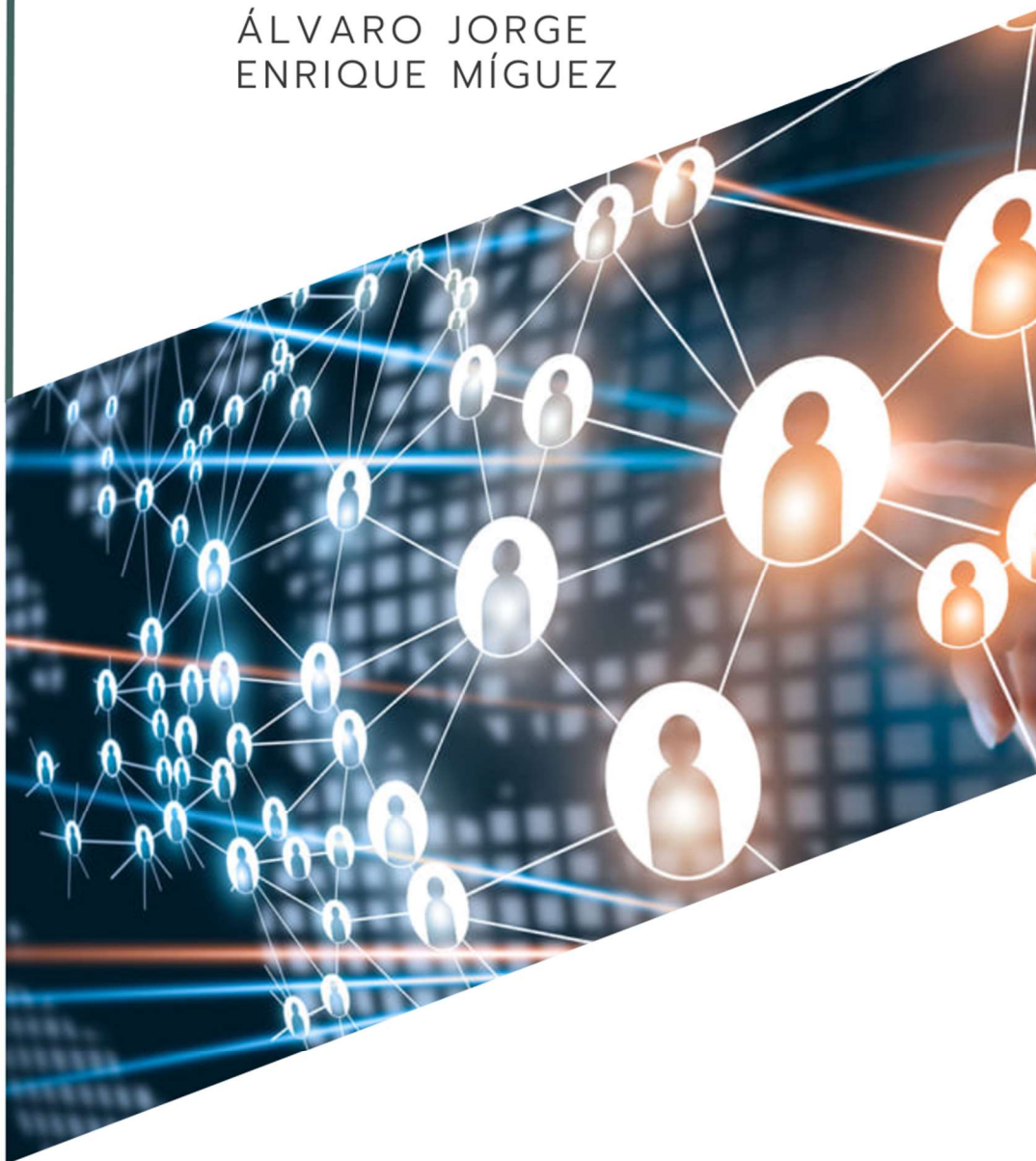




PROYECTO **DE REDES**

ÁLVARO JORGE
ENRIQUE MÍGUEZ



ABRIL 2023



CONTENIDO

1. Introducción.....3

2. Plano4

3. VLAN7

4. Portchannel.....8

5. SSH.....9

6. SEGURIDAD DE PUERTOS..... 11

7. DHCP 12

8. NAT 13

9. Spanning Tree14

1. INTRODUCCIÓN

¡Bienvenidos a nuestro proyecto de redes! Nuestro objetivo es facilitar la eficiente y segura compartición de información entre todos los empleados de la gestoría.

