Examen Redes 04/04/2025

Sergio Armenteros Rodríguez - 154045

Parte I: Conceptos y Teoría:

Ejercicio 1: El Mural de las Siete Capas

Interpretando el enunciado voy a hacer una explicación y comparación de los dos modelos de capas en redes. TCP/IP y OSI.

Empezaremos matizando la definición de qué son estos dos modelos para que sirven en el ámbito de redes.

Los modelos **TCP/IP** y **OSI** son modelos de referencia para la comunicación en redes. Sirven para estructurar la forma en que los dispositivos intercambian datos y garantizan la interoperabilidad entre diferentes sistemas y tecnologías.

Analizaremos entonces las capas de cada uno y sus diferentes funcionalidades.

TCP/IP	APLICACIONES
Capa acceso a la red	Define cómo los datos se transmiten físicamente a través del medio, ya sea por cables o inalámbricamente.
Capa de internet	Se encarga del direccionamiento y enrutamiento de los paquetes de datos a través de diferentes redes usando IP.
Capa de transporte	Garantiza la entrega de datos de extremo a extremo, asegurando que lleguen completos y en orden. Usa TCP para fiabilidad y UDP para velocidad.
Capa de aplicación	Proporciona servicios y aplicaciones que permiten a los usuarios acceder a la red, como el correo electrónico, la web y la transferencia de archivos.

OSI	APLICACIONES
Capa física	Define las características del hardware, como cables, señales eléctricas y conectores.
Capa de enlace de datos	Controla el acceso al medio físico y la detección de errores en la transmisión de datos.
Capa de red	Se ocupa del direccionamiento y encaminamiento de paquetes a través de diferentes redes.
Capa de transporte	Asegura que los datos se transmitan sin errores y en el orden correcto, usando protocolos como TCP y UDP.
Capa de sesión	Establece, gestiona y finaliza sesiones de comunicación entre dispositivos.
Capa de presentación	Se encarga del formato de datos, cifrado y compresión para garantizar la compatibilidad entre sistemas.
Capa de aplicación	Interactúa con el usuario y proporciona servicios como navegación web, correo electrónico y transferencia de archivos.

En su comparación las podemos representar de la siguiente manera:

TCP/IP	OSI
CAPA DE APLICACIÓN	Capa de aplicación
	Capa de presentación
	Capa de sesión
Capa de transporte	Capa de transporte
Capa de internet	Capa de red
Capa de acceso a la red	Capa de enlace de datos
	Capa Física

OSI es más detallado pero conceptual, mientras que **TCP/IP es el que realmente se usa en redes modernas** como Internet.

Ejercicio 2: Los Dos Pergaminos del Mensajero

Interpretando el enunciado, voy a hacer una explicación y comparación de los modelos TCP/IP y UDP.

Cuando se trata de transmitir datos en redes, **TCP** (Transmission Control Protocol) y **UDP** (User Datagram Protocol) son los dos principales protocolos de la capa de transporte. Ambos cumplen el mismo **objetivo**: *enviar información entre dispositivos conectados a una red, pero lo hacen de maneras muy diferentes.*

Diferencia Clave: Conexión vs. Sin Conexión

La principal diferencia entre **TCP y UDP** radica en la forma en que manejan la entrega de datos:

- **TCP *(Mensajero confiable)* está orientado a conexión**, lo que significa que establece una comunicación segura antes de enviar los datos. Se asegura de que cada paquete llegue correctamente y en el orden correcto, utilizando técnicas como el **"handshake" de tres vías**, confirmaciones de recepción y retransmisiones en caso de error.

- **UDP*(Mensajero veloz)*, en cambio, es un protocolo sin conexión**. Envía paquetes sin verificar si llegan o si lo hacen en orden. Esto lo hace mucho más rápido, pero sin garantía de entrega ni corrección de errores.

Aspecto	TCP (Fiabilidad y Orden)	UDP (Velocidad y Baja Latencia)
Tipo de conexión	Orientado a conexión (requiere un handshake previo).	Sin conexión (envía los datos sin establecer comunicación).
Fiabilidad	Alta: confirma la recepción y retransmite si hay errores.	Baja: no verifica si los paquetes llegan o se pierden.
Orden de entrega	Garantiza que los datos lleguen en orden.	No garantiza el orden de los paquetes.
Velocidad	Más lento debido al control de errores y reenvíos.	Más rápido porque no tiene controles adicionales.
Consumo de recursos	Mayor, ya que requiere más procesamiento y memoria.	Menor, ideal para sistemas con pocos recursos.
Corrección de errores	Sí, mediante retransmisión de paquetes perdidos.	No, si un paquete se pierde, no se recupera.

