UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

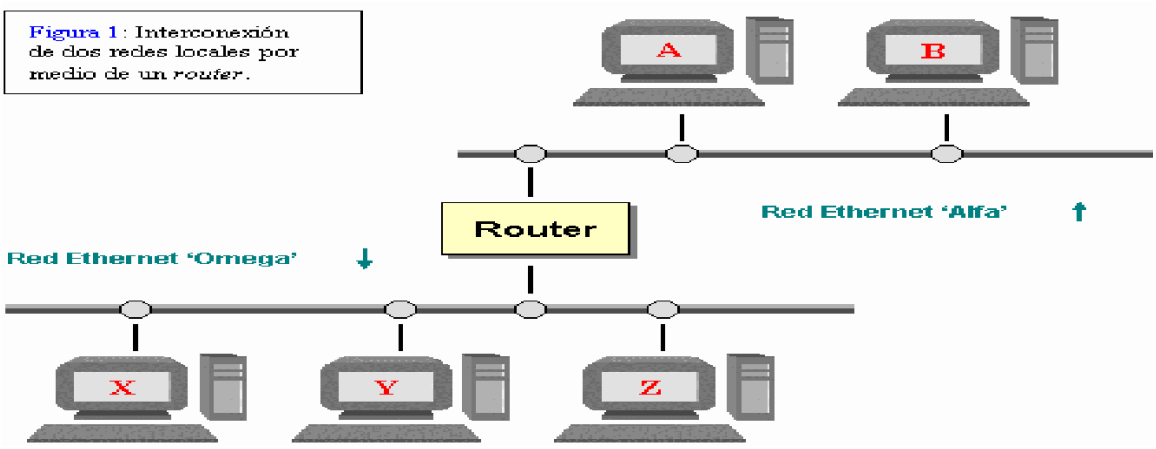
Centro de e-Learning
Secretaría de Cultura y Extensión Universitaria

Trabajo Final Modulo 2

Curso: Experto Universitario en Seguridad de la Información

Alumno: Rodrigo Vila

Ejercicio 1: Del gráfico expuesto, deducir y exponer 3 problemas en esta topología, y que aplicarían para mitigar o solucionar los mismos.:



Problemas potenciales en esta topología:

1 - Cuello de botella en el router:

Descripción: El router es el único punto de conexión entre las redes 'Alfa' y 'Omega'. Todo el tráfico que fluye entre las dos redes debe pasar por el router. Si hay un aumento significativo en el tráfico de red, el router puede convertirse en un cuello de botella, lo que puede provocar lentitud, congestión y pérdida de paquetes.

Solución: Implementar un balanceo de carga de red para distribuir el tráfico entre varios routers o enlaces. Esto puede ayudar a reducir la carga en un solo router y mejorar el rendimiento general de la red.

2 - Falta de redundancia:

Descripción: Si el router falla, las redes 'Alfa' y 'Omega' se aislarán entre sí. Esto puede provocar interrupciones del servicio y pérdida de conectividad entre los dispositivos de las dos redes.

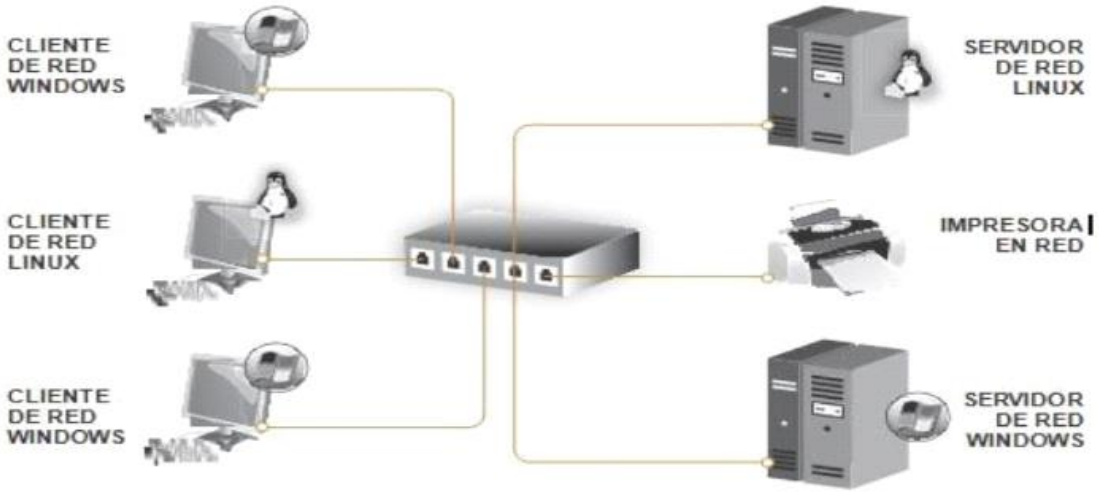
Solución: Implementar redundancia en la red mediante la instalación de un router secundario o la configuración de rutas alternativas. Esto puede ayudar a garantizar la disponibilidad de la red en caso de que falle un componente crítico.

3 - Falta de seguridad:

Descripción: La topología de la imagen no muestra ningún elemento de seguridad visible, como firewalls o sistemas de detección de intrusiones. Esto hace que la red sea vulnerable a ataques y intrusiones.

Solución: Implementar medidas de seguridad adecuadas, como firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones. Estas medidas pueden ayudar a proteger la red de accesos no autorizados, malware y otras amenazas.

Ejercicio 2: Usted pertenece al área de soporte y se encuentra con este escenario, explicar los pasos a seguir que piensa que son necesarios para que la red funcione adecuadamente, esto significa que cambiaría o agregaría en cuanto a lo enseñado.



Para asegurar que la red funcione adecuadamente, seguiría los siguientes pasos:

En primer lugar lo que observo es que tanto el Servidor Linux, como el Servidor Windows están utilizando el mismo puerto del Switch. Si bien en clase vimos algo

referido a utilizar distintos dispositivos a un mismo puerto, no lo veo como algo recomendable y es algo que en mi práctica cambiaría para evitar posibles problemas como por ejemplo: congestion del tráfico de red, entre otros.

Tomando como premisa no expandir excesivamente la red para que quede lo mas parecida al ejemplo posible, lo primero que haria es reemplazar el switch por uno con mayor cantidad de puertos. Asi poder dedicar un puerto por cada dispositivo y tener la opcion de expandir la red.

Evaluaria seriamente modificar la topologia añadiendo Firewalls, IPS, HIDS, etc. de ser posible y mejorar la redundancia de la red, pero sigamos apegandonos al ejemplo.

Como principios:

- Asignar direcciones IP estáticas o configurar un servidor DHCP: Me aseguraria de que cada dispositivo tenga una dirección IP única dentro del mismo rango de red. Podria asignar direcciones IP estáticas a cada dispositivo o configurar un servidor DHCP para asignar direcciones IP automáticamente.

- Configurar una puerta de enlace predeterminada: Asegurarme de que todos los dispositivos estén configurados con la dirección IP del router como su puerta de enlace predeterminada. Esto permite que los dispositivos se comuniquen entre sí.

- Configurar correctamente las máscaras de subred: Asegurarme de que todos los dispositivos estén configurados con la misma máscara de subred para que puedan comunicarse correctamente dentro de la red.

- En cuestiones de seguridad, dado que la red posee servidores, evaluaria la posibilidad de incorporar dispositivos de seguridad como por ejemplo: Firewalls, IPS, NIDs, HIDs.

- Configurar reglas de firewall: Como hay dispositivos que necesitan comunicarse a través de la red externa, (por ejemplo los servidores) hay que asegurarse de configurar las reglas de firewall adecuadas para permitir el tráfico necesario y seguro.

- Comprobar la conectividad entre los dispositivos: Después de configurar las direcciones IP, las máscaras de subred y la puerta de enlace predeterminada, realizar pruebas de conectividad entre todos los dispositivos para asegurarse de que puedan comunicarse entre sí correctamente.

- Configurar el acceso a recursos compartidos: Sobre los recursos compartidos en los servidores, como archivos o impresoras, asegurarse de configurar los permisos adecuados para que los clientes de red puedan acceder a ellos según sea necesario.

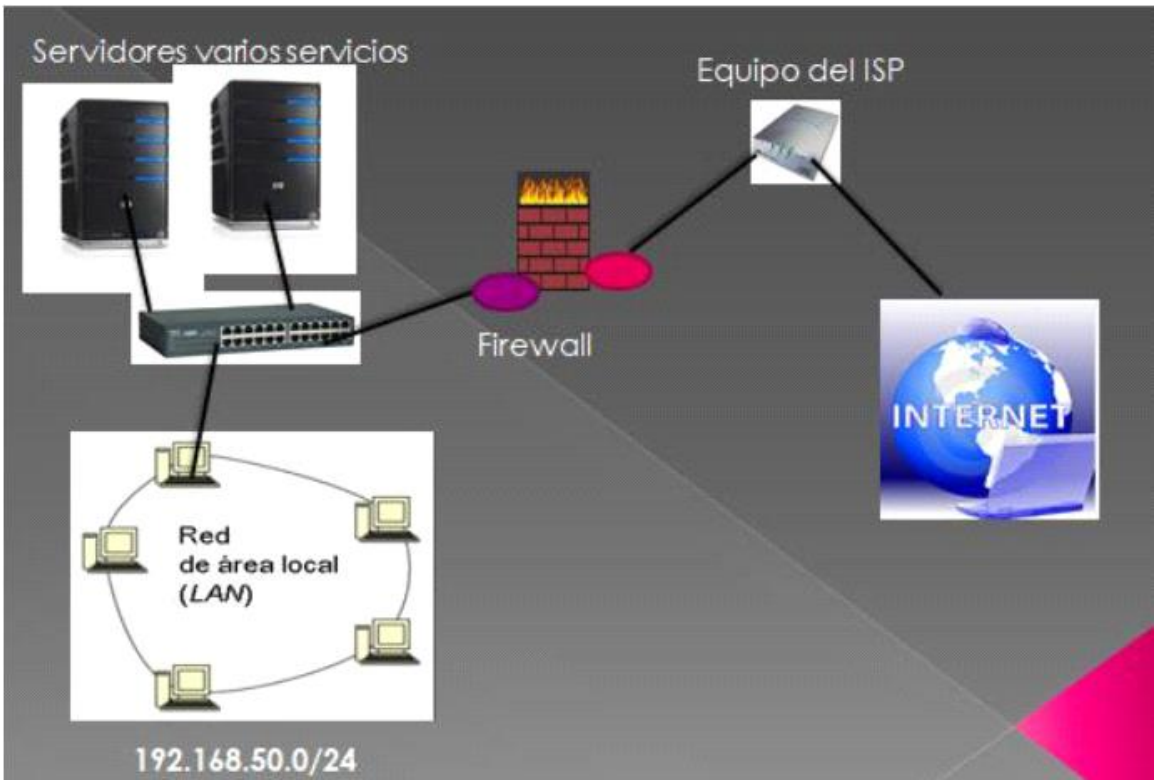
- Configurar la impresora en los dispositivos cliente: Asegurarse de instalar y configurar los drivers necesarios y la configuracion correcta de la conexion con

la impresora para que los clientes puedan enviar trabajos de impresión a través de la red.

- Implementar medidas de seguridad: Trataria de implementar medidas de seguridad adecuadas, como contraseñas fuertes, filtrado de direcciones MAC, actualizaciones de firmware regulares y encriptación de datos para proteger la red contra accesos no autorizados y ataques.

- Aislar los servidores en una Vlan también podria ser una buena práctica.

Ejercicio 3: De acuerdo a lo que vemos, que podríamos agregar para mejorar esta red, puede ser aspectos físicos como nuevo hardware o lógicos como servicios de Vlan.



Supondré que es una red de una pequeña oficina de una PYME, siendo ésta la única sucursal y no necesitando acceso a los servidores desde el exterior.

Para mejorar esta red agregaria:

- Un IPS atras del equipo del ISP para prevenir actividad maliciosa.

- Dividiría el Router L3 en 2 VLANs, una para los servidores y otra para la red LAN de PCs.

- Agregaria un IDS conectado al Switch L3 para monitorear intentos de acceso no

autorizado.

- Agregaria enlaces redundantes entre el Firewall y el Switch L3 para garantizar la disponibilidad en caso de fallos.
- Configuraría una ACL en el switch L3 para garantizar que se bloquee todo tráfico que no venga de los equipos clientes de la red LAN hacia los servidores.
- Agregaria un servidor de Back Up para respaldar los datos de los servidores.
- Agregaria un UPS para prolongar la conexion en caso de cortes de energia.

Esta red podría expandirse de manera infinita, por eso elegí no salirme tanto de la estructura presentada originalmente y presentar una propuesta de mejoramiento no tan extensa ni tan costosa.

También, al no extender tanto los cableríos o redundancias, al ser una red pequeña, facilitaría las tareas del administrador de red en su monitoreo e identificación de fallos.

Eso si, suponiendo que el rol del administrador de red se encuentra cubierto en todo momento.

Beneficios de una red simple en comparación de redes mas complejas:

- Facilidad de gestión: Una red simple es más fácil de configurar, mantener y gestionar. Con menos dispositivos, menos configuraciones y menos componentes, es más sencillo para los administradores de red supervisar y solucionar problemas.
- Costos reducidos: Al tener menos dispositivos y componentes, una red simple tiende a ser más económica en términos de hardware, software y tiempo empleado en la configuración y mantenimiento.
- Menor complejidad: Con menos nodos y menos conexiones, la red es menos propensa a problemas de compatibilidad, conflictos de configuración y otros desafíos asociados con la complejidad.
- Mayor velocidad y eficiencia: Al tener menos dispositivos intermedios, como switches y routers, los datos pueden fluir más rápidamente a través de la red, lo que resulta en una mejor velocidad y eficiencia de la red.
- Facilidad de expansión: Aunque una red simple puede tener menos capacidades avanzadas, es más fácil de escalar y expandir según las necesidades cambiantes de la organización. Agregar nuevos dispositivos y ampliar la red es más sencillo cuando la infraestructura es simple.

- Menos puntos de fallo: Con menos componentes, hay menos puntos potenciales de fallo en la red. Esto puede hacer que la red sea más confiable y fácil de diagnosticar en caso de problemas.

En resumen, una red simple puede ser una excelente opción para organizaciones que no necesitan una infraestructura de red compleja y que valoran la facilidad de gestión, la confiabilidad y la eficiencia. Sin embargo, es importante equilibrar la simplicidad con la capacidad de satisfacer las necesidades operativas y de seguridad de la organización.

Bibliografía:

- Revisión de las Unidades presentadas en el Módulo 1 y 2 de ésta cursada.
- Algunos textos e ideas desarrolladas fueron pulidas con diferentes herramientas de inteligencia artificial. Como lo son Chat GPT y Gemini.

Rodrigo Vila.-