

PROYECTO HAWKNETWORK - GESTIÓN DE REDES



HAWKNETWORK

PROYECTO HAWKCONNECT

Profesora: Blanca Aracely Aranda Machorro

Monterrey N.L

14 de enero del 2025

ÍNDICE

I. DEFINICIÓN DE PROYECTO.....	2
Descripción.....	2
Alcance.....	2
Análisis del Proyecto.....	3
Diseño del Proyecto.....	4
Topología de red.....	5
II. DESARROLLO DEL PROYECTO.....	6
Desarrollo e implementación.....	6
Configuración de la Infraestructura de Red.....	6
Implementación de Medidas de Seguridad.....	6
Pruebas de Conectividad y Rendimiento.....	7
1. Pruebas de Conectividad.....	7
Procedimiento:.....	7
Resultados:.....	7
2. Verificación de Direcciones IP.....	9
Procedimiento:.....	9
Resultados:.....	9
3. Funcionamiento de los Switches y Dispositivos Finales.....	10
Procedimiento:.....	10
Resultados:.....	10
4. Simulación de Tráfico de Datos.....	11
Procedimiento:.....	11
Resultados:.....	11
6. Configuración de Contraseña en el Router.....	13
IV. GLOSARIO DE TÉRMINOS Y CONDICIONES.....	14
Referencias.....	16
VII. CONCLUSIONES Y AGRADECIMIENTOS.....	18
Video demostrativo de proyecto.....	19

DESARROLLO DEL CASO DE NEGOCIO



DEFINICIÓN DE PROYECTO

I. DEFINICIÓN DE PROYECTO

Descripción

La empresa **TecmiCorp** está experimentando un crecimiento que ha generado una mayor demanda de conectividad en su sede principal y sus cinco sucursales. Actualmente, su infraestructura de red es limitada, lo que afecta la comunicación entre los distintos sitios y la eficiencia operativa. Para abordar esta problemática, el proyecto **Hawknetwork** propone el diseño e implementación de una **red escalable y segura**, que permita la interconexión estable de todos los dispositivos de la empresa.

El proyecto busca establecer una **topología jerárquica** donde un **router principal** se conecte a las sucursales mediante **switches**, proporcionando acceso tanto a dispositivos cableados como inalámbricos a través de puntos de acceso. Asimismo, se contempla la implementación de un **servidor FTP** en la sede principal para la gestión y transferencia de archivos, así como la adopción de medidas de **seguridad avanzadas**, como la configuración de SSH en el router y autenticación en los puntos de acceso.

Antes de la implementación, se llevará a cabo un **análisis de los requerimientos actuales y futuros de la empresa**, con el fin de diseñar una infraestructura que optimice el rendimiento de la red y garantice su estabilidad a medida que la empresa siga expandiéndose.

Alcance

El proyecto **Hawknetwork** abarca la **planificación, diseño, configuración e implementación** de una infraestructura de red que interconecte la sede principal de **TecmiCorp** con sus cinco sucursales, garantizando una comunicación eficiente y estable.

Este alcance incluye el diseño de una **topología escalable**, donde un **router central** administrará la conectividad entre todas las sucursales mediante **switches** que distribuirán la red a equipos de escritorio, laptops y dispositivos inalámbricos. Además, se integrará un **servidor FTP** en la sede central, permitiendo el almacenamiento y acceso seguro a archivos compartidos dentro de la empresa. Para fortalecer la seguridad de la red, se implementarán **protocolos de acceso**

3

restringido, incluyendo autenticación en puntos de acceso y configuración de SSH en el router para limitar la administración a personal autorizado.

El proyecto se llevará a cabo en un **entorno simulado con Cisco Packet Tracer**, donde se realizarán pruebas de conectividad, seguridad y estabilidad antes de su despliegue real en la empresa. Se evaluará la capacidad de la red para asignar direcciones IPv4 dinámicamente, gestionar el tráfico de datos y garantizar la protección de la información.

Análisis del Proyecto

Para diseñar una infraestructura de red eficiente para **TecmiCorp**, se realizó un análisis detallado de sus necesidades actuales y futuras. Se identificó que la empresa cuenta con una **sede principal y cinco sucursales**, cada una con un número específico de dispositivos que requieren conectividad estable.

