1 - Que es una VLAN?

Una VLAN es una red de área local que está lógicamente segmentada. Es decir, agrupa dispositivos de red que están en segmentos de red diferentes como si estuvieran en la misma LAN, sin importar su ubicación física.

Normalmente, un switch de red se encarga de segmentar los dominios de difusión. Esto significa que cuando un dispositivo envía una señal a todos los dispositivos de una red (una difusión), el switch solo la reenvía a los dispositivos que están en la misma LAN. Si los dispositivos están en diferentes switches o en diferentes pisos de un edificio, se necesitaría un router para que puedan comunicarse entre sí.

Una VLAN usa software para agrupar dispositivos de red, aunque no estén físicamente conectados al mismo switch o no compartan el mismo dominio de difusión. Por ejemplo, se puede crear una VLAN para el departamento de contabilidad y otra para el departamento de recursos humanos. Los dispositivos dentro de cada VLAN pueden comunicarse entre sí como si estuvieran en la misma red, pero los de la VLAN de contabilidad no podrán comunicarse con los de la VLAN de recursos humanos.

Beneficios de usar VLANs:

- **Seguridad:** Las VLANs proporcionan seguridad porque separan el tráfico de red. Si un dispositivo está comprometido, no puede afectar a dispositivos en otras VLANs.
- **Mejor rendimiento:** Reducen los dominios de difusión, lo que significa que hay menos tráfico de red innecesario, mejorando el rendimiento.
- **Flexibilidad:** Facilita la gestión de la red, ya que puedes mover, agregar o eliminar dispositivos sin necesidad de reconfigurar la infraestructura física.
- **Ahorro de costos:** Al reducir la necesidad de hardware adicional (como routers), se reducen los costos.

2 - Que es una VPN?

Una VPN es una red privada virtual que permite crear una conexión segura y cifrada a través de una red pública, como Internet. La idea principal es proteger la privacidad y seguridad en línea, haciendo que los datos sean ilegibles para terceros y enmascarando las direcciones IP reales de los equipos de la red.

Al conectarse a una VPN un dispositivo establece una conexión con un servidor remoto operado por el servicio de VPN. En lugar de que el tráfico de internet vaya directamente desde el dispositivo a su destino (por ejemplo, un sitio web), pasa a través de un "túnel" cifrado hasta el servidor de la VPN y el servidor de la VPN es el que luego envía el tráfico al destino final.

Esto tiene dos efectos principales:

1. **Cifrado de datos:** Todo el tráfico que viaja por el túnel VPN está cifrado. Esto significa que si alguien (proveedor de servicios de internet, hackers en una red Wi-Fi pública o el gobierno) intenta interceptar datos, sólo verá información sin sentido.
2. **Anonimato:** La dirección IP real queda oculta, y el sitio web o servicio que visitado solo ve la dirección IP del servidor VPN. Esto mantiene el anonimato en línea y puede permitir acceder a contenido que está geográficamente restringido.

Es importante no confundir una VPN con una VLAN, ya que, aunque ambas son "virtuales", tienen propósitos muy diferentes.

- **VPN** es una tecnología de seguridad y privacidad que crea una conexión segura entre un dispositivo y una red a través de Internet. Su objetivo es proteger los datos y ocultar la identidad en línea.
- **VLAN** es una tecnología de segmentación de red que divide una red física en varias redes lógicas. Su objetivo es mejorar la organización, el rendimiento y la seguridad dentro de una red local, sin necesariamente involucrar la conexión a Internet.

En resumen, una VLAN se usa para organizar redes internas, mientras que una VPN se usa para crear una conexión segura a través de redes externas, como Internet.

3 - Que es una SAN?

Una SAN (Storage Area Network) es una red de área de almacenamiento dedicada y de alta velocidad que conecta servidores con dispositivos de almacenamiento de datos. En lugar de que cada servidor tenga su propio almacenamiento local (como discos duros internos), una SAN centraliza el almacenamiento, permitiendo que múltiples servidores accedan a un pool compartido de recursos de almacenamiento.

Una SAN no es una simple conexión de red como una LAN. Opera en un nivel diferente, a nivel de "bloque", lo que significa que los servidores ven el almacenamiento de la SAN como si fueran discos locales. Esto permite un acceso a datos extremadamente rápido y eficiente.

Las SAN están compuestas principalmente por tres capas:

- **Capa de Host:** Los servidores de la red que necesitan acceder al almacenamiento.
- **Capa de Estructura (Fabric):** La infraestructura de red que interconecta los servidores y el almacenamiento. Esto incluye switches, cables y otros dispositivos de red de alta velocidad (como los que usan el protocolo Fibre Channel).
- **Capa de Almacenamiento:** Los dispositivos físicos de almacenamiento, como matrices de discos (RAID), cintas o unidades de estado sólido (SSD).

Beneficios de una SAN

- **Alto rendimiento:** El tráfico de almacenamiento está separado del tráfico de red normal, lo que reduce la congestión y mejora la velocidad de acceso a los datos.
- **Escalabilidad:** Se puede añadir más almacenamiento fácilmente a la red de forma centralizada sin necesidad de apagar servidores.
- **Alta disponibilidad:** Al ser una red dedicada, la SAN ofrece redundancia y la capacidad de recuperar datos rápidamente en caso de fallo, lo que es crucial para la continuidad del negocio.
- **Gestión centralizada:** Administrar el almacenamiento de toda una empresa desde un solo punto simplifica las tareas de copias de seguridad, recuperación de desastres y gestión de datos.

4 - Diferencias entre un Hub, Repetidor, Router y SWITCH. Explicar las diferencias.

A continuación, te explico las diferencias clave entre un Hub, un Repetidor, un Switch y un Router, que son dispositivos fundamentales en la interconexión de redes.

1. Repetidor (Repeater)

Un repetidor es el dispositivo más básico de todos. Su función principal es regenerar una señal débil para que pueda viajar una distancia más larga. Funciona en la **capa 1 (física)** del modelo OSI. No tiene inteligencia para filtrar o dirigir el tráfico, simplemente toma una señal de entrada y la amplifica y retransmite. Es como un megáfono para la señal de red.

2. Hub

Un hub es un concentrador que conecta múltiples dispositivos en una red local (LAN) y funciona también en la **capa 1 (física)**. Cuando recibe datos en uno de sus puertos, los envía a todos los demás puertos, sin importar cuál sea el destino real. Esto crea un "dominio de colisión" grande y genera mucho tráfico innecesario, ya que todos los dispositivos de la red ven todos los datos. Por esta razón, los hubs están prácticamente obsoletos.

