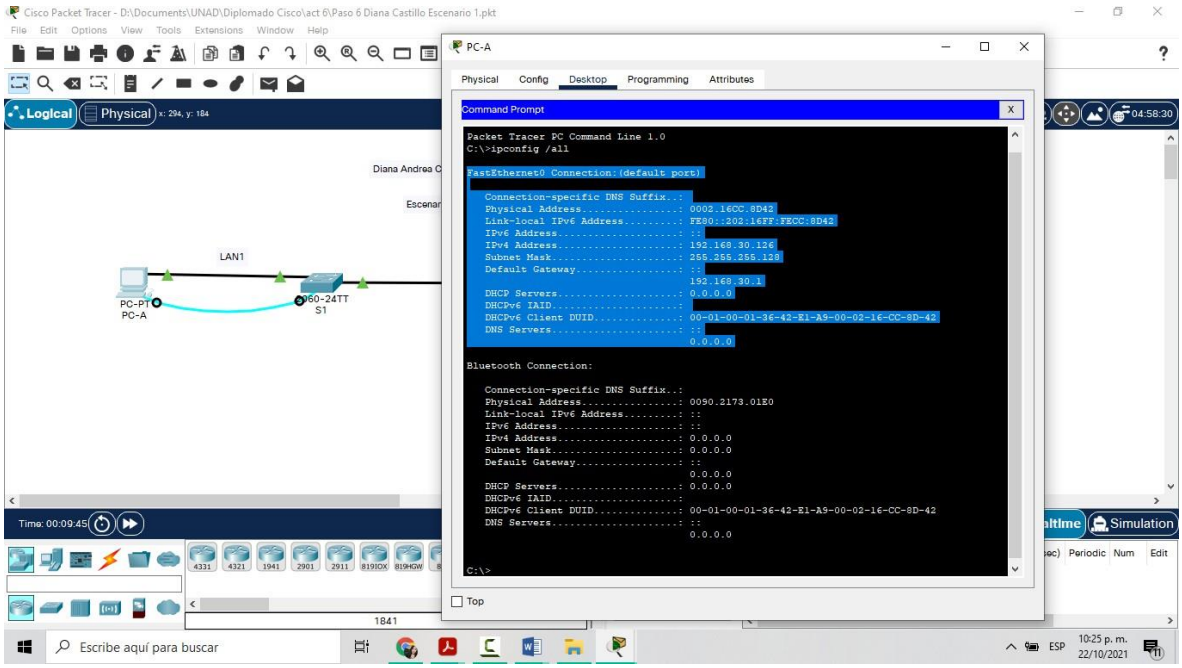
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando ipconfig /all.

Tabla 4. Configuración PC-A.

PC-A NETWORK CONFIGURATION	
Descripción	Configuración del PC-A conectado a S1
Dirección Física	0002.16CC.8D42
Dirección IP	192.168.30.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.30.1

Fuente: Autor

Figura 2. Comando ipconfig /all para PC-A.



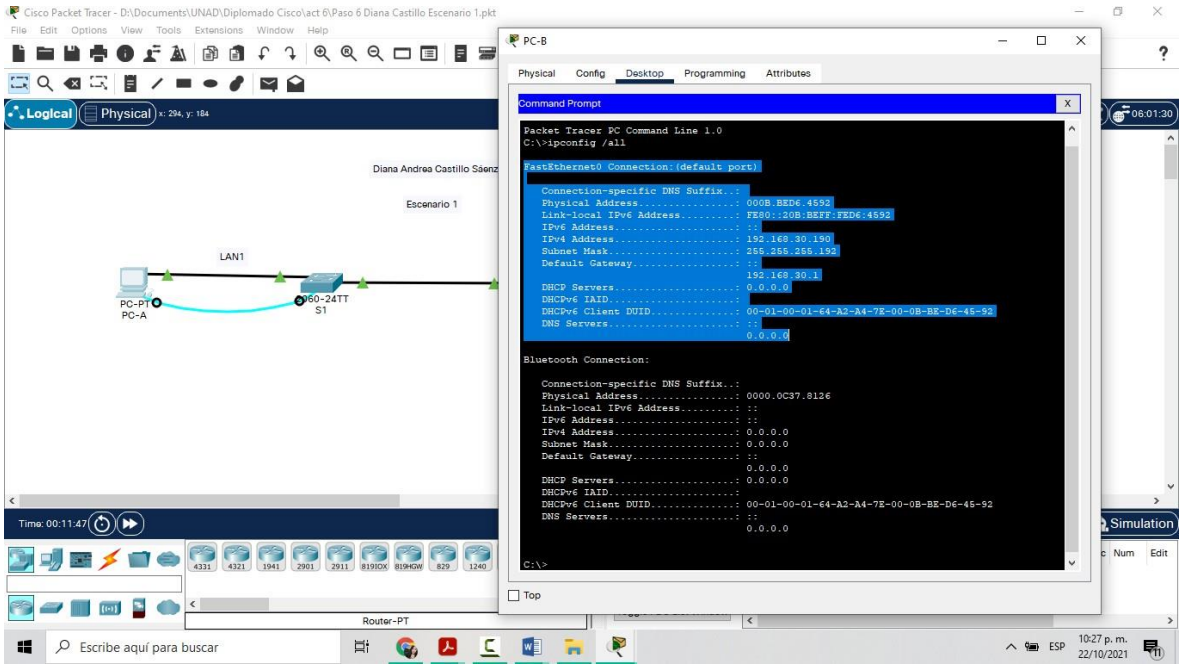
Fuente: Autor

Tabla 5. Configuración PC-B.

PC-B NETWORK CONFIGURATION	
Descripción	Configuración del PC-B conectado a R1
Dirección Física	000B.BED6.4592
Dirección IP	192.168.30.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.30.1

Fuente: Autor

Figura 3. Comando ipconfig /all PC-B



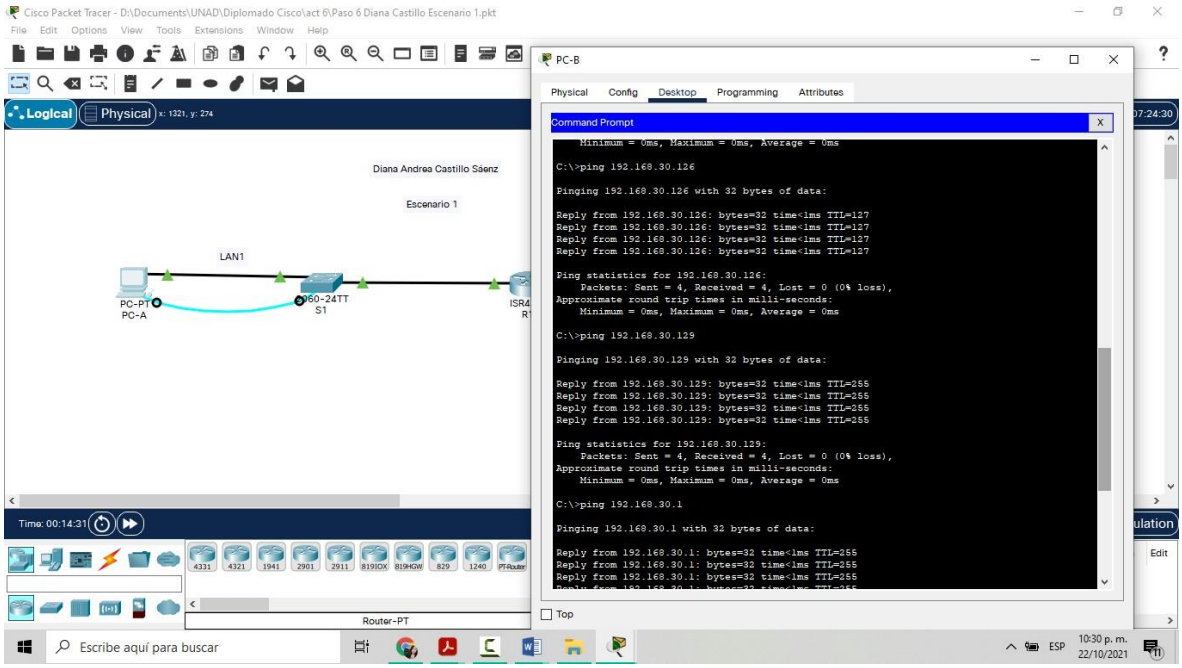
Fuente: Autor

1.4. Realización de Pruebas

1.4.1. Prueba de ping desde PC-B

Se realiza prueba con el comando ping en el command prompt de PC-B, se ingresan las direcciones IP de PC-A (192.168.30.126), la dirección IP de R1 (192.168.30.1, 192.168.30.129), y la dirección IP de S1 (192.168.30.2), todas con buenas respuestas de comunicación tal y como se muestra en la siguiente figura:

Figura 4. Comando ping desde PC-B

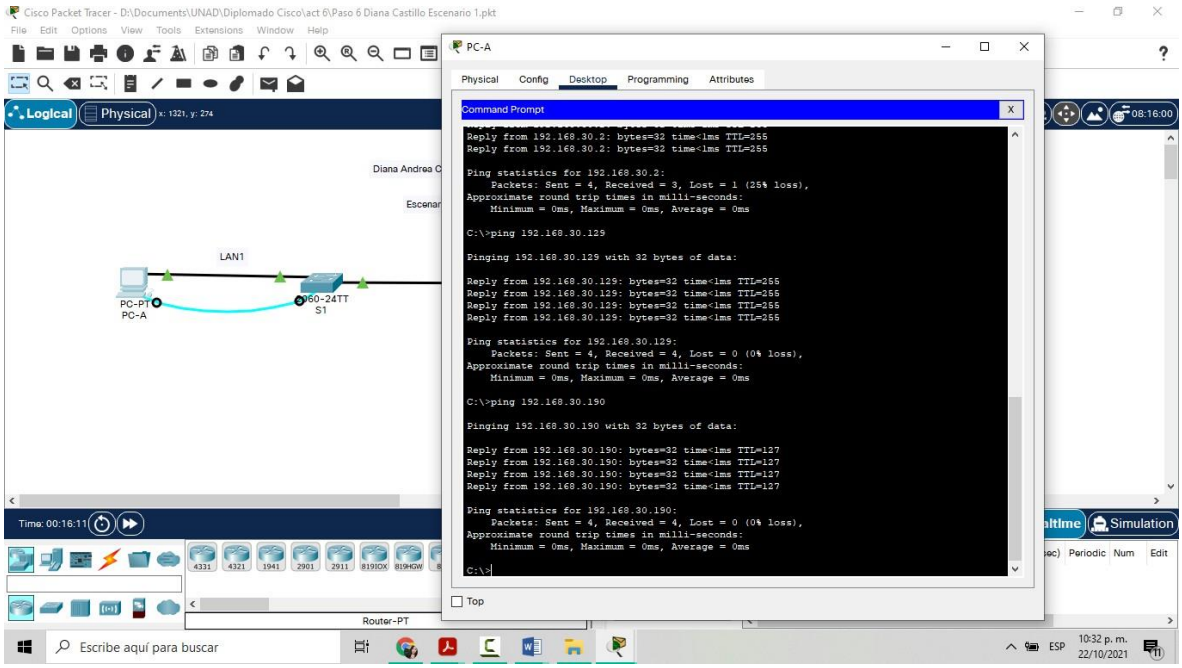


Fuente: Autor

1.4.2. Prueba de ping de PC-A

Se realiza prueba con el comando ping en el command prompt de PC-A, se ingresan las direcciones IP de PC-B (192.168.30.190), la dirección IP de R1 (192.168.30.1, 192.168.30.129), y la dirección IP de S1 (192.168.30.2), todas con buenas respuestas de comunicación tal y como se muestra en la siguiente figura:

Figura 5. Comando ping desde PC-A



Fuente: Autor

1.4.3. Prueba de configuración de S1

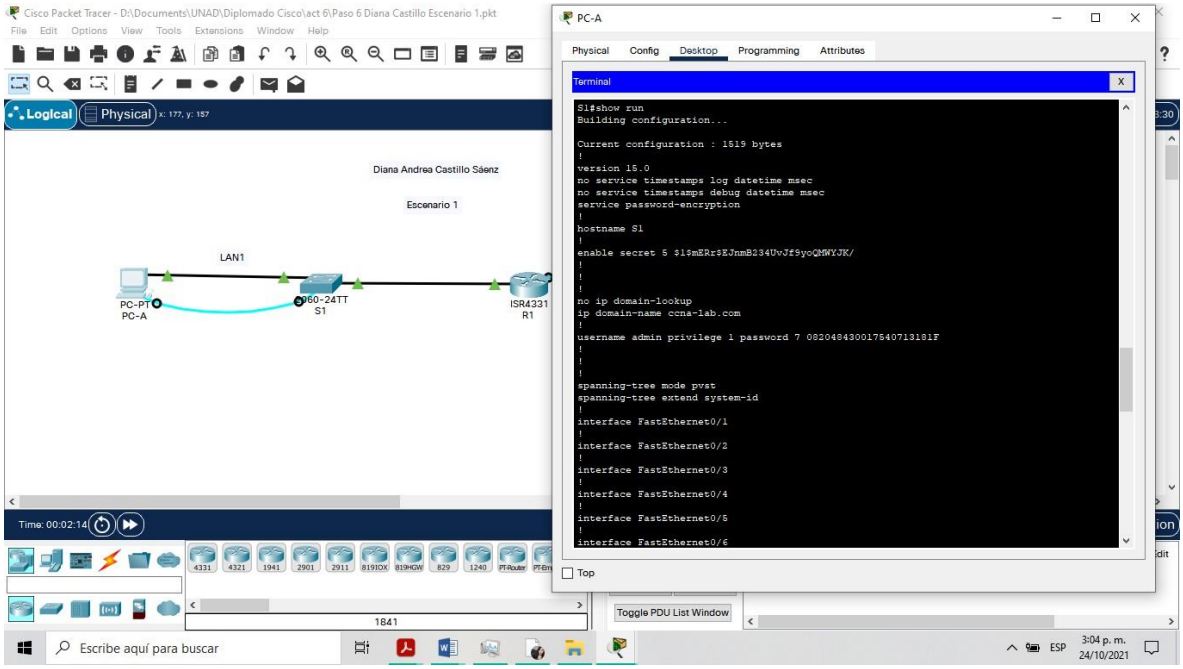
Para realizar esta prueba se utiliza el comando show run en el switch S1 con el fin de observar si la configuración realizada fue guardada correctamente, tal y como se muestra en la figura y en el código arrojado al ingresar el comando.

```
S1#show run
Building configuration...

Current configuration : 1519 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$EJnmB234UvJf9yoQMWYJK/
!
```

```
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
username admin privilege 1 password 7 082048430017540713181F
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/3
interface FastEthernet0/4
interface FastEthernet0/5
interface FastEthernet0/6
interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 ip address 192.168.30.2 255.255.255.128
```

```
!
ip default-gateway 192.168.30.1
!
banner motd ^CAcceso no autorizado para personal ajeno a la
UNAD.^C
!
line con 0
 password 7 0822455D0A1606181C1B0D1739
 login
!
line vty 0 4
 password 7 0825454F0718061E010803
 login local
transport input ssh
line vty 5 15
 password 7 0825454F0718061E010803
 login local
 transport input ssh
!
End
```

Figura 6. Comando Show run en S1.



Fuente: Autor

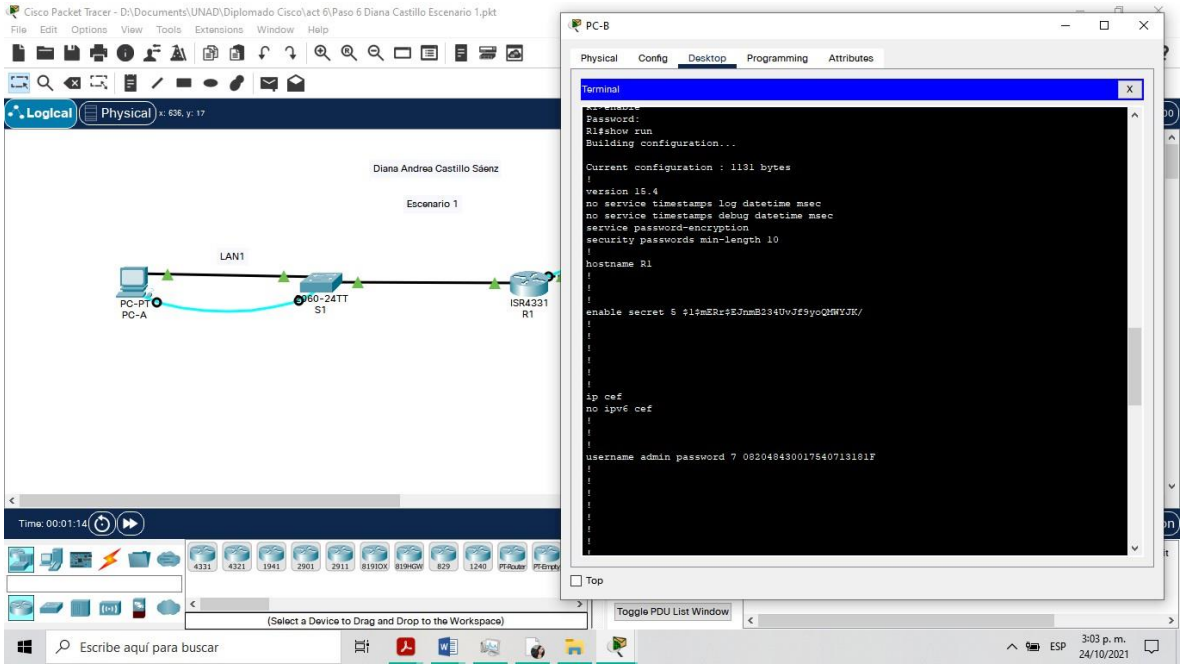
1.4.4. Prueba de configuración de R1

Para realizar esta prueba se utiliza el comando show run en el router R1 con el fin de observar si la configuración realizada fue guardada correctamente, tal y como se muestra en la figura y en el código arrojado al ingresar el comando.

