11- Explicar el servicio de DNS.

El servicio de DNS (Sistema de Nombres de Dominio) funciona como una agenda decontactos de Internet. Generalmente recordamos mejor los nombres como *google.com* o *youtube.com* que las largas direcciones de números que usan las computadoras como por ejemplo *142.250.190.14*

El DNS se encarga de traducir los nombres de las páginas web que escribimos en el navegador a la dirección IP que corresponde a esa página. Así, cuando ponemos [*www.google.com*](http://www.google.com), el DNS busca cuál es su dirección real en Internet y nos lleva hasta allí, sino de lo contrario tendríamos que memorizar números difíciles para visitar cada sitio.

12- Explicar las tecnologías Wireless, y sus estándares.

Las tecnologías Wireless (o inalámbricas) permiten conectarse a Internet o a una red sin necesidad de cables. En lugar de usar un cable para conectarse, los dispositivos se comunican a través del aire usando ondas de radio.

El Wi-Fi es uno de los ejemplos más conocidos de tecnología Wireless, gracias a él podemos movernos libremente mientras seguimos conectados.

Existen diferentes estándares de Wi-Fi que fueron mejorando con el tiempo. Cada uno indica la velocidad, el alcance y la calidad de la conexión. Algunos ejemplos son:

* 802.11b: uno de los primeros, más lento y con menos alcance.
* 802.11ac: aún más rápido, ideal para ver videos o jugar online.
* 802.11ax (también llamado Wi-Fi 6): el más nuevo, mucho más veloz y preparado para conectar muchos dispositivos al mismo tiempo.

Cada vez que usamos Wi-Fi, estamos usando uno de estos estándares sin darnos cuenta.

13- ¿Qué es un Proxy?

Un Proxy es como un intermediario entre la computadora e Internet. Cuando se quiere entrar a una página web, en vez de conectarse directamente, primero se le pide al Proxy, y él se encarga de buscar la página. Es un "puente" que ayuda a controlar, proteger o acelerar nuestras conexiones a Internet.

El Proxy puede servir para varias cosas, por ejemplo:

* Proteger identidad (la página no ve directamente la dirección).
* Filtrar contenidos (bloqueo de algunas páginas usando un Proxy).
* Ahorrar Internet (guarda copias de páginas que ya se visitaron para no descargarlas de nuevo).

14- Explicar el protocolo Spanning tree.

El protocolo Spanning Tree es un sistema que se usa en las redes para evitar problemas cuando hay caminos duplicados, organiza y protege la red para que funcione bien, incluso cuando hay muchos cables conectados.

Cuando en una red hay varios cables o conexiones entre los mismos dispositivos (por ejemplo, varios switches conectados entre sí), puede pasar que los datos den vueltas en círculo sin parar generando errores y lentitud.

El Spanning Tree detecta esas conexiones duplicadas y las apaga temporalmente quedando la red con un solo camino activo entre cada dispositivo evitando los circuitos cerrados que pueden colapsar toda la red.

15- Explicar el protocolo de comunicaciones OSPF.

El protocolo OSPF (Open Shortest Path First) es un sistema que usan los routers para encontrar el mejor camino por donde enviar los datos dentro de una red ayudando a que el tráfico en las redes grandes sea más rápido, organizado y confiable.

Cuando varios routers están conectados, OSPF compara diferentes caminos y elige el más rápido o más corto para que la información llegue antes a su destino.  
Además, si un camino se rompe, por ejemplo si un cable se corta, OSPF busca automáticamente otra ruta para que los datos sigan viajando sin problemas.

16- Explicar el protocolo ARP.

El protocolo ARP (Address Resolution Protocol) se usa en las redes para encontrar la dirección física (llamada MAC) de un dispositivo a partir de su dirección IP. ARP traduce direcciones IP en direcciones físicas para que los dispositivos puedan hablar entre sí en una red.

Por ejemplo, cuando una computadora quiere enviar algo a otra dentro de la misma red primero necesita saber la dirección MAC. Entonces, usa ARP para preguntar:  
"¿Quién tiene esta IP? ¡Pásame la dirección MAC!", de ese modo el dispositivo que tiene esa IP responde con su dirección MAC, y así la comunicación puede seguir.

17- ¿Qué es un Firewall?

Un Firewall es como un guardia de seguridad que protege una red o una computadora de amenazas externas. Se encarga de controlar qué datos pueden entrar y salir según reglas que se configuran.

Puede ser un programa instalado en la computadora o un dispositivo especial en la red. Por ejemplo, puede bloquear conexiones peligrosas, permitir solo ciertos programas o evitar que entren virus y ataques.

18- ¿Qué es una DMZ?

Una DMZ (Zona Desmilitarizada) en redes es un área especial que se crea para poner servidores que deben ser accesibles desde Internet, como una página web o un servidor de correo. Sirve para dar acceso a ciertos servicios públicos manteniendo protegida la red interna.

Está separada del resto de la red interna para proteger los datos importantes, de modo que, si alguien ataca un servidor en la DMZ, no puede llegar directamente a las computadoras privadas de la empresa o de la casa.

19- ¿Qué es un Gateway?

Un Gateway (o puerta de enlace) es el dispositivo que conecta una red con otra.  
Por ejemplo, en una casa o en una empresa, el Gateway suele ser el router que conecta la red local con Internet.

Cuando un dispositivo necesita comunicarse con algo que está fuera de su red, manda los datos al Gateway, y este se encarga de enviarlos al destino correcto. Es el "puente" que nos permite salir de nuestra red y comunicarnos con otras redes.

20- Según Microsoft, ¿qué significa NBL?

En el contexto de Microsoft, NBL significa "Network Binding Layer" (Capa de enlace de red), es un nivel que facilita la interacción de las aplicaciones con las redes para que los datos se transmitan de manera eficiente

Es un componente que gestiona la comunicación entre las aplicaciones y las redes en los sistemas operativos de Microsoft, encargándose de organizar y dirigir el tráfico de datos entre las aplicaciones y la red, asegurando que los mensajes lleguen al destino correcto.

34- ¿Qué experiencia tienen en redes?

Mi experiencia en redes es bastante básica. He configurado el router de mi casa en algunas ocasiones, cambiando la contraseña de Wi-Fi o ajustando algunos parámetros, pero no he trabajado mucho más allá de eso. No tengo experiencia profesional en redes, pero me interesa aprender más sobre cómo funcionan y cómo se gestionan diferentes dispositivos dentro de una red.  
En los dos años que llevo estudiando la carrera de desarrollador de software, he aprendido conceptos básicos de redes, como el funcionamiento de protocolos, direccionamiento IP y la importancia de la seguridad en las redes, aunque no he tenido la oportunidad de aplicarlos en proyectos prácticos hasta ahora. Muchas gracias!