Parte 1:

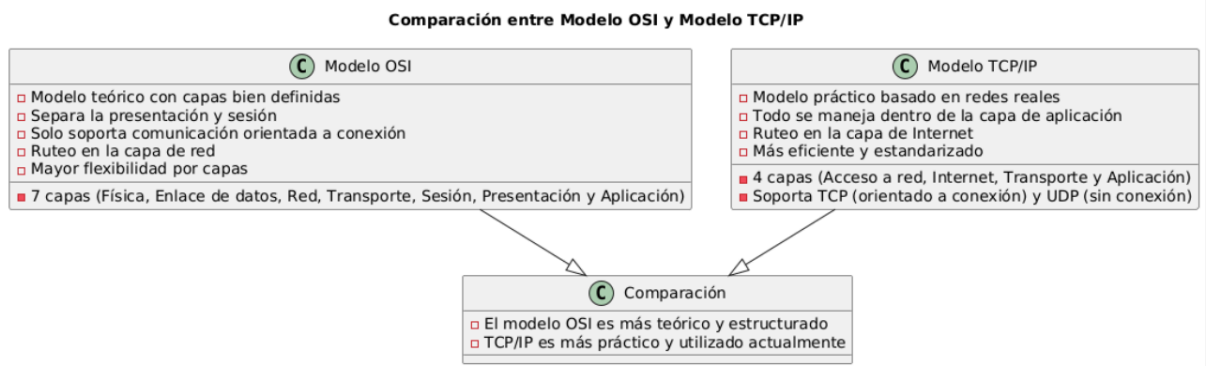
1.El Mural de las Siete Capas:

En el estudio de redes de comunicación, el proceso de transmisión de datos sigue un conjunto de reglas y niveles que garantizan una comunicación eficiente y estructurada. En este contexto, el modelo OSI (Open Systems Interconnection) define **siete capas** que representan las distintas etapas por las que pasa un mensaje desde su origen hasta su destino.

Cada una de estas capas tiene una función específica, asegurando que los datos sean correctamente preparados, transmitidos, transportados y presentados al usuario final. La analogía del mural con siete franjas nos ayuda a visualizar este proceso, ya que, al igual que en el modelo OSI, cada nivel refina o transforma la información antes de que llegue a su destinatario.

A continuación, se presenta una tabla que detalla las capas del modelo OSI y su relación con la estructura del mural encontrado.

Característica	**Modelo OSI**	**Modelo TCP/IP**
Número de capas	7 capas (Física, Enlace de datos, Red, Transporte, Sesión, Presentación y Aplicación)	4 capas (Acceso a red, Internet, Transporte y Aplicación)
Orientación	Modelo teórico con capas bien definidas	Modelo práctico basado en protocolos usados en redes reales
Capa de aplicación	Separa la presentación y sesión	Todo se maneja dentro de la capa de aplicación
Capa de transporte	Solo soporta comunicación orientada a conexión	Soporta tanto conexión (TCP) como sin conexión (UDP)
Ruteo de paquetes	Se realiza en la capa de red	Se realiza en la capa de internet
Flexibilidad	Mayor flexibilidad para definir protocolos en cada capa	Enfocado en la eficiencia y en protocolos ya estandarizados
Conclusión:	El modelo OSI es más estructurado y teórico, mientras que el TCP/IP es un modelo más práctico y utilizado en la actualidad.	



2.Los Dos Pergaminos del Mensajero

En la transmisión de datos dentro de las redes de comunicación, existen diferentes enfoques para garantizar que los mensajes lleguen a su destino de manera eficiente. Algunos métodos priorizan la confiabilidad, asegurando que cada dato enviado sea recibido correctamente, mientras que otros priorizan la velocidad, enviando información sin verificar si ha sido entregada con éxito.

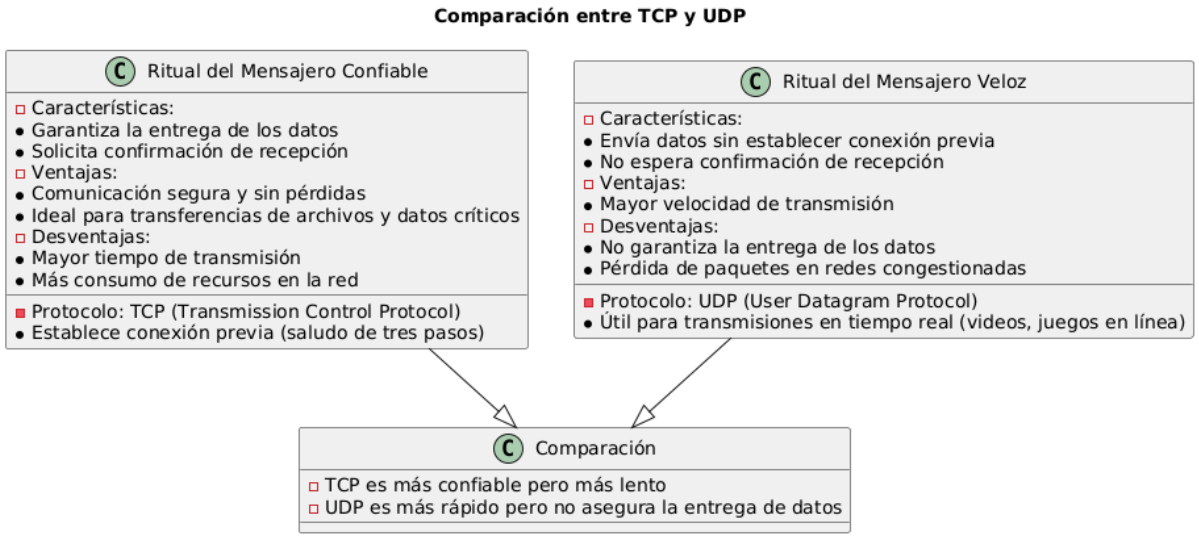
Los dos pergaminos encontrados representan estos dos enfoques a través de metáforas: el Ritual del Mensajero Confiable, que valida la recepción de los mensajes y reintenta el envío en caso de fallos, y el Ritual del Mensajero Veloz, que transmite información sin esperar confirmaciones.

Estos rituales encuentran su equivalencia en los protocolos de comunicación modernos, donde TCP (Transmission Control Protocol) actúa como el mensajero confiable, asegurando la entrega de datos de manera ordenada, mientras que UDP (User Datagram Protocol) representa el mensajero veloz, que envía información rápidamente sin mecanismos de control de errores.

A continuación, se presenta una tabla comparativa que ilustra las características, ventajas y desventajas de cada enfoque en redes modernas.

Ritual	**Protocolo Equivalente**	**Características**	**Ventajas**	**Desventajas**
Ritual del Mensajero Confiable	TCP (Transmission Control Protocol)	Establece una conexión previa (saludo de tres pasos), garantiza la entrega y solicita confirmación. Si un mensaje se pierde, lo reenvía.	Comunicación segura y sin pérdidas. Ideal para envíos de documentos, correos electrónicos y acceso a bases de datos universitarias.	Mayor tiempo de transmisión debido a la verificación constante. Más consumo de recursos en la red.

Ritual del Mensajero Veloz	UDP (User Datagram Protocol)	Envía datos sin establecer conexión previa ni esperar confirmación de recepción.	Mayor velocidad. Útil para videollamadas, transmisiones en vivo de clases y juegos en red.	No garantiza la entrega de todos los datos. Algunos paquetes pueden perderse en la red.



3.El Enigma de las Subredes

La dirección base 192.168.50.0 pertenece a la clase C, cuya máscara por defecto es 255.255.255.0 (/24).

Para dividirla en 4 subredes, necesitamos más bits en la parte de red.

Número de bits necesarios:

- Se requieren 2 bits adicionales en la máscara, ya que 2^2 = 4 subredes
- Nueva máscara: /26 (255.255.255.192)

Con una máscara /26, quedan 6 bits para hosts:

- 2^6 = 64 direcciones totales por subred
- Se restan 2 direcciones (una para la dirección de red y otra para la de broadcast).
- Hosts utilizables: 64−2=62 direcciones por subred.

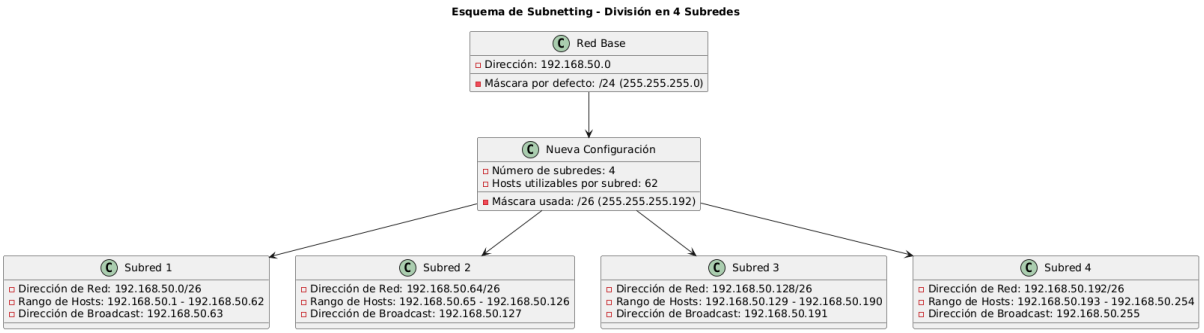
Subred	**Dirección de Red**	**Rango de Hosts**	**Dirección de Broadcast**
Subred 1	192.168.50.0/26	192.168.50.1 - 192.168.50.62	192.168.50.63
Subred 2	192.168.50.64/26	192.168.50.65 -	192.168.50.127

		192.168.50.126	
Subred 3	192.168.50.128/26	192.168.50.129 - 192.168.50.190	192.168.50.191
Subred 4	192.168.50.192/26	192.168.50.193 - 192.168.50.254	192.168.50.255

Resumen

- Máscara utilizada: /26 (255.255.255.192)
- Número de subredes: 4
- Hosts utilizables por subred: 62
- Cada subred tiene su propia dirección de red y de broadcast, evitando interferencias entre departamentos.

Este método permite organizar mejor la red y segmentar el tráfico de cada área sin afectar a las demás.



4.La Encrucijada de las Rutas

El tótem con flechas en la encrucijada representa el concepto moderno de una **tabla de enrutamiento**, que es el mecanismo mediante el cual un router decide por qué camino enviar los datos dentro de una red.

¿Qué es una tabla de enrutamiento y cómo funciona en un router?

Una tabla de enrutamiento es un conjunto de reglas almacenadas en un router que contiene información sobre las rutas disponibles para alcanzar diferentes redes de destino. Cada entrada en la tabla especifica:

- La dirección de la red de destino
- La interfaz o el siguiente salto (next hop) a través del cual los paquetes deben ser enviados
- La métrica o costo de la ruta, en caso de haber múltiples opciones

Cuando un paquete llega a un router, este consulta su tabla de enrutamiento para determinar el mejor camino y reenviarlo al siguiente nodo en la red.

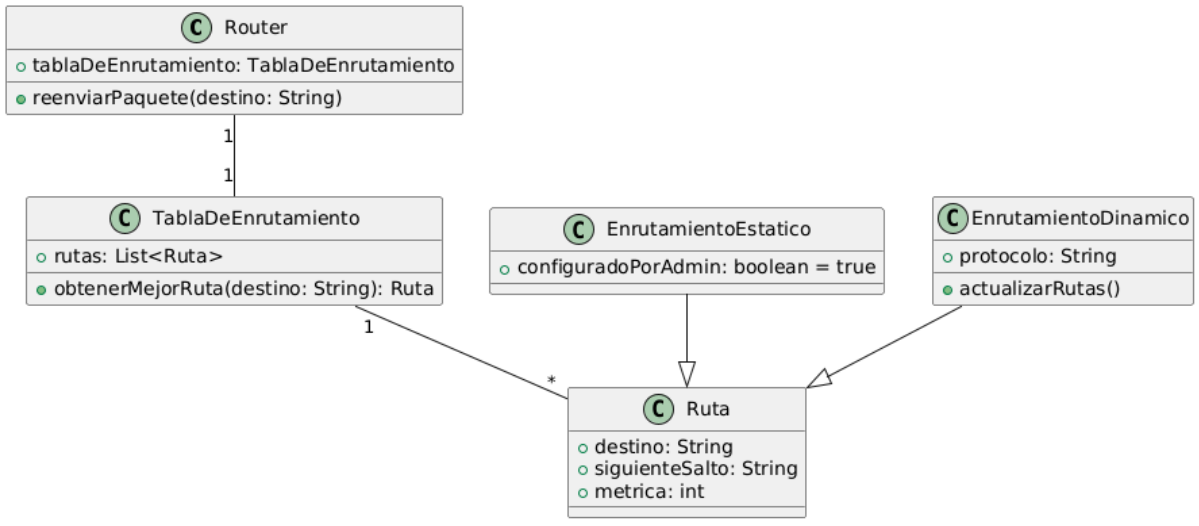
Interpretación de las flechas: Enrutamiento estático vs. dinámico

Elemento en la encrucijada	Equivalente en redes	Descripción
Flechas talladas en piedra	Enrutamiento estático	Rutas configuradas manualmente por un administrador de red. Son fijas y no cambian automáticamente si una ruta deja de estar disponible.
Flechas móviles	Enrutamiento dinámico	Rutas que se ajustan automáticamente según las condiciones de la red, utilizando protocolos como RIP, OSPF o BGP.

Diferencia clave entre enrutamiento estático y dinámico

- El enrutamiento estático es simple y seguro, pero inflexible. Si una ruta falla, el administrador debe actualizar manualmente la tabla.
- El enrutamiento dinámico permite que los routers intercambien información y adapten las rutas en tiempo real, asegurando mejor eficiencia y resiliencia en redes complejas.

En resumen, el tótem actúa como un router primitivo, dirigiendo los caminos de la información según reglas preestablecidas o cambiantes, de la misma manera en que los routers actuales deciden la mejor ruta para los paquetes de datos en Internet.



5.El Guardián de la Máscara Única

La leyenda del Guardián de la Máscara representa el concepto moderno de NAT (Network Address Translation), una técnica utilizada en redes para permitir que múltiples dispositivos dentro de una red privada compartan una única dirección IP pública al comunicarse con el exterior.

¿Qué es NAT y cómo funciona?

NAT es un proceso mediante el cual un router o firewall traduce direcciones IP privadas de los dispositivos internos en una única dirección IP pública cuando estos acceden a Internet. Al recibir respuestas desde el exterior, NAT recuerda qué dispositivo interno originó la solicitud y le reenvía el paquete adecuado.

Este mecanismo se asemeja al guardián de la leyenda porque:

- Cuando un mensaje sale de la red local, NAT reemplaza la dirección IP privada del dispositivo con la dirección pública del router (equivalente a la máscara del guardián).
- Desde el punto de vista del mundo exterior, todos los mensajes parecen provenir de una única dirección (la del guardián).
- Cuando llega una respuesta, NAT recuerda qué dirección privada la originó y la reenvía correctamente (como el guardián devolviendo la máscara a su dueño).

Beneficios de NAT en las redes actuales

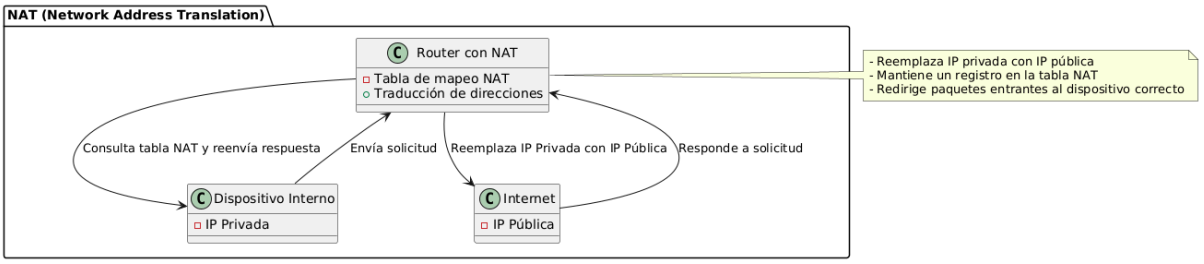
1. Conservación de direcciones IPv4: Dado que el número de direcciones IPv4 es limitado, NAT permite que miles de dispositivos usen una sola dirección pública, optimizando su uso.

2. Mayor seguridad: Los dispositivos internos no son visibles directamente desde el exterior, lo que proporciona una capa adicional de protección contra accesos no autorizados.

En conclusión, NAT actúa como el guardián de la red, ocultando la identidad de los dispositivos internos y permitiéndoles comunicarse con el exterior usando una única dirección IP, asegurando eficiencia y seguridad en la transmisión de datos.

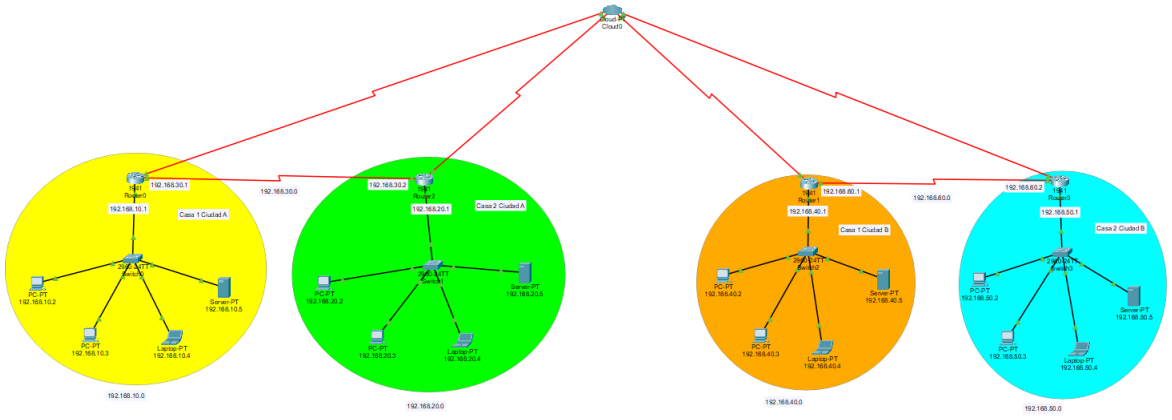
Elemento de la Leyenda	Concepto en Redes	Explicación
Guardián con dos caras	NAT (Network Address Translation)	NAT permite que múltiples dispositivos dentro de una red privada usen una única dirección IP pública para comunicarse con el exterior.
Mensajero que sale con la máscara del guardián	**Traducción de direcciones IP** (NAT)	Cuando un dispositivo de la red interna envía un mensaje al exterior, NAT reemplaza su dirección IP privada con la dirección IP pública de la red.
El guardián recuerda la máscara original	Tabla de mapeo de NAT	NAT mantiene un registro de qué dirección privada envió cada solicitud, para reenviar correctamente las

		respuestas entrantes.
Mensajes de regreso se reenvían al habitante correcto	Redirección de paquetes (NAT dinámico o PAT)	Cuando llega una respuesta desde el exterior, NAT consulta su tabla y dirige el mensaje de vuelta al dispositivo interno correcto.
La ciudad oculta usa un único rostro para el exterior	Ocultación de la red interna	NAT oculta la estructura de la red privada, permitiendo que los dispositivos internos compartan una única dirección IP pública.



Parte 2:

Ejercicio 2: La Ciudad de las Redes Aisladas



La imagen es una topología de red creada en Cisco Packet Tracer, donde se representan varias redes locales (LAN) interconectadas a través de routers y una nube central.

Explicación de la Red

1. **División en Subredes**:

- Hay cuatro redes LAN, cada una representada con un color distinto (amarillo, verde, naranja y celeste).

- Cada LAN tiene un rango de direcciones IP dentro de diferentes subredes.

2. **Dispositivos en cada LAN**:

- Cada LAN contiene un router, un switch, varios PCs, laptops y servidores.

- Los dispositivos finales (PCs y laptops) están conectados al switch, el cual a su vez está conectado al router de la subred.

- Los routers tienen direcciones IP dentro de la subred a la que pertenecen.

3. **Interconexión entre redes**:

- Los routers de cada LAN están conectados entre sí a través de una nube central (Cloud0), la cual representa una conexión de red más amplia (probablemente Internet o una WAN).

- Cada router tiene una interfaz con una IP pública que permite la comunicación entre las distintas redes.

4. **Asignación de Direcciones IP**:

- Cada subred tiene un segmento de red único:

    - 192.168.10.0/24 (Casa 1 Ciudad A)

    - 192.168.20.0/24 (Casa 2 Ciudad A)

    - 192.168.40.0/24 (Casa 1 Ciudad B)

    - 192.168.50.0/24 (Casa 2 Ciudad B)

- Los routers tienen interfaces de conexión con direcciones en la subred 192.168.30.0/24 y 192.168.60.0/24, lo que indica que están actuando como puntos de interconexión entre las redes locales.

Cómo se hizo en Cisco Packet Tracer

- **Routers**: Se agregaron desde la paleta de dispositivos y se configuraron sus interfaces con IPs correspondientes.

- **Switches**: Se añadieron para conectar los dispositivos finales a la red.

- **PCs, laptops y servidores**: Se conectaron a los switches con cables adecuados (cables directos).

- **Configuración de IPs**: Se asignaron direcciones IP estáticas a cada dispositivo dentro de sus respectivas subredes.

- **Conexión entre routers**: Se estableció mediante la nube central, lo que simula una WAN.

Este diseño representa una estructura de comunicación entre diferentes ubicaciones, permitiendo que las PCs en distintas ciudades se comuniquen a través de la red.

Justificación del Uso de la Nube en la Reconstrucción de la Ruta Sagrada de Datos

La inclusión de la nube en esta topología de red representa la modernización de la conectividad entre las ciudades. En el contexto de redes, la nube puede tener varios propósitos clave:

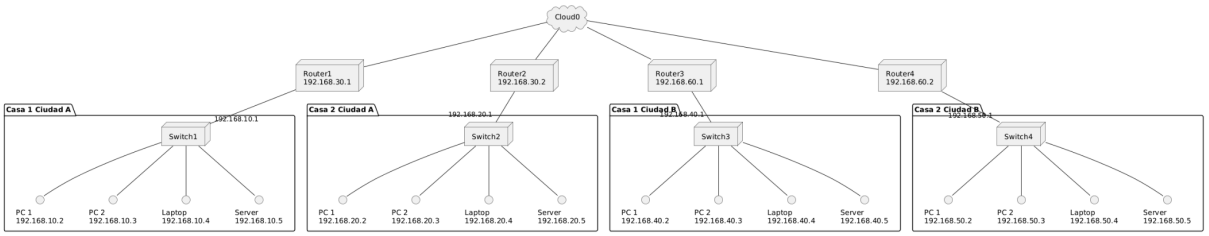
1. **Simulación del Proveedor de Servicios**
- La nube en esta topología representa la infraestructura de un ISP (Proveedor de Servicios de Internet), que facilita la interconexión entre redes distantes.
- En la vida real, las ciudades no suelen estar conectadas directamente con un cable físico punto a punto, sino que dependen de un ISP para la comunicación.

2. **Facilitación del Enrutamiento Escalable**
- En redes empresariales y gubernamentales modernas, el tráfico de datos se enruta a través de la nube utilizando protocolos dinámicos como BGP (Border Gateway Protocol) en lugar de simples rutas estáticas.
- Simular esta conectividad en Packet Tracer ayuda a entender cómo los routers pueden enrutar tráfico a través de la nube sin depender de enlaces físicos directos.

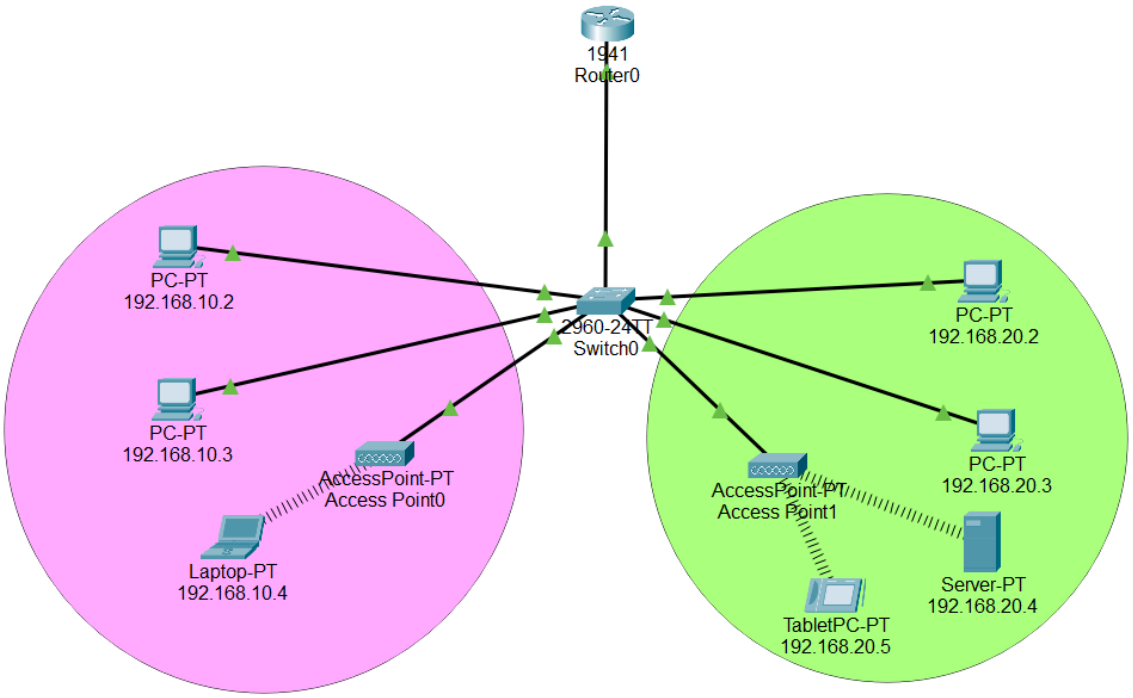
3. **Redundancia y Confiabilidad**
- En el pasado, las ciudades dependían de un único enlace, pero con la nube, pueden existir múltiples caminos de comunicación, mejorando la tolerancia a fallos.
- Si el enlace entre los routers falla, la nube podría representar rutas de respaldo a través de otros medios (como MPLS o VPNs).

4. **Escalabilidad y Expansión de la Red**
- En una red real, más ciudades o sucursales podrían agregarse fácilmente a la nube sin necesidad de modificar la infraestructura física de cada una.
- Esto permite una mejor administración y expansión sin costos excesivos.

En conclusión, la nube en esta simulación representa la infraestructura moderna que permite interconectar redes distantes sin necesidad de enlaces físicos directos. A través de ella, las ciudades pueden compartir información y recursos de manera más eficiente, segura y escalable



Ejercicio 2: La Ciudad de las Redes Aisladas



La imagen muestra una topología de red creada en Cisco Packet Tracer, en la que se han configurado dos VLANs (VLAN 10 y VLAN 20) para segmentar la red. A continuación, te explico los elementos de la topología:

1. Dispositivos en la Red

Router 1941 (Router0):

- Es el dispositivo encargado de la comunicación entre las diferentes VLANs.
- Se conecta al Switch0 mediante un enlace troncal (*trunk*), permitiendo el tráfico de ambas VLANs.

Switch 2960-24TT (Switch0):
Es el punto central de conexión para ambas VLANs. Se han creado dos VLANs en este switch:

- VLAN 10: Para la red con IP 192.168.10.x
- VLAN 20: Para la red con IP 192.168.20.x

Los puertos del switch han sido asignados a las respectivas VLANs.

Access Points (Puntos de acceso inalámbricos)
Access Point0

- Conectado a Switch0 en un puerto de acceso en VLAN 10.
- Permite la conexión inalámbrica de los dispositivos con direcciones 192.168.10.x.

Access Point1

- Conectado a Switch0 en un puerto de acceso en VLAN 20.
- Permite la conexión de dispositivos con direcciones 192.168.20.x.

Dispositivos finales:
Se han conectado computadoras (PC-PT), un Laptop-PT, un TabletPC-PT y un Server-PT.
Se dividen en dos VLANs diferentes:

- VLAN 10 (192.168.10.x) → Conectados a Access Point0.
- VLAN 20 (192.168.20.x) → Conectados a Access Point1.

Comunicación entre VLANs

- Dentro de cada VLAN, los dispositivos pueden comunicarse entre sí de manera directa.
- Para la comunicación entre VLAN 10 y VLAN 20, el router actúa como gateway usando Inter-VLAN Routing con subinterfaces.

Este diseño mejora la segmentación y seguridad de la red, asegurando que cada VLAN tenga su propio dominio de broadcast.