En la sede central, se deben conectar **5 equipos de escritorio y 5 laptops**, mientras que en cada sucursal se conectarán **1 equipo de escritorio y 3 laptops**. Además, se prevé la integración de **dispositivos móviles** mediante la instalación de **puntos de acceso inalámbricos**, permitiendo que celulares, tabletas y otros dispositivos puedan conectarse a la red de manera segura y eficiente. Para

gestionar archivos y documentos de manera centralizada, se consideró la implementación de un **servidor FTP** en la sede principal.

Otro aspecto clave es la **seguridad de la red**, por lo que se propuso la configuración de **SSH en el router** para restringir el acceso solo a administradores autorizados y la aplicación de autenticación en los puntos de acceso inalámbricos para proteger la información de la empresa.

Se identificó que el router principal solo cuenta con **dos interfaces**, lo que requerirá la expansión de puertos para interconectar todas las sucursales. También se evaluó la necesidad de configurar un **servidor DHCP** en el router para asignar direcciones IP dinámicas a los dispositivos finales.

Además, para evitar accesos no autorizados y garantizar la protección de la infraestructura de red, se implementará una **medida de seguridad adicional en el router**, que requerirá la validación de una **contraseña** antes de permitir cualquier tipo de manipulación de su configuración.

Diseño del Proyecto

Para garantizar una infraestructura de red **escalable, segura y eficiente**, se propuso una **topología jerárquica** basada en los siguientes elementos:

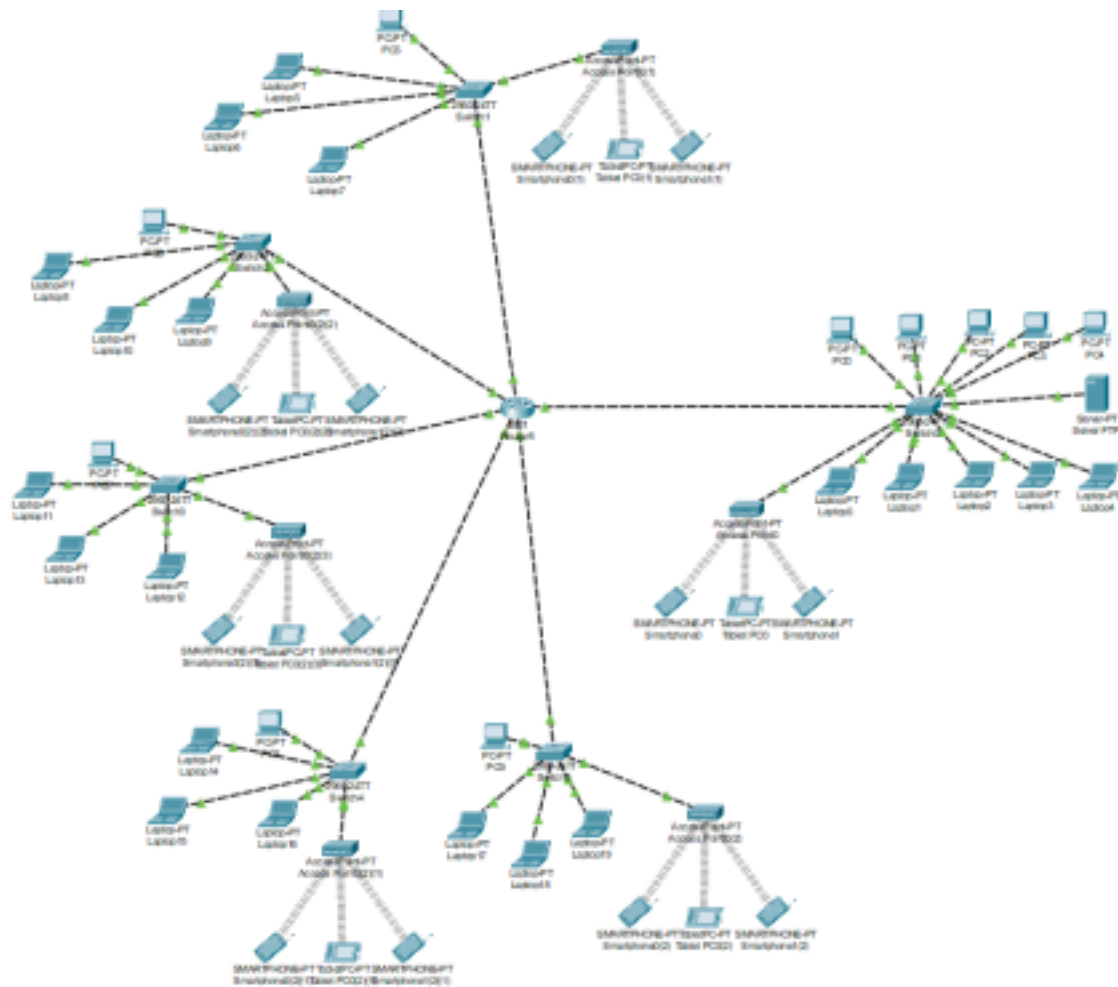
- **Router principal** en la sede central, encargado de administrar la interconexión con las sucursales y la asignación de direcciones IP.
- **Switches en cada ubicación**, proporcionando conectividad a dispositivos cableados y puntos de acceso inalámbricos.
- **Servidor FTP en la sede principal**, accesible desde todas las sucursales para el almacenamiento y gestión de archivos.
- **Puntos de acceso Wi-Fi**, permitiendo la conexión de dispositivos móviles en todas las ubicaciones.