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

Current configuration : 1131 bytes
!
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
enable secret 5 $1$mERr$EJnmB234UvJf9yoQMWYJK/
!
ip cef
no ipv6 cef
!
username admin password 7 082048430017540713181F
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
 description Esta es la interfaz de la LAN 2
 ip address 192.168.30.129 255.255.255.192
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 description Esta es la interfaz de la LAN 1
 ip address 192.168.30.1 255.255.255.128
 duplex auto
 speed auto
!
```

```
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip flow-export version 9
!
no cdp run
!
banner motd ^CAcceso no autorizado para personal ajeno a la UNAD.^C
!
line con 0
 password 7 0822455D0A1606181C1B0D1739
 login
!
line aux 0
!
line vty 0 4
 password 7 0825454F0718061E010803
 login local
 transport input ssh
!
!
!
End
```

Figura 7. Comando Show run en R1.



Fuente: Autor

1.4.5. Prueba de ingreso a S1 por command prompt

Se digita el siguiente comando en command prompt

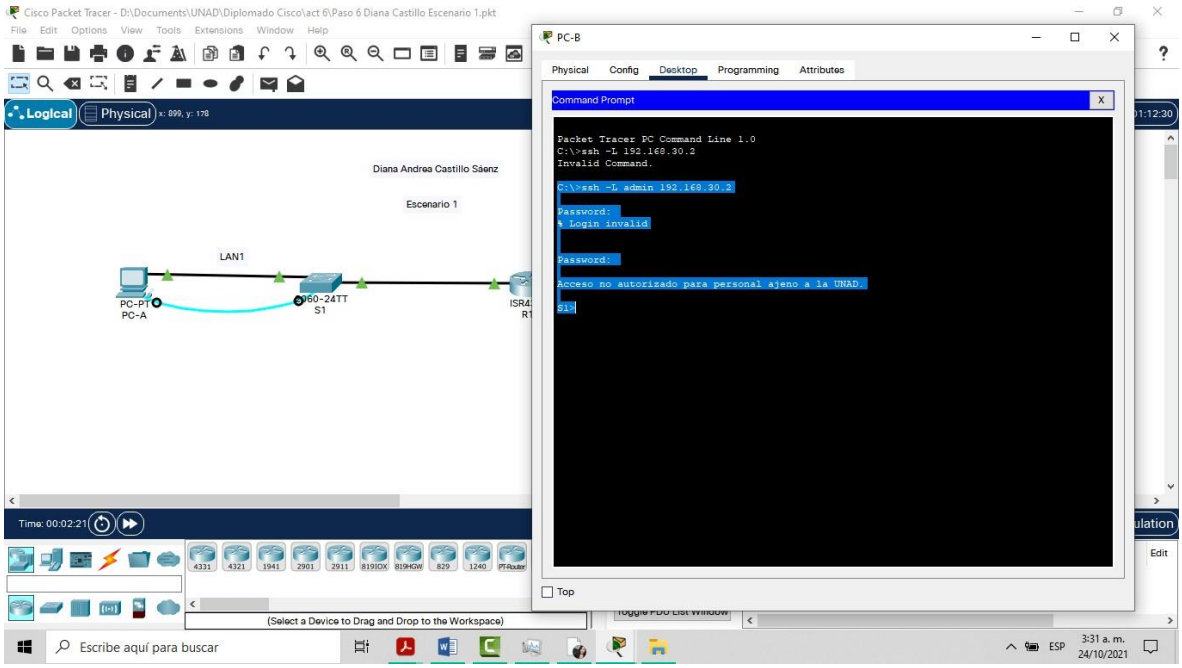
```
ssh -L admin 192.168.30.2
```

Y arroja lo siguiente:

```
Password:

Acceso no autorizado para personal ajeno a la UNAD.
S1>
```

Se adjunta pantallazo como evidencia de acceso al S1 por medio de command prompt.

Figura 8. Comando ssh -l admin.



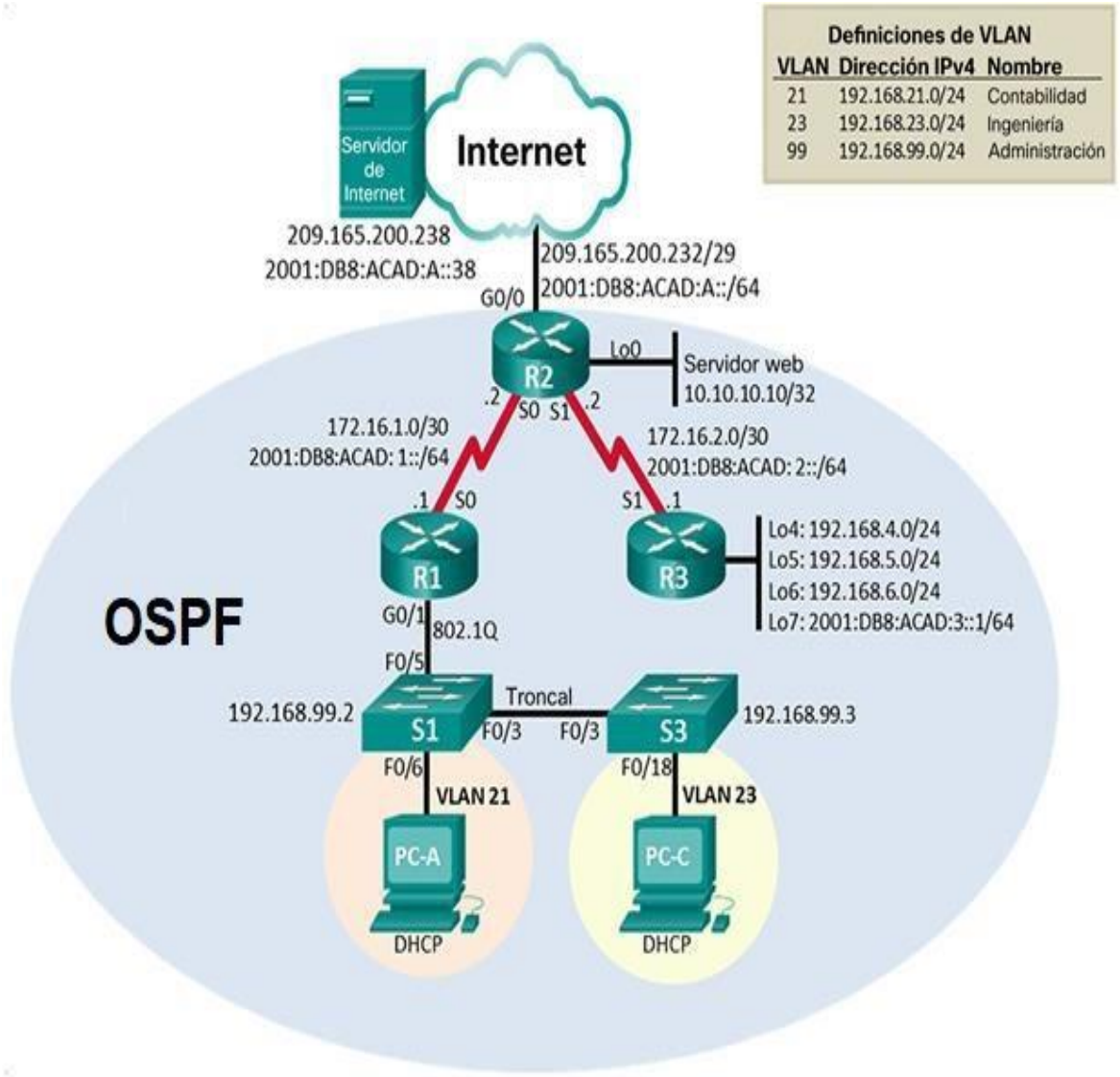
Fuente: Autor

Se evidencia que se debe introducir una contraseña para poder acceder al dispositivo en acceso remoto, ya por telnet no lo hace.

2. ESCENARIO 2

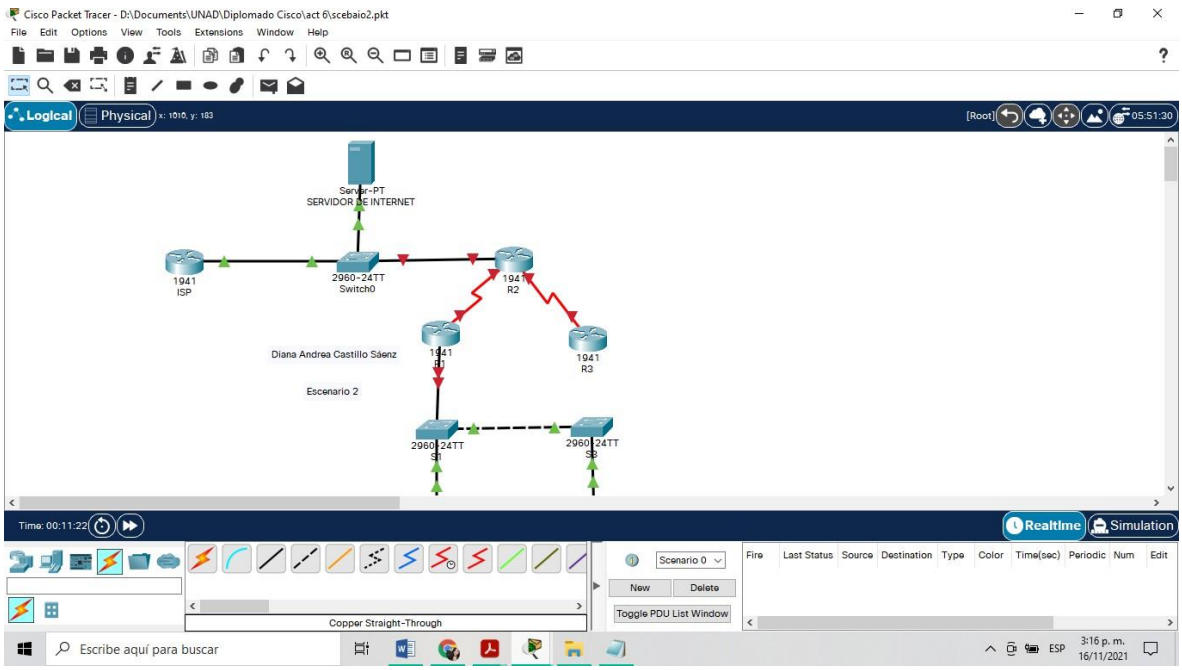
Se debe configurar una red pequeña para que admita conectividad IPv4 e IPv6, seguridad de switches, routing entre VLAN, el protocolo de routing dinámico OSPF, el protocolo de configuración de hosts dinámicos (DHCP), la traducción de direcciones de red dinámicas y estáticas (NAT), listas de control de acceso (ACL) y el protocolo de tiempo de red (NTP) servidor/cliente. Durante la evaluación, probará y registrará la red mediante los comandos comunes de CLI.

Figura 9. Escenario 2.



Fuente: Evaluación: Prueba de habilidades prácticas CCNA

Figura 10. Topología en packet tracer.



Fuente: Autor

2.1. Inicializar dispositivos

2.1.1. Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos. Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.
Tareas de inicializar y volver a cargar los routers y los switches

- Eliminar el archivo startup-config de todos los routers
- Volver a cargar todos los routers
- Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior
- Volver a cargar ambos switches
- Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

A continuación se anexa el código de inicialización y cargue del R1, R2 y R3:

```
Router>enable                                   Se ingresa al modo EXEC privilegiado
Router#erase startup-config                     Se realiza un borrado de la configuración inicial del router
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]                             Se confirma el borrado de la configuración inicial
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload                                   Se realiza el cargue del router
Proceed with reload? [confirm]                  Se confirma el cargue
```

A continuación se anexa el código de inicialización y cargue del S1 y S2:

```
Switch>enable                                   Se ingresa al modo EXEC privilegiado
Switch#show flash                               Se verifica las Vlan almacenadas
Directory of flash:/

    1  -rw-     4670455          <no date> 2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
Switch#erase startup-config                     Se realiza el borrado de la configuración inicial del switch
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]                             Se confirma el borrado
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload                                   Se realiza el cargue del switch
Proceed with reload? [confirm]                  Se confirma el cargue
```

2.2. Configurar los parámetros básicos de los dispositivos

2.2.1. 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):

- Dirección IPv4
- Máscara de subred para IPv4
- Gateway predeterminado: 209.165.200.233
- Dirección IPv6/subred
- Gateway predeterminado IPv6: 2001:DB8:ACAD:A::1/64

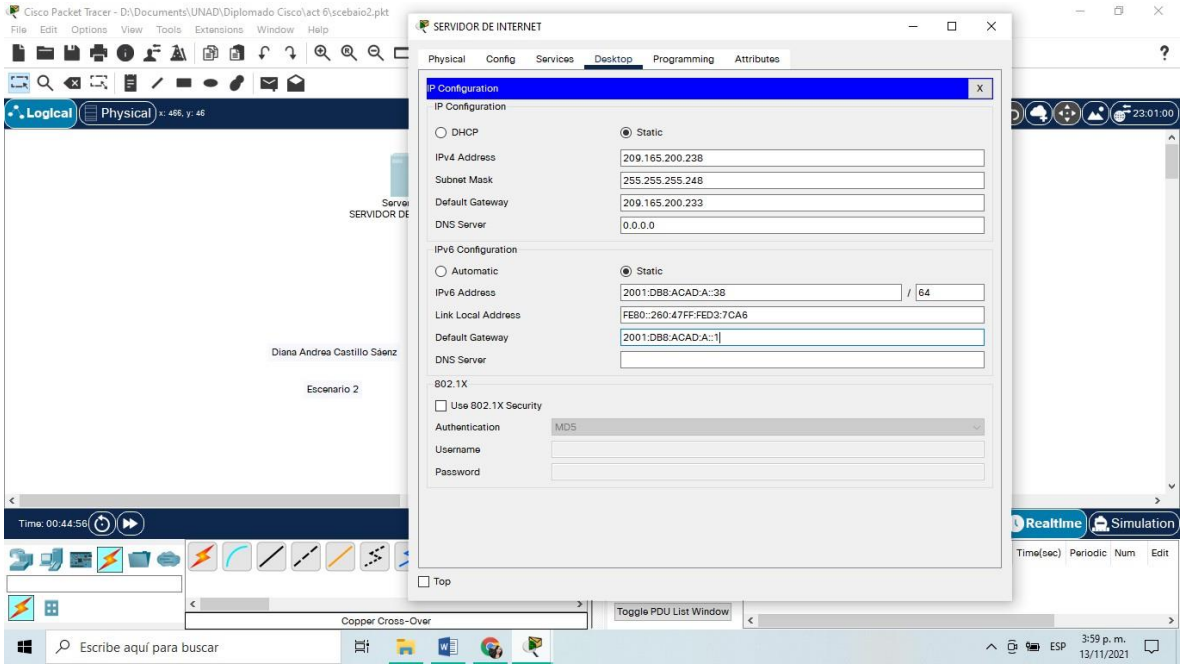
Tabla 6. Configuración servidor de internet.

Tareas	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Fuente: Autor

A continuación se anexa imagen de configuración de la computadora de internet:

Figura 11. Configuración Servidor de internet.



Fuente: Autor

A continuación se ejecuta el siguiente código en el router ISP, con el fin de configurar las interfaces:

```
Router>enable                                   Se ingresa al modo EXEC privilegiado
Router#configure terminal                       Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int g0/0                         Se ingresa a la interfaz g0/0 del router
Router(config-if)#ip address 209.165.200.234 255.255.255.248    Se configura la dirección IP y máscara de subred para esa interfaz
Router(config-if)#no shutdown                   Se activa la interfaz
```

2.2.2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

- Desactivar la búsqueda DNS

- Nombre del router: R1
- Contraseña de exec privilegiado cifrada: class
- Contraseña de acceso a la consola: cisco
- Contraseña de acceso Telnet: cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD: Se prohíbe el acceso no autorizado.
- Interfaz S0/0/0:
  Establezca la descripción
  Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones
  Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones
  Establecer la frecuencia de reloj en 128000
  Activar la interfaz
- Rutas predeterminadas:
  Configurar una ruta IPv4 predeterminada de S0/0/0
  Configurar una ruta IPv6 predeterminada de S0/0/0

A continuación se anexa el código de configuración de R1:

`Router>enable`	Se ingresa al modo EXEC privilegiado
`Router#configure terminal`	Se ingresa al modo de configuración
`Enter configuration commands, one per line. End with CNTL/Z.`	
`Router(config)#no ip domain-lookup`	Se desactiva la búsqueda DNS
`Router(config)#hostname R1`	Se le ingresa nombre al router R1
`R1(config)#enable secret class`	Se configura contraseña para EXEC privilegiado cifrada
`R1(config)#line console 0`	Se ingresa al modo de configuración de línea de la consola
`R1(config-line)#password cisco`	Se ingresa la contraseña para la línea de consola
`R1(config-line)#login`	Se utiliza para que el router requiera autenticación al iniciar sesión.
`R1(config-line)#line vty 0 4`	Se ingresa a la configuración de la línea VTY del router
`R1(config-line)#password cisco`	Se pone contraseña a esa línea VTY
`R1(config-line)#login`	Se utiliza para que el router requiera autenticación a la línea VTY.
`R1(config-line)#exit`	Se sale de la configuración de línea VTY

```
R1(config)#service password-encryption
```
Se cifran las contraseñas de texto no cifrado

```
R1(config)#banner motd #
```
Se ingresa un mensaje de aviso

```
Enter TEXT message. End with the character '#'.
Se prohibe el acceso no autorizado.#

R1(config)#ipv6 unicast-routing
R1(config)#int s0/0/0
```
Se ingresa a la interfaz s0/0/0

```
R1(config-if)#description interface hacia el router R2
```
Se realiza descripción de la interfaz

```
R1(config-if)#ip address 172.16.1.1 255.255.255.252
```
Se digita la dirección IP y máscara de subred a la interfaz

```
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
```
Se ingresa dirección IPV6 a la interfaz

```
R1(config-if)#clock rate 128000
```
Se establece la frecuencia de reloj en 128000

```
R1(config-if)#no shutdown
```
Se activa la interfaz

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```
Se configura la ruta predeterminada IPV4 para la interfaz s0/0/0

```
%Default route without gateway, if not a point-to-point interface,
may impact performance
R1(config)#ipv6 route ::/0 s0/0/0
```
Se configura la ruta predeterminada IPV6 para la interfaz s0/0/0

2.2.3. Configurar R2

La configuración del R2 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del router: R2
- Contraseña de exec privilegiado cifrada: class
- Contraseña de acceso a la consola: cisco
- Contraseña de acceso Telnet: cisco
- Cifrar las contraseñas de texto no cifrado
- Habilitar el servidor HTTP
- Mensaje MOTD: Se prohíbe el acceso no autorizado.
- Interfaz S0/0/0:
  Establezca la descripción
  Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.
  Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.

Activar la interfaz

- Interfaz S0/0/1:
  Establecer la descripción
  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
  Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
  Establecer la frecuencia de reloj en 128000.
  Activar la interfaz
- Interfaz G0/0 (simulación de Internet):
  Establecer la descripción.
  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
  Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.
  Activar la interfaz
- Interfaz loopback 0 (servidor web simulado):
  Establecer la descripción.
  Establezca la dirección IPv4.
- Ruta predeterminada:
  Configure una ruta IPv4 predeterminada de G0/0.
  Configure una ruta IPv6 predeterminada de G0/0.

A continuación se anexa el código de configuración de R2:

```
Router>enable                                   Se ingresa al modo EXEC privilegiado
Router#configure terminal                       Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup              Se desactiva la búsqueda DNS
Router(config)#hostname R2                      Se le ingresa nombre al router R2
R2(config)#enable secret class                  Se configura contraseña para EXEC privilegiado cifrada
R2(config)#line console 0                       Se ingresa al modo de configuración de línea de la consola
R2(config-line)#password cisco                  Se ingresa la contraseña para la línea de  consola
R2(config-line)#login                           Se utiliza para que el router requiera autenticación al iniciar sesión
R2(config-line)#line vty 0 4                    Se ingresa a la configuración de la línea VTY del router
R2(config-line)#password cisco                  Se pone contraseña a esa línea VTY
```

```
R2(config-line)#login                    Se utiliza para que el router requiera
autenticación a la línea VTY
R2(config-line)#exit                     Se sale de la configuración de línea
VTY
R2(config)#service password-encryptionSe cifran las contraseñas de texto
no cifrado
R2(config)#banner motd #                 Se ingresa un mensaje de aviso
Enter TEXT message. End with the character '#'.
Se prohbe el acceso no autorizado.#
R2(config)#ipv6 unicast-routing
R2(config)#int s0/0/0                    Se ingresa a la interfaz s0/0/0
R2(config-if)#description interface hacia el R1 Se realiza descripción
de la interfaz
R2(config-if)#ip address 172.16.1.2 255.255.255.252    Se digita la
dirección IP y máscara de subred a la interfaz
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64    Se establece la
frecuencia de reloj en 128000
R2(config-if)#no shutdown                Se activa la interfaz
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#int s0/0/1                 Se ingresa a la interfaz s0/0/1
R2(config-if)#description interface hacia el R3 Se realiza descripción
de la interfaz
R2(config-if)#ip address 172.16.2.1 255.255.255.252    Se digita la
dirección IP y máscara de subred a la interfaz
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 Se ingresa dirección
IPV6 a la interfaz
R2(config-if)#clock rate 128000          Se establece la frecuencia de reloj
en 128000
R2(config-if)#no shutdown                Se activa la interfaz
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config)#ipv6 unicast-routing
R2(config)#int g0/0                      Se ingresa a la interfaz g0/1
R2(config-if)#description interface hacia Internet    Se realiza
descripción de la interfaz
R2(config-if)#ip address 209.165.200.233 255.255.255.248  Se digita la
dirección IP y máscara de subred a la interfaz
R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 Se ingresa dirección
IPV6 a la interfaz
R2(config-if)#no shutdown                Se activa la interfaz
R2(config-if)#int loopback 0             Se ingresa a la interfaz loopback 0
%LINK-5-CHANGED: Interface Loopback0, changed state to up
R2(config-if)#description servidor WEBSe realiza descripción de la interfaz
R2(config-if)#ip address 10.10.10.10 255.255.255.255    Se digita la
dirección IP y máscara de subred a la interfaz
```

```
R2(config-if)#exit                          Se sale de la interfaz
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0    Se configura la ruta predeterminada IPV4 para la interfaz g0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#ipv6 route ::/0 G0/0             Se configura la ruta predeterminada IPV6 para la interfaz g0/0
```

2.2.4. Configurar R3

La configuración del R3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del router: R3
- Contraseña de exec privilegiado cifrada: class
- Contraseña de acceso a la consola: cisco
- Contraseña de acceso Telnet: cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD: Se prohíbe el acceso no autorizado
- Interfaz S0/0/1:
  Establecer la descripción
  Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.
  Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
  Activar la interfaz
- Interfaz loopback 4:
  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
- Interfaz loopback 5:
  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
- Interfaz loopback 6
  Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
- Interfaz loopback 7
  Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
- Rutas predeterminadas

A continuación se anexa el código de configuración de R3:

```
Router>enable                                   Se ingresa al modo EXEC privilegiado
Router#configure terminal                       Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup              Se desactiva la búsqueda DNS
Router(config)#hostname R3                      Se le ingresa nombre al router R3
R3(config)#enable secret class                  Se configura contraseña para EXEC privilegiado cifrada
R3(config)#line console 0                       Se ingresa al modo de configuración de línea de la consola
R3(config-line)#password cisco                  Se ingresa la contraseña para la línea de  consola
R3(config-line)#login                           Se utiliza para que el router requiera autenticación al iniciar sesión
R3(config-line)#line vty 0 4                    Se ingresa a la configuración de la línea VTY del router
R3(config-line)#password cisco                  Se pone contraseña a esa línea VTY
R3(config-line)#login                           Se utiliza para que el router requiera autenticación a la línea VTY
R3(config-line)#exit                            Se sale de la configuración de línea VTY
R3(config)#service password-encryption          Se cifran las contraseñas de texto no cifrado
R3(config)#banner motd #                        Se ingresa un mensaje de aviso
Enter TEXT message.  End with the character '#'.
Se prohbe el acceso no autorizado.#

R3(config)#ipv6 unicast-routing
R3(config)#int s0/0/1                           Se ingresa a la interfaz s0/0/1
R3(config-if)#description interface hacia el router R2   Se realiza descripción de la interfaz
R3(config-if)#ip address 172.16.2.2 255.255.255.252  Se digita la dirección IP y máscara de subred a la interfaz
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64  Se ingresa dirección IPV6 a la interfaz
R3(config-if)#no shutdown                       Se activa la interfaz
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#int loopback 4                    Se ingresa a la interfaz loopback 4
%LINK-5-CHANGED: Interface Loopback4, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed
state to up
R3(config-if)#ip  address  192.168.4.1  255.255.255.0    Se digita la
dirección IP y máscara de subred a la interfaz
R3(config-if)#exit                    Se sale de la configuración de la
interfaz
R3(config)#int loopback 5             Se ingresa a la interfaz loopback 5
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed
state to up
R3(config-if)#ip  address  192.168.5.1  255.255.255.0    Se digita la
dirección IP y máscara de subred a la interfaz
R3(config-if)#exit                    Se sale de la configuración de la
interfaz
R3(config)#int loopback 6             Se ingresa a la interfaz loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed
state to up
R3(config-if)#ip  address  192.168.6.1  255.255.255.0    Se digita la
dirección IP y máscara de subred a la interfaz
R3(config-if)#exit                    Se sale de la configuración de la
interfaz
R3(config)#int loopback 7             Se ingresa a la interfaz loopback 7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed
state to up
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64  Se ingresa dirección
IPV6 a la interfaz
R3(config-if)#exit                    Se sale de la configuración de la
interfaz
R3(config)#ip  route  0.0.0.0  0.0.0.0  S0/0/1    Se configura la ruta
predeterminada IPV4 para la interfaz 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     Se configura la ruta predeterminada
IPV6 para la interfaz s0/0/1
```

2.2.5. Configurar S1

La configuración del S1 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del switch: S1
- Contraseña de exec privilegiado cifrada: class
- Contraseña de acceso a la consola: cisco
- Contraseña de acceso Telnet: cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD: Se prohíbe el acceso no autorizado.

A continuación se anexa el código de configuración de S1:

```
Switch>enable                          Se ingresa al modo EXEC privilegiado
Switch#configure terminal              Se ingresa al modo de configuración
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup     Se desactiva la búsqueda DNS
Switch(config)#hostname S1             Se le ingresa nombre al switch S1
S1(config)#enable secret class         Se configura contraseña para EXEC privilegiado cifrada
S1(config)#line console 0              Se ingresa al modo de configuración de línea de la consola
S1(config-line)#password cisco         Se ingresa la contraseña para la línea de  consola
S1(config-line)#login                  Se utiliza para que el switch requiera autenticación al iniciar sesión
S1(config-line)#line vty 0 15          Se ingresa a la configuración de la línea VTY del switch
S1(config-line)#password cisco Se pone contraseña a esa línea VTY
S1(config-line)#login                  Se utiliza para que el router requiera autenticación a la línea VTY
S1(config)#service password-encryptionSe cifran las contraseñas de texto no cifrado
S1(config)#banner motd #               Se ingresa un mensaje de aviso
Enter TEXT message. End with the character '#'.
Se prohibe el acceso no autorizado.#
```

2.2.6. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- Desactivar la búsqueda DNS
- Nombre del switch: S3
- Contraseña de exec privilegiado cifrada: class
- Contraseña de acceso a la consola: cisco
- Contraseña de acceso Telnet: cisco
- Cifrar las contraseñas de texto no cifrado
- Mensaje MOTD: Se prohíbe el acceso no autorizado.

A continuación se anexa el código de configuración de S3:

```
Switch>enable                          Se ingresa al modo EXEC privilegiado
Switch#configure terminal              Se ingresa al modo de configuración
Switch(config)#no ip domain-lookup     Se desactiva la búsqueda DNS
Switch(config)#hostname S3             Se le ingresa nombre al switch S3
S3(config)#enable secret class         Se configura contraseña para EXEC privilegiado cifrada
S3(config)#line console 0              Se ingresa al modo de configuración de línea de la consola
S3(config-line)#password cisco         Se ingresa la contraseña para la línea de  consola
S3(config-line)#login                  Se utiliza para que el switch requiera autenticación al iniciar sesión
S3(config-line)#line vty 0 15          Se ingresa a la configuración de la línea VTY del switch
S3(config-line)#password cisco Se pone contraseña a esa línea VTY
S3(config-line)#login                  Se utiliza para que el router requiera autenticación a la línea VTY
S3(config-line)#exit                   Se sale de la configuración de línea VTY
S3(config)#service password-encryptionSe cifran las contraseñas de texto no cifrado
S3(config)#banner motd #               Se ingresa un mensaje de aviso
Enter TEXT message. End with the character '#'.
Se prohibe el acceso no autorizado. #
```

2.2.7. Verificar la conectividad de la red

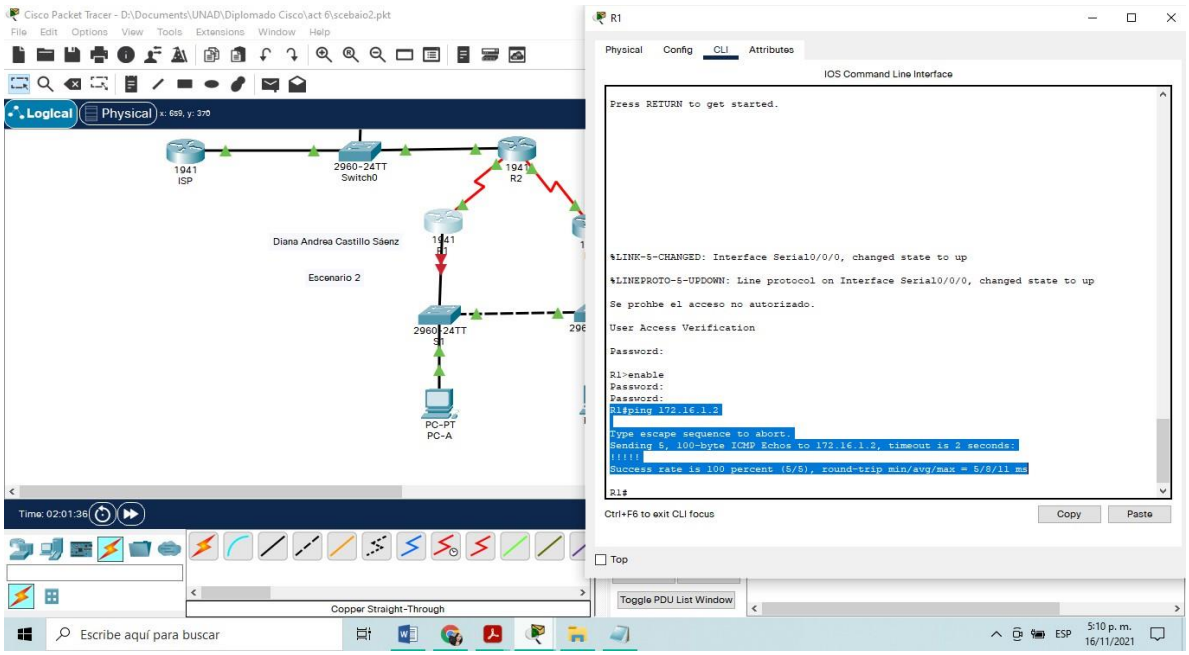
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

- Desde R1 a R2, S0/0/0 dirección ip 172.16.1.2

