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

DIANA LICETH VARON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD.
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISTEMAS
NEIVA
2021

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

DIANA LICETH VARON

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

TUTOR:
Ing. MARIA ALEJANDRA LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD.
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE SISTEMAS
NEIVA
2021

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____
FIRMA

_____
FIRMA

_____
FIRMA

Neiva, 01 de diciembre de 2021

AGRADECIMIENTOS

Primero que todo le agradezco a Dios por permitirme alcanzar esta nueva meta dentro de mi vida profesional, Agradezco enormemente a mi familia por ser ese apoyo incondicional cuando yo más lo necesitaba.

CONTENIDO

LISTA DE TABLAS.

LISTA DE FIGURAS

GLOSARIO

DHCP:
El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Internet:
Internet (el internet o, también, la internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyan una red lógica única de alcance mundial.

Protocolo De Red
Es el conjunto de reglas estándar que se utilizan para la comunicación en redes de computadores de cualquier tipo, ya sean LAN, WAN, etc. Por los que se establece una semántica y sintaxis a seguir para que sea más fácil de entender a la misma vez que funciona de la manera más óptima.

Red:
Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Red De Área Amplia (WAN):
Es el conjunto de redes más pequeñas que cubren gran parte del planeta por lo que permiten la comunicación hoy en día entre usuarios de distintos lugares comunicarse casi en tiempo real incluso a miles de kilómetros de distancia dando una gran velocidad que cada vez se ha ido aumentando en capacidad ya que la demanda mundial del servicio es muy grande, en este caso se hacen conexiones de todo tipo cableadas, inalámbricas y satelitales para poder brindar servicios de conexión a tantos usuarios.

Red De Área Local (LAN):
Se define como un conjunto de dispositivos conectados en una red local, en donde estos dispositivos de cómputo o móviles pueden compartir información como archivos, documentos y datos, es decir, entre ellos puede haber envió de estos archivos, un ejemplo es cuando en alguna oficina todos los computadores están conectados. En este caso los dispositivos se pueden conectar a la red por medios cableados o inalámbricos.

RESUMEN

En éste trabajo se va a desarrollar e implementar 2 escenarios redes, en las cuales se va a realizar sus montajes bajo tecnología y dispositivos CISCO. El hecho de emplear esta tecnología permite gran confiabilidad y seguridad a la red lo que se verá reflejado en un buen servicio hacia los clientes.

El proceso que se va a abordar inicia desde cero conociendo la temática desde el módulo de CCNA1 y CCNA2, de esta manera se describirá cada uno de los pasos, desde el proceso de recolección de la información de la entidad hasta su puesta en funcionamiento. Se configurará cada uno de los dispositivos que hacen parte de la red, se mostrarán los comandos empleados para cada aspecto. Para su direccionamiento se empleará tanto IPV4 como IPV6 y se realizará VLSM con el fin de poder adaptar el tamaño de la red a las necesidades reales del mismo. Se configurará los Protocolos de Enrutamiento que permitirán establecer esos caminos entre las diferentes redes y poder conectar el origen y el destino. Se realizará la configuración de cada uno de los dispositivos que hacen posible la conmutación de los paquetes entre las diferentes rutas y poder seleccionar el mejor camino.

Para lograr un correcto funcionamiento de la red se debe configurar una serie de protocolos o rutas por defecto que permitan tener un alcance de extremo a extremo de los dispositivos que hacen parte de la organización, se aplicará todo lo que tiene que ver con la creación y configuración de las VLAN, NAT, ACL y DHCP.

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

ABSTRACT

In this work, 2 network scenarios will be developed and implemented, in which they will be assembled under CISCO technology and devices. The fact of using this technology allows us great reliability and security to the network, which will be reflected in a good service to customers.

The process to be addressed starts from scratch knowing the subject from the CCNA1 and CCNA2 module, in this way each of the steps will be described, from the process of collecting the entity's information to its start-up. Each of the devices that are part of the network will be configured, the commands used for each aspect will be displayed. For its addressing we will use both IPV4 and IPV6 and we will carry out VLSM in order to be able to adapt the size of the network to its real needs. The Routing Protocols will be configured that will allow me to establish those paths between the different networks and be able to connect the origin and destination.

The configuration of each of the devices that make it possible to switch the packets between the different routes and to be able to select the best path will be carried out.

To achieve a correct functioning of the network, a series of protocols or default routes must be configured that allow me to have an end-to-end reach of the devices that are part of the organization, everything that has to do with the creation will be applied. and VLAN, NAT, ACL and DHCP configuration.

Keywords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCION

La tecnología en los últimos tiempos ha tenido muchos avances, crece de una forma tan exponencial y forma parte de la vida de todas las personas, tanto que ayuda en muchas de las actividades cotidianas. Si se mira la tecnología desde el punto de la información se puede ver que gracias a las redes y los dispositivos que hacen parte de la misma se hace posible el flujo de grandes cantidades ayudando en la toma de decisiones. La tecnología cambia constantemente y en especial lo hace y se adapta rápidamente a las necesidades de éstos tiempos, e incluso llega a puntos en los cuales avanza más que las necesidades reales.

Ya para referirse un poco más a ésta actividad, se busca profundizar en todo lo aprendido y que mejor manera que adentrarse en aspectos de las telecomunicaciones, tecnología que por donde se mire hace parte, ya no solo en una rama sino en muchos aspectos de la vida, agronomía, ciencia, deportes, etc.

Se va a suministrar una guía en la cual se muestra una serie de exigencias de 2 redes y una cantidad de parámetros que se deben configurar uno por uno con el fin de poder culminar con un correcto funcionamiento. El proceso de direccionamiento, se la va a desarrollar utilizando VLSM tanto para IPV4 como para direccionamiento IPV6 se configurará también protocolos de enrutamiento, tal como OSPF que permitirá el intercambio de información entre las diferentes subredes. Se implementan una serie de ACL los cuales permitirán tener un control total de cada uno de los espacios de la red lo cual brindará una seguridad total.

DESARROLLO

1. ESCENARIO 1

Topología

Figura 1. Topología escenario 1

Fuente: Autoría 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

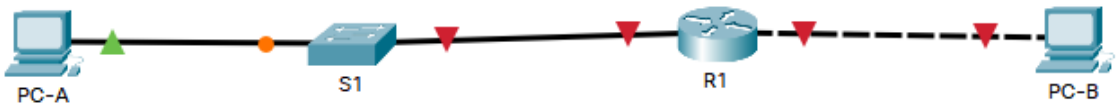
Aspectos básicos/situación

En el desarrollo del caso de estudio usted implementa la topología mostrada en la figura y configura el Router R1 y el swich S1, y los PCs. Con la dirección suministrada realizará el subnetting y cumplirá el requerimiento para la LAN1 (100 host) y la LAN2 (50 hosts).

Parte 1: Construya la Red

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

Figura 2. Topología en Packet Tracer.



Fuente: Autoría 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 192.168.56.0 donde X corresponde a los últimos dos dígitos de su cédula.

Subneteo del rango IP:
Lo primero que se debe hacer en el caso de que se conoce la topología con los requisitos de cada una de las subredes es proceder a subnetear el rango asignado, el mismo nos queda de la siguiente manera:

La red en general está formada por 2 subredes:

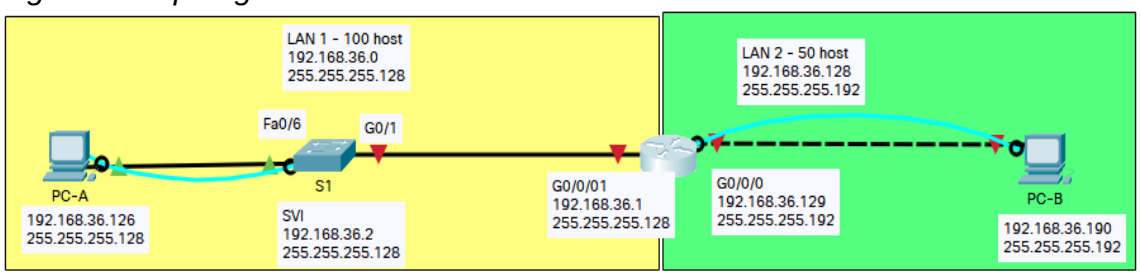
Tabla 1. Asignación de subredes.

RED	N° IP	Dirección de red	Mascara de subred	/	1re IP	ultima IP	Broadcast.	N° HOST
LAN 1	100	192.168.56.0	255.255.255.128	25	192.168.56.1	192.168.56.126	192.168.36.127	126
LAN 2	50	192.168.56.128	255.255.255.192	26	192.168.56.129	192.168.56.190	192.168.56.191	62

Fuente: Autoría propia.

Como ya se conocen los rangos IP para cada una de las subredes se puede proceder a realizar la asignación de la IP correspondiente a cada una de las interfaces que intervienen, este queda como se indica a continuación:

Figura 3. Topología escenario 1.



Fuente: Autoría propia.

Se procede a realizar la asignación a cada interfaz y a realizar las primeras configuraciones a cada uno de los dispositivos.

Tabla 2. Configuración básica y asignación de direcciones IP.

Tarea	Especificación.
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 Int g0/0/1 Ip addres 192.168.56.1 255.255.255.128
R1 G0/0/0	Primera dirección de host de la subred LAN2 Int g0/0/0 Ip addres 192.168.56.129 255.255.255.192
S1 SVI	Segunda dirección de host de la subred LAN1 Int vlan 1 Ip address 192.168.56.2 255.255.255.128
PC-A	Última dirección de host de la subred LAN1 IP: 192.168.56.126 Mask: 255.255.255.128
PC-B	Última dirección de host de la subred LAN2

	IP: 192.168.56.190 Mask: 255.255.255.192

Fuente: Autoría 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:

Como siguiente paso se procede a realizar la configuración básica de R1 con el fin de agregar seguridad al mismo y poder configurar sus interfaces, el proceso es indicado a continuación:

Tabla 3. Configuración básica R1.

Tarea	Especificación
Desactivar la búsqueda DNS	Se procede a desactivar la búsqueda DNS aplicando el siguiente comando en el router R1. No ip domain lookup
Nombre del router	Se agrega el nombre al dispositivo con el fin de poderlo identificar de una manera sencilla hostname R1
Nombre de dominio	ccna-lab.com ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXECprivilegiado	Se debe cifrar las contraseñas: Ciscoenpass

	enable secret ciscoenpass
Contraseña de acceso a la consola	Se procede a configurar las líneas de consola empleando la contraseña: Ciscoconpass line console 0 password ciscoconnpass login
Establecer la longitud mínima para lascontraseñas	Se establece una condición con el fin de que el tamaño mínimo de las contraseñas sea de 10 caracteres: security password min-length 10
Crear un usuario administrativo en la base dedatos local	Nombre de usuario: **admin** Password: **admin1pass** username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	Se procede a configurar las líneas vty 0 15 line vty 0 15 login local
Configurar VTY solo aceptando SSH	transport input ssh login
Cifrar las contraseñas de texto no cifrado	De esta manera se logra que las contraseñas permanezcan encriptadas y que permanezcan ocultas. Service password-encyption
Configure un MOTD Banner	Este mensaje aparece cada vez que se ingresa a un dispositivo, es un mensaje persuasivo.

	banner motd % Se prohíbe el acceso no autorizado.%
Configurar interfaz G0/0/0	Establezca la descripción Establece la dirección IPv4. Activar la interfaz. Config t Int g0/0/0 Ip address 192.168.36.129 255.255.255.192
Configurar interfaz G0/0/1	Establezca la descripción Establece la dirección IPv4. Activar la interfaz. Configure terminal Interface g0/0/01 Ip address 192.168.36.1 255.255.255.128
Generar una clave de cifrado RSA	Módulo de 1024 bits crypto key generate rsa general-keys modulus 1024

Fuente: Autoría propia.