La gestoría consta de tres plantas, cada una con sus respectivos departamentos y despachos. A continuación, detallamos los departamentos:

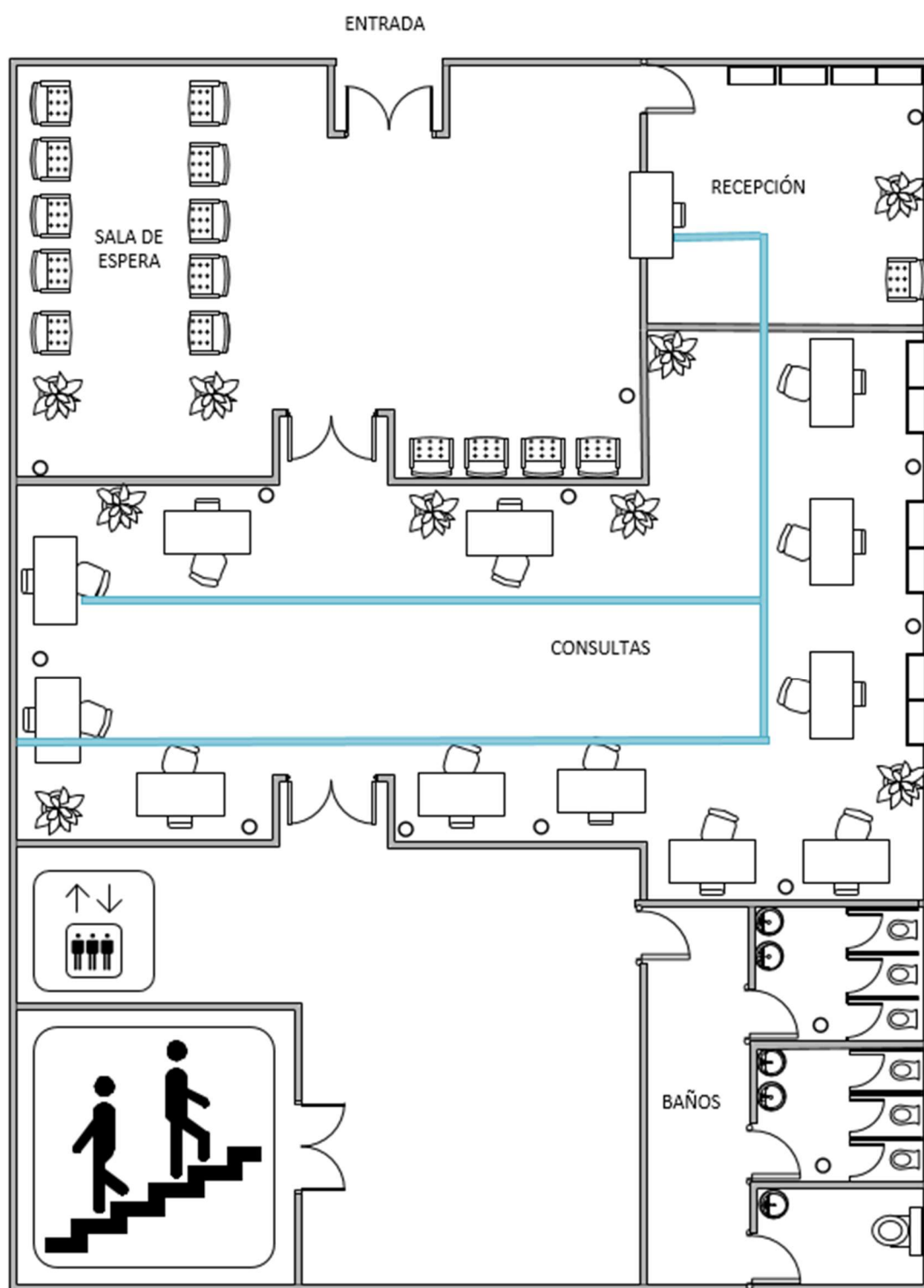
- **Departamento fiscal:** Este departamento se encargará de las gestiones fiscales y consta de 10 puestos de trabajo.
- **Departamento de inmigración:** Este departamento se dedica a las gestiones relacionadas con inmigración y cuenta con 16 puestos de trabajo.
- **Departamento jurídico:** Aquí se llevan a cabo las gestiones jurídicas y dispone de 19 puestos de trabajo.
- **Departamento comercial:** Su función es gestionar los aspectos comerciales y cuenta con 13 puestos de trabajo.
- **Dirección:** Este sector se encarga de la dirección y gestión de la empresa y consta de 3 puestos de trabajo.

