OZonE
CIBERSECURITY

TOPOLOGIAS DE RED Y CIBERSEGURIDAD

Ruben Apablaza Muñoz
-OZonE-

TOPOLOGÍAS DE RED

El termino se refiere a como se disponen y conectan los distintos elementos de una red informática, como lo son, dispositivos finales, cables y dispositivos/puntos de conexión.

La topología determina como fluyen los datos dentro de la red, lo que afecta directamente el rendimiento y la eficiencia. Cada una tiene sus ventajas y desventajas.

Las topologías o arquitecturas de red, deben abordar 4 características principales:

- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

"Conocer la topología de red permite identificar vulnerabilidades, planificar defensas, responder a incidentes y diseñar infraestructuras seguras."

TOPOLOGÍA EN ESTRELLA

Es el **tipo de configuración más común**. La red está organizada de modo que los **nodos estén conectados a un dispositivo central**. El switch gestiona la transmisión de datos a través de la red. Es decir, cualquier dato enviado a través de la red viaja a través del dispositivo central antes de terminar en su destino.

Ventajas:

- Gestión conveniente desde una ubicación central.
- Si un nodo o cable falla, no afecta a toda la red.
- Los dispositivos se pueden agregar o apartar sin interrumpir la red.
- Más fácil de administrar identificar y aislar los problemas de rendimiento.

Desventajas:

- Si el dispositivo central falla, toda su red dejará de funcionar.
- El rendimiento y el ancho de banda están limitados por el nodo central.

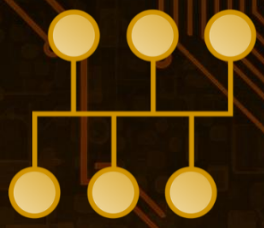
Uso común:

- Oficinas, hogares, pequeñas y medianas empresas.

Ejemplo de uso en ciberseguridad:

- *Red de una pequeña empresa con segmentación y monitoreo central.*
  ¿Por qué?: Permite aplicar un firewall o IDS/IPS en el switch central para inspeccionar todo el tráfico entrante y saliente. Ideal para control de acceso.

TOPOLOGÍA EN BUS



Los dispositivos están conectados a lo largo de un solo cable central que se extiende desde un extremo de la red hasta el otro. Los datos fluirán a lo largo del cable a medida que viaja a su destino.

Ventajas:

- Económico para redes más pequeñas.
- Diseño simple; todos los dispositivos conectados a través de un cable.
- Se pueden agregar más nodos alargando la línea.

Desventajas:

- Una falla en el cable central afecta toda la red.
- Cada nodo agregado disminuye la velocidad de transmisión.
- Difícil de diagnosticar fallos.
- Los datos solo se pueden enviar en una dirección a la vez.

Uso común:

- Redes pequeñas y temporales.

Ejemplo de uso en ciberseguridad:

- *Laboratorios de pruebas de malware o análisis forense.*
  ¿Por qué?: Fácil y barato de montar, ideal para ambientes controlados donde se quiere estudiar cómo se propaga un ataque por un solo canal de comunicación.

TOPOLOGÍA EN ANILLO

Cada dispositivo se conecta con otros dos formando un patrón circular. Los datos viajan a través de cada dispositivo a medida que viajan a través del anillo. En una red grande, es posible que se necesiten repetidores para evitar la pérdida de paquetes durante la transmisión. Las topologías de anillo se pueden configurar como anillo único (half-dúplex) o anillo doble (full-dúplex) para permitir que el tráfico fluya en ambas direcciones simultáneamente.

Ventajas:

- Buen rendimiento con poco tráfico.
- Problemas de rendimiento fáciles de identificar.

Desventajas:

- Una falla puede afectar toda la red.
- Todos los dispositivos comparten ancho de banda, lo que puede limitar el rendimiento de transferencias.
- Agregar o eliminar nodos significa tiempo de inactividad para toda la red.

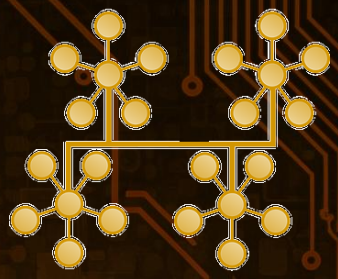
Uso común:

- Algunas redes industriales o sistemas heredados.

Ejemplo de uso en ciberseguridad:

- *Sistemas SCADA o redes industriales antiguas.*
  ¿Por qué?: Aunque en desuso, aún se encuentra en entornos donde el tráfico sigue rutas fijas. Los profesionales de ciberseguridad deben entender cómo asegurar estos entornos legacy.

TOPOLOGÍA EN ÁRBOL



Es una **combinación de topología estrella en estructura jerárquica** (ramificada). El eje central es como el tronco del árbol. Donde las ramas se conectan son los concentradores secundarios o los nodos de control y luego los dispositivos conectados se conectan a los branches.

Ventajas:

- Extremadamente flexible y escalable.
- Facilidad para identificar errores, ya que cada branch de la red puede diagnosticarse individualmente.

Desventajas:

- Si falla un nodo central, los nodos se desconectarán (aunque las ramas pueden seguir funcionando de forma independiente).
- La estructura puede ser difícil de gestionar de forma eficaz.
- Cableado complejo.

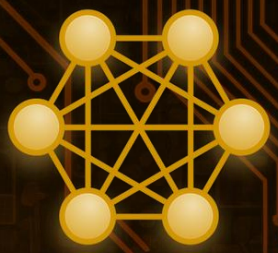
Uso común:

- Ideal para dividir redes grandes en subredes o departamentos.

Ejemplo de uso en ciberseguridad:

- *Universidades o empresas grandes con estructura jerárquica.*
  ¿Por qué?: Puedes aplicar políticas de seguridad por niveles o departamentos. Facilita el control de acceso basado en roles (RBAC) y segmentación lógica.

TOPOLOGÍA DE MALLA



En el modo full-mesh, **cada dispositivo está conectado a TODOS los demás**. En una topología de malla parcial, la mayoría de los dispositivos se conectan directamente. Esto proporciona múltiples rutas para la entrega de datos. Los datos se envían a la distancia más corta disponible para la transmisión.

Ventajas:

- Alta redundancia y tolerancia a fallos.
- Ningún fallo de un solo nodo desconecta la red.

Desventajas:

- Grado complejo de interconectividad entre nodos.
- Mano de obra intensiva para instalar.
- Utiliza mucho cableado para conectar todos los dispositivos.
- Muy costosa.

Uso común:

- Centros de datos, redes críticas (militares, bancarias).

Ejemplo de uso en ciberseguridad:

- *Centros de datos o infraestructura crítica (como banca o defensa).*
  ¿Por qué?: Alta disponibilidad. Ideal para aplicar control de tráfico interno, microsegmentación, y protección contra *"lateral movement"* en ataques avanzados.

TOPOLOGÍA HÍBRIDA

Utiliza varias estructuras de topología. Esto es más común en organizaciones grandes donde cada departamento puede tener un tipo de topología, como estrella o línea, con el switch del departamento conectando a un switch central.

Ventajas:

- Flexibilidad.
- Puede personalizarse según las necesidades del cliente.
-

Desventajas:

- La complejidad aumenta.
- Se requiere experiencia en múltiples topologías.
- Puede ser más difícil determinar los problemas de rendimiento.

Uso común:

- Grandes empresas, redes escalables.

Ejemplo de uso en ciberseguridad:

- *Red corporativa moderna con múltiples sucursales y servicios en la nube.*

  ¿Por qué?: Mezcla lo mejor de cada topología. El equipo de ciberseguridad puede usar firewalls distribuidos, redes definidas por software (SDN) y Zero Trust para asegurar distintos segmentos.

CONCLUSIÓN

Entonces ***¿para qué le sirve conocer las topologías de red a un estudiante o profesional de ciberseguridad?***

La topología no es solo una estructura física o lógica**,** también es una **guía táctica y estratégica** para proteger, analizar y fortalecer una red. Conocer las topologías de red**,** es fundamental para un estudiante o profesional de ciberseguridad por las siguientes razones:

1. Entender la superficie de ataque

- Cada topología presenta diferentes **puntos vulnerables**.
  - En **estrella**, el switch central es crítico.
  - En **malla**, hay más redundancia pero más puntos a proteger.

2. Diseño de defensas eficientes

- Ayuda a decidir dónde colocar firewalls, IDS/IPS, segmentaciones VLAN, WAF, etc.
- Ejemplo: En una red en árbol, puedes aplicar seguridad por niveles jerárquicos.

3. Análisis y respuesta a incidentes

- Permite **rastrear** más rápido el origen de un ataque o anomalía.
- Saber cómo fluye el tráfico te da ventaja al investigar intrusiones o propagaciones.

4. Planificación de medidas de contingencia

- Si conoces la topología, puedes prever **puntos únicos de fallo** y aplicar medidas como balanceo, backups o enlaces redundantes.

5. Optimización del monitoreo

- Saber cómo está estructurada la red te permite ubicar mejor herramientas como:
  - SIEM
  - Honeypots
  - Sensores de tráfico

6. Mejora la comunicación con equipos de redes

- En ambientes reales, el equipo de ciberseguridad trabaja codo a codo con redes.
- Conocer topologías permite hablar el mismo idioma y proponer soluciones viables.

"Conocer la topología de red permite identificar vulnerabilidades, planificar defensas, responder a incidentes y diseñar infraestructuras seguras."

Referencias.

- Topología de Red: conozca los principales tipos https://www.internationalit.com/post/topologia-de-red-conozca-los-principales-tipos?lang=es

- ¿Qué es la topología de red? https://www.ibm.com/mx-es/topics/network-topology