



Proyecto Final

**Maestra: Blanca Aracely Aranda Machorro
Monterrey Nuevo León a 23 de Enero del 2025**

Índice

| | |
|--|-----------|
| 1. Caso (Contexto de la empresa) | 4 |
| 2. Objetivo | 4 |
| 3. Definición de requerimientos: | 5 |
| 3.1 Requerimientos de la Red | 5 |
| 3.2 Objetivos de la Red | 5 |
| 3.3 Puntos Claves a Considerar | 5 |
| 4. Proceso de el Diseño de la red: | 6 |
| 4.1 Topología de Red | 6 |
| 4.3 División de redes | 8 |
| 5. Configuración de los dispositivos: | 10 |
| 5.1Subredes IPV4 | 10 |
| Pruebas de Conectividad entre Sedes: | 13 |
| Pruebas de Red con "Simple PDU": | 13 |
| 7.- Implementación de Servidor FTP: | 14 |
| 8.-Conexiones Inalámbricas | 15 |
| 9.-Implementación DHCP | 16 |
| 10.-Autenticacion Usuarios FTP | 19 |
| 11.-Autenticación SSH en Routers | 19 |
| 12.- Identificación de Amenazas Comunes | 20 |
| Glosario | 29 |
| Bibliografía: | 31 |
| Autores | 32 |
| Conclusiones | 34 |

Proyecto TecmiNetCorp



Equipo 3 NetCraft

1. Caso (Contexto de la empresa)

1.1 Caso

Eres un consultor de redes y fuiste contratado por "TecmiCorp", una pequeña empresa en expansión. La organización necesita una actualización en su infraestructura de red para responder a la creciente demanda de conectividad por parte de sus empleados y clientes. Con una sede central y cinco sucursales, es imperativo establecer una red sólida y escalable, capaz de adaptarse al crecimiento del negocio.

En la primera fase del proyecto, el enfoque se centrará en el diseño y la configuración de las redes tanto para el sitio principal como para las sucursales. Aplicando los conocimientos adquiridos para desarrollar una infraestructura de red segura y escalable.

Para satisfacer las necesidades de conectividad de "TecmiCorp", se requiere conectar en la sede principal 5 equipos de escritorio y 5 laptops; en tanto que, en cada sucursal es necesario conectar 1 equipo de escritorio y 3 laptops.

1.2 Qué es TecmiCorp

TecmiCorp es una empresa especializada en soluciones tecnológicas y telecomunicaciones, que ofrece servicios de infraestructura de redes, seguridad informática y servicios en la nube a empresas de diferentes sectores.

| Sucursal | Funcion |
|------------|---------------------------------------|
| Sucursal 1 | Soporte Técnico Remoto |
| Sucursal 2 | Desarrollo de Software |
| Sucursal 3 | Seguridad y Monitoreo de Redes |
| Sucursal 4 | Servicios en la Nube y Hosting |
| Sucursal 5 | Gestión de Infraestructura y Hardware |

2. Objetivo

Diseñar y configurar una red empresarial mediante Cisco Packet Tracer, para establecer una infraestructura sólida que proporcione conectividad y soporte para los dispositivos de red de una empresa en crecimiento.

3. Definición de requerimientos:

3.1 Requerimientos de la Red

Para que la conectividad y el soporte necesarios puedan lograrse, se necesitan de ciertos requerimientos tanto técnicos como operativos:

Dispositivos y Conexiones

- **Sede Central:**
 - 5 Computadoras de escritorio (Conexión Cableada)
 - 5 Laptops (Conexión Wi-Fi)
 - 1 Router Principal para gestionar la conexión de la **Sede Central** y las Sucursales
 - 1 switch administrable para conectar los dispositivos cableados
 - 1 Access Point (AP) para proporcionar conectividad inalámbrica a las laptops
- **Sucursales (5 en total):**
 - 1 Computadora de escritorio (Conexión Cableada)
 - 3 laptops (Conexión Wi-Fi)
 - 1 Router para conectar la Sucursal con la **Sede Central**.
 - 1 Switch de acceso para la conexión de dispositivos cableados
 - 1 Access Point (AP) para conectar las laptops

3.2 Objetivos de la Red

- Conectar todos los dispositivos en la **Sede Central** y **Sucursales** de forma eficiente.
- Permitir la comunicación entre la **Sede Central** y las **Sucursales** mediante routers y Direcciónamiento IP.
- Garantizar acceso a Internet y recursos internos a través de la configuración de la red.
- Implementar **Seguridad Básica**, como contraseñas para Wi-Fi y segmentación de redes con VLANs.

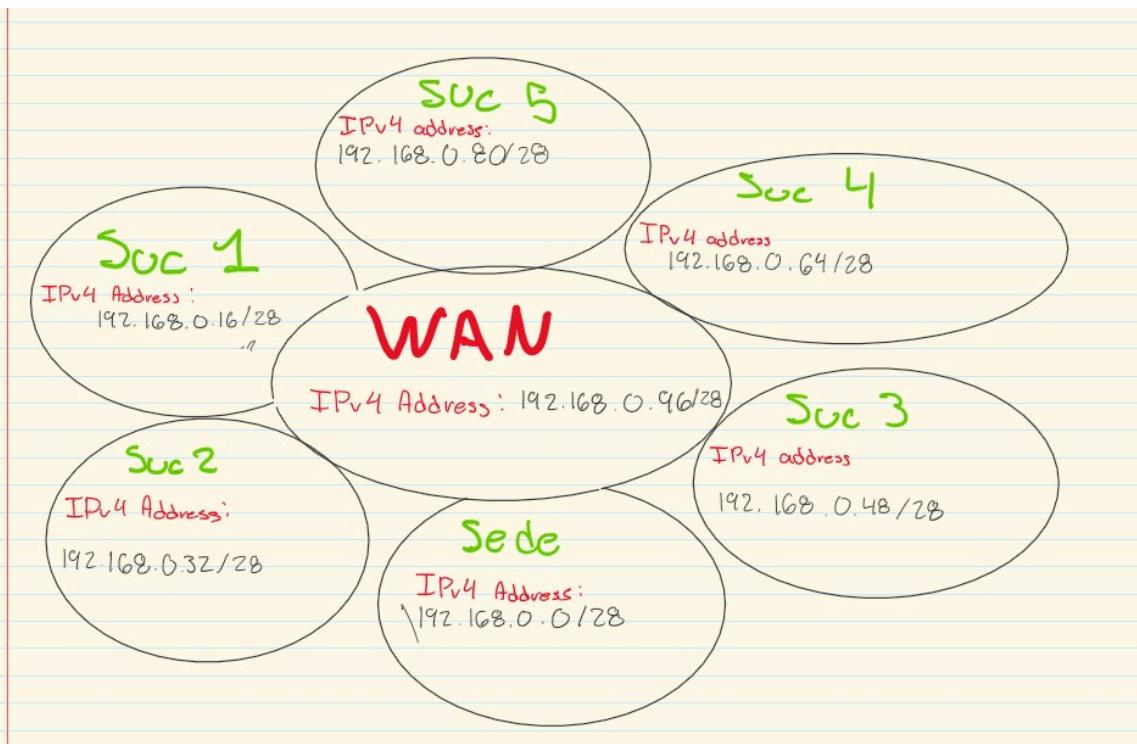
3.3 Puntos Claves a Considerar

- Dirección IP y Subredes: Se dividirá la red en subredes para organizar mejor los dispositivos.

- Asignación de Direcciones: Se usará DHCP para asignar direcciones IP automáticamente.
- Wi-Fi Seguro: Se configurará Wi-Fi con cifrado WPA2 para proteger la red.
- Red Escalable: La Topología debe permitir la adición de más dispositivos a futuro.

4. Proceso de el Diseño de la red:

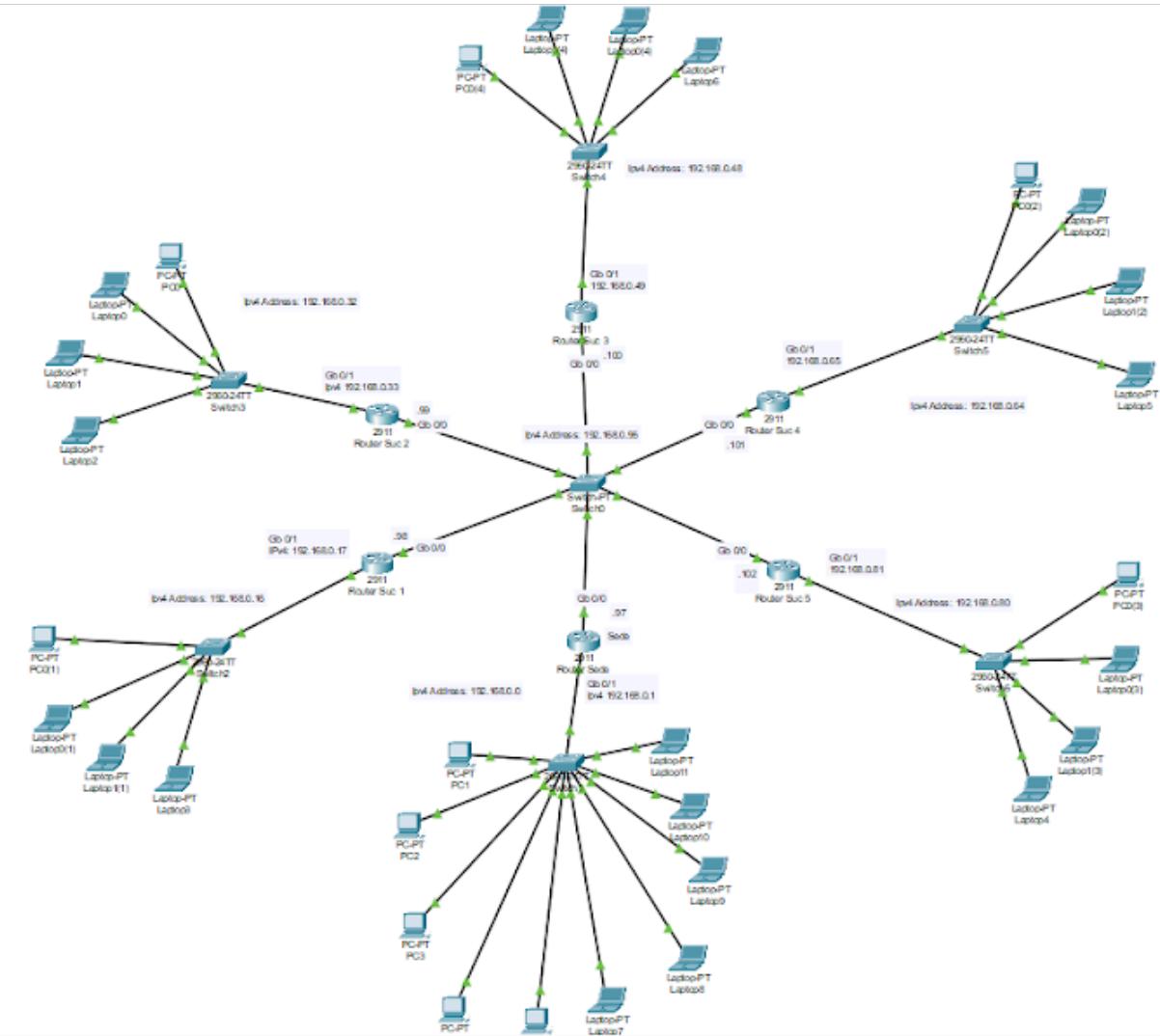
4.1 Topología de Red



Topología de Estrella

Seleccionamos una topología de Estrella, en base a un análisis que realizamos comparando con otras topologías como bus o anillo ya que a diferencia de alguna de estas la topología de Estrella puede seguir funcionando si algún equipo llega a ser removido mientras esté no sea el central a diferencia de las otras topologías que pueden llegar a dejar de funcionar si alguno de sus equipos es removido.

