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

ANDRES FELIPE RENDON RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

INGENIERÍA DE SISTEMAS

VILLAVICENCIO

2021

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

ANDRES FELIPE RENDON RODRIGUEZ

DIPLOMADO DE OPCIÓN DE GRADO PRESENTADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

MAG. MARIA ALEJANDRA LOPEZ
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

INGENIERÍA DE SISTEMAS

VILLAVICENCIO

2021

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO.

_____

FIRMA DEL JURADO.

_____

FIRMA DEL JURADO.

Villavicencio, octubre 2021

AGRADECIMIENTOS

Este espacio se lo quiero dedicar a mi familia, a la cual le estoy infinitamente agradecido por todo el apoyo brindado, han sido el motor en mi vida, su incondicional apoyo me ha llevado ir alcanzando cada una de mis metas e ir trabajando por ponerme nuevas y luchar por alcanzarlas.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

GLOSARIO

DHCP: El protocolo de configuración dinámica de hosts, es un protocolo red que permite asignar la configuración de la interfaz de red a los hosts conectados a la red local mediante un router o servidor, la información asignada a esta configuración incluye dirección IP, gateway, mascara de red y dns a utilizar.

IP Privada: Son las direcciones visibles únicamente en la red local, estas redes están conectadas por routers que permiten que los hosts de la red local puedan tener acceso a internet usando una IP Publica.

NAT: Este método se encarga de dar acceso a internet a todo un grupo de ordenadores de una misma red local, usando una única dirección IP conocida como IP Publica.

OSPF: Este es un protocolo de direccionamiento del tipo enlace-estado, basado en el algoritmo de la primera vía más corta. En las redes OSPF los enrutadores y conmutadores mantienen una base de datos de enlace – estado idéntica, estas bases de datos son generadas a partir de los anuncios enlace – estado que reciben estos dispositivos desde los otros presentes en la red.

Router: En telecomunicaciones y redes se le llama router o enrutador al dispositivo que permite la comunicación entre redes, el router se encarga de controlar el flujo de datos, transportando los datos que vienen desde el exterior (Internet) hasta los ordenadores o demás hosts que los hayan solicitado, también funcionan como gateway para lograr establecer conexión de los equipos en la red local con la red externa más conocida como internet.

SSH: Es un protocolo por el cual podemos acceder a dispositivos remotos dentro de la red de una manera segura, SSH maneja la encriptación de credenciales de acceso a estos dispositivos.

Switch: Se trata de un dispositivo de red compuesto por puertos, el cual es capaz de decidir a cuál puerto enviar cada paquete recibido desde el exterior, esto ayuda a no sobrecargar el cable con información que más tarde será descargada por los ordenadores y demás hosts de la red local.

TELNET: Se trata de un protocolo de telecomunicación que nos permite acceder a dispositivos remotos a través de red, a diferencia de SSH, TELNET no maneja un servicio de encriptación de credenciales, lo cual lo hace bastante vulnerable.

VLAN: Una VLAN es la agrupación lógica de hosts de varias redes LAN que permite que estos se comuniquen e interactúen como si estuviesen en una sola.

RESUMEN

El presente trabajo describe los pasos a seguir para la configuración de dispositivos como routers y switches, también muestra las buenas prácticas en cuanto a la seguridad a implementar en estos dispositivos, a su vez muestran los pasos a seguir para implementar direccionamiento IPv6, routing dinámico OSPF, DHCP y NAT.

Palabras clave: CISCO, IPv4, Router, Switch, IPv6, OSPF, DHCP, NAT, Vlans.

ABSTRACT

This document describes the steps to follow for the configuration of devices such as routers and switches, and also shows the best practices in terms of security to be implemented in these devices, in addition shows the steps to implement IPv6 addressing, OSPF dynamic routing, DHCP and NAT.

KEYWORDS: CISCO, IPv4, Router, Switch, IPv6, OSPF, DHCP, NAT, Vlans.

INTRODUCCION

El presente trabajo es realizado con fines de la obtención del título de ingeniero de sistemas de la universidad nacional abierta y a distancia, para cumplir este fin en este escrito se desarrollarán dos escenarios prácticos que buscarán plasmar todo el conocimiento adquirido durante el desarrollo del seminario de profundización, en el primero de ellos se abordarán temas relacionados a la configuración inicial de routers y switches así como la implementación de buenas prácticas de seguridad tales como: Cifrado de contraseñas, habilitación de acceso únicamente por ssh y configurar el inicio de sesión en las líneas VTY para que use la base de datos local. En el segundo escenario se tocarán temáticas sobre direccionamiento IPv6, routing entre vlans, routing dinámico OSPF, DHCP, NAT y las listas de control de acceso ACL.

DESARROLLO

ESCENARIO 1

Topología:

Ilustración 1 - topología correspondiente al escenario 1

Fuente: Elaboración propia

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

Objetivos

Parte 1: Construir en el simulador la Red

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

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

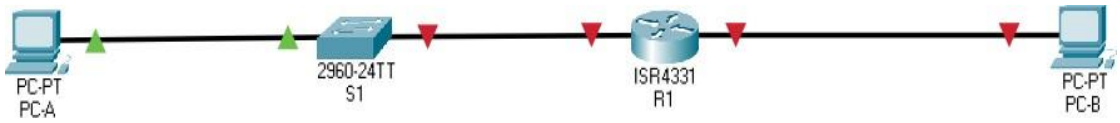
Parte 4: Configurar los ajustes básicos de seguridad en el R1 y S1

Parte 5: Configurar los hosts y verificar la conectividad entre los equipos

Parte 1: Construya la Red

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

Ilustración 2 - Topología del escenario 1 realizada en Packet Tracer.



Fuente: Elaboración propia

Parte 2: Desarrolle el esquema de direccionamiento IP

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

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

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

Se procede a calcular las subredes correspondientes según el número de hosts solicitados para cada una.

Red Original 192.168.72.0/24

1. Identificamos la red con mayor número de hosts solicitados: Lan 1 (100)
2. Identificamos la máscara de red de la red original:

Ilustración 3 - Mascara de red de la red 192.168.72.0/24 –

Decimal:	255.								255.								255.								0							
Binario:	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	0

Fuente: Elaboración propia

3. Con ayuda de la formula $2^n >= hosts$ buscamos el exponente que mas se acomode a los hosts solicitados, dicho exponente lo usaremos para hallar la nueva mascara de la subred correspondiente a la Lan 1.

Ilustración 4 - Tabla de la función 2^n

n	8	7	6	5	4	3	2	1
2^n	256	128	64	32	16	8	4	2

Fuente: Elaboración propia

$$2^n \geq 100$$
$$2^7 = 128\,;2^7 \geq 100$$

4. Ahora con el exponente sacaremos la nueva mascará de red que tendrá la primera subred LAN 1, nos indica que dejemos apagados los últimos 7 bits.

Ilustración 5 - Mascara de red para la nueva subred Lan 1.

Decimal	255								255								255								128							
Binario	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

Fuente: Elaboración propia.

Entonces la subred para la Lan 1, será la 192.168.72.0/25 con mascará de red 255.255.255.128.

5. Cálculo del salto de red, para identificar donde empezara la siguiente subred se debe calcular el salto de red, restando a 256 el valor del último octeto de la nueva mascara de red.

256 – 128 = 128

Por lo tanto la próxima subred comenzara en 192.168.72.128

6. Teniendo en cuenta la máscara de red de la red original, se calcula el exponente nos permitirá satisfacer los hosts solicitados para la siguiente subred con más hosts solicitados, en este caso es la Lan 2 (50)

$$2^n \geq 50$$
$$2^6 = 64\,;2^7 \geq 50$$

7. Ahora con el exponente sacaremos la nueva mascará de red que tendrá la primera subred LAN 1, nos indica que dejemos apagados los últimos 6 bits.

Ilustración 6 -– Mascara de red para la nueva subred Lan 2.

Decimal	255								255								255								192							
Binario	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

Fuente: Elaboración propia.

Entonces para la subred Lan 2 la máscara de red será 255.255.255.192 con la dirección 192.168.72.128/26.

8. Calculamos el salto de red, para identificar donde comenzaría una hipotética siguiente red, de esta forma podremos obtener el broadcast de nuestra subred actual.

   256 – 192 = 64

   128 + 64 = 192

   Por lo tanto el salto de red seria de 64, y la nueva subred empezaría en 192.168.72.192, dándonos como broadcast de nuestra subred actual: 192.168.72.191

Tabla 2 Tabla de direccionamiento de las subredes creadas.

	Direccion de red	Mascara de subred	Primera direcccion de hosts	Ultima dirección de hosts	Broadcast
0	192.168.72.0	255.255.255.128	192.168.72.1	192.168.72.126	192.168.72.127
1	192.168.72.128	255.255.255.192	192.168.72.129	192.168.72.190	192.168.72.191

Fuente: Elaboración propia

Parte 3: Configure aspectos básicos

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

Paso 1: configurar los ajustes básicos

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 – Requerimientos de configuración en R1.

Tarea	**Especificación**
Desactivar la búsqueda DNS	Los comandos se detallarán más adelante.
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	Los comandos se detallarán más adelante.
Configurar VTY solo aceptando SSH	Los comandos se detallarán más adelante.
Cifrar las contraseñas de texto no cifrado	Los comandos se detallarán más adelante.
Configure un MOTD Banner	Los comandos se detallarán más adelante.
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz.
Generar una clave de cifrado RSA	Módulo de 1024 bits

Fuente: Prueba de habilidades Cisco CCNA II

Ejecución de tareas en R1:
Desactivar la búsqueda DNS:

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

Router(config)#exit

Router#

%SYS-5-CONFIG_I: Configured from console by console

Desactivamos las búsquedas DNS, habilitando en primer lugar el modo exec privilegiado, entramos a la configuración del terminal y posteriormente desactivamos las búsquedas dns con ***ip domain-lookup.***

Nombre del router:

```
Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console
```

Cambiamos el nombre del host, habilitando en primer lugar el modo exec privilegiado, entramos a la configuración del terminal y posteriormente cambiamos el hostname con el comando ***hostname R1***, donde R1 será el nombre que llevará el router de aquí en adelante.

Nombre de dominio:

```
R1>en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip domain n

R1(config)#ip domain name ccna-lab.com

R1(config)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console
```

Para configurar el nombre del dominio en el router, debemos ingresar al Exec privilegiado, posteriormente ingresamos a la configuración de terminal, y con el comando ***ip domain name ccna-lab.com*** configuramos el nombre del dominio en el router.

Contraseña cifrada para el modo EXEC privilegiado:

```
R1>en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#enable secret ciscoenpass

R1(config)#exit

R1#

%SYS-5-CONFIG_I: Configured from console by console
```

Para configurar la contraseña de exec privilegiado, habilitamos el modo exec privilegiado, posteriormente accedemos al apartado de configuración del terminal y habilitamos la contraseña de exec privilegiado, para ello ejecutamos ***enable secret*** seguido de la contraseña a asignar.

