10-   Explicar el servicio de DHCP.

El **servicio de DHCP** (*Dynamic Host Configuration Protocol*) es un protocolo de red que asigna automáticamente direcciones IP y otros parámetros de configuración a dispositivos en una red.

**🔹 ¿Para qué sirve?**

En lugar de asignar manualmente una dirección IP a cada dispositivo, un servidor DHCP lo hace de manera dinámica, evitando conflictos de IP y facilitando la administración de la red.

**🔹 ¿Cómo funciona?**

1. **Descubrimiento (Discover):** Un dispositivo nuevo en la red envía una solicitud en busca de un servidor DHCP.
2. **Oferta (Offer):** El servidor DHCP responde con una dirección IP disponible y otros parámetros (como máscara de subred, puerta de enlace, DNS, etc.).
3. **Solicitud (Request):** El dispositivo elige la oferta y envía una confirmación al servidor.
4. **Confirmación (ACK):** El servidor asigna la dirección IP y el dispositivo ya puede comunicarse en la red.

**🔹 Beneficios**

✅ Asignación automática de IPs  
✅ Evita conflictos de direcciones  
✅ Facilita la gestión de redes grandes  
✅ Permite cambiar configuraciones sin afectar a los dispositivos

Es súper útil en redes empresariales, hogares con múltiples dispositivos y en cualquier entorno donde no se quiera asignar IPs manualmente. 🚀

11-   Explicar el servicio de DNS.

El **servicio de DNS** (Domain Name System) es un sistema que traduce nombres de dominio (como google.com) en direcciones IP (como 142.250.190.46), permitiendo que los dispositivos se comuniquen en la red sin necesidad de recordar números complicados.

### 🔹 ¿Para qué sirve?

Los dispositivos en Internet se identifican con direcciones IP, pero recordar esas direcciones sería un dolor de cabeza. El DNS hace que podamos usar nombres fáciles de recordar en lugar de IPs.

### 🔹 ¿Cómo funciona?

1. **Consulta:** Cuando escribes google.com en el navegador, tu dispositivo pregunta al servidor DNS cuál es la IP de ese dominio.
2. **Búsqueda en caché:** Si la IP ya está guardada en caché, se usa directamente; si no, se consulta a servidores DNS más altos en la jerarquía.
3. **Respuesta:** El servidor DNS responde con la IP correspondiente.
4. **Conexión:** Tu dispositivo usa esa IP para conectarse al servidor y cargar la página.

### 🔹 Tipos de Servidores DNS

📌 **Recursivo:** Se encarga de buscar la IP consultando otros servidores si no tiene la respuesta.  
📌 **Raíz:** Son la base de la jerarquía DNS y dirigen las consultas a los servidores adecuados.  
📌 **TLD (Top-Level Domain):** Administran dominios de nivel superior, como .com, .org, .net.  
📌 **Autoritativo:** Contienen la información oficial sobre un dominio específico.

### 🔹 Beneficios

✅ Permite usar nombres amigables en vez de IPs  
✅ Acelera el acceso a sitios web gracias a la caché  
✅ Mejora la seguridad con filtros de phishing o malware  
✅ Es clave para el funcionamiento de Internet

Sin el DNS, navegar en Internet sería como recordar los números de teléfono de todos tus contactos en vez de usar sus nombres. 😅

12-  Explicar las tecnologías Wireless, y sus estándares.

### 📡 ****Tecnologías Wireless y sus Estándares****

Las tecnologías **wireless (inalámbricas)** permiten la comunicación sin cables a través de ondas electromagnéticas. Estas tecnologías han evolucionado con diversos estándares, cada uno diseñado para diferentes necesidades de conectividad.

## 🔹 **1. Wi-Fi (Wireless Fidelity)**

Es la tecnología más común para redes inalámbricas en hogares y oficinas. Utiliza los estándares **IEEE 802.11**.