4.2 Dispositivos que conforman la Red

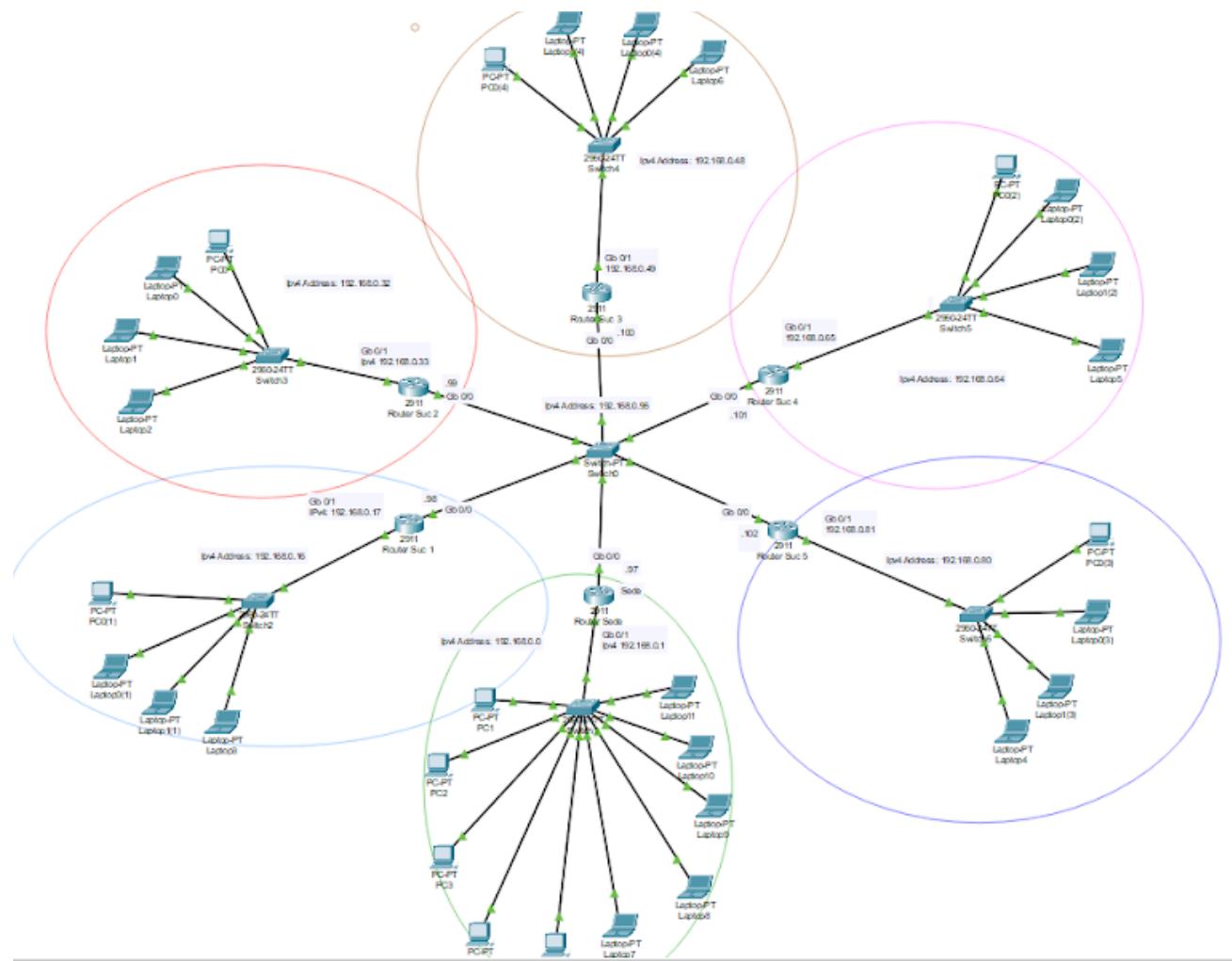


La imagen representa la distribución de los dispositivos que conformarán la red. Entre ellos se encuentran los routers, encargados de gestionar el tráfico entre subredes, y los switches, que facilitan la comunicación entre los distintos dispositivos dentro de la misma red. Su disposición estratégica contribuye a optimizar el rendimiento y reducir la latencia en la transmisión de datos.

Por otro lado los dispositivos, como computadoras y laptops, corresponden a los equipos que harán uso de la infraestructura de red. Este esquema permite visualizar de manera clara la organización de los elementos de la red, lo que facilita su implementación y garantiza un diseño eficiente para cumplir con las necesidades de conectividad.

El diseño de la red busca proporcionar una infraestructura eficiente, escalable y segura para la sede principal y las sucursales de la empresa. Esto incluye garantizar la conectividad entre dispositivos, segmentación adecuada de la red y seguridad en las comunicaciones.

4.3 División de redes



En la imagen se representa la división de una red en varias subredes, cada una diferenciada por un color específico. En el centro se encuentra la red principal (RED 1), que alberga los dispositivos clave, como routers y switches, encargados de gestionar la conectividad entre todas las subredes. Las secciones contienen computadoras y laptops que dependen de la red principal para acceder a los recursos y mantener la comunicación entre sí.

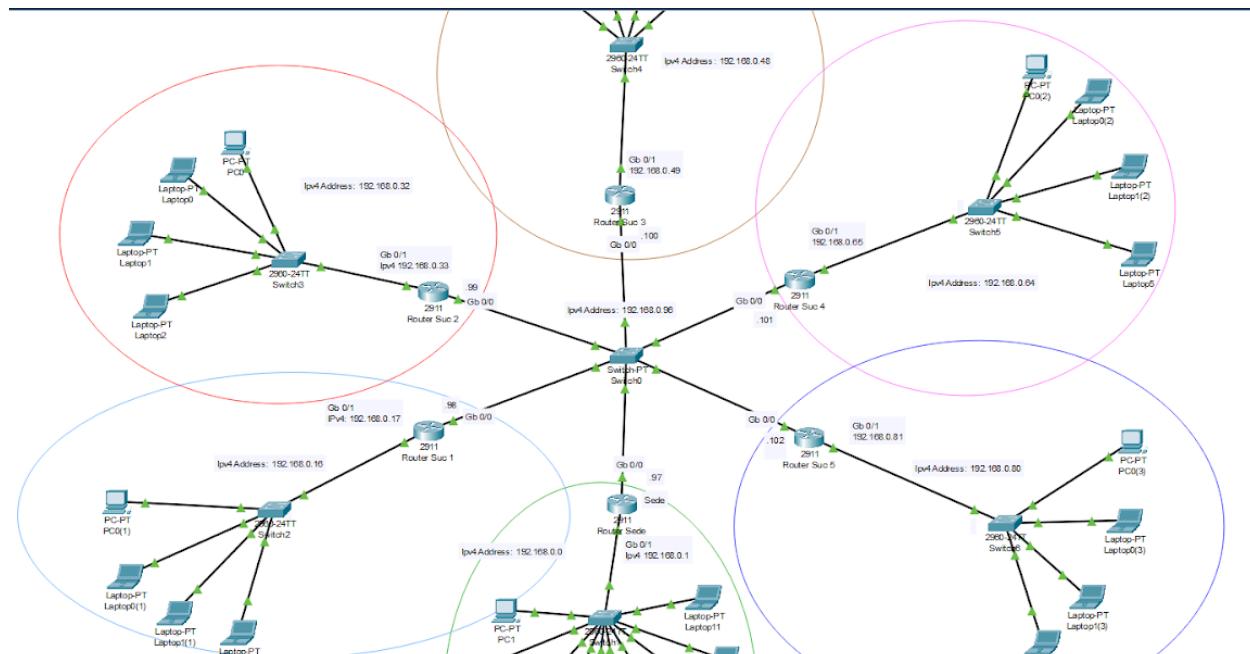
Esta organización sugiere una estructura optimizada para distribuir eficientemente el tráfico de datos y mejorar la seguridad, permitiendo aislar segmentos según sea necesario. La segmentación en diferentes áreas facilita la administración de la red y su planificación, asegurando un rendimiento óptimo y una mejor gestión de la infraestructura.

Conexiones entre dispositivos:

- Router Sede Principal → Switch Sede Principal → Dispositivos finales (PCs, laptops)
- Router Sucursales → Switch Sucursal → Dispositivos finales (PCs, laptops)
- Conexión WAN entre el Router Sede Principal y los Routers de las sucursales (puedes simular una conexión a través de un cable Serial o Ethernet dependiendo del tipo de conexión WAN que utilices).

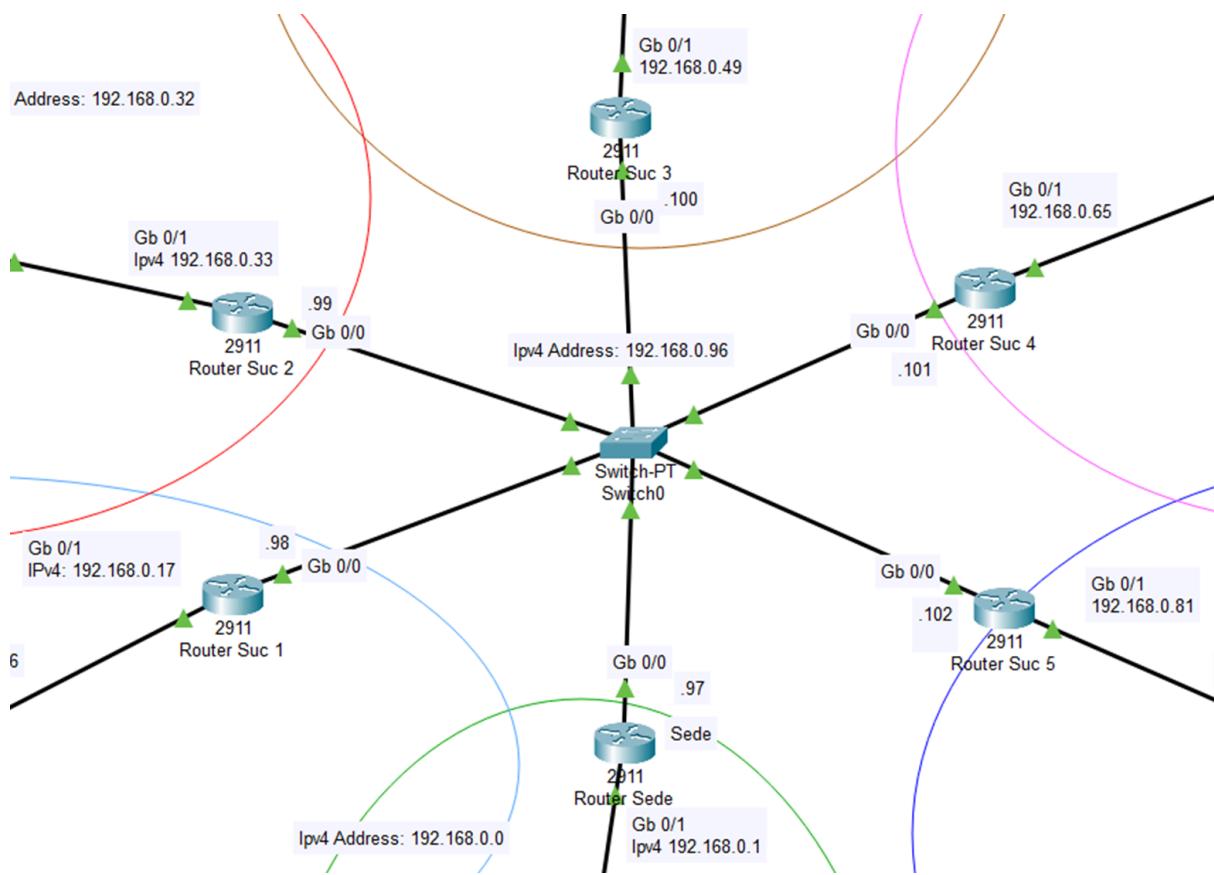
Segmentación de la red:

- VLANs: Para optimizar la gestión del tráfico y mejorar la seguridad, se han creado VLANs para separar diferentes tipos de tráfico (por ejemplo, una VLAN para empleados, otra para servidores, etc.).