Contraseña de acceso a la consola:

```
R1>en

Password:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#line con 0

R1(config-line)#password ciscoconpass

R1(config-line)#login

R1(config-line)#exit
```

Se procede a configurar una contraseña de consola en el R1, para ello accedemos al modo exec privilegiado, posteriormente ingresamos al modo configurar terminal, para después ingresar al modo de configuración de línea de consola con el comando: ***line con 0,*** en este modo configuramos la contraseña a usar para acceder en posteriores ocasiones a la consola del Router, esto se logra con el comando password seguido de la contraseña a configurar. ***password ciscoconpass*** en este caso se usó esta contraseña.

Establecer la longitud mínima para las contraseñas:

```
R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#sec

R1(config)#security pass

R1(config)#security passwords min

R1(config)#security passwords min-length 10

R1(config)#
```

Para establecer la longitud mínima de una contraseña, debemos primero acceder al modo configuración de terminal, para ello previamente debemos acceder al modo exec privilegiado, una vez en el modo configuración de terminal se ejecuta el

comando ***security passwords min-length 10***, donde la parte numérica serán los caracteres mínimos que deberá tener la contraseña.

Crear un usuario administrativo en la base de datos local:

R1>en

Password:

Password:

R1#config t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#username admin password admin1pass

R1(config)#

Creamos un usuario en la base de datos local del router, ya que esta es una buena práctica recomendada ya que con esto se asegura que solo estos usuarios listados en la base de datos local sean los únicos que puedan acceder a la configuración del router.

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

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#line vty 0 4

R1(config-line)#login local

R1(config-line)#exit

Se configura el inicio de sesión en las líneas VTY para que use la base de datos local, accediendo al modo configuración del dispositivo, después ingresando a la línea vty y habilitando dicho uso de la base de datos local con el comando ***login local.***

Configurar VTY solo aceptando SSH:

R1#en

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#line vty 0 4

R1(config-line)#transport in

R1(config-line)#transport input ss

R1(config-line)#transport input ssh

Se configura la línea VTY para que solo acepte ssh con el comando ***transport input ssh***, con esto logramos implementar una buena práctica para solo conectamos por

medio de ssh, lo cual nos da mejor seguridad gracias al cifrado que este ofrece a las credenciales que se envían por este medio.

Cifrar las contraseñas de texto no cifrado:

R1>en

Password:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#service pass

R1(config)#service password-encryption

Se configura el cifrado de las contraseñas de texto no cifrado alojadas en el router, esta buena práctica ayuda a potenciar aún más la seguridad en el dispositivo, con esta práctica, nos aseguramos de que las contraseñas no puedan ser visualizadas de forma textual al ejecutar comandos como: ***show running-config*** o ***show startup-config***.

Configure un MOTD Banner:

R1>en

Password:

Password:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#banner mo

R1(config)#banner motd " ... Solo acceso de personal autorizado ..."

R1(config)#

Se configura el banner para advertir al personal que trata de ingresar a la configuración del dispositivo que solo lo pueden hacer personal previamente autorizado, para ello ingresamos al modo configuración del terminal con configure terminal, después ingresamos el comando banner motd y escribimos el mensaje a mostrar entre comillas***: R1(config)#banner motd " ... Solo acceso de personal autorizado ..."***

Configurar interfaz G0/0/0:

... Solo acceso de personal autorizado ...

User Access Verification

Password:

R1>en

Password:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#interface g0/0/0

R1(config-if)#ip add

R1(config-if)#ip address 192.168.72.129 255.255.255.192

R1(config-if)#no shutdown

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)#desc

R1(config-if)#description Primera direccin de host de la subred LAN2 Direccion ip - 192.168.72.129

R1(config-if)#exit

Se configura la interfaz G0/0/0 del R1, asignándole dirección ip, descripción y activando la interfaz, para ello se accede al modo exec privilegiado después de hacer la verificación del usuario ***R1>en***, posteriormente se accede al modo de configuración de terminal ***R1#conf t***, ingresamos al modo de configuración de interfaz en este caso la interfaz G0/0/0 ***R1(config)#interface g0/0/0***, asignamos ip address y activamos la interfaz ***R1(config-if)#ip address 192.168.72.129 255.255.255.128, R1(config-if)#no shutdown***. Por último asignamos la descripción a la interfaz: ***R1(config-if)#description Primera dirección de host de la subred LAN2 Direccion ip - 192.168.72.129.***

Configurar interfaz G0/0/1

R1(config)#interface g0/0/1

R1(config-if)#ip address 192.168.72.1 255.255.255.128

R1(config-if)#no shutdown

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)#des

R1(config-if)#description Primera direccion de host de la subred LAN1 Direccion ip - 192.168.72.1

R1(config-if)#exit

Al igual que en el paso anterior, se accede al modo de configuración de interfaz en este caso la G0/0/1, asignamos una dirección ip con su respectiva mascara de red, se activa la interfaz y se agrega la descripción de la misma.

Generar una clave de cifrado RSA:

R1>en

Password:

Password:

R1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#crypto key generate rsa general-keys modulus 1024

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

% The key modulus size is 1024 bits

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

**Mar 1 0:2:45.267: %SSH-5-ENABLED: SSH 1.99 has been enabled*

Se genera un cifrado para encriptar los datos, en este caso se usa un módulo de 1024 bits, recordando que este comando acepta módulos desde 360 a 2048 bits, siendo 1024 lo mínimo recomendado.

Las tareas de configuración de S1 incluyen lo siguiente:

Tabla 4 – Requerimientos en S1.

Tarea	**Especificación**
Desactivar la búsqueda DNS.	Los comandos usados se detallarán más adelante.
Nombre del switch	**S1**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**

Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Los comandos usados se detallarán más adelante.
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	Los comandos usados se detallarán más adelante.
Cifrar las contraseñas de texto no cifrado	Los comandos usados se detallarán más adelante.
Configurar un MOTD Banner	Los comandos usados se detallarán más adelante.
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.

Fuente: Pruebas de habilidad Cisco CCNA II

Ejecución de tareas en S1:

Desactivar la búsqueda DNS:

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

Se configura la desactivación de búsquedas dns ingresando al modo exec privilegiado, posteriormente se ingresa al modo de configuración global de terminal y allí se usa el comando ***Switch(config)#no ip domain-lookup*** para desactivar las búsquedas dns.

Nombre del switch:

```
Switch>en
Switch#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname S1

S1(config)#
```

Se le da nombre al Switch ingresando al modo exec privilegiado, posteriormente ingresamos al modo de configuración global, después cambiamos el nombre con el siguiente comando:***Switch(config)#hostname S1***

Nombre de dominio:

```
S1>en

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#ip domain

S1(config)#ip domain name ccna-lab.com
```

Se configura el nombre del dominio, ingresando al modo exec privilegiado, posteriormente en el modo de configuración global, ingresamos el comando: ***S1(config)#ip domain name ccna-lab.com*** para asignarle un nombre al dominio.

Contraseña cifrada para el modo EXEC privilegiado:

```
S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#enable secret ciscoenpass

S1(config)#end

S1#

%SYS-5-CONFIG_I: Configured from console by console
```

Para configurar la contraseña de exec privilegiado, habilitamos el modo exec privilegiado, posteriormente accedemos al apartado de configuración del terminal y habilitamos la contraseña de exec privilegiado, para ello ejecutamos **S1(config)#enable secret ciscoenpass.**

Contraseña de acceso a la consola:

```
S1>en

Password:

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#line con 0

S1(config-line)#password ciscoconpass
```

Se configura una contraseña de acceso a consola, ingresando al modo exec privilegiado, posteriormente ingresamos al modo de configuración global, una vez

dentro del modo de configuración global, ingresamos al modo de configuración de línea de consola con el siguiente comando: ***S1(config)#line con 0,*** alli se configura la contraseña de consola con este comando: ***S1(config-line)#password ciscoconpass.***

Crear un usuario administrativo en la base de datos local:

```
S1>en

Password:

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

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

Creamos un usuario en la base de datos local del switch, ya que esta es una buena práctica recomendada ya que con esto se asegura que solo estos usuarios listados en la base de datos local sean los únicos que puedan acceder a la configuración del switch.

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

```
S1>en

Password:

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#line vty 0 4

S1(config-line)#login local

S1(config-line)#exit
```

Se configura el inicio de sesión en las líneas VTY por medio de la base de datos local, ingresando al modo exec privilegiado, después se accede al modo de configuración global, posteriormente se accede al modo de configuración de líneas VTY usando el siguiente comando: ***S1(config)#line vty 0 4*** y por último se configura el inicio de sesión con la base de datos local: ***S1(config-line)#login local***

Configurar un MOTD Banner:

```
S1>en

Password:

Password:

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#banner

S1(config)#banner m
```

```
S1(config)#banner motd ″... Solo personal autorizado ...″
```

Se realiza la configuración del banner para advertir al personal que trata de ingresar a la configuración del dispositivo que solo lo pueden hacer personal previamente autorizado, en primer lugar ingresamos al modo exec privilegiado el cual es el que usamos para acceder posteriormente al modo de configuración global de configuración de terminal, una vez en este modo se procede a crear el banner con el siguiente comando***: S1(config)#banner motd " ... Solo personal autorizado ..."***

Generar una clave de cifrado RSA

```
S1(config)#cryp

S1(config)#crypto key generate rsa ge

S1(config)#crypto key generate rsa general-keys mo

S1(config)#crypto key generate rsa general-keys modulus 1024

The name for the keys will be: S1.ccna-lab.com

% The key modulus size is 1024 bits

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

*Mar 1 0:7:39.538: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Se genera un cifrado para encriptar los datos, en este caso se usa un módulo de 1024 bits, recordando que este comando acepta módulos desde 360 a 2048 bits, siendo 1024 lo mínimo recomendado

Configurar la interfaz de administración (SVI):

```
... Solo personal autorizado ...


S1>en

Password:

S1#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#interface vlan1

S1(config-if)#ip address 192.168.72.2 255.255.255.128

S1(config-if)#no shutdown


S1(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on interface Vlan1, changed state to up
```

Configuramos la Interfaz virtual del switch (SVI) ingresando al modo exec privilegiado, luego al modo global de configuración de terminal, allí ingresaremos a la interfaz vlan1 la cual es la interfaz predeterminada para usar como SVI, a esta interfaz ingresamos usando este comando: ***S1(config)#interface vlan1*** por último se le asigna la configuración ip a la interfaz con este comando: ***S1(config-if)#ip address 192.168.72.2 255.255.255.128.***