```
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/11
ms
```

Se observa ping satisfactorio

Figura 12. Ping de R1 a R2.



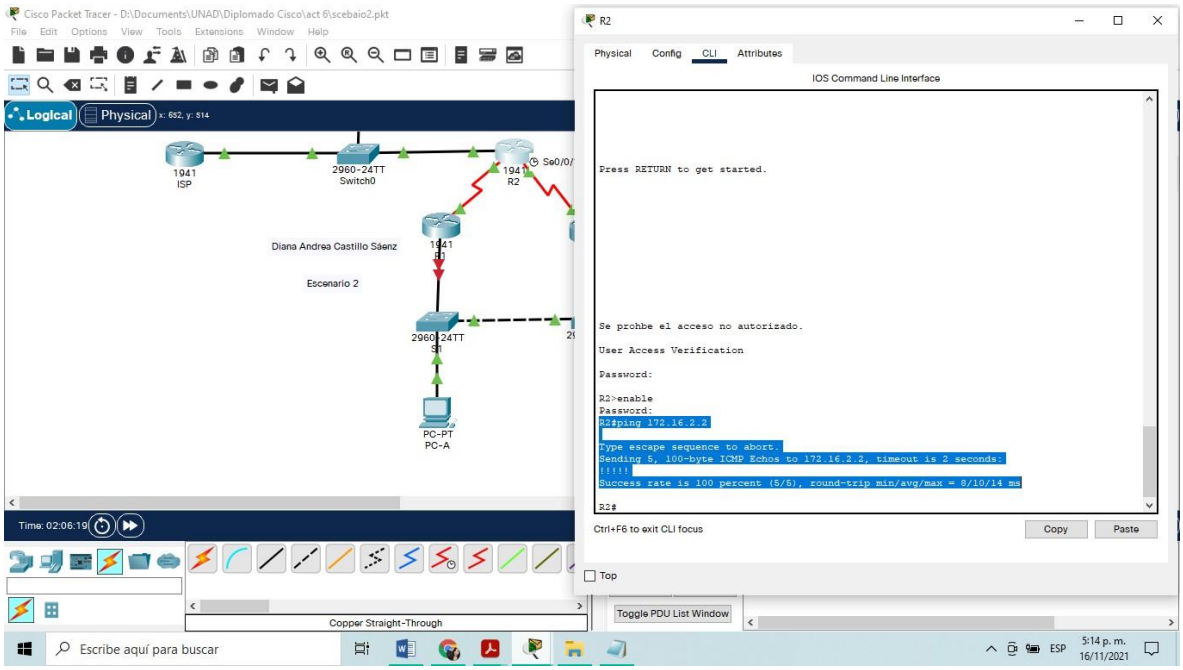
Fuente: Autor

- Desde R2 a R3, S0/0/1 dirección ip 172.16.2.2, 2001:DB8:ACAD:2::1

```
R2#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/14
ms
```

Se observa ping satisfactorio

Figura 13. Ping de R2 a R3 172.16.2.2

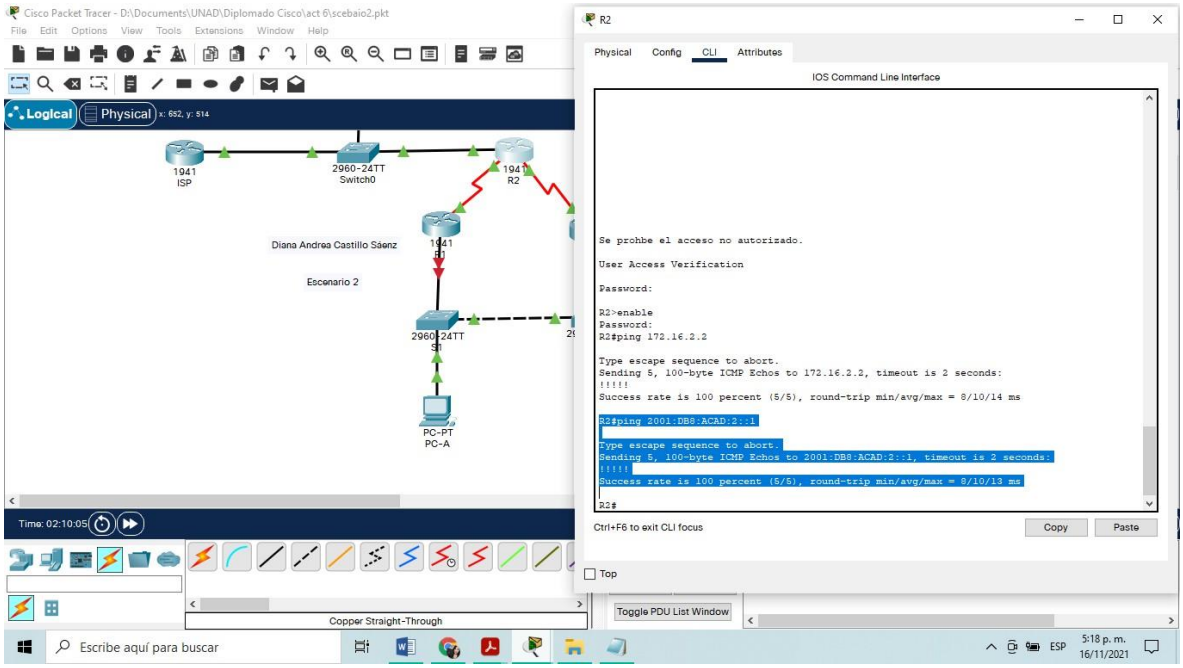


Fuente: Autor

```
R2#ping 2001:DB8:ACAD:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/13
ms
```

Se observa ping satisfactorio

Figura 14. Ping de R2 a R3 2001:DB8:ACAD:2::1



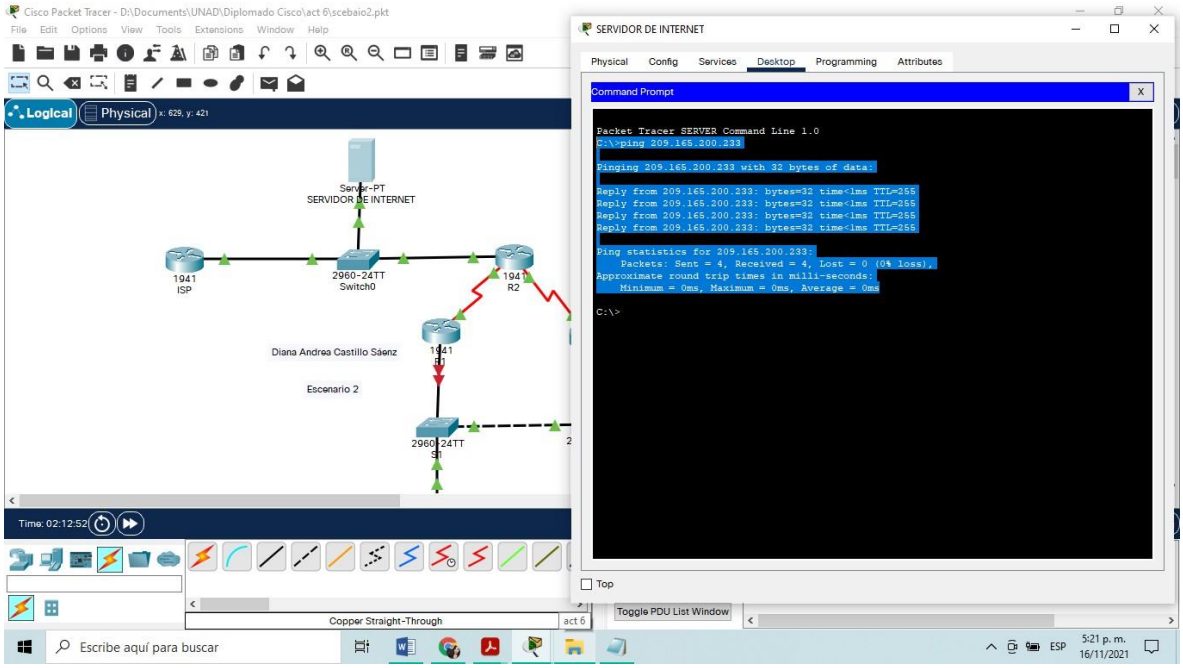
Fuente: Autor

- PC de internet a Gateway predeterminado dirección ip 209.165.200.233, 2001:DB8:ACAD:A::1

```
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 TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255
Reply from 209.165.200.233: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Se observa ping satisfactorio

Figura 15. PC de internet a Gateway 209.165.200.233

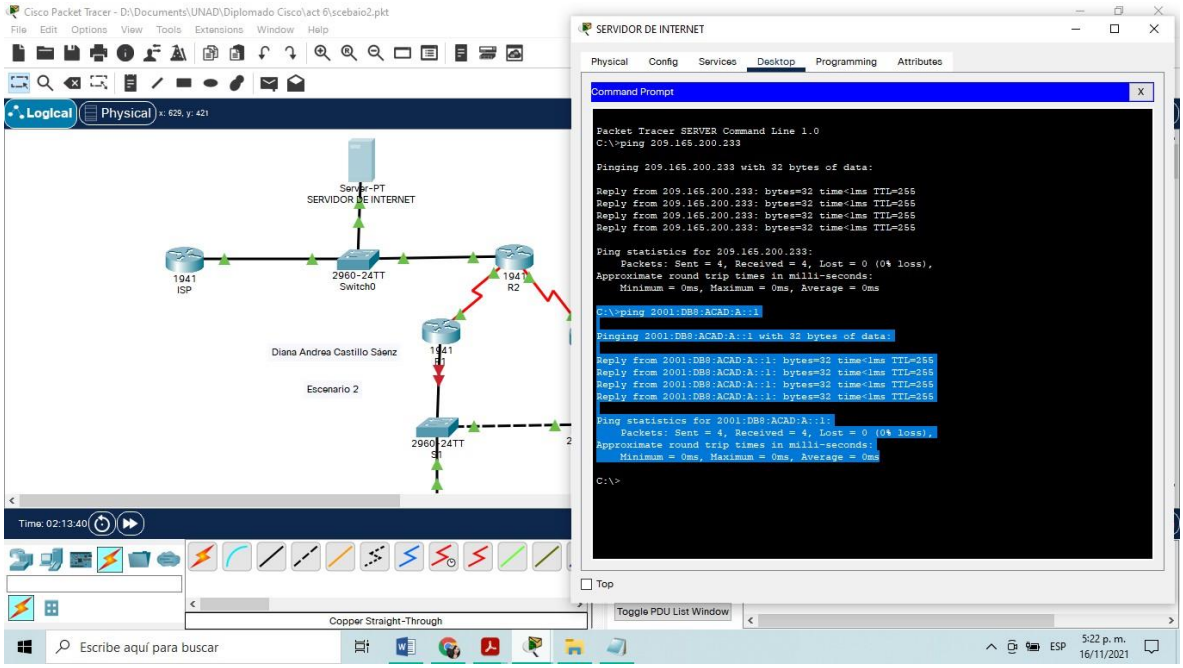


Fuente: Autor

```
C:\>ping 2001:DB8:ACAD:A::1

Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Se observa ping satisfactorio

Figura 16. PC de internet a Gateway 2001:DB8:ACAD:A::1



Fuente: Autor

2.3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN

2.3.1. Configurar S1

La configuración del S1 incluye las siguientes tareas:

- Crear la base de datos de VLAN: Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
- Asignar la dirección IP de administración:
  Asigne la dirección IPv4 a la VLAN de administración.
  Utilizar la dirección IP asignada al S1 en el diagrama de topología
- Asignar el gateway predeterminado: Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
- Forzar el enlace troncal en la interfaz F0/3: Utilizar la red VLAN 1 como VLAN nativa.
- Forzar el enlace troncal en la interfaz F0/5: Utilizar la red VLAN 1 como VLAN nativa.
- Configurar el resto de los puertos como puertos de acceso: Utilizar el comando interface range

- Asignar F0/6 a la VLAN 21
- Apagar todos los puertos sin usar

A continuación se anexa el código de configuración de seguridad, Vlan de S1:

```
S1(config)#vlan 21                      Se crea la vlan 21 en el S1
S1(config-vlan)#name contabilidad       Se le da nombre a la vlan 21
S1(config-vlan)#vlan 23                 Se crea la vlan 23
S1(config-vlan)#name ingenieria         Se le da nombre a la vlan 23
S1(config-vlan)#vlan 99                 Se crea la vlan 99
S1(config-vlan)#name administracion     Se le da nombre a la vlan 99
S1(config-vlan)#int vlan 99             Se ingresa a la interfaz vlan 99
%LINK-5-CHANGED: Interface Vlan99, changed state to up
S1(config-if)#ip address 192.168.99.2 255.255.255.0    Se digita la
dirección IP y máscara de subred a la interfaz
S1(config-if)#no shutdown               Se activa la interfaz
S1(config-if)#exit                      Se sale de la interfaz
S1(config)#ip default-gateway 192.168.99.1    Se asigna el gateway
predeterminado
S1(config)#int f0/3                     Se ingresa a la interfaz f0/3
S1(config-if)#sw mode trunk             Se fuerza el enlace troncal en la
interfaz
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
S1(config-if)#sw trunk native vlan 1  Se utiliza la vlan 1 como enlace
troncal nativa
S1(config-if)#exit                      Se sale de la interfaz
S1(config)#int f0/5                     Se ingresa a la interfaz f0/3
S1(config-if)#sw mode trunk             Se fuerza el enlace troncal en la
interfaz
S1(config-if)#sw trunk native vlan 1  Se utiliza la vlan 1 como enlace
troncal nativa
S1(config-if)#exit                      Se sale de la interfaz
S1(config)#int range f0/1- f0/2         Se ingresa al rango de interfaces
f0/1 – f0/2
S1(config-if-range)#sw mode access    Se configura como puertos de
acceso
```

```
S1(config-if-range)#int range f0/7- f0/24   Se ingresa al rango de interfaces f0/7 – f0/24
S1(config-if-range)#sw mode access   Se configura como puertos de acceso
S1(config-if-range)#exit   Se sale de ese rango de interfaces
S1(config)#int f0/6   Se ingresa a la interfaz f0/6
S1(config-if)#sw mode access   Se configura como puertos de acceso
S1(config-if)#sw access vlan 21 Se asigna la vlan 21 a la interfaz f0/6
S1(config-if)#exit   Se sale de la configuración mode access
S1(config)#int range f0/7- f0/24   Se ingresa al rango de interfaces f0/7 – f0/24
S1(config-if-range)#shutdown   Se apagan los puertos de ese rango sin usar
```

2.3.2. Configurar el S3

La configuración del S3 incluye las siguientes tareas:

- Crear la base de datos de VLAN: Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
- Asignar la dirección IP de administración: Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología.
- Asignar el gateway predeterminado: Asignar la primera dirección IP en la subred como gateway predeterminado.
- Forzar el enlace troncal en la interfaz F0/3: Utilizar la red VLAN 1 como VLAN nativa.
- Configurar el resto de los puertos como puertos de acceso: Utilizar el comando interface range.
- Asignar F0/18 a la VLAN 21.
- Apagar todos los puertos sin usar.

A continuación se anexa el código de configuración de seguridad, Vlan de S3:

```
S3(config)#vlan 21   Se crea la vlan 21 en el S3
S3(config-vlan)#name contabilidad   Se le da nombre a la vlan 21
S3(config-vlan)#vlan 23   Se crea la vlan 23 en el S3
S3(config-vlan)#name ingenieria   Se le da nombre a la vlan 23
```

```
S3(config-vlan)#vlan 99                Se crea la vlan 99 en el S3
S3(config-vlan)#name administracion    Se le da nombre a la vlan 99
S3(config-vlan)#exit                   Se sale de la interfaz
S3(config)#int vlan 99                 Se ingresa a la Vlan 99
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
S3(config-if)#ip address 192.168.99.3 255.255.255.0    Se digita la
dirección IP y máscara de subred a la interfaz
S3(config-if)#no shutdown              Se activa la interfaz
S3(config-if)#exit                     Se sale de la interfaz
S3(config)#ip default-gateway 192.168.99.1    Se asigna el gateway
predeterminado
S3(config)#int f0/3                    Se ingresa a la interfaz f0/3
S3(config-if)#sw mode trunk            Se fuerza el enlace troncal en la
interfaz
S3(config-if)#sw trunk native vlan 1   Se utiliza la vlan 1 como enlace
troncal nativa
S3(config-if)#exit                     Se sale de la interfaz
S3(config)#int range f0/1 - f0/2       Se ingresa al rango de interfaces
f0/1 – f0/2
S3(config-if-range)#sw mode access     Se configura como puertos de
acceso
S3(config-if-range)#int range f0/7 - f0/24    Se ingresa al rango de
interfaces f0/7 – f0/24
S3(config-if-range)#sw mode access     Se configura como puertos de
acceso
S3(config-if-range)#exit               Se sale de ese rango de interfaces
S3(config)#int f0/18                   Se ingresa a la interfz f0/18
S3(config-if)#sw access vlan 21        Se asigna la vlan 21 a la interfaz
f0/18
S3(config-if)#exit                     Se sale de la interfaz
S3(config)#int range f0/7 - f0/17      Se ingresa al rango de interfaces
f0/7 – f0/17
S3(config-if-range)#shutdown           Se apagan esos puertos
S3(config-if-range)#exit               Se sale de ese rango de interfaces
S3(config)#int range f0/19 - f0/24     Se ingresa al rango de interfaces
f0/19 – f0/24
S3(config-if-range)#shutdown           Se apagan esos puertos
```

2.3.3. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

- 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
- 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
- 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
- Activar la interfaz G0/1

A continuación se anexa el código de configuración subinterfaces de R1:

```
R1(config)#int g0/1                    Se ingresa a la interfaz g0/1
R1(config-if)#no shutdown              Se activa la interfaz
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)#exit                     Se sale de la interfaz
R1(config)#int g0/1.21                 Se ingresa a la subinterfaz g0/1.21
%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
R1(config-subif)#description Lan contabilidad..Se realiza descripción de
la subinterfaz
R1(config-subif)#encapsulation dot1q 21 Se habilita 802.1Q y asociar una
VLAN específica VLAN a la subinterfaz
R1(config-subif)#ip address 192.168.21.1 255.255.255.0.. Se digita la
dirección IP y máscara de subred a la subinterfaz
R1(config-subif)#exit                  Se sale de la subinterfaz
R1(config)#int g0/1.23                 Se ingresa a la subinterfaz g0/1.23
%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
R1(config-subif)#description Lan ingenieria Se realiza descripción de la subinterfaz
R1(config-subif)#encapsulation dot1q 23 Se habilita 802.1Q y asociar una VLAN específica VLAN a la subinterfaz
R1(config-subif)#ip address 192.168.23.1 255.255.255.0 Se digita la dirección IP y máscara de subred a la subinterfaz
R1(config-subif)#exit Se sale de la subinterfaz
R1(config)#int g0/1.99 Se ingresa a la subinterfaz g0/1.99
%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-subif)#description Lan administracion Se realiza descripción de la subinterfaz
R1(config-subif)#encapsulation dot1q 99 Se habilita 802.1Q y asociar una VLAN específica VLAN a la subinterfaz
R1(config-subif)#ip address 192.168.99.1 255.255.255.0 Se digita la dirección IP y máscara de subred a la subinterfaz
R1(config-subif)#exit Se sale de la subinterfaz

2.3.4. Verificar la conectividad de la red

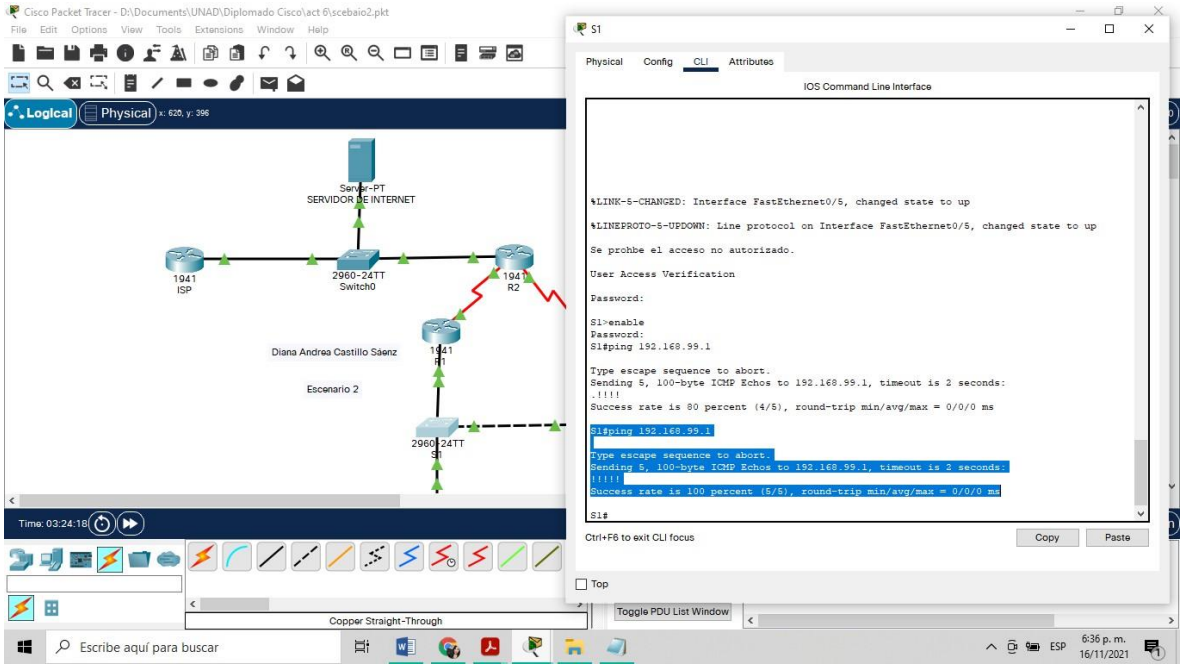
Utilice el comando ping para probar la conectividad entre los switches y el R1.
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

- Desde S1 a R1, dirección VLAN 99 Dirección ip 192.168.99.1

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Se realiza ping satisfactorio

Figura 17. Ping desde S1 a R1 192.168.99.1



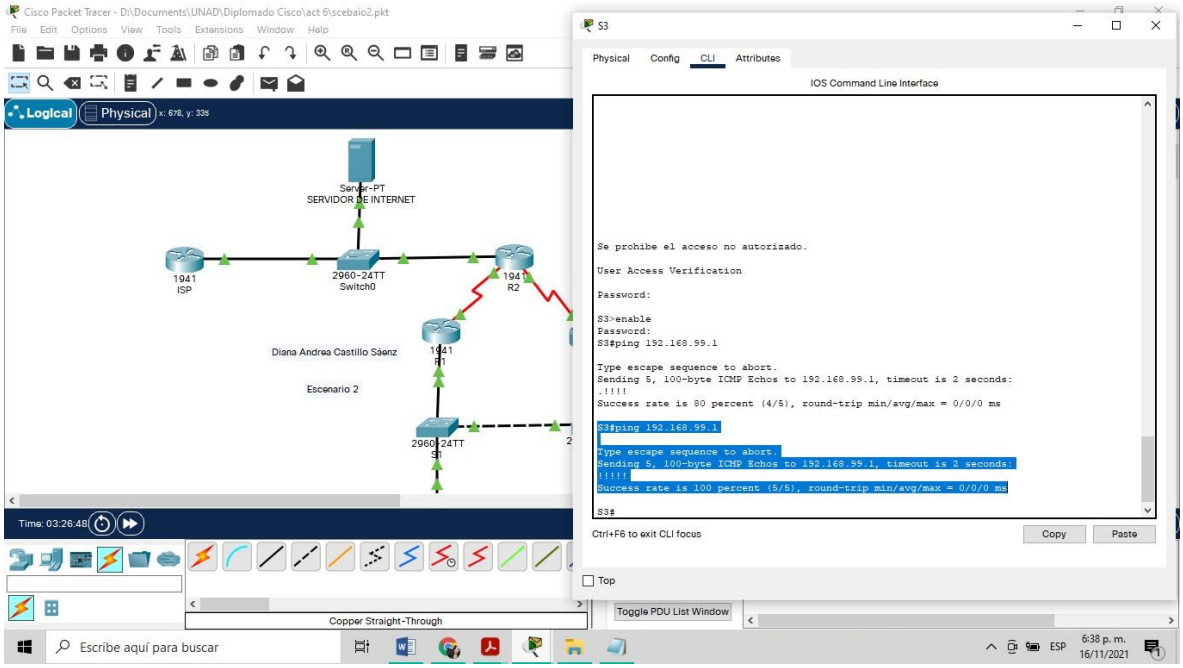
Fuente: Autor

- Desde S3 a R1, dirección VLAN 99 Dirección ip 192.168.99.1

```
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Se realiza ping satisfactorio

Figura 18. Ping desde S3 a R1 192.168.99.1



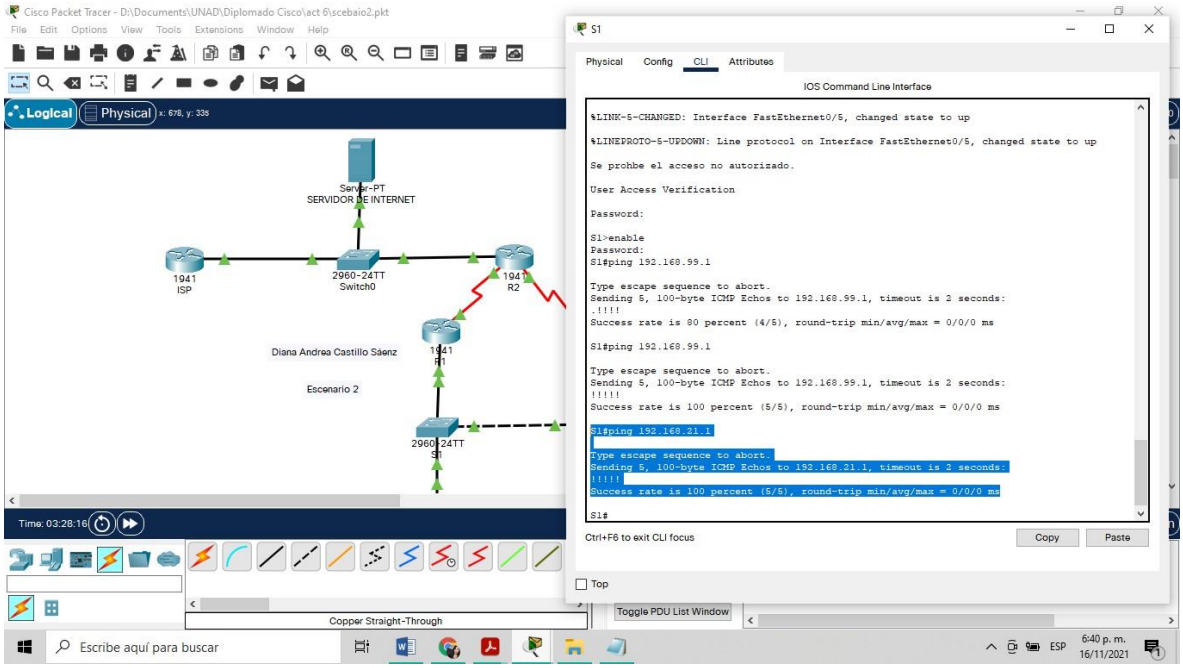
Fuente: Autor

- Desde S1 a R1, dirección VLAN 21 Dirección ip 192.168.21.1

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Se realiza ping satisfactorio

Figura 19. Ping desde S1 a R1 192.168.21.1



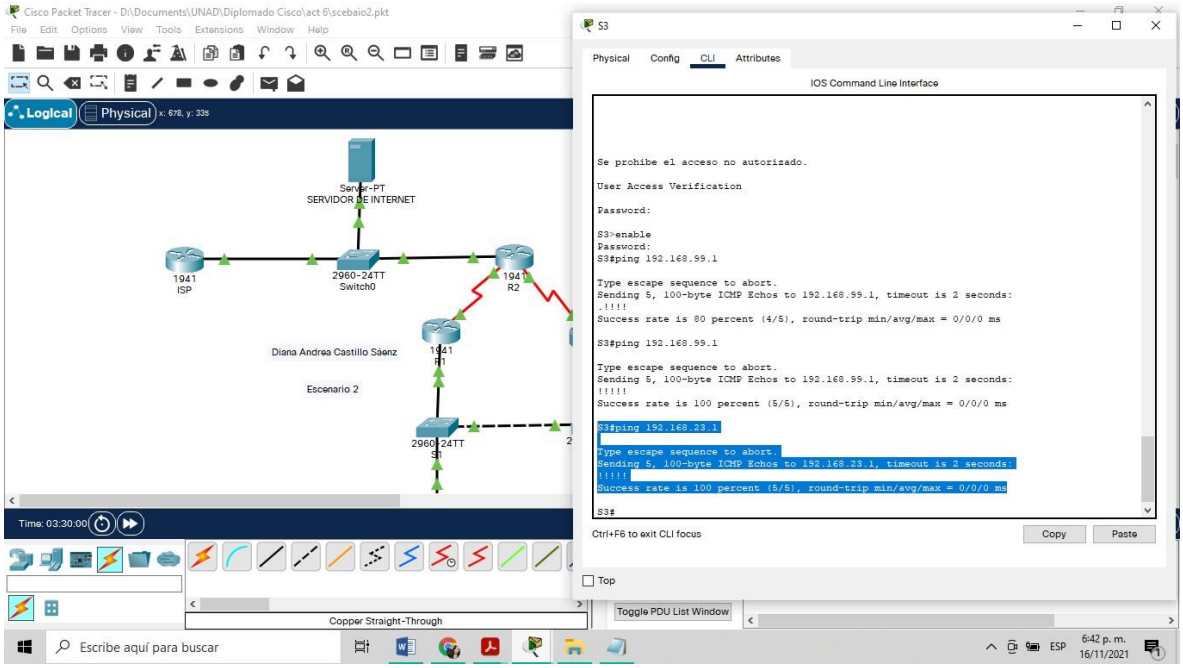
Fuente: Autor

- Desde S3 a R1, dirección VLAN 23 Dirección ip 192.168.23.1

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Se realiza ping satisfactorio

Figura 20. Ping desde S3 a R1 192.168.21.1



Fuente: Autor

2.4. Configurar el protocolo de routing dinámico OSPF

2.4.1. Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente: Asigne todas las redes conectadas directamente.
- Establecer todas las interfaces LAN como pasivas
- Desactive la sumarización automática En el protocolo ospf no se realiza sumarización automática

A continuación se anexa el código de configuración de OSPF en R1:

`R1(config)#router ospf 30` Activar protocolo de enrutamiento ospf en el R1

R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 Red conectada y se configura en el área 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 Red conectada y se configura en el área 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 Red conectada y se configura en el área 0
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 Red conectada y se configura en el área 0
R1(config-router)#passive-interface g0/1 Se establece la interface g0/1 como pasiva
R1(config-router)#passive-interface g0/1.21 Se establece la interface g0/1.21 como pasiva
R1(config-router)#passive-interface g0/1.23 Se establece la interface g0/1.23 como pasiva
R1(config-router)#passive-interface g0/1.99 Se establece la interface g0/1.99 como pasiva

2.4.2. Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

- Configurar OSPF área 0
- Anunciar las redes conectadas directamente: Nota: Omitir la red G0/0.
- Establecer la interfaz LAN (loopback) como pasiva
- Desactive la sumarización automática. En el protocolo ospf no se realiza sumarización automática

A continuación se anexa el código de configuración de OSPF en R2:

R2(config)#router ospf 30 Activar protocolo de enrutamiento ospf en el R2
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 Red conectada y se configura en el área 0
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 Red conectada y se configura en el área 0
03:52:44: %OSPF-5-ADJCHG: Process 30, Nbr 192.168.99.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 Red conectada y se configura en el área 0
R2(config-router)#passive-interface loopback 0 Se establece la interface loopback 0 como pasiva

2.4.3. Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

- Configurar OSPF área 0
- Anunciar redes IPv4 conectadas directamente
- Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas
- Desactive la sumarización automática. En el protocolo ospf no se realiza sumarización automática

A continuación se anexa el código de configuración de OSPFv3 en R3:

`R3(config)#ipv6 router ospf 31`	Activar protocolo de enrutamiento ospfv3 en el R3
`R3(config-rtr)#router-id 2.2.2.2`	Se identifica el R3 como ospfv3
`R3(config-rtr)#exit`	Se sale la configuración del protocolo ospfv3
`R3(config)#int s0/0/1`	Se ingresa a la interfaz s0/0/1
`R3(config-if)#ipv6 ospf 31 area 0`	Activar protocolo de enrutamiento ospfv3 en la interfaz s0/0/1 y se configura en el área 0
`R3(config-if)#exit`	Se sale de esa configuración
`R3(config)#int loopback 7`	Se ingresa a la interfaz loopback 7
`R3(config-if)#ipv6 ospf 31 area 0`	Activar protocolo de enrutamiento ospfv3 en la interfaz loopback 7 y se configura en el área 0
`R3(config-if)#exit`	Se sale de esa configuración
`R3(config)#ipv6 router ospf 31`	Protocolo de enrutamiento ospfv3 en el R3
`R3(config-rtr)#passive-interface lo 4`	Se establece la interface loopback 4 como pasiva
`R3(config-rtr)#passive-interface lo 5`	Se establece la interface loopback 5 como pasiva
`R3(config-rtr)#passive-interface lo 6`	Se establece la interface loopback 6 como pasiva

2.4.4. Verificar la información de OSPF

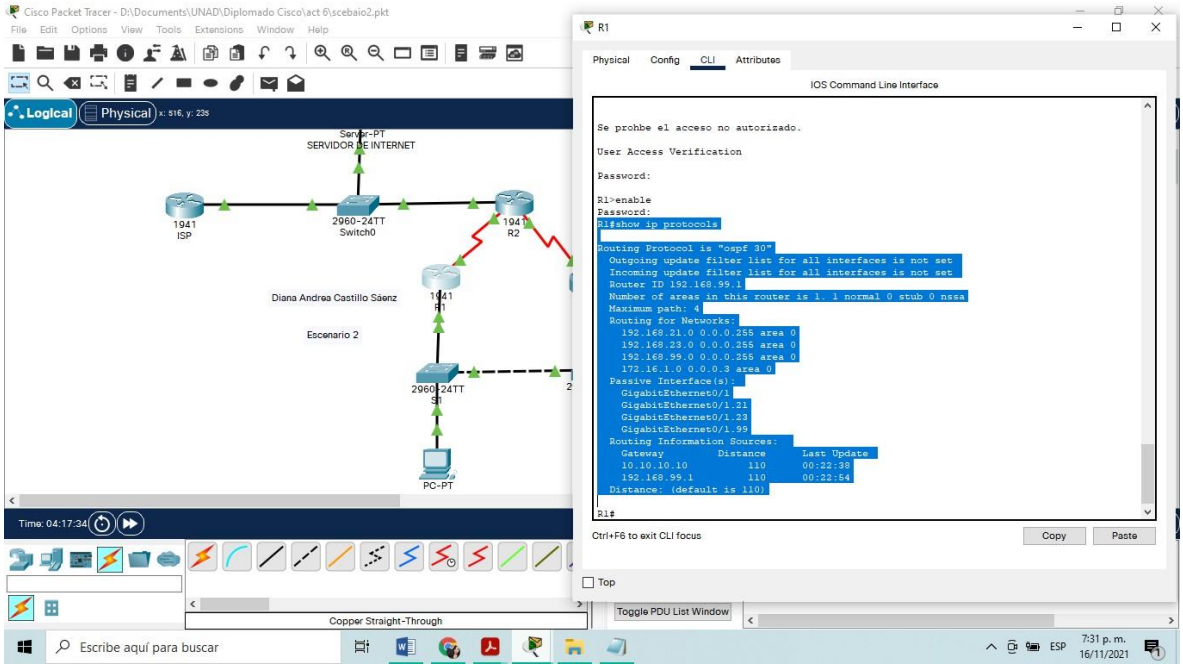
Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

- ¿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 utiliza el comando show ip protocols