5. Configuración de los dispositivos:

5.1 Subredes IPV4



En la imagen se representa la división de una red en varias subredes IPv4, estructuradas para conectar diferentes sucursales y una sede principal a través de una red WAN. Cada ubicación dispone de un bloque de direcciones IPv4 específico con una máscara de subred /28, lo que facilita una asignación eficiente de direcciones y una mejor organización de la comunicación interna.

Esta distribución permite gestionar el tráfico de datos de manera más efectiva, reforzar la seguridad y mejorar el control sobre los dispositivos en la red. La WAN funciona como el canal principal que enlaza todas las sucursales con la sede, garantizando una conectividad bien estructurada y acorde a las necesidades de la red.

5.2 Configuración de routers

Esta configuración de rutas estáticas se hace por la razón de que como cada router no tiene “Visibilidad” aparte de su propia red a la que se encuentra conectada tenemos que configurar las rutas estáticas para cada router para darle la instrucción al router de donde mandar los paquetes en caso de tener un paquete con “x” dirección

Config Router sede:

| | | |
|--------------------------------------|-----------------|---------------|
| Hacía Rsuc 1 - IP route 192.168.0.16 | 255.255.255.240 | 192.168.0.98 |
| Hacía Rsuc 2 - IP route 192.168.0.32 | 255.255.255.240 | 192.168.0.99 |
| Hacía Rsuc 3 - IP route 192.168.0.48 | 255.255.255.240 | 192.168.0.100 |
| Hacía Rsuc 4 - IP route 192.168.0.64 | 255.255.255.240 | 192.168.0.101 |
| Hacía Rsuc 5 - IP route 192.168.0.80 | 255.255.255.240 | 192.168.0.102 |

Config Router Suc 1:

| | | |
|--------------------------------------|-----------------|---------------|
| Hacía Rsuc 1 - IP route 192.168.0.0 | 255.255.255.240 | 192.168.0.97 |
| Hacía Rsuc 2 - IP route 192.168.0.32 | 255.255.255.240 | 192.168.0.99 |
| Hacía Rsuc 3 - IP route 192.168.0.48 | 255.255.255.240 | 192.168.0.100 |
| Hacía Rsuc 4 - IP route 192.168.0.64 | 255.255.255.240 | 192.168.0.101 |
| Hacía Rsuc 5 - IP route 192.168.0.80 | 255.255.255.240 | 192.168.0.102 |

Config Router Suc 2:

| | | |
|--------------------------------------|-----------------|---------------|
| Hacía Rsuc 1 - IP route 192.168.0.16 | 255.255.255.240 | 192.168.0.98 |
| Hacía Rsuc 2 - IP route 192.168.0.0 | 255.255.255.240 | 192.168.0.97 |
| Hacía Rsuc 3 - IP route 192.168.0.48 | 255.255.255.240 | 192.168.0.100 |
| Hacía Rsuc 4 - IP route 192.168.0.64 | 255.255.255.240 | 192.168.0.101 |
| Hacía Rsuc 5 - IP route 192.168.0.80 | 255.255.255.240 | 192.168.0.102 |

Config Router Suc 3:

| | | |
|--------------------------------------|-----------------|---------------|
| Hacía Rsuc 1 - IP route 192.168.0.16 | 255.255.255.240 | 192.168.0.98 |
| Hacía Rsuc 2 - IP route 192.168.0.32 | 255.255.255.240 | 192.168.0.99 |
| Hacía Rsuc 3 - IP route 192.168.0.0 | 255.255.255.240 | 192.168.0.97 |
| Hacía Rsuc 4 - IP route 192.168.0.64 | 255.255.255.240 | 192.168.0.101 |
| Hacía Rsuc 5 - IP route 192.168.0.80 | 255.255.255.240 | 192.168.0.102 |

Config Router Suc 4:

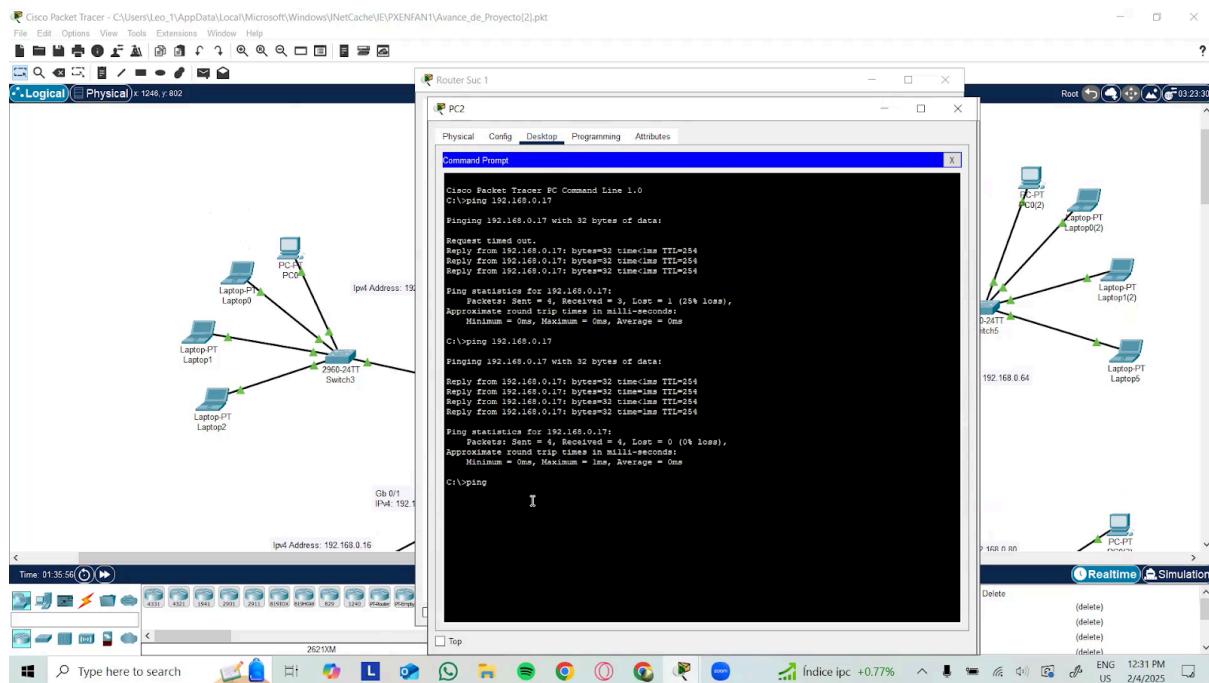
| | | |
|--------------------------------------|-----------------|---------------|
| Hacía Rsuc 1 - IP route 192.168.0.16 | 255.255.255.240 | 192.168.0.98 |
| Hacía Rsuc 2 - IP route 192.168.0.32 | 255.255.255.240 | 192.168.0.99 |
| Hacía Rsuc 3 - IP route 192.168.0.48 | 255.255.255.240 | 192.168.0.100 |
| Hacía Rsuc 4 - IP route 192.168.0.0 | 255.255.255.240 | 192.168.0.97 |
| Hacía Rsuc 5 - IP route 192.168.0.80 | 255.255.255.240 | 192.168.0.102 |

Config Router Suc 5:

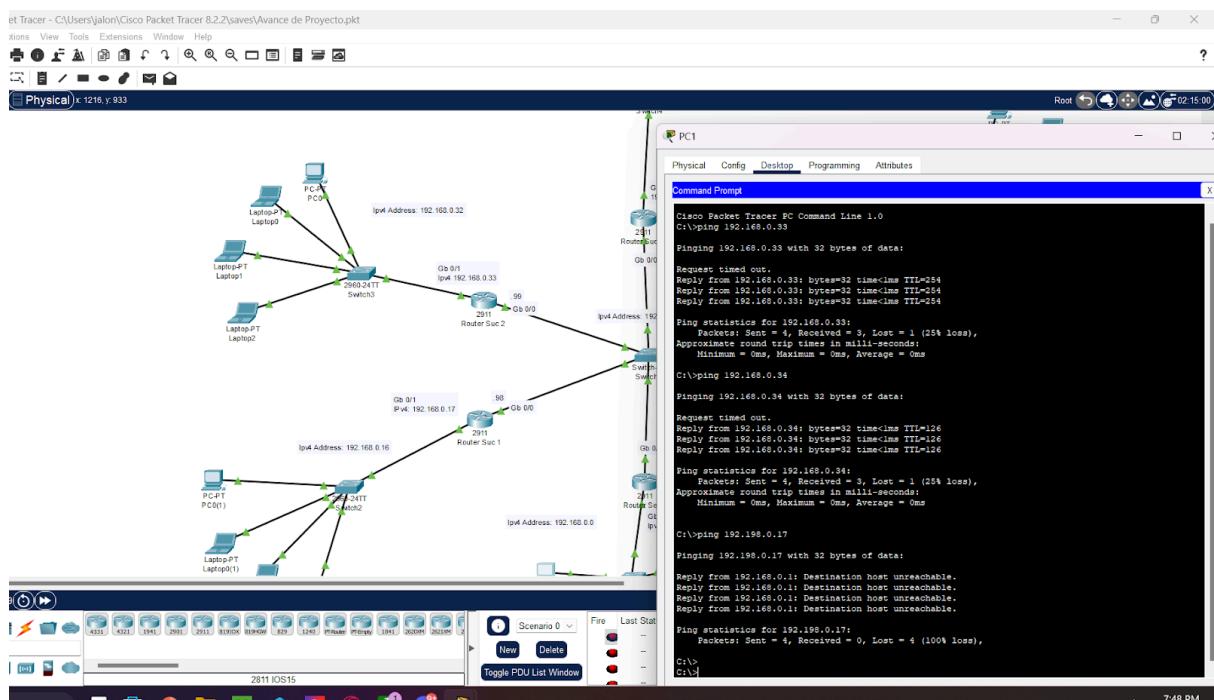
| | | | |
|-------------------------|--------------|-----------------|---------------|
| Hacía Rsuc 1 - IP route | 192.168.0.16 | 255.255.255.240 | 192.168.0.98 |
| Hacía Rsuc 2 - IP route | 192.168.0.32 | 255.255.255.240 | 192.168.0.99 |
| Hacía Rsuc 3 - IP route | 192.168.0.48 | 255.255.255.240 | 192.168.0.100 |
| Hacía Rsuc 4 - IP route | 192.168.0.64 | 255.255.255.240 | 192.168.0.101 |
| Hacía Rsuc 5 - IP route | 192.168.0.0 | 255.255.255.240 | 192.168.0.97 |

Con la información anterior el router estático es fundamental en este caso para establecer la comunicación entre sucursales y la sede. Dado que el router que recibe un paquete no posee la información necesaria para determinar su destino exacto, mediante rutas estáticas se le indica específicamente a cada router a qué dirección IP debe enviar los paquetes dirigidos a una determinada red.