Paso 2: Se verifica a ingresar la configuración del dispositivo tal como se muestra a continuación:

Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#username admin secret admin1pass
R1(config)#line vty 0 15

```
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#banner motd %prohibido el acceso no autorizado%
```

Paso 3: Se procede a realizar la configuración de las interfaces de este dispositivo:

```
R1(config)#int g0/0/1
R1(config-if)#ip address 192.168.56.1 255.255.255.128
R1(config-if)#no shutdown
R1(config-if)#

R1(config-if)#int g0/0/0
R1(config-if)#ip address 192.168.56.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#

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

Paso 4: Las tareas de configuración de **S1** incluyen lo siguiente:

Tabla 4. Configuración básica S1.

Tarea	Especificación
Desactivar la búsqueda DNS.	Se debe desactivar la búsqueda DNS de esta manera se ahorra recursos: No ip domain lookup
Nombre del switch	Se agrega el nombre a nuestro dispositivo S1 con el fin de poderlo identificar, por lo general en redes más grandes se emplean nombres más extensos para identificarlos con seguridad. hostname S1

Nombre de dominio	**ccna-lab.com** ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Se crea la contraseña de EXCEC privilegiado y se cifra Ciscoenpass enable secret ciscoenpass
Contraseña de acceso a la consola	**Ciscoconpass** line console 0 password ciscoconpass login
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass** username admin secret admin1pass
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	line vty 0 15 login local
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	transport input ssh
Cifrar las contraseñas de texto no cifrado	Este comando sirve para cifrar todas las contraseñas que aún no lo han hecho. Service password-encyption
Configurar un MOTD Banner	Se configura el mensaje que aparece en el dispositivo cuando se ingresa al mismo: banner motd % Se prohíbe el acceso no autorizado.%
Generar una clave de cifrado RSA	**Módulo de 1024 bits**

	crypto key generate rsa general-keys modulus 1024
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 conforme la tabla de direccionamiento int vlan 1 description subnet A ip address 192.168.56.2 255.255.255.128
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada conforme a la tabla dedireccionamiento. ip default-gateway 192.168.56.1

Fuente: Autoría propia.

Paso 5: Se procede a realizar la configuración básica del dispositivo S1, tal como se indica en la tabla anterior:

Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin secret admin1pass
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config)#service password-encryption
S1(config)#banner motd %prohibido acceso sin autorizacin%
S1(config)#crypto key generate rsa general-keys modulus 1024

Paso 6: Se procede a realizar la de las interfaces del S1:

```
S1(config)#
S1(config)#int vlan 1
S1(config-if)#description subnet A
S1(config-if)#ip address 192.168.10.2 255.255.255.128
S1(config-if)#ip default-gateway 192.168.10.1
```

Paso 7: Configurar los equipos PC.

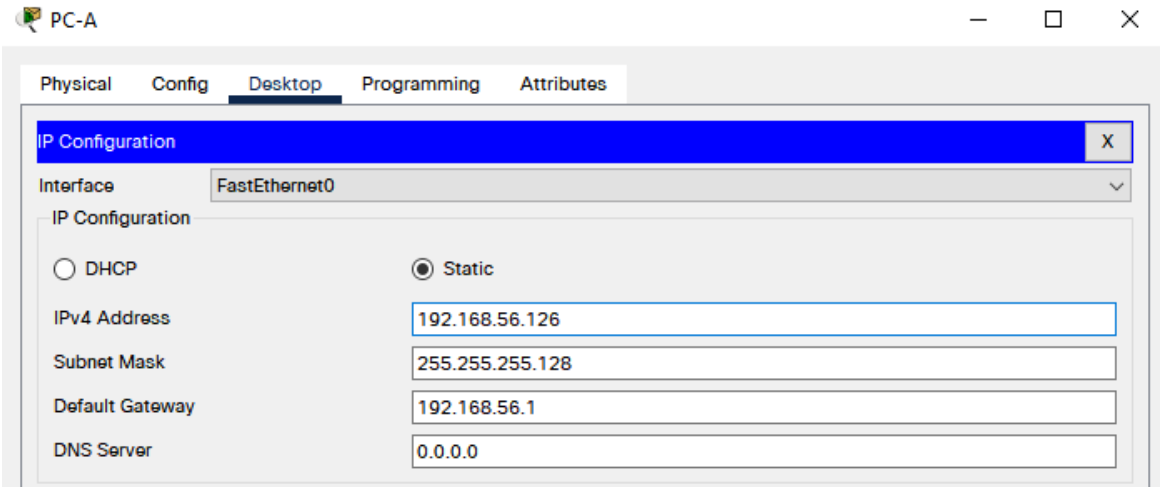
Configure los equipos host PC-A y PC-B conforme a la tabla de direccionamiento, registre las configuraciones de red del host con el comando **ipconfig /all**.

Tabla 5. Configuración PC-A.

PC-A Network Configuration	
Descripción	PC-A
Dirección física	
Dirección IP	192.168.56.126
Máscara de subred	255.255.255.128
Gateway predeterminado	192.168.56.1

Fuente: Autoría propia.

Figura 4. Configuración PC-A



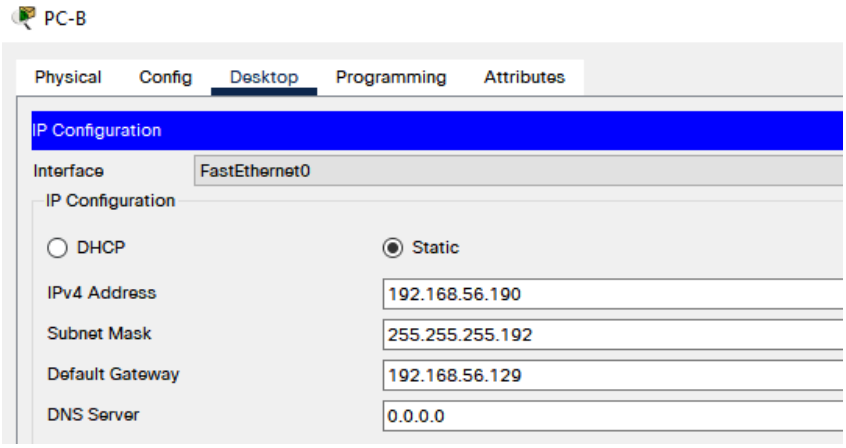
Fuente: Autoría propia.

Tabla 6. Configuración PC-B

PC-B Network Configuration	
Descripción	PC-B
Dirección física	
Dirección IP	192.168.56.190
Máscara de subred	255.255.255.192
Gateway predeterminado	192.168.56.129

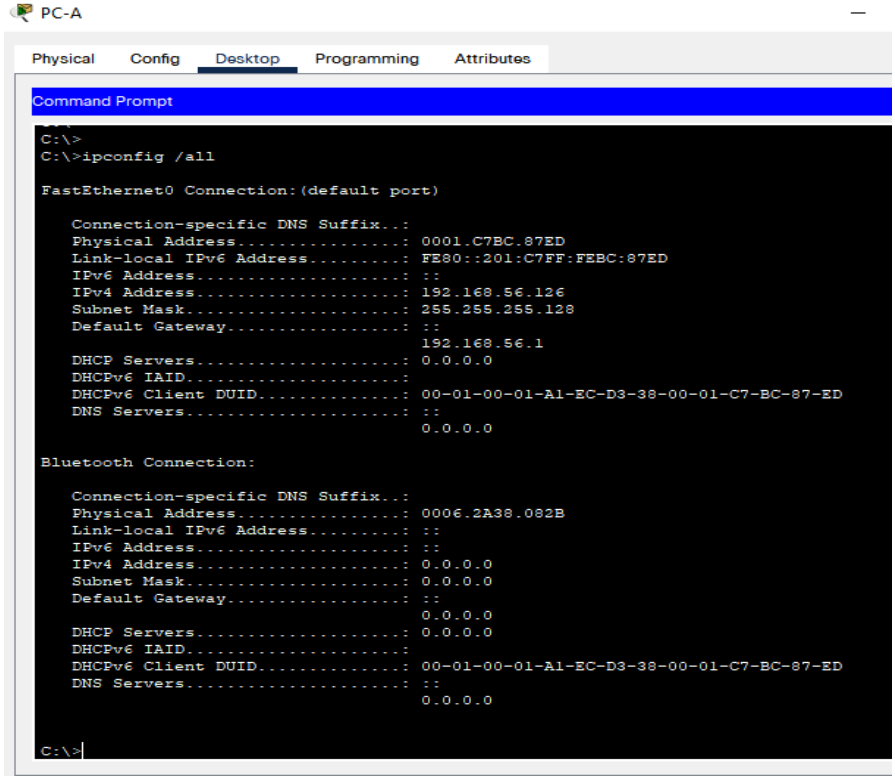
Fuente: Autoría propia.

Figura 5. Configuración PC-B



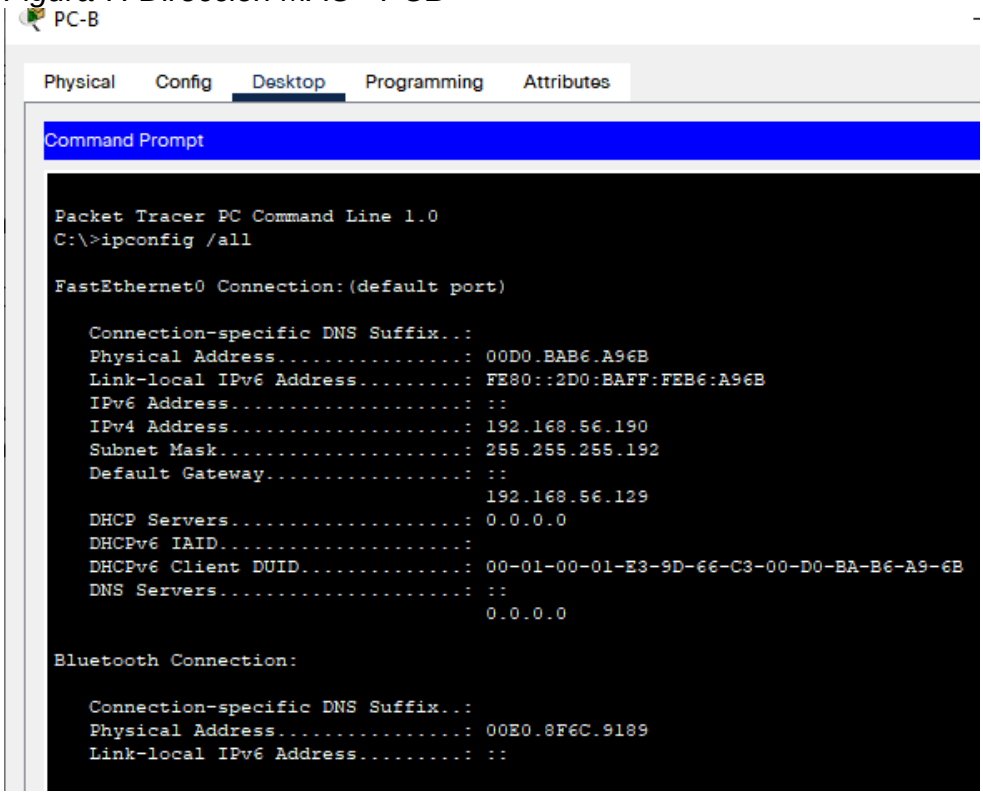
Fuente: Autoría propia.

Figura 6. MAC PC-A



Fuente: Autoría propia.

Figura 7. Dirección MAC - PCB



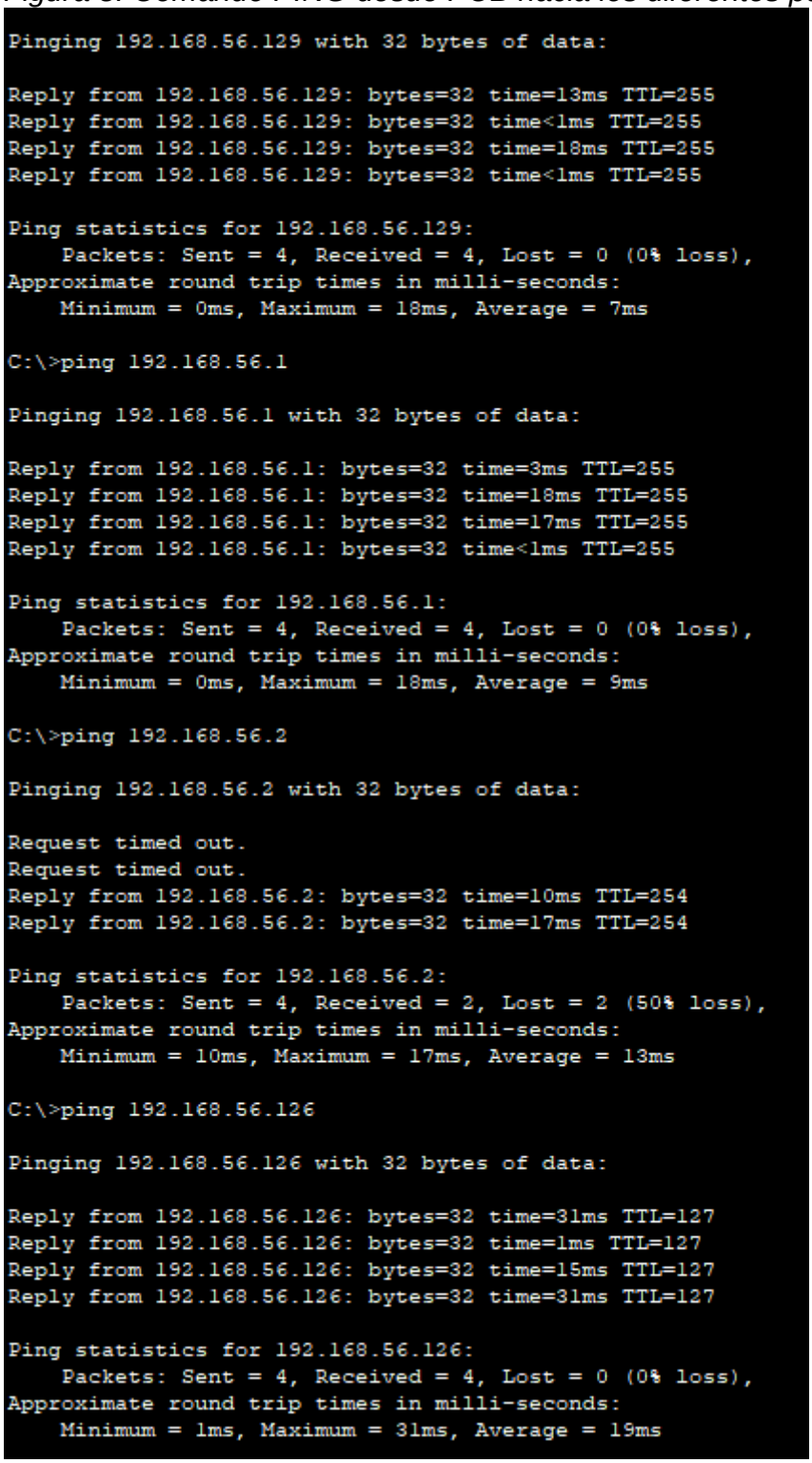
Fuente: Autoría propia.

Paso 8: Se procede a realizar las respectivas proveas de conectividad:

Desde PCA hacia los diferentes puertos de la red.

Se procede a realizar la verificación de lo hecho hasta el momento, para nuestro caso se emplea el comando PING desde PCB hacia los diferentes puntos de la red.

Figura 8. Comando PING desde PCB hacia los diferentes puntos de la red.