Ejercicio 3: El Enigma de las Subredes

1. **Bits prestados:**
    - Se toman prestados bits de la parte de host de la dirección IP para crear subredes.
    - El número de subredes creadas es 2^n, donde "n" es el número de bits prestados.
2. **Máscara de subred:**
    - La máscara de subred se ajusta para reflejar los bits prestados.
    - Los bits prestados se establecen en 1 en la máscara de subred.
3. **Direcciones de host:**
    - El número de direcciones de host utilizables por subred es 2^h - 2, donde "h" es el número de bits de host restantes.
    - Se restan 2 direcciones: la dirección de red y la dirección de broadcast.

Para crear la tabla de enrutamiento, primero necesitamos definir las subredes:

- **Red Base:** 192.168.50.0 /24
- **Máscara de Subred:** 255.255.255.192 (como calculamos anteriormente)
- **Número de Subredes:** 4

Esto nos da las siguientes subredes:

1. **Subred 1:** 192.168.50.0 /26
2. **Subred 2:** 192.168.50.64 /26
3. **Subred 3:** 192.168.50.128 /26
4. **Subred 4:** 192.168.50.192 /26

Suponiendo que el enrutador está conectado directamente a estas cuatro subredes, la tabla de enrutamiento sería la siguiente:

Destino de Red	Máscara de Red	Puerta de Enlace	Interfaz	Métrica
192.168.50.0	255.255.255.192	Directamente Conectada	Interfaz 1	0
192.168.50.64	255.255.255.192	Directamente Conectada	Interfaz 2	0
192.168.50.128	255.255.255.192	Directamente Conectada	Interfaz 3	0
192.168.50.192	255.255.255.192	Directamente Conectada	Interfaz 4	0
0.0.0.0	0.0.0.0	Dirección IP del Router ISP	Interfaz de Salida a Internet	1

Ejercicio 4: La encrucijada de las rutas:

El tótem con flechas representa de manera alegórica el concepto fundamental del enrutamiento en redes de datos. En esencia, el enrutamiento es el proceso de determinar la ruta o camino óptimo para que los paquetes de información viajen desde un origen hasta su destino a través de una red.

- **Flechas de piedra (Enrutamiento estático):** Simbolizan el enrutamiento estático, donde las rutas son predefinidas y configuradas manualmente por un administrador de red. Estas rutas permanecen fijas a menos que el administrador las modifique explícitamente.
- **Flechas móviles (Enrutamiento dinámico):** Representan el enrutamiento dinámico, donde los dispositivos de red (routers) intercambian información de enrutamiento entre sí y ajustan las rutas de forma automática en respuesta a cambios en la topología de la red, como fallos en enlaces o congestión.

Tabla de Enrutamiento

Una tabla de enrutamiento es una estructura de datos esencial que reside en cada router y que contiene la información necesaria para tomar decisiones de reenvío de paquetes.

- **Función:** La tabla de enrutamiento permite al router determinar la mejor ruta para enviar un paquete de datos hacia su destino, basándose en la dirección IP de destino del paquete.
- **Contenido:** Cada entrada en la tabla de enrutamiento específica:
    - **Destino de red:** La dirección IP de la red o subred a la que se quiere llegar.
    - **Máscara de red:** Indica qué parte de la dirección IP de destino se utiliza para identificar la red.
    - **Puerta de enlace:** La dirección IP del siguiente dispositivo (router) al que se debe enviar el paquete para alcanzar el destino.
    - **Interfaz:** La interfaz física del router a través de la cual se debe enviar el paquete.
    - **Métrica:** Un valor que representa el "costo" de usar una ruta particular (por ejemplo, número de saltos, ancho de banda, retardo). El router utiliza la métrica para seleccionar la mejor ruta entre varias opciones posibles.

En resumen, la tabla de enrutamiento es la brújula que guía a los routers en el proceso de dirigir el tráfico de red de manera eficiente.

Ejercicio 5: El Guardián de la máscara única

La técnica de redes moderna que se refleja en la leyenda del Guardián de la Máscara es la **Traducción de Direcciones de Red (NAT)**.

