9) Defina una red según su topología. Explicar distintas variantes.

La **topología de red** describe la forma en que los dispositivos (nodos) y los enlaces (cables o conexiones inalámbricas) están organizados dentro de una red. Es un concepto clave para diseñar, administrar y optimizar redes, ya que permite comprender cómo fluye la información y cómo se interconectan los equipos.

Existen diferentes **tipos de topologías de red**:

* **Punto a punto:** conexión directa entre dos dispositivos.
* **Bus:** todos los dispositivos comparten un único canal de comunicación.
* **Anillo:** los dispositivos están conectados formando un círculo cerrado; los datos viajan en una sola dirección.
* **Estrella:** cada dispositivo se conecta a un nodo central (hub o switch).
* **Árbol:** estructura jerárquica que combina varias estrellas conectadas a un nodo central superior.
* **Malla:** cada dispositivo se conecta directamente a varios otros, formando múltiples caminos posibles.
* **Híbrida:** mezcla dos o más topologías anteriores, adaptándose a necesidades específicas.

**Topología de malla**  
En esta configuración, los dispositivos se interconectan de forma descentralizada. No dependen de un concentrador central, sino que se conectan directamente entre sí, lo que permite múltiples rutas para la transmisión de datos. Esto mejora la **redundancia**, la **tolerancia a fallos** y la **escalabilidad** de la red.

Existen dos variantes principales:

* **Malla completa:** cada dispositivo está conectado directamente con todos los demás.
* **Malla parcial:** solo algunos dispositivos tienen conexiones directas entre sí; los demás se conectan a través de otros nodos. Es más económica y práctica en redes grandes.

10) Explicar el servicio de DHCP.

El Protocolo de Configuración Dinámica de Host (DHCP) es un sistema para asignar direcciones IP a cada dispositivo de red (conocido como host) en la red de una organización. Un host puede ser una computadora de escritorio, una portátil, una tableta, un dispositivo móvil, un cliente ligero u otros tipos de dispositivos. Cada host debe tener una [dirección IP](https://www.akamai.com/glossary/what-is-an-ip-address) para comunicarse con otros dispositivos a través de internet. El protocolo de red DHCP asigna direcciones automáticamente, sin necesidad de que los administradores de red las asignen manualmente. DHCP también se encarga de asignar automáticamente nuevas direcciones IP cuando los dispositivos se trasladan a nuevas ubicaciones en la red. Además de las direcciones IP, un servicio DHCP asigna parámetros de configuración como direcciones del Sistema de Nombres de Dominio (DNS), máscaras de subred y puertas de enlace predeterminadas, esenciales para las comunicaciones de red.

El protocolo DHCP permite a las organizaciones y administradores de red:

* Optimice la gestión de la red. DHCP reduce la carga de los administradores de red al gestionar de forma eficiente y automática la asignación de direcciones IP. DHCP es especialmente eficaz para dispositivos que requieren actualizaciones frecuentes, como teléfonos móviles que se mueven entre diferentes ubicaciones en una red inalámbrica.
* Optimice las direcciones IP. La posibilidad de reutilizar direcciones IP minimiza el número total de direcciones necesarias para una red.
* Simplifique la gestión de cambios. DHCP permite a las organizaciones cambiar los esquemas de direcciones IP de un rango a otro sin interrumpir a los usuarios finales.
* Minimiza los errores. DHCP centraliza y automatiza la gestión de direcciones IP, minimizando la posibilidad de que dos dispositivos reciban la misma dirección o que un dispositivo reciba una dirección incorrecta.

11- Explicar el servicio de DNS.

El **Protocolo de Configuración Dinámica de Host (DHCP, por sus siglas en inglés)** es un servicio de red que asigna de forma **automática** direcciones IP y otros parámetros de configuración a los dispositivos conectados a una red. De esta manera, los administradores no tienen que asignar manualmente direcciones IP a cada equipo.

Cada **host** (computadora, portátil, tablet, teléfono móvil, impresora, etc.) necesita una dirección IP para comunicarse en la red. El servicio DHCP no solo otorga esta dirección, sino que también puede asignar:

* **Máscara de subred**
* **Puerta de enlace predeterminada (gateway)**
* **Servidores DNS**
* Otros parámetros necesarios para la conectividad de red

**Ventajas y funciones del DHCP:**

* **Automatización y eficiencia:** simplifica la gestión de la red al asignar direcciones IP de manera dinámica y automática, especialmente útil en redes grandes o con dispositivos móviles.
* **Optimización de direcciones IP:** permite reutilizar direcciones cuando los dispositivos se desconectan o cambian de ubicación, reduciendo el número total necesario.
* **Flexibilidad en cambios:** facilita modificar los rangos de direcciones IP sin interrumpir a los usuarios.
* **Reducción de errores:** al centralizar y automatizar la asignación de direcciones, disminuye el riesgo de conflictos de IP (dos dispositivos con la misma dirección) o configuraciones erróneas.