En la planta 1, se encuentra el RACK que alberga los diferentes switches y routers. Estos dispositivos brindan conectividad a toda la empresa al estar ubicados en un punto central. Además, contamos con impresoras distribuidas en los distintos departamentos para imprimir documentos de manera conveniente.

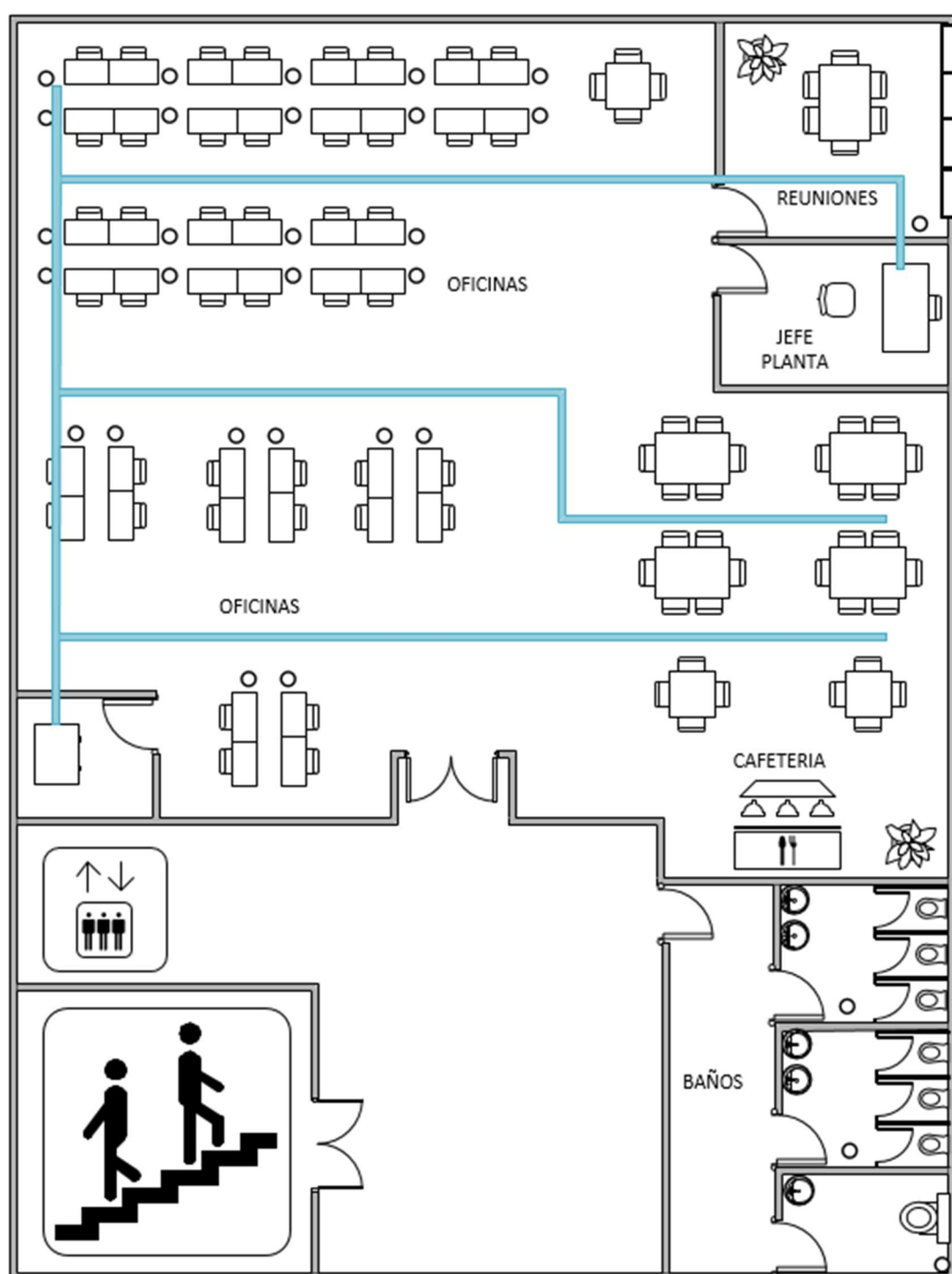
Todos los equipos están configurados mediante DHCP, lo que permite que cada uno de ellos reciba automáticamente una dirección IP en la red correspondiente a su respectivo departamento.