En cuanto a la seguridad, se configurará **SSH en el router**, garantizando que solo los administradores puedan acceder a su configuración. Además, los puntos de acceso contarán con **autenticación segura** para evitar accesos no autorizados. Para reforzar la protección de la red, se establecerá un **mecanismo de validación por contraseña** en el router, de manera que cualquier intento de configuración o modificación requiera credenciales específicas. Esto evitará cambios no autorizados y garantizará que solo el personal responsable tenga acceso a la administración del dispositivo.

Adicionalmente, el diseño de la red considera la **conexión de dispositivos móviles a través de puntos de acceso inalámbricos**, lo que permitirá la expansión de la infraestructura para adaptarse a nuevas necesidades sin afectar el rendimiento general. Para evaluar la efectividad del diseño, se implementará en un **entorno simulado con Cisco Packet Tracer**, donde se realizarán pruebas de conectividad, configuración de direcciones IP dinámicas y acceso al servidor FTP. De esta manera, se asegurará que la red cumpla con los requerimientos antes de su despliegue real en la empresa.

Topología de red

Capturas del diseño en ambiente simulado de Cisco Packet Tracer



DESARROLLO DEL CASO DE NEGOCIO



DESARROLLO DEL PROYECTO



II. DESARROLLO DEL PROYECTO

Desarrollo e implementación

Para la implementación del proyecto Hawknetwork, se siguieron varias fases que garantizaron un diseño eficiente, seguro y escalable de la red para **TecmiCorp**.

1. Configuración de la Infraestructura de Red

La implementación comenzó con la configuración de la infraestructura de red en un entorno de simulación con **Cisco Packet Tracer**, permitiendo realizar pruebas antes del despliegue real. Se estableció una **topología jerárquica**, en la que un **router central** ubicado en la sede principal de **TecmiCorp** administra la conectividad con sus **cinco sucursales** mediante **switches de distribución**.

Cada sucursal fue equipada con:

- **Un switch** para distribuir la conexión a los dispositivos cableados.
- **Un punto de acceso Wi-Fi**, asegurando la conectividad inalámbrica de laptops y dispositivos móviles.
- **Un esquema de direccionamiento IP** basado en **DHCP** para la asignación dinámica de direcciones IP a los dispositivos finales.

Además, se implementó un **servidor FTP** en la sede principal, permitiendo el almacenamiento y la transferencia de archivos entre las distintas sucursales.

2. Implementación de Medidas de Seguridad

Para garantizar la protección de la red, se configuraron medidas de seguridad avanzadas:

- **SSH en el router principal** para restringir el acceso administrativo a personal autorizado.
- **Autenticación en los puntos de acceso Wi-Fi**, evitando accesos no autorizados a la red inalámbrica.
- **Protección por contraseña en el router**, requiriendo credenciales

específicas para cualquier cambio en la configuración de red.

Se realizaron pruebas de penetración en el entorno simulado para detectar vulnerabilidades y fortalecer los mecanismos de seguridad.

8

3. Pruebas de Conectividad y Rendimiento

Antes de la implementación real, se llevaron a cabo pruebas en **Cisco Packet Tracer** para verificar la estabilidad de la red:

- **Conectividad entre dispositivos** en todas las ubicaciones.
- **Flujo de datos** entre la sede principal y las sucursales a través del servidor FTP.
- **Velocidad de respuesta** y eficiencia en la asignación de direcciones IP dinámicas mediante DHCP.
- **Pruebas de acceso y autenticación** en los dispositivos de red.