En resumen, **DHCP** es un protocolo esencial para la administración moderna de redes, ya que automatiza la configuración de los dispositivos y mejora la eficiencia y confiabilidad del entorno de red.

12) Explicar las tecnologías Wireless, y sus estándares.

Las **tecnologías Wireless** (o redes inalámbricas) son redes informáticas que utilizan **radiofrecuencia (RF)** para conectar dispositivos sin necesidad de cables. Son muy comunes en hogares, empresas y redes de telecomunicaciones, ya que permiten movilidad y facilidad de instalación.

Además de las redes **LAN inalámbricas (Wi-Fi)**, existen otros tipos de redes Wireless:

* **PAN (Personal Area Network):** redes de corto alcance para conectar dispositivos personales (por ejemplo, Bluetooth).
* **MAN (Metropolitan Area Network):** redes inalámbricas que cubren ciudades o áreas metropolitanas.
* **WAN (Wide Area Network):** redes que abarcan grandes distancias, incluso países o continentes.

Una red inalámbrica basada en **Wi-Fi** envía señales mediante ondas de radio (como lo hacen los celulares y las radios, pero en frecuencias y modulaciones distintas).

**Estándares Wireless (IEEE 802.11):**  
El estándar principal para redes inalámbricas es **IEEE 802.11**, que se actualiza de manera continua con enmiendas identificadas por letras. Los más conocidos son:

* **802.11a:** opera en la banda de 5 GHz, hasta 54 Mbps, usando OFDM (multiplexación ortogonal por división de frecuencia).
* **802.11b:** en la banda de 2,4 GHz, hasta 11 Mbps, usando modulación CCK.
* **802.11g:** mejora las velocidades en 2,4 GHz, compatible con 802.11b, usando OFDM.
* **802.11n:** opera en 2,4 y 5 GHz, introduce **MIMO** (múltiples antenas para transmitir y recibir), con mayores velocidades y alcance.
* **802.11ac:** opera en 5 GHz, mejora la velocidad y capacidad respecto a 802.11n.
* **802.11ax (Wi-Fi 6):** unifica especificaciones en todas las bandas disponibles, usa **OFDMA** para mejorar la eficiencia del espectro y es el estándar actual en la mayoría de dispositivos nuevos.

**Otros estándares 802.11:**  
A lo largo de los años se han creado más enmiendas, centradas en mejorar la **seguridad**, **calidad de servicio**, **eficiencia energética** y otras características.

En resumen, las tecnologías **Wireless** permiten la conexión sin cables y, gracias a los distintos estándares, se han ido adaptando a mayores velocidades, mejor rendimiento y más seguridad.

13) ¿Qué es un Proxy?

Un **servidor proxy** es un intermediario entre un cliente (por ejemplo, una computadora) y un servidor de destino. Se encarga de recibir las solicitudes del cliente, reenviarlas al servidor correspondiente y devolver las respuestas al cliente. Esto permite anonimato, mejora de la seguridad, control de acceso y, en algunos casos, aceleración de las conexiones mediante almacenamiento en caché.

En otras palabras, el proxy actúa como **“representante”** o mediador entre dos sistemas informáticos. El cliente no se comunica directamente con el servidor final, sino a través del proxy, que utiliza su propia dirección IP para interactuar con el destino. A menudo, ni el cliente ni el servidor saben que existe un proxy en medio de la comunicación.

**Ventajas y usos principales de un servidor proxy:**

* **Anonimato y privacidad:** Oculta la dirección IP del usuario, protegiendo su identidad en Internet.
* **Aceleración de carga:** Mediante almacenamiento en caché, reduce el tráfico de datos y mejora los tiempos de respuesta.
* **Balanceo de carga:** Distribuye las solicitudes entre varios servidores para optimizar recursos.
* **Control de acceso:** En empresas y centros educativos se utilizan para restringir o filtrar contenidos.
* **Eludir bloqueos geográficos:** Permite simular la ubicación del usuario para acceder a contenido restringido en determinadas regiones.
* **Seguridad adicional:** Puede bloquear tráfico sospechoso y proteger frente a sitios web potencialmente dañinos.

En resumen, un proxy ofrece **mayor control, seguridad y flexibilidad** en la comunicación entre usuarios y servidores.

14- Explicar el protocolo Spanning tree.

El **Spanning Tree Protocol (STP)** es un protocolo utilizado en redes Ethernet que evita la formación de **tramas duplicadas** y, por lo tanto, previene problemas como **tormentas de broadcast** que pueden saturar o paralizar la red.