Configuración del gateway predeterminado:

```
... Solo personal autorizado ...


S1>en
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip default-gateway 192.168.72.1
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Se configura el gateway predeterminado en el switch, el primer paso es ingresar al modo exec privilegiado, después se debe acceder al modo de configuración global de terminal, para finalizar se asigna la ip gateway predeterminada con el siguiente comando: ***S1(config)#ip default-gateway 192.168.72.1***

Paso 2. Configurar los equipos

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

Tabla 5 – Registro de la configuración en PC-A

PC-A Network Configuration	
Descripción	PC-A
Dirección física	*0030.A367.53E3*
Dirección IP	*192.168.72.126*
Máscara de subred	*255.255.255.128*

Gateway predeterminado	*192.168.72.1*

Fuente: Elaboración propia.

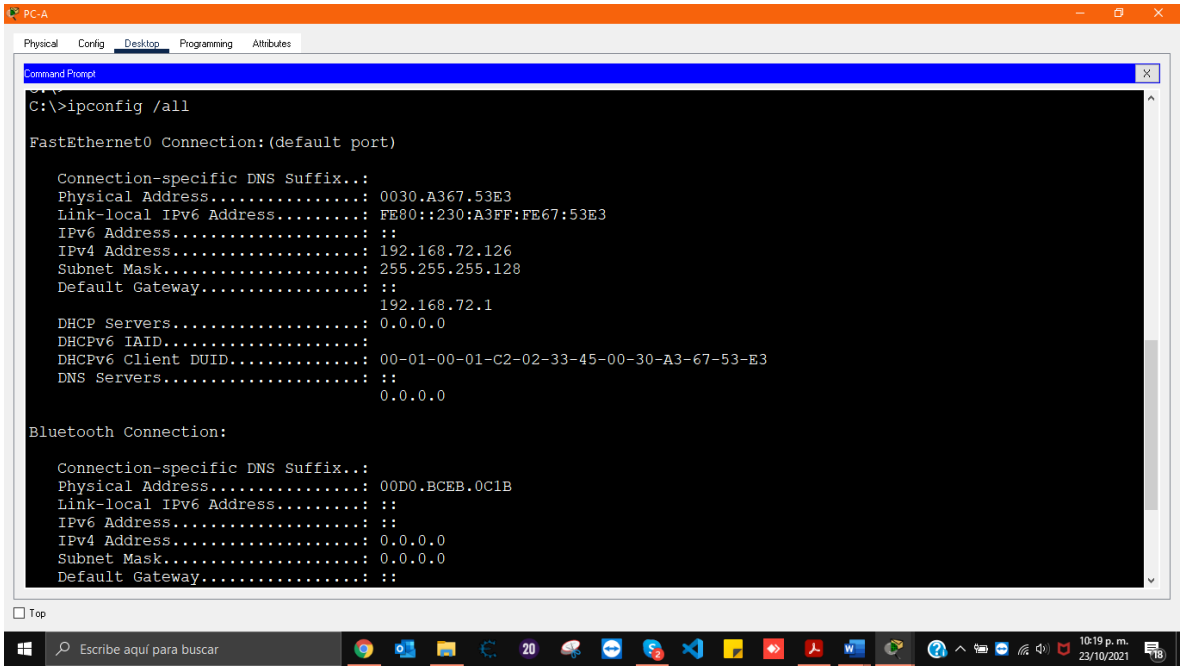
Configuración del PC-A

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.....: 0030.A367.53E3
   Link-local IPv6 Address.....: FE80::230:A3FF:FE67:53E3
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.72.126
   Subnet Mask.....: 255.255.255.128
   Default Gateway.....: ::
                                  192.168.72.1
   DHCP Servers.....: 0.0.0.0
   DHCPv6 IAID.....:
   DHCPv6 Client DUID.....: 00-01-00-01-C2-02-33-45-00-30-A3-67-53-E3
   DNS Servers.....: ::
                                  0.0.0.0


Bluetooth Connection:


   Connection-specific DNS Suffix..:
   Physical Address.....: 00D0.BCEB.0C1B
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                  0.0.0.0
   DHCP Servers.....: 0.0.0.0
   DHCPv6 IAID.....:
   DHCPv6 Client DUID.....: 00-01-00-01-C2-02-33-45-00-30-A3-67-53-E3
```

DNS Servers. . . . . : ::

0.0.0.0

Ilustración 7- Información de la configuración de red en el equipo PC-A obtenida mediante Ipconfig/all



Fuente: Elaboración propia

Tabla 6 – Registro de la configuración en PC-B

PC-B Network Configuration	
Descripción	
Dirección física	*0001.C93A.5489*
Dirección IP	*192.168.72.190*
Máscara de subred	*255.255.255.192*
Gateway predeterminado	*192.168.72.129*

Fuente: Elaboración propia.

