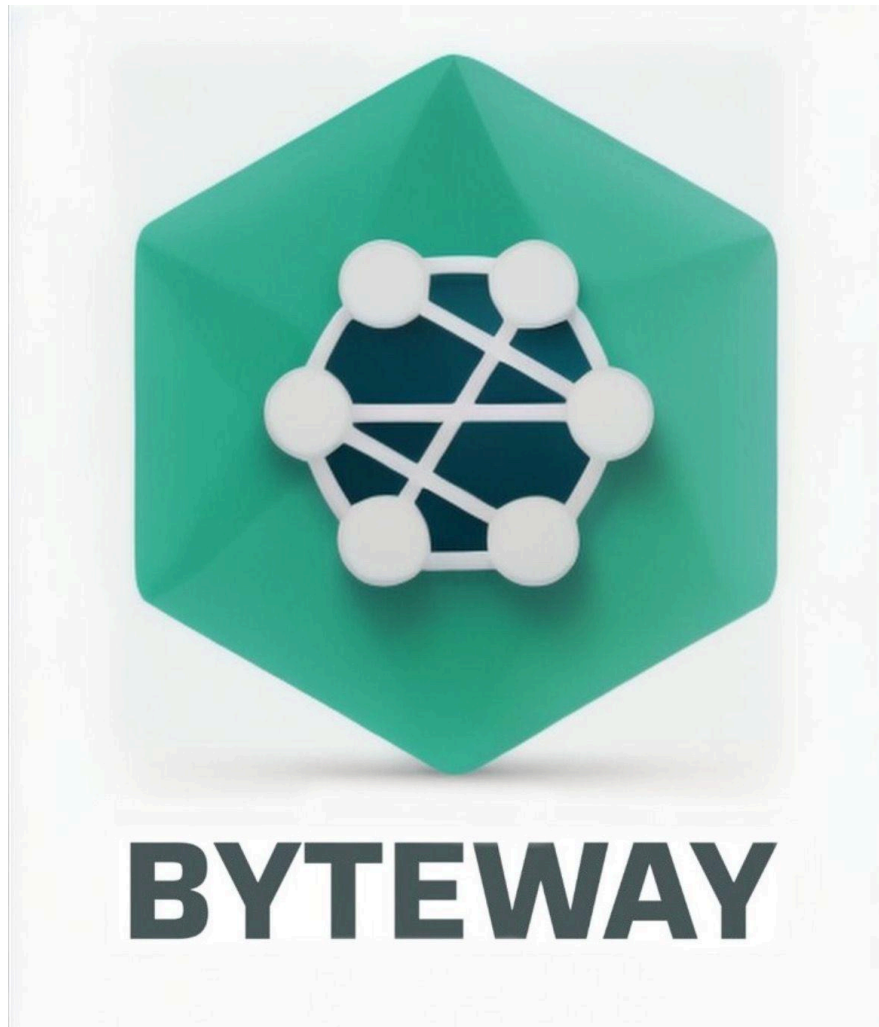


PROYECTO FINAL - GESTIÓN DE REDES



PROPUESTA DE INFRAESTRUCTURA DE RED PARA TECMICORP

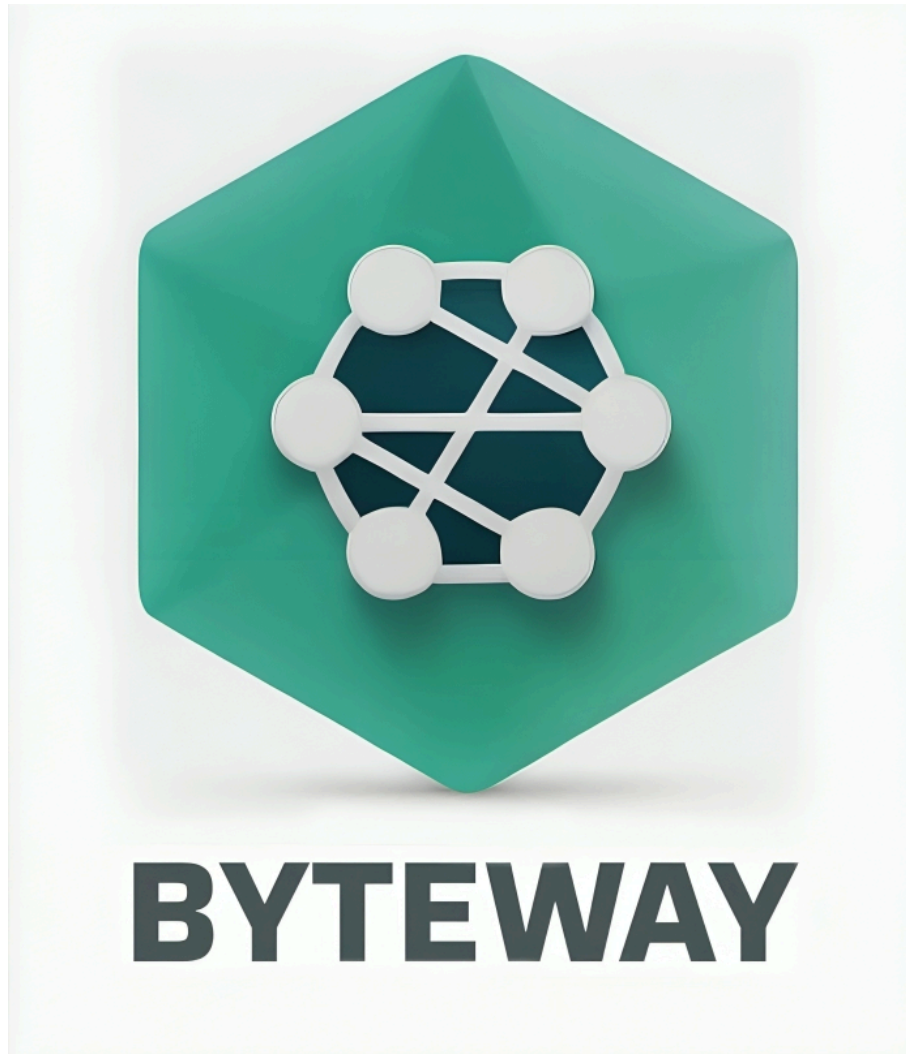
Profesora: Blanca Aracely Aranda Machorro
Monterrey, N.L.
14 de Enero del 2025

ÍNDICE

DEFINICIÓN DEL PROYECTO.....	2
SOBRE NUESTRO CLIENTE.....	3
DESCRIPCIÓN.....	3
ALCANCE.....	4
ANÁLISIS Y DISEÑO.....	5
DESARROLLO DEL PROYECTO.....	9
DESARROLLO E IMPLEMENTACIÓN.....	10
1- Estructura de redes locales (LANs).....	10
2- Estructura de red pública simulada (WAN).....	17
3- Enrutamiento.....	19
PRUEBAS, RESULTADOS E IDENTIFICACIÓN DE AMENAZAS.....	22
PRUEBAS Y RESULTADOS.....	23
EJEMPLO DE FLUJO DE OPERACIONES CON LA RED:.....	24
IDENTIFICACIÓN DE AMENAZAS.....	24
IDENTIFICACIÓN DE POSIBLES ATAQUES.....	25
PROPUESTAS DE MEDIDAS DE SEGURIDAD.....	25
PROPUESTA PARA UNA RED CONFIABLE.....	26
RESÚMEN DE COMPLEJIDADES AÑADIDAS, CONCLUSIONES Y REFERENCIAS.....	27
COMPLEJIDADES EXTRA AÑADIDAS:.....	28
GLOSARIO DE TERMINOLOGÍA.....	28
BIBLIOGRAFÍAS.....	30
AUTORES.....	30
CONCLUSIONES Y AGRADECIMIENTOS.....	31
VIDEO DEMOSTRATIVO DE LA PROPUESTA.....	31

En caso de términos no familiares, refiérase a la sección GLOSARIO DE TERMINOLOGÍA.

(La empresa cliente en este proyecto es ficticia).



I

DEFINICIÓN DEL PROYECTO

Con el propósito de realizar una propuesta viable de estructura de red para la empresa
TECMICORP.

SOBRE NUESTRO CLIENTE

TecmiCorp es una **agencia de marketing digital y estrategia online** especializada en ofrecer estrategias de marketing viables y benefactoras para empresas, negocios u otros emprendimientos que desean mejorar su presencia e imagen en línea, aumentar su alcance y atraer clientes. Los siguientes son los servicios que ofrece TecmiCorp, que servirán como contexto para la infraestructura de red propuesta y las elecciones de servicios que se incluirán:

- **Gestión de redes sociales:** Creación de contenido, programación de publicaciones, monitoreo de interacción y campañas pagadas en plataformas como Facebook, Instagram, LinkedIn y Twitter.
- **Publicidad digital:** Desarrollo y optimización de campañas en Google Ads, Meta Ads y otras plataformas.
- **Diseño web y branding:** Creación de sitios web optimizados para identidad visual y diseño gráfico.
- **Análisis de datos y métricas:** Uso de herramientas como Google Analytics para evaluar el impacto de las campañas y ajustar estrategias.