Estamos comprometidos en garantizar una infraestructura de red confiable y eficiente para facilitar el trabajo colaborativo y seguro en la gestoría.

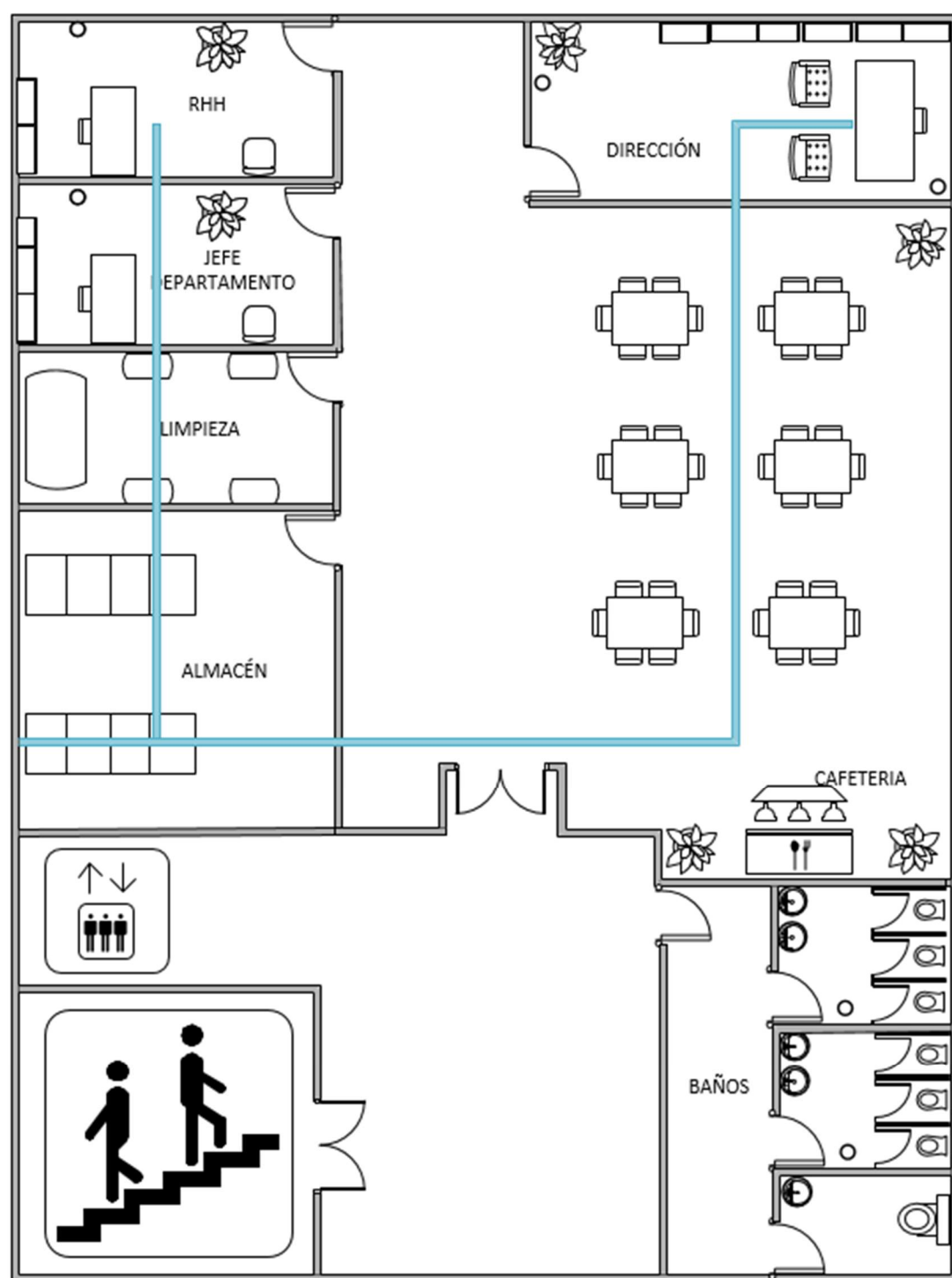
2. PLANO



PLANTA 0



PLANTA 1



PLANTA 2

3. VLAN

| | | |
|------------------|----------|------------------|
| DEP. FISCAL | VLAN 10 | 192.168.10.0/24 |
| DEP. INMIGRACIÓN | VLAN 20 | 192.168.20.0/24 |
| DEP. JURIDICO | VLAN 30 | 192.168.30.0/24 |
| DEP. COMERCIAL | VLAN 40 | 192.168.40.0/24 |
| DIRECCION | VLAN 50 | 192.168.50.0/24 |
| GESTIÓN | VLAN 200 | 192.168.200.0/24 |

Dividir la red en VLANs (Virtual Local Area network) es útil por razones de seguridad y para limitar el ámbito del tráfico de difusión, esto nos permitirá decidir el acceso al contenido de la red de los distintos usuarios. Las VLANs nos ayudarán a gestionar el tráfico ya que reducirán el tamaño del dominio de colisión en un segmento de Ethernet. Además, optimizan la red al enviar los mensajes broadcast a dominios pequeños en vez de toda la red.

La pertenencia a una VLAN es flexible y nos permitirá cambiar a un equipo de VLAN según las circunstancias. En nuestro proyecto hemos clasificado las VLANs según los distintos departamentos, cada VLAN tiene una capacidad de 254 host al tener mascara de red 24

La VLAN de gestión será la que posea todos los permisos y servirá para que los informáticos de la empresa puedan acceder todos los dispositivos, incluyendo routers y switches con el objetivo de monitorizar la red. Esta VLAN será una VLAN nativa, es decir, su trafico será sin etiquetas y se asignará con el comando switch port trunk.