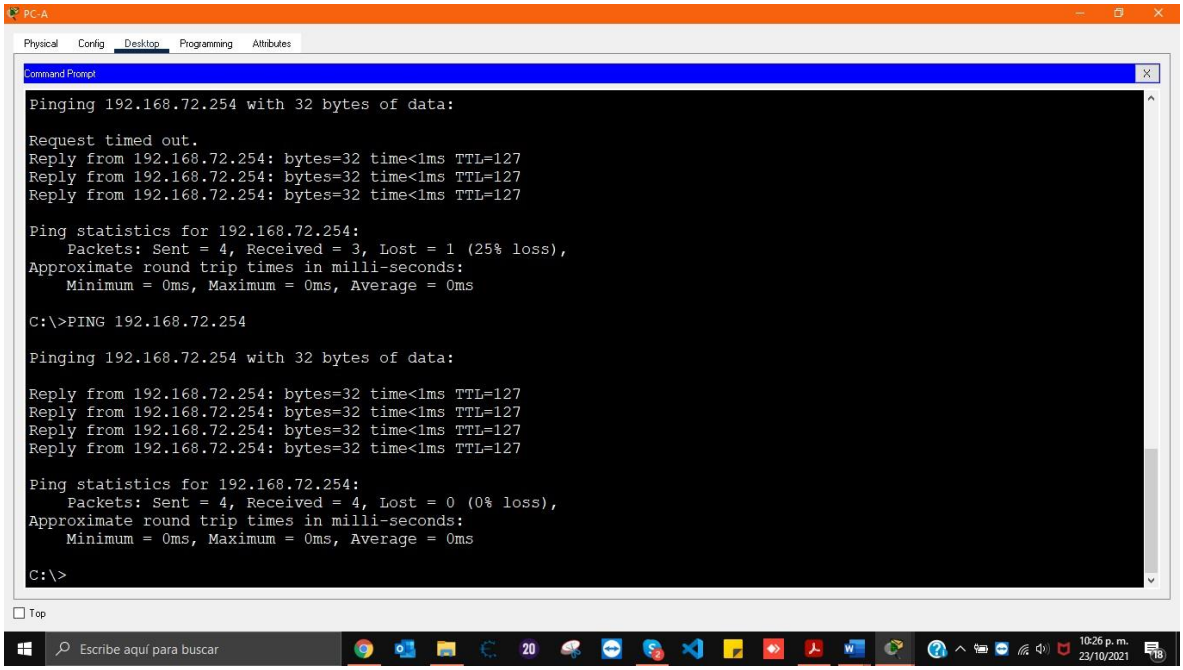
Configuración del PC-B

C:\>ipconfig /all

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.............: 0001.C93A.5489
   Link-local IPv6 Address.....: FE80::201:C9FF:FE3A:5489
   IPv6 Address.................: ::
   IPv4 Address.................: 192.168.72.190
   Subnet Mask..................: 255.255.255.192
   Default Gateway..............: ::
                                  192.168.72.129
   DHCP Servers.................: 0.0.0.0
   DHCPv6 IAID..................:
   DHCPv6 Client DUID...........: 00-01-00-01-1E-A4-80-5C-00-01-C9-3A-54-89
   DNS Servers..................: ::
                                  0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.............: 0009.7C10.A04A
   Link-local IPv6 Address.....: ::
 --More--
```

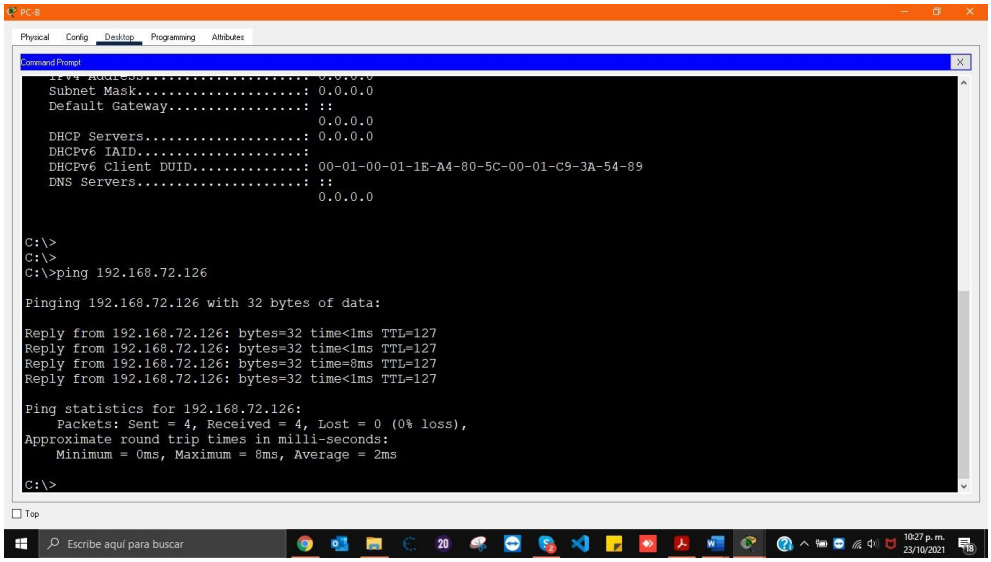
Pruebas de conectividad:
Pruebas de ping:

Ilustración 8 - Ping exitoso desde la PC-A hacia la PC-B



Fuente: Elaboración propia

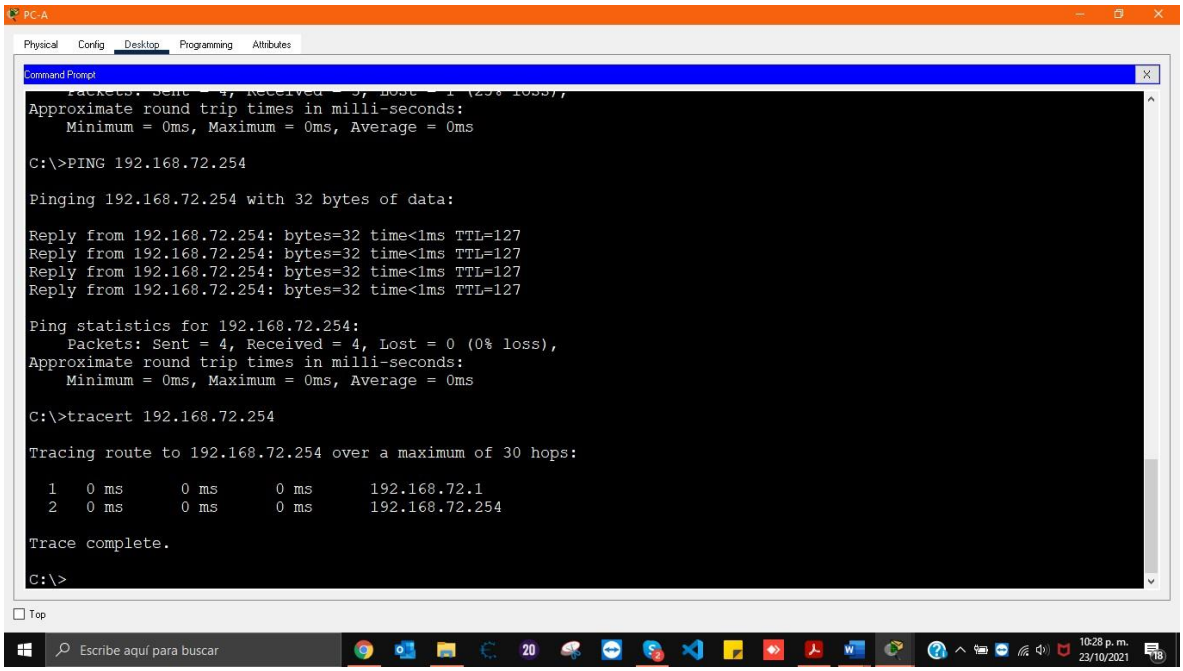
Ilustración 9 - Ping exitoso desde la PC-B hacia la PC-A



Fuente: Elaboración propia

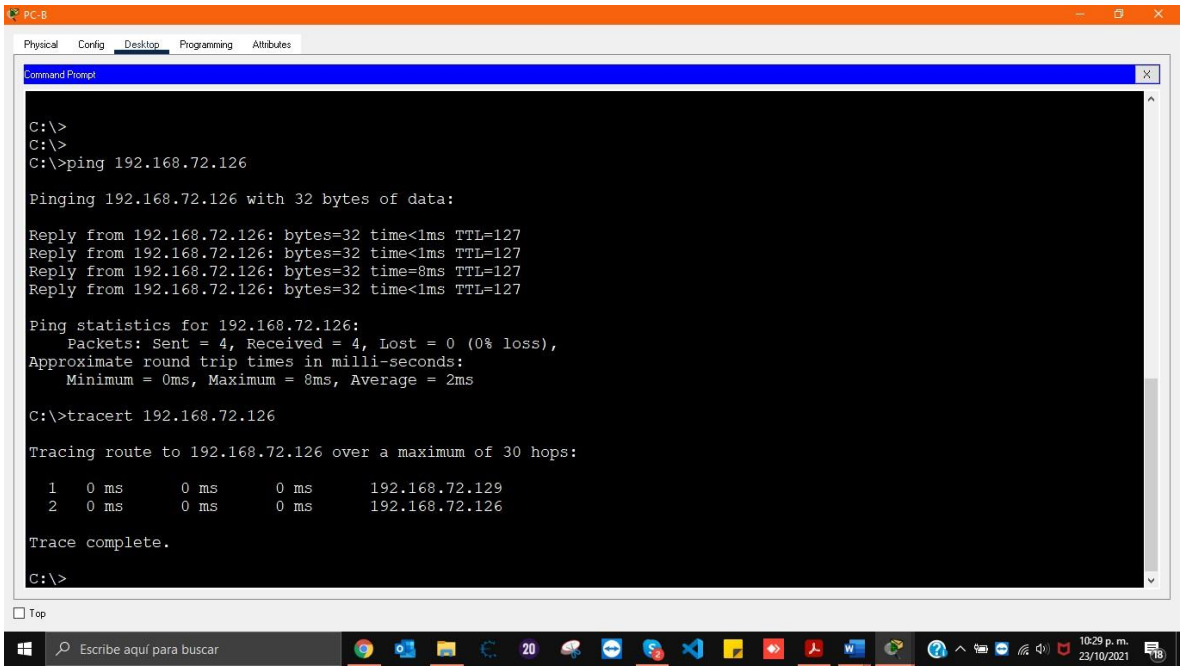
Pruebas de traceroute:

Ilustración 10 - Traceroute hacia PC-B desde la PC-A



Fuente: Elaboración propia

Ilustración 11- Traceroute hacia PC-A desde PC-B



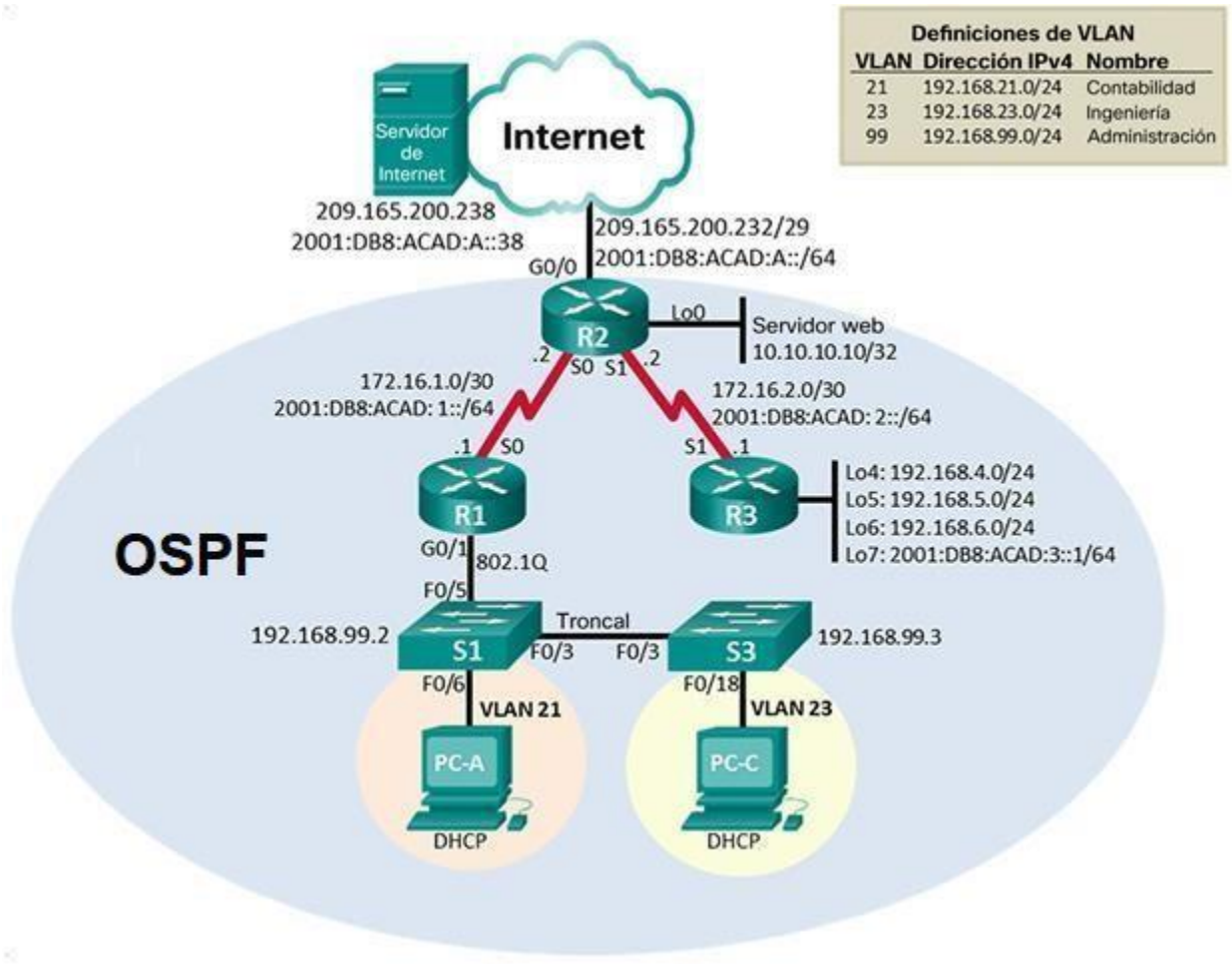
Fuente: Elaboración propia

ESCENARIO 2

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

Ilustración 12 – topología del escenario número 2.

Topología



Fuente: Elaboracion propia.

Parte 1: Inicializar dispositivos
Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 7 – Proceso de inicial en los routers y switches

Tarea	**Comando de IOS**
Eliminar el archivo startup-config de todos los routers	Router#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 2010 by cisco Systems, Inc. Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB CISCO1941/K9 platform with 524288 Kbytes of main memory Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled Readonly ROMMON initialized

	program load complete, entry point: 0x80803000, size: 0x1b340 program load complete, entry point: 0x80803000, size: 0x1b340 IOS Image Load Test ———————————— Digitally Signed Release Software program load complete, entry point: 0x81000000, size: 0x2bb1c58 Self decompressing the image : ## ## #### [OK]
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch#delete vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory)
Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4) Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory. 2960-24TT starting...

	Base ethernet MAC Address: 000D.BD1B.7523 Xmodem file system is available. Initializing Flash... flashfs[0]: 1 files, 0 directories flashfs[0]: 0 orphaned files, 0 orphaned directories flashfs[0]: Total bytes: 64016384 flashfs[0]: Bytes used: 4670455 flashfs[0]: Bytes available: 59345929 flashfs[0]: flashfs fsck took 1 seconds. ...done initializing Flash. Boot Sector Filesystem (bs:) installed, fsid: 3 Parameter Block Filesystem (pb:) installed, fsid: 4 Loading "flash:/2960-lanbasek9-mz.150-2.SE4.bin"... ## [OK]
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>en Switch#show flash Directory of flash:/ 1 -rw- 4670455 <no date> 2960-lanbasek9-mz.150-2.SE4.bin 64016384 bytes total (59345929 bytes free)

Parte 2: Configurar los parámetros básicos de los dispositivos
Paso 1: Configurar la computadora de Internet

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

Tabla 8 – Configuración del servidor de internet

Elemento o tarea de configuración	**Especificación**
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.0
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Fuente: Prueba de habilidades Cisco CCNA II

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 9 – Requisitos de configuración en R1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Los comandos usados se detallarán más adelante.
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	Los comandos usados se detallarán más adelante.
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

Fuente: Prueba de habilidades Cisco CCNA II

- **Desactivar las búsquedas DNS:**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Dar nombre al dispositivo:**

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

- **Contraseña Exec privilegiado:**

```
R1(config)#enable secret class
```

```
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso a la consola:**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface con 0
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

- **Contraseña de acceso TELNET:**

```
R1(config)# line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

- **Cifrar las contraseñas de texto no cifrado:**

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#encr
R1(config)#encry
R1(config)#service pas
R1(config)#service password-encryption
R1(config)#
R1#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configuración del Mensaje MOTD:**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#bann
R1(config)#banner Mt
R1(config)#banner Mo
R1(config)#banner Motd "Advertencia: Solo ingresar si cuenta con una previa autorizacion"
R1(config)#end
```

- **Configuración interfaz S0/0/0:**

Se configura la interfaz Serial 0/0/0 asignándole una dirección de IPv4 según lo mostrado en la topología del escenario, también se levanta la interfaz y se le da una frecuencia de reloj de 128000.

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#clock ra
R1(config-if)#clock rate 128000
R1(config-if)#desc
R1(config-if)#description "Interfaz Serial 0/0/0 Router 1"
R1(config-if)#
```

Se finaliza asignando la IPv6 a la interfaz.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
```

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10 – Parámetros a configurar en R2

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Los comandos usados se detallarán más adelante.
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	Los comandos usados se detallarán más adelante.
Habilitar el servidor HTTP	Los comandos usados se detallarán más adelante.
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.