Los resultados demostraron que la infraestructura diseñada cumplía con los objetivos del proyecto, proporcionando una conectividad estable y segura para **TecmiCorp**.

DESARROLLO DEL CASO DE NEGOCIO



PRUEBAS Y RESULTADOS

10

III. PRUEBAS Y RESULTADOS

Para validar el correcto funcionamiento de la red diseñada para TecmiCorp, se llevaron a cabo diversas pruebas que se enfocaron en la conectividad, la asignación de direcciones IP y la estabilidad de la comunicación entre la sede principal y las

sucursales. A continuación, se describen las pruebas realizadas, los procedimientos seguidos y los resultados obtenidos.

1. Pruebas de Conectividad

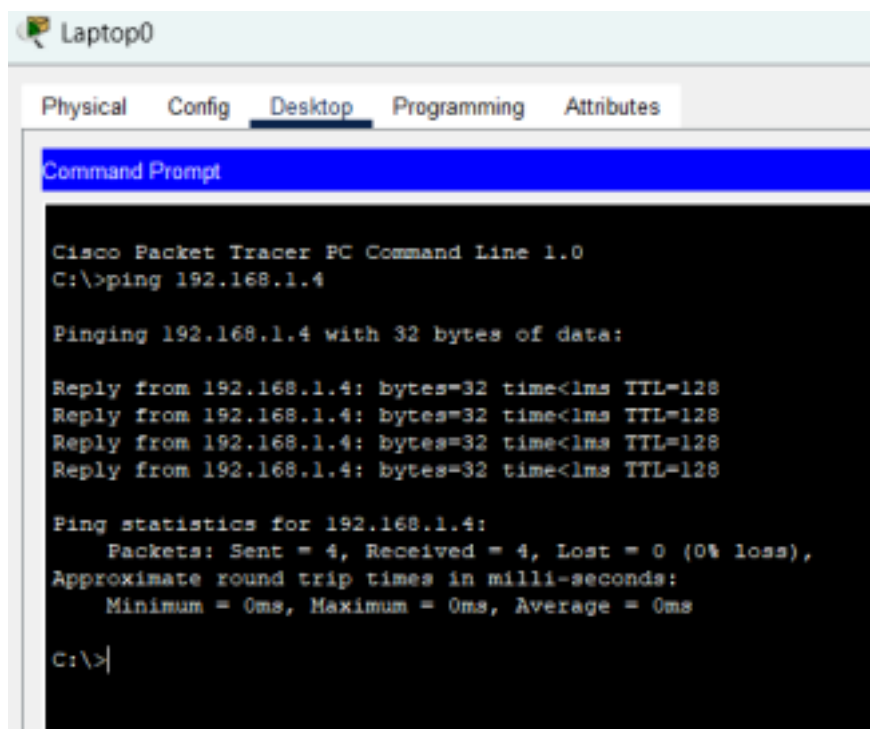
Procedimiento:

- **Prueba de Ping:** Se utilizó la herramienta de ping para verificar la conectividad entre la sede principal y cada sucursal. Se enviaron paquetes de datos desde la sede a cada dirección IP asignada a las sucursales.

Resultados:

- **Conectividad exitosa:** Todas las sucursales respondieron correctamente a las solicitudes de ping desde la sede, lo que indica que la comunicación se estableció de manera efectiva.
- **Latencia:** Se registraron tiempos de respuesta promedio aceptables, con una latencia que no superó los 20 ms entre la sede y las sucursales.