```
R1#show ip protocols
Routing Protocol is "ospf 30"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.99.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.21.0 0.0.0.255 area 0
    192.168.23.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
    172.16.1.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10          110      00:22:38
    192.168.99.1         110      00:22:54
  Distance: (default is 110)
```

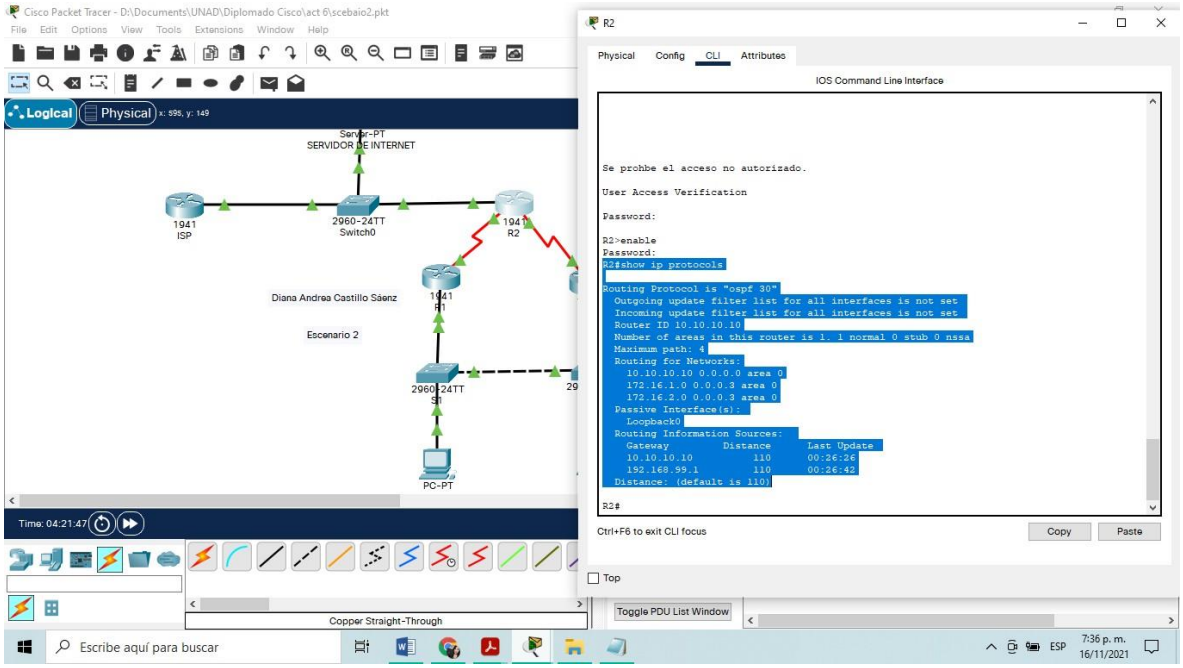
Figura 21. Show ip protocols en R1.



Fuente: Autor

```
R2#show ip protocols
Routing Protocol is "ospf 30"
  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:
    10.10.10.10 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10           110      00:26:26
    192.168.99.1          110      00:26:42
  Distance: (default is 110)
```

Figura 22. Show ip protocols en R2.



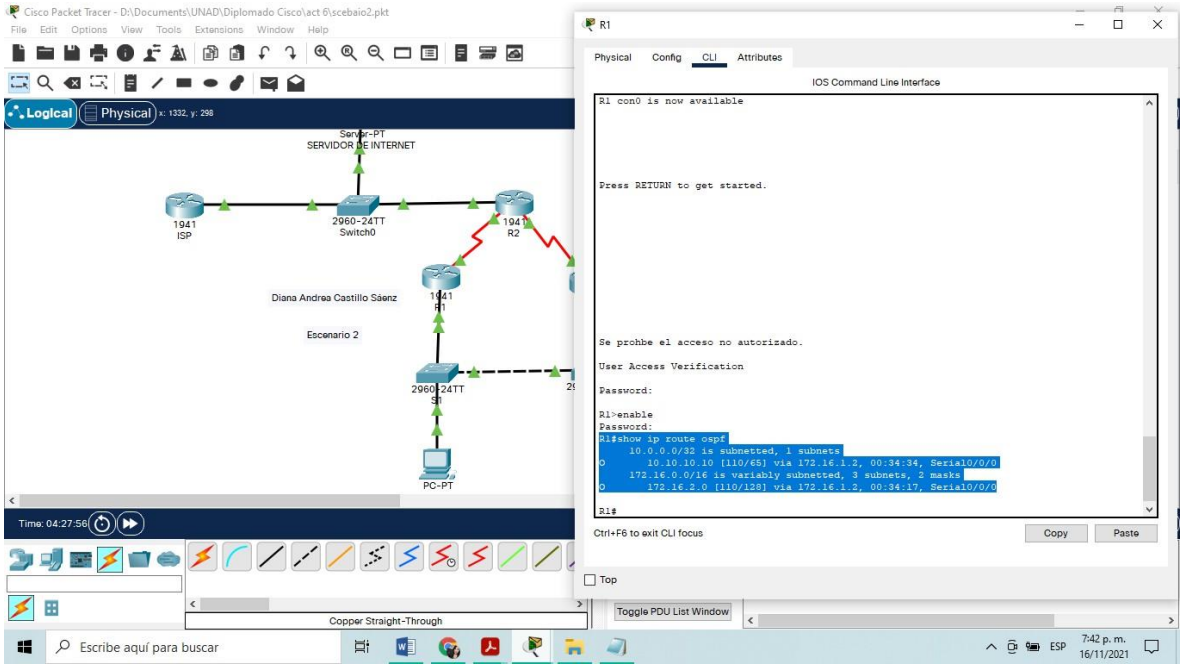
Fuente: Autor

- ¿Qué comando muestra solo las rutas OSPF?

Se utiliza el comando show ip route ospf

```
R1#show ip route ospf
     10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10 [110/65] via 172.16.1.2, 00:34:34, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.2.0 [110/128] via 172.16.1.2, 00:34:17, Serial0/0/0
```

Figura 23. Show ip route ospf en R1.



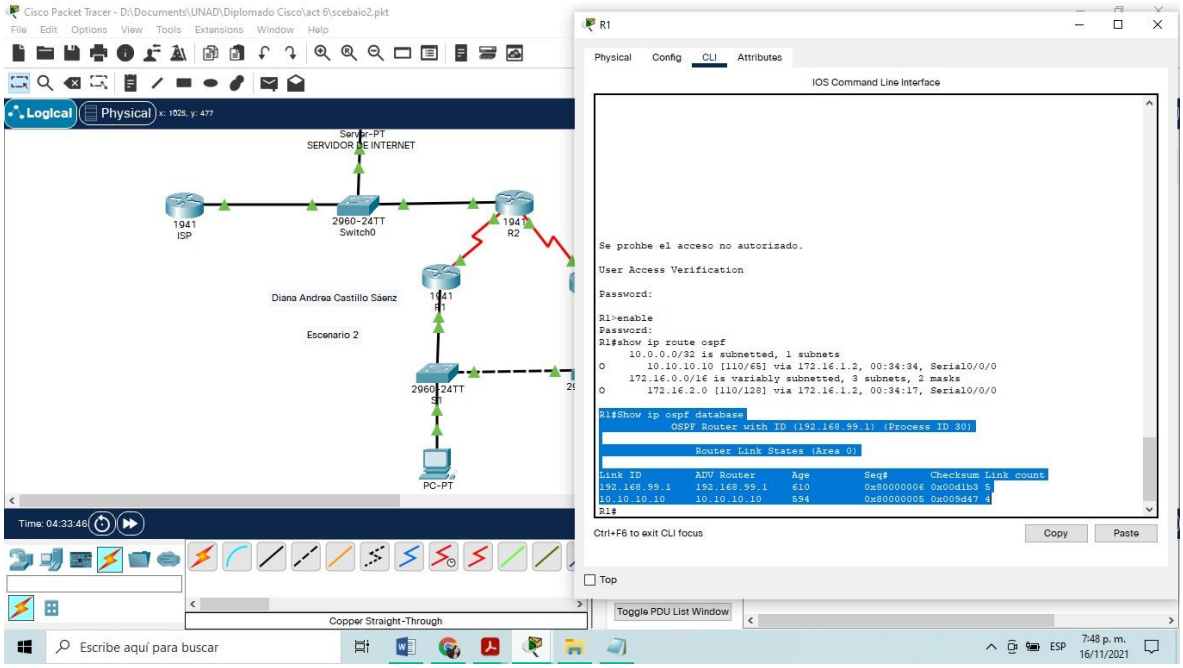
Fuente: Autor

- ¿Qué comando muestra la sección de OSPF de la configuración en ejecución?

Se utiliza el comando show ip ospf database

```
R1#Show ip ospf database
            OSPF Router with ID (192.168.99.1) (Process ID 30)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link
count
192.168.99.1    192.168.99.1    610          0x80000006 0x00d1b3 5
10.10.10.10     10.10.10.10     594          0x80000005 0x009d47 4
```

Figura 24. Show ip ospf database en R1.



Fuente: Autor

2.5. Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

- Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.
- Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas.
- 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
- Crear un pool de DHCP para la VLAN 23:
  Nombre: ENGNR
  Servidor DNS: 10.10.10.10
  Nombre de dominio: ccna-sa.com

Establecer el gateway predeterminado

A continuación se anexa el código de configuración de R1 como servidor de DHCP para las VLAN 21 y 23:

`R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20` Se reservan las primeras 20 direcciones IP en la vlan 21 para configuraciones estáticas
`R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20` Se reservan las primeras 20 direcciones IP en la vlan 23 para configuraciones estáticas
`R1(config)#ip dhcp pool ACCT` Se crea un pool de DHCP con nombre ACCT
`R1(dhcp-config)#network 192.168.21.0 255.255.255.0` Se establece la Vlan 21 para el pool DHCP
`R1(dhcp-config)#domain-name ccna-sa.com` Se establece nombre de dominio como ccna-sa.com
`R1(dhcp-config)#dns-server 10.10.10.10` Se establece servidor DNS 10.10.10.10
`R1(dhcp-config)#default-router 192.168.21.1` Se establece el gateway predeterminado
`R1(dhcp-config)#exit` Se sale de la configuración DHCP
`R1(config)#ip dhcp pool ENGNR` Se crea un pool de DHCP con nombre ENGNR
`R1(dhcp-config)#network 192.168.23.0 255.255.255.0` Se establece la Vlan 23 para el pool DHCP
`R1(dhcp-config)#dns-server 10.10.10.10` Se establece servidor DNS 10.10.10.10
`R1(dhcp-config)#domain-name ccna-sa.com` Se establece nombre de dominio como ccna-sa.com
`R1(dhcp-config)#default-router 192.168.23.1` Se establece el gateway predeterminado

2.5.2. Configurar la NAT estática y dinámica en el R2.

La configuración del R2 incluye las siguientes tareas:

- Crear una base de datos local con una cuenta de usuario
  Nombre de usuario: webuser
  Contraseña: cisco12345
  Nivel de privilegio: 15

- Habilitar el servicio del servidor HTTP
- Configurar el servidor HTTP para utilizar la base de datos local para la autenticación
- Crear una NAT estática al servidor web: Dirección global interna: 209.165.200.229
- Asignar la interfaz interna y externa para la NAT estática
- Configurar la NAT dinámica dentro de una ACL privada:
  Lista de acceso: 1
  Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1
  Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
- Defina el pool de direcciones IP públicas utilizables:
  Nombre del conjunto: INTERNET
  El conjunto de direcciones incluye:
  209.165.200.225 – 209.165.200.228
- Definir la traducción de NAT dinámica

A continuación se anexa el código de configuración de la NAT estática y dinámica en el R2:

```
R2(config)#username webuser privilege 15 password cisco12345  Se crea base de datos local con nombre de usuario webuser y contraseña cisco12345y privilegio 15
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.233 Se crea una nat estática
R2(config)#int g0/0                    Se ingresa a la interfaz g0/0
R2(config-if)#ip nat outside          Asignación de nat externa
R2(config-if)#int S0/0/0               Se ingresa a la interfaz s0/0/0
R2(config-if)#ip nat inside           Asignación de nat interna
R2(config-if)#int S0/0/1               Se ingresa a la interfaz s0/0/1
R2(config-if)#ip nat inside           Asignación de nat interna
R2(config-if)#int lo 0                 Se ingresa a la interfaz loopback 0
R2(config-if)#ip nat inside           Asignación de nat interna
R2(config-if)#exit                     Se sale de la configuración de la interfaz
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255  Lista de acceso 1 para contabilidad
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255  Lista de acceso 1 para ingeniería
R2(config)#access-list 1 permit 192.168.0.0 0.0.3.255  Lista de acceso 1 para redes LAN (loopback) en el R3
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
```