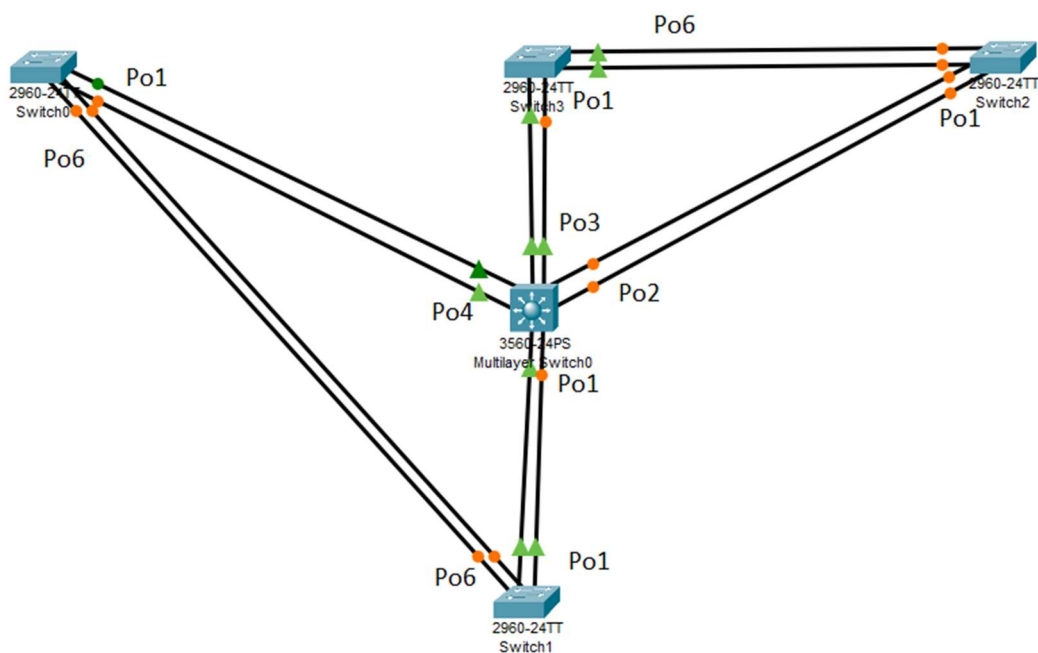
4. PORTCHANNEL

El Portchannel se utiliza para juntar varios enlaces físicos en un único enlace lógico, lo que proporciona un aumento de ancho de banda, mejora de la redundancia, balanceo de carga y simplificación de la administración en redes de comunicación...

En nuestro proyecto hemos utilizado los primeros puertos (Gio/1) o los últimos puertos (Fao/24) para la combinación de ellos.

Hemos configurado en todos los switches y catalyst los Portchannels correspondientes excepto en el de las salidas al router y la conexión con el servidor.

Esto es una recreación de los Portchannels, he asignado a todos el Portchannel 1 desde su dispositivo y al Portchannel del core les he numerado:



5. SSH

En nuestro proyecto hemos incluido el SSH, es un protocolo que nos ayudará a administrar nuestro dispositivo (routers, switchs...) de forma remota y segura.

Además, eso nos evitará tener que conectar por cable de consola a configurar nuestros dispositivos, ya que lo haremos remotamente.

Le hemos asignado dos usuarios con permisos diferentes.

| NOMBRE | PRIVILEGIOS |
|----------|-------------|
| Cisco | 15 |
| Operator | 7 |

El usuario Operator con privilegios 7 tendrá acceso a funcionalidades y comandos avanzados que están reservados para usuarios con privilegios elevados como estos:

- **Configuración del sistema:** Puede acceder y modificar la configuración del sistema operativo y los servicios en el dispositivo remoto. Esto implica realizar cambios en la configuración de red, administrar usuarios y permisos, establecer políticas de seguridad, entre otros.
- **Instalación y actualización de software:** Puede instalar, actualizar y administrar software en el dispositivo remoto. Esto incluye la instalación de paquetes, la configuración de servicios y la gestión de dependencias.
- **Monitoreo y resolución de problemas:** Tiene acceso a herramientas y comandos para monitorear el rendimiento del sistema, verificar el estado de los servicios, revisar los registros de eventos y diagnosticar problemas en el dispositivo remoto.