### ****Estándares Wi-Fi:****

| **Estándar** | **Año** | **Velocidad Máx.** | **Frecuencia** | **Características** |
| --- | --- | --- | --- | --- |
| **802.11** | 1997 | 2 Mbps | 2.4 GHz | Primera versión, muy lenta. |
| **802.11a** | 1999 | 54 Mbps | 5 GHz | Menos interferencias pero menor alcance. |
| **802.11b** | 1999 | 11 Mbps | 2.4 GHz | Más alcance pero más interferencias. |
| **802.11g** | 2003 | 54 Mbps | 2.4 GHz | Compatibilidad con 802.11b, más rápido. |
| **802.11n** | 2009 | 600 Mbps | 2.4/5 GHz | Introduce MIMO (múltiples antenas). |
| **802.11ac (Wi-Fi 5)** | 2014 | 1.3 Gbps | 5 GHz | Mayor velocidad, mejor cobertura. |
| **802.11ax (Wi-Fi 6)** | 2019 | 9.6 Gbps | 2.4/5 GHz | Mejor rendimiento en redes congestionadas. |
| **802.11be (Wi-Fi 7)** | 2024 | 46 Gbps | 2.4/5/6 GHz | Aumento en ancho de banda y menor latencia. |

✅ **Wi-Fi 6 y Wi-Fi 7** mejoran la eficiencia y la capacidad en redes con muchos dispositivos.

## 🔹 **2. Bluetooth**

Tecnología de corto alcance para la conexión de dispositivos personales como audífonos, teclados y teléfonos.

### ****Versiones de Bluetooth:****

| **Versión** | **Año** | **Velocidad** | **Alcance** | **Características** |
| --- | --- | --- | --- | --- |
| **1.0-1.2** | 1999-2003 | 1 Mbps | 10 m | Primeras versiones con problemas de compatibilidad. |
| **2.0-2.1** | 2004-2007 | 3 Mbps | 10-30 m | Introducción de EDR (Enhanced Data Rate). |
| **3.0** | 2009 | 24 Mbps | 10-30 m | Uso de Wi-Fi para mayor velocidad. |
| **4.0-4.2** | 2010-2014 | 1 Mbps | 50-100 m | Bajo consumo de energía (BLE). |
| **5.0-5.3** | 2016-2022 | 2 Mbps | 200-400 m | Mayor velocidad, alcance y estabilidad. |

✅ **Bluetooth 5+** mejora la eficiencia para dispositivos IoT y audio inalámbrico.

## 🔹 **3. NFC (Near Field Communication)**

Tecnología de corto alcance (máx. 10 cm) usada en pagos móviles (Google Pay, Apple Pay), tarjetas de transporte y autenticación.

* **Velocidad:** 106-424 Kbps
* **Frecuencia:** 13.56 MHz
* **Usos:** Pagos sin contacto, acceso seguro, intercambio de datos entre teléfonos.

✅ **Ventaja:** No requiere emparejamiento como Bluetooth.

## 🔹 **4. Zigbee & Z-Wave**

Protocolos inalámbricos diseñados para el **Internet de las Cosas (IoT)** y automatización del hogar.

| **Tecnología** | **Frecuencia** | **Velocidad** | **Alcance** | **Uso Principal** |
| --- | --- | --- | --- | --- |
| **Zigbee** | 2.4 GHz | 250 Kbps | 10-100 m | Domótica (Luces, sensores). |
| **Z-Wave** | 908 MHz (EE.UU.), 868 MHz (Europa) | 100 Kbps | 30-100 m | Casas inteligentes. |

✅ **Ventaja:** Consumo de energía ultra bajo.

## 🔹 **5. LTE, 5G y Redes Celulares**

Tecnologías móviles para comunicación de datos en dispositivos celulares.

### ****Evolución de redes móviles:****

| **Generación** | **Año** | **Velocidad Máx.** | **Características** |
| --- | --- | --- | --- |
| **1G** | 1980s | 2.4 Kbps | Solo llamadas analógicas. |
| **2G (GSM, CDMA)** | 1990s | 50 Kbps | SMS y llamadas digitales. |
| **3G (UMTS, HSPA)** | 2000s | 2 Mbps | Internet móvil básico. |
| **4G (LTE, LTE-A)** | 2010s | 100 Mbps - 1 Gbps | Streaming HD, juegos en línea. |
| **5G** | 2020s | 10 Gbps | Baja latencia, IoT masivo, redes inteligentes. |

✅ **5G** permite velocidades ultra rápidas y menor latencia para IA, IoT y realidad aumentada.