```
R2(config-std-nacl)#deny any
R2(config-std-nacl)#!
R2(config-std-nacl)#exit
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248                    Se configura pool de direcciones IP
```
públicas utilizables con nombre INTERNET
```
R2(config)#ip nat inside source list 1 pool INTERNET   Se define
```
traducción de nat dinámica

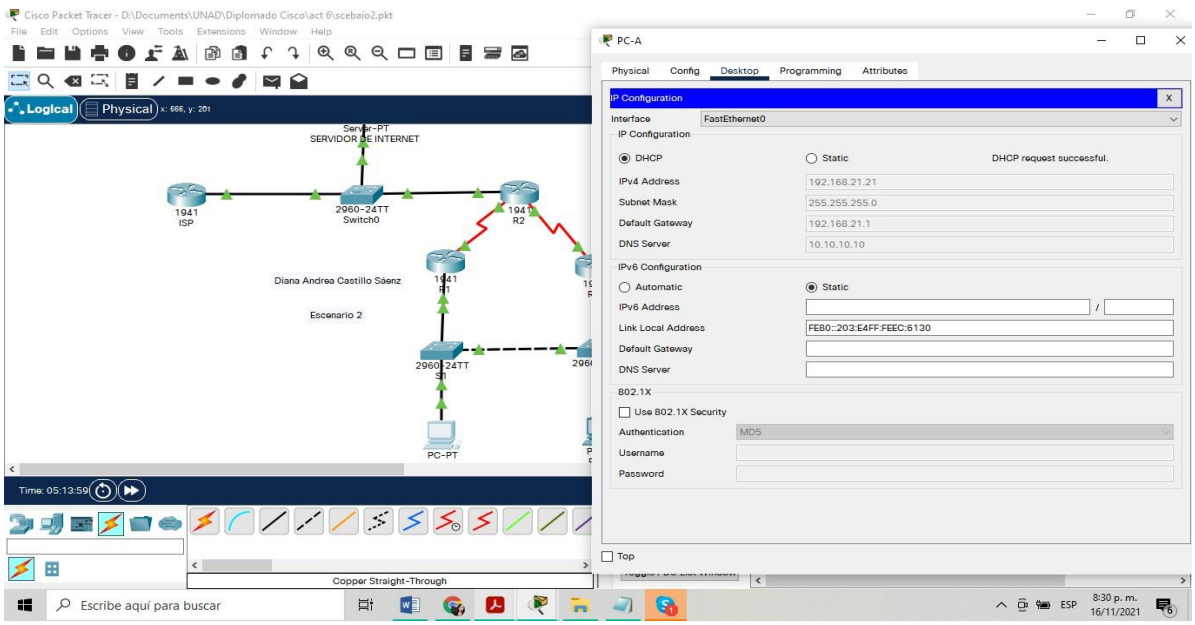
2.5.3. Verificar el protocolo DHCP y la NAT estática

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.

- Verificar que la PC-A haya adquirido información de IP del servidor de DHCP

Se realiza la verificación de que la PC-A adquirió la información IP de servidor de DHCP, se anexa imagen de confirmación:

Figura 25. PC-A con DHCP.

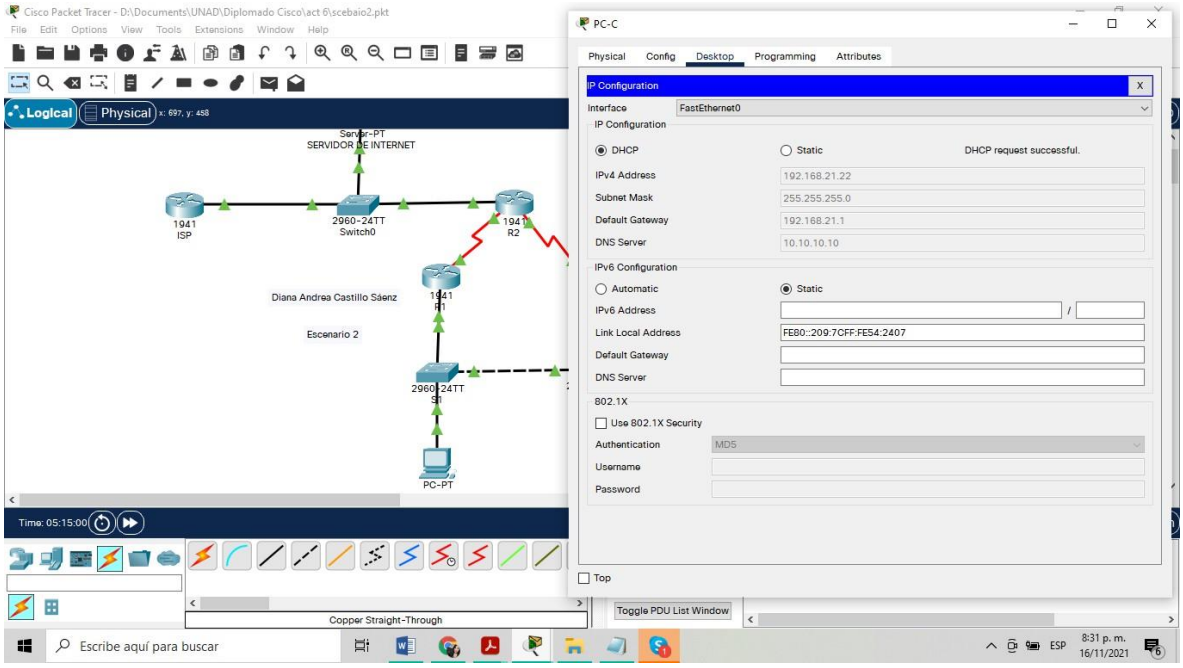


Fuente: Autor

- Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

Se realiza la verificación de que la PC-B adquirió la información IP de servidor de DHCP, se anexa imagen de confirmación:

Figura 26. PC-C con DHCP.



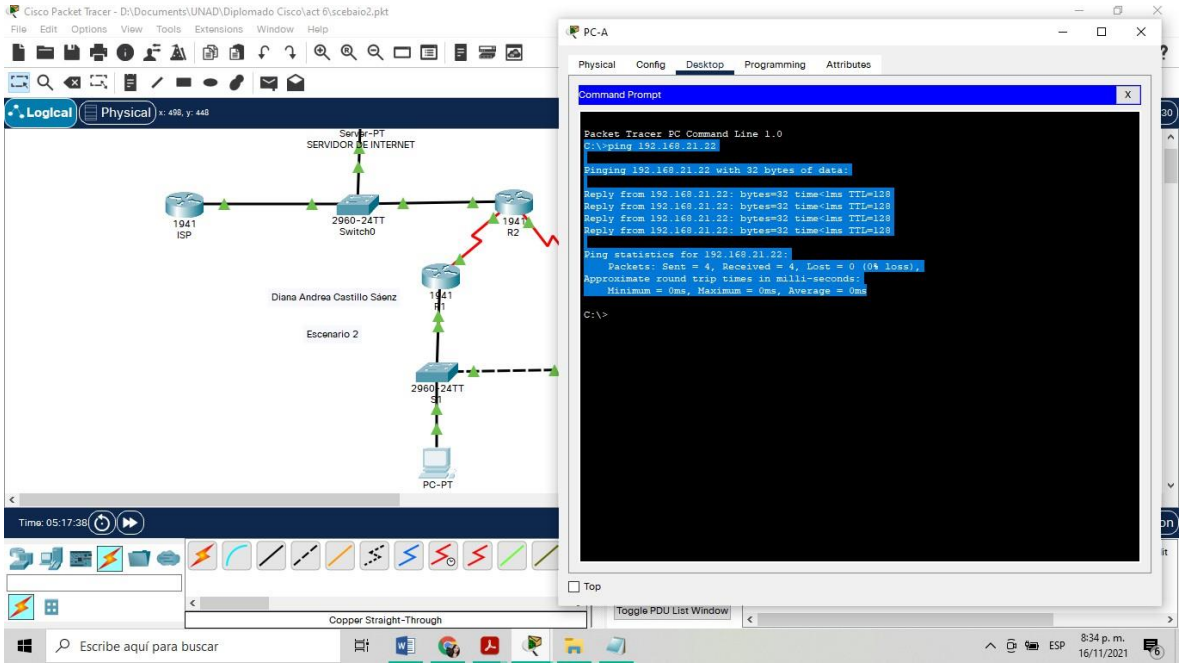
Fuente: Autor

- Verificar que la PC-A pueda hacer ping a la PC-C

```
C:\>ping 192.168.21.22

Pinging 192.168.21.22 with 32 bytes of data:

Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128
Reply from 192.168.21.22: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.21.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 27. Ping PC-A a PC-C.

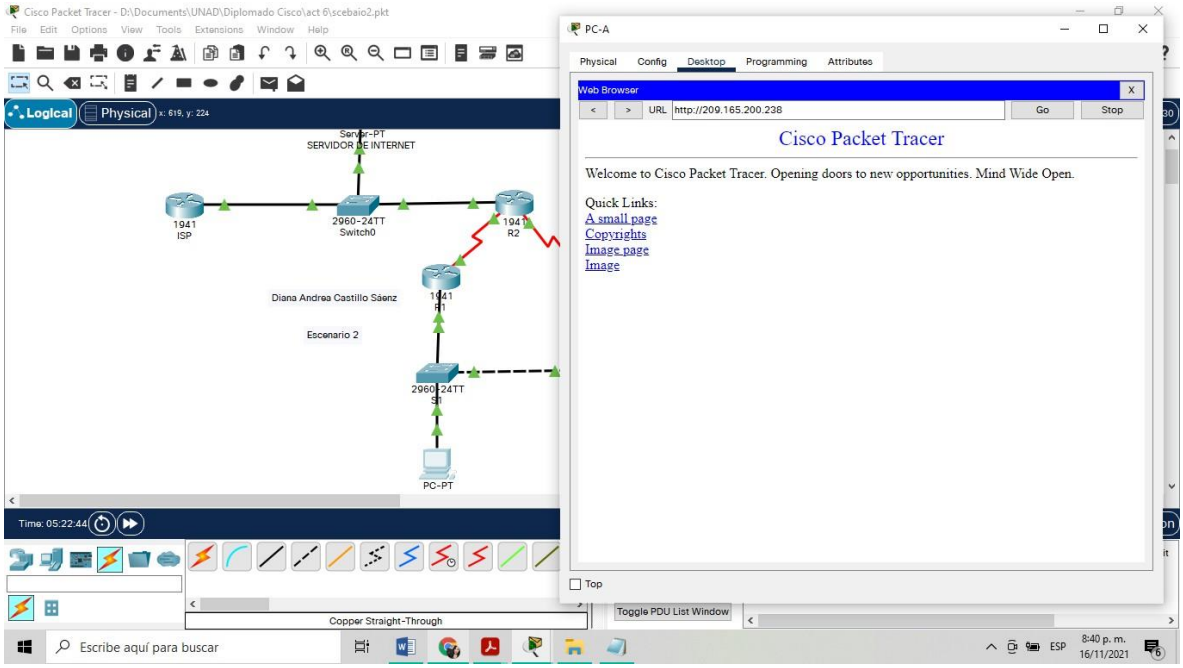


Fuente: Autor

- Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.238) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345

Se ingresa a la PC-A desde web browser y se verifica acceso al servidor web 209.165.200.238 se anexa imagen de confirmación:

Figura 28. Acceder al servidor web desde un navegador del pc.



Fuente: Autor

2.6. Configurar NTP

- Ajuste la fecha y hora en R2: 5 de marzo de 2016, 9 a. m.
- Configure R2 como un maestro NTP: Nivel de estrato: 5
- Configurar R1 como un cliente NTP: Servidor: R2
- Configure R1 para actualizaciones de calendario periódicas con hora NTP.
- Verifique la configuración de NTP en R1.

A continuación se anexa el código de configuración de la NTP en R2:

```
R2#clock set 09:00:00 05 march 2016          Se realiza ajuste de la hora en el R2
5 de marzo de 2016, 9 a. m
R2#configure terminal                        Se ingresa a la configuración del
terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5                      Se configura R2 como un maestro
NTP nivel 5
```

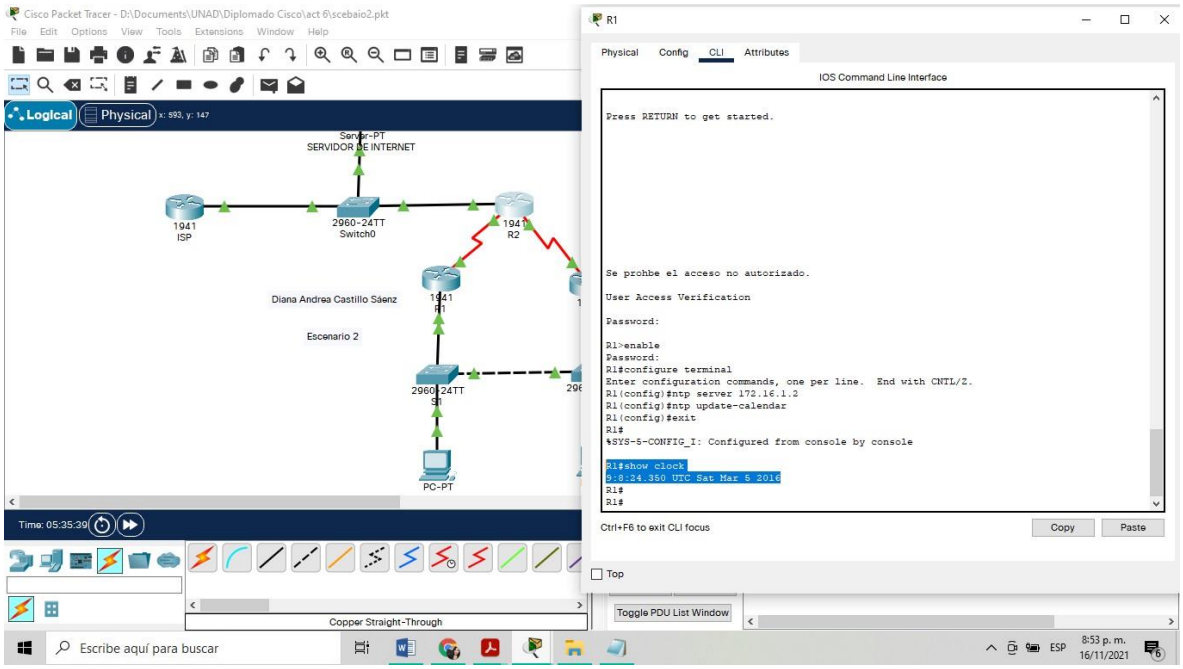
A continuación se anexa el código de configuración en R1 como cliente:

```
R1(config)#ntp server 172.16.1.2          Se configura R1 como cliente NTP de Servidor R2
R1(config)#ntp update-calendar            Se configuran actualizaciones periódicas con hora NTP
R1(config)#exit                           Se sale de la configuración del terminal
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Se realiza verificación de configuración de NTP en R1

```
R1#show clock                             Se verifica la hora desde R1
9:8:24.350 UTC Sat Mar 5 2016
```

Figura 29. Verificación de NTP en R1



Fuente: Autor

2.7. Configurar y verificar las listas de control de acceso (ACL)

2.7.1. Restringir el acceso a las líneas VTY en el R2

- Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2: Nombre de la ACL: ADMIN-MGT
- Aplicar la ACL con nombre a las líneas VTY
- Permitir acceso por Telnet a las líneas de VTY
- Verificar que la ACL funcione como se espera

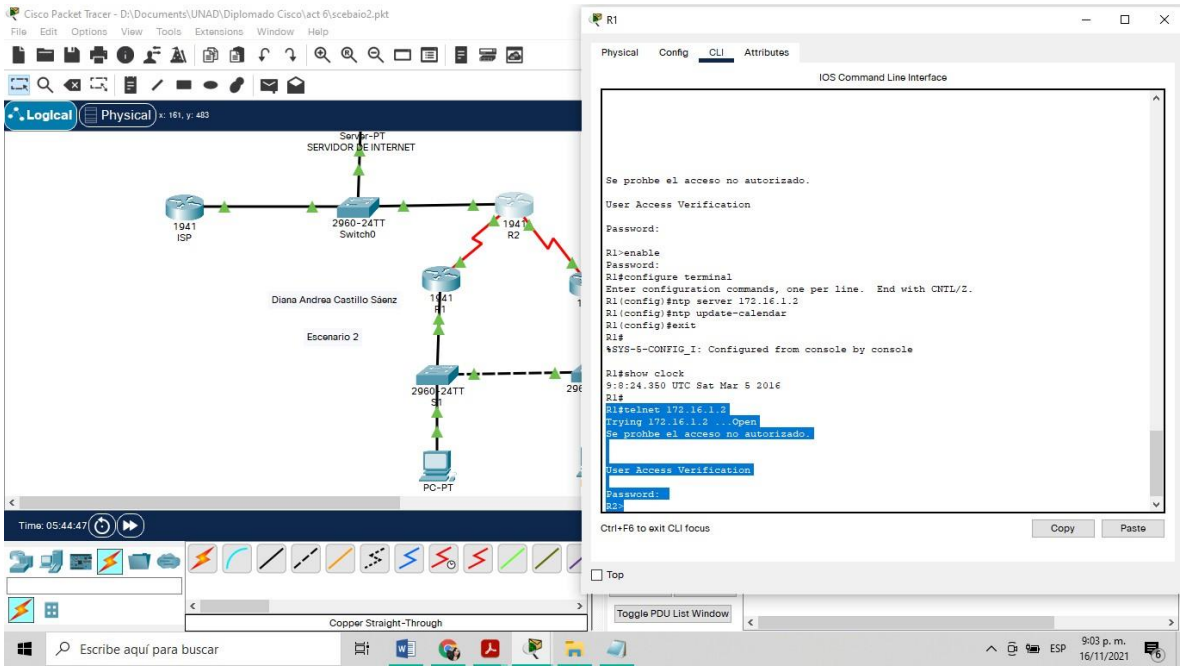
A continuación se anexa el código de configuración de restricción al acceso a las líneas VTY en el R2:

```
R2(config)#ip access-list standard ADMIN-MGT Se da nombre a la ACL como ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1     Se permite acceso a 172.16.1.1
R2(config-std-nacl)#deny any                   Se niega acceso a otros
R2(config-std-nacl)#!
R2(config-std-nacl)#exit                       Se sale de la configuración ACL
R2(config)#line vty 0 4                        Se ingresa a la línea VTY 0 4 del R2
R2(config-line)#ip access-class ADMIN-MGT in Se aplica ACL con nombre a las lineas VTY
R2(config-line)#transport input telnet Se permite acceso por Telnet a las lineas VTY
```

Se realiza verificación:

```
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...Open
Se prohbe el acceso no autorizado.