6. Prueba de conectividad Local



Pruebas de Conectividad entre Sedes:



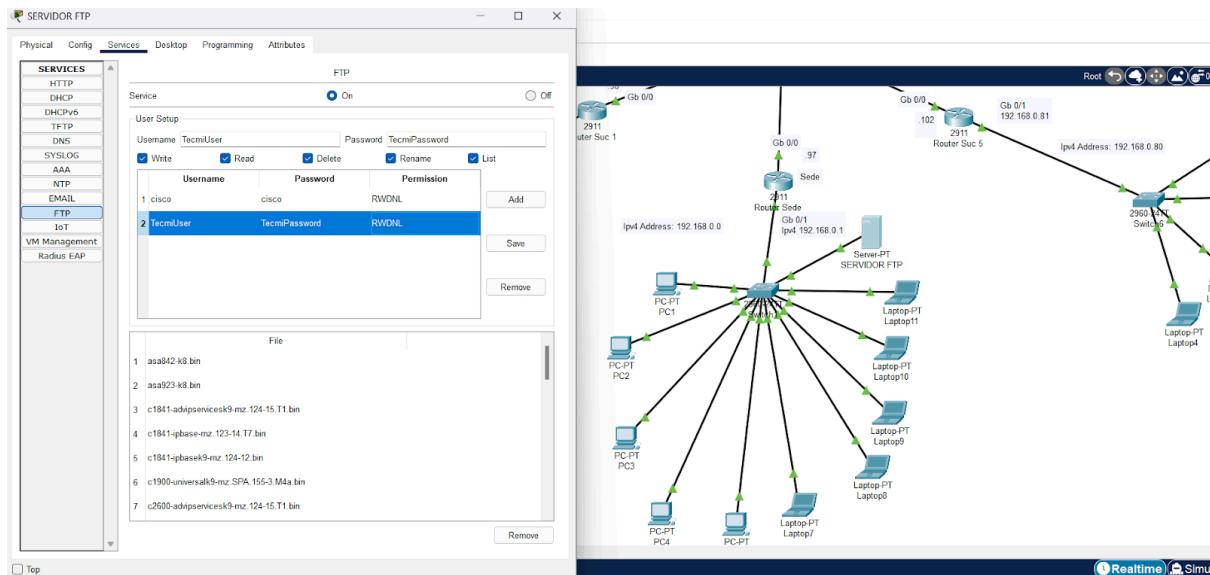
Aquí desde la una de las computadoras de la sede mandamos a hacer ping a 3 diferentes computadoras de 2 sedes distintas y podemos ver como como llegan la respuestas confirmando la correcta comunicación

Pruebas de Red con "Simple PDU":

| PDU List Window | | | | | | | | | | |
|-----------------|-------------|-----------|-------------|------|-------|-----------|----------|-----|--------|----------|
| Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete |
| ● | Successful | PC0(4) | PC0(2) | ICMP | ■ | 0.000 | N | 0 | (edit) | (delete) |
| ● | Successful | PC0(4) | PC0(4) | ICMP | ■ | 0.000 | N | 1 | (edit) | (delete) |
| ● | Successful | Laptop1 | Laptop1(2) | ICMP | ■ | 0.000 | N | 2 | (edit) | (delete) |
| ● | Successful | Laptop... | PC2 | ICMP | ■ | 0.000 | N | 3 | (edit) | (delete) |
| ● | Successful | PC0(1) | Laptop9 | ICMP | ■ | 0.000 | N | 4 | (edit) | (delete) |
| ● | Successful | Laptop2 | PC4 | ICMP | ■ | 0.000 | N | 5 | (edit) | (delete) |

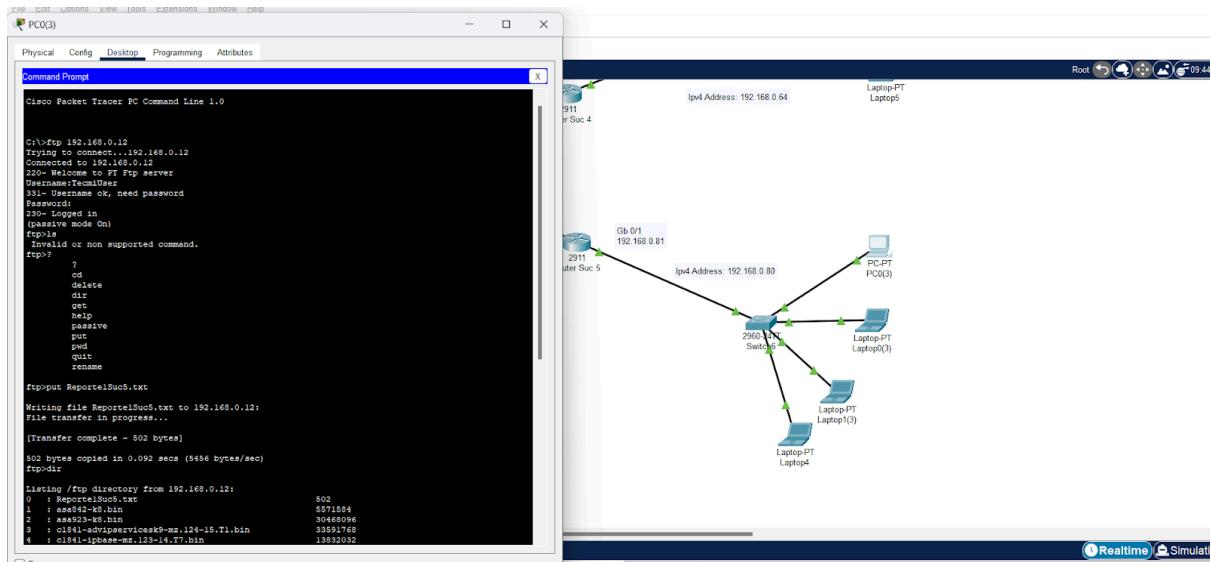
6.- Implementación de Servidor FTP:

En este punto agregamos un servidor para habilitar la transmisión de archivos a través de este con el uso de credenciales establecidas en el mismo

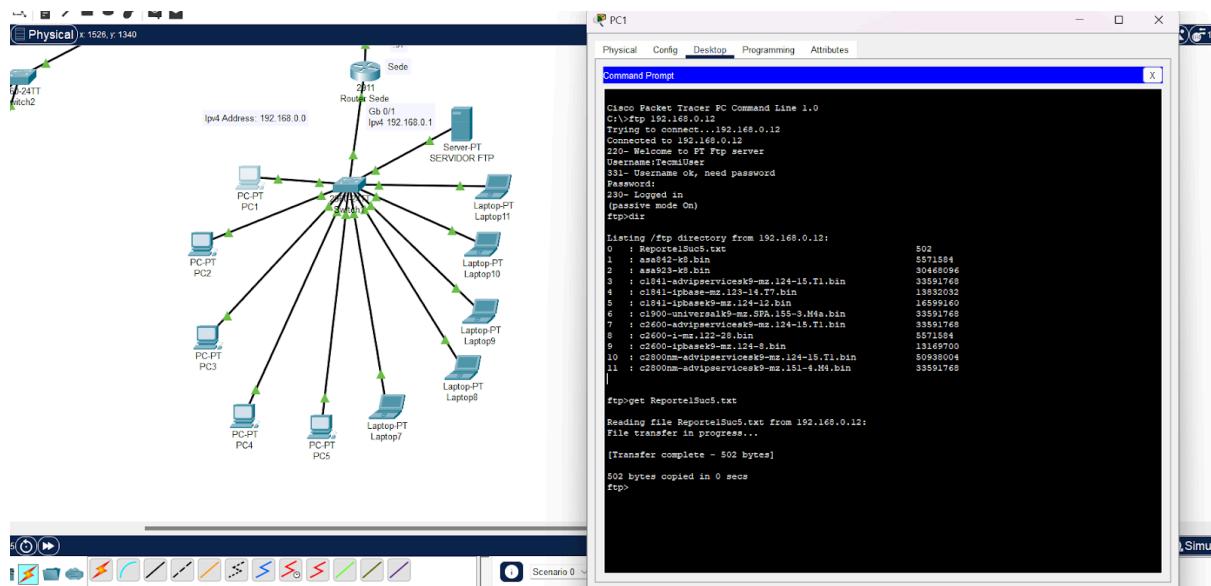


Conectamos el Servidor a la sede central y agregamos las credenciales con las cuales van a poder conectarse los demás usuarios de la red llamado TecmiUser con TecmiPassword de contraseña

Para comprobar la funcionalidad de este vamos a generar un archivo de texto para simular un reporte de sucursal. Este va a ser desde la pc de la sucursal 5 y se va cargar al servidor ftp y ya desde una pc de la sede central se va a descargar para dar como éxito la implementación del servidor ftp



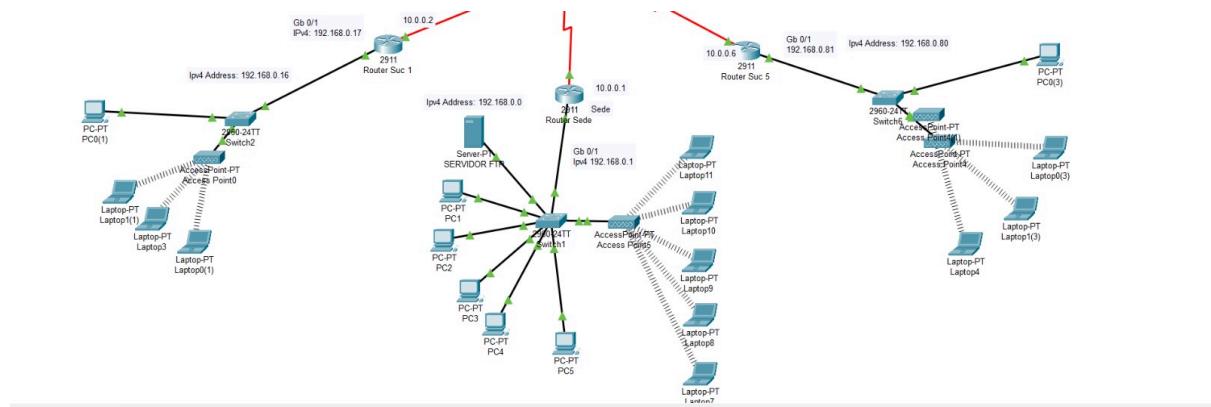
Subida de Archivo desde Sucursal 5 y se confirma de que se encuentra dentro del servidor