Traducción de Direcciones de Red (NAT)

- **Descripción:** NAT es un mecanismo que permite que múltiples dispositivos en una red privada (como una red doméstica o una red de oficina) compartan una única dirección IP pública para comunicarse con Internet. El enrutador NAT actúa como intermediario, traduciendo las direcciones IP privadas de los dispositivos internos a la dirección IP pública al salir de la red, y realizando la traducción inversa cuando las respuestas regresan.
- **Funcionamiento:**
    1. Cuando un dispositivo en la red privada envía un paquete a Internet, el enrutador NAT intercepta el paquete.
    2. El enrutador NAT reemplaza la dirección IP privada del dispositivo de origen con su propia dirección IP pública. También rastrea esta conexión en una tabla NAT, registrando el puerto de origen original.
    3. El paquete modificado se envía a Internet.
    4. Cuando el servidor remoto responde, envía el paquete a la dirección IP pública del enrutador NAT.
    5. El enrutador NAT consulta la tabla NAT para determinar a qué dispositivo en la red privada se debe reenviar el paquete, utilizando el puerto de destino en el paquete y la información almacenada previamente.
    6. El enrutador NAT reemplaza la dirección IP de destino (su propia dirección IP pública) con la dirección IP privada del dispositivo original y reenvía el paquete al dispositivo.

Beneficios de NAT:

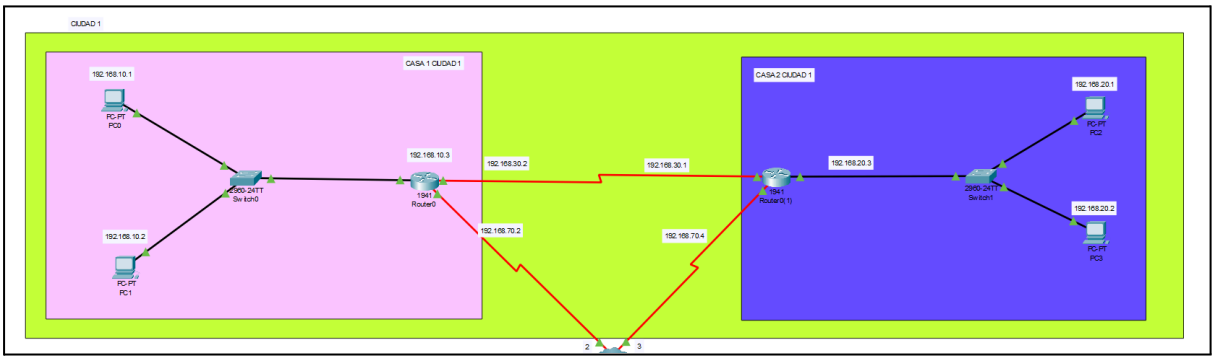
- **Ahorro de direcciones IP:** NAT permite que múltiples dispositivos utilicen una única dirección IP pública, lo cual es crucial debido al agotamiento de las direcciones IPv4.
- **Seguridad:** NAT oculta las direcciones IP privadas de los dispositivos en la red interna, proporcionando una capa de seguridad al dificultar que los atacantes externos se dirijan directamente a esos dispositivos.

PARTE 2: EJERCICIOS DE CISCO

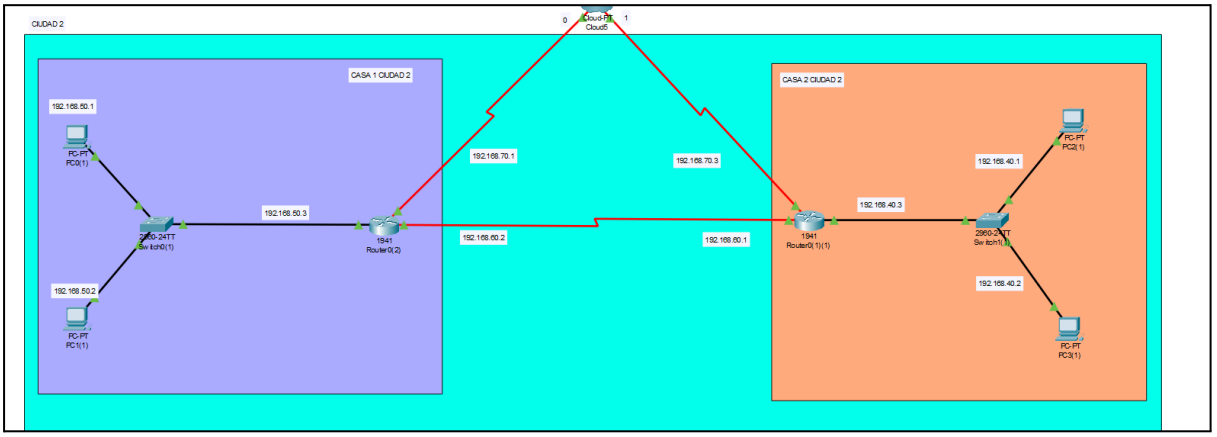
Ejercicio 1: La Ruta Perdida entre Dos Reinos