User Access Verification

Password:
R2>
```

Figura 30. Verificación de ingreso a R2 a través de R1.



Fuente: Autor

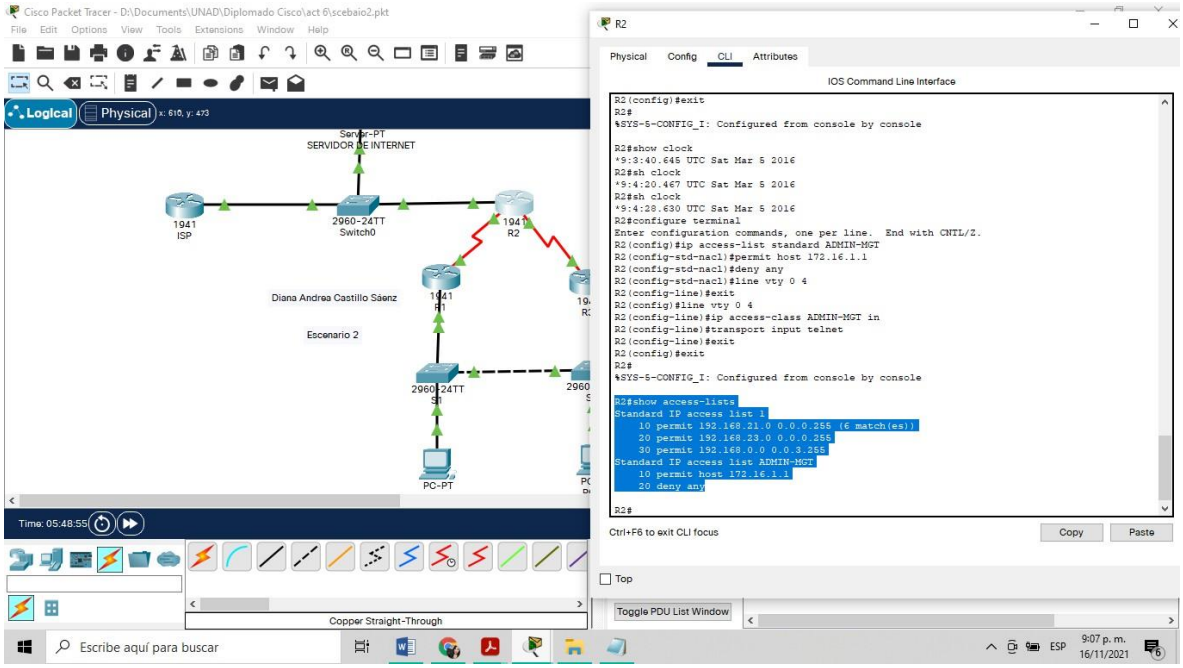
2.7.2. Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

- Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

Se utiliza el comando show access lists para mostrar las coincidencias recibidas por lista de acceso

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255 (6 match(es))
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.0.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
    20 deny any
```

Figura 31. Show access-lists



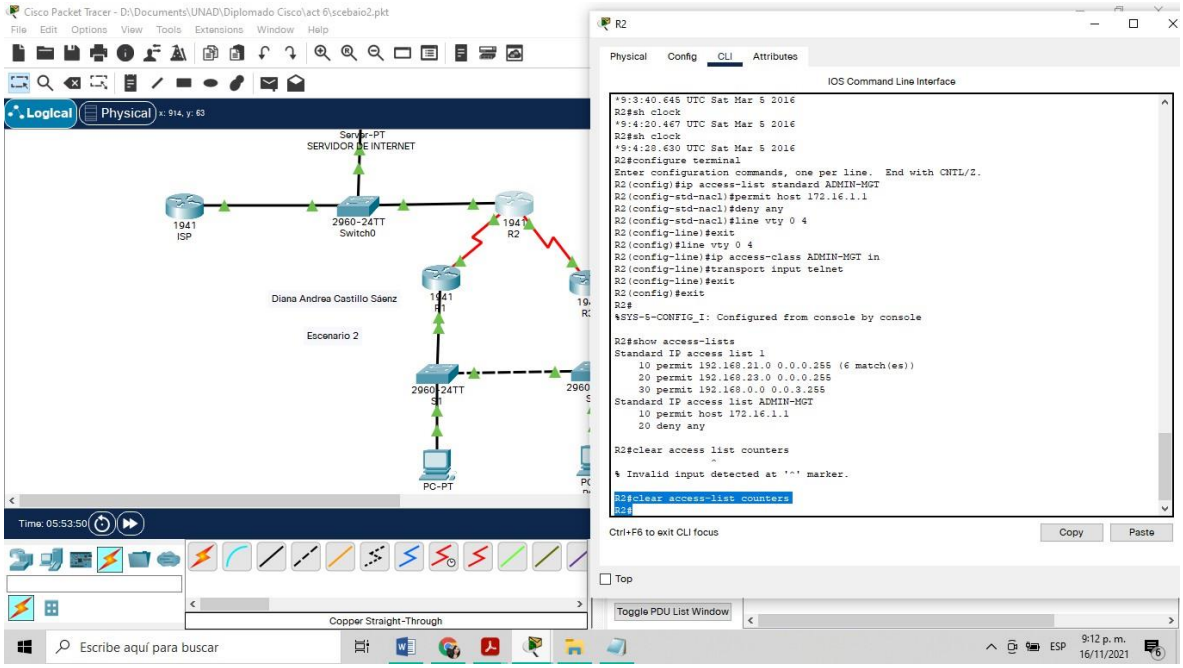
Fuente: Autor

- Restablecer los contadores de una lista de acceso

El comando para restablecer los contadores es clear access-list counters

```
R2#clear access-list counters
R2#
```

Figura 32. Restablecer los contadores de una lista de acceso



Fuente: Autor

- ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

Se utiliza el comando show run para mostrar ACL se aplica en las interfaces

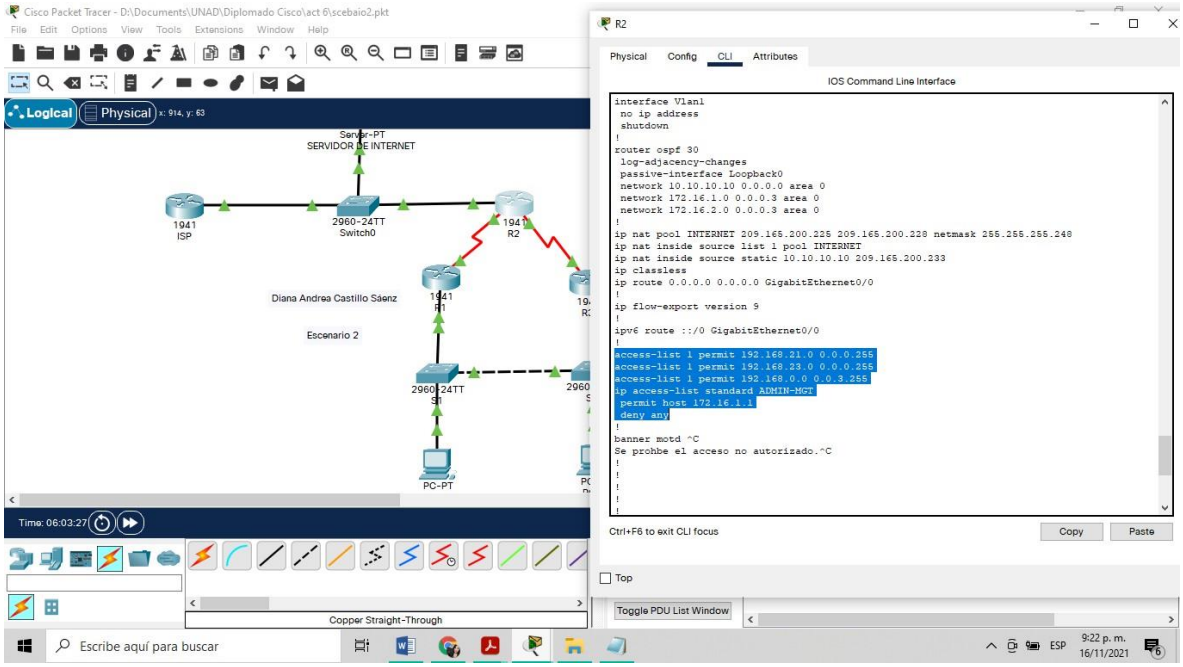
```
R2#show run
Building configuration...

Current configuration : 2141 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R2
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

```
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
username webuser privilege 15 password 7 0822455D0A165445415F59
!
!
license udi pid CISCO1941/K9 sn FTX1524WKC8-
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
interface Loopback0
 description servidor WEB
 ip address 10.10.10.10 255.255.255.255
 ip nat inside
!
interface GigabitEthernet0/0
 description interface hacia Internet
 ip address 209.165.200.233 255.255.255.248
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 description interface hacia el R1
 ip address 172.16.1.2 255.255.255.252
 ip nat inside
```

```
 ipv6 address 2001:DB8:ACAD:1::2/64
!
interface Serial0/0/1
 description interface hacia el R3
 ip address 172.16.2.1 255.255.255.252
 ip nat inside
 ipv6 address 2001:DB8:ACAD:2::2/64
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 30
 log-adjacency-changes
 passive-interface Loopback0
 network 10.10.10.10 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
!
ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.233
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0
!
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.0.0 0.0.3.255
ip access-list standard ADMIN-MGT
 permit host 172.16.1.1
 deny any
!
banner motd ^C
Se prohbe el acceso no autorizado.^C
!
!
!
!
```

```
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!
line vty 0 4
 ipv6 access-class ADMIN-MGT in
 password 7 0822455D0A16
 login
 transport input telnet
!
!
ntp server 172.16.1.2
ntp master 5
ntp update-calendar
!
End
```

Figura 33. Show run para ver access list.



Fuente: Autor

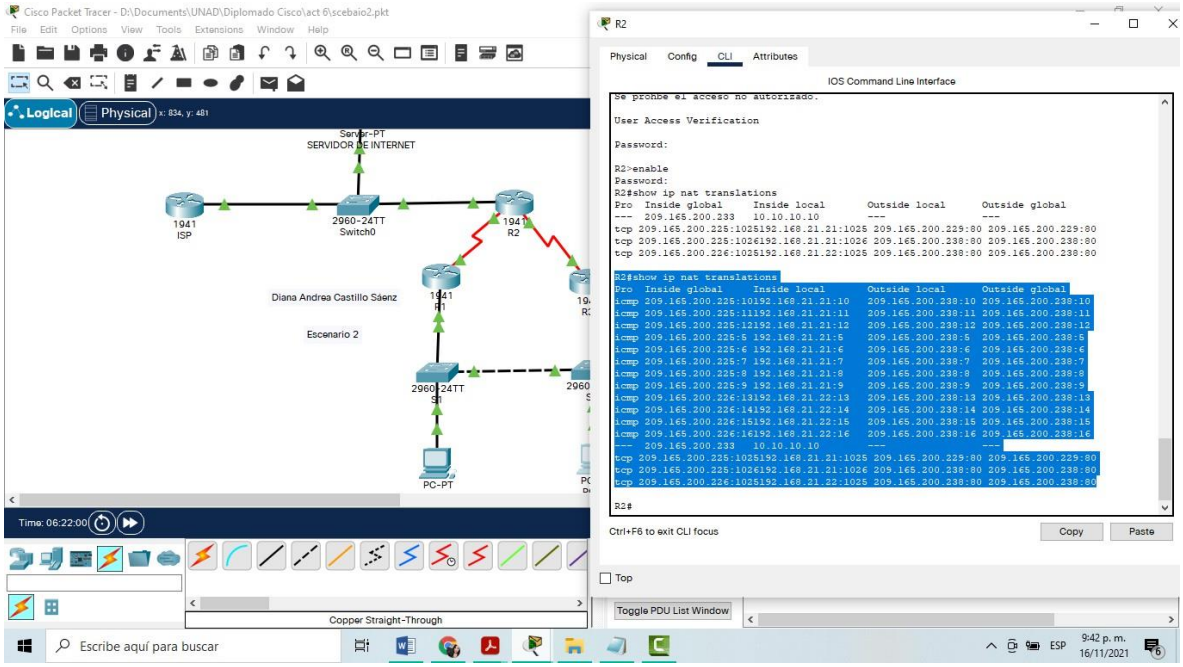
- ¿Con qué comando se muestran las traducciones NAT?: Nota: Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.

El comando que se utiliza es el show ip nat translations, se tiene en cuenta que se debe hacer con anticipación ping desde la computadora de internet a la PC-A y la PC-C.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
icmp   209.165.200.225:10192.168.21.21:10        209.165.200.238:10
209.165.200.238:10
icmp   209.165.200.225:11192.168.21.21:11        209.165.200.238:11
209.165.200.238:11
icmp   209.165.200.225:12192.168.21.21:12        209.165.200.238:12
209.165.200.238:12
icmp   209.165.200.225:5   192.168.21.21:5         209.165.200.238:5
209.165.200.238:5
icmp   209.165.200.225:6   192.168.21.21:6         209.165.200.238:6
209.165.200.238:6
icmp   209.165.200.225:7   192.168.21.21:7         209.165.200.238:7
209.165.200.238:7
icmp   209.165.200.225:8   192.168.21.21:8         209.165.200.238:8
209.165.200.238:8
icmp   209.165.200.225:9   192.168.21.21:9         209.165.200.238:9
209.165.200.238:9
icmp   209.165.200.226:13192.168.21.22:13        209.165.200.238:13
209.165.200.238:13
icmp   209.165.200.226:14192.168.21.22:14        209.165.200.238:14
209.165.200.238:14
icmp   209.165.200.226:15192.168.21.22:15        209.165.200.238:15
209.165.200.238:15
icmp   209.165.200.226:16192.168.21.22:16        209.165.200.238:16
209.165.200.238:16
---  209.165.200.233   10.10.10.10        ---                ---
tcp    209.165.200.225:1025192.168.21.21:1025    209.165.200.229:80
209.165.200.229:80
```

```
tcp    209.165.200.225:1026192.168.21.21:1026    209.165.200.238:80
209.165.200.238:80
tcp    209.165.200.226:1025192.168.21.22:1025    209.165.200.238:80
209.165.200.238:80
```

Figura 34. Show ip nat translations



Fuente: Autor

- ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?

El comando que se utiliza es el clear ip nat translation

CONCLUSIONES

Al realizar SSH en la configuración de los dispositivos como routers y switches se evita que personas extrañas ingresen y tengan acceso al dispositivo sin autorización a través de un servidor remoto, puesto que este protocolo proporciona un mecanismo para autenticar un usuario remoto y garantizar que las comunicaciones hacia y desde el servidor remoto se den de manera encriptada.

Emplear el protocolo DHCP en la red ayuda al manejo interno de información permitiendo el uso correcto y controlado de la misma, este protocolo es de fácil configuración puesto que permite asignar direcciones IP de forma automática, además de mejorar el rendimiento y estabilidad de las conexiones.

Gracias a manejo de listas de acceso se puede limitar el tráfico de red mejorando así el rendimiento de la misma puesto que se detiene el tráfico o se permite solamente el tráfico especifico en la red; además proporciona un nivel de seguridad para el acceso a la red y se controlan las áreas de red a las que puede acceder el cliente.

Al utilizar el protocolo de enrutamiento OSPF se puede dividir el sistema en áreas y mantenerlas separadas para disminuir el tráfico de direccionamiento de OSPF, además al emplear este protocolo no hay limitaciones para el conteo de saltos, permitiendo un mejor balance de carga ya que éste protocolo es capaz de detectar cambios en la topología dentro de un sistema autónomo.

La importancia de utilizar NAT en la red es bastante puesto que proporciona seguridad ya que los dispositivos conectados mediante este protocolo no serán visibles desde el exterior, por lo cual cualquier atacante externo no puede averiguar si el dispositivo está conectado o no a la red ya que oculta todo el espacio de direcciones privadas detrás de una sola dirección IP, además NAT genera un ahorro de direcciones IPv4.

Gracias al manejo de estos protocolos y diferentes configuraciones en los routers y switches se obtiene un buen grado de seguridad en la información evitando ataques de extraños a la red, además de proporcionar eficacia y confiabilidad al estar conectado en la red.

BIBLIOGRAFÍA

ARIGANELLO, Ernesto. Redes Cisco. Guía de estudio para la certificación CCNA routing y Switching. 4° edición. Grupo editorial RA-MA, 2016.

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

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

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

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

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

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

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

CISCO. (2019). Ethernet. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. (2019). Capa de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

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

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

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

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

CISCO. (2019). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11

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

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

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

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

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