```
Pinging 192.168.56.129 with 32 bytes of data:

Reply from 192.168.56.129: bytes=32 time=13ms TTL=255
Reply from 192.168.56.129: bytes=32 time<1ms TTL=255
Reply from 192.168.56.129: bytes=32 time=18ms TTL=255
Reply from 192.168.56.129: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.56.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 7ms

C:\>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:

Reply from 192.168.56.1: bytes=32 time=3ms TTL=255
Reply from 192.168.56.1: bytes=32 time=18ms TTL=255
Reply from 192.168.56.1: bytes=32 time=17ms TTL=255
Reply from 192.168.56.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 9ms

C:\>ping 192.168.56.2

Pinging 192.168.56.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.56.2: bytes=32 time=10ms TTL=254
Reply from 192.168.56.2: bytes=32 time=17ms TTL=254

Ping statistics for 192.168.56.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 17ms, Average = 13ms

C:\>ping 192.168.56.126

Pinging 192.168.56.126 with 32 bytes of data:

Reply from 192.168.56.126: bytes=32 time=31ms TTL=127
Reply from 192.168.56.126: bytes=32 time=1ms TTL=127
Reply from 192.168.56.126: bytes=32 time=15ms TTL=127
Reply from 192.168.56.126: bytes=32 time=31ms TTL=127

Ping statistics for 192.168.56.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 31ms, Average = 19ms
```

Fuente: Autoría propia.

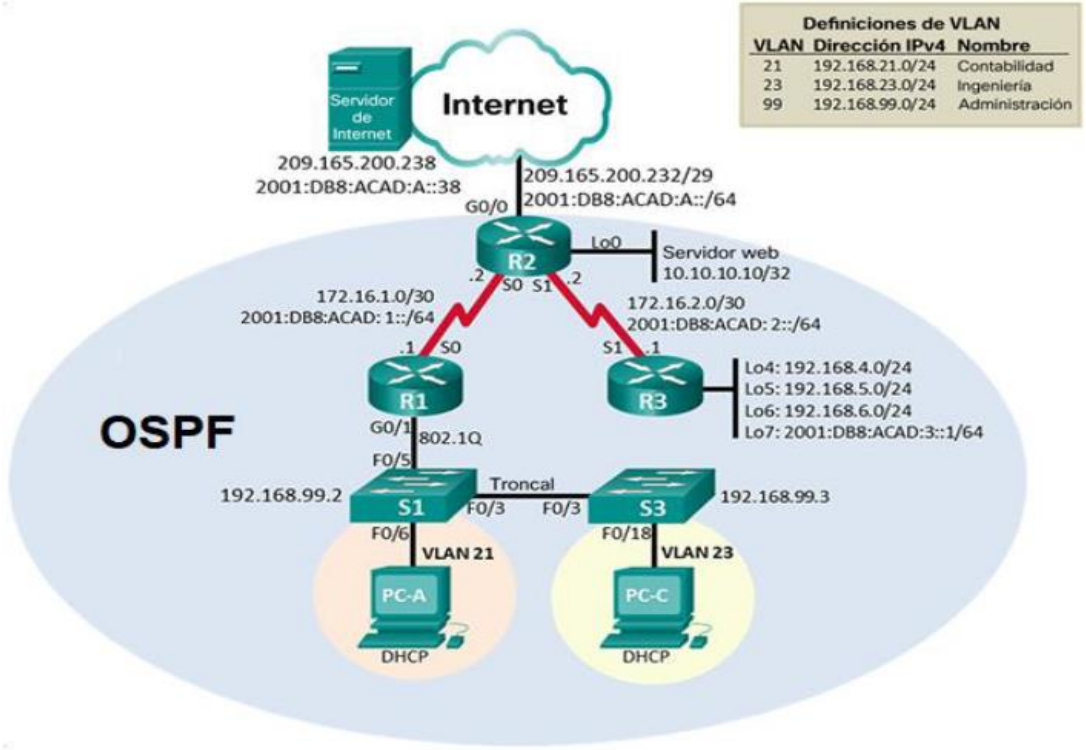
DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

2. 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 RIPv2, 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.

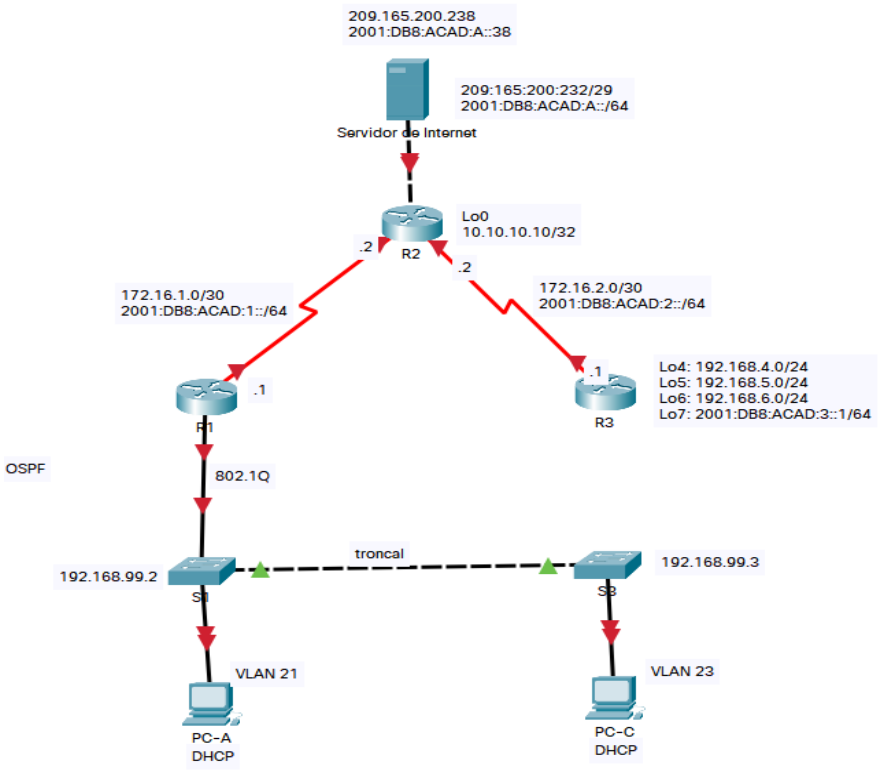
Topología

Figura 9. Topología Escenario 2.



Fuente: Guía de actividades.

Figura 10. Dispositivos conectados simulador.



Fuente: Autoría 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.

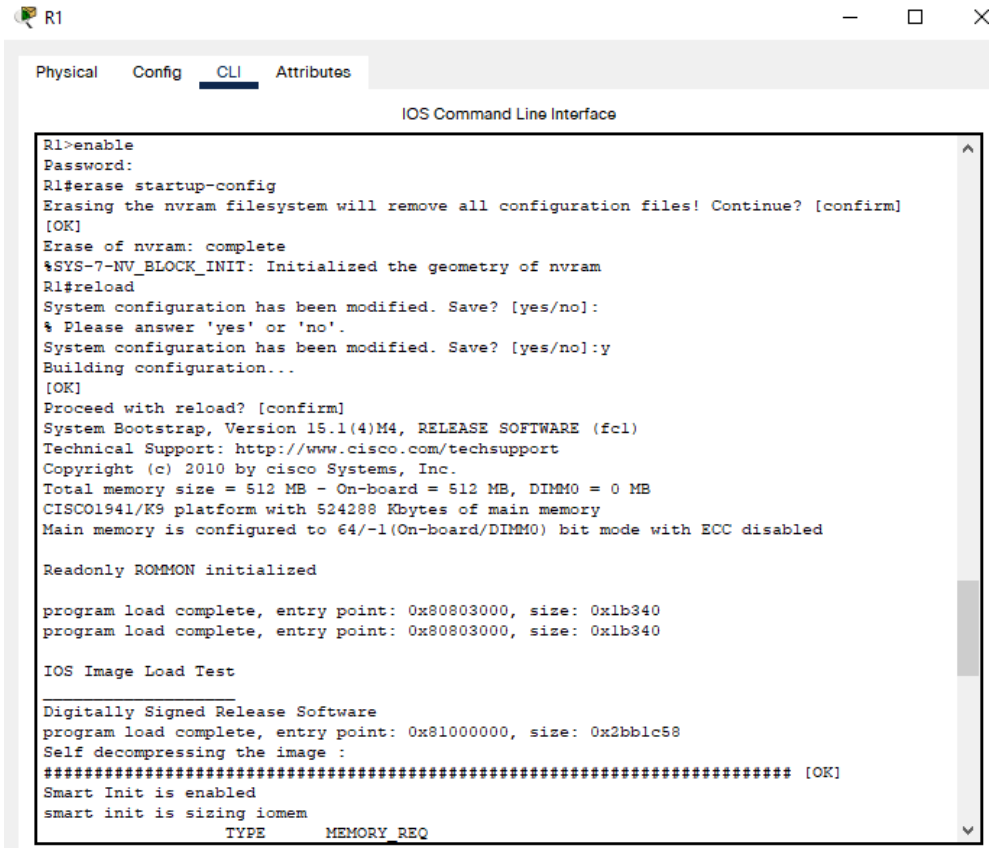
Tabla 7. Inicialización de dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	erase startup-config
Volver a cargar todos los routers	Reload

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	erase startup-config delete vlan.dat
Volver a cargar ambos switches	Se reinicia el dispositivo. Reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	show flash

Fuente: Autoría propia.

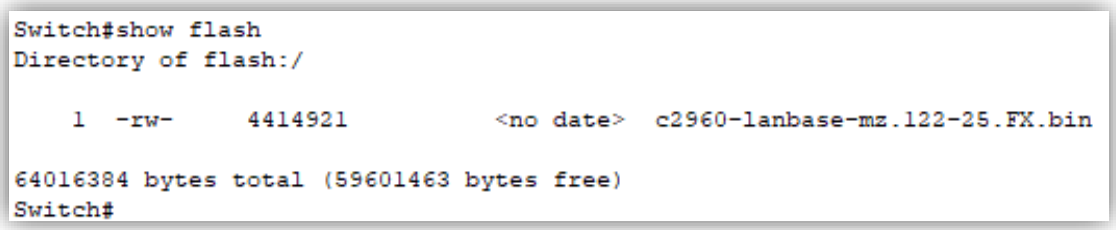
Figura 11. Inicialización dispositivos.



Fuente Autoría Propia.

Se verifica que la base de datos de la VLAN no esté en el dispositivo, en éste caso se observa que solo se tiene el archivo de configuración, el vlan.dat ya no aparece.

Figura 12. Show Flash



Fuente: Autoría propia.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

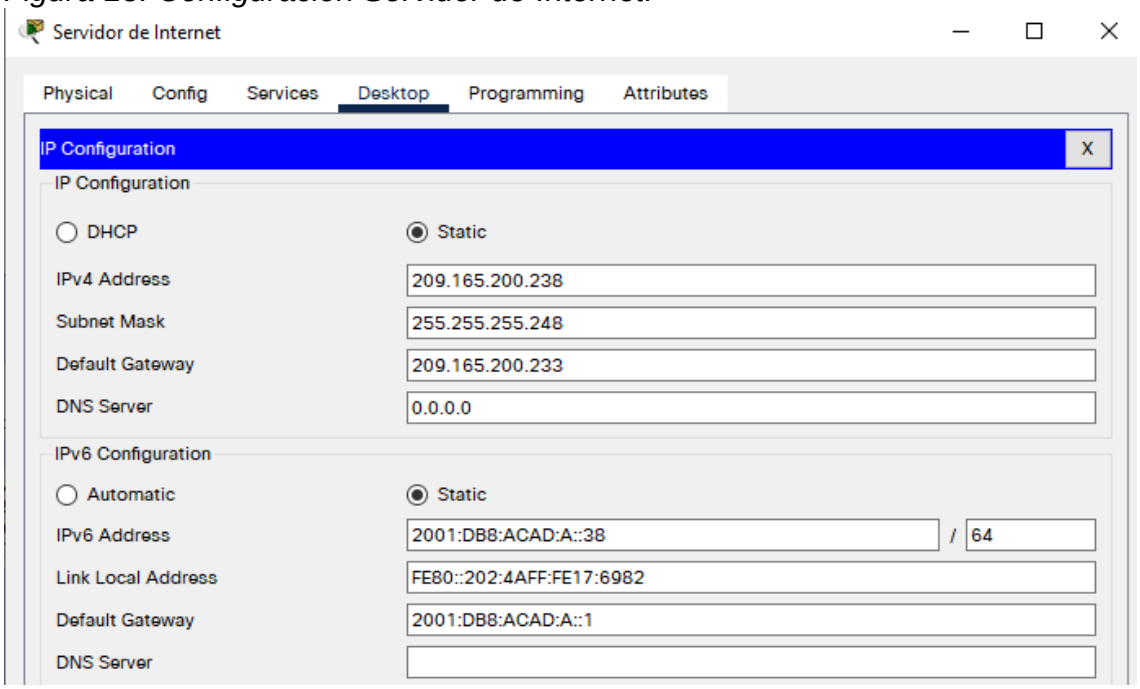
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Tabla 8. Configuración IP PC-internet

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

Fuente: Autoría propia.

Figura 13. Configuración Servidor de Internet.



Fuente: Autoría propia.

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. Configuración básica R1

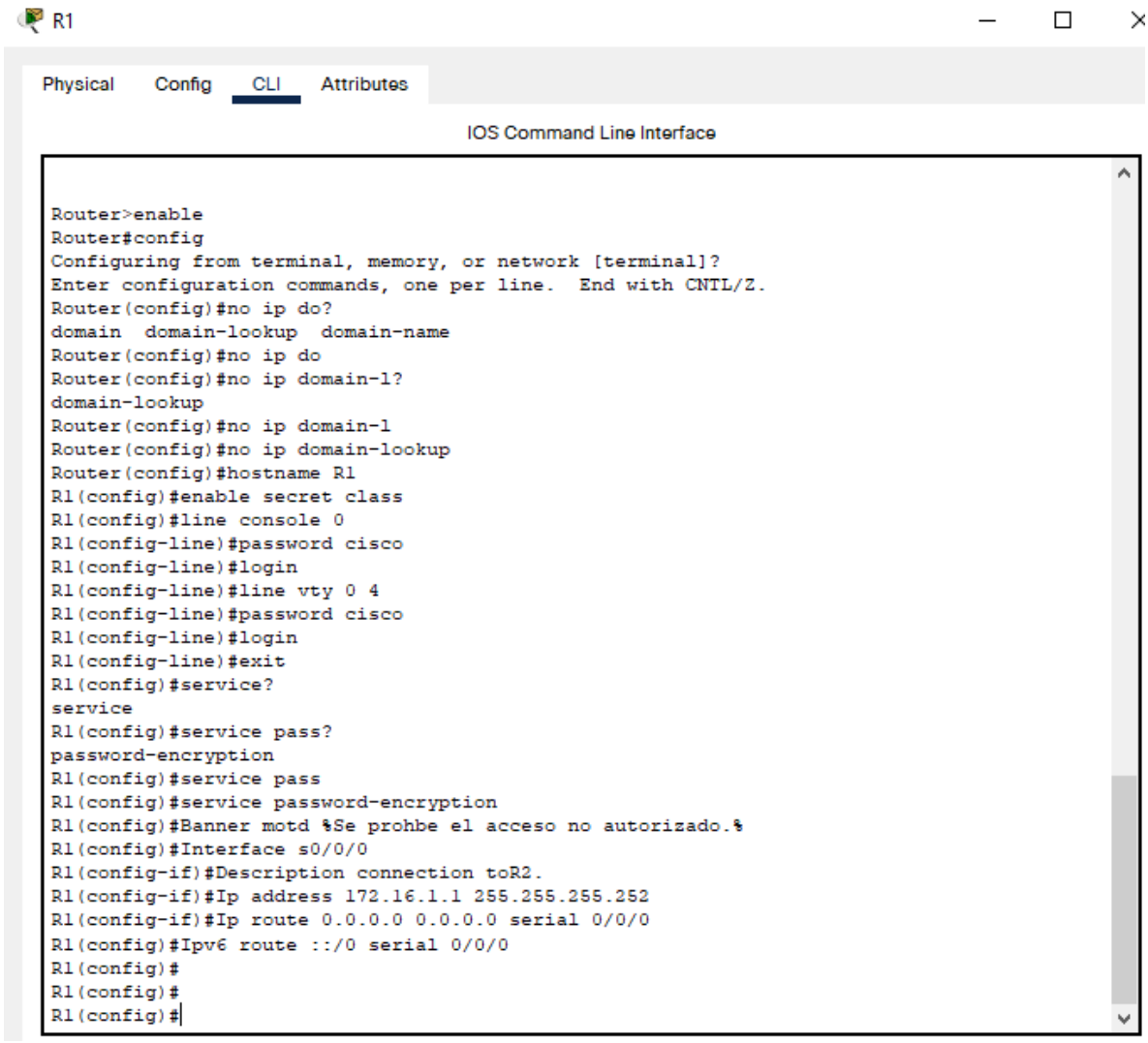
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del router	Hostname R1
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line console 0 Password cisco Login

Contraseña de acceso Telnet	Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encyption
Mensaje MOTD	Banner 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 Interface s0/0/0 Description connection toR2. Ip address 172.16.1.1 255.255.255.252
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0 Ip route 0.0.0.0 0.0.0.0 serial 0/0/0 Ipv6 route ::/0 serial 0/0/0

Fuente: Autoría propia.

Nota: Todavía no configure G0/1.

Figura 14. Configuración básica R1.



Fuente: Autoría propia.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 10. Configuración básica R2

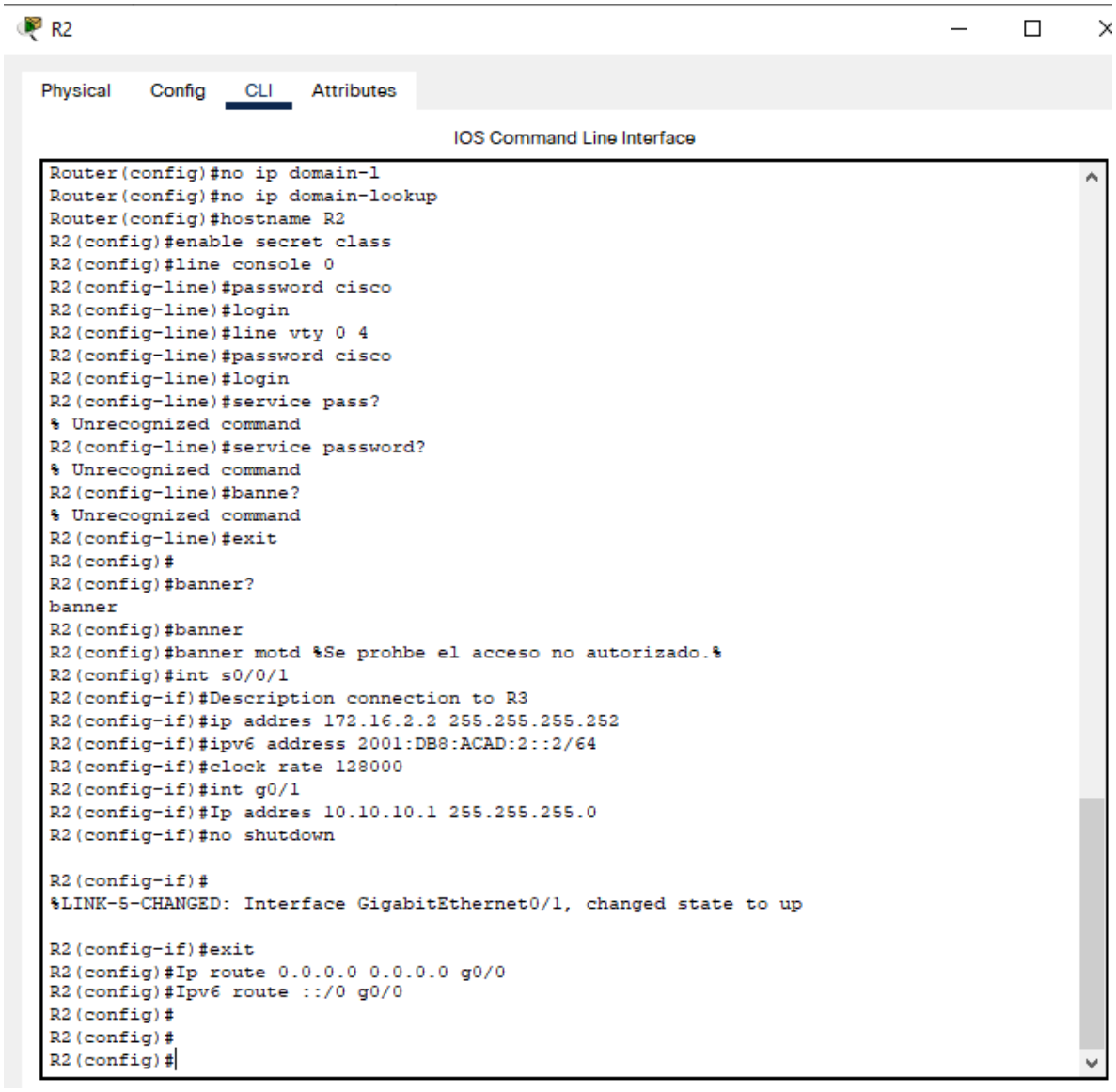
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del router	Hostname R2
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line console 0 Password cisco Login
Contraseña de acceso Telnet	Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encyption
Habilitar el servidor HTTP	ip http server el comendo indicado el simulador no lo soporta, es por esto que se opta por montar un servidor WEB. R2 (config)# R2 (config)#ip http server % Invalid input detected at ´^´
Mensaje MOTD	Banner 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 Interface s0/0/0 Description connection to R1 ip addres 172.16.1.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:1::2/64
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 Interface s0/0/1 Description connection to R3 ip addres 172.16.2.2 255.255.255.252 ipv6 address 2001:DB8:ACAD:2::2/64 clock rate 128000

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 Interface G0/0 Description connection to Internet ip addres 209.165.200.233 255.255.255.248 ipv6 address 2001:DB8:ACAD:A::1/64
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4. Int g0/1 Ip addres 10.10.10.1 255.255.255.0 No shutdown
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. Ip route 0.0.0.0 0.0.0.0 g0/0 Ipv6 route ::/0 g0/0

Fuente: Autoría propia.

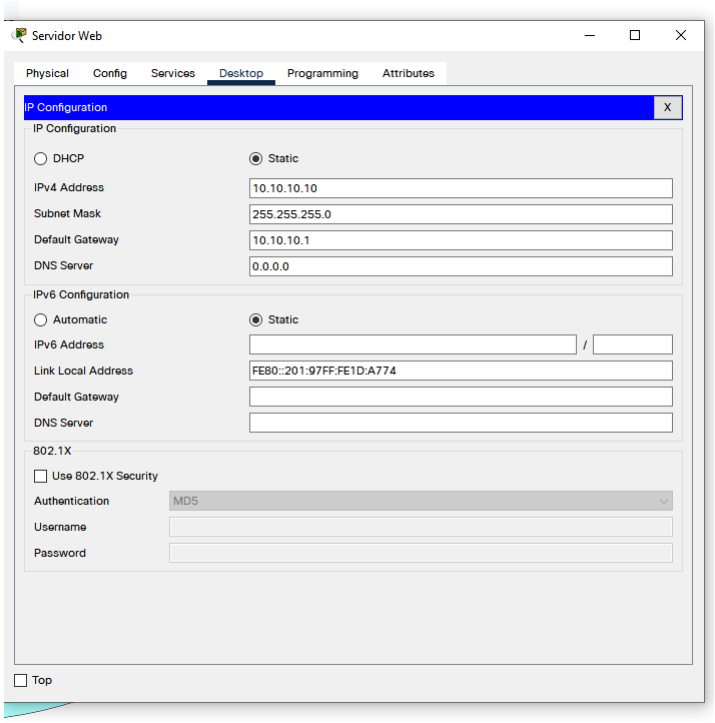
Figura 15. Configuración básica R2.



Fuente Autoría propia.

- Configuración del servidor WEB.

Figura 16. Configuración IP Servidor WEB



Fuente: Autoría propia.

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 11. Configuración básica R3

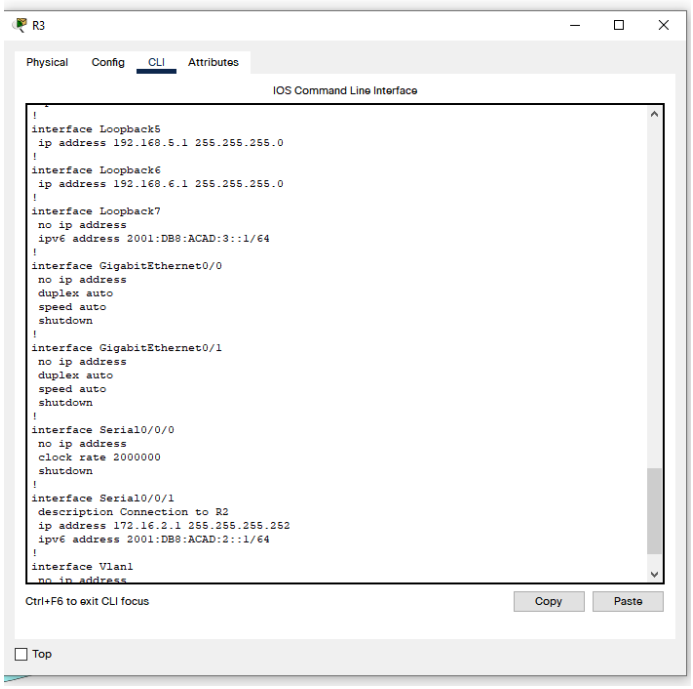
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del router	Hostname R3
Contraseña de exec privilegiado cifrada	Enable secret class

Contraseña de acceso a la consola	Line console 0 Password cisco Login
Contraseña de acceso Telnet	Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encyption
Mensaje MOTD	Banner 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 Interface s0/0/1 Description connection to R2 Ip address 172.16.2.1 255.255.255.252 Ipv6 address 2001:DB8:ACAD:2::1/64
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Interface loopback4 Ip address 192.168.4.1 255.255.255.0
Interfaz loopback 5	Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred. Interface loopback5 Ip address 192.168.5.1 255.255.255.0

Interfaz loopback 6	Establezca la dirección Ipv4. Utilizar la primera dirección disponible en la subred. Interface loopback6 Ip address 192.168.6.1 255.255.255.0
Interfaz loopback 7	Establezca la dirección Ipv6. Consulte el diagrama de topología para conocer la información de direcciones. Interface loopback7 Ip address 192.168.7.1 255.255.255.0
	interface Loopback4 ip address 192.168.4.1 255.255.255.0 ! interface Loopback5 ip address 192.168.5.1 255.255.255.0 ! interface Loopback6 ip address 192.168.6.1 255.255.255.0 ! interface Loopback7 no ip address ipv6 address 2001:DB8:ACAD:3::1/64
Rutas predeterminadas	ip route 0.0.0.0 0.0.0.0 Serial0/0/1 ipv6 route ::/0 Serial0/0/1

Fuente: Autoría propia.

Figura 17. Configuración R3 - loopback



Fuente: Autoría propia.

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

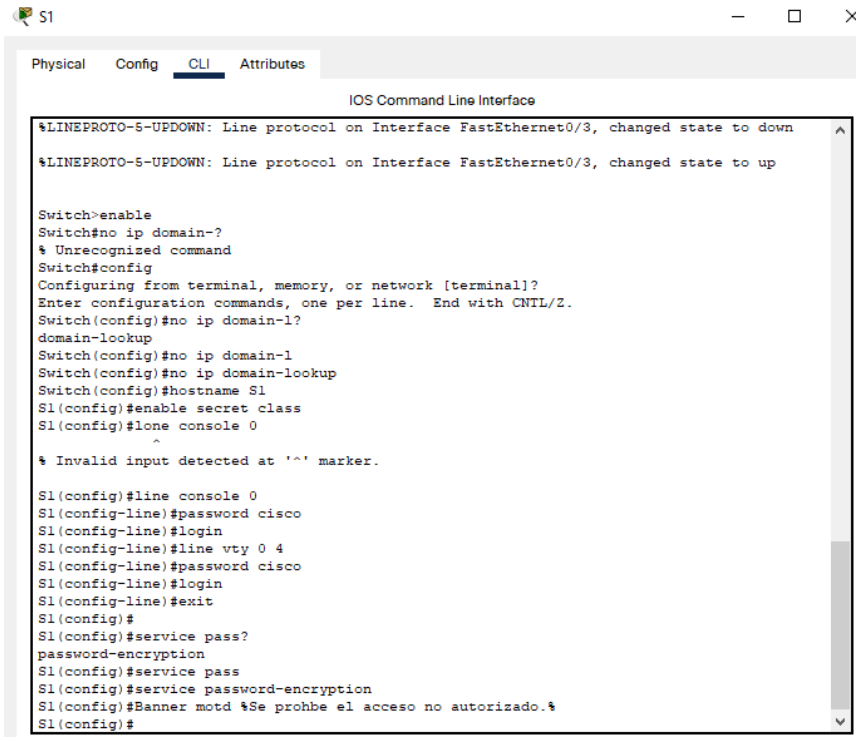
Tabla 12. Configuración contraseñas S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del switch	Hostname S1
Contraseña de exec privilegiado cifrada	Enable secret class

Contraseña de acceso a la consola	Line console 0 Password cisco Login
Contraseña de acceso Telnet	Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encyption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Fuente: Autoría propia.

Figura 18. Configuración básica S1.



Fuente: Autoría propia.

Paso 6: Configurar el S3

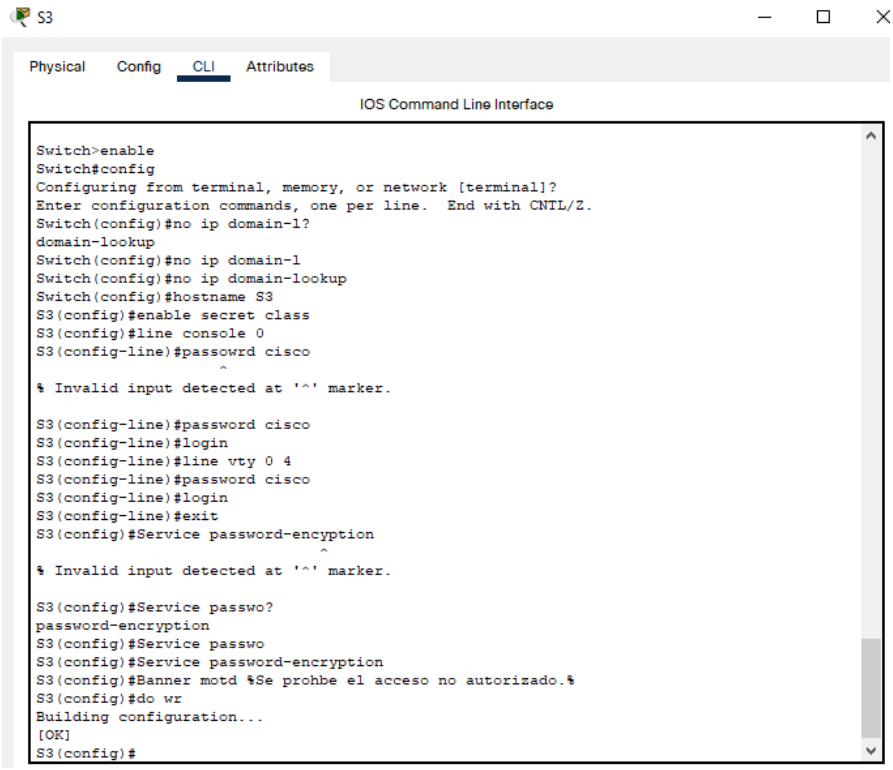
La configuración del S3 incluye las siguientes tareas:

Tabla 13. Configuración contraseñas S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	No ip domain lookup
Nombre del switch	Hostname S3
Contraseña de exec privilegiado cifrada	Enable secret class
Contraseña de acceso a la consola	Line console 0 Password cisco Login
Contraseña de acceso Telnet	Line vty 0 4 Password cisco Login
Cifrar las contraseñas de texto no cifrado	Service password-encyption
Mensaje MOTD	Banner motd %Se prohíbe el acceso no autorizado.%

Fuente: Autoría propia.

Figura 19. Configuración básica S3.



Fuente: Autoría propia.

Paso 7: Verificar la conectividad de la red

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

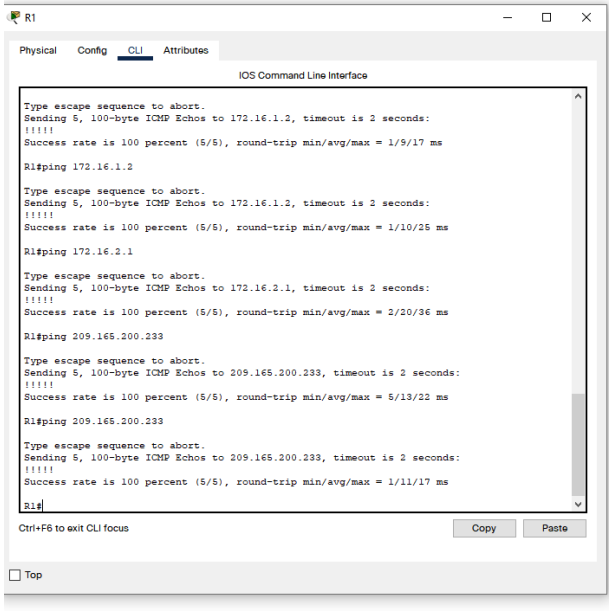
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 14. Verificación PING desde R1,R2,PC internet.

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	Exitoso
R2	R3, S0/0/1	172.16.2.1	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.233	Exitoso

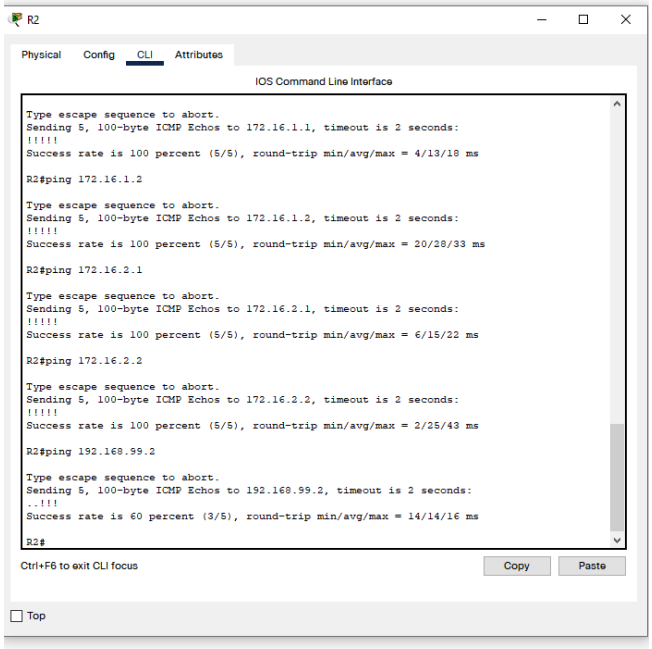
Fuente: Autoría propia.

Figura 20. Comando PING desde el R1 hacia los diferentes puntos de la red.



Fuente: Autoría propia.

Figura 21. Comando PING desde el R2 hacia los diferentes puntos de la red.



Fuente: Autoría propia.

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

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:

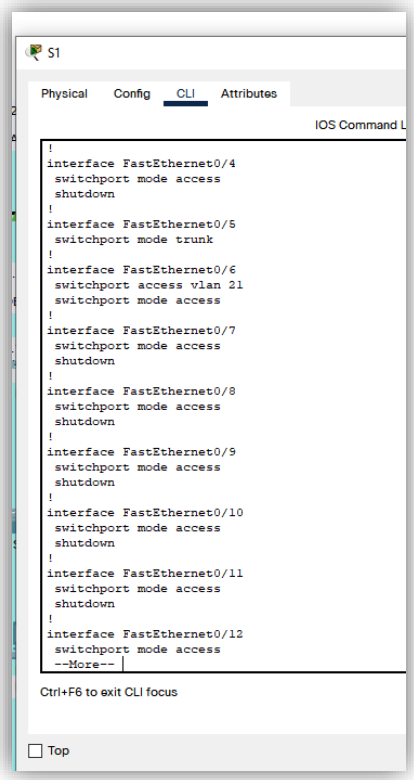
Tabla 15. Configuración S1 interfaces.

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 Interface fa0/6 Interface vlan 21 Switchport mode Access
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 Interface vlan 99 Ip address 192.168.99.2 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa interface FastEthernet0/3 switchport mode trunk switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa interface FastEthernet0/5 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range fastethernet 1-2, fa0/4, fa0/6-24, g1/1-2 switchport mode access
Asignar F0/6 a la VLAN 21	Emplea el siguiente comando interface F0/6 switchport mode access switchport access vlan 21
Apagar todos los puertos sin usar	interface range F0/1-2, F0/4, F0/7-24, G0/1-2 shutdown

Fuente: Autoría propia.

Figura 22. Configuración interfaces S1



.

Fuente: Autoría propia.

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

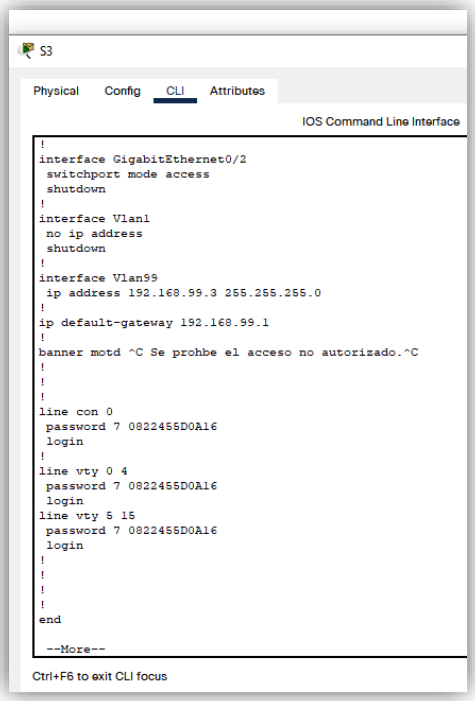
Tabla 16. Configuración S3 interfaces.

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. interface FastEthernet 0/18 switchport mode access switchport access vlan 23
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 Interface vlan 99 Ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa interface FastEthernet0/3 switchport mode trunk switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range int range fa 0/1-2, fa0/4-24, g1/1-2 switchport mode access

Asignar F0/18 a la VLAN 23	interface F0/18 switchport mode access switchport access vlan 23
Apagar todos los puertos sin usar	interface range Fa0/1-2, Fa0/4-17, Fa0/19-24, G0/1-2 shutdown

Fuente: Autoría propia.

Figura 23. Configuración interfaces S3



Fuente: Autoría propia.

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configuración subinterfaces 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 interface GigabitEthernet0/1.21 description Accounting LAN encapsulation dot1Q 21 ip address 192.168.21.1 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz interface GigabitEthernet0/1.23 description Accounting LAN encapsulation dot1Q 23 ip address 192.168.23.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz interface GigabitEthernet0/1.99 description Accounting LAN encapsulation dot1Q 99 ip address 192.168.99.1 255.255.255.0
Activar la interfaz G0/1	interface g0/1 no shutdown

Fuente: Autoría propia.

Figura 24. Configuración sub-interfaz R1

```
interface GigabitEthernet0/1.21
 description Accounting LAN
 encapsulation dot1Q 21
 ip address 192.168.21.1 255.255.255.0
!
interface GigabitEthernet0/1.23
 description Engineering LAN
 encapsulation dot1Q 23
 ip address 192.168.23.1 255.255.255.0
!
interface GigabitEthernet0/1.99
 description Management LAN
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
```

Fuente: Autoría propia.

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 PING desde S1 y S3. Hacia las VLAN.

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	192.168.21.1	Exitoso
S3	R1, dirección VLAN 23	192.168.23.1	Exitoso

Fuente: Autoría propia.

Figura 25. Comando ping desde los switche.

```
S1#ping 192.168.99.1

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

S1#ping 192.168.99.1

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


S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/8 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/20 ms

S3#ping 192.168.23.1

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

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#ping 192.168.21.1

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

S1#ping 192.168.21.1

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

Fuente: Autoría propia.

Parte 4: Configurar el protocolo de routing dinámico OSPF

Paso 1: Configurar OSPF en el R1

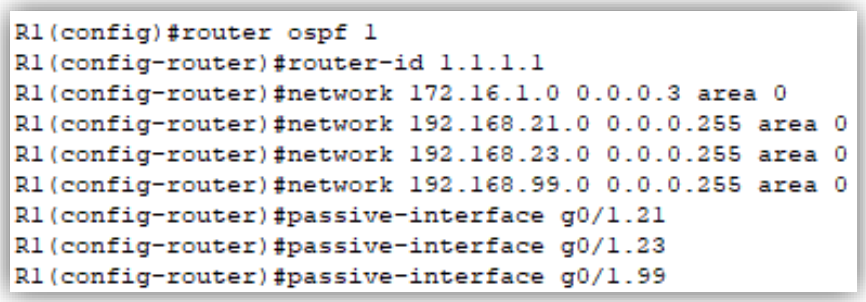
Las tareas de configuración para R1 incluyen las siguientes:

Tabla 19. Configuración protocolo OSPF el R1.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 1.1.1.1
Anunciar las redes conectadas directamente	network 172.16.1.0 0.0.0.3 area 0 network 192.168.21.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

Fuente: Autoría propia.

Figura 26. Configuración de OSPF en el router 1.



Fuente: Autoría propia.

Paso 2: Configurar OSPF en el R2

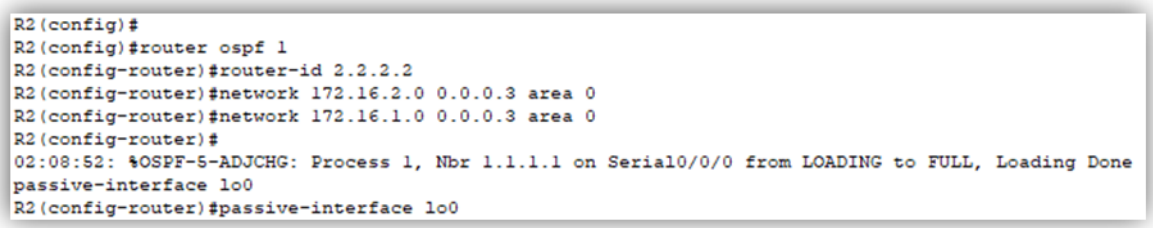
La configuración del R2 incluye las siguientes tareas:

Tabla 20. Configuración protocolo OSPF el R2.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 2.2.2.2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0. network 172.16.2.0 0.0.0.3 area 0 network 172.16.1.0 0.0.0.3 area 0
Establecer la interfaz LAN (loopback) como pasiva	passive-interface lo0 passive-interface g0/1
Desactive la sumarización automática.	no auto-summary

Fuente: Autoría propia.

Figura 27. Configuración de OSPF en el router 2.



Fuente: Autoría propia.

Paso 3: Configurar OSPFv3 en el R3

La configuración del R3 incluye las siguientes tareas:

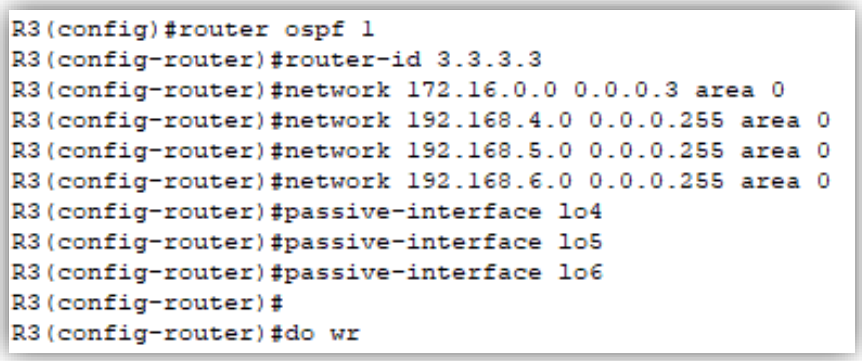
Tabla 21. Configuración protocolo OSPF el R3.

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1(config)#router ospf 1 R1(config-router)#router-id 3.3.3.3
Anunciar redes IPv4 conectadas directamente	network 172.16.2.0 0.0.0.3 area 0 network 192.168.4.0 0.0.0.255 area 0 network 192.168.5.0 0.0.0.255 area 0 network 192.168.6.0 0.0.0.255 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface lo4 passive-interface lo5 passive-interface lo6

Desactive la sumarización automática.	no auto-summary

Fuente: Autoría propia.

Figura 28. Configuración de OSPF en el router 3.



Fuente: Autoría propia.

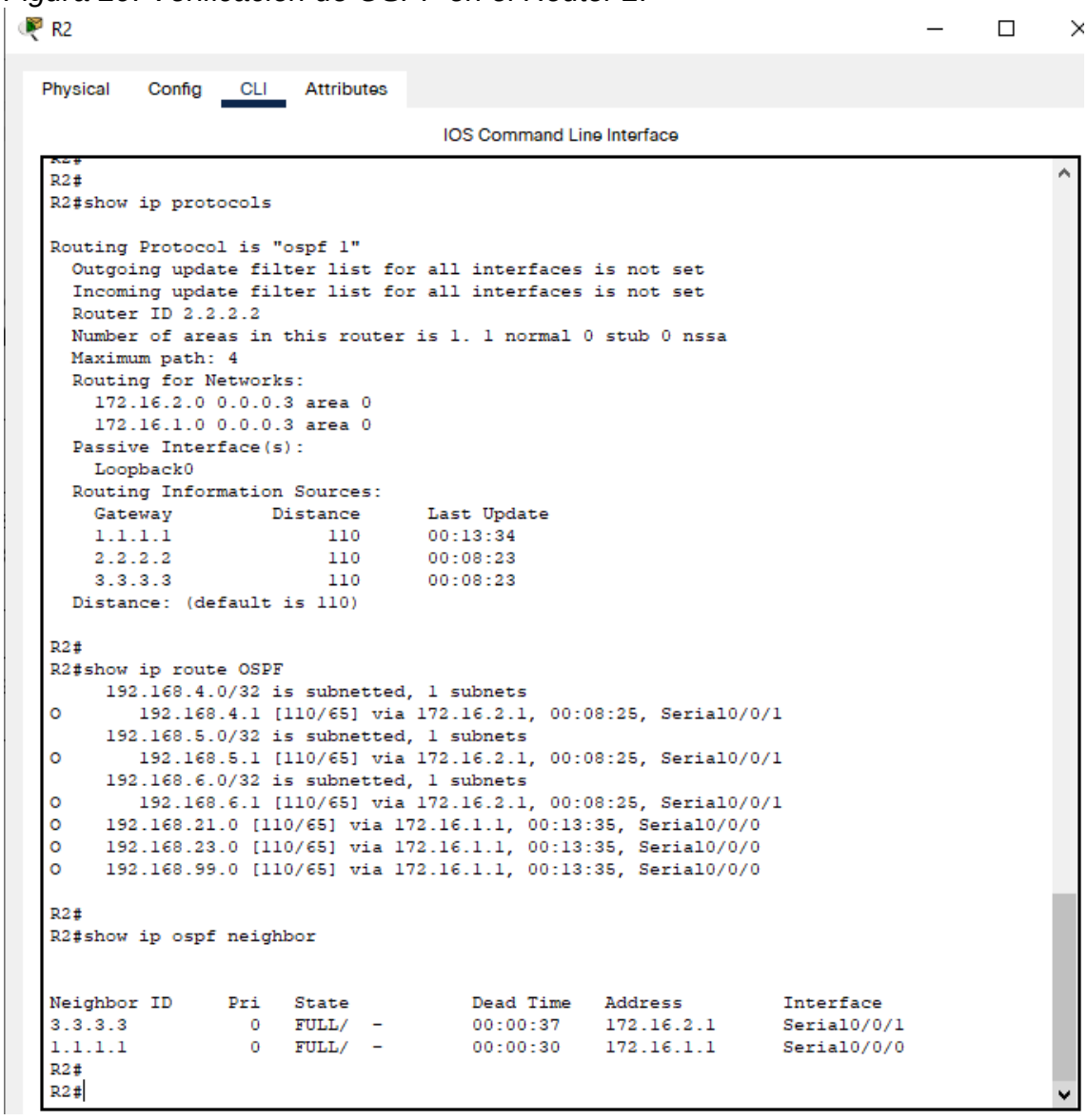
Paso 4: Verificar la información de OSPF

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

Tabla 22. Verifcación de configuración protocolo OSPF el R2.

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?	show ip protocols
¿Qué comando muestra solo las rutas OSPF?	show ip route OSPF
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show ip ospf neighbor

Figura 29. Verificación de OSPF en el Router 2.



Fuente: Autoría propia.

Parte 5: Implementar DHCP y NAT para IPv4

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

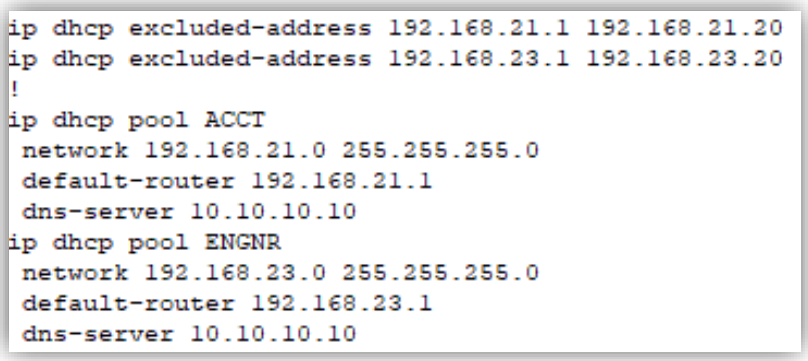
Las tareas de configuración para R1 incluyen las siguientes:

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

Elemento o tarea de configuración	**Especificación**
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
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 ip dhcp pool ACCT network 192.168.21.0 255.255.255.0 default-router 192.168.21.1 dns-server 10.10.10.10 domain-name ccna-sa.com
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 ip dhcp pool ENGNR network 192.168.23.0 255.255.255.0 default-router 192.168.23.1 dns-server 10.10.10.10 domain-name ccna-sa.com

Fuente: Autoría propia.

Figura 30. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23



```
ip dhcp excluded-address 192.168.21.1 192.168.21.20
ip dhcp excluded-address 192.168.23.1 192.168.23.20
!
ip dhcp pool ACCT
 network 192.168.21.0 255.255.255.0
 default-router 192.168.21.1
 dns-server 10.10.10.10
ip dhcp pool ENGNR
 network 192.168.23.0 255.255.255.0
 default-router 192.168.23.1
 dns-server 10.10.10.10
```

Fuente: Autoría propia.

.

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

La configuración del R2 incluye las siguientes tareas:

Tabla 24. Configurar la NAT estática y dinámica en el 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** User webuser privilege 15 secret cisco 12345
Habilitar el servicio del servidor HTTP	ip http server el simulador no soporta este comando.
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local packet tracer no soporta este commando

Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** Ip nat inside source static 10.10.10.10 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	interface g0/0 ip nat outside interface g0/1 ip nat inside
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 Access-list 1 permit 192.168.21.0 0.0.0.255 Access-list 1 permit 192.168.23.0 0.0.0.255 Access-list 1 permit 192.168.4.0 0.0.3.255
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** Ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Se hace el NAT dinamico con el fin de poder hacer la tradución empleando la lista 1. ip nat inside source list 1 pool INTERNET

Fuente: Autoría propia.

Figura 31. Configurar la NAT estática y dinámica en el R2

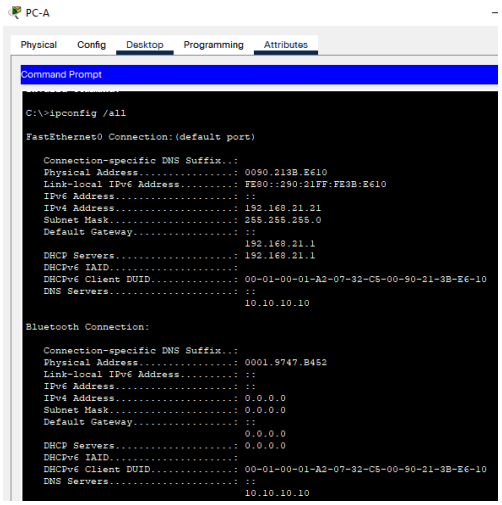
```
ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
ip nat inside source list 1 pool INTERNET
ip nat inside source static 10.10.10.10 209.165.200.237
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
ipv6 route ::/0 GigabitEthernet0/0
!
access-list 1 permit 192.168.21.0 0.0.0.255
access-list 1 permit 192.168.23.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
ip access-list standard ADMIN-MGT
 permit host 172.16.1.1
```

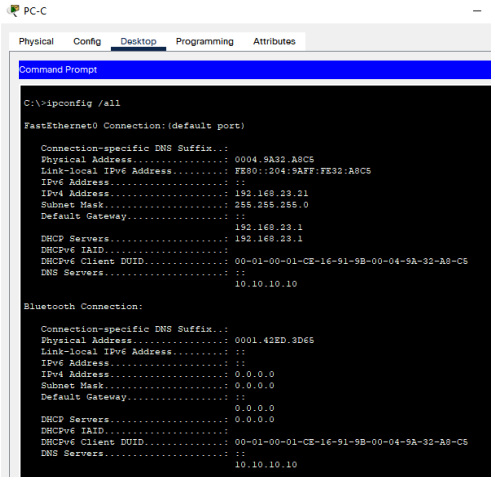
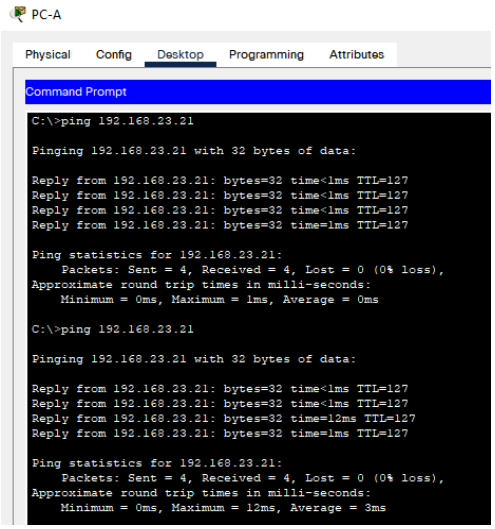
Fuente: Autoría propia.

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.

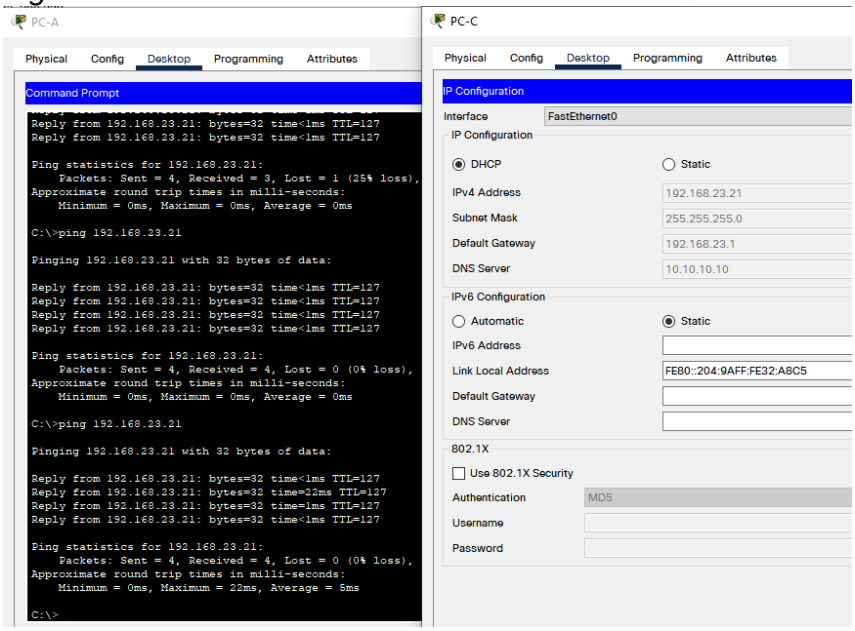
Tabla 25. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	*Figura 32. Configuración DHCP – PC-A*  *Fuente: Autoría propia.*

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	*Figura 33. Configuración DHCP – PC-C*  *Fuente: Autoría propia.*
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	*Figura 34. PING desde PC-A hacia PC-C*  *Fuente: Autoría propia.*
Utilizar un navegador web en la computadora de Internet para acceder al servidor web **(209.165.200.237)** Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	Exitoso.

Fuente: Autoría propia.

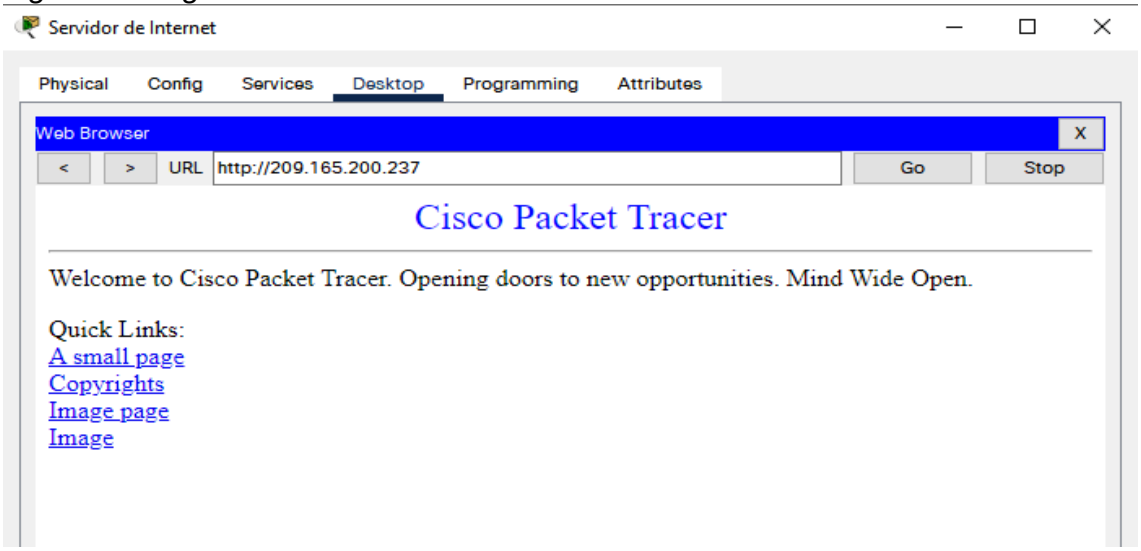
Figura 35. PING desde PC-A hacia PC-C



Fuente: Autoría propia.