Fuente: Prueba de habilidades Cisco CCNA II

- **Desactivar búsquedas DNS:**

```
Router>en
```

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

- **Dar nombre al Router:**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#
```

- **Contraseña de exec privilegiada:**

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable secret class
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso a consola:**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso TELNET**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Cifrar contraseñas de texto no cifrado:**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ser
R2(config)#service p
R2(config)#service password-encryption
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Habilitar el servidor HTTP:**

```
R2#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip http server
```

- **Mensaje MOTD:**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#banner m
R2(config)#banner motd "Advertencia: Solo ingresar si cuenta con una previa autorizacion"
R2(config)#end
```

- **Configurar Interfaz Serial 0/0/0:**

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#clock rate 128000
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#des
R2(config-if)#description "Interfaz serial 0/0/0 perteneciente al R2"
R2(config-if)#exit
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Se configura la interfaz serial 0/0/0 del R2, asignándole su respectiva IPv4, junto con su IPv6, también se procede a levantar la interfaz y darle su descripción.

- **Configurar Interfaz Serial 0/0/1:**

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#exit
```

Se configura la interface serial 0/0/1, asignándole dirección ipv4 e ipv6, se procede a darle una frecuencia de reloj a la interfaz y se levanta.

- **Configurar interfaz G0/0:**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface gi
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#descrip
R2(config-if)#description "Interfaz de simulacion de internet"
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown
```

- **Configurar interfaz Loopback 0:**

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface loo
R2(config)#interface loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on interface Loopback0, changed state to up
```

```
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#des
R2(config-if)#description "Loopback 0 - Servidor web simulado"
R2(config-if)#
```

- **Configurar rutas predeterminadas:**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip rou
R2(config)#ip route
R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)#
R2(config)#ipv6 route ::/0 G0/0
```

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11 - Parámetros a configurar en R3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Los comandos usados se detallarán más adelante.
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	Los comandos usados se detallarán más adelante.
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.

Fuente: Prueba de habilidades Cisco CCNA II

Desactivar Busquedas DNS:

```
Router>EN
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip doma
Router(config)#no ip domain
Router(config)#no ip domain-l
Router(config)#no ip domain-lookup
Router(config)#
```

- **Asignar nombre al router:**

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)#hostname R3
R3(config)#
```

- **Contraseña Exec privilegiada:**

```
R3(config)#enable secret class
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso a consola**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso telnet:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Cifrar las contraseñas:**

```
R3#conf terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ser
R3(config)#service pas
R3(config)#service password-encryption
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Mensaje MOTD:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ban
R3(config)#banner mo
R3(config)#banner motd "Advertencia: Solo ingresar si cuenta con una previa autorizacion"
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar la Interfaz Serial S0/0/1:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface serial 0/0/1
R3(config-if)#desc
R3(config-if)#description "Interfaz serial 0/0/1 del R3"
R3(config-if)#ip address 172.16.2.2 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#ipv6 address
%LINEPROTO-5-UPDOWN: Line protocol on interface Serial0/0/1, changed state to up
```

```
% Incomplete command.
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Se realiza la configuración de la interfaz Serial 0/0/1, asignándole direccionamiento IPv4 e IPv6 según los requerimientos del escenario, también se asignó una descripción de interfaz y finalmente se levantó la interface.

- **Configurar interfaz Loopback 4:**

```
R3#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface loop
R3(config)#interface loopback 4

R3(config-if)#
%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
R3(config-if)#no shut
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar interfaz Loopback 5:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface loopback 5
```

```
R3(config-if)#
%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
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar interfaz Loopback 6:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface 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
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar interfaz Loopback 7:**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface 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
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 12 – Parámetros a configurar en S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Los comandos usados se detallarán más adelante.
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	Los comandos usados se detallarán más adelante.
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Fuente: Prueba de habilidades Cisco CCNA II

- **Desactivar búsquedas DNS:**

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

```
%SYS-5-CONFIG_I: Configured from console by console
```

- **Nombre del Switch:**

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de exec privilegiado:**

```
S1>en
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso a la consola:**

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso TELNET:**

```
S1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Cifrar contraseñas de texto no cifrado:**

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Mensaje MOTD:**

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd ″Advertencia: Solo ingresar si cuenta con una previa autorizacion. ″
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 13 – Parámetros a configurar en S3.

Elemento o tarea de configuración	Especificación

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.

Fuente: Prueba de habilidades Cisco CCNA II

- **Desactivar búsquedas DNS:**

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-l
Switch(config)#no ip domain-lookup
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Asignar un nombre al Switch:**

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de exec privilegiado:**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#enable secret class
S3(config)#end
```

```
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso a la consola:**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Contraseña de acceso TELNET:**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Cifrar contraseñas de texto no cifrado:**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#service pa
S3(config)#service password-encryption
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Mensaje MOTD:**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#banner motd
% Incomplete command.
S3(config)#banner motd ″Advertencia: Solo ingresar si tiene una autorizacion previa. ″
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red.

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

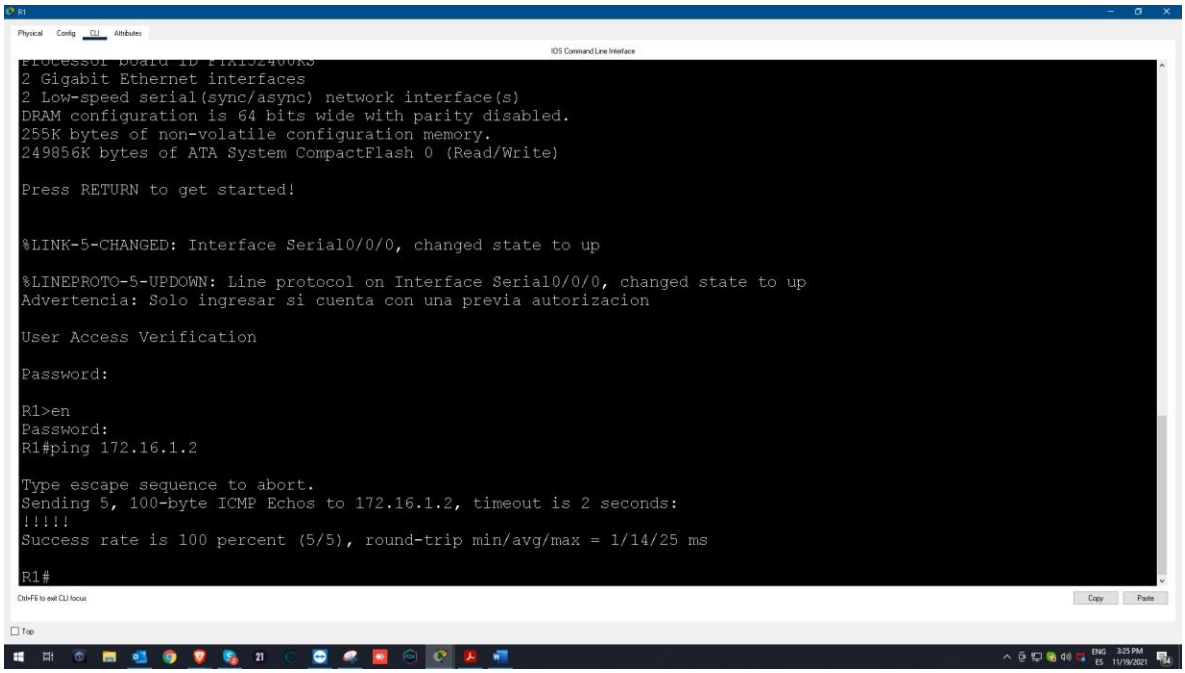
Tabla 14 – Tabla de pings

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	***172.16.1.2***	Exitoso
R2	R3, S0/0/1	***172.16.2.2***	Exitoso
PC de Internet	Gateway predeterminado	***209.165.200.233***	Exitoso

Fuente: Prueba de habilidades Cisco CCNA II

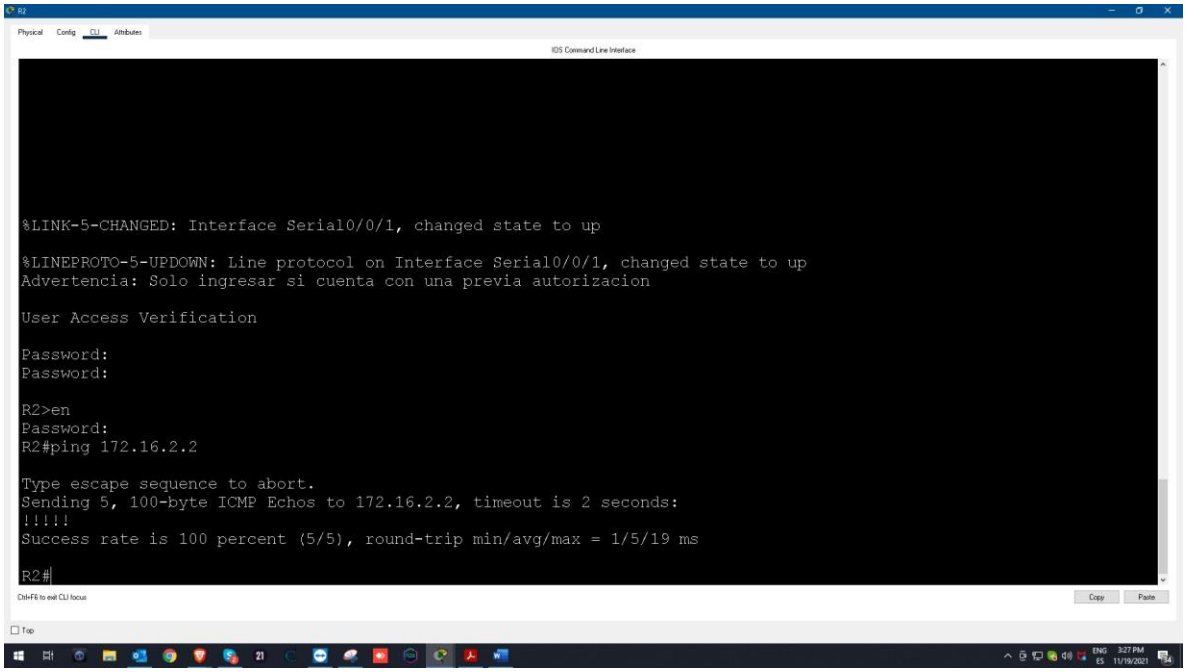
Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Ilustración 13 - Ping exitoso desde R1 a la interfaz S0/0/0 de R2