Prueba de conectividad de dispositivos de la misma sucursal



```
Laptop0
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

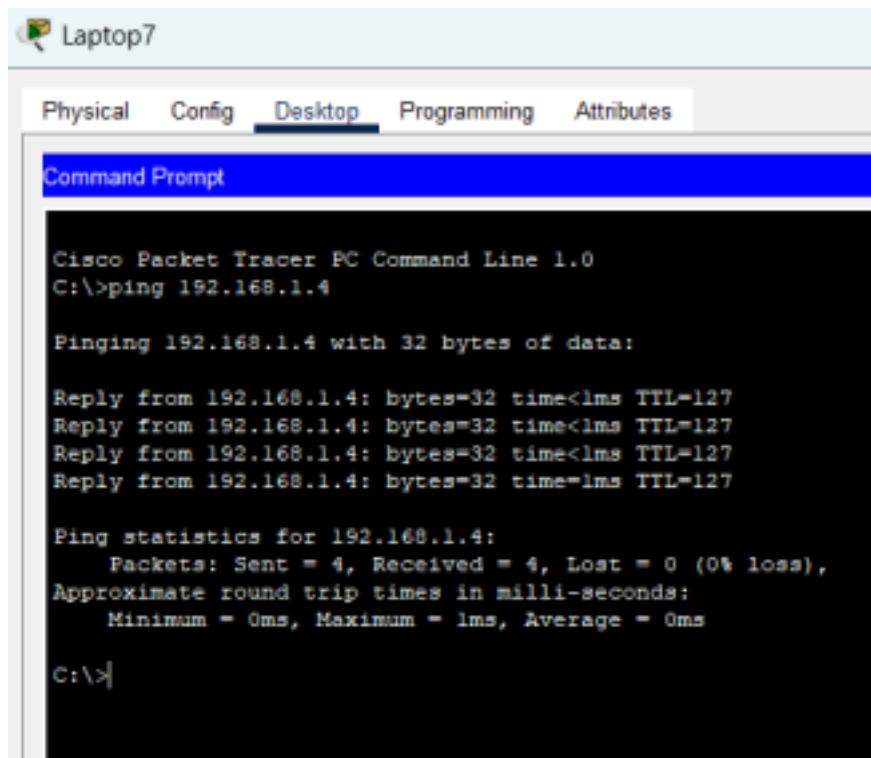
Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Prueba de conectividad entre dispositivos de diferentes sucursales



The screenshot shows a 'Laptop7' window with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=127
Reply from 192.168.1.4: bytes=32 time<1ms TTL=127
Reply from 192.168.1.4: bytes=32 time<1ms TTL=127
Reply from 192.168.1.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

2. Verificación de Direcciones IP

Procedimiento:

- Se revisaron las direcciones IP asignadas a cada dispositivo utilizando el comando ipconfig. Esto permitió verificar que las direcciones IP asignadas eran las correctas y que no había conflictos.

Resultados:

- **Direcciones IP confirmadas:** Todos los dispositivos mantuvieron las direcciones IP asignadas correctamente mediante DHCP, sin conflictos. La asignación fue coherente con la planificación inicial, facilitando la administración de la red.