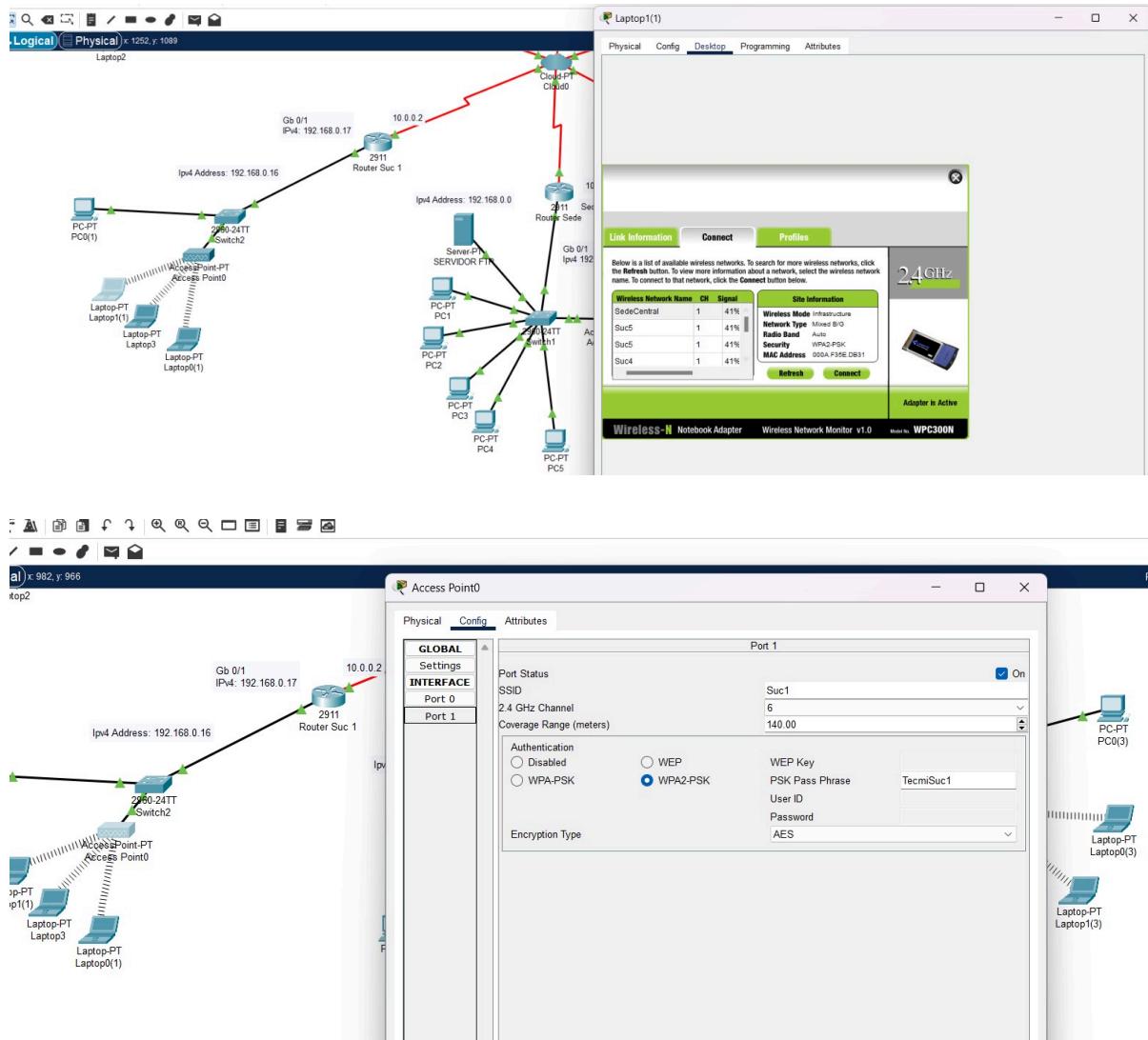


Descarga del archivo desde Sede Central

7.-Conexiones inalámbricas

Decidimos emplear conexiones inalámbricas ya que al tener sucursales en distintos puntos, es más viable usarlas de maneras inalámbricas, en este caso mantendremos los routers en la sede central y nos comunicaremos con ellos vía inalámbrica con módems, cada sucursal contará con uno de estos, con una conexión inalámbrica nos ahorraremos problemas que tendríamos con conexiones alámbricas, como pueden ser la extensión del cableado.



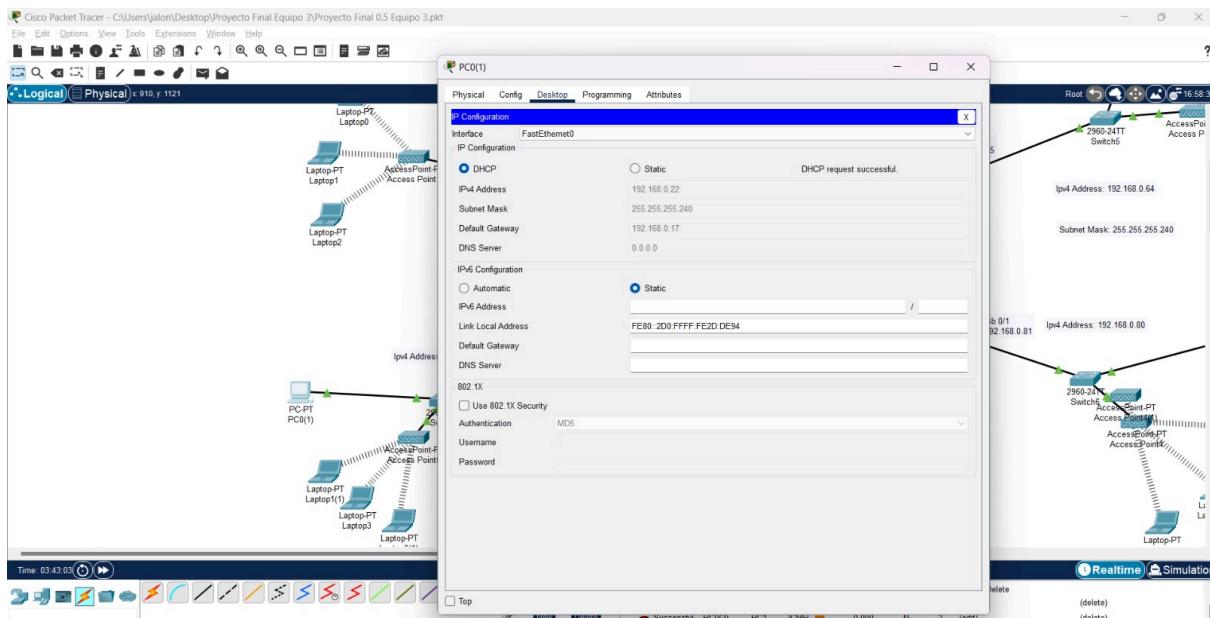
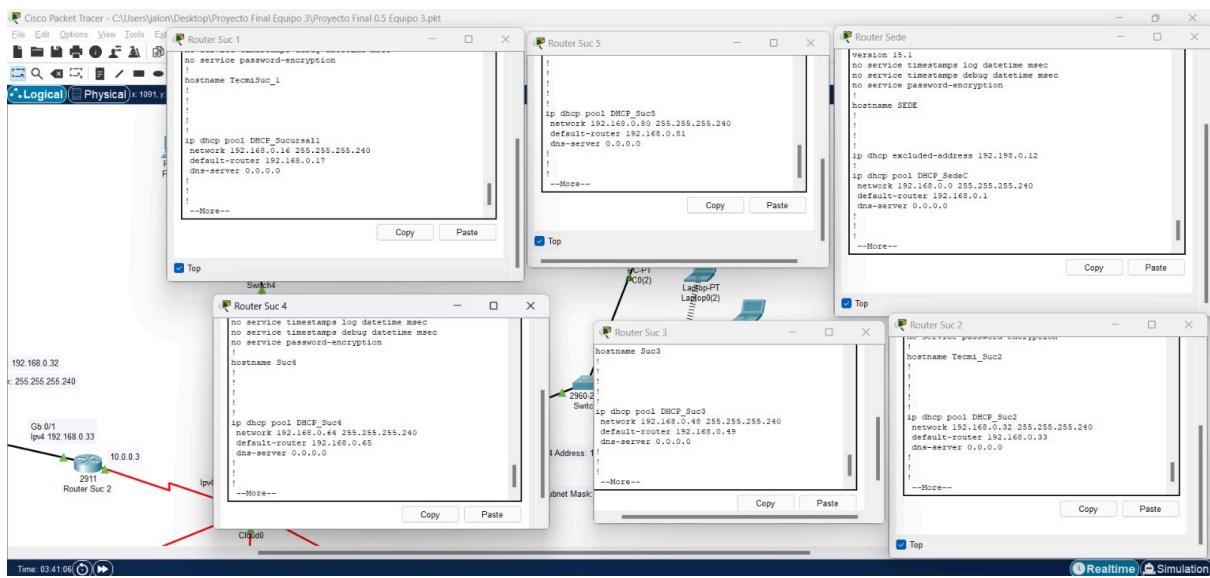


8.-Implementación de DHCP

Para optimizar la gestión de direcciones IP en la red de **TecmiCorp**, se implementó **DHCP (Dynamic Host Configuration Protocol)** tanto en la sede central como en cada una de las sucursales. Esta configuración permite que los dispositivos obtengan automáticamente una dirección IP válida dentro de su respectiva subred, evitando la necesidad de configuraciones manuales, reduciendo errores y facilitando la administración de la red.

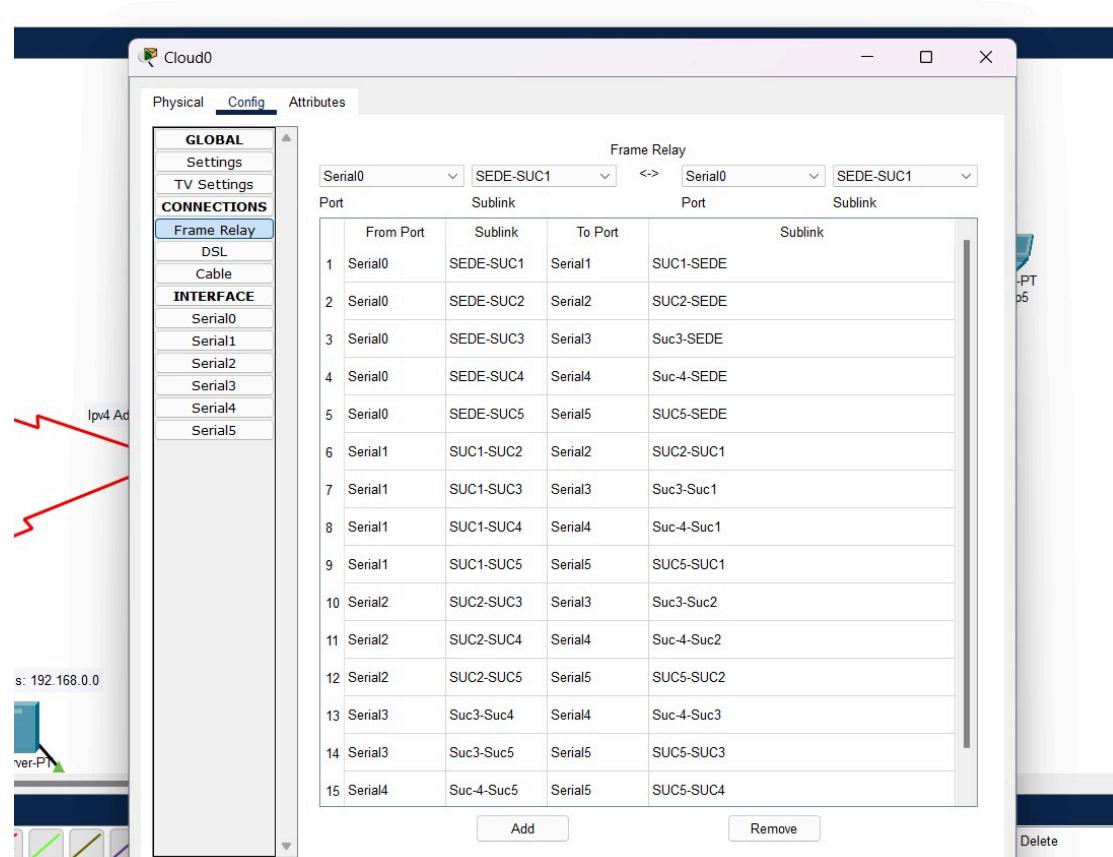
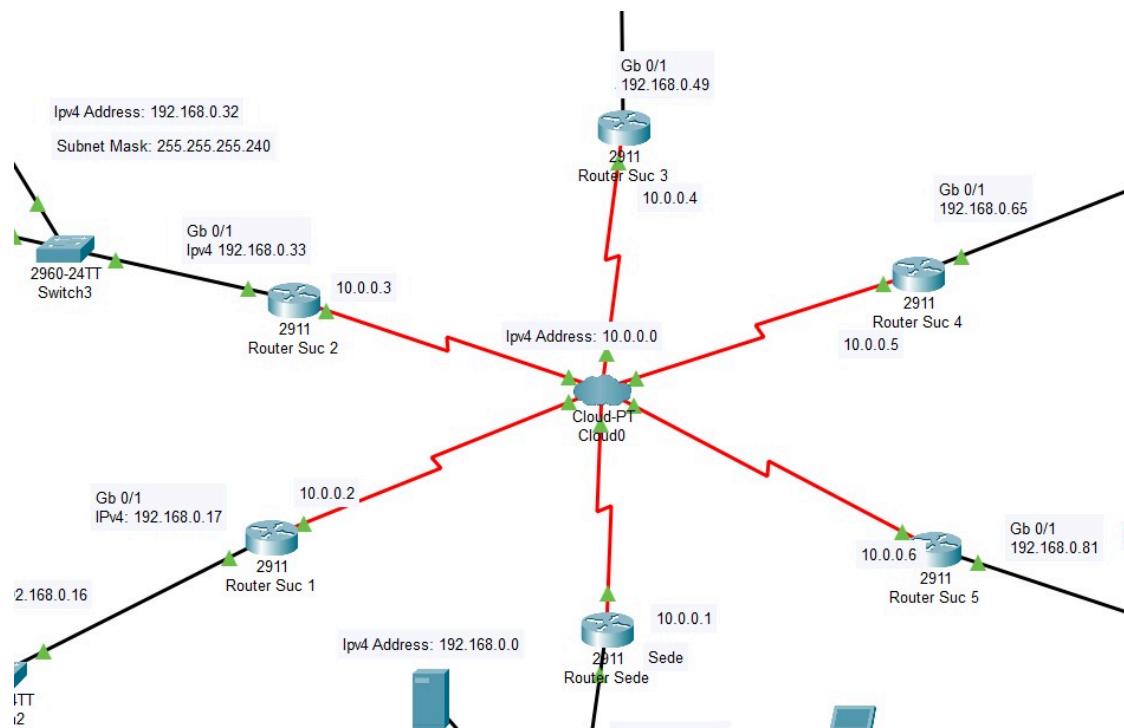
Configuración:

- Se establecen **rangos de direcciones IP** para cada subred.
- Se **excluyen direcciones** para equipos críticos como routers y servidores
 - Como en el caso del Servidor FTP, Como la Ip del Servidor debe ser estática su ip se excluye del rango de IP's del Servidor FTP



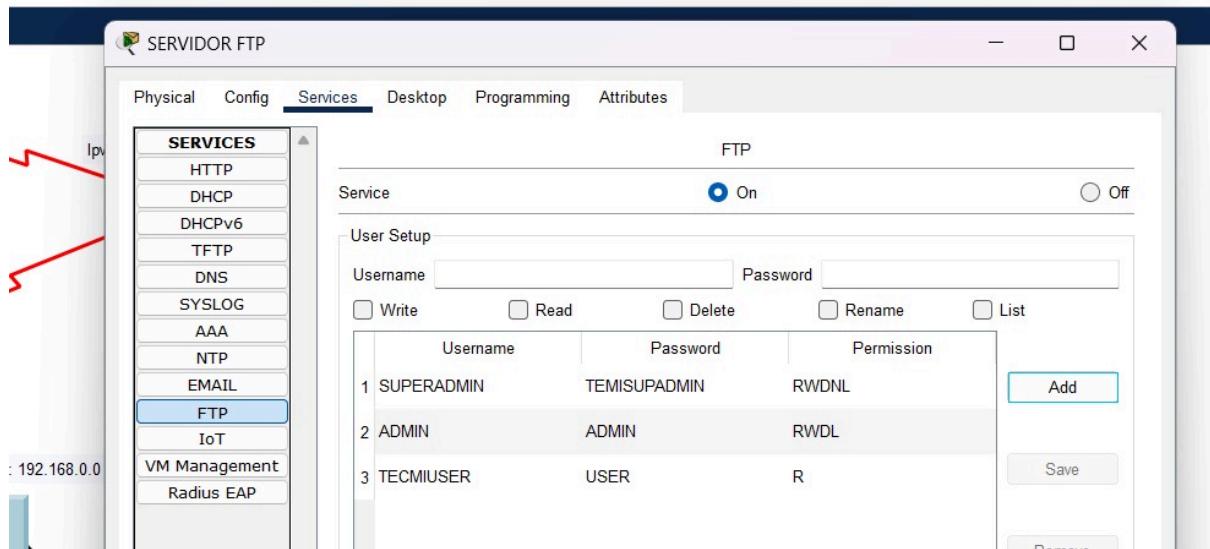
9.-Implementación Frame Relay de Nube

Se utilizó una implementación de Frame Relay en la nube para simular el ISP que permitirá la comunicación entre sedes. A través de DLCI's, la nube actúa como un medio de interconexión, asignando rutas virtuales entre los routers de cada sede. Esto optimiza la transmisión de datos sin enlaces físicos directos, replicando el funcionamiento de un ISP real y validando la conectividad de la red.



10.- Autenticacion Usuarios FTP

Empleamos el uso de FTP para mejorar la seguridad en la transferencia de archivos en la red, con el FTP damos de alta usuarios que podrán mandar y recibir archivos, así evitamos que externos a la red puedan acceder fácilmente a esta y extraigan algún archivo de suma importancia



11.-Autenticación SSH en routers

Se aseguró la configuración CLI de los routers para que solo el personal autorizado pueda modificarla, evitando accesos no autorizados. Dado que cualquier error podría afectar la comunicación entre sucursales, se implementaron contraseñas, privilegios administrativos y protocolos seguros para proteger la red.

```
11 Suc
SEDE>enable
SEDE#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SEDE(config)#ip domain-name TecmiCorp.net
SEDE(config)#crypto key generate rsa
The name for the keys will be: SEDE.TecmiCorp.net
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

SEDE(config)#line vty 0 5
*Mar 1 2:53:5.632: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 2:53:5.633: %SSH-5-ENABLED: SSH 1.5 has been enabled
SEDE(config-line)#transport input ssh
SEDE(config-line)#login local
SEDE(config-line)#exit
SEDE(config)#username admin privilege 15 password admin
SEDE(config)#enable secret admin
SEDE(config)#exit
SEDE#
%SYS-5-CONFIG_I: Configured from console by console

SEDE#
```

12.-Identificación de Amenazas Comunes

- Acceso no autorizado (Amenaza externa e interna)
- Individuos malintencionados o empleados con fines fraudulentos pueden intentar ingresar a la red sin los permisos necesarios.
- Malware y virus (Amenaza externa)
- Archivos maliciosos pueden infiltrarse en la red a través de correos electrónicos o dispositivos USB comprometidos.
- Ataques de denegación de servicio (DDoS) (Amenaza externa)
- Un atacante puede saturar la red con un volumen excesivo de tráfico, dejándola fuera de servicio.
- Phishing (Amenaza externa e interna)
- Los empleados pueden ser manipulados para entregar sus credenciales o información confidencial mediante correos electrónicos fraudulentos.
- Configuración incorrecta de dispositivos (Amenaza interna)
- Errores en la configuración de routers, switches o firewalls pueden crear brechas de seguridad que pueden ser explotadas.
- Suplantación de direcciones MAC (MAC Spoofing)
- Un atacante dentro de la red puede falsificar la dirección MAC de un dispositivo autorizado para obtener acceso a recursos restringidos.
- Ataque Man-in-the-Middle (MitM)

- Un atacante puede interceptar las comunicaciones entre la sede principal y las sucursales para robar información sensible.
- Ataques a la red Wi-Fi
- Un atacante puede intentar descifrar la contraseña WPA2 de la red inalámbrica para conectarse sin autorización.
- Medidas de Seguridad para Proteger la Red
- Implementación de VLANs y control de acceso

Segmentar los dispositivos en VLANs según su rol (empleados, invitados, servidores) para limitar el movimiento lateral de posibles atacantes.

Beneficio: Minimiza el impacto de un ataque y mejora la segmentación de la red.

Autenticación segura y control de acceso

Utilizar autenticación RADIUS o 802.1X para asegurar que solo dispositivos autorizados puedan acceder a la red.

Beneficio: Previene el acceso no autorizado incluso si se conocen las credenciales de Wi-Fi.

Configuración de un firewall y listas de acceso (ACLs)

LIMITAR EL TRÁFICO ENTRANTE Y SALIENTE EN LOS ROUTERS MEDIANTE LISTAS DE CONTROL DE ACCESO (ACLs).

Beneficio: Filtra el tráfico no autorizado y protege la red frente a ataques externos.

Monitoreo y detección de intrusos (IDS/IPS)

IMPLEMENTAR SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA IDENTIFICAR ACTIVIDADES SOSPECHOSAS EN LA RED.

Beneficio: Permite tomar medidas rápidas ante amenazas potenciales.

Capacitación y concienciación de seguridad para empleados

REALIZAR ENTRENAMIENTOS SOBRE SEGURIDAD INFORMÁTICA PARA REDUCIR EL RIESGO DE ATAQUES DE PHISHING Y ERRORES HUMANOS.

Beneficio: Aumenta la conciencia sobre amenazas y fortalece la seguridad general.

Propuesta para una Red Confiable

Para asegurar una red confiable en "TecmiCorp", se recomienda:

Redundancia en enlaces WAN

Establecer un enlace secundario de respaldo para mantener la conectividad entre la sede principal y las sucursales.

Beneficio: Previene caídas de la red en caso de fallos del enlace principal.

Implementación de Protocolos de Alta Disponibilidad (HSRP/VRRP)

Configurar routers en modo redundante con HSRP o VRRP para garantizar la disponibilidad continua de la red.

Beneficio: Asegura la continuidad del servicio incluso si un router falla.

Mantenimiento y actualización de equipos

Implementar un plan de mantenimiento regular para actualizar el firmware y aplicar parches de seguridad en routers y switches.

Beneficio: Protege la red contra vulnerabilidades explotables.

Respaldo y recuperación ante desastres

Establecer copias de seguridad de configuraciones y datos clave para restaurar la red en caso de fallos o ataques.

Beneficio: Minimiza el tiempo de inactividad y la pérdida de datos.

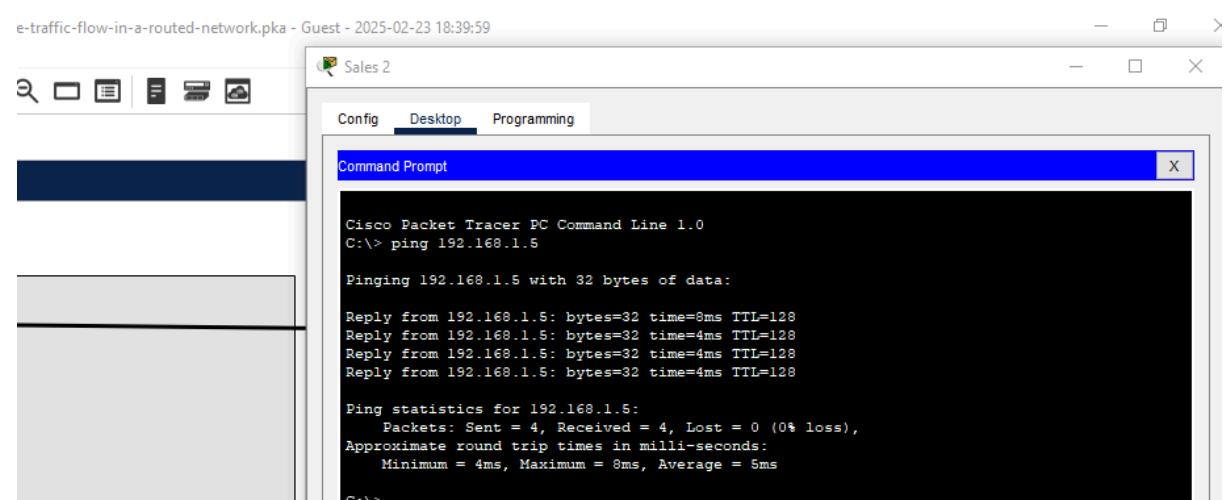
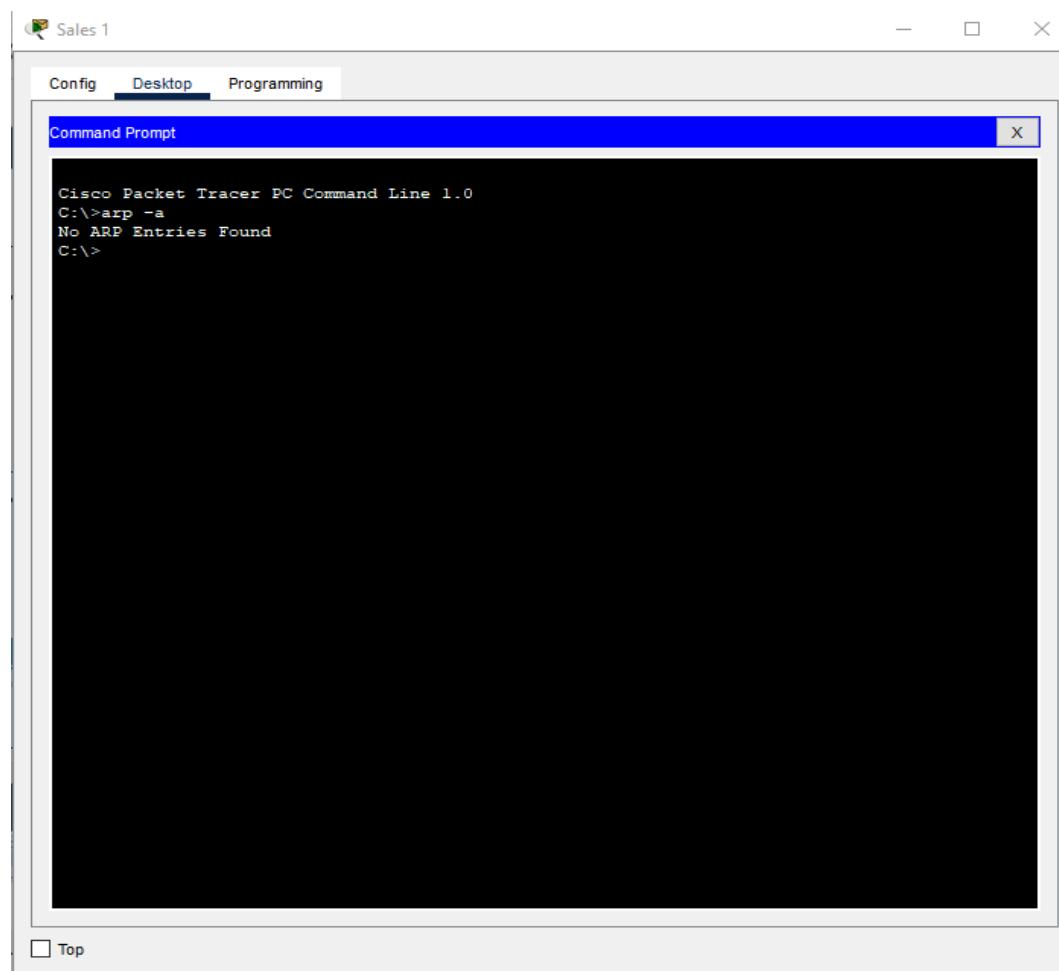
Gestión centralizada de la red

Utilizar herramientas de monitoreo y gestión para supervisar el estado de la red en tiempo real.

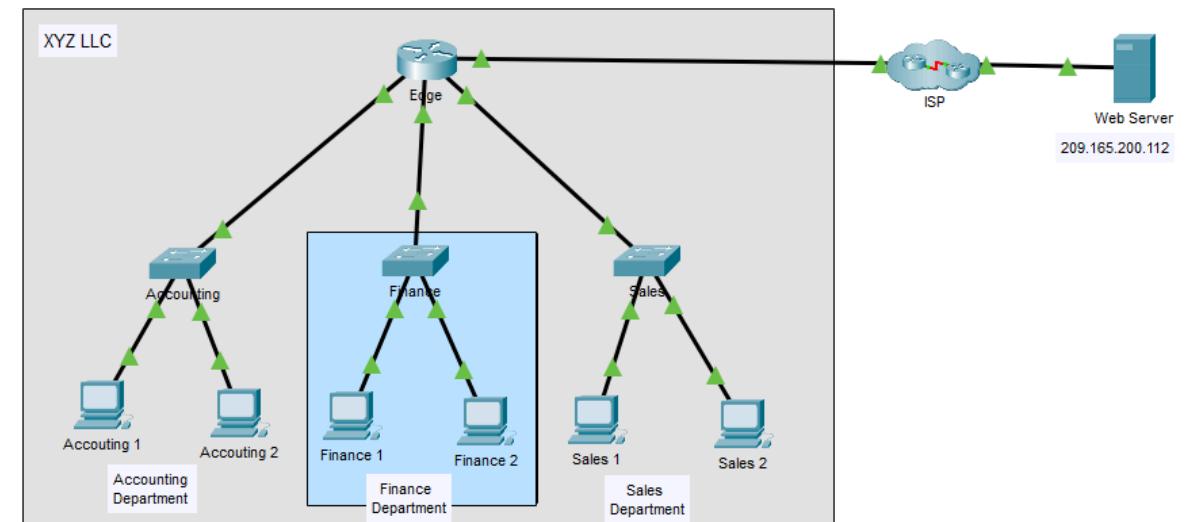
Beneficio: Permite una respuesta rápida ante problemas de rendimiento o seguridad

Laboratorio de Cisco Packet Tracer

Parte 1: Observar el flujo de tráfico en una LAN no enrutada



Parte 2: Reconfigurar la red para enrutar entre las LAN.



Finance 1

Config Desktop Programming

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:97FF:FE2C:9DA6
IPv6 Address.....: :::
IPv4 Address.....: 192.168.1.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
                           192.168.1.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
                           0.0.0.0

C:\>ipconfig /renew

IP Address.....: 192.168.2.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1
DNS Server.....: 0.0.0.0

C:\>
C:\>
```

Finance 2

Config Desktop Programming

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /renew

IP Address.....: 192.168.2.3
Subnet Mask....: 255.255.255.0
Default Gateway.: 192.168.2.1
DNS Server.....: 0.0.0.0

C:\>
```

Top

Sales 1

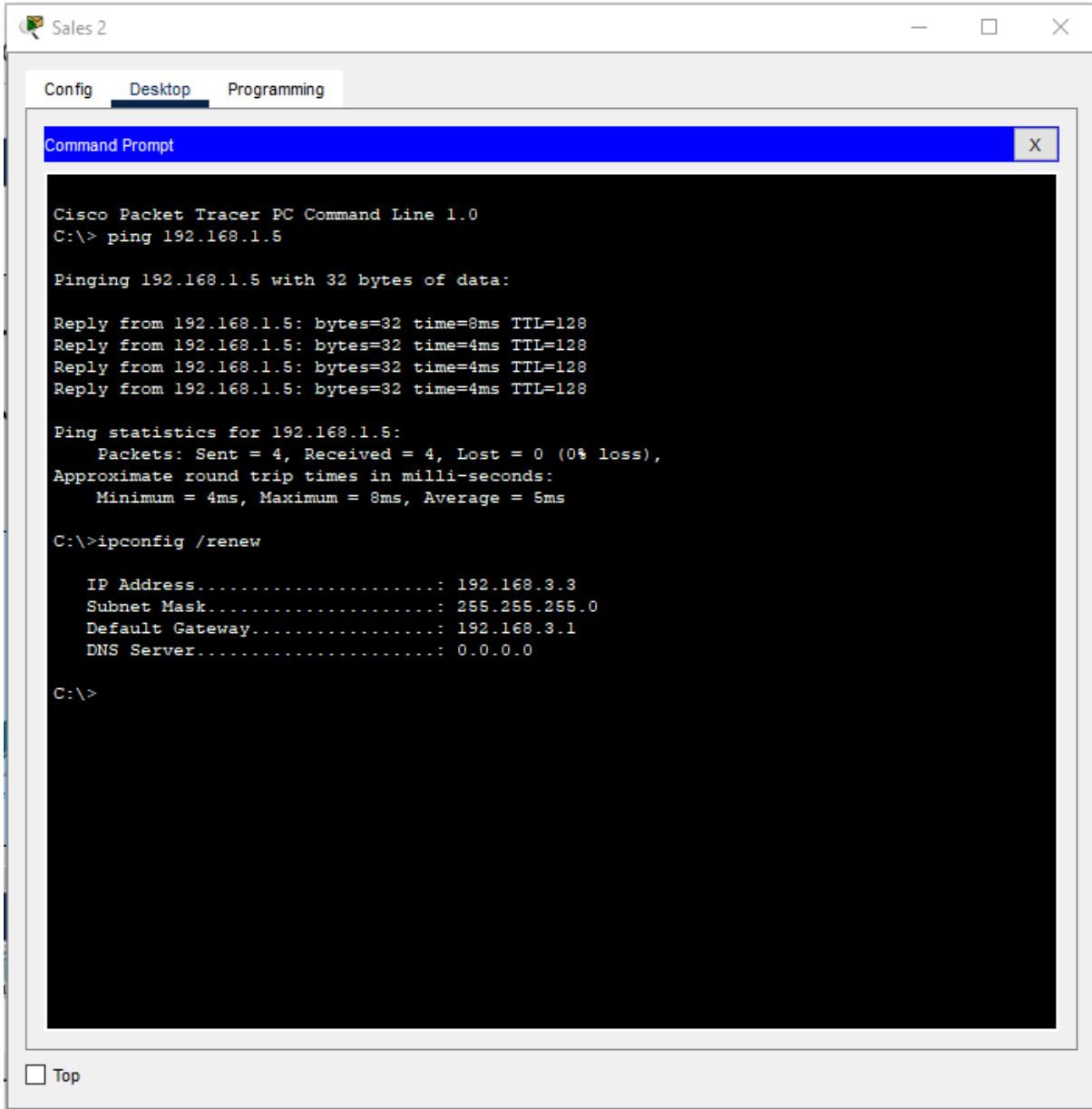
Config Desktop Programming

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>ipconfig /renew

IP Address.....: 192.168.3.2
Subnet Mask....: 255.255.255.0
Default Gateway.: 192.168.3.1
DNS Server.....: 0.0.0.0