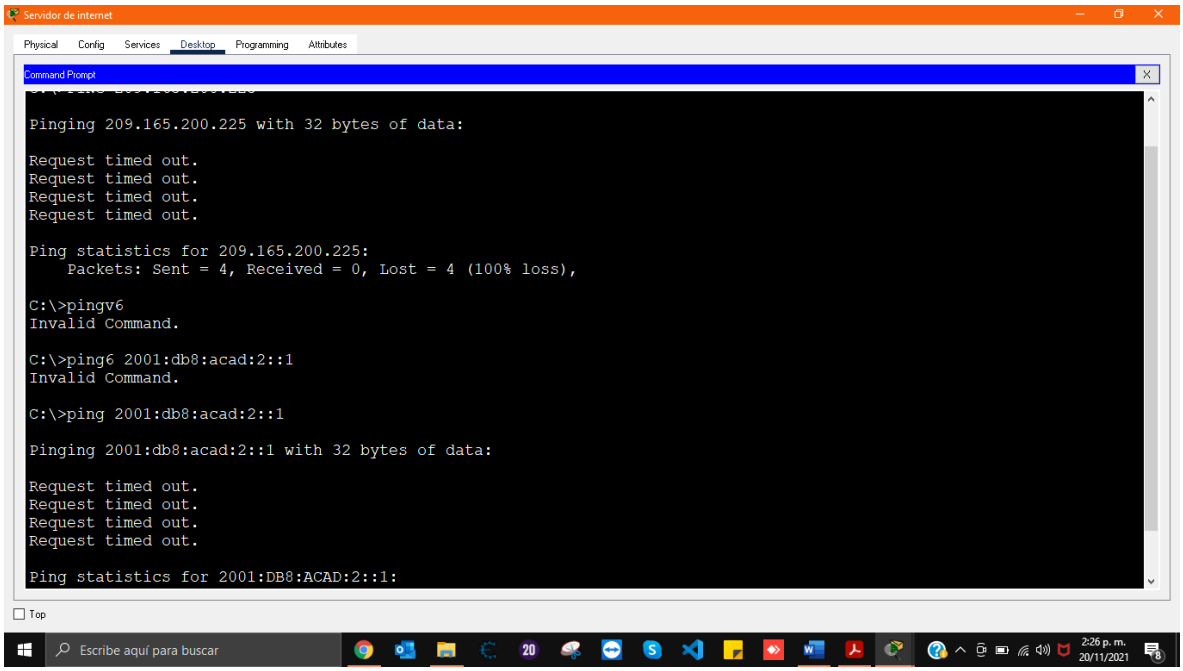
Fuente: Elaboración propia.

Ilustración 14 - Ping exitoso desde R2 a la interfaz S0/0/1 de R3



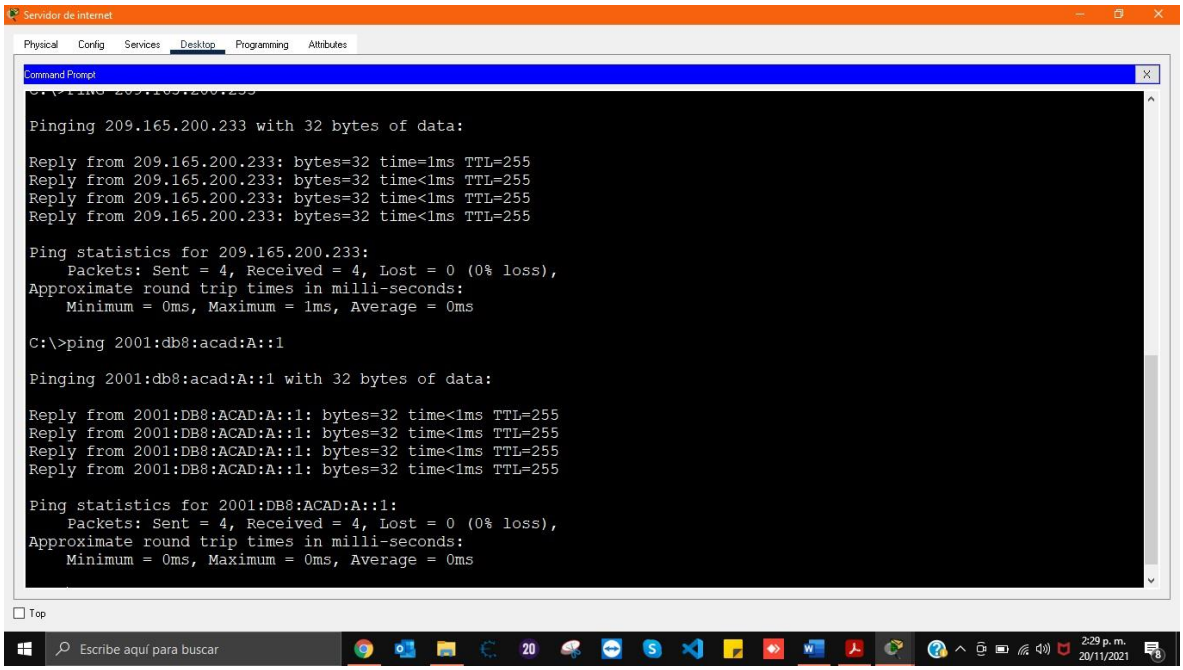
Fuente: Elaboración propia.

Ilustración 15 –– Ping desde el servidor hacia sus gateways IPv4 e IPv6



Fuente: Elaboración propia.

Ilustración 16 -– Ping desde el servidor de internet hacia los gateways IPv4 e IPv6 después de asignarles los gateways correctos.



Fuente: Elaboración propia.

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN
Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 15 – Parámetros a configurar en S1.

Elemento o tarea de configuración	**Especificación**
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	Los comandos usados se detallarán más adelante.
Apagar todos los puertos sin usar	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Crear la base de datos de VLAN**

```
S1>en
Password:
S1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by cons

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 23
S1(config-vlan)#name ingenieria
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Asignar la dirección IP de administración.**

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Asignar el gateway predeterminado**

```
S1>en
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip de
S1(config)#ip default-gateway 192.168.99.1
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Forzar el enlace troncal en la interfaz F0/3**

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface fas
S1(config)#interface fastEthernet 0/3
S1(config-if)#swi
S1(config-if)#switchport
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3
(99), with S3 FastEthernet0/3 (
% Incomplete command.
S1(config-if)#swi
S1(config-if)#switchport mode
S1(config-if)#switchport mode t
S1(config-if)#switchport mode trunk
S1(config-if)#sw
S1(config-if)#switchport tr
S1(config-if)#switchport trunk na
S1(config-if)#switchport trunk native vlan 1
```

- **Forzar el enlace troncal en la interfaz F0/5**

```
S1(config)#interface fa
S1(config)#interface fastEthernet 0/5
```

```
S1(config-if)#sw
S1(config-if)#switchport mode
S1(config-if)#switchport mode t
S1(config-if)#switchport mode trunk
S1(config-if)#sw
S1(config-if)#switchport tr
S1(config-if)#switchport trunk na
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar el resto de los puertos como puertos de acceso**

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface
S1(config)#interface ra
S1(config)#interface range fa
S1(config)#interface range fastEthernet 0/1-2
S1(config-if-range)#sw
S1(config-if-range)#switchport mod
S1(config-if-range)#switchport mode a
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#interface fastEthernet 0/4
S1(config-if)#switchport mode access
S1(config-if)#exit
S1(config)#interface range fastEthernet 0/6-24
S1(config-if-range)#sw
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

```
S1(config)#
```

- **Asignar F0/6 a la VLAN 21**

```
S1(config)#interface fast
S1(config)#interface fastEthernet 0/6
S1(config-if)#swit
S1(config-if)#switchport mode
S1(config-if)#switchport mode acces
S1(config-if)#switchport mode access
S1(config-if)#swi
S1(config-if)#switchport access
S1(config-if)#switchport access vlan 21
S1(config-if)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Apagar todos los puertos sin usar**

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range fas
S1(config)#interface range fastEthernet 0/1-2
S1(config-if-range)#shutdo
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
S1(config-if-range)#exit

S1(config)#interface fastEthernet 0/4
S1(config-if)#shutdown
```

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

S1(config-if)#exit

S1(config)#interface range fas

S1(config)#interface range fastEthernet 0/7-24

S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

```
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively
down
S1(config-if-range)#end
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 16 – Parámetros a configurar en S3.

Elemento o tarea de configuración	Especificación
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	Los comandos usados se detallarán más adelante.
Apagar todos los puertos sin usar	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Crear la base de datos de VLAN**

```
S3>en
Password:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
S3(config)#vlan 23
S3(config-vlan)#name ingenieria
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Asignar la dirección IP de administración**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface vlan 99
S3(config-if)#
%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
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Asignar el gateway predeterminado**

```
S3>en
Password:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#ip de
S3(config)#ip default-gateway 192.168.99.1
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Forzar el enlace troncal en la interfaz F0/3**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface fas
S3(config)#interface fastEthernet 0/3
S3(config-if)#swit
S3(config-if)#switchport mode
S3(config-if)#switchport mode t
S3(config-if)#switchport mode trunk
S3(config-if)#s
S3(config-if)#sw
S3(config-if)#switchport t
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar el resto de los puertos como puertos de acceso**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface range fa
S3(config)#interface range fastEthernet 0/1-2
```

```
S3(config-if-range)#sw
S3(config-if-range)#switchport mode
S3(config-if-range)#switchport mode a
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
S3(config)#interface range fastEthernet 0/4-24
S3(config-if-range)#sw
S3(config-if-range)#switchport mode a
S3(config-if-range)#switchport mode access
S3(config-if-range)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Asignar F0/18 a la VLAN 21**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface fast
S3(config)#interface fastEthernet 0/18
S3(config-if)#switch
S3(config-if)#switchport access vlan 21
S3(config-if)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Apagar todos los puertos sin usar**

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface range fa
S3(config)#interface range fastEthernet 0/1-2
S3(config-if-range)#shut
S3(config-if-range)#shutdown
```