- **Gestión de almacenamiento:** Puede administrar los dispositivos de almacenamiento, como discos duros y sistemas de archivos, en el dispositivo remoto. Esto puede implicar la creación y gestión de particiones, el montaje de unidades de almacenamiento y la gestión de la capacidad de almacenamiento.

Y el usuario Cisco con privilegios 15 tendrá acceso completo y total al dispositivo y todas las funcionalidades y comandos disponibles.:

- **Acceso completo a la configuración:** Puede ver, modificar y configurar todos los aspectos de la configuración del dispositivo, incluyendo interfaces de red, enrutamiento, políticas de seguridad, servicios y mucho más.
- **Ejecución de comandos avanzados:** Tiene acceso a comandos y funcionalidades avanzadas, como la ejecución de comandos de diagnóstico, la visualización de tablas de enrutamiento, la configuración de listas de control de acceso (ACL) y la gestión de servicios y protocolos de red.

- Configuración de privilegios de usuario: Puede crear, modificar y administrar cuentas de usuario, asignar niveles de privilegio y establecer restricciones de acceso para otros usuarios que acceden al dispositivo.
- Supervisión y resolución de problemas: Tiene acceso a herramientas de supervisión y resolución de problemas, como la visualización de registros de eventos, la captura de paquetes de red, la verificación del estado de los enlaces de red y la administración de protocolos de enrutamiento.

```
username cisco privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username operador privilege 7 secret 5 $1$mERr$T/J6uB5M/cb.uAFEIdGoU/
```

6. SEGURIDAD DE PUERTOS

En nuestro proyecto activaremos la seguridad de puerto para todos los equipos conectados, este protocolo será bastante restrictivo ya que los equipos solo podrán aprender una dirección MAC de los ordenadores, es decir que, si quitamos una conexión de un ordenador, y conectamos otro en su lugar el puerto se apagará

Esto se lo hemos implementado solamente a la VLAN de Gestión.