- Acceso al servidor web desde el PC Internet

Figura 36. Ingreso WEB desde servidor de internet hacia servidor web.



Fuente: Autoría propia.

Parte 6: Configurar NTP

Tabla 26. 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.	ntp update-calendar
Verifique la configuración de NTP en R1.	Show ntp associations

Fuente: Autoría propia.

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

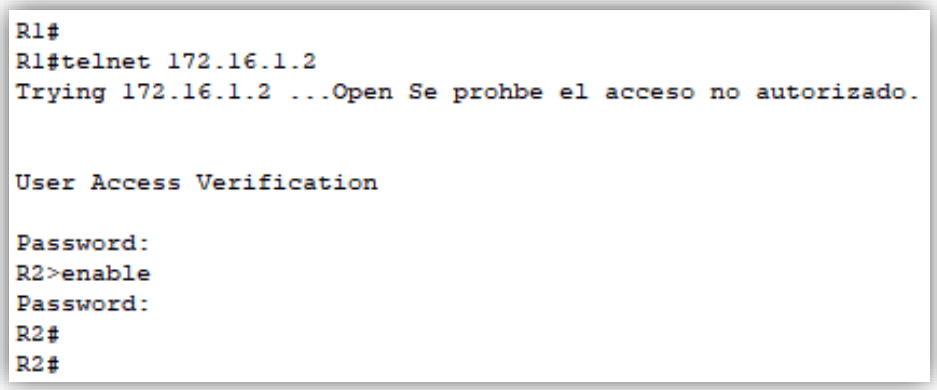
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** Ip Access-list standard ADMIN-MGT Permit host 172.16.1.1 Solo la red de R1 se puede conectar a R2.

Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!^ User Access Verification Password: R2>en Password: R2#

Fuente: Autoría propia.

- Telnet desde RI a R2

Figura 37. Telnet desde R1 hacia R2



Fuente: Autoría propia.

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

Tabla 28. Comando de CLI

Descripción del commando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show access-lists *Figura 30 – show access-lists en R2* R2# R2#show access-lists Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 (6 match(es)) 20 permit 192.168.23.0 0.0.0.255 (2 match(es)) 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (2 match(es)) R2# *Fuente: Autoría propia.*
Restablecer los contadores de una lista de acceso	clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface
¿Con qué comando se muestran las traducciones NAT?	**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. Show ip nat translation Show ip nat statics

¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translations *

Fuente: Autoría propia.

Se verifica las traducciones NAT en R2.

Se observa las traducciones que ha hecho el R2.

Figura 38. Show ip NAT.

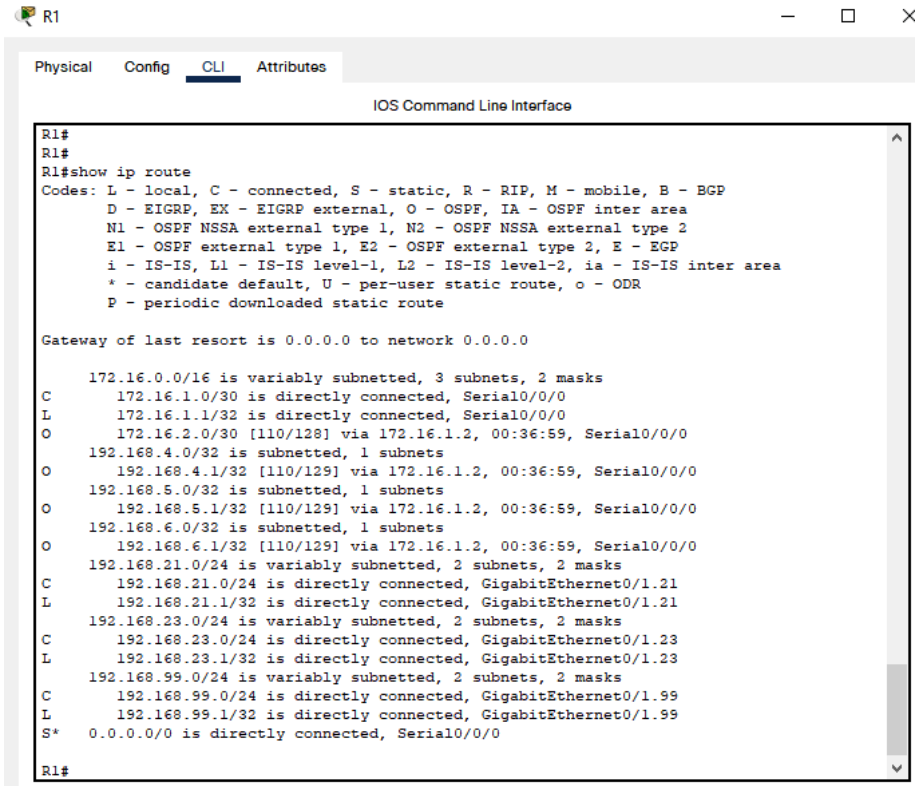
```
R2#
R2#show ip nat tra?
translations
R2#show ip nat tra
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.237   10.10.10.10        ---                ---
tcp 209.165.200.233:1025192.168.21.21:1025 209.165.200.229:80 209.165.200.229:80
tcp 209.165.200.233:1026192.168.21.21:1026 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.233:1027192.168.21.21:1027 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.234:1025192.168.23.21:1025 209.165.200.237:80 209.165.200.237:80
tcp 209.165.200.237:80 10.10.10.10:80     209.165.200.238:1025209.165.200.238:1025
tcp 209.165.200.237:80 10.10.10.10:80     209.165.200.238:1026209.165.200.238:1026

R2#
```

Fuente: Autoría propia.

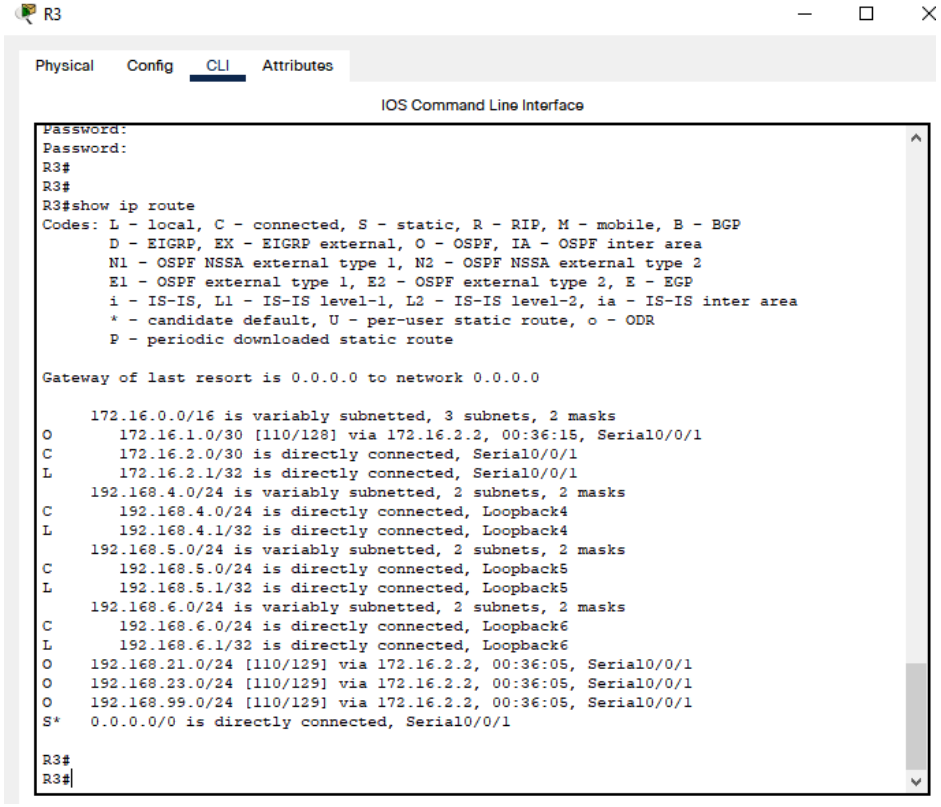
Se procede a verificar las rutas que por medio del protocolo OSPF tienen aprendidos los dispositivos, los resultados con los siguientes:

Figura 39. Show ip route en R1.



Fuente: Autoría propia.

Figura 40. Show Ip Route en R3.



Fuente: Autoría propia.

CONCLUSIONES

Luego de realizar el proceso de configuración se pudo verificar que existe total conectividad dentro de las redes configuradas, se comprende el proceso de desarrollo e implementación de la red aplicando para ello comandos específicos para cada una de las situaciones.

El material que se suministra para el desarrollo de la actividad es muy completo, igualmente el acompañamiento del tutor fue la adecuada para el desarrollo de cada una de las actividades. El simulador de PACKET TRACER se convirtió en la herramienta fundamental para el desarrollo de la actividad.

Gracias a VLSM se aplica el direccionamiento de las 2 redes, cada una ajustada exactamente a las necesidades reales de las mismas.

Se comprendió el funcionamiento de cada uno de los protocolos de enrutamiento dentro de la red, las posibilidades que cada uno de ellos tiene y las diferentes alternativas en las cuales es conveniente su configuración.

Es de vital importancia documentar los pasos desarrollados para la configuración de cada uno de los aspectos de la red y en cada uno de los dispositivos, lo cual permitió y posibilitó en gran medida el encontrar errores de configuración. La red es totalmente funcional.

BIBLIOGRAFÍA

ANDREW S. Tanenbaum (2003). Redes de Computadoras (Cuarta Edicion). Mexico. PEARSON Prentice Hall.

ASOCIACION AMERICANA DE PSICOLOGOS. Referencias Bibliograficas según normas A.P.A [En Linea] Disponible en: http://www.slideshare.net/anafenech/modelo-apa-bibliografia [2014, 22 de Junio].

CISCO SYSTEMS INC. MÓDULO DE ESTUDIO CCNA EXPLORATION 4.0. Conceptos y protocolos de enrutamiento. [Documento PDF en línea]. Disponible en: http://www.mediafire.com/view/5y052miul2vezhj/Modulo_De_Estudio_CCNA_2_Exploration.pdf [2014, 19 de Junio]

CISCO PACKET TRACER [En Linea] Disponible en: https://www.netacad.com/web/about-us/cisco-packet-tracer [2014, 19 de Junio].

CP CCNA 1 I-2014. CCNA Exploration: Aspectos Basicos de Networking [En Linea] Disponible en: https://1314297.netacad.com/courses/125408 [2014, 4 de Febrero].

CP CCNA 2 I-2014. CCNA Exploration: Conceptos y Protocolos de Enrutamiento [En Linea] Disponible en: https://1314297.netacad.com/courses/144284 [2014, 26 de Abril].

COMUNICACIÓN A TRAVES DE LA RED. [En Linea] Disponible en: http://www.utp.edu.co/~fgallego/claseXcapitulo/clase02.pdf [2014, 21 de Junio].

EJEMPLO DE MONOGRAFIA. FUNDAMENTOS DE INVESTIGACION [En Linea]

Disponible en: http://es.scribd.com/doc/90703635/Ejemplo-de-Monografia-1

PUBLICATION MANUAL PREPARACION DE UNA MONOGRAIA Según APA (5° Edicion) [En Linea] Disponible en: http://www.slideshare.net/craupru/monografia-apa-1012210 [2014, 19 de Junio].

ANEXOS.

Link ejercicio escenario 1	https://drive.google.com/file/d/1Nz50dhioAZFTtU61nCXQihUUKGbv_BZi/view?usp=sharing
Link ejercicio escenario 2	https://drive.google.com/file/d/1K-6hZsC03yXw8l-Vz9GoTP5lZSw1g1cC/view?usp=sharing
Link artículo científico	https://docs.google.com/document/d/1IfOXi79zL1twMrQNgQ4tdBObiIeUXBTO/edit?usp=sharing&ouid=112479188443631567712&rtpof=true&sd=true