El problema que STP aborda surge cuando existen **múltiples rutas simultáneas** entre dos conmutadores. Sin un control, los paquetes podrían circular indefinidamente, generando congestión. STP soluciona esto creando un **árbol lógico** de la red, en el que se determina la **mejor ruta** para la transmisión de datos y se **desactivan temporalmente los puertos redundantes**.

**Funcionamiento básico:**

* Los conmutadores intercambian **Bridge Protocol Data Units (BPDU)** a intervalos regulares (cada 2 segundos), usando la dirección MAC especial 01-80-C2-00-00-10.
* Gracias a estas BPDU, STP obtiene un **mapa completo de la topología de la red** y elige la conexión más rápida y eficiente.
* Los puertos no utilizados se bloquean hasta que sea necesario reactivar la conexión.

**Gestión de fallos:**

* Si un enlace falla y no se reciben BPDU, el conmutador detecta el fallo y **recalcula la topología** del árbol.
* Las conexiones previamente desactivadas pueden activarse para mantener la comunicación, asegurando **la máxima disponibilidad y velocidad**.
* En configuraciones complejas, este proceso puede tardar más de 30 segundos, dependiendo del tamaño de la red.

**Resumen de beneficios:**

* Evita **bucles de red** y tormentas de broadcast.
* Garantiza **conectividad redundante** sin interrupciones prolongadas.
* Optimiza la transmisión de datos mediante la selección de la ruta más rápida.

15- Explicar el protocolo de comunicaciones OSPF.

El **OSPF (Open Shortest Path First)** es un **protocolo de enrutamiento interior (IGP)** utilizado para intercambiar información de enrutamiento dentro de redes IP. Fue diseñado para superar las limitaciones de protocolos anteriores como **RIP** y es ampliamente usado en **redes grandes y complejas**.

**Características principales:**

* **Enrutamiento con estado de enlace:** Cada router conoce la **topología completa** de la red y calcula la mejor ruta para enviar paquetes, considerando el ancho de banda disponible.
* **Algoritmo de camino más corto:** OSPF determina la ruta más eficiente entre dos puntos usando el **algoritmo de Dijkstra**.
* **Estructura por áreas:** La red se divide en **áreas** para limitar la cantidad de información de enrutamiento que se distribuye. Las áreas se conectan mediante un **router de frontera de área (ABR)**, que intercambia información entre ellas.

**Aplicaciones y ventajas:**

* **Enrutamiento en redes WAN:** Distribuye la información de forma eficiente en redes de gran tamaño.
* **Optimización del tráfico:** Calcula rutas alternativas ante fallas, mejorando eficiencia y disponibilidad.
* **Soporte de múltiples VLAN:** Facilita la administración y monitoreo de redes segmentadas.
* **Integración con otros protocolos:** Compatible con protocolos como **BGP**, para una gestión más eficiente de rutas.
* **Escalabilidad:** Permite agregar nuevas redes sin interrumpir el funcionamiento de la red existente

16- Explicar el protocolo ARP.

El **ARP (Address Resolution Protocol)** es un protocolo que permite **asociar una dirección IP a una dirección física (MAC)** dentro de una red de área local (LAN). Esto es fundamental porque los dispositivos necesitan conocer la dirección MAC del destino para enviar datos correctamente, aunque solo tengan su dirección IP.

**Funcionamiento básico:**

1. Cuando un dispositivo desea enviar datos a otro en la LAN, verifica su **caché ARP** para ver si ya tiene la correspondencia IP → MAC.
2. Si no la tiene, envía una **solicitud ARP** a la red para obtener la dirección MAC correspondiente a la IP deseada.
3. Una vez recibida la respuesta, se almacena en la caché ARP (dinámica o estática) para futuras comunicaciones.

**Caché ARP:**

* Mantiene temporalmente las asociaciones IP → MAC.
* Se purga periódicamente para liberar espacio y proteger la privacidad.

**Tipos y variantes de ARP:**

* **ARP de proxy:** Un dispositivo responde a solicitudes ARP de una red distinta, ofreciendo su propia dirección MAC como destino.
* **ARP gratuito:** Un host anuncia o actualiza su dirección IP a MAC sin que exista una solicitud previa.
* **ARP reverso (RARP):** Permite a un host conocer su propia dirección IP usando su dirección MAC.
* **ARP inverso (IARP):** Permite obtener la dirección IP a partir de una dirección MAC.

**Ventajas:**

* Facilita la comunicación en redes LAN.
* Automatiza la resolución de direcciones, evitando errores de envío.
* Permite implementaciones avanzadas como proxies o anuncios de dirección.

33- (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes?

Ejemplos.: Accedo y configuro el router de mi casa como admin, en mi trabajo

hago tareas relacionadas a networking, configuro una PAN hogareña para mi o mi

familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no

tengo ninguna experiencia, etc.

No tengo experiencia técnica previa en redes ni he realizado configuraciones avanzadas. Mi conocimiento se limita al uso domestico de las redes