



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

...

T E S I S

QUE PARA OBTENER EL GRADO DE:

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A :

PÉREZ ROMERO NATALIA ABIGAIL

TUTOR

DR. JOSÉ DAVID FLORES PEÑALOZA



CIUDAD UNIVERSITARIA, CD. Mx., 2023

Capítulo 1

title

Capítulo 2

Introducción

Las redes virtuales privadas (VPN) han sido de gran utilidad en el internet moderno desde necesidades empresariales como la transmisión de datos entre diferentes oficinas, como uso personal para proteger la privacidad de los usuarios.

Existen protocolos de VPN como QUIC, OpenVPN, IPsec, Wireguard, entre otros. En el presente trabajo nos enfocamos en Wireguard, un protocolo de VPN de código abierto, de alto rendimiento, más simple y más rápido que otros protocolos de VPN, como OpenVPN y IPsec.

2.1. Protocolo IP

El protocolo IP (Internet Protocol) Junto con el protocolo TCP (Transmission Control Protocol) son los dos protocolos más importantes en el Internet.

IP determinará el formato de los paquetes de datos que se envían y reciben a través de la red. TCP se encargará de la transmisión de los datos.

Existen dos versiones de IP, la versión 4 (IPv4) y la versión 6 (IPv6). La versión 4 es la más utilizada en la actualidad, pero se está migrando a la versión 6 debido a la falta de direcciones IP disponibles en la versión 4.

2.2. Protocolo TCP

El protocolo TCP (Transmission Control Protocol) es un protocolo de transporte orientado a conexión. TCP se encarga de la transmisión de los datos de manera fiable, es decir, garantiza que los datos lleguen a su destino en el orden correcto y sin errores. TCP también se encarga de controlar el flujo de datos, es decir, de evitar que el emisor saturé al receptor con datos.

2.3. Protocolo UDP

El protocolo UDP provee un servicio de transporte no orientado a conexión. UDP es más simple que TCP, ya que no tiene control de flujo, control de errores, ni re-

transmisión de paquetes.

2.4. VPN

Las VPN (Virtual Private Network) son redes privadas virtuales que permiten a los usuarios conectarse a una red privada a través de una red pública, como Internet. Las VPN se utilizan para proteger la privacidad y la seguridad de la información transmitida a través de la red.

2.5. Wireguard

Wireguard es un protocolo de VPN de código abierto y de alto rendimiento. Wireguard es más simple y más rápido que otros protocolos de VPN, como OpenVPN y IPsec.

2.6. NAT

NAT (Network Address Translation) es una técnica que permite a varios dispositivos compartir una única dirección IP pública. Esta técnica ha sido de gran utilidad ante la escasez de direcciones IP en IPv4. NAT traduce las direcciones IP privadas de los dispositivos de una red local a una única dirección IP pública.

2.7. NAT Translation Table

2.8. IP Masquerade

IP Masquerade que permite a una red local compartir una única dirección IP pública, similar a un NAT one-to-many encontrado en un router.

Es particularmente útil en un host de Linux que tiene un modem y actúa como PPP (Point to Point Protocol) o SLIP server, permitiendo a los clientes de la red local acceder a Internet si estos no tienen direcciones IP públicas.

2.9. IP Forwarding

2.10. Tablas de ruteo

2.11. IPTables

IPTables es una herramienta de configuración de firewall en sistemas operativos basados en Linux. Entre sus funciones se encuentran el filtrado de paquetes, redireccionamiento de paquetes, traducción de direcciones de red, etc.

2.12. Relay network

Capítulo 3

Desarrollo

3.1. Casos de uso

Registro de usuario

En el registro del usuario se deberá solicitar al usuario su nombre, correo electrónico y contraseña, que será enviada al orquestrador en texto plano para su registro, si es exitoso el orquestrador deberá enviar un mensaje de confirmación al usuario.

Registrar usuario

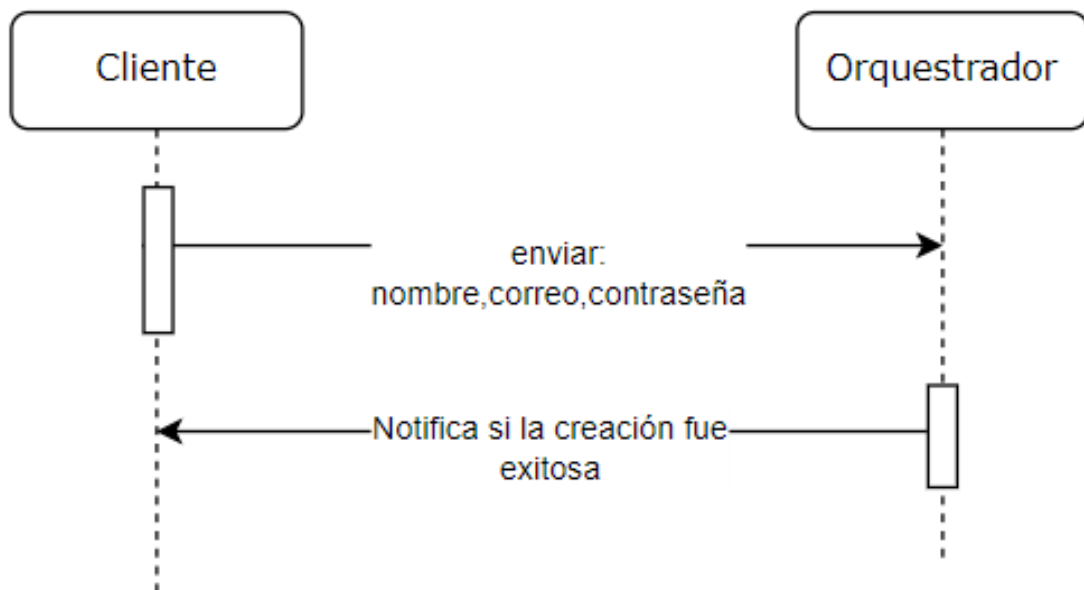


Figura 3.1: Diagrama de caso de uso: registro de usuario

3.1.1. Identificación del usuario

En esta primera version no nos preocuparemos de que la información del usuario se transmita de forma segura, por lo que el usuario deberá identificarse con un nombre de usuario, correo electrónico y contraseña. Que será enviada al orquestador en texto plano para su verificación.

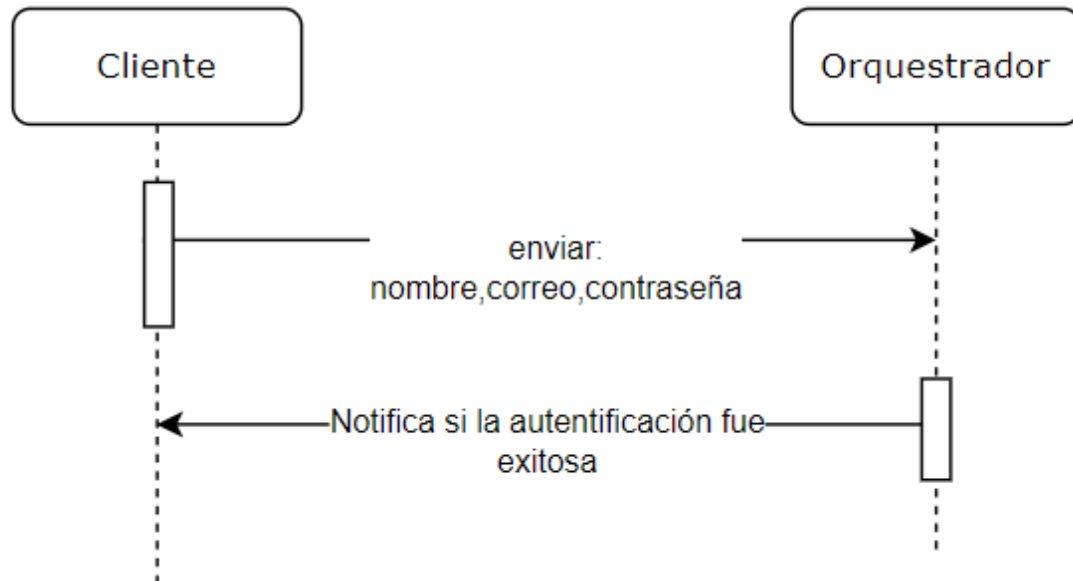


Figura 3.2: Diagrama de caso de uso: identificación del usuario

3.1.2. Registro de una red privada

Deseamos que el usuario pueda registrar las redes privadas a las que desea conectarse, para ello se deberá implementar un mecanismo de registro de redes privadas. El cliente deberá enviar un mensaje al orquestador con el nombre de la red privada que desea crear, si la red privada existe el orquestador deberá notificar al cliente, si la red privada no existe, el orquestador deberá crearla y enviar un mensaje de confirmación con la información siguiente: IP asignada, rango, máscara de la red privada creada.

Una red privada desde el punto de vista del orquestador es un objeto que contiene la siguiente información:

- Identificador
- Nombre de la red privada
- Lista de dispositivos finales
- Lista de conexiones

Creación de la red privada

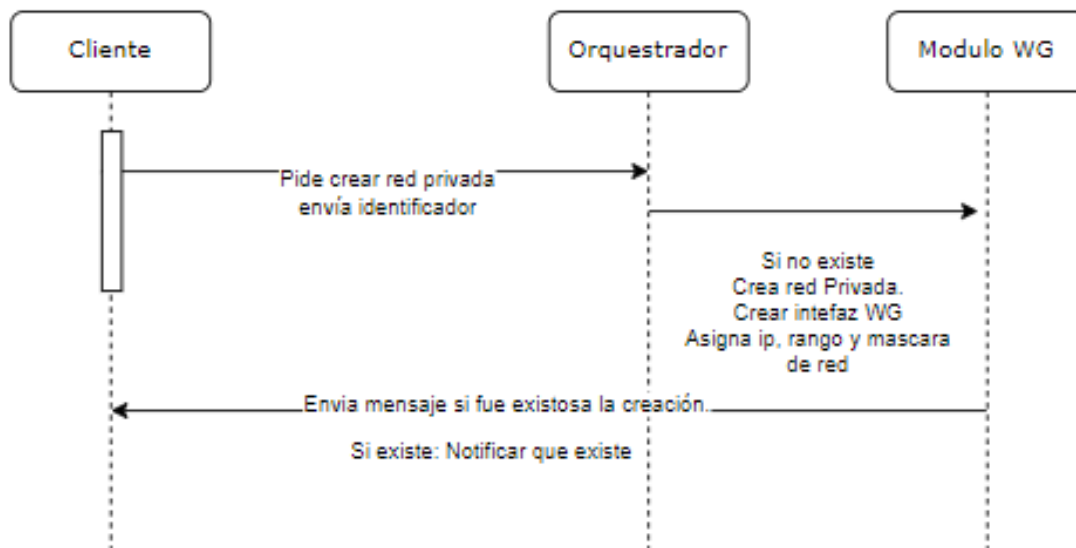


Figura 3.3: Diagrama de caso de uso: registro de red privada

La idea es crear este objeto para almacenar y consultar datos sobre las redes privadas de un cliente. Luego el razonamiento tras crear un interfaz virtual de Wireguard es que en caso de que la comunicación entre los dispositivos finales no sea posible, el orquestrador pueda actuar como relay dentro de la red privada virtual.

3.1.3. Registro de un dispositivo final

Uno de los objetivos del orquestrador será registrar los dispositivos finales conectados a la red privada, para ello se deberá implementar un mecanismo de registro de dispositivos.

El cliente enviara al orquestrador el identificador de la red privada y el dispositivo final que desea registrar. El orquestrador deberá validar que la red privada exista y que el dispositivo final no esté registrado en la red privada, si es así el orquestrador deberá registrar el dispositivo final y enviar un mensaje de confirmación al cliente.

El orquestrador sera quien asigne la IP de los dispositivos finales dentro de una red privada de los clientes. Así que tambien deberá asignar el rango y la mascara de la red privada.

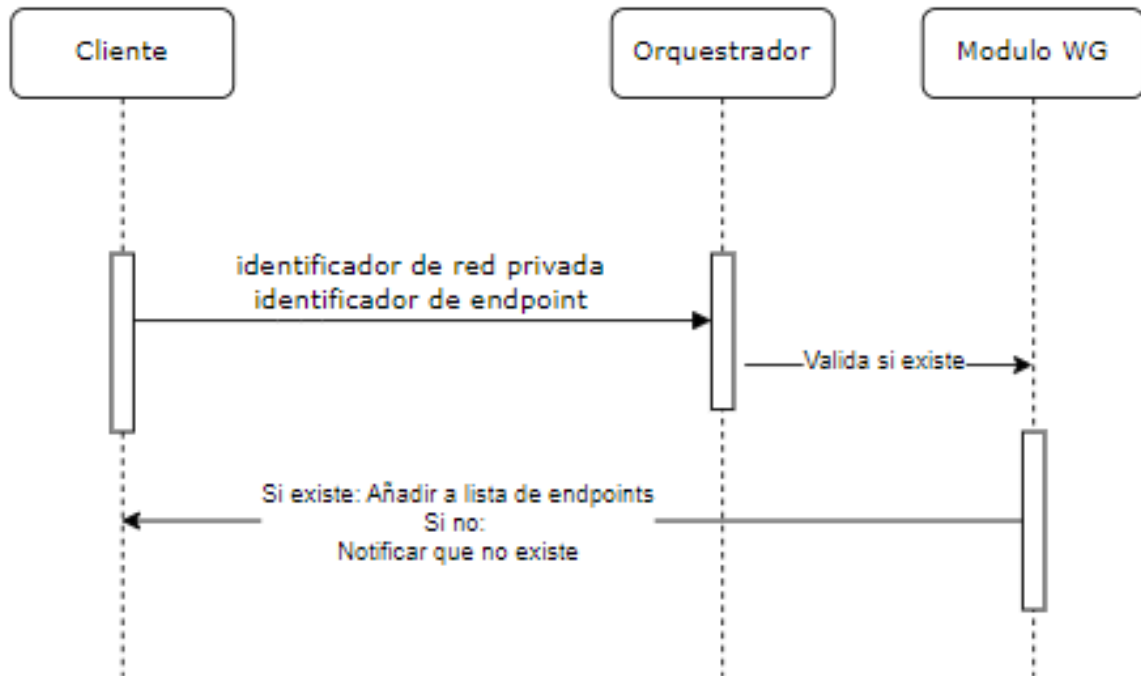


Figura 3.4: Diagrama de caso de uso: registro de dispositivo final

3.1.4. Cliente verifica conectividad con sus endpoint registrados

El cliente deberá informar al orquestrador si es posible que se comunique con los demás dispositivos finales de la red privada, para ello deberá enviar un mensaje al orquestrador para conocer que dispositivos finales supone que están conectados a la red privada. Luego este cliente verificara si alcanza a los demás dispositivos finales de la red, mediante un mensaje enviado desde la interfaz Wireguard, es decir, usando las IP asignadas por el orquestrador.

Este caso de uso se deberá hacer con cierta periodicidad, para que el cliente pueda tener información actualizada de la red privada. Y en caso de que el orquestrador la solicite el cliente tendrá la información de la red privada actualizada.

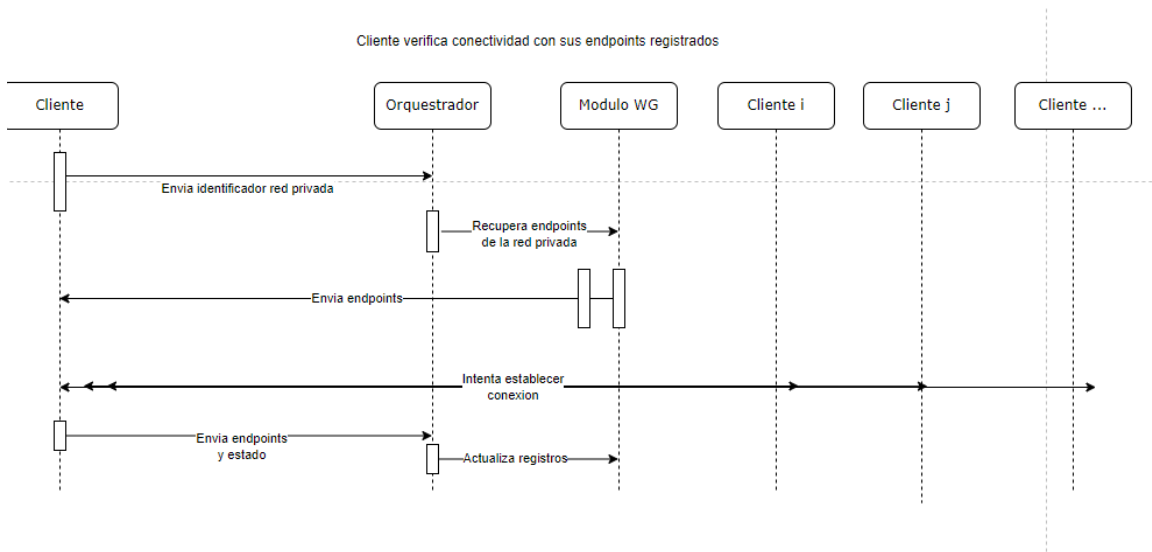


Figura 3.5: Diagrama de caso de uso: cliente verifica conectividad con sus endpoint registrados

3.1.5. Cliente consulta información de red privada al orquestrador

El cliente deberá poder consultar la información de la red privada a la que está conectado, para ello deberá enviar un mensaje al orquestrador con el identificador de la red privada, el orquestrador deberá responder con la información de la red privada.

3.1.6. Cliente consulta redes privadas disponibles

El cliente deberá poder consultar las redes privadas disponibles, para ello deberá enviar un mensaje al orquestrador, el orquestrador deberá responder con la lista de redes privadas conocidas.

3.1.7. Orquestrador divulga tablero de red privada

Si el cliente envía una solicitud del estado de una red privada al orquestrador, este deberá responder con un tablero de la red privada, que contiene la información de los dispositivos finales conectados a la red privada, las conexiones entre los dispositivos finales y la alcanzabilidad de los dispositivos finales desde el punto de vista del orquestrador.

Esto se deberá hacer con cierta periodicidad, para que el cliente pueda tener información actualizada de la red privada.

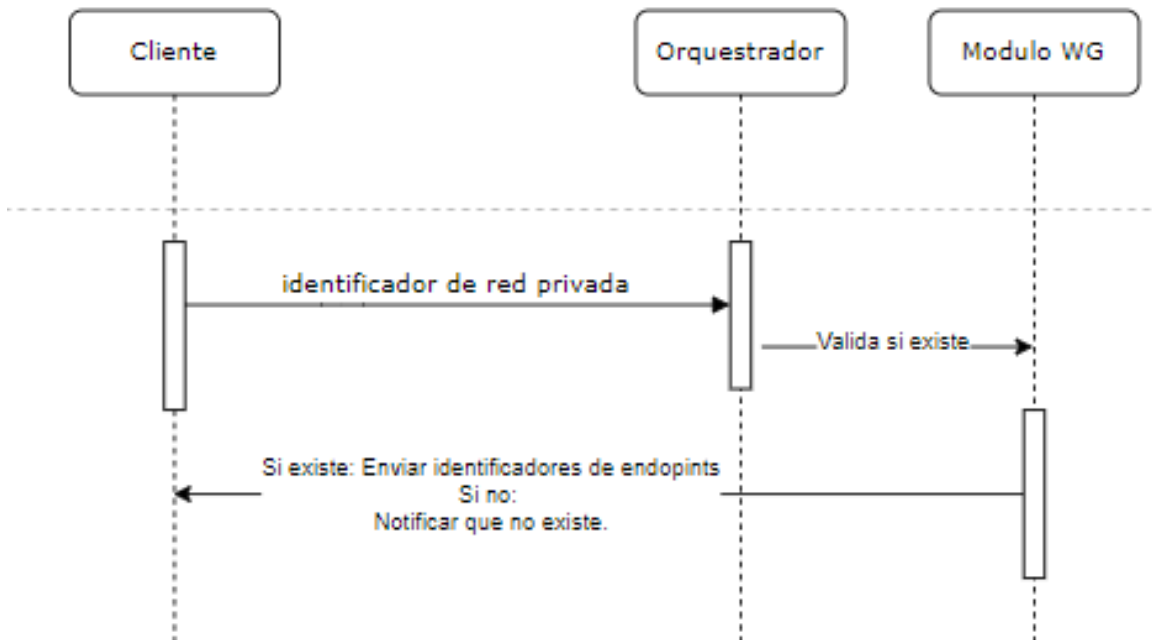


Figura 3.6: Diagrama de caso de uso: cliente consulta información de red privada al orquestrador

3.1.8. Conexión de dispositivos finales

Tendremos dos casos en cuando se quieran conectar dos o más dispositivos finales, el primero es cuando es posible que se comuniquen entre si por que tienen direcciones IP ruteables. El segundo caso es cuando los dispositivos finales no pueden comunicarse entre si por que no tienen direcciones IP ruteables, en este caso el orquestrador deberá ofrecer un mecanismo para que los dispositivos finales puedan conectarse entre sí mediante un relay.

Conexión de dispositivos finales con direcciones IP ruteables. Directa

En este caso el uno de los clientes se comunica directamente con el otro cliente, el orquestrador deberá enviar un mensaje de confirmación al cliente que solicita la conexión. Para esto el cliente A enviara mediante ping al cliente B a la dirección IP y puerto que el orquestrador le proporcionó para la interfaz Wireguard.

Si se obtiene una respuesta entonces consideramos que la conexión fue exitosa (los dispositivos son alcanzables).

Conexión de dispositivos finales con direcciones IP no ruteables. Relay

En este caso el orquestrador deberá ofrecer un mecanismo para que los dispositivos finales puedan conectarse entre sí mediante un relay. El cliente A se comunica con el orquestrador para solicitar la conexión con el cliente B, el orquestrador deberá enviar un mensaje de confirmación al cliente A con la dirección IP y puerto del orquestrador,

Servicio de listar redes disponibles

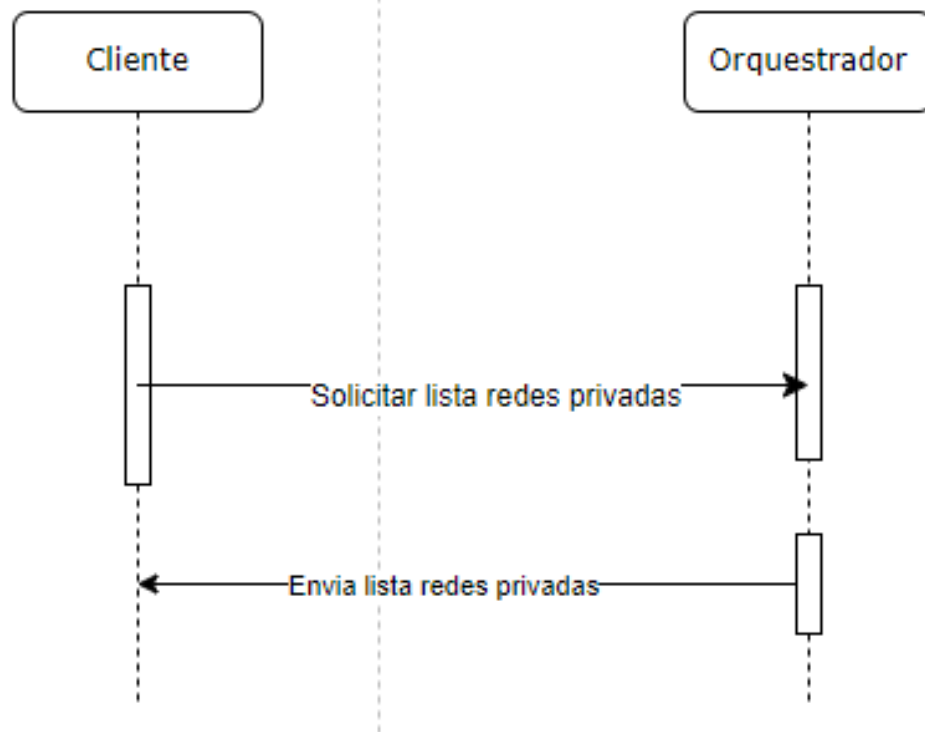


Figura 3.7: Diagrama de caso de uso: cliente consulta redes privadas disponibles

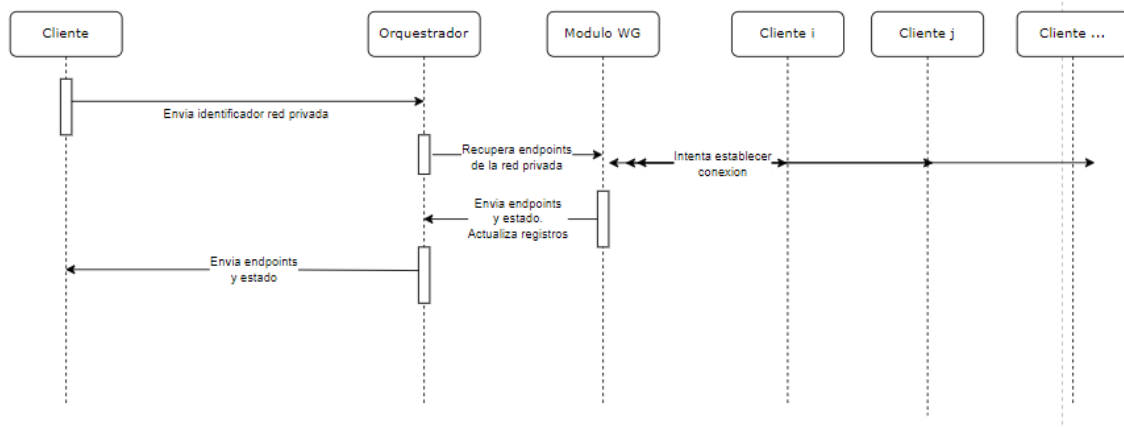


Figura 3.8: Diagrama de caso de uso: orquestrador divulga tablero de red privada

el cliente A deberá enviar un mensaje al orquestrador para que este se comunice con el cliente B.

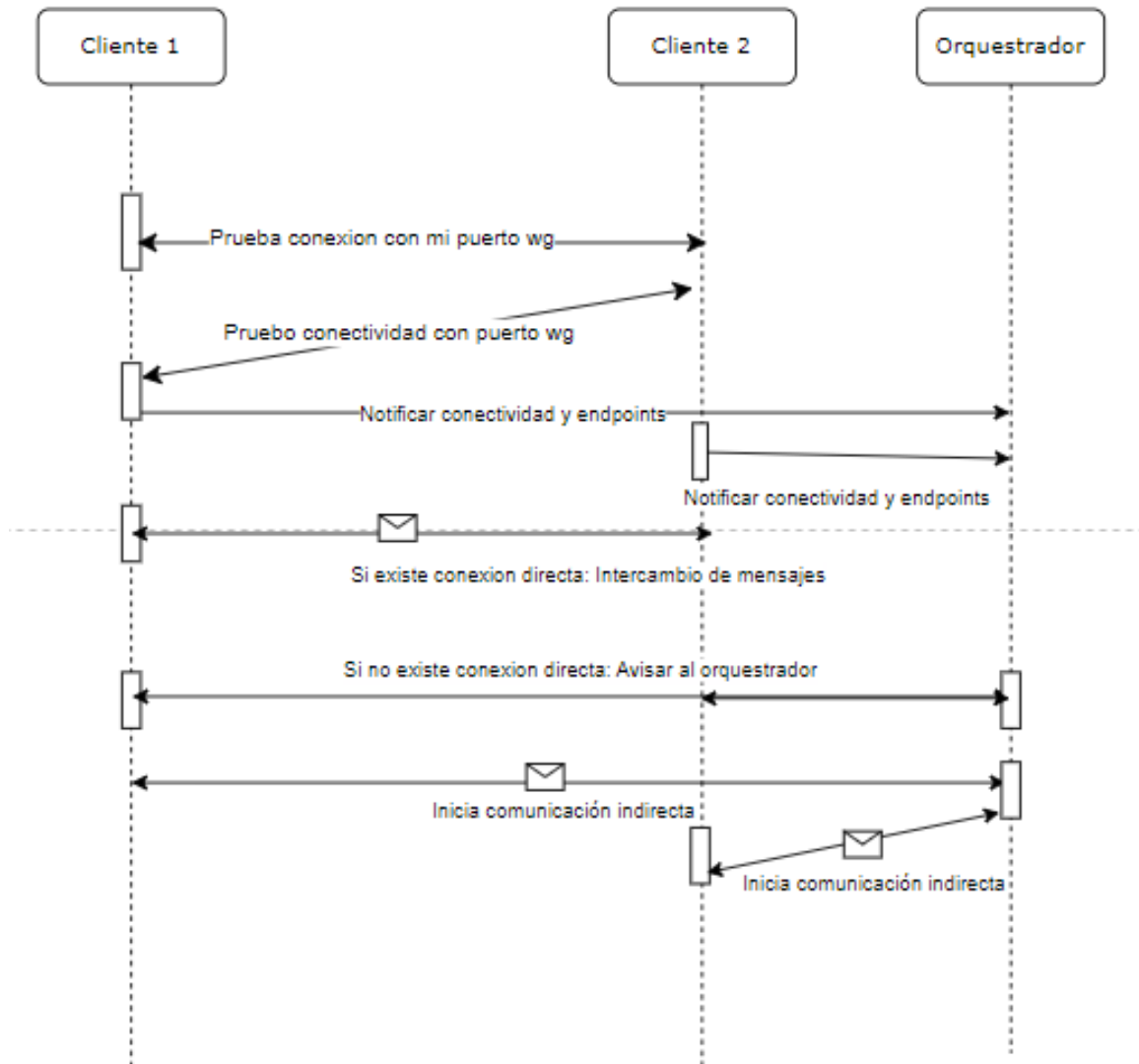


Figura 3.9: Diagrama de caso de uso: conexión de dispositivos finales

3.2. Diagrama de clases

Para el orquestrador tendremos las siguientes clases:

Bajo la idea de que el orquestrador es el encargado de orquestrar la conexión entre los dispositivos finales dentro de una red privada de un cliente, tendremos las siguientes clases:

- **Cliente:** Clase que representa a un cliente que se conecta a la red privada de otro cliente.
- **Endpoint:** Clase que representa a un dispositivo final que se conecta a la red privada de un cliente.
- **Conexión:** Clase que representa una conexión entre dos dispositivos finales.

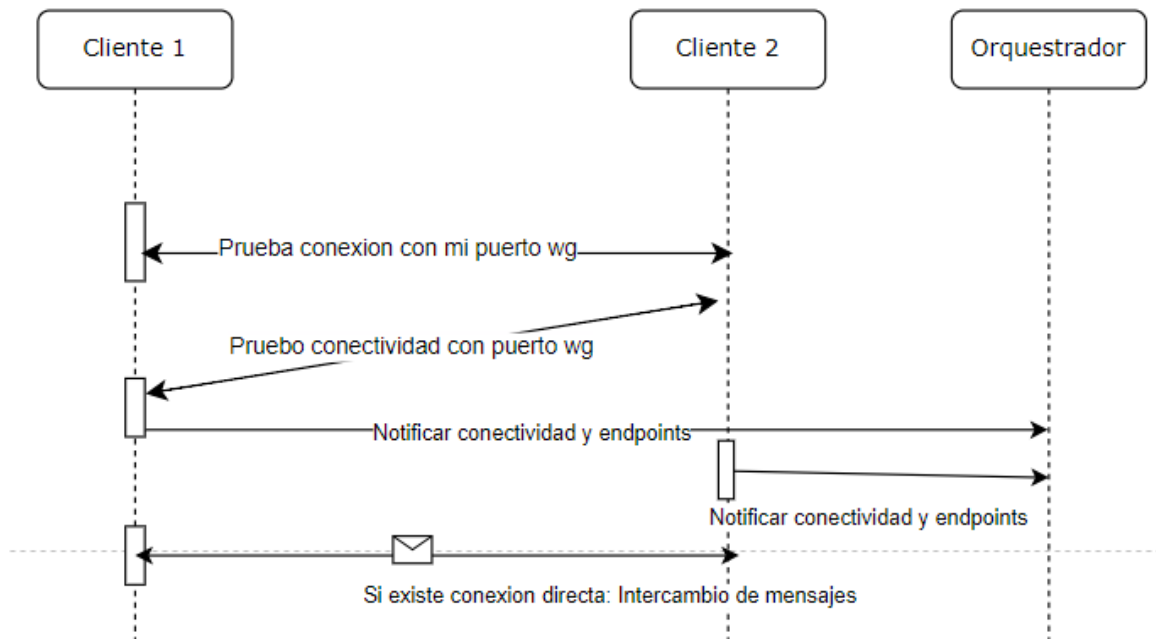


Figura 3.10: Diagrama de caso de uso: conexión de dispositivos finales con direcciones IP ruteables. Directa

La idea de esta clase es que el orquestrador sepa que dispositivos finales están conectados entre si y para cuales es necesario relay.