### 🎯 ****Resumen General****

| **Tecnología** | **Estándar** | **Frecuencia** | **Velocidad** | **Uso** |
| --- | --- | --- | --- | --- |
| **Wi-Fi** | IEEE 802.11 | 2.4/5/6 GHz | Hasta 46 Gbps | Redes domésticas y empresariales. |
| **Bluetooth** | Bluetooth SIG | 2.4 GHz | Hasta 24 Mbps | Accesorios y dispositivos personales. |
| **NFC** | ISO/IEC 18092 | 13.56 MHz | Hasta 424 Kbps | Pagos móviles, acceso seguro. |
| **Zigbee/Z-Wave** | IEEE 802.15.4 | 2.4 GHz / 868 MHz | 100-250 Kbps | IoT y automatización del hogar. |
| **5G/LTE** | 3GPP | 700 MHz - 39 GHz | Hasta 10 Gbps | Internet móvil y redes inteligentes. |

Cada una de estas tecnologías tiene su propósito y ventajas dependiendo de la aplicación. 🚀

13- ¿Qué es un Proxy?

Un **proxy** es un servidor que actúa como intermediario entre tu dispositivo e Internet. En lugar de conectarte directamente a un sitio web, primero te conectas al proxy, y este se encarga de reenviar tu solicitud al destino final.

### 🔹 ****¿Para qué sirve un proxy?****

✅ **Ocultar tu IP:** El servidor web ve la IP del proxy en lugar de la tuya.  
✅ **Filtrar contenido:** Puede bloquear sitios web o controlar el acceso en una empresa o escuela.  
✅ **Mejorar seguridad:** Puede actuar como un cortafuegos, evitando conexiones no seguras.  
✅ **Acelerar la navegación:** Guarda en caché páginas visitadas, reduciendo el tiempo de carga.  
✅ **Saltar restricciones geográficas:** Permite acceder a contenido bloqueado en ciertas regiones.

### 🔹 ****Tipos de Proxies****

🔹 **Proxy Transparente:** No oculta la IP del usuario y es usado para filtrado de contenido.  
🔹 **Proxy Anónimo:** Oculta la IP real, pero indica que se usa un proxy.  
🔹 **Proxy Élite:** Oculta tanto la IP como el hecho de que se está usando un proxy.  
🔹 **Proxy Reverso:** Protege servidores en lugar de clientes, actuando como intermediario en solicitudes entrantes.

### 🔹 ****Ejemplo de cómo funciona un proxy****

1️⃣ Tú solicitas www.ejemplo.com.  
2️⃣ Tu dispositivo envía la petición al proxy.  
3️⃣ El proxy la reenvía al sitio web usando su propia IP.  
4️⃣ El sitio web responde al proxy.  
5️⃣ El proxy te envía la respuesta.

Es como si alguien pidiera comida por ti en un restaurante para que no sepan quién eres. 🍽️😆

14-   Explicar el protocolo Spanning tree.

## 🌳 **Protocolo Spanning Tree (STP) - IEEE 802.1D**

El **Spanning Tree Protocol (STP)** es un protocolo de red que previene **bucles** en redes conmutadas (switches) al desactivar enlaces redundantes.

### 🔹 ****¿Por qué es necesario?****

En una red con múltiples switches, pueden existir caminos redundantes para mejorar la disponibilidad. Sin STP, estos caminos pueden generar **bucles** que:  
❌ Saturan la red con tráfico duplicado.  
❌ Causan colisiones y fallos en la comunicación.  
❌ Evitan que los dispositivos reciban correctamente los paquetes.

STP **desactiva temporalmente los enlaces redundantes** hasta que sean necesarios (por ejemplo, si un enlace principal falla).

### 🔹 ****¿Cómo funciona STP?****

1️⃣ **Elección del Root Bridge**

* Todos los switches eligen uno como **Root Bridge** (switch principal) basado en la prioridad más baja (Bridge ID).

2️⃣ **Cálculo del camino más corto**

* Se elige el **camino más eficiente** desde cada switch hacia el Root Bridge, basado en el **costo del enlace** (menor costo = mejor camino).

3️⃣ **Desactivación de enlaces redundantes**

* STP **pone en estado de bloqueo** (Blocking) los enlaces que podrían generar bucles.

4️⃣ **Monitoreo y reactivación**

* Si un enlace principal falla, STP **reactiva** un enlace bloqueado para restaurar la conectividad.

### 🔹 ****Estados de un puerto en STP****

| **Estado** | **Función** |
| --- | --- |
| **Blocking** | Bloquea tráfico para evitar bucles. |
| **Listening** | Evalúa si debe activarse o no. |
| **Learning** | Aprende direcciones MAC antes de reenviar tráfico. |
| **Forwarding** | Reenvía tráfico normalmente. |
| **Disabled** | Puerto apagado o sin conexión. |

### 🔹 ****Variantes de STP****

🚀 **RSTP (Rapid STP - IEEE 802.1w):** Versión mejorada con convergencia más rápida.  
🚀 **MSTP (Multiple STP - IEEE 802.1s):** Maneja múltiples VLANs eficientemente.  
🚀 **PVST (Per VLAN STP - Cisco):** Ejecuta STP por cada VLAN en switches Cisco.

### 🔹 ****Ejemplo práctico****

Imagina tres switches conectados en un **triángulo**. Sin STP, los datos podrían circular en un bucle infinito. Con STP:  
✔️ Un switch es elegido **Root Bridge**.  
✔️ Se selecciona el **camino más corto** a ese switch.  
✔️ **Un enlace se bloquea** para evitar bucles.

Si un enlace principal cae, STP **habilita el enlace bloqueado** y mantiene la red operativa. 💡

### 🎯 ****Resumen****

🔹 **Evita bucles en redes conmutadas.**  
🔹 **Selecciona un Root Bridge y bloquea enlaces redundantes.**  
🔹 **Reactiva enlaces bloqueados si hay fallos.**  
🔹 **RSTP es una versión más rápida y eficiente.**

STP es clave en redes con switches para evitar caos y mantener la estabilidad. 🚀

15-   Explicar el protocolo de comunicaciones OSPF.

## 🏛️ **Protocolo OSPF (Open Shortest Path First) - RFC 2328**

**OSPF (Open Shortest Path First)** es un **protocolo de enrutamiento dinámico** que usa el **algoritmo de estado de enlace (Link-State)** para encontrar la mejor ruta en redes grandes. Se basa en el **menor costo** en lugar de la distancia en saltos (hops), lo que lo hace más eficiente que RIP.

### 🔹 ****Características principales de OSPF****

✅ **Protocolo de enrutamiento de estado de enlace.**  
✅ **Usa el algoritmo de Dijkstra** para calcular la mejor ruta.  
✅ **Divide la red en áreas** para mejorar el rendimiento.  
✅ **Convergencia rápida** (se adapta rápidamente a cambios).  
✅ **Soporta VLSM y CIDR** (permite sumarización de rutas).  
✅ **Evita bucles** sin necesidad de límite de saltos como RIP.

### 🔹 ****¿Cómo funciona OSPF?****

1️⃣ **Elección del Router Designado (DR) y Backup (BDR)**

* En redes broadcast, se eligen un **DR** (Router Designado) y un **BDR** (Backup) para reducir tráfico.

2️⃣ **Descubrimiento de vecinos**

* Los routers OSPF intercambian mensajes Hello para descubrir routers vecinos y formar adyacencias.

3️⃣ **Intercambio de bases de datos de estado de enlace (LSDB)**

* Cada router comparte información de su topología con los demás.

4️⃣ **Cálculo de rutas con el Algoritmo de Dijkstra**

* Se construye un **árbol SPF** para encontrar el camino más corto basado en costos de enlace.

5️⃣ **Actualización de rutas solo cuando hay cambios**

* OSPF no envía actualizaciones periódicas, solo cuando hay cambios en la topología.

### 🔹 ****Áreas en OSPF****

Para mejorar escalabilidad, OSPF divide la red en **áreas**.

* **Área 0 (Área Backbone):** Centro de la red, todos los demás deben conectarse a ella.
* **Áreas normales:** Conectadas al área 0, reducen el tamaño de las tablas de enrutamiento.
* **Áreas Stub y Totally Stubby:** Reducen la cantidad de rutas intercambiadas.
* **Área NSSA (Not-So-Stubby Area):** Similar a Stub, pero permite rutas externas.

### 🔹 ****Tipos de Mensajes OSPF****

📡 **Hello:** Descubre y mantiene vecinos.  
📡 **DBD (Database Description):** Resume la LSDB.  
📡 **LSR (Link-State Request):** Solicita información de la topología.  
📡 **LSU (Link-State Update):** Envía cambios en la red.  
📡 **LSAck (Link-State Acknowledgment):** Confirma la recepción de actualizaciones.

### 🔹 ****Ejemplo práctico de OSPF****

Imagina una empresa con varias sucursales conectadas.

* Cada router OSPF aprende sobre su entorno y envía información a sus vecinos.
* El router principal en el centro de la red es el **DR**.
* Si una conexión falla, OSPF recalcula rápidamente la mejor ruta alternativa.

### 🎯 ****Resumen****

🔹 **Encuentra la mejor ruta basada en costos, no en saltos.**  
🔹 **Se adapta rápidamente a cambios en la red.**  
🔹 **Divide la red en áreas para mayor eficiencia.**  
🔹 **Usa el algoritmo de Dijkstra para el cálculo de rutas.**

OSPF es el protocolo ideal para **redes empresariales grandes y complejas**. 🚀

16-   Explicar el protocolo ARP.

El **Protocolo de Resolución de Direcciones (ARP - Address Resolution Protocol)** es un protocolo de red utilizado para encontrar la dirección MAC (Media Access Control) de un dispositivo a partir de su dirección IP dentro de una red local (LAN).

**📌 ¿Por qué es necesario ARP?**

Las redes IP utilizan direcciones IP para identificar dispositivos, pero la comunicación real dentro de una red local se realiza mediante direcciones MAC. Como los dispositivos no saben de antemano qué dirección MAC corresponde a una IP específica, ARP se encarga de resolver esta información.

**🔄 Funcionamiento del ARP**

1. **Consulta ARP (ARP Request)**:
   * Cuando un dispositivo necesita comunicarse con otro en la misma red, envía un mensaje de difusión (broadcast) preguntando:  
     *"¿Quién tiene la IP X.X.X.X? Respóndeme con tu dirección MAC."*
2. **Respuesta ARP (ARP Reply)**:
   * El dispositivo que tiene la IP consultada responde directamente al emisor con su dirección MAC.
3. **Almacenamiento en caché**:
   * Para mejorar el rendimiento, las direcciones MAC aprendidas se guardan en una tabla ARP temporalmente, evitando consultas innecesarias.

**🛠 Tipos de ARP**

* **ARP estático**: Entradas fijas configuradas manualmente en la tabla ARP.
* **ARP dinámico**: Las direcciones MAC se aprenden automáticamente y se almacenan temporalmente.
* **ARP inverso (RARP)**: Permite que un dispositivo descubra su propia IP a partir de su dirección MAC.
* **ARP gratuito (Gratuitous ARP)**: Se usa para detectar IP duplicadas o actualizar información en la red.

**⚠ Vulnerabilidades del ARP**

ARP no tiene autenticación, lo que lo hace vulnerable a ataques como el **ARP Spoofing**, donde un atacante finge ser otro dispositivo en la red para interceptar tráfico.

**📌 Conclusión**

ARP es esencial para la comunicación en redes locales, ya que permite traducir direcciones IP a MAC, facilitando la entrega de paquetes dentro de una LAN. Sin él, los dispositivos no podrían comunicarse eficientemente en redes Ethernet. 🚀

17- ¿Qué es un Firewall?