C:\>
```



Sales 2

Config Desktop Programming

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=8ms TTL=128
Reply from 192.168.1.5: bytes=32 time=4ms TTL=128
Reply from 192.168.1.5: bytes=32 time=4ms TTL=128
Reply from 192.168.1.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 6ms

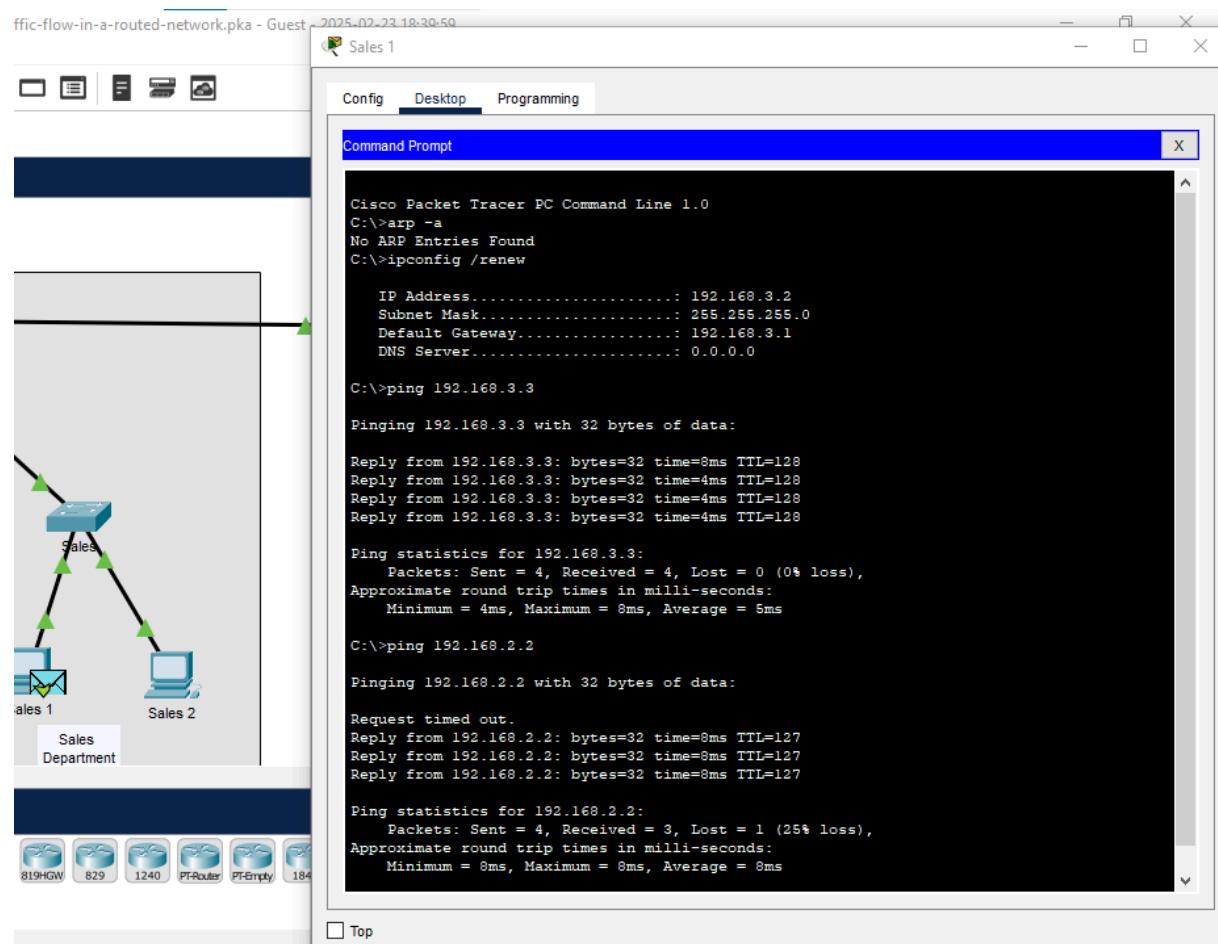
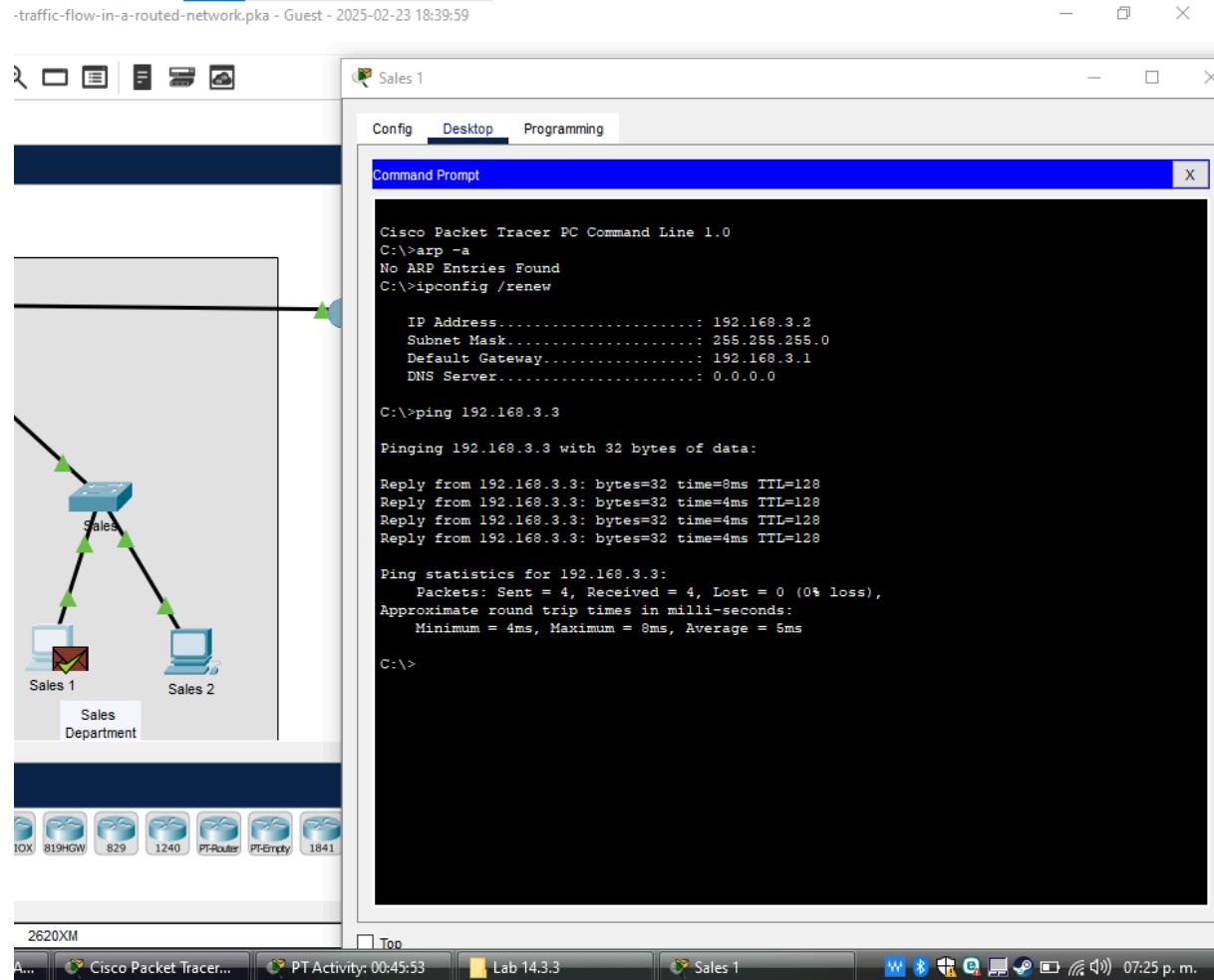
C:\>ipconfig /renew

    IP Address...: 192.168.3.3
    Subnet Mask...: 255.255.255.0
    Default Gateway...: 192.168.3.1
    DNS Server...: 0.0.0.0

C:\>
```

Top

Parte 3: Observar el flujo de tráfico en la red enrutada.



Glosario

- **ACLs (Access Control Lists):** Listas de control de acceso utilizadas en routers y firewalls para definir qué tráfico de red está permitido o denegado.
- **Autenticación RADIUS:** Protocolo de autenticación remota que proporciona acceso seguro a la red mediante servidores de autenticación centralizados.
- **Cisco Packet Tracer:** Software de simulación de redes utilizado para diseñar y probar configuraciones de dispositivos de red.
- **DHCP (Dynamic Host Configuration Protocol):** Protocolo que asigna automáticamente direcciones IP a los dispositivos de una red.
- **Dirección IP:** Identificador numérico único asignado a cada dispositivo conectado a una red.
- **DDoS (Denial of Service Distribuido):** Ataque que inunda una red con tráfico excesivo para interrumpir su funcionamiento.
- **Firewall:** Dispositivo o software que filtra y controla el tráfico de red para mejorar la seguridad.
- **FTP (File Transfer Protocol):** Protocolo estándar para la transferencia de archivos entre dispositivos en una red.
- **HSRP (Hot Standby Router Protocol):** Protocolo de redundancia de routers que permite que un router secundario tome el control en caso de falla del principal.
- **IDS/IPS (Intrusion Detection System / Intrusion Prevention System):** Sistemas de detección y prevención de intrusos que monitorean y bloquean amenazas en la red.
- **MAC Spoofing:** Técnica de ataque en la que un atacante falsifica la dirección MAC de un dispositivo autorizado para obtener acceso no autorizado.
- **Man-in-the-Middle (MitM):** Ataque donde un tercero intercepta y altera la comunicación entre dos dispositivos sin que los usuarios lo sepan.
- **Máscara de subred:** Número que define qué parte de una dirección IP corresponde a la red y cuál a los dispositivos dentro de ella.
- **Ping:** Comando utilizado para comprobar la conectividad entre dos dispositivos en una red.
- **Red VLAN (Virtual Local Area Network):** Técnica que segmenta una red en diferentes subredes lógicas para mejorar la seguridad y el rendimiento.
- **Rutas estáticas:** Configuración manual en routers para definir el camino que debe seguir el tráfico de red hacia una dirección específica.
- **Segmentación de red:** División de una red en partes más pequeñas (subredes) para mejorar la seguridad y gestión del tráfico.
- **Servidor FTP:** Servidor que permite la transferencia de archivos mediante el protocolo FTP.

- **Subnetting (Subredes):** Proceso de dividir una red en segmentos más pequeños para mejorar la organización y eficiencia del tráfico.
- **Switch:** Dispositivo de red que conecta múltiples dispositivos y gestiona la comunicación entre ellos dentro de una red local.
- **Topología de red:** Estructura física o lógica que define cómo los dispositivos de una red están interconectados.
- **VRRP (Virtual Router Redundancy Protocol):** Protocolo que proporciona alta disponibilidad de routers en una red.
- **WAN (Wide Area Network):** Red que conecta múltiples ubicaciones geográficas, como sucursales de una empresa.
- **Wi-Fi WPA2:** Protocolo de seguridad inalámbrica que cifra la conexión para evitar accesos no autorizados.

Bibliografia:

Rashid, N. B. A., Othman, M. Z. B., Johan, R. B., & Sidek, S. F. B. H. (2019). Cisco Packet Tracer Simulation as Effective Pedagogy in Computer Networking Course. *International Journal Of Interactive Mobile Technologies (iJIM)*, 13(10), 4. <https://doi.org/10.3991/ijim.v13i10.11283>

Netalit. (2024, 3 enero). *Network security threats*. Check Point Software. https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/network-security-threats/?utm_source

Ginsburg, D. (2024, 10 diciembre). Mejores prácticas de seguridad en la red: Cómo proteger su empresa de las ciberamenazas. *Aryaka Unified SASE Solution For Secure*.

https://www.aryaka.com/es/blog/network-security-best-practices/?utm_source

Trend Micro - Spain (ES). (s. f.). *¿Cuáles son las medidas de la seguridad de red?* Trend Micro.

https://www.trendmicro.com/es_es/what-is/network-security/network-security-measures.html?utm_source

Tokio School. (s.f.). Tipos de amenazas informáticas.

Tokio School.

<https://www.tokioschool.com/noticias/tipos-amenazas-informaticas/>

Autores



- Alejandro Juárez Aragón



- José Alonso Corona Contreras



- **Leonardo Yahir Martínez Estrada**



- **Artur Emmanuel Martínez Martínez**



- **Juan Pablo Peñuelas Valenzuela**

Conclusiones

Durante el desarrollo del proyecto se presentaron varios desafíos que pusieron a prueba nuestro proceso de toma de decisiones. Por ejemplo, la elección del tipo de topología implicó evaluar cuidadosamente las ventajas y limitaciones de cada opción, ya que la estructura seleccionada determinaría el rendimiento y la escalabilidad de la red. Este análisis, junto con el diseño general, generó debates y diferencias de criterio que, aunque en ocasiones resultaron en inconformidades, enriquecieron el enfoque del proyecto al obligarnos a considerar múltiples perspectivas.

Además, se enfrentaron dificultades técnicas con algunos dispositivos y durante las simulaciones, lo que nos impulsó a buscar soluciones alternativas y ajustar nuestros métodos de trabajo. A pesar de estos retos, la perseverancia del equipo permitió culminar el proyecto sin incidencias mayores, obteniendo resultados satisfactorios y valiosas lecciones en gestión de conflictos y resolución de problemas.