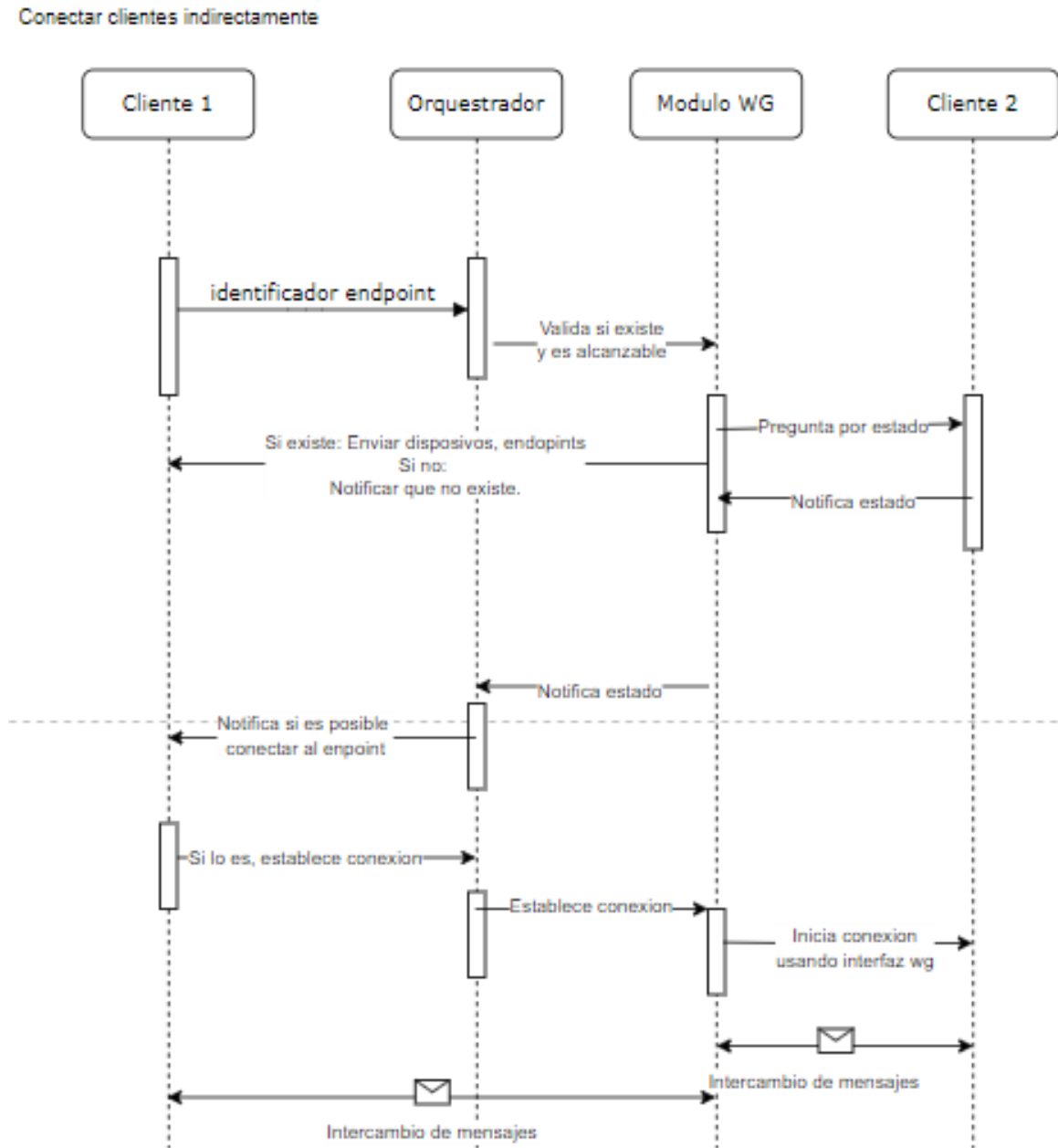


Figura 3.11: Diagrama de caso de uso: conexión de dispositivos finales con direcciones IP no ruteables. Relay

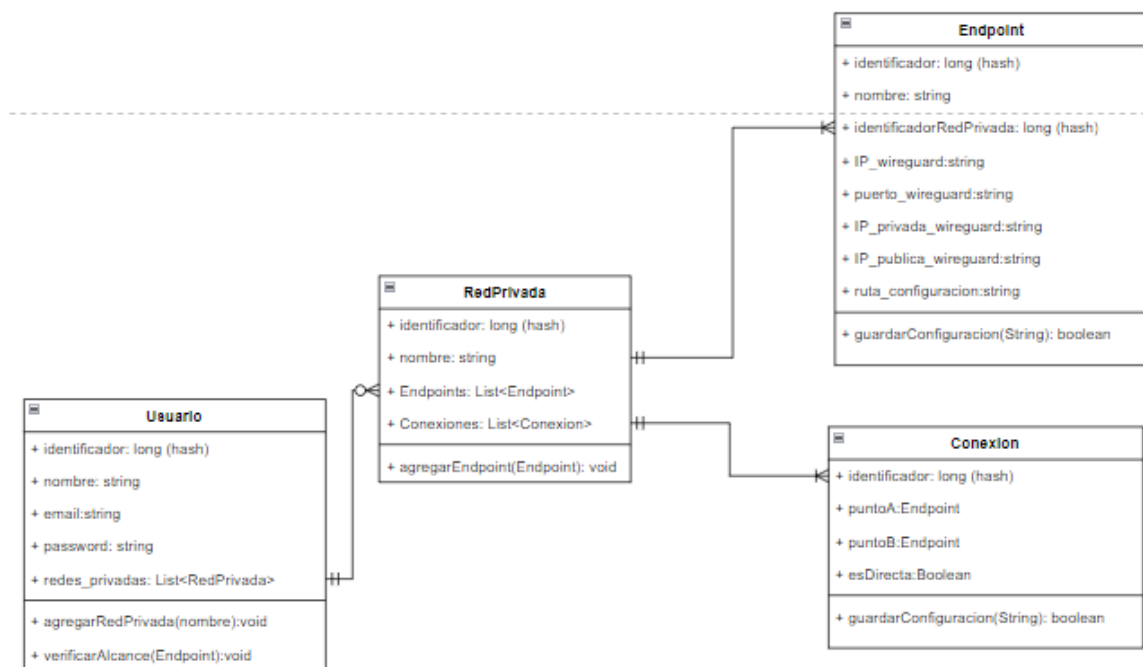


Figura 3.12: Diagrama de clases

Capítulo 4

Resultados

Capítulo 5

Conclusiones

Bibliografía

- [1] Kurose, J. F., & Ross, K. W. (2017). *Computer networking: a top-down approach*, Pearson, 7th edition.
- [2] WireGuard, *WireGuard: fast, modern, secure VPN tunnel*, <https://www.wireguard.com/>, 2021.
- [3] Linux Documentation Project, *Linux Advanced Routing & Traffic Control HOWTO*, <https://tldp.org/HOWTO/Adv-Routing-HOWTO/index.html>, 2021.
- [4] Bautts, M., & Dawson, M. (2000). *Linux Network Administrator's Guide*, O'Reilly Media, 3rd edition.
- [5] Bautts, M., & Dawson, M. (2000). *Linux IP Masquerade HOWTO*, <https://tldp.org/HOWTO/IP-Masquerade-HOWTO/index.html>, 2021.