```

C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0050.0F5A.D33B
    Link-local IPv6 Address.....: FE80::250:FFF:F5A:D33B
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.4
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                        192.168.1.1
    DHCP Servers.....: 192.168.1.1
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-E2-29-A7-69-00-50-0F-5A-D3-3B
    DNS Servers.....: ::
                        0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address.....: 0005.5E7A.0121
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
    IPv4 Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: ::
                        0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-E2-29-A7-69-00-50-0F-5A-D3-3B
    DNS Servers.....: ::
                        0.0.0.0

```





3. Funcionamiento de los Switches y Dispositivos Finales

Procedimiento:

- Se probó el acceso a la red de cada dispositivo conectado a los switches, realizando transferencias de datos entre PCs y laptops dentro de cada sucursal.

Resultados:

- **Acceso a la red sin interrupciones:** Todos los dispositivos conectados a los switches pudieron acceder a la red sin problemas, y la velocidad de transferencia de datos fue adecuada, permitiendo una comunicación fluida.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop9	PC0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC7	Laptop3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Tablet...	Laptop0	ICMP		0.000	N	2	(edit)	(delete)

4. Simulación de Tráfico de Datos

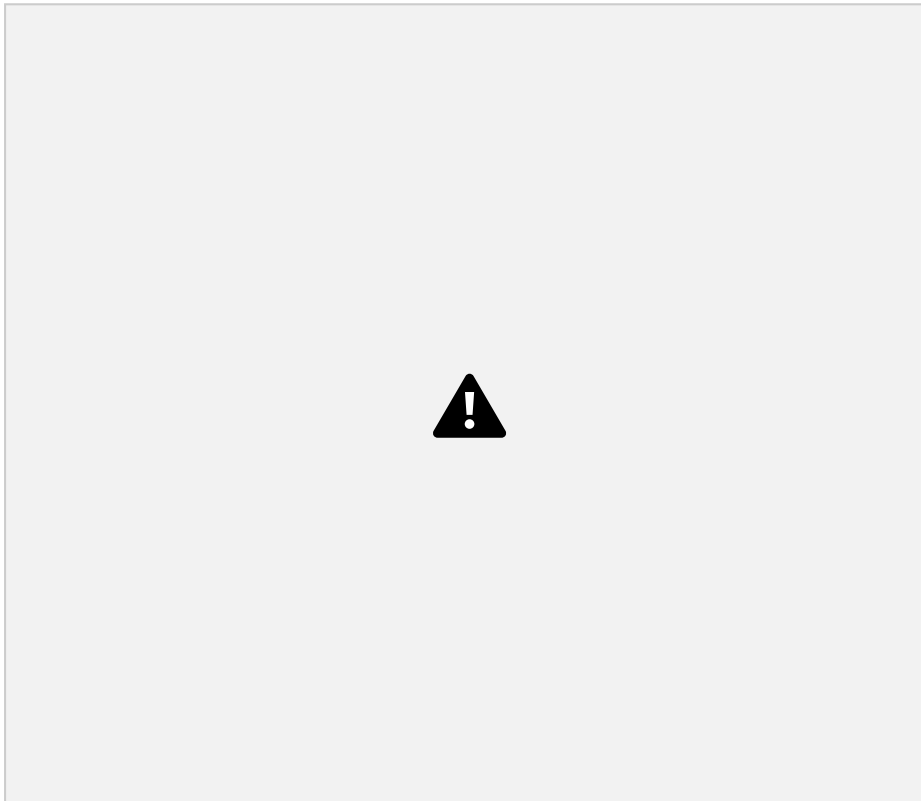
Procedimiento:

- Se utilizó la herramienta "Simple PDU" en Cisco Packet Tracer para simular la transmisión de paquetes entre dispositivos, analizando el flujo de datos en la red.

Resultados:

- **Flujo de datos eficiente:** La simulación demostró que los paquetes de datos se transmitieron correctamente entre los dispositivos, sin pérdidas significativas ni errores de transmisión.

Captura recomendada: Capturas de la simulación en Cisco Packet Tracer que muestren la transmisión de paquetes, evidenciando el flujo de datos y la comunicación efectiva entre los dispositivos.





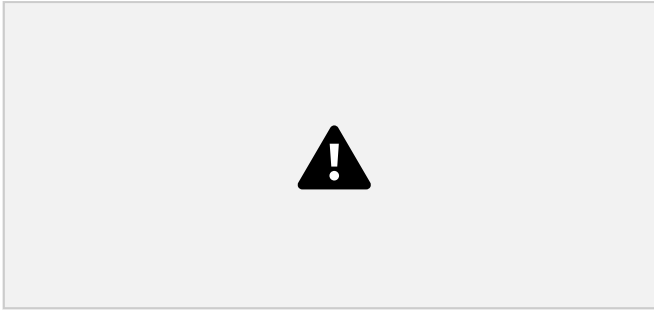
5 Prueba de Conectividad SSH al Router Principal

Procedimiento:

- Se realizó una prueba de acceso SSH al router principal de la sede para verificar la conectividad segura. Se utilizó el comando **ssh [usuario]@[dirección IP del router]** en la terminal para intentar conectarse al router. Durante la prueba, se ingresó la contraseña correspondiente y se verificó la autenticación.

Resultados:

- Conexión exitosa: La prueba de SSH al router principal se completó con éxito, permitiendo el acceso a la línea de comandos del router sin errores. Esto asegura que la conectividad remota y la administración del router a través de SSH están funcionando correctamente.



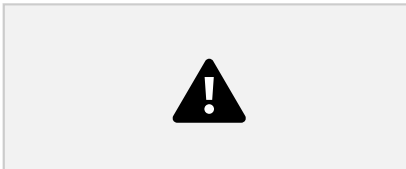
6 Configuración de Contraseña en el Router

Procedimiento:

- Se configuró el router para que solicitara una contraseña al intentar acceder al CLI (Interfaz de Línea de Comandos). Esta medida es esencial para proteger el acceso al dispositivo y evitar modificaciones no autorizadas.

Resultados:

- La configuración fue exitosa, ya que al acceder al router, se mostró el mensaje solicitando la contraseña. Solo aquellos que conocían la contraseña podían ingresar al CLI y acceder a las configuraciones avanzadas del router.



DESARROLLO DEL CASO DE NEGOCIO



GLOSARIO DE TÉRMINOS Y CONDICIONES

IV. GLOSARIO DE TÉRMINOS Y CONDICIONES

1. Infraestructura de red