Se dividen las responsabilidades que conllevan estos servicios a través de sus diferentes ubicaciones, con cada sucursal ofreciéndolos a clientes de la zona, pero la conectividad mutua entre ubicaciones es imperativa debido a la utilización de recursos compartidos, como el flujo de archivos multimedia entre sucursales o plataformas internas para coordinación de operaciones y colaboración.

La empresa cuenta con alrededor de 100 empleados y está en crecimiento constante, por lo que optó por contratar los servicios de Byteway de consultoría de redes para mejorar su comunicación y establecer una arquitectura de red confiable y escalable, ya que prevé seguir creciendo rápidamente. A continuación se define el caso más a detalle.

DESCRIPCIÓN

El equipo de **BYTEWAY** ha sido contratado por la empresa **TECMICORP** para diseñar su infraestructura de red con el objetivo de responder a las crecientes necesidades de conectividad que demandan sus operaciones. La empresa cuenta con una cantidad considerable de ubicaciones, conformada por una sede central y cinco sucursales. El equipo ha sido proporcionado con las especificaciones y cantidades de dispositivos con los que cada ubicación cuenta, y su trabajo es diseñar infraestructuras de red (tanto locales como una a larga distancia para su interconexión) usando la herramienta **Cisco Packet Tracer** considerando las necesidades y los objetivos, que serán definidos a continuación. Esto con el propósito de llevar a cabo la fase de diseño antes de su confirmación y posterior implementación física. En este documento se definen todas las características del diseño de

red que el equipo recomienda para la empresa, por qué, y cómo sería implementada la estructura de red en el ámbito físico.

ALCANCE

Con respecto al alcance del proyecto, se consideran los siguientes puntos:

- Objetivos

(Estos objetivos también serán definidos como los criterios de éxito)

1. **Escalabilidad:** Es de imperativa importancia que la infraestructura de red sea escalable, es decir, que tenga flexibilidad y mantenga su correcto funcionamiento ante la agregación de nuevos dispositivos (como sucedería en la inauguración de una nueva sucursal o la expansión de una existente). Esto con el propósito de eliminar la necesidad de cambiar configuraciones de red o instalar componentes físicos a cada equipo nuevo manualmente, requiriendo conocimientos específicos y en algunos casos causando un cese temporal de las operaciones, sin mencionar la posibilidad de que la red se vuelva obsoleta y deje de funcionar en su totalidad tras cruzar cierto límite de expansión. Para lograr este objetivo, es necesario hacer uso de tantos protocolos de red dinámicos y conexiones inalámbricas como sea posible, así como implementar la tolerancia a fallas en el margen posible y educar a los empleados de TecmiCorp en la configuración más básica de red de nuevos dispositivos.
2. **Seguridad:** Siendo una cualidad de máxima importancia debido al riesgo de pérdida y/o robo de datos, ya sea por ciberataques o fugas de información, se prestará especial atención a la seguridad. Se considerará como el mayor enfoque a la hora de definir el modo de comunicación entre las redes (la topología de la red de área amplia).
3. **Rendimiento:** Probablemente el más importante de los objetivos, ya que la expectativa principal del resultado del proyecto es conectividad eficaz y de alto rendimiento. Este objetivo se alcanza a través de la configuración correcta de las conexiones y el uso de las tecnologías adecuadas. La elección de estos componentes se explicará a detalle en este documento.

- Entregables

1. **Archivo .pkt (Cisco Packet Tracer):** Demostrando la infraestructura de las redes de cada sucursal (y la representación de la red pública) de manera clara, apegada a los objetivos definidos y con pruebas de conectividad realizadas.
2. **Archivo Microsoft Word/PDF:** Documentación del proyecto.

- Limitaciones

1. **Limitaciones del software Cisco Packet Tracer:** Estas limitaciones serán explicadas conforme afecten la elaboración del proyecto. Se hará uso de otras opciones disponibles para representar las tecnologías adecuadas, justificando

la elección y explicando el equivalente correcto en una red real en la documentación.

- **Consideraciones**

1. Esta propuesta no está basada en ningún presupuesto o cantidad de recursos y/o tiempo específicos, pero se consideró el costo y las necesidades de recursos para ofrecer una infraestructura tanto accesible como confiable.

ANÁLISIS Y DISEÑO

Se llevará a cabo un análisis del problema para idear una solución que cumpla con los objetivos y estándares de calidad.

- **Contexto**

- El equipo corporativo de TecmiCorp se ha enfrentado a limitaciones de conectividad a medida que la empresa va expandiendo sus operaciones, por lo que se ha contratado a un equipo de consultores de redes de la empresa Byteway para diseñar una infraestructura de red que abarque la sede principal más cinco sucursales en diferentes ubicaciones, permitiendo la comunicación entre ellas.

- **Evaluación de Arquitecturas de Red y Justificaciones de Diseño**

- A continuación se analizan dos opciones de arquitecturas para la conexión entre las redes de las sucursales (**comunicación externa**):
 - **Arquitectura jerárquica:** Las redes se conectan a un proveedor de servicios de Internet (ISP) que actúa como nodo central para comunicarse a través de Internet.
 - **Arquitectura directa:** Las redes se conectan entre sí directamente sin necesidad de un nodo central.

Ambas arquitecturas implican sus propias ventajas y desventajas en cuanto a nuestros criterios de éxito, y ambas cumplen el propósito de generar una red de redes (WAN). A continuación se muestra un cuadro comparativo de cada tipo de conexión en base a los criterios de éxito del proyecto:

Criterio	Arquitectura jerárquica	Arquitectura directa
Rendimiento	Más estable y optimizado. Sin embargo, puede generar latencias adicionales por el enrutamiento a través del nodo central si este no está bien equipado para manejar el tráfico eficientemente.	Puede reducir la latencia debido a que los datos viajan directamente entre las redes, pero también se pueden generar cuellos de botella.

Escalabilidad	Más fácil de escalar, ya que cada nueva sucursal solo necesita conectarse al ISP central sin afectar a las demás. Sin embargo, puede volverse costoso con el tiempo.	Se vuelve más compleja a medida que crecen las conexiones, ya que cada nueva sucursal requiere más enlaces directos para mantener la comunicación eficiente.
Seguridad	Generalmente más segura, ya que el tráfico pasa por el ISP, que puede ofrecer medidas de protección ya establecidas como firewalls y monitoreo centralizado. Sin embargo, si el ISP es comprometido, toda la red está en riesgo.	Puede ser menos segura si no se implementan protocolos adecuados, ya que cada enlace entre sucursales es un punto potencial de vulnerabilidad. Sin embargo, no depende de un solo punto (ISP), lo cual habilita cierta tolerancia a fallas.

En la versión final de este proyecto, se optó por diseñar la red con **arquitectura jerárquica** debido a su relativa simplicidad y ventajas en escalabilidad y rendimiento en redes relativamente pequeñas, elementos claves en la elaboración del proyecto. Las posibles desventajas dependerán en gran medida del proveedor de servicios de Internet elegido, pero se toma en consideración que los grandes proveedores ya cumplen con normas de seguridad importantes y estándares de Internet. Los detalles acerca del funcionamiento de la topología que conlleva este modelo jerárquico se especificarán en la sección de desarrollo del proyecto.

- También se deben tener en cuenta los protocolos dinámicos que se utilizarán tanto para la asignación de direcciones IP y enrutamiento de datos.
 - **Asignación de direcciones IP:** DHCP (dinámica)
 - **Enrutamiento:** OSPF (se implementa RIP en la simulación por razones especificadas en su sección correspondiente)

La implementación de estos protocolos se explicará a medida que sean necesarios en el desarrollo del proyecto.

- Dispositivos para Redes Locales

- En cuanto a la arquitectura de cada una de las redes (**comunicación interna**), también se seguirá un modelo jerárquico **acceso - distribución - núcleo**, ya que los dispositivos que la empresa nos ha informado serán usados en cada ubicación se prestan para esta arquitectura con facilidad de implementación y las ventajas ya mencionadas. A continuación se definen los dispositivos que se están considerando en el diseño de la red y la justificación de ciertas elecciones de conectividad:

- **Routers (núcleo):** Para enrutar el tráfico de datos (usando el protocolo RIP) hacia otros dispositivos en la red y hacia redes externas y asignar direcciones IP a los dispositivos. Actúan como nodo central en cada red.
- **Switch (distribución):** Intermediarios entre los routers y los dispositivos de salida. Permiten que dichos dispositivos se conecten en conjunto a una interfaz del router.
- **Dispositivos de salida conectados físicamente (acceso):** PCs (cinco en sede principal y una en cada sucursal) y laptops para uso empresarial.