Hemos añadido dos PCs para comprobar que cuando las MACs son diferentes, automáticamente apague el puerto ya que sería un intento de "violación".

Esto nos permitirá que, si alguien quiere poner su ordenador, al conectar el cable no tendría ningún acceso

7. DHCP

En la gestoría, al haber tantos dispositivos, necesitamos un protocolo que nos agilice la asignación de las IPs para todos ellos.

Por ello implementamos el DHCP, es un protocolo que asigna automáticamente direcciones IP a los dispositivos en una red. Sus beneficios son:

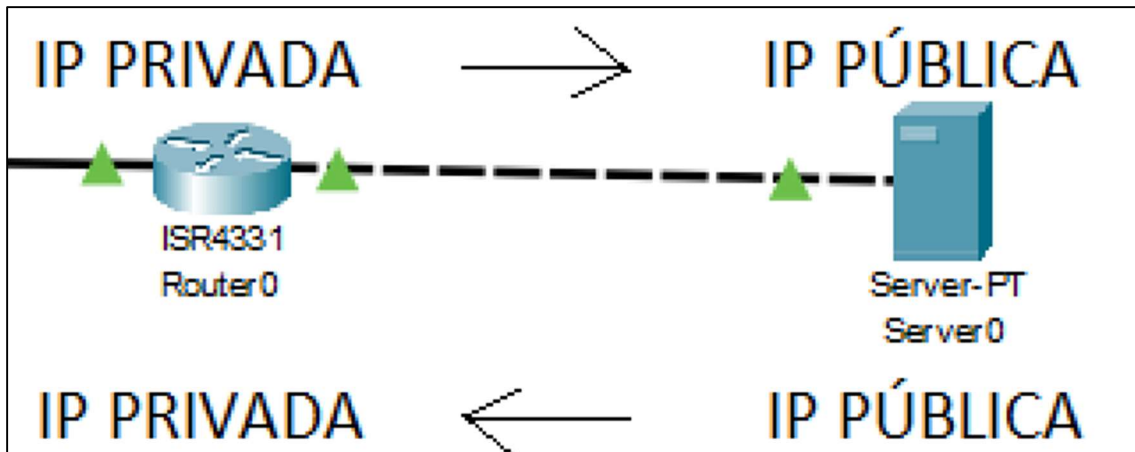
- **Ahorro de tiempo:** DHCP evita tener que configurar manualmente cada dispositivo en la red, asignando direcciones IP automáticamente.
- **Organización sencilla:** Permite definir rangos de direcciones IP para cada parte de la red, evitando conflictos y facilitando la gestión
- **Flexibilidad:** DHCP también proporciona información adicional, como servidores DNS y puerta de enlace predeterminada, simplificando aún más la configuración de los dispositivos.
- **Escalabilidad:** A medida que la red crece, DHCP permite añadir nuevos dispositivos sin necesidad de configuraciones manuales complejas.

Además, hemos excluido las 10 primeras IPs de cada VLAN para que podamos usarlas de manera manual, por ejemplo, en el servidor o en el Switch de Capa 3, poner IPs reservadas y de esta manera nunca cambiarán.

8. NAT

NAT es una técnica utilizada para traducir direcciones IP privadas a direcciones IP públicas y viceversa, lo que permite que múltiples dispositivos en una red privada compartan una única dirección IP pública.

Además, las direcciones publicas pueden utilizarse por varios dispositivos ya que hemos implementado el PAT, lo que permite a cada dispositivo distinguirse por su número de puerto único, de esta manera permitirán que múltiples conexiones se establezcan simultáneamente a través de la misma dirección IP pública.



9. SPANNING TREE

Se ha determinado PVSTP como protocolo de Spanning Tree, eligiendo el equipo "CoreCat" como root para todas las VLAN, y eligiendo los interfaces de más velocidad (Gi) como Portchannel desde todos los switches para lograr una topología en estrella con el mejor rendimiento de interfaces.

Se han creado dos Portchannels más, con interfaces Fa, que han quedado deshabilitados por STP, pero que dan la redundancia necesaria en caso de caída de los Portchannels principales.