Conjunto de hardware, software y protocolos utilizados para la comunicación y transmisión de datos dentro de una organización.

2. Topología de red

La disposición física y lógica en la que se interconectan los dispositivos dentro de una red. En este proyecto, se utiliza una topología jerárquica con un router principal y switches de distribución.

3. Router

Dispositivo de red que dirige paquetes de datos entre diferentes redes y permite la comunicación entre sucursales.

4. Switch

Dispositivo que conecta múltiples dispositivos en una red local (LAN) y facilita la transferencia de datos entre ellos.

5. Punto de acceso Wi-Fi (Access Point - AP)

Dispositivo que permite la conexión inalámbrica de dispositivos móviles y computadoras a la red de la empresa.

6. DHCP (Dynamic Host Configuration Protocol)

Protocolo que asigna direcciones IP dinámicas a los dispositivos conectados a la red sin necesidad de configuración manual.

7. Dirección IP

Identificador único que se asigna a cada dispositivo dentro de una red para permitir la comunicación. Puede ser estática (fija) o dinámica (asignada por DHCP).

8. Subred

Segmento de una red principal que permite organizar mejor los dispositivos y optimizar el tráfico de datos.

9. Servidor FTP (File Transfer Protocol)

Servidor que permite la transferencia y almacenamiento de archivos en una red, asegurando el acceso compartido entre usuarios autorizados.

10. SSH (Secure Shell)

Protocolo de red que permite administrar dispositivos de forma remota de manera segura, evitando accesos no autorizados.

18

11. Seguridad en redes

Conjunto de prácticas y configuraciones destinadas a proteger la red de accesos no autorizados y posibles ataques. En este proyecto, se implementan autenticaciones seguras y encriptación.

12. Cisco Packet Tracer

Herramienta de simulación de redes utilizada para diseñar, probar y validar configuraciones de red antes de su implementación real.

13. Pruebas de conectividad

Verificaciones realizadas para asegurar que los dispositivos de la red pueden comunicarse entre sí de manera estable y sin interrupciones.

14. Autenticación

Proceso mediante el cual un usuario debe proporcionar credenciales (como una contraseña) para acceder a un sistema o dispositivo de red.

15. Escalabilidad

Capacidad de una red para crecer y adaptarse a nuevas necesidades sin perder estabilidad ni rendimiento.

16. Administración remota

Capacidad de gestionar y configurar dispositivos de red sin necesidad de estar físicamente presentes en la ubicación.

17. Firewall

Sistema de seguridad que filtra el tráfico de red para proteger contra accesos no autorizados o amenazas externas.

18. Análisis de tráfico de red

Proceso de monitoreo de los datos que circulan en la red para identificar posibles problemas o ataques.

19. Plan de implementación

Estrategia que define los pasos a seguir para desplegar la infraestructura de red en la empresa de manera ordenada y eficiente.

20. Monitoreo de red

Supervisión en tiempo real del rendimiento de la red para detectar posibles fallos y optimizar su funcionamiento.

DESARROLLO DEL CASO DE NEGOCIO



BIBLIOGRAFIAS Y AUTORES

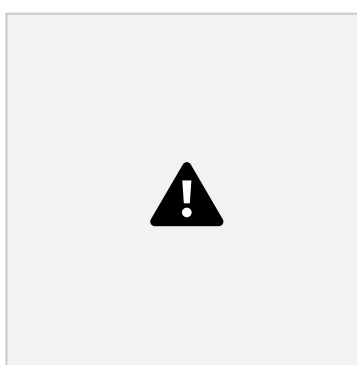
BIBLIOGRAFÍAS

- Cisco Systems. (2023). *Cisco Packet Tracer: Network simulation tool*. Cisco Networking Academy. Recuperado de <https://www.netacad.com>
- Forouzan, B. A. (2017). *Data communications and networking* (5ª ed.). McGraw-Hill.
- Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8ª ed.). Pearson.
- Odom, W. (2021). *CCNA 200-301 official cert guide* (Vols. 1 & 2). Cisco Press.