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

S3(config-if-range)#exit

S3(config)#interface range fa

S3(config)#interface range fastEthernet 0/4-17

S3(config-if-range)#shut

S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

S3(config-if-range)#exit

S3(config)#interface range fas

S3(config)#interface range fastEthernet 0/19-24

S3(config-if-range)#shut

S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

S3(config-if-range)#end

```
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 - Configuración de subinterfaces en R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
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	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Configurar la subinterfaz 802.1Q .21 en G0/1**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/1.21
R1(config-subif)#desc
R1(config-subif)#description Lan de Contabilidad
R1(config-subif)#enca
R1(config-subif)#encapsulation dot
R1(config-subif)#encapsulation dot1Q 21
```

```
R1(config-subif)#ip address 192.168.21.2 255.255.255.0
R1(config-subif)#no shut
R1(config-subif)#no shutdown
R1(config-subif)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar la subinterfaz 802.1Q .23 en G0/1**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/1.23
R1(config-subif)#desc
R1(config-subif)#description Lan de ingenieria
R1(config-subif)#encap
R1(config-subif)#encapsulation d
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.2 255.255.255.0
R1(config-subif)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configurar la subinterfaz 802.1Q .99 en G0/1**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/1.99
R1(config-subif)#des
R1(config-subif)#description Lan de Administracion
R1(config-subif)#enca
R1(config-subif)#encapsulation d
R1(config-subif)#encapsulation dot1Q 99
```

```
R1(config-subif)#ip a
R1(config-subif)#ip ad
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Activar la interfaz G0/1**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface gi
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#no shut
R1(config-if)#no shutdown

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

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

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

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

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

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

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

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

Paso 4: Verificar la conectividad de la red

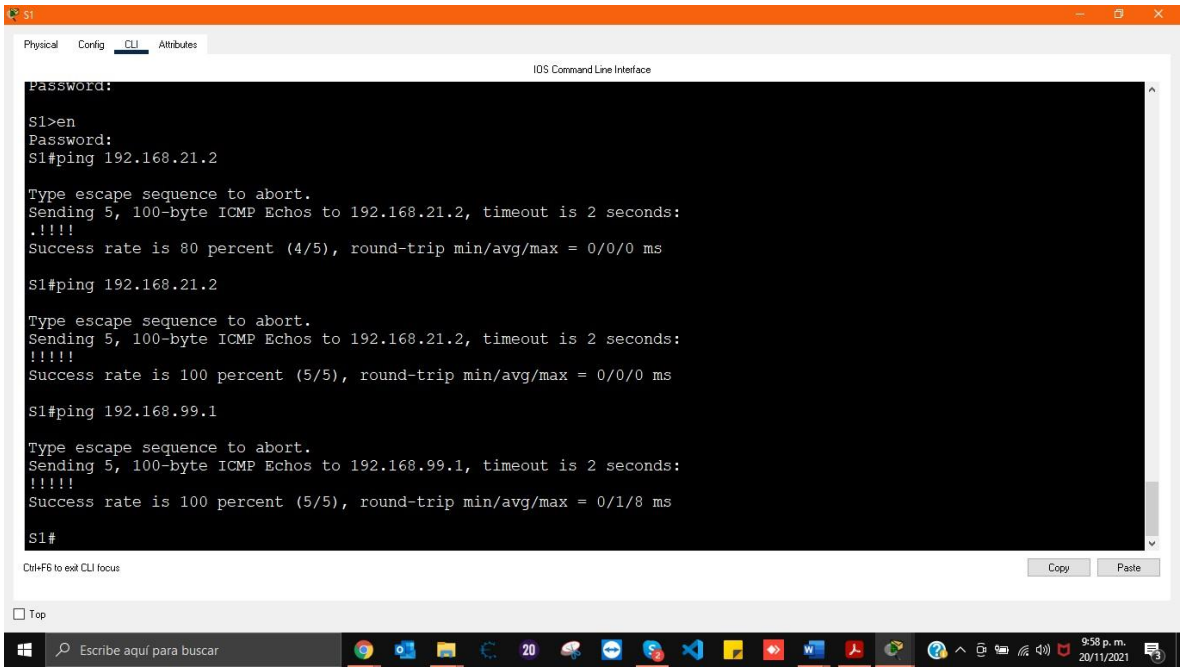
Utilice el comando **ping** para probar la conectividad entre los switches y el R1.

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

Tabla 18 - Verificación de conectividad de la red.

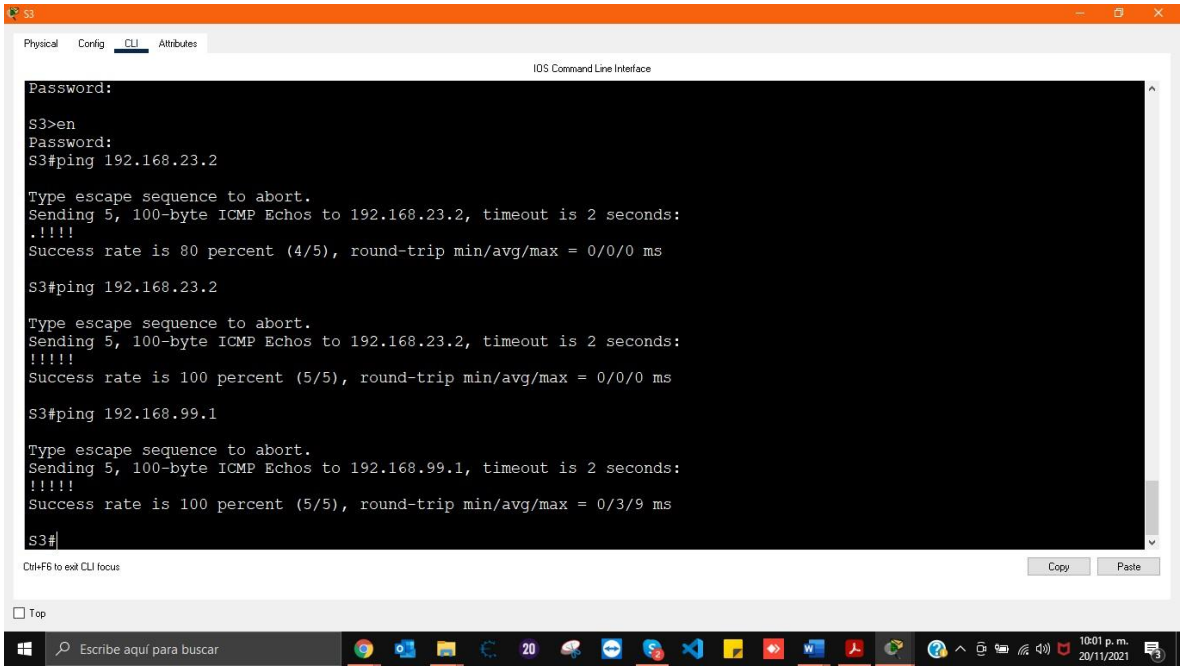
Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Exitoso
S3	R1, dirección VLAN 99	192.168.99.1	Exitoso
S1	R1, dirección VLAN 21	192.168.21.2	Exitoso
S3	R1, dirección VLAN 23	192.168.23.2	Exitoso

Ilustración 17 - Ping desde S1 hacia las subinterfaces 802.1Q 99 y 802.1Q21 en Gi0/1 de R1



Fuente: Elaboración propia.

Ilustración 18 - Ping desde S3 hacia las subinterfaces 802.1Q 99 y 802.1Q23 en Gi0/1 de R1



Fuente: Elaboración propia.

Parte 4: Configurar el protocolo de routing dinámico OSPF
Paso 1: Configurar OSPF en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19 – Parámetros para configurar OSPF en R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	Los comandos usados se detallarán más adelante.
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	Los comandos usados se detallarán más adelante.
Desactive la sumarización automática	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Configurar OSPF área 0**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router os
R1(config)#router ospf 0
                       ^
% Invalid input detected at '^' marker.

R1(config)#router ospf 1
R1(config-router)#router
R1(config-router)#router-id 1.1.1.1
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Anunciar las redes conectadas directamente**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
R1(config-router)#network 192.168.21.0 0.0.0.255 area 0
R1(config-router)#network 192.168.23.0 0.0.0.255 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
```

- **Establecer todas las interfaces LAN como pasivas**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#passive-interface ser
R1(config-router)#passive-interface serial 0/0/0
R1(config-router)#passi
R1(config-router)#passive-interface g
R1(config-router)#passive-interface gigabitEthernet 0/1
R1(config-router)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Desactive la sumarización automática**

```
R1(config-router)#no auto-summary
```

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 20 – Parámetros para configurar OSPF en R2.

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	Los comandos usados se detallarán más adelante.
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	Los comandos usados se detallarán más adelante.
Desactive la sumarización automática.	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Configurar OSPF área 0**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#route ospf 1
R2(config-router)#router-id 2.2.2.2
```

- **Anunciar las redes conectadas directamente**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#route ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
```

- **Establecer la interfaz LAN (loopback) como pasiva**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#route ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#
```

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#passi
R2(config-router)#passive-interface loop
R2(config-router)#passive-interface loopback 0
R2(config-router)#end
R2#
```

- **Desactive la sumarización automática.**

```
R1(config-router)#no auto-summary
```

Paso 3: Configurar OSPFv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Ilustración 19 – Instrucciones para configurar OSPF en R2

Elemento o tarea de configuración	**Especificación**
Configurar OSPF área 0	Los comandos usados se detallarán más adelante.
Anunciar redes IPv4 conectadas directamente	Los comandos usados se detallarán más adelante.
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Los comandos usados se detallarán más adelante.
Desactive la sumarización automática.	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Configurar OSPF área 0**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#route ospf 1
R3(config-router)#router
R3(config-router)#router-id 3.3.3.3
```

- **Anunciar redes IPv4 conectadas directamente**

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#route ospf 1
R3(config-router)#router
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
```

- **Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas**

```
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
```

- **Desactive la sumarización automática.**

```
R3(config-router)#no auto-summary
```

Paso 4: Verificar la información de OSPF

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

Tabla 21 - Resolución a preguntas acerca de OSPF.

Pregunta	**Respuesta**
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	R2#show ip protocols
¿Qué comando muestra solo las rutas OSPF?	R2#show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	R2#show ip route

Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 22 – Parámetros para configurar DHCP en R1.

Elemento o tarea de configuración	**Especificación**
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

Fuente: Prueba de habilidades Cisco CCNA II

- **Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas**

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas**

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Crear un pool de DHCP para la VLAN 21.**

```
R1(config)#ip dhcp e
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#dns
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domai
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#defa
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#netw
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#exit
```

- **Crear un pool de DHCP para la VLAN 23**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dh
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#dns
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#defa
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#net
```

```
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#exit
```

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

La configuración del R2 incluye las siguientes tareas:

Tabla 23 – Parámetros para configurar NAT en R2.

Elemento o tarea de configuración	**Especificación**
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	Los comandos usados se detallarán más adelante.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Los comandos usados se detallarán más adelante.
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	Los comandos usados se detallarán más adelante.
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	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Crear una base de datos local con una cuenta de usuario**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser pr
R2(config)#user webuser privilege 15 secret cisco12345
```

- **Habilitar el servicio del servidor HTTP**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip http server
               ^
% Invalid input detected at '^' marker.
```

Comando no compatible con Packet tracer.

- **Configurar el servidor HTTP para utilizar la base de datos local para la autenticación**

```
R2(config)#ip http authentication local
               ^
% Invalid input detected at '^' marker.
```

Comando no compatible con Packet tracer

- **Crear una NAT estática al servidor web**

```
R2(config)#ip nat
R2(config)#ip nat ins
R2(config)#ip nat inside source sta
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
```

- **Asignar la interfaz interna y externa para la NAT estática**

```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip nat outside
```

```
R2(config-if)#interface gigabitEthernet 0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

- **Configurar la NAT dinámica dentro de una ACL privada**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.6.1 0.0.0.255
R2(config)#access-list 1 permit 192.168.5.1 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.1 0.0.0.255
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Defina el pool de direcciones IP públicas utilizables.**

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat pool
R2(config)#ip nat pool INTERNET
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
```

- **Definir la traducción de NAT dinámica**

```
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 3: Verificar el protocolo DHCP y la NAT estática

