Proyecto Final

Gestión de redes

Mejora de Red para TecmiCorp

Profesora: Blanca Aracely Aranda Machorro

Monterrey, N.L.

14 de febrero del 2025

DESCRIPCIÓN

NetCrew es una empresa especializada en la planificación, diseño e implementación de redes seguras y escalables para empresas en crecimiento. En esta ocasión, trabajamos con TecmiCorp, una compañía en expansión que ha identificado la necesidad de mejorar su infraestructura de red para optimizar la comunicación y la eficiencia operativa entre su sede principal y sus cinco sucursales.

Actualmente, la infraestructura de red de TecmiCorp presenta limitaciones que afectan la conectividad y la administración eficiente de los recursos tecnológicos. Para resolver estos desafíos, el proyecto NetCrew propone el diseño e implementación de una red robusta, que permita la interconexión estable de todos los dispositivos dentro de la empresa.

El proyecto establece una topología jerárquica donde un router principal se conecta a las sucursales mediante switches, proporcionando acceso tanto a dispositivos cableados como inalámbricos a través de puntos de acceso. 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 llevó a cabo un análisis detallado 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 TecmiCorp siga expandiéndose.

GLOSARIO DE TÉRMINOS Y CONDICIONES

Red de Computadoras: Conjunto de dispositivos interconectados para compartir recursos y comunicarse.

Switch: Dispositivo que conecta múltiples dispositivos dentro de una red local (LAN).

Router: Dispositivo que dirige el tráfico de red entre diferentes redes.

IP (Internet Protocol): Dirección única asignada a cada dispositivo en una red.

Escalabilidad: Capacidad de una red o sistema para aumentar su tamaño y rendimiento sin degradaciones

VLAN (Virtual LAN): Segmentación lógica de una red en subredes virtuales para mejorar la seguridad y el rendimiento.

Firewall: Sistema de seguridad que monitorea y controla el tráfico de red entrante y saliente.

Ancho de Banda: Capacidad de transmisión de datos de una red en un período de tiempo.

Latencia: Tiempo que tarda un paquete de datos en viajar desde el origen al destino.

QoS (Quality of Service): Mecanismo que gestiona el tráfico de red para priorizar aplicaciones críticas y mejorar el rendimiento general.

OSPF (Open Shortest Path First): Protocolo de enrutamiento dinámico que encuentra la mejor ruta en la red.

VPN (Virtual Private Network): Tecnología que permite conexiones seguras a través de redes públicas.

ALCANCE

El proyecto NetCrew 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 proyecto mejorará la conectividad organizacional mediante tecnologías clave como VLANs, QoS y VPNs.

Estructura y Cobertura Geográfica

- **Sede principal**: Ciudad de México
- **Sucursales**: Guadalajara, Monterrey, Puebla, Querétaro y Cancún
- **Topología**: Diseño escalable con diferentes topologías para cada sucursal
- **Arquitectura central**: Router principal que administrará la conectividad entre todas las sucursales mediante switches para la distribución de red

Dispositivos y Conectividad

- Equipos de escritorio y laptops
- Dispositivos inalámbricos
- Impresoras
- Servidores

Tecnologías e Implementaciones

- **Redes**: VLANs, QoS, enrutamiento dinámico (OSPF)
- **Seguridad**: Protocolos de acceso restringido, configuración SSH en routers, firewalls
- **Infraestructura de servidores**: Servidor FTP en la sede central para almacenamiento y acceso seguro a archivos compartidos
- **Autenticación**: Sistemas de control de acceso en puntos de conexión

Plazo de Ejecución

- 6 meses totales, divididos en fases de:
    - Diseño
    - Desarrollo
    - Implementación
    - Pruebas

ANÁLISIS

Actualmente, la red de TecmiCorp enfrenta diversas limitaciones que afectan su rendimiento y seguridad:

1. *Alta congestión en la sede principal, lo que provoca latencia y pérdida de paquetes.*
2. *Falta de segmentación de la red, lo que complica la administración y aumenta riesgos de seguridad.*
3. *Conectividad ineficiente entre sucursales y la sede principal, dificultando el acceso a los recursos compartidos.*
4. *Falta de escalabilidad en la infraestructura, impidiendo su crecimiento futuro.*

Requerimientos Técnicos:

Sede Principal: 5 equipos de escritorio, 5 laptops, 2 servidores (uno para aplicaciones y otro para almacenamiento) y 3 impresoras.

Sucursales: 1 equipo de escritorio, 3 laptops y 1 impresora por sucursal.

Conectividad: Internet de alta velocidad (fibra óptica) en la sede principal y conexiones VPN seguras para las sucursales.

Objetivos del Proyecto:

1. Implementar una infraestructura escalable que soporte el crecimiento futuro.
2. Asegurar la comunicación entre la sede central y las sucursales mediante VPN.
3. Garantizar la seguridad de la red mediante firewalls y segmentación con VLANs.
4. Mejorar el rendimiento de la red con QoS y enrutamiento dinámico.

DISEÑO

El diseño de la red se realizará utilizando Cisco Packet Tracer y se basará en las mejores prácticas de networking. Los componentes principales incluyen:

Topología de Red:

Sede Principal:

- 1 router central (Cisco ISR 4000 Series).

- 2 switches de capa 3 (Cisco Catalyst 3650) para manejar VLANs.

- 1 firewall (Cisco ASA) para seguridad perimetral.

- Conexión a Internet mediante fibra óptica.

Sucursales:

- 1 router (Cisco ISR 1000 Series) por sucursal.

- 1 switch (Cisco Catalyst 2960) por sucursal.

- Conexión VPN a la sede principal.

Asignación de Direcciones IP:

- El direccionamiento IPv4 se estructurará en subredes específicas para mejorar la gestión de tráfico:

- **VLAN 10 (Administración):** 192.168.10.0/24
- **VLAN 20 (Usuarios):** 192.168.20.0/24
- **VLAN 30 (Servidores):** 192.168.30.0/24

Medidas de Seguridad:

- Implementación de VLANs para segmentar el tráfico.

- Configuración de firewalls para filtrar tráfico no autorizado.

- Uso de VPNs para conexiones seguras entre sucursales.

DESARROLLO

El desarrollo de la red se llevará a cabo en las siguientes etapas:

1. Modelado de la Red:

- Creación de la topología en Cisco Packet Tracer.

- Configuración de dispositivos (routers, switches, firewalls).

2. Configuración de VLANs:

- Creación de VLANs para segmentar la red.

- Asignación de puertos a VLANs en los switches.

3. Configuración de Enrutamiento:

- Implementación de OSPF (Open Shortest Path First) para enrutamiento dinámico.

- Configuración de rutas estáticas para conexiones VPN.

4. Configuración de Seguridad:

- Activación de firewalls y políticas de seguridad.

- Configuración de VPNs para sucursales.

IMPLEMENTACIÓN

Para minimizar el impacto en las operaciones, la implementación se dividirá en tres fases clave:

1. Instalación de hardware: Se instalarán routers, switches y firewalls en la sede y sucursales, asegurando una conectividad física estable.

2. Configuración de dispositivos: Se definirán VLANs, enrutamiento dinámico y VPNs para garantizar una red segmentada y segura.

3. Pruebas y ajustes: Se verificarán la conectividad y seguridad mediante pruebas de ping, transferencia de archivos y evaluación de políticas de firewall.

PRUEBAS

Se realizarán pruebas exhaustivas para garantizar el correcto funcionamiento de la red:

1. **Pruebas de Conectividad:**

   - Uso del comando **ping** para verificar la comunicación entre dispositivos.

   - Verificación de conexiones VPN entre sucursales y sede principal.

2. **Pruebas de Transmisión de Datos:**

   - Uso de la herramienta Simple PDU** en Cisco Packet Tracer para simular tráfico.

   - Pruebas de transferencia de archivos entre servidores y estaciones de trabajo.

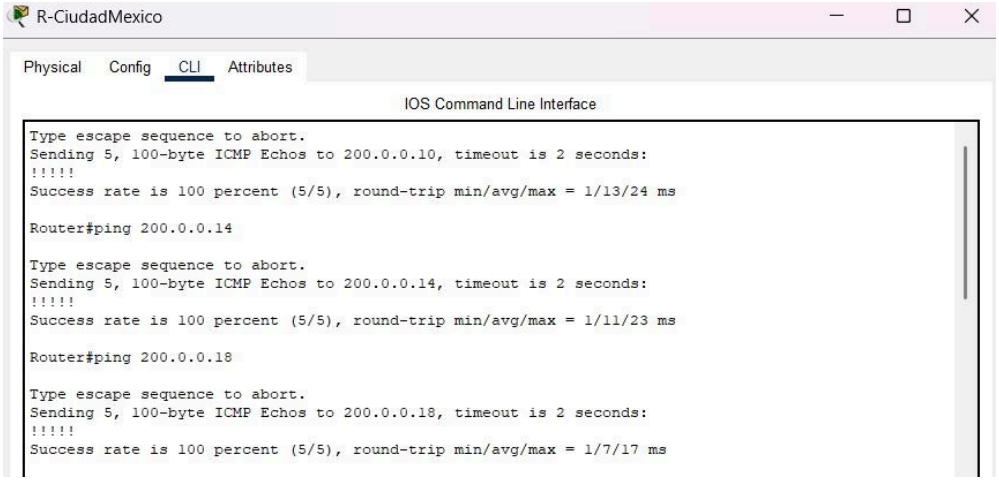
3. **Pruebas de Seguridad:**

   - Verificación de políticas de firewall.

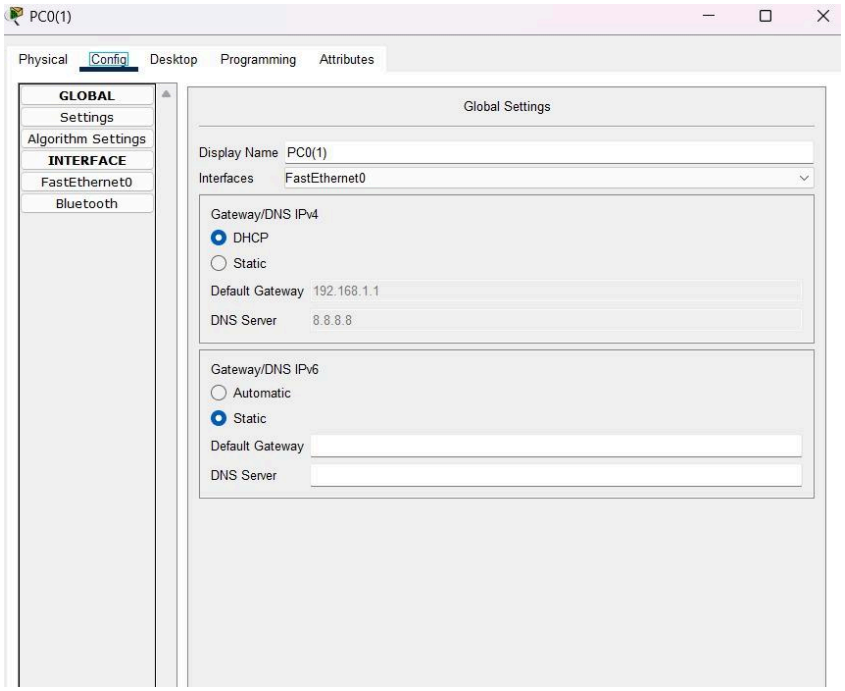
   - Pruebas de penetración para identificar vulnerabilidades.

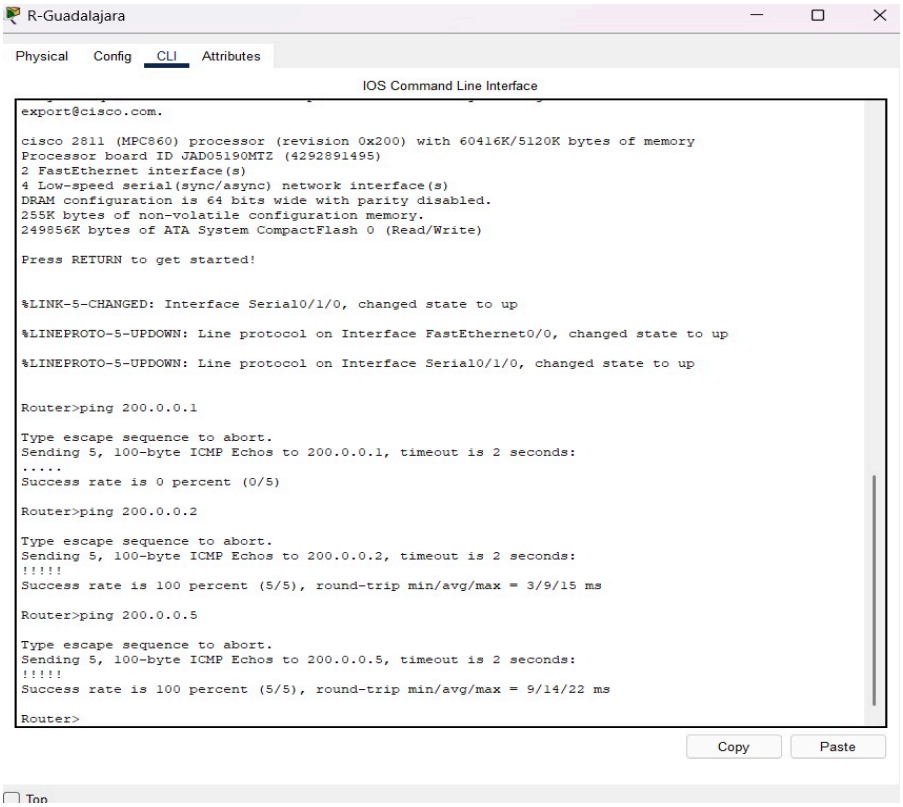
4. **Corrección de Incidencias:**

   - Solución de problemas detectados en la conectividad o seguridad.



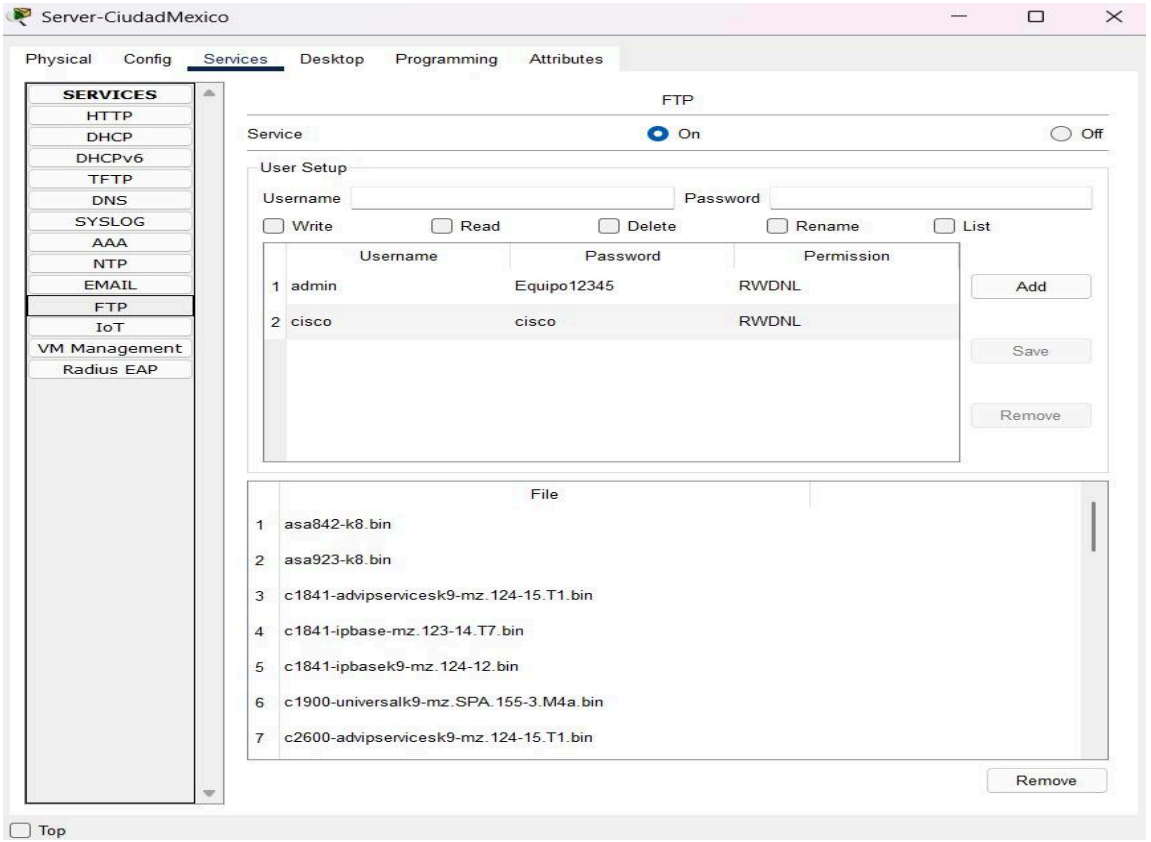
Prueba de son DHCP (dinámicas)





Ping del servidor

Respuesta del router de Guadalajara si responde a las demás sucursales


Server-CiudadMexico
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
FTP
Service
On
Off
User Setup
Username
Password
Write
Read
Delete
Rename
List
Username
Password
Permission
1 admin Equipo12345 RWDNL
2 cisco cisco RWDNL
Add
Save
Remove
File
1 asa842-k8.bin
2 asa923-k8.bin
3 c1841-advipservicesk9-mz.124-15.T1.bin
4 c1841-ipbase-mz.123-14.T7.bin
5 c1841-ipbasek9-mz.124-12.bin
6 c1900-universalk9-mz.SPA.155-3.M4a.bin
7 c2600-advipservicesk9-mz.124-15.T1.bin
Remove
Top

Seguridad en la Infraestructura de Red

La seguridad es un aspecto crítico en la infraestructura de red de TecmiCorp, ya que protege los datos, dispositivos y comunicaciones frente a amenazas internas y externas. Para garantizar un entorno seguro, se identificaron riesgos potenciales y se implementaron estrategias de mitigación adecuadas.

Identificación de Amenazas Comunes

Las principales amenazas que pueden afectar la red de TecmiCorp incluyen:

- **Phishing:** Correos electrónicos fraudulentos diseñados para engañar a los empleados y obtener credenciales de acceso.
- **Ataques de denegación de servicio (DDoS):** Sobrecarga de la red con tráfico falso, afectando la disponibilidad de los servicios.
- **Malware y ransomware:** Software malicioso que puede infectar los sistemas, comprometiendo datos o bloqueando su acceso hasta el pago de un rescate.
- **Intrusiones no autorizadas:** Accesos indebidos a la red mediante vulnerabilidades en los dispositivos o credenciales robadas.
- **Amenazas internas:** Usuarios internos con acceso indebido a información sensible o que pueden generar fallos en la seguridad, intencionalmente o por error.

Estrategias de Seguridad Implementadas

Para mitigar estas amenazas, se han implementado diversas medidas de seguridad en la red:

Firewall y Control de Acceso

Se configuró un firewall perimetral para filtrar el tráfico de red y bloquear accesos no autorizados. Además, se aplicaron listas de control de acceso (ACLs) en los switches y routers para restringir la comunicación entre dispositivos según su función en la red.

Segmentación de Red con VLANs

Para reducir la superficie de ataque y mejorar la gestión de la seguridad, se implementaron VLANs que separan los diferentes tipos de tráfico:

- **VLAN 10 (Administración):** Acceso restringido solo a personal autorizado.
- **VLAN 20 (Usuarios):** Aislamiento del tráfico de usuarios generales.
- **VLAN 30 (Servidores):** Protección adicional para los datos críticos de la empresa.

Protección contra Phishing y Malware

Se implementó un sistema de filtrado de contenido en el firewall y en los servidores DNS para bloquear sitios web sospechosos. Además, se configuró un antivirus empresarial con actualizaciones automáticas para detectar y eliminar malware.

Seguridad en la Comunicación (VPNs y Cifrado)

Para proteger la comunicación entre la sede principal y las sucursales, se establecieron túneles VPN con cifrado AES-256, asegurando que la información transmitida no pueda ser interceptada por terceros.

Monitoreo y Detección de Intrusos

Se implementó un sistema de detección de intrusos (IDS) que analiza el tráfico de red en busca de comportamientos anómalos o intentos de intrusión. Adicionalmente, se configuraron registros de eventos (logs) para auditar accesos y detectar posibles vulnerabilidades.

Políticas de Seguridad y Buenas Prácticas

Además de las medidas técnicas, se establecieron políticas de seguridad para reducir los riesgos asociados al factor humano:

1. **Capacitación del personal:** Se instruyó a los empleados en reconocimiento de amenazas, como phishing y manipulación social.
2. **Gestión de contraseñas:** Se implementó una política de contraseñas seguras con autenticación multifactor (MFA).
3. **Accesos con privilegios mínimos:** Se restringió el acceso a información sensible solo a usuarios que lo requieran para su función laboral.
4. **Copias de seguridad regulares:** Se configuraron respaldos automatizados en servidores internos y almacenamiento en la nube con cifrado.

Resultados y Beneficios Obtenidos

Con la implementación de estas estrategias, TecmiCorp ha logrado:

Mayor protección ante amenazas cibernéticas, reduciendo el riesgo de accesos no autorizados y malware.
Mejora en la segmentación de la red, limitando la propagación de ataques internos.
Comunicación segura entre sucursales, gracias al uso de VPNs con cifrado.
Mayor conciencia y preparación del personal, disminuyendo la vulnerabilidad a ataques de ingeniería social.

Análisis Detallado de Vulnerabilidades

Vulnerabilidades Específicas: Además de las amenazas comunes (phishing, DDoS, malware), identifica vulnerabilidades específicas de la infraestructura de TecmiCorp, como posibles puntos débiles en la configuración de VLANs, firewalls o VPNs.

Análisis de Riesgos: Evalúa el impacto potencial de cada vulnerabilidad en la confidencialidad, integridad y disponibilidad de los datos y servicios de la empresa.

Mitigación con Soluciones Propuestas: Explica cómo cada medida de seguridad implementada (firewalls, VLANs, VPNs, IDS) mitiga las vulnerabilidades identificadas.

RESULTADOS DE LAS PRUEBAS

Las pruebas realizadas confirmaron que la nueva infraestructura de red cumple con los objetivos de seguridad, rendimiento y escalabilidad:

- **Conectividad:** Se logró una comunicación fluida entre la sede principal y las sucursales.
- **Rendimiento:** Se redujo la latencia y se optimizó el uso del ancho de banda.
- **Seguridad:** Los firewalls y VPNs aseguran la protección de la información.
- **Escalabilidad:** La red está preparada para el crecimiento futuro de TecmiCorp.

Demostración de la Robustez de la Seguridad:

- **Métricas de Seguridad**: Utiliza métricas para demostrar la efectividad de las medidas de seguridad implementadas, como la reducción en el número de intentos de intrusión o la mejora en el tiempo de respuesta ante incidentes de seguridad.
- **Escenarios de Ataque y Defensa**: Describe escenarios específicos de ataques simulados y cómo la red respondió a ellos, demostrando la capacidad de la infraestructura para proteger los activos de la empresa.

Impacto en el Negocio

- **Eficiencia Operativa:** Detalla cómo la reducción de la latencia y el aumento del ancho de banda mejoran la velocidad de las operaciones diarias.
- **Productividad**: Explica cómo la conectividad confiable y segura facilita la colaboración y el acceso a recursos críticos, aumentando la productividad de los empleados.
- **Reducción del Tiempo de Inactividad**: Cuantifica cómo la redundancia y la alta disponibilidad de la nueva red minimizan las interrupciones del servicio.
- **Velocidad de Transferencia de Datos**: Muestra cómo la optimización de la red acelera la transferencia de archivos y el acceso a aplicaciones, mejorando la eficiencia general.

Gestión de la Red

- **Monitoreo del Rendimiento**: Describe las herramientas (por ejemplo, Cisco Prime Infrastructure, SolarWinds) y los procesos para supervisar el rendimiento de la red, detectar cuellos de botella y garantizar la calidad del servicio (QoS).
- **Detección y Resolución de Problemas**: Explica cómo se utilizarán los sistemas de detección de intrusiones (IDS) y los registros de eventos (logs) para identificar y resolver problemas de seguridad y conectividad.
- **Actualizaciones y Mantenimiento**: Detalla el proceso para realizar actualizaciones de software, aplicar parches de seguridad y mantener la infraestructura al día con las últimas tecnologías y mejores prácticas.
- **Gestión de la Seguridad**: Describe cómo se gestionan los firewalls, las VPNs y otros dispositivos de seguridad para proteger la red contra amenazas internas y externas.
- **Capacitación del Personal**: Menciona la importancia de capacitar al personal de TI en la gestión y el mantenimiento de la nueva infraestructura.

TOPOLOGÍA DE RED DE TECMICORP

Se implementa una topología jerárquica para mejorar el rendimiento, la escalabilidad y la seguridad de la red de TecmiCorp.

Dispositivos conectados:

- 5 equipos de escritorio.
- 5 laptops.
- 2 servidores (uno de aplicaciones y otro de almacenamiento).
- 3 Impresoras.

- **Sucursales (Guadalajara, Monterrey, Puebla, Queretaro, Cancun)**
  - 1 router (Cisco ISR 1000 series) por sucursal.
  - 1 switch (Cisco Catalyst 2960) por sucursal.
  - Conexión VPN con la sede principal.

Dispositivos conectados:

- 1 equipo de escritorio.
- 3 laptops.
- 1 Impresora.

Esquema de Direccionamiento IP

- **VLAN 10 (Administración)-** 192.168.10.0/24
- **VLAN 20 (Usuarios)-** 192.168.20.0/24
- **VLAN 30 (Servidores)-** 192.168.30.0/24

Beneficio de la red:

1.Escabilidad

-La infraestructura soportará el crecimiento futuro de la empresa sin afectar el rendimiento.

2.Segmentación y Seguridad

-Uso de VLANs para dividir la red y mejorar la seguridad.

-Configuración de firewalls para protección contra amenazas.

3.Conectividad Eficiente

-OSPF permite el enrutamiento dinámico, optimizando el tráfico.

-VPNs seguras para facilitar la comunicación entre sedes y sucursales.

4.Mejor Rendimiento

-Implementación de QoS para priorizar tráfico crítico.

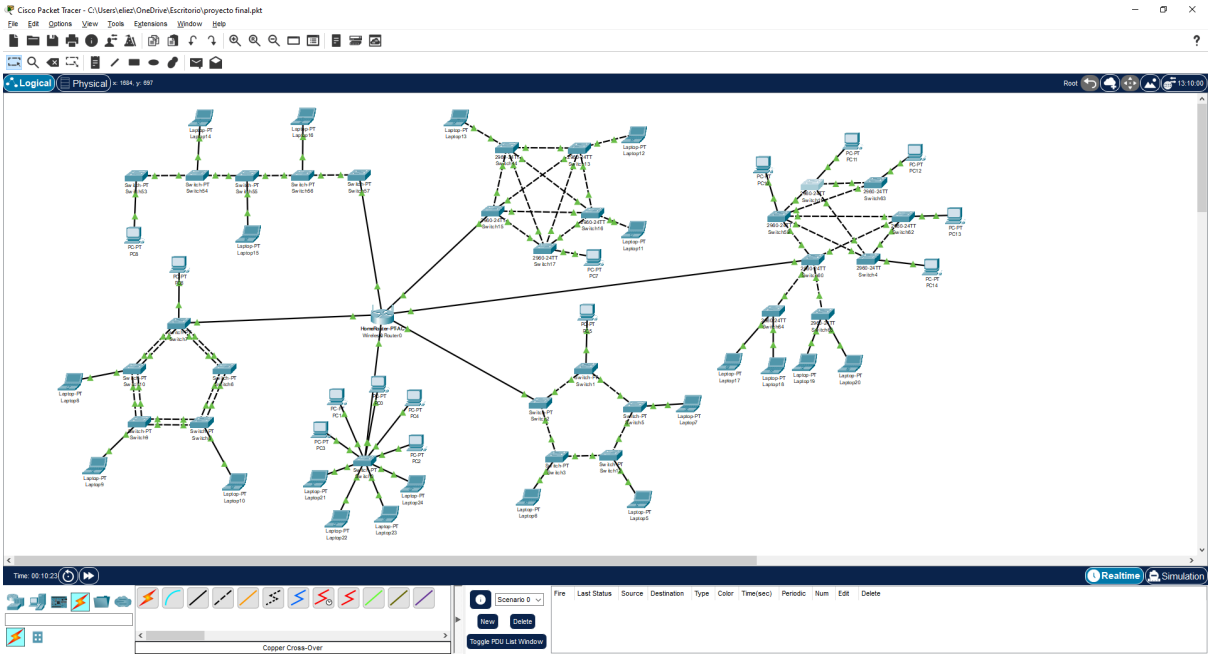
-Reducción de latencia y congestión con switches de capa 3.

5.Redundancia y Alta Disponibilidad

-Equipos y conexiones distribuidos estratégicamente para minimizar fallos.

Topologías usadas

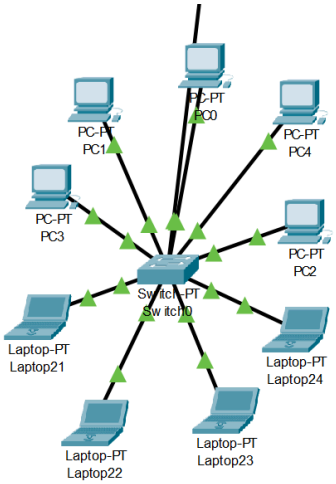
Topología Completa:



En la red de TecmiCorp, se ha implementado una combinación de diferentes topologías de red en cada sucursal, optimizando el rendimiento, la escalabilidad y la tolerancia a fallos según las necesidades de cada ubicación.

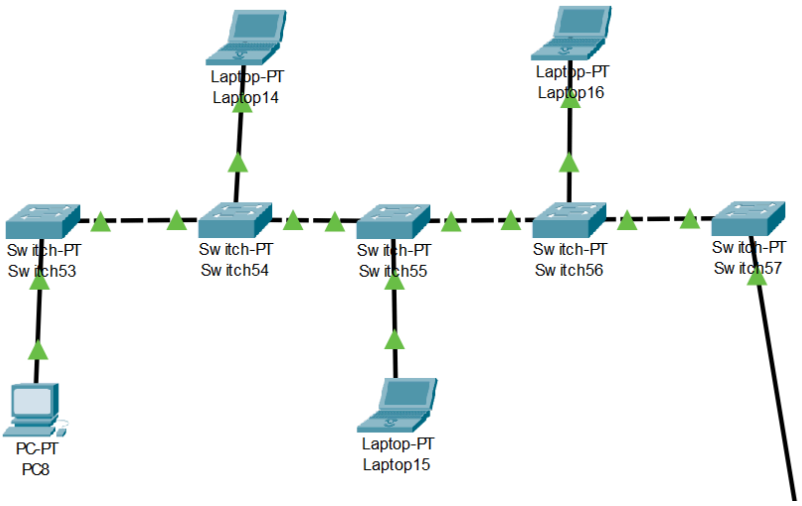
Sede Principal (NETCREW-CDMX) → Topología en Estrella

La matriz utiliza una topología en estrella, donde un switch central administra la comunicación entre los dispositivos. Esta estructura permite un fácil mantenimiento y escalabilidad, además de minimizar la posibilidad de colisiones en la red.



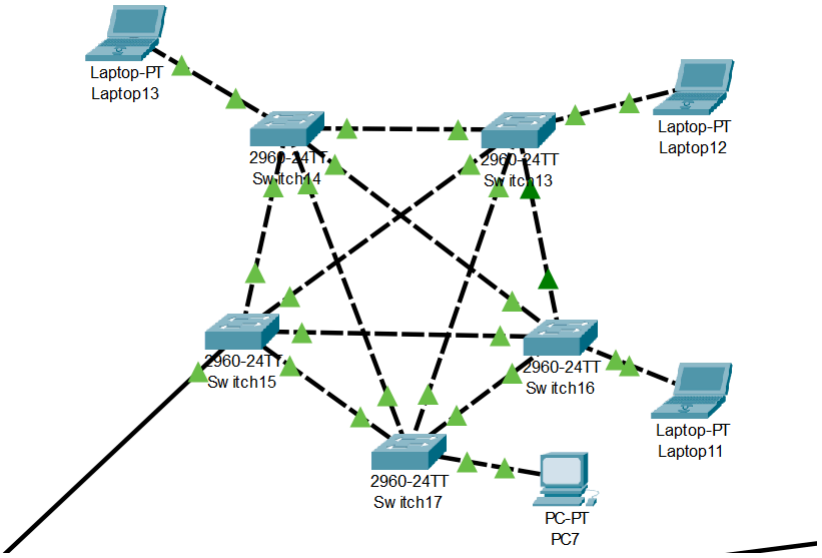
Sucursal 1 (NETCREW-GDL) → Topología en Bus

La Sucursal 1 está organizada en una topología en bus, donde todos los dispositivos están conectados a un único medio de transmisión. Este diseño es eficiente en costos y sencillo de implementar, aunque presenta limitaciones en términos de escalabilidad y tolerancia a fallos.



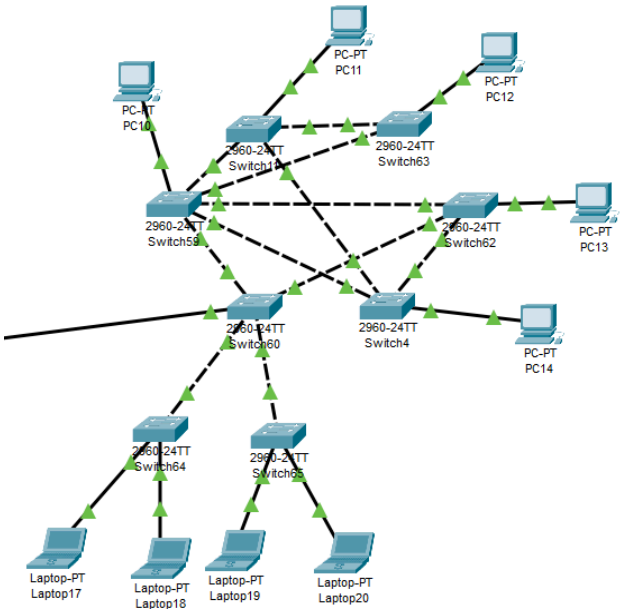
Sucursal 2 (NETCREW-MTY) → Topología Totalmente Conexa

En la Sucursal 2, se ha implementado una topología totalmente conexa, donde cada dispositivo está directamente conectado con los demás. Este enfoque proporciona la máxima redundancia y confiabilidad, reduciendo la posibilidad de puntos únicos de falla, aunque requiere una mayor inversión en infraestructura.