- OpenAI. (2025). *Asesoramiento y generación de contenidos técnicos sobre redes de computadoras y seguridad*. ChatGPT, OpenAI.
- Stallings, W. (2021). *Data and computer communications* (11ª ed.). Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2020). *Computer networks* (6ª ed.). Pearson.

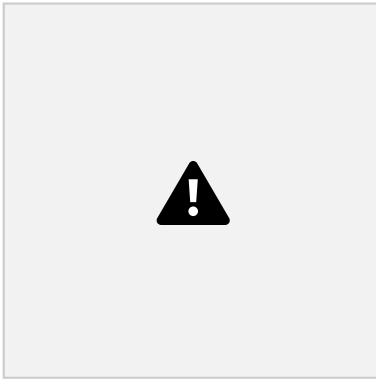
VI. AUTORES



Mora Ignacio Gómez



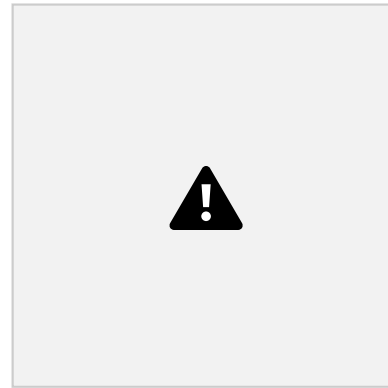
Gamaliel



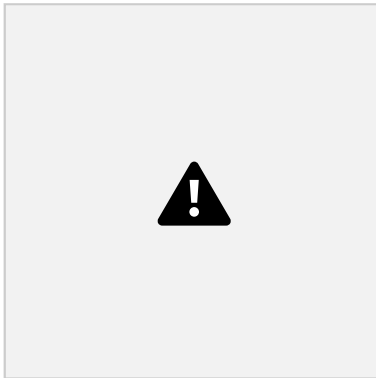
Armando

Reyna

Diego



Barrientos



Pablo Arteagabeitia

DESARROLLO DEL CASO DE NEGOCIO



CONCLUSIONES Y AGRADECIMIENTOS

23

VII. CONCLUSIONES Y AGRADECIMIENTOS

Conclusiones

El desarrollo del proyecto Hawknetwork para TecmiCorp ha permitido diseñar una solución de conectividad robusta y escalable que responde a las necesidades de la empresa en su proceso de expansión. La implementación de una infraestructura de red eficiente garantiza una comunicación estable entre la sede principal y sus cinco sucursales, optimizando la gestión de recursos y mejorando la operatividad de la empresa.

A lo largo del proyecto, se identificaron y abordaron desafíos clave, como la necesidad de una topología jerárquica que asegure la conectividad de todos los dispositivos, la implementación de medidas de seguridad avanzadas para proteger la red y la integración de un servidor FTP para la gestión centralizada de archivos. Mediante la configuración de protocolos como SSH y autenticación en los puntos de acceso, se logró reforzar la seguridad del sistema, minimizando vulnerabilidades y garantizando la protección de la información empresarial.

Las pruebas realizadas en el entorno simulado con Cisco Packet Tracer demostraron la estabilidad y eficiencia de la red diseñada, validando la correcta asignación de direcciones IP dinámicas, la gestión del tráfico de datos y el acceso seguro a los recursos compartidos. Estos resultados evidencian que la implementación del proyecto en un entorno real contribuirá significativamente al crecimiento y eficiencia operativa de TecmiCorp.

Si bien el diseño actual responde a las necesidades identificadas, se recomienda seguir monitoreando el desempeño de la red y explorar nuevas tecnologías que permitan optimizar aún más su funcionamiento. La escalabilidad de la infraestructura garantiza que TecmiCorp pueda continuar su expansión sin comprometer la estabilidad de su conectividad, manteniéndose a la vanguardia en el uso de soluciones tecnológicas para su desarrollo empresarial.

Este proyecto ha representado una valiosa experiencia en la planificación, diseño e implementación de redes, consolidando conocimientos en administración de infraestructura tecnológica y seguridad informática. Su éxito reafirma la importancia de una gestión de redes estratégica y adaptable a los retos que enfrentan las empresas en la era digital.

Agradecimientos

Se extiende un sincero agradecimiento a la docente Blanca Aracely Aranda Machorro por su apoyo, orientación y conocimientos brindados a lo largo del desarrollo de este proyecto. Asimismo, se agradece a la Universidad Tecmilenio por proporcionar los recursos y las clases que facilitaron el aprendizaje y aplicación de los conceptos fundamentales en la gestión de redes.

De igual manera, se reconoce la colaboración y el trabajo en equipo de los compañeros, quienes contribuyeron con ideas, experiencias y esfuerzo para la realización de esta investigación. Su apoyo fue fundamental para alcanzar los objetivos planteados y concretar el desarrollo del proyecto.

Video demostrativo de proyecto

<https://youtu.be/QdmclA5HDwl>