Para la realización de este ejercicio he realizado una conexión entre dos ciudades que cuentan con 2 casas cada una, donde en cada casa hay 2 PC's, 1 switch y 1 router.

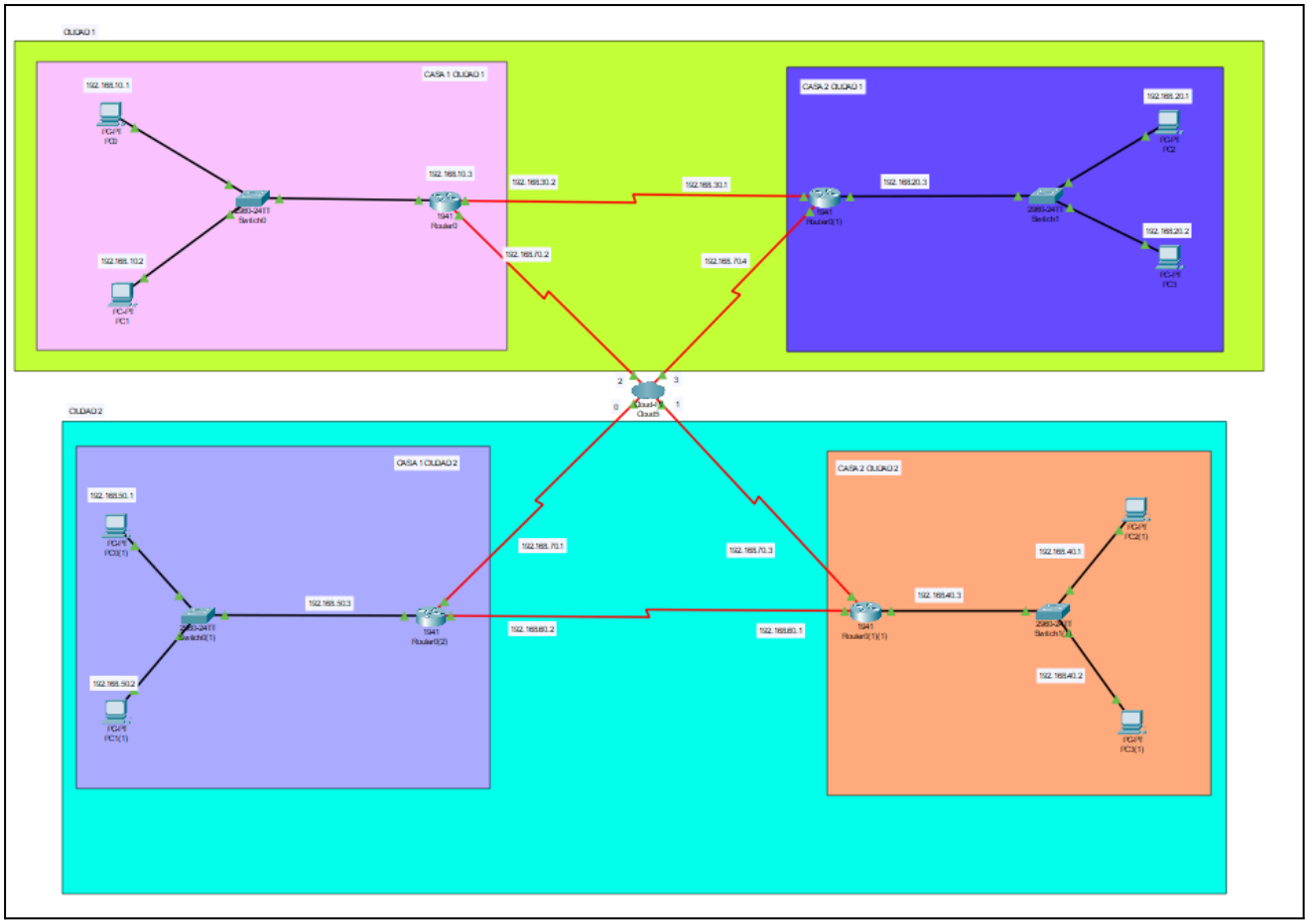
Las casas de una misma ciudad se conectan a través de un cable serial DTE, y para conectarse entre las ciudades, he empleado el uso de un Cloud donde a través de frame relay y asignaciones individuales de los puertos de entrada he relacionado los distintos routers de cada casa.



- *Ciudad 1 con las respectivas ip de cada elemento*



- *Ciudad 2 con las respectivas ip de cada elemento*



- *Conexión entre dos ciudades al completo con todas las ip's de los elementos*

Frame Relay

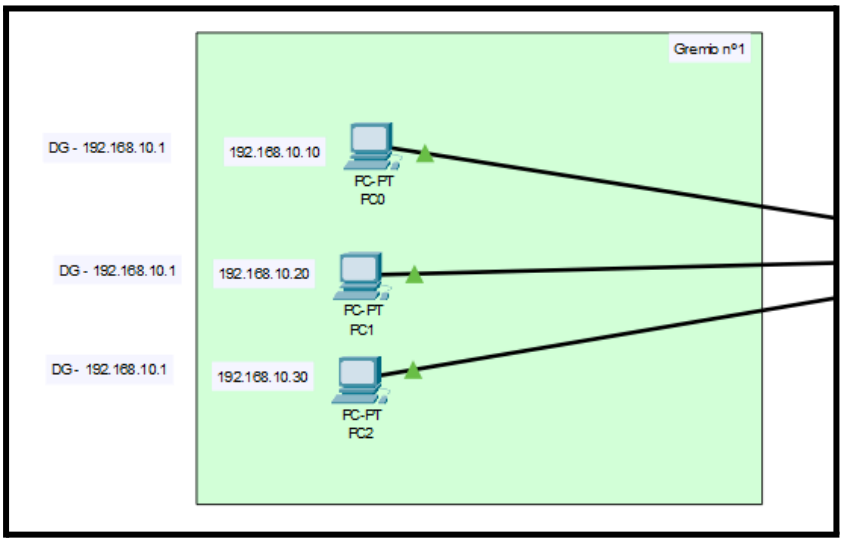
Serial0	Router3.Router1	<->	Serial0	Router3.Router1
Port	Sublink		Port	Sublink

	From Port	Sublink	To Port	Sublink
1	Serial0	Router3.Router1	Serial2	Router1.Router3
2	Serial0	Router3.Router2	Serial3	Router2.Router3
3	Serial1	Router4.Router1	Serial2	Router1.Router4
4	Serial1	Router4.Router2	Serial3	Router2.Router4