Un **firewall** es un sistema de seguridad que controla y filtra el tráfico de red, permitiendo o bloqueando conexiones según un conjunto de reglas predefinidas. Su objetivo principal es proteger dispositivos y redes contra accesos no autorizados, ataques cibernéticos y tráfico malicioso.

**🔥 Funciones principales de un firewall**

1. **Filtrado de tráfico**: Inspecciona los datos que entran y salen de la red, bloqueando lo que no cumple con las reglas de seguridad.
2. **Protección contra ataques**: Defiende contra amenazas como ataques DDoS, malware o intentos de intrusión.
3. **Control de acceso**: Restringe qué dispositivos o usuarios pueden conectarse a ciertos recursos.
4. **Monitoreo y registros**: Mantiene un historial del tráfico para detectar posibles amenazas o anomalías.

**🏢 Tipos de firewalls**

📌 **Según su implementación**

* **Firewall de hardware**: Es un dispositivo físico que protege toda una red.
* **Firewall de software**: Se instala en equipos individuales y protege solo ese dispositivo.

📌 **Según su funcionamiento**

* **Firewall de filtrado de paquetes**: Examina cada paquete de datos y lo bloquea o permite según reglas predefinidas.
* **Firewall de inspección de estado**: Analiza el estado de la conexión y decide si el tráfico es seguro.
* **Firewall de aplicación (Proxy)**: Actúa como intermediario entre el usuario y la red, filtrando tráfico específico de aplicaciones.
* **Firewall de próxima generación (NGFW)**: Combina varias tecnologías avanzadas, como inspección profunda de paquetes, detección de intrusos y protección contra malware.

**🚨 ¿Por qué es importante un firewall?**

* Evita accesos no autorizados.
* Protege contra ataques de hackers y malware.
* Controla qué aplicaciones pueden acceder a internet.
* Mejora la privacidad y seguridad en la red.

En resumen, un firewall es la primera línea de defensa en ciberseguridad, ayudando a mantener redes y dispositivos protegidos. 🔒🚀

18- ¿Qué es una DMZ?

Una **DMZ (Zona Desmilitarizada)** en redes informáticas es un área de seguridad intermedia entre la red interna (privada) y la red externa (internet). Su objetivo es agregar una capa extra de protección para los sistemas que deben ser accesibles desde internet, como servidores web, de correo o de bases de datos.

**🔍 ¿Cómo funciona una DMZ?**

En una arquitectura de red con DMZ, el firewall separa tres zonas principales:

1. **Red interna (LAN)**: La red privada y segura donde están los dispositivos de la empresa.
2. **DMZ**: Un área intermedia donde se ubican los servidores que necesitan acceso desde internet.
3. **Red externa (WAN/Internet)**: La red pública desde donde los usuarios externos acceden a los servicios.

El firewall controla el tráfico entre estas zonas, permitiendo conexiones desde internet solo a la DMZ y restringiendo el acceso directo a la red interna.

**🔥 ¿Por qué usar una DMZ?**

✔ **Mayor seguridad**: Si un atacante compromete un servidor en la DMZ, aún no tiene acceso directo a la red interna.  
✔ **Protección de datos sensibles**: La LAN sigue siendo inaccesible para usuarios externos.  
✔ **Mejor control del tráfico**: Se pueden aplicar reglas específicas de acceso y filtrado.

**🏢 Ejemplo de uso de una DMZ**

* Un **servidor web** colocado en la DMZ permite que los usuarios accedan a un sitio sin exponer toda la red.
* Un **servidor de correo** en la DMZ recibe correos desde internet sin riesgo directo para la LAN.
* Un **servidor proxy** en la DMZ filtra el tráfico antes de que llegue a la red interna.

**🚨 Conclusión**

La DMZ es una estrategia clave en seguridad de redes que minimiza riesgos al exponer servicios al público sin comprometer la red privada. Es como una zona de cuarentena donde los servicios accesibles desde internet están protegidos, pero aislados. 🔒🚀

34- (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.