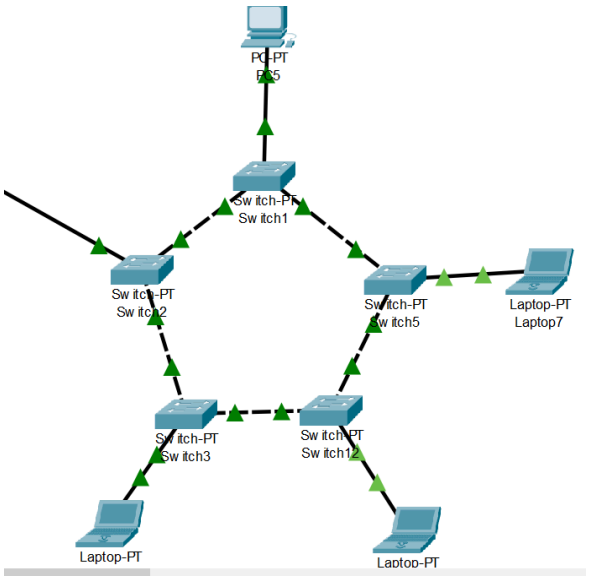
Sucursal 3 (NETCREW-PUE) → Topología Híbrida (Malla y Árbol)

La Sucursal 3 cuenta con una combinación de topologías de malla y árbol. La topología de malla proporciona rutas alternativas para mejorar la tolerancia a fallos, mientras que la estructura jerárquica del árbol optimiza la administración y segmentación de la red.



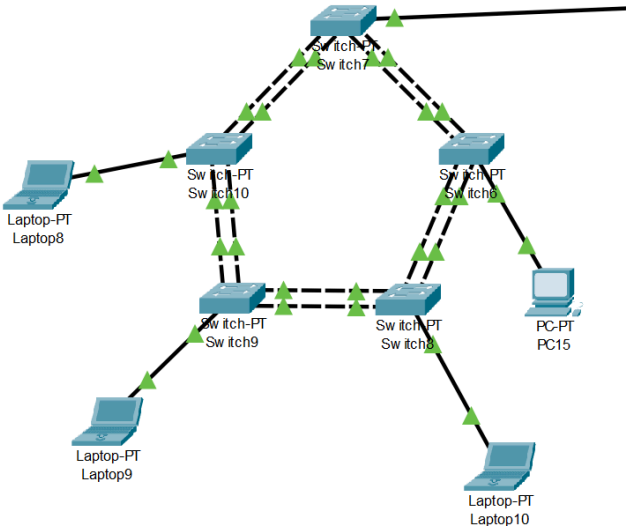
Sucursal 4 (NETCREW-QRO) → Topología en Anillo

En la Sucursal 4, los dispositivos están conectados en un anillo, donde los datos viajan en una sola dirección hasta alcanzar su destino. Esta topología permite una transmisión de datos eficiente, aunque su principal desventaja es que una sola falla puede afectar toda la comunicación.



Sucursal 5 (NETCREW-CUN) → Topología en Doble Anillo

Para aumentar la tolerancia a fallos, la Sucursal 5 emplea una topología en doble anillo, lo que proporciona redundancia adicional. Si un enlace falla, la comunicación puede continuar por el anillo secundario, asegurando una mayor disponibilidad de la red.



BIBLIOGRAFÍA

- CCNA: Introduction to networks (no date) Cisco Networking Academy: Learn Cybersecurity, Python & More. Available at: https://www.netacad.com/courses/ccna-introduction-networks (Accessed: 25 February 2025).

- *Computer Networks, 6th Edition* (no date) *Computer Networks*. Available at: https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188/9780137523214 (Accessed: 25 February 2025).

- *Data and Computer Communications* (no date) *Goodreads*. Available at: https://www.goodreads.com/book/show/299634.Data_and_Computer_Communications (Accessed: 25 February 2025).

- *Cisco Secure Firewall ASA* (2022) *Cisco*. Available at: https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/series.html (Accessed: 25 February 2025).

CONCLUSIONES Y/O AGRADECIMIENTOS

La actualización de la infraestructura de red de TecmiCorp representa un avance significativo en términos de eficiencia, seguridad y escalabilidad. La segmentación con VLANs, la implementación de QoS y el uso de VPNs han optimizado el rendimiento de la red, garantizando una conectividad confiable entre la sede principal y sus sucursales. Este proyecto no solo resuelve los desafíos actuales, sino que también establece una base sólida para el crecimiento y evolución futura de la empresa.

Agradecemos a todo el equipo de TecmiCorp por su compromiso y colaboración en la implementación de este proyecto. Extendemos nuestro reconocimiento a los especialistas en redes y tecnología, cuyo conocimiento y apoyo fueron clave para el desarrollo de una infraestructura robusta y eficiente. Finalmente, expresamos nuestra gratitud a nuestros compañeros y profesoras, cuyo asesoramiento y dedicación fueron fundamentales para el éxito de este trabajo.

AUTORES

Hector David Ortega Garcia

Erick Mauricio Santiago Díaz

Andres Jair Abarca Ulloa

Emilia Isabel Garcia Karo

Eliezer de la Cruz Peña

Alejandro Roman Ramirez

VIDEO DEMOSTRATIVO DE LA RED

Link del video: https://youtu.be/C8KmyMmPGZw