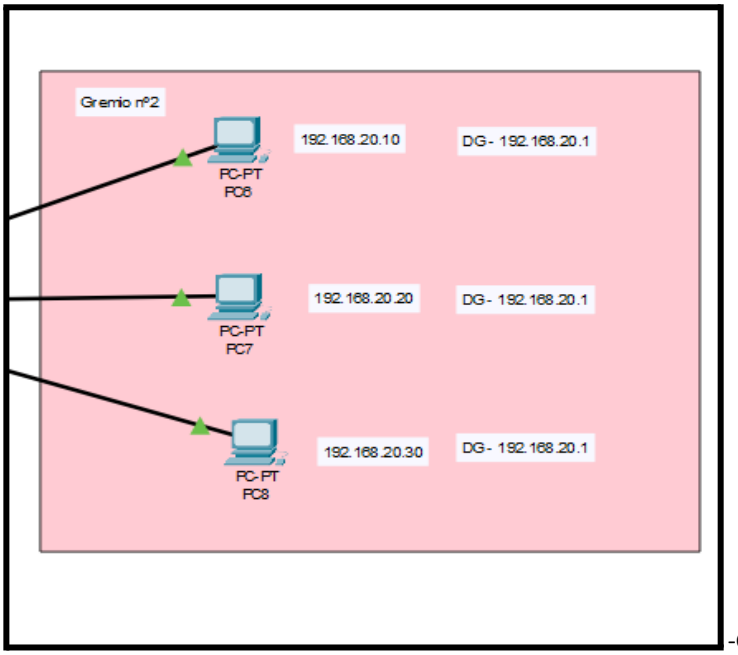
- *Tabla de frame relay de la nube*

Ejercicio 2: La Ciudad de las Redes Aisladas

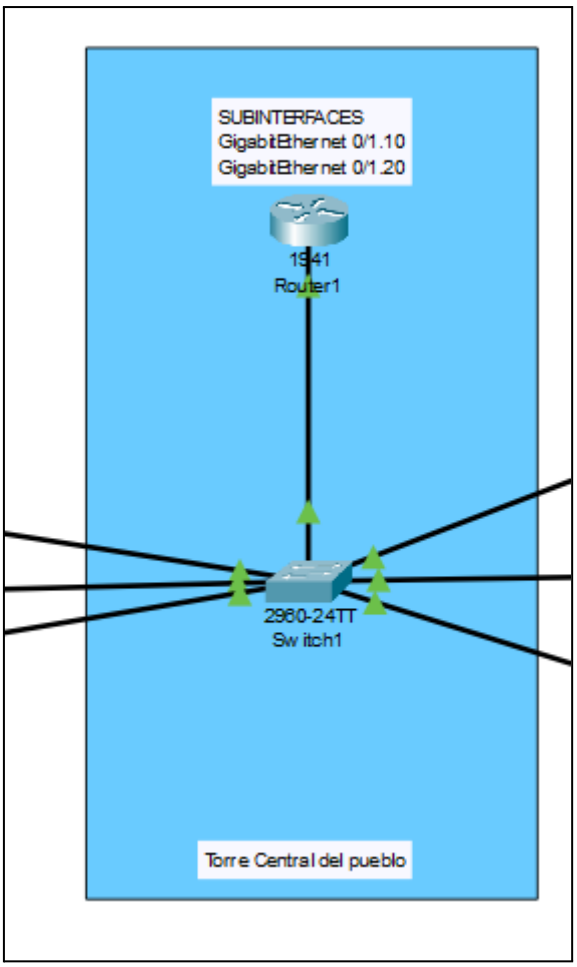
Para plantear este ejercicio, he diseñado dos “Gremios” distintos que trabajan bajo las ip’s 192.168.10.0 y 192.168.20.0, cada uno funciona con su propia VLAN se conectan a un switch central que se conecta a un router central, configurado para almacenar diferentes subintefaces a través del cable GigabitEthernet 0/1.



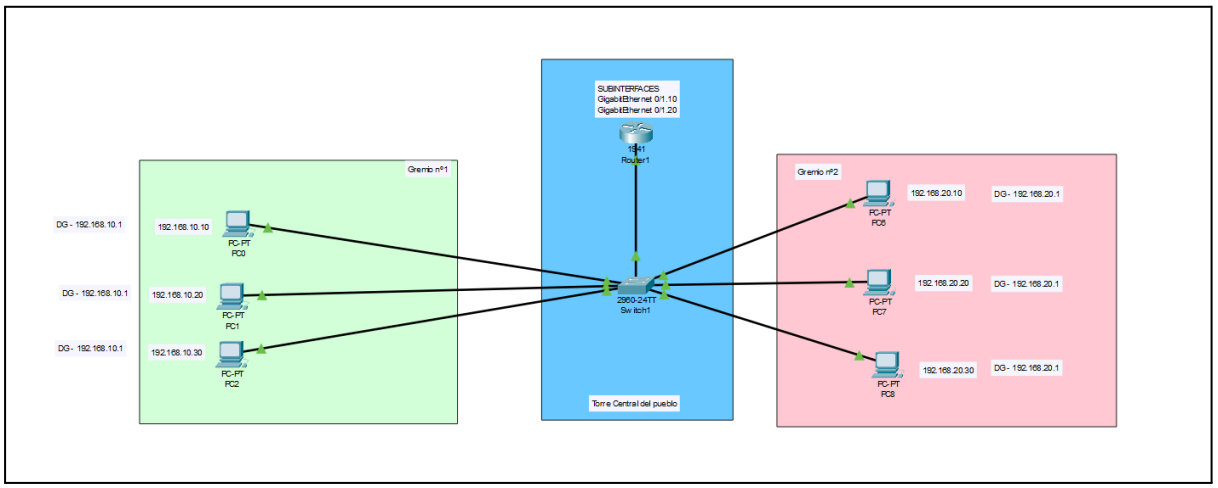
-*Gremio nº1 con ip 198.162.10.X*



-Gremio nº2 con ip 198.162.20.X



- Torre central con subinterfaces



- Esquema general