¿Por qué conexiones físicas?

Aunque es completamente posible y viable hacer uso de conexiones inalámbricas (por Wi-Fi) para los dispositivos de uso empresarial móviles (laptops), se recomienda hacer uso de conexiones físicas ya que implica ventajas significativas en seguridad y rendimiento, las cuales se han decidido priorizar sobre la comodidad del acceso inalámbrico. Al establecer una conexión física directa, el tráfico de datos viaja a través de cables y no ondas de radio, las cuales son más fáciles de interceptar y de proveer acceso remoto a la red a terceros (en cuanto a seguridad) y son más propensas a interferencias, las cuales afectan la velocidad y la conectividad (en cuanto a rendimiento). Sin embargo, la conectividad inalámbrica es más escalable y cómoda para los individuos, por lo que se incluirán también soluciones inalámbricas, detalladas en el siguiente punto.

- **Puntos de acceso inalámbricos:** A pesar de no ser incluido en el reporte de la empresa como una necesidad, se incluye en cada sucursal un punto de acceso inalámbrico a la red. Esto debido a la necesidad moderna de conectividad constante en el nivel personal, es decir, por medio de smartphones y otros dispositivos móviles. Para la representación visual de estos accesos, se incluirán en el modelo de Packet Tracer dos smartphones y una tableta móvil en cada ubicación, pero dichos puntos de acceso son escalables mucho más allá de solo tres dispositivos móviles de esta variedad limitada.
- Byteway incluye la siguiente consideración que aplica solo a la red de la sede principal:
 - **Servidores:** Como parte de los servicios de Byteway, se incluyen en la propuesta de diseño y estructura de red los servidores de los que la empresa puede hacer uso. Para propósitos de representación visual simple, se colocarán en Cisco Packet Tracer dos servidores diferentes, uno para FTP (File Transfer Protocol) para establecer un repositorio de archivos central compartido en todas las ubicaciones y otro para proveer servicios web (HTTP/S y DNS). Se ofrece también un dominio público para que la empresa cuente con su propio sitio web. Estos servicios son opcionales y negociables y solo estarán incluidos como

recomendaciones o adiciones a la propuesta como parte de nuestro servicio de customización de red para el cliente debido a las operaciones que TecmiCorp lleva a cabo.

- **Medidas Adicionales de Seguridad y Rendimiento**

- **Segmentación de redes:** Se implementa la segmentación de la red de cada sucursal en diferentes subredes para dividir el tráfico. Esto con el objetivo de evitar la saturación, los cuellos de botella, y añadir una capa de seguridad (si un atacante compromete un dispositivo en una subred, no puede moverse fácilmente a otras partes de la red sin atravesar medidas de seguridad adicionales, como firewalls o sistemas de detección de intrusos. Además, la propagación de ataques se ve limitada a la subred afectada en vez de extenderse a toda la red).
- **Implementación de IPv6:** IPv6 mejora la seguridad, escalabilidad y rendimiento en comparación con IPv4 (aunque en esta propuesta se opta por implementar ambos protocolos y llevar a cabo las operaciones por medio de IPv4). Incorpora IPSec de forma nativa, dificultando ataques como el spoofing y el escaneo de redes, además de eliminar la necesidad de NAT, reduciendo vulnerabilidades. En la red global, su enorme espacio de direcciones permite conectar miles de millones de dispositivos sin problemas, facilitando la expansión del IoT (Internet of Things) y eliminando la escasez de direcciones IP. También optimiza el enrutamiento y la latencia al simplificar la estructura de las direcciones y eliminar traducciones innecesarias, mejorando el rendimiento.
- **SSH:** Cada router tendrá SSH (Secure Shell) implementado. Esto nos permite acceder de manera segura a la línea de comandos del router de manera remota, desde un dispositivo en la red.
¿Por qué no Telnet? Telnet, a pesar de compartir la misma funcionalidad con SSH, se considera obsoleto e inseguro debido a la falta de autenticación y cifrado de datos, exponiendo los datos a terceros con intenciones dañinas y añadiendo vulnerabilidad a la red.
- **Contraseñas en cada router:** Además de la contraseña que se pedirá al acceder de manera remota, al acceder a la línea de comandos directamente desde el router también se pedirá una contraseña antes de poder hacer cualquier operación.



II

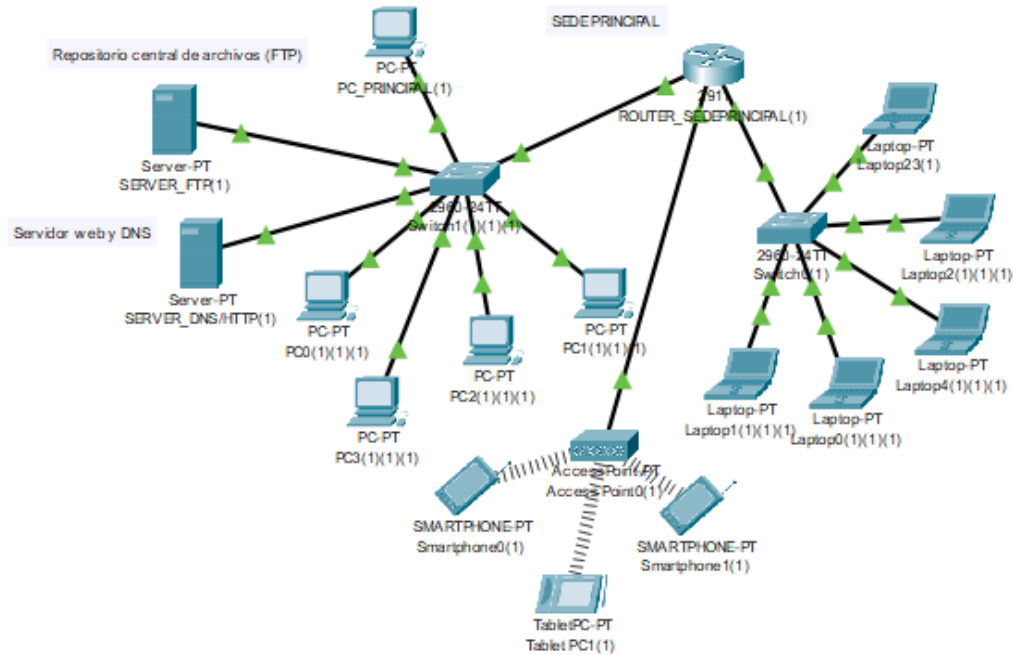
DESARROLLO DEL PROYECTO

Con el propósito de diseñar un modelo de red fiel a los estándares y especificaciones descritos en la primera parte en Cisco Packet Tracer.

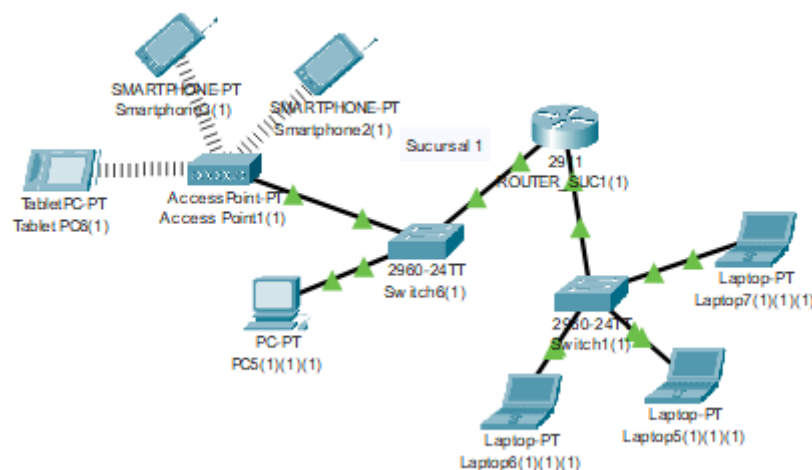
DESARROLLO E IMPLEMENTACIÓN

1- Estructura de redes locales (LANs)

Primero, se diseñó la estructura de la red privada de la sede principal, y se tomó como base para las demás redes:



Así se ve la misma arquitectura aplicada a las especificaciones de cada sucursal (5 en total), sirviendo como versiones a menor escala de la misma infraestructura de red:



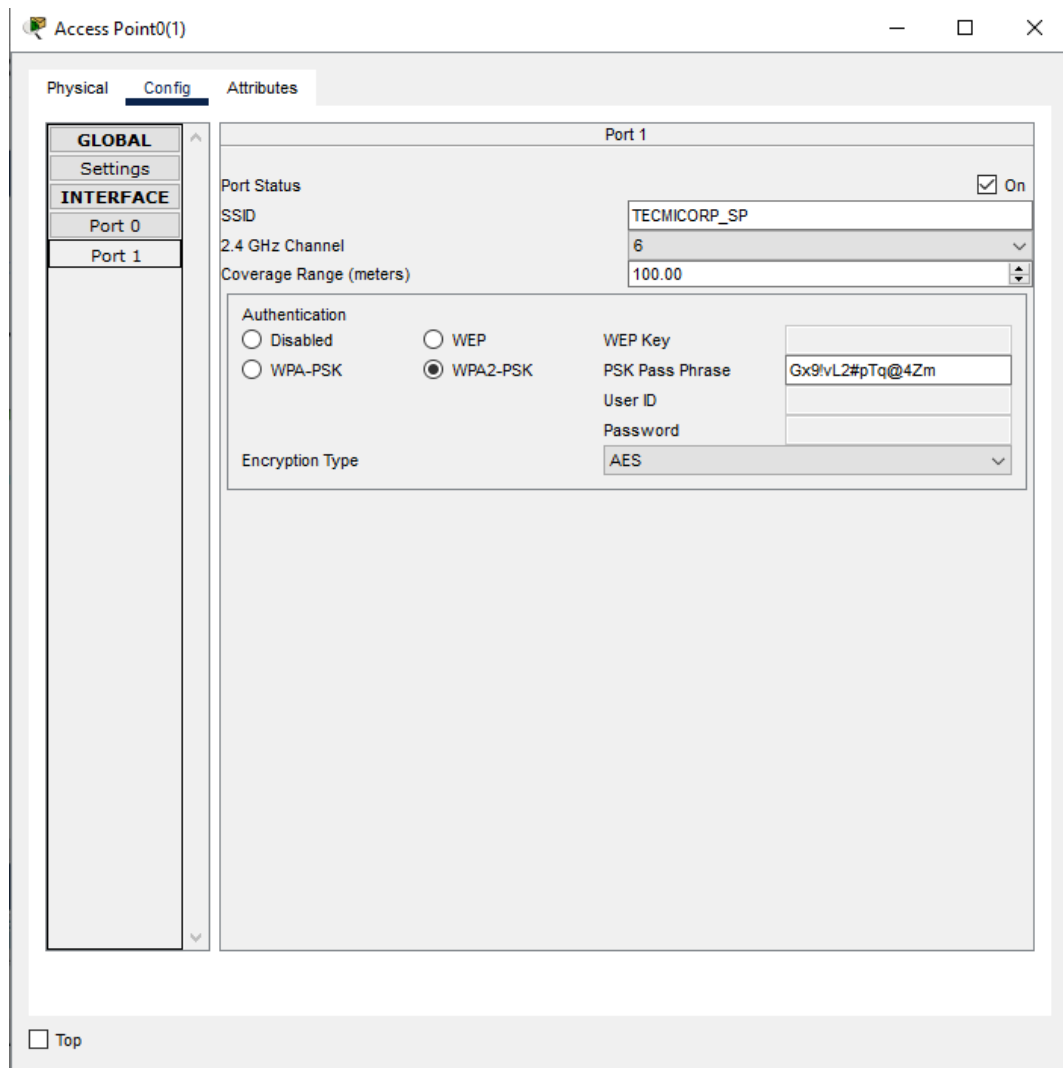
Explicación

- **Elección de router:** El router elegido (tanto para la sede principal como para las sucursales) es el **2911 estándar** (es decir, no cuenta con tecnología inalámbrica de

manera nativa). Se eligió dicho router debido a su cantidad de puertos Ethernet disponibles y a su balance amigable de complejidad y capacidad de enrutamiento. En otros términos, el router 2911 tiene simplicidad de configuración y uso sin sacrificar cantidad de capacidades. Por estas razones, el equipo considera que este router es el más adecuado para la actual tarea.

- **Elección de switch:** Se eligió el switch Cisco 2960-24TT debido a que está diseñado para redes empresariales pequeñas y medianas. Debido a su cantidad de puertos Ethernet (24) y medidas de seguridad, como autenticación y control de dispositivos que pueden acceder a la red, nos provee con ventajas en escalabilidad, rendimiento y seguridad, además a un costo razonable.
- **Conexiones físicas:** En la sede principal, las computadoras de escritorio y los servidores propuestos están conectados directamente al router por medio de cables de cobre trenzados (estándar Ethernet que reduce la interferencia) a través de un switch (el cual en el modelo jerárquico elegido distribuye la conexión del núcleo, en este caso una interfaz del router). La interfaz del router a la que está conectado el switch (GigabitEthernet0/0) representa una subred de la sede principal. La otra subred se genera de la misma manera, conectada a la interfaz GigabitEthernet0/1. Las laptops se conectan a esta subred mediante otro switch. En cuanto a las sucursales, se replica el modelo de segmentación con los dispositivos especificados y no se incluyen los servidores.
- **Conexiones inalámbricas:** Como el router 2911 no dispone de conectividad wireless nativa, se usó un punto de acceso conectado físicamente a una interfaz del router, GigabitEthernet0/2, generando la tercera subred de la sede principal. Esta tercera subred no existe en las demás sucursales, ya que el punto de acceso existe en la misma subred que la única computadora de escritorio de la ubicación. Se optó por segmentar en una nueva subred para esta conexión en la sede principal debido a que las demás subredes estaban ya un tanto saturadas, y debemos considerar que uno de los propósitos de la segmentación es prevenir exactamente esto, considerando que la subred inalámbrica tendrá un número variable y generalmente mayor de dispositivos conectados. Sin embargo, en las demás ubicaciones, la subred de la computadora de escritorio cuenta solamente con dicho dispositivo, además conectado directamente por cable, por lo que no implica ningún daño al rendimiento incluir la conexión inalámbrica ahí.

Los dispositivos identifican el punto de acceso mediante su SSID y se conectan a él mediante una contraseña establecida. El SSID y contraseña mostradas en la siguiente imagen son recomendaciones, el SSID por identificación fácil de la red y la contraseña por seguridad. Este nombramiento puede ser cambiado cuando se establezca la red real. La imagen muestra la configuración del punto de acceso de la sede principal, pero se siguen los mismos estándares para la configuración y nombramiento de los puntos de acceso en las demás sucursales.



- **DHCP IPv4:** Aquí se configura el primer protocolo para la escalabilidad que había sido mencionado. Se consideró el uso de un servidor para manejar el protocolo, pero para reducir la complejidad y costo por uso excesivo de dispositivos se optó por configurar el DHCP directamente desde el CLI (Command Line Interface) del router, ya que es un servicio incluido en el modelo 2911, haciendo uso de los siguientes comandos:

```
ip dhcp pool SP_1
network 192.168.0.0 255.255.255.0
default router 192.168.0.1
dns-server 192.168.0.50
ip dhcp excluded-address 192.168.0.1
```

Estos comandos inician un pool de DHCP, establecen la red en la que trabajará, el router de la red (en este caso, la IP de la interfaz de la subred), el servidor DNS, y especifican que la dirección del default router no sea incluida en la lista de direcciones a asignar. Al ejecutar los mismos comandos en las demás subredes y habilitar DHCP

en cada dispositivo, cada uno tendrá su IPv4 dinámicamente asignada, y serán capaces de comunicarse entre sí.

El diseño de la estructura es el mismo para todas las sucursales. Se considera que cada router tendrá siempre dos direcciones IPv4 privadas para las subredes a donde se conectarán las PCs y laptops respectivamente (o tres, en el caso único de la sede principal) y una IPv4 pública para su conexión a la red amplia (WAN), lo cual será explicado en la sección siguiente.

- **Implementación de IPv6:** Las direcciones IPv6 se implementan de manera automática en cada dispositivo corriendo los siguientes comandos en el CLI del router:

```
Router(config)#interface gi0/1
Router(config-if)#ipv6 address 2001:db8:12::1/64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ipv6 unicast-routing
Router(config)#exit
```

De este modo, se le puede asignar a cada dispositivo una IPv6 de manera automática. Esta asignación se considera automática, pero no necesariamente requiere DHCP ya que los dispositivos pueden autoasignarse direcciones IPv6. La dirección IPv6 puede ser estática o dinámica. Cuando un dispositivo obtiene una dirección IPv6 automáticamente, esta dirección IP es única para el dispositivo a nivel global, excepto en el caso de direcciones link-local, que solo son válidas dentro de la misma red local. A pesar de las claras ventajas de IPv6, para lo que resta del desarrollo del proyecto se seguirá trabajando con direcciones IPv4 debido a su simplicidad y utilidad para el cumplimiento del propósito del diseño en Packet Tracer como representación visual y teórica de la red.

- **SSH:** Secure Shell se configura a través de los siguientes comandos. Los usuarios y contraseñas establecidos en todas las capturas son ejemplos y no se adhieren a estándares de nomenclatura segura. (No se incluye el texto que aparece en el CLI que pide parámetros, solo el texto necesario por línea):

```
ip domain-name midominio.com
crypto key generate rsa
1024
ip ssh version 2
username admin privilege 15 secret
MiContraseñaSegura
line vty 0 4
transport input ssh
login local
exit
```

- **Contraseña del router:** Se emplean los siguientes comandos:

```
line console 0
password ContraseñaSegura123
login
exec-timeout 10 0 # (Opcional: cierra sesión tras
10 min de inactividad)
exit
```

- **Configuración de servidor FTP:** La configuración del servidor es la siguiente:

The screenshot shows the 'FTP' configuration page. At the top, the 'Service' is set to 'On' with a radio button. Below this is the 'User Setup' section. It contains two input fields for 'Username' and 'Password'. Below these are five checkboxes for permissions: 'Write', 'Read', 'Delete', 'Rename', and 'List'. A table lists two users: 'ftp_admin@tecnicor...' with password 'ftpadmin' and permission 'RWDNL', and 'ftp_user@tecnicorp....' with password 'ftpuser' and permission 'RWL'. To the right of the table are 'Add', 'Save', and 'Remove' buttons.

	Username	Password	Permission
1	ftp_admin@tecnicor...	ftpadmin	RWDNL
2	ftp_user@tecnicorp....	ftpuser	RWL

Se establecen dos usuarios con sus respectivas contraseñas. Una para administradores con todos los permisos de operaciones CRUD (Create, Read, Delete, Update, o en este caso RWDNL), y otra para usuarios con permisos de lectura, listado y escritura de nuevos archivos. Con estos usuarios establecidos, podemos acceder al repositorio de archivos de la empresa desde cualquier dispositivo en la red amplia mediante los siguientes comandos en la terminal:

ftp 192.168.0.70

Posteriormente, se pedirán las credenciales y al ingresarlas correctamente se habrá accedido al repositorio exitosamente:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.0.70
Trying to connect...192.168.0.70
Connected to 192.168.0.70
220- Welcome to PT Ftp server
Username:ftp_admin@tecmicorp.com
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.0.70:
0   : asa842-k8.bin                      5571584
1   : asa923-k8.bin                      30468096
2   : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3   : c1841-ipbase-mz.123-14.T7.bin        13832032
4   : c1841-ipbasek9-mz.124-12.bin         16599160
5   : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6   : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7   : c2600-i-mz.122-28.bin               5571584
8   : c2600-ipbasek9-mz.124-8.bin          13169700
9   : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10  : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11  : c2800nm-ipbase-mz.123-14.T7.bin      5571584
12  : c2800nm-ipbasek9-mz.124-8.bin        15522644
13  : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14  : c2950-i6q412-mz.121-22.EA4.bin      3058048
15  : c2950-i6q412-mz.121-22.EA8.bin      3117390
16  : c2960-lanbase-mz.122-25.FX.bin       4414921
17  : c2960-lanbase-mz.122-25.SEE1.bin     4670455
18  : c2960-lanbasek9-mz.150-2.SE4.bin     4670455
19  : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20  : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21  : c800-universalk9-mz.SPA.152-4.M4.bin  33591768
22  : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23  : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24  : cgr1000-universalk9-mz.SPA.154-2.CG  159487552
```

Nota: Las direcciones IPv4 de los servidores deben ser estáticas (no DHCP), porque proveen servicios a los que acceden otros dispositivos a través de su dirección IP, y si esta cambia, los dispositivos serán incapaces de encontrar los servidores y acceder a los servicios.

- **Configuración de servidor web (HTTP/S y DNS):** Como parte del servicio que ofrece ByteWay de personalización de red para el cliente, se propone la inclusión de un servidor web con DNS y HTTPS o HTTP (a elección de la empresa) debido a que se considera que la empresa TecmiCorp se vería beneficiada de una plataforma digital. **El costo del alojamiento web será cubierto por ByteWay durante el primer año.** Se eligió como nombre de dominio www.tecmicorp.com. La configuración del DNS (para que el nombre de dominio se resuelva a la dirección IPv4) es la siguiente:

BYTEWAY - Propuesta de red para TecmiCorp

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record ▾

Address

Add Save Remove

No.	Name	Type	Detail
0	www.tecmicorp.com	A Record	192.168.0.50

La configuración HTTP/S es la siguiente:

HTTP

HTTP ☒ On ☐ Off

HTTPS ☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

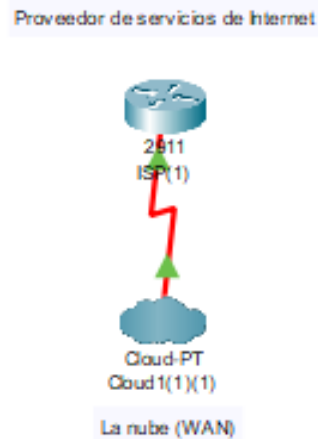
Se provee acceso a los archivos del sitio web a los administradores de la empresa. Como placeholder, **index.html** se vería de la siguiente forma inicialmente:



2- Estructura de red pública simulada (WAN)

El siguiente paso es establecer una WAN central. Se optó por usar una **topología en estrella** (arquitectura jerárquica), la cual consiste en conectar todas las redes a un nodo central en común.

Es en esta parte del proyecto en la que se pueden observar más discrepancias entre la simulación de Cisco Packet Tracer y una WAN real. Debido a las limitaciones del software, no contamos con una representación 100% acertada de las conexiones por WAN. Por ejemplo, en una WAN real, el nodo central (el punto de conexión entre todas las redes) sería el Internet o la nube, pero este último componente en Cisco Packet Tracer no retransmite datos después de recibirlos, por lo que es inútil como punto de conexión entre dos o más redes. Se optó por representar la WAN a través de un router representativo del proveedor de servicios de Internet, con una nube conectada a él como representación visual de lo que sería el Internet en sí o la nube en la red real. En la simulación, el router es el punto que conecta las redes entre sí y hace posible su comunicación, pero en la vida real, esto funciona de manera diferente, lo cual será explicado posterior a esta justificación de diseño. Se eligió el mismo modelo de las redes locales (2911) para el router central porque no hay necesidad de acceder a funciones diferentes o especiales.



Adicionalmente, como se puede observar, el router representaría en una red real el proveedor de servicios de Internet (ISP), que conectaría las redes a la red pública. Esta conexión no se realizaría a través de un router central, pero con eso está siendo representado en la simulación. Por último, también es importante mencionar que en Packet Tracer, las conexiones abstractas, inalámbricas y/o a larga distancia se representan por cables seriales (color **rojo**), aunque en la red real se conectarán por sus medios adecuados.

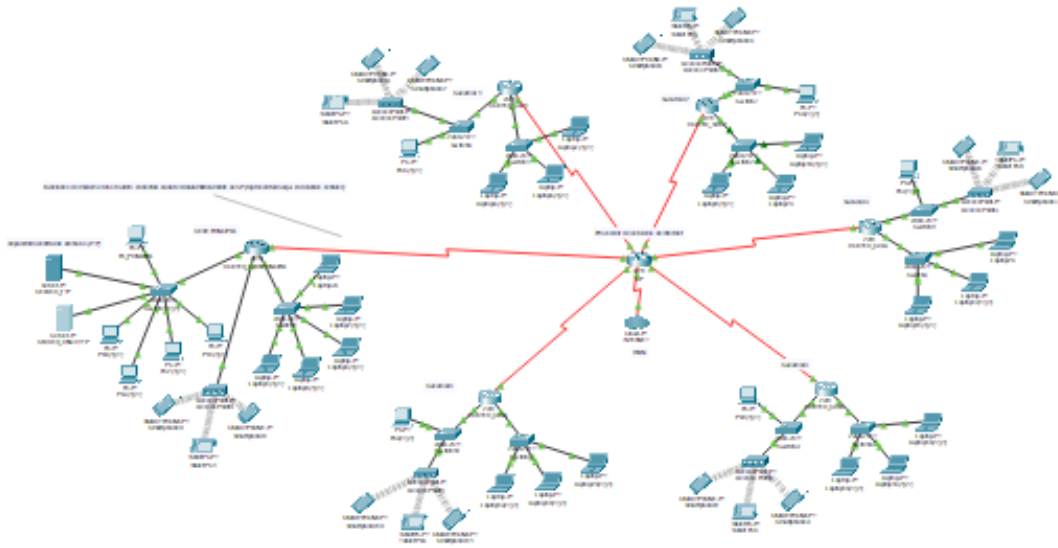
¿Cómo funciona en una red real?

En una red real, no habría router central al que todas las redes (ubicaciones) se puedan conectar simultáneamente. Es verdad que habría un nodo central (el Internet/la nube), y la topología sería exactamente la misma (en estrella), pero las sucursales se conectarían a la WAN mediante módems o servicios de Internet en sus mismos routers. A través de los servicios del ISP de elección, las redes pueden comunicarse con otras redes conectadas a la WAN. En el caso de Internet, con cualquier dispositivo público en la red global (por ejemplo, servidores web).

Medida de seguridad adicional

Se podría considerar el uso de una VPN (Virtual Private Network) para mayor seguridad. Estas redes crean túneles cifrados dentro de los cuales el tráfico entre sucursales viaja, disminuyendo el riesgo de interceptación de datos. De este modo, se establece una red privada dentro de la red pública, protegiendo la información de la empresa de manera efectiva.

Al establecer las conexiones entre las sucursales, la sede principal y el router central, obtenemos la siguiente estructura:



Los cables seriales se conectan a **interfaces seriales** en cada router, y se les asigna una dirección IPv4 **pública** (no puede pertenecer a los rangos de direcciones privadas). En este caso, todas las direcciones públicas pertenecen a la red **192.0.2.0**.

El último paso es establecer el enrutamiento de los datos entre las redes locales.

3- Enrutamiento

RIP

RIP (Routing Information Protocol) es un protocolo de enrutamiento dinámico que permite a los routers intercambiar información sobre redes dentro de un sistema autónomo. Funciona enviando periódicamente actualizaciones con la cantidad de "saltos" (hops) necesarios para llegar a cada destino. Usa un límite de 15 saltos, lo que lo hace adecuado para redes pequeñas, pero menos eficiente en redes grandes, como la Internet pública. En este caso, no hace daño usarlo ya que la red es relativamente pequeña, pero esto no es del todo escalable, considerando además que a pesar de ser técnicamente dinámico, este protocolo requiere agregar las nuevas redes a las tablas (listas) respectivas de manera manual, y en algún momento se alcanzará el límite de 15 redes y las sobrantes estarán completamente aisladas y privadas de comunicación de las demás. Para propósitos de simplicidad del modelo simulado, aun con estas limitaciones se optó por usar RIP, pero en la red real, existe la siguiente alternativa:

OSPF (alternativa escalable)

OSPF (Open Shortest Path First) es un protocolo de enrutamiento dinámico que encuentra la mejor ruta en una red utilizando el algoritmo de estado de enlace. A diferencia de RIP, que solo cuenta saltos, OSPF calcula rutas basándose en costos, considerando factores como el ancho de banda. Además, es más eficiente para redes grandes porque envía actualizaciones solo cuando hay cambios, en lugar de periódicamente como RIP.

En OSPF, las tablas de enrutamiento se actualizan automáticamente cuando se detecta una nueva red con el mismo protocolo. Esto es posible gracias a su sistema de identificación de 'vecinos', donde los routers intercambian información sobre sus rutas y colaboran para calcular el camino más eficiente para los paquetes de datos.

Implementación de RIP en Packet Tracer

En cada sucursal (y la sede principal), se añaden a la tabla de RIP las direcciones IP de las redes que se considerarán para el enrutamiento:

RIP Routing (v2)

Network
<input type="text"/>
Add

Network Address
172.16.0.0
192.0.2.0
192.168.0.0
192.168.1.0

Remove

Se agregan las direcciones de red privada (en este caso, las direcciones de todas las subredes, porque queremos mandar y recibir paquetes tanto en las PCs y laptops como en dispositivos móviles) y la dirección de la red pública (a la que pertenece la interfaz que se conecta al router central).

Luego, en el router central, el cual distribuirá el tráfico a la red adecuada, hay que agregar a la tabla cada una de las redes privadas, y por supuesto, la red pública. Es importante recordar que la red pública es necesaria porque es la red que conecta las redes privadas. Sin ella, las redes privadas no se podrían comunicar. En un caso más realista, habría conflictos en esta comunicación porque las direcciones IPv4 privadas no son entendidas por las públicas, por lo que se requiere hacer uso de un protocolo de traducción en los routers que permita que datos salgan de y entren a la red privada. Este protocolo es NAT, pero en esta simulación, el enrutamiento RIP se encarga de hacer las conversiones adecuadas, eliminando la necesidad de configurar NAT en cada router. En la red real, al trabajar con IPv6, se eliminaría la necesidad de configurar NAT debido a su cantidad de direcciones disponibles.

RIP Routing (v2)

Network	
	Add

Network Address	
172.16.0.0	
192.0.2.0	
192.168.0.0	
192.168.1.0	
192.168.2.0	
192.168.3.0	
192.168.4.0	

Remove

RIP Routing (v2)

Network	
	Add

Network Address	
192.168.5.0	
192.168.6.0	
192.168.7.0	
192.168.8.0	
192.168.9.0	
192.168.10.0	
192.168.11.0	

Remove

Total de redes en la tabla del router central (ISP): 14

Con estas configuraciones, ya tendremos el proyecto desarrollado por la parte teórica. Haremos algunas pruebas para verificar la conectividad entre los dispositivos de diferentes sucursales.



III

PRUEBAS, RESULTADOS E IDENTIFICACIÓN DE AMENAZAS

Con el propósito de exponer los resultados obtenidos en la implementación simulada de la estructura de red propuesta e identificar posibles amenazas a la seguridad, proponiendo igual sus respectivas soluciones..

PRUEBAS Y RESULTADOS

El siguiente es un ping de una laptop de la sede principal a la PC de escritorio de la sucursal 1:

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=25ms TTL=125
Reply from 192.168.2.2: bytes=32 time=10ms TTL=125
Reply from 192.168.2.2: bytes=32 time=64ms TTL=125
Reply from 192.168.2.2: bytes=32 time=13ms TTL=125

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 64ms, Average = 28ms
```

Como se puede observar, el resultado es positivo. Las redes están efectivamente conectadas entre sí. Es importante que todos los dispositivos tengan direcciones IPs, máscaras de subred y puertas de enlace válidas, idealmente asignadas por DHCP, que las redes estén presentes en las tablas RIP adecuadas, y que la configuración física sea la correcta (interfaces correctas, cables o medios de conexión adecuados, etc.)

Todas las pruebas de conectividad deberían ser satisfactorias si se cumplen estos simples criterios. Para evitar redundancia en este documento, las siguientes pruebas se harán por medio de PDUs directos.

PDU List Window										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC9(1)(1)	Laptop2(1)(1)	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Laptop6(...)	PC7(1)(1)	ICMP		0.000	N	1	(edit)	(delete)
	Failed	Laptop10(...)	Laptop16(1)(1)	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Laptop10(...)	Laptop16(1)(1)	ICMP		0.000	N	3	(edit)	(delete)
	Failed	PC8(1)(1)	Laptop25	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC8(1)(1)	Laptop25	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Laptop18(...)	PC1(1)(1)	ICMP		0.000	N	6	(edit)	(delete)
	Successful	Laptop6(...)	PC6(1)(1)	ICMP		0.000	N	7	(edit)	(delete)
	Successful	Router13	Laptop10(1)(1)	ICMP		0.000	N	8	(edit)	(delete)
	Successful	PC8(1)(1)	PC4(1)(1)	ICMP		0.000	N	9	(edit)	(delete)

Existe un bug común en Cisco Packet Tracer que consiste en que algunos PDUs fallan a pesar de que los dispositivos estén completamente bien configurados y conectados. Este es un error del software y no hay manera de evitarlo en ocasiones. Este error se soluciona volviendo a mandar el paquete de datos o generando más tráfico en la red. En este caso, el error apareció un par de veces, pero después de cada uno se volvió a mandar el mismo PDU de la misma fuente al mismo destinatario para comprobar que el error es del software y no un error de conectividad.

Se puede observar que la conectividad entre dispositivos de diferentes redes existe y es posible a través de una WAN (red de redes). Con estas comprobaciones, se puede dar por terminado el proyecto y entregar este modelo de infraestructura y diseño como propuesta para la red de TecmiCorp.

EJEMPLO DE FLUJO DE OPERACIONES CON LA RED:

El siguiente es un ejemplo del flujo de las operaciones empresariales de TecmiCorp haciendo uso de los elementos definidos en la propuesta de infraestructura de red:

1. Un equipo de la sede central diseña una estrategia para un cliente y la sube al **servidor web** para que el cliente la revise en un portal privado.
2. El equipo de redes sociales crea imágenes y videos, los almacena en el **servidor FTP** y los distribuye a las sucursales para su publicación.
3. Los empleados en las sucursales revisan métricas de rendimiento accediendo al **servidor web** y ajustan estrategias en base a los resultados.
4. Un diseñador sube una maqueta web al **FTP**, permitiendo que el cliente y el equipo la revisen antes del lanzamiento.
5. Se programan campañas de publicidad y automatización de correos desde la sede central, y los equipos regionales supervisan la conversión local.

IDENTIFICACIÓN DE AMENAZAS

A continuación, definiremos algunas amenazas comunes y las protecciones adecuadas contra ellas. Dichas opciones de protección pueden ser implementadas en la red real, y se ofrecen como servicios de Byteway. Se implementará cualquier servicio por el que el cliente opte.

- **Malware (externa):** Son programas maliciosos que pueden infiltrarse en la red a través de correos electrónicos, descargas no seguras o dispositivos infectados que estén conectados a la red.
- **Intercepción de tráfico de datos (externa):** Las conexiones inalámbricas pueden ser interceptadas más fácilmente que las conexiones cableadas. Un atacante externo podría realizar ataques para interceptar y modificar datos en tránsito.
- **Acceso no autorizado a dispositivos y servidores (interna):** Sin una adecuada segmentación de redes y control de accesos, empleados o intrusos dentro de la empresa pueden obtener acceso a información que no deberían ver. Si la red tiene password, se incrementa la seguridad, pero si las credenciales son débiles, el acceso no autorizado sigue siendo una amenaza.
- **Engaños y manipulación para obtener información (externa e interna):** Los atacantes pueden engañar a empleados para que revelen credenciales o información sensible. Este tipo de amenazas puede originarse externamente, por ejemplo, un hacker enviando un correo falso, o interna, cuando un empleado malintencionado obtiene datos de sus compañeros.

- **Ataques de denegación de servicio (DDoS) (externa):** Una sobrecarga de tráfico malicioso puede afectar la disponibilidad de la red y de los servidores, especialmente si TecmiCorp decide hospedar servicios web internos. Este tipo de ataque puede interrumpir la comunicación entre las sucursales y afectar la operatividad de la empresa.

IDENTIFICACIÓN DE POSIBLES ATAQUES

- **Ataque de suplantación de identidad en redes internas (Spoofing):** Este ataque ocurre cuando un atacante falsifica la dirección IP o la dirección MAC de un dispositivo legítimo dentro de la red para engañar al sistema y obtener acceso no autorizado. El riesgo es que un atacante podría hacerse pasar por un router o servidor y redirigir el tráfico de datos a su equipo para robar información sensible.
- **Ataques a la red inalámbrica mediante accesos no autorizados:** Como TecmiCorp incluye puntos de acceso inalámbricos, la red está expuesta a ataques como el punto de acceso falso, que esto se refiere a que un atacante puede instalar un punto de acceso no autorizado cerca de las instalaciones y configurarlo con el mismo SSID de la de TecmiCorp. Con esto, puede engañar a los empleados para que se conecten a él y robar sus datos.
- **Ataque de intrusión por explotación de puertos abiertos:** Este ataque ocurre cuando un atacante escanea la red en busca de puertos abiertos en dispositivos o servidores, con el objetivo de explotar vulnerabilidades en los servicios que los utilizan.

PROPUESTAS DE MEDIDAS DE SEGURIDAD

Las siguientes medidas de seguridad se definen como propuestas de servicios de seguridad ofrecidos por Byteway:

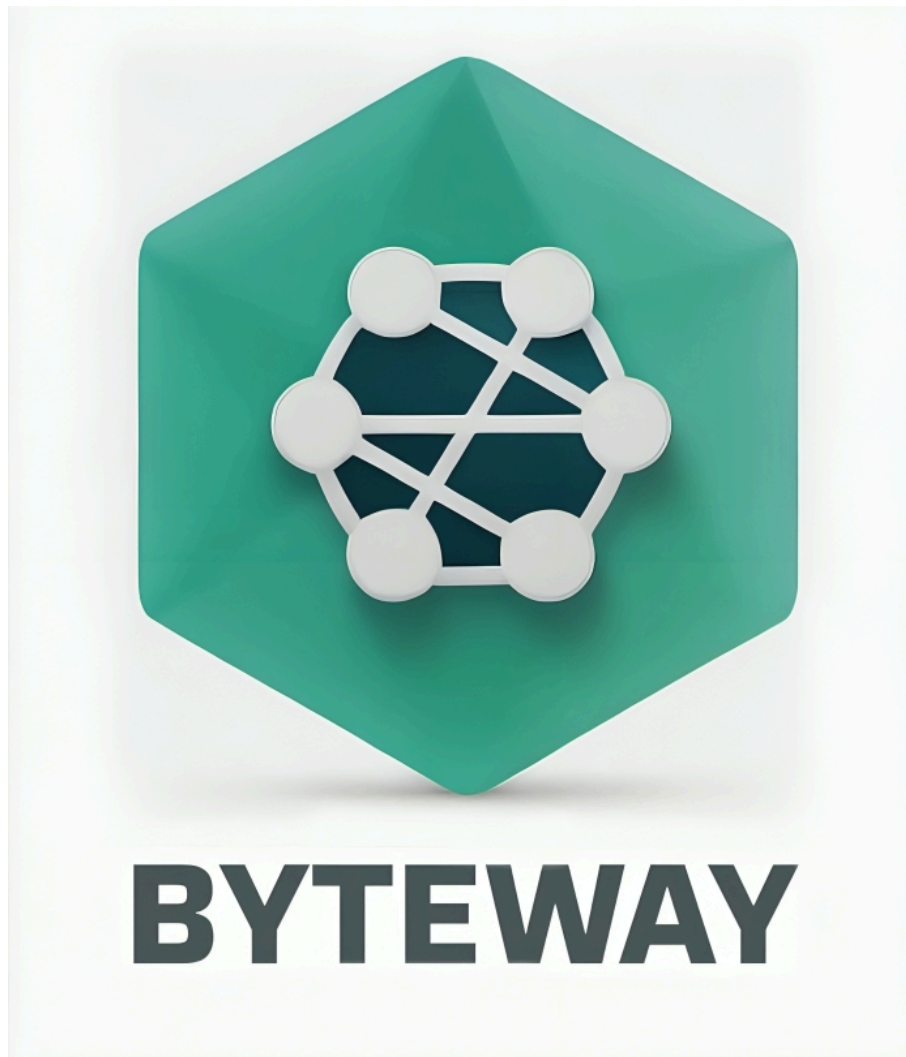
- **Implementación de firewalls y filtrado de tráfico:** Un firewall actúa como una barrera de seguridad entre la red interna de TecmiCorp y el tráfico externo. Se puede configurar para bloquear conexiones sospechosas, restringir el acceso a servicios esenciales y prevenir ataques de intrusión.
- **Segmentación de red y uso de VLANs:** Dividir la red en subredes separadas (VLANs) evita que un atacante que comprometa una parte de la red pueda moverse libremente a otros sistemas. Un beneficio es que protege dispositivos sensibles, como servidores, de accesos no autorizados y aumenta la eficiencia del tráfico de red y mejora el rendimiento.
- **Monitoreo y detección de intrusos (IPS):** Un sistema de prevención de intrusos permiten identificar y bloquear actividad sospechosa en la red. Su implementación es instalar IPS en el firewall para analizar el tráfico en tiempo real y implementar reglas de detección de anomalías en switches y routers.
- **Cifrado de datos y seguridad en accesos remotos:** Para proteger la comunicación dentro de la red de TecmiCorp, hemos implementado el cifrado en la transmisión de

datos mediante protocolos seguros. En particular, utilizamos SSH en lugar de Telnet para los accesos remotos a routers y switches, garantizando que la administración de la red se realice de manera segura y evitando que credenciales o configuraciones sensibles sean interceptadas por atacantes. Con esta medida, reforzamos la protección de la infraestructura y aseguramos una gestión eficiente y segura de los dispositivos de red.

- **Gestión segura de datos y acceso a servidores:** Para garantizar la seguridad y estabilidad de la red de TecmiCorp, hemos implementado medidas que protegen la información dentro de la infraestructura. La segmentación de la red nos permite administrar el tráfico de datos de manera eficiente y evitar accesos no autorizados a servidores. Además, el uso de contraseñas en los routers y servidores asegura que solo el personal autorizado pueda realizar configuraciones y gestionar los recursos críticos.

PROPUESTA PARA UNA RED CONFIABLE

Nuestra red en TecmiCorp ha sido diseñada para garantizar confiabilidad, seguridad y escalabilidad, asegurando que las operaciones empresariales se mantengan estables y protegidas ante cualquier amenaza. La implementación de SSH en lugar de Telnet refuerza la seguridad en la administración remota de los routers, evitando que credenciales sean interceptadas. Además, la segmentación de la red en subredes permite controlar mejor el tráfico y dificulta la propagación de ataques, lo que mejora la estabilidad y seguridad del sistema. La incorporación de IPv6 fortalece la confiabilidad al proporcionar una estructura más eficiente para la asignación de direcciones y permitir la integración de IPSec, lo que refuerza la protección de los datos en tránsito. La configuración de contraseñas en cada router evita accesos no autorizados y fortalece la seguridad de la infraestructura, asegurando que solo personal autorizado pueda realizar cambios en la red. Para la gestión de servidores, hemos implementado un servidor FTP y un servidor web (HTTPS y DNS) con control de usuarios y permisos específicos, lo que garantiza que la información compartida se maneje de forma segura. La integración de DHCP en nuestra infraestructura permite la asignación dinámica de direcciones IP, reduciendo la necesidad de configuraciones manuales y mejorando la eficiencia operativa. El uso de RIP facilita la comunicación entre las distintas sucursales, asegurando que el tráfico fluya correctamente dentro de la red de TecmiCorp. Por último, nuestra red está interconectada mediante una topología jerárquica con un ISP central, lo que proporciona estabilidad en la comunicación entre la sede principal y las sucursales. Con estas medidas, garantizamos que la red de TecmiCorp sea confiable, segura y escalable, permitiendo el crecimiento y la adaptación a nuevas necesidades sin comprometer el rendimiento ni la protección de los datos.



IV

RESÚMEN DE COMPLEJIDADES AÑADIDAS, CONCLUSIONES Y REFERENCIAS

Con el propósito de proporcionar información de terminología usada en el proyecto y listar fuentes, autores, conclusiones y agradecimientos.

COMPLEJIDADES EXTRA AÑADIDAS:

Como parte de los servicios de Byteway, se añadieron las siguientes complejidades a la propuesta de la infraestructura de red para TecmiCorp, sin costo adicional:

1. **Accesos inalámbricos:** Para responder a la demanda de conectividad personal constante, se añadieron accesos inalámbricos a cada sucursal. En el caso de la sede principal, este acceso representa una subred adicional. En cuanto a las demás sucursales, no se agrega una nueva subred. No estuvo en los requerimientos del proyecto considerar el uso de dispositivos inalámbricos.
2. **Servidor web:** Se incluyó un servidor web con DNS y HTTP habilitado, así como acceso al repositorio de archivos para la modificación de estos. Se incluye el dominio web www.tecmicorp.com. Byteway cubrirá el costo del alojamiento web durante el primer año.

GLOSARIO DE TERMINOLOGÍA

Con el objetivo de aclarar conceptos y términos clave al lector para un fácil entendimiento del proyecto. Refiérase a esta sección en caso de dudas sobre algún término. No se incluyen los conceptos explicados durante el desarrollo.


Definiciones

- **Router:** Un router es un dispositivo que permite conectar redes y dispositivos a una red. Sin embargo, un router no representa la red en sí, y actúa como un punto de conexión. Los routers disponen de interfaces a las que se les dan direcciones IP, tanto públicas (WAN) como privadas (LAN).
- **Switch:** Es un dispositivo que conecta equipos en una red local (LAN). Su función es distribuir el tráfico de datos entre los dispositivos conectados, lo que permite que se comuniquen e intercambien información.
- **Dispositivos de salida:** Los dispositivos de salida son aparatos que reciben información y la muestran al usuario en formato visual, sonoro o impreso (laptops, PCs, etc.)
- **Dirección IP privada:** Una dirección IP privada es una dirección numérica que identifica a un dispositivo en una red local.
- **Dirección IP pública:** Una dirección IP pública es una dirección numérica que identifica a un dispositivo en una red pública. Las direcciones IP públicas y privadas no son compatibles entre sí.
- **DHCP:** Es un protocolo de red que asigna direcciones IP y otra información de direccionamiento dinámicamente a los dispositivos que se conectan a una red.

- **Conexiones inalámbricas:** Las conexiones inalámbricas son aquellas que permiten que los dispositivos se conecten a una red sin necesidad de cables. Se utilizan ondas electromagnéticas para transmitir y recibir información entre los equipos. Por ejemplo, Wi-Fi.
- **Conexiones físicas:** Las conexiones físicas son los medios tangibles que transportan datos entre dispositivos. Se realizan a través de cables en interfaces de dispositivos.
- **LAN:** Por sus siglas en inglés, Red de Área Local. Se refiere a un grupo de dispositivos interconectados en un mismo lugar, como una casa, oficina o escuela.
- **WAN:** Por sus siglas en inglés, Red de Área Amplia. Se trata de una tecnología que interconecta redes más pequeñas, es decir, una red de redes. El Internet es una WAN global.
- **Enrutamiento:** El enrutamiento en redes es el proceso de seleccionar la ruta más adecuada para enviar paquetes de datos entre redes. Esto se realiza dando a dispositivos como routers información sobre las redes en su rango de proximidad para que mapeen la infraestructura y calculen las rutas óptimas.
- **Punto de acceso (Access Point):** Es un dispositivo que, como su nombre lo indica, proporciona un punto de acceso inalámbrico a una red.
- **Arquitectura de red:** El diseño estructural y funcional de una red de comunicación, incluyendo su topología, protocolos, hardware y software. Define cómo los dispositivos se conectan, cómo se gestionan los datos y cómo se establecen las reglas de comunicación. Su objetivo es garantizar eficiencia, seguridad y escalabilidad en la transmisión de información.
- **Topología:** La estructura o disposición física y lógica de los dispositivos y conexiones dentro de una red. Puede describir cómo los dispositivos están conectados entre sí (topología física) y cómo se transmiten los datos entre ellos (topología lógica).
- **SSH:** Protocolo de red que permite acceder y administrar de forma segura dispositivos remotos a través de una conexión cifrada. Se utiliza principalmente para administrar servidores, transferir archivos de manera segura y ejecutar comandos de forma remota. SSH protege la comunicación mediante cifrado y autenticación, evitando que terceros intercepten o manipulen los datos transmitidos.
- **Segmentación de red:** Proceso de dividir una red en segmentos más pequeños y aislados para mejorar el rendimiento, la seguridad y la gestión del tráfico. Al separar dispositivos en diferentes subredes o VLANs, se reduce la congestión, se minimiza la propagación de fallos y se limita el acceso no autorizado.
- **Ethernet:** Estándar de comunicación para redes de área local (LAN) que permite la transmisión de datos entre dispositivos mediante cables. Utiliza un protocolo basado en tramas y direccionamiento MAC para garantizar una comunicación eficiente y confiable. Es ampliamente utilizado debido a su velocidad, estabilidad y compatibilidad con diversas tecnologías de red.
- **DNS:** Domain Name System. Es el sistema encargado de traducir nombres de dominio legibles por humanos (como www.ejemplo.com) en direcciones IP numéricas (como 192.168.1.1) que los dispositivos pueden utilizar para comunicarse entre sí en la red. Se puede pensar como una agenda telefónica de sitios web.

- **HTTP/S:** (Hypertext Transfer Protocol) es el protocolo utilizado para la transferencia de información en la web, permitiendo la comunicación entre navegadores y servidores web. HTTPS es la versión segura de HTTP, donde la "S" significa seguridad y emplea SSL/TLS para cifrar la información que se transmite, protegiendo así los datos contra interceptaciones y asegurando la autenticidad del servidor. HTTPS es esencial para garantizar la privacidad y seguridad en transacciones online, como compras o inicio de sesión.
- **HTML:** (HyperText Markup Language) es el lenguaje estándar utilizado para crear y estructurar páginas web. Utiliza "etiquetas" o "elementos" para definir diferentes partes del contenido, como encabezados, párrafos, imágenes, enlaces y formularios. Aunque HTML no es un lenguaje de programación, es esencial para estructurar la información de manera que los navegadores puedan mostrarla correctamente a los usuarios.

BIBLIOGRAFÍAS

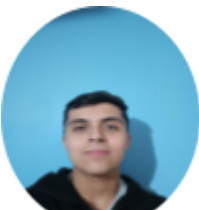
1. FS.com. (n.d.). *RIP vs OSPF: ¿Cuál es la diferencia?*. Recuperado de <https://www.fs.com/es/blog/rip-vs-ospf-what-is-the-difference-5221.html>
2. Alex Castillo. (2017, octubre 24). *Como crear red wan Cisco Packet Tracer [Video]*. Youtube.  Como crear red wan Cisco Packet Tracer
3. OpenAI. (2024). ChatGPT (modelo GPT-4-turbo) [Asistente de IA]. <https://openai.com/chatgpt>

AUTORES

Los alumnos que participaron en el proyecto fueron:



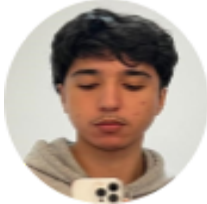
David Alejandro Siu Manjarrez



Asbiel Said Frausto Flores



Luis Fernando Ruiz Valenzuela



Angel Alejandro Reyes Carrasco

CONCLUSIONES Y AGRADECIMIENTOS

Se concluye que el proyecto fue un éxito debido a la implementación exitosa de la infraestructura propuesta en Cisco Packet Tracer y se espera que la empresa TecmiCorp acceda a replicar esta estructura en su red real. Como equipo de consultores de redes, nos ofrecemos a prestar los servicios de implementación en la red real si se decide que el modelo es satisfactorio.

Agradecimientos a la maestra Blanca Aracely Aranda Machorro y a nuestros compañeros de otros equipos, que nos proporcionaron apoyo muy valioso para la resolución de problemas y la obtención de ideas nuevas e ingeniosas para el proyecto.

VIDEO DEMOSTRATIVO DE LA PROPUESTA

https://www.youtube.com/watch?v=eofp2x6zIQY&ab_channel=LuisFernandoRuizValenzuela