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

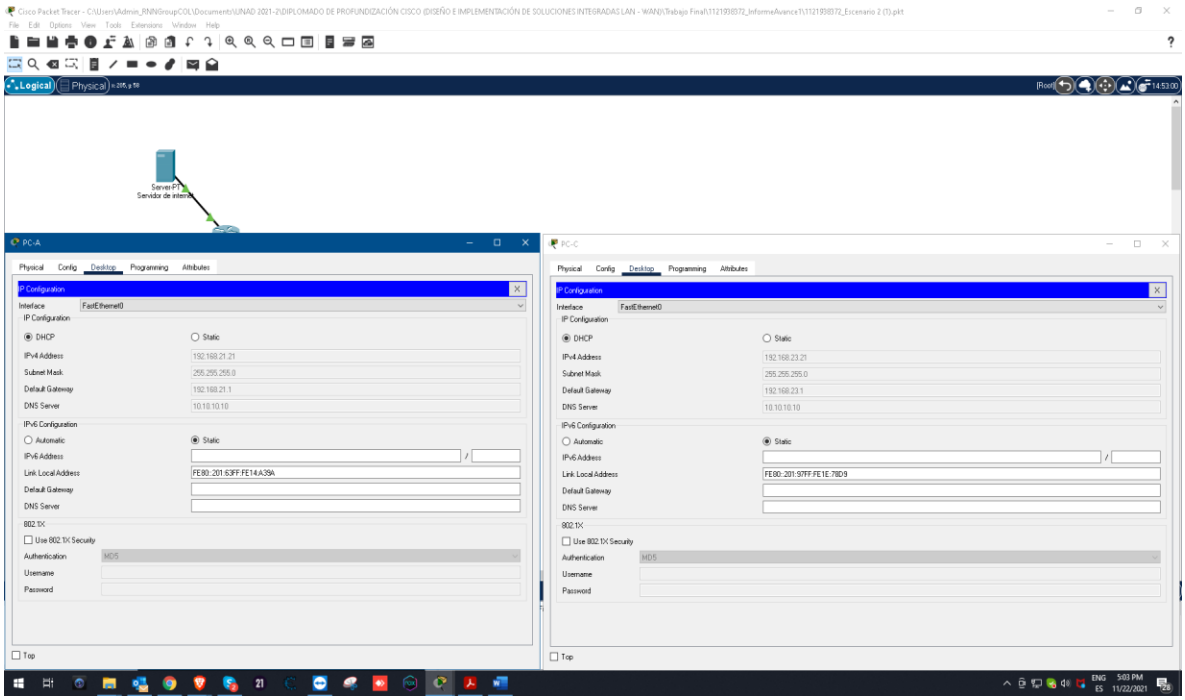
Tabla 24 – Tareas para verificar la funcionalidad de NAT y DHCP

Prueba	**Resultados**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Exitoso, se le asigno la IP 192.168.21.21
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	En primera instancia se le asignaba la IP 192.168.21.22, se pasó el puerto fa0/18 del S3 a la VLAN 23: S3>en Password: S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#interface fas S3(config)#interface fastEthernet 0/18 S3(config-if)#sw S3(config-if)#switchport mode access S3(config-if)#sw S3(config-if)#switchport a S3(config-if)#switchport access vlan 23 S3(config-if)#exit S3(config)# S3(config)#exit Al volver a solicitar una dirección IP por medio de DHCP se le asigno la 192.168.23.21

Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Los comandos usados se detallarán más adelante.
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

Ilustración 20 - Asignación de IP por medio de DHCP a los equipos de la VLAN 21 Y VLAN 23



Fuente: Elaboración propia.

Parte 6: Configurar NTP

Tabla 25 – Parámetros para configurar NTP.

Elemento o tarea de configuración	**Especificación**
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.	Los comandos usados se detallarán más adelante.
Verifique la configuración de NTP en R1.	Los comandos usados se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Ajuste la fecha y hora en R2.**

```
R2#clock
R2#clock s
R2#clock set ?
  hh:mm:ss Current Time
R2#clock set 09:00:00 ?
  <1-31> Day of the month
  MONTH   Month of the year
R2#clock set 09:00:00 mar ?
  <1-31> Day of the month
R2#clock set 09:00:00 mar 5 ?
  <1993-2035>  Year
R2#clock set 09:00:00 mar 5 2016
```

- **Configure R2 como un maestro NTP.**

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp mas
R2(config)#ntp master ?
  <1-15>  Act as NTP master clock
  <cr>
R2(config)#ntp master 5
R2(config)#
```

- **Configurar R1 como un cliente NTP.**

```
R1>en
Password:
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp ser
R1(config)#ntp server 172.16.1.2
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Configure R1 para actualizaciones de calendario periódicas con hora NTP.**

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp up
R1(config)#ntp update-calendar
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

- **Verifique la configuración de NTP en R1.**

```
R1#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s
system poll interval is 4, never updated.
```

```
R1(config)#do show ntp status
Clock is synchronized, stratum 6, reference is 172.16.1.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is DA60367B.000001BB (9:8:11.443 UTC Sat Mar 5 2016)
clock offset is 1.00 msec, root delay is 13.00  msec
root dispersion is 10.27 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s
system poll interval is 4, last update was 2 sec ago.
```

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

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

Tabla 26 – Parámetros para configurar ACL en R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN- MGT**
Aplicar la ACL con nombre a las líneas VTY	Los comandos se detallarán más adelante.
Permitir acceso por Telnet a las líneas de VTY	Los comandos se detallarán más adelante.
Verificar que la ACL funcione como se espera	Los comandos se detallarán más adelante.

Fuente: Prueba de habilidades Cisco CCNA II

- **Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2**

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip acc
R2(config)#ip access-list s
R2(config)#ip access-list standard ADMiN-MGT
R2(config-std-nacl)#permit h
```

```
R2(config-std-nacl)#permit host 172.16.1.1
```

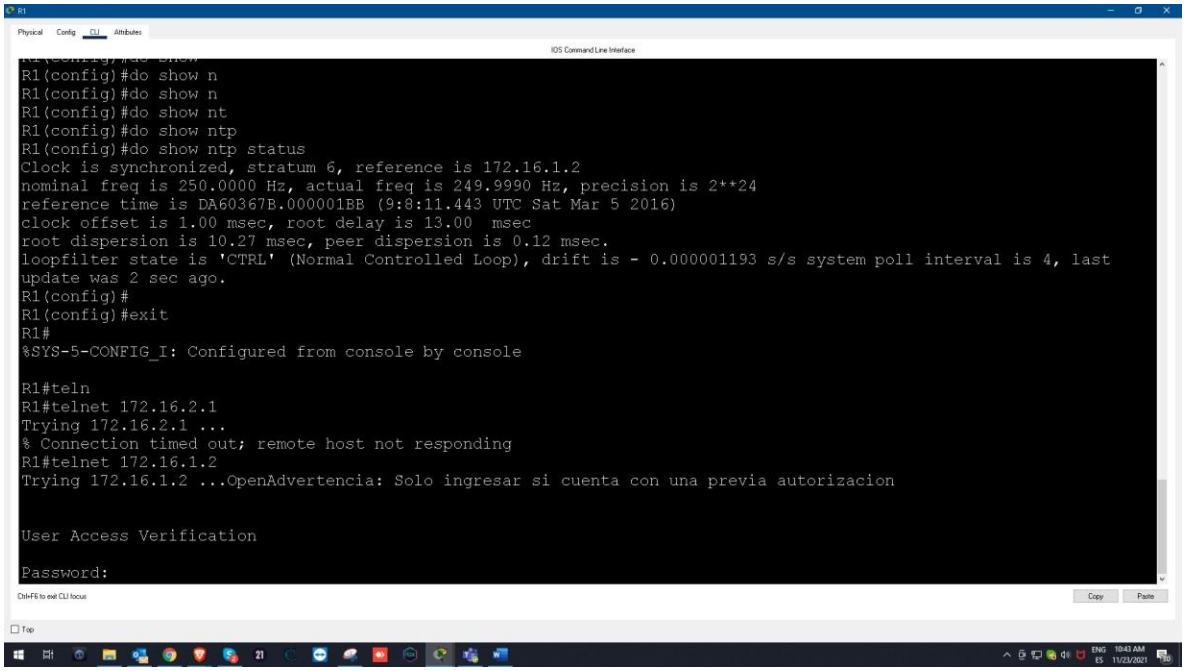
- **Aplicar la ACL con nombre a las líneas VTY, Permitir acceso por Telnet a las líneas de VTY**

```
R2(config)#line vty 0 4
R2(config-line)#acc
R2(config-line)#acce
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#exit
```

- **Verificar que la ACL funcione como se espera**

```
R1#telnet 172.16.2.1
Trying 172.16.2.1 ...
% Connection timed out; remote host not responding
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenAdvertencia: Solo ingresar si cuenta con una previa autorizacion


User Access Verification


Password:
```

Ilustración 21 - Accediendo a R2 mediante TELNET desde R1



Fuente: Elaboración propia.

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

Tabla 27 – Resolución de preguntas acerca de ACL.

Descripción del comando	**Entrada del estudiante (comando)**
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-lists
Restablecer los contadores de una lista de acceso	R2#clear access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface R2#show access-lists

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

Fuente: Prueba de habilidades Cisco CCNA II

CONCLUSIONES

Al desarrollo del primer escenario podemos concluir lo siguiente:

- Para permitir una conexión remota de forma segura a un router o un switch se implementa ssh, también se efectúan buenas prácticas en cuanto a la seguridad de estos dispositivos tales como: Desactivación de las búsquedas por dns, dar un nombre a los mismos, contraseñas para el modo exec privilegiado y consola, cifrado RSA, configuración de la línea VTY para que solo use el usuario administrador de la base de datos local y a su para que solo acepte sesión por medio de ssh.
- Para asegurar una buena conectividad entre ambos extremos de la red, es importante subnetear bien la misma, a su vez que es fundamental asignar correctamente los gateway tanto en el switch como en ambos equipos de los extremos.

Una vez desarrollado el segundo escenario podemos concluir lo siguiente:

- Para la administracion de redes con una cantidad de hosts considerable, es una buena práctica casi indispensable, la implementación de un servidor DHCP, en este caso dicho servidor se configuro en el mismo router.
- Como buena práctica de seguridad es aconsejable generar listas de acceso a las líneas vty 0 4 las cuales cumplen la función de TELNET, de esta manera nos aseguramos de que únicamente ciertos hosts puedan acceder al router.

REFERENCIAS BIBLIOGRAFICAS

CISCO. “Capa de red. Fundamentos de Networking”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. “Configuración del Switch. Principios de Enrutamiento y Conmutación”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#5

CISCO. “DHCP. Principios de Enrutamiento y Conmutación”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. “Direccionamiento IP. Fundamentos de Networking”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7

CISCO. “División de redes IP en subredes. Fundamentos de Networking”. {2019}. {En línea}. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

CISCO. “Ethernet. Fundamentos de Networking”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5

CISCO. “Listas de Control de Acceso. Principios de Enrutamiento y Conmutación”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. “Redes Conmutadas. Principios de Enrutamiento y Conmutación”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

CISCO. “Routing Estático. Principios de Enrutamiento y Conmutación”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2

CISCO. “VLAN. Principios de Enrutamiento y Conmutación”. {En línea}. {2019}. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

UNAD. “Configuración de Switches y Routers” [OVA]. {En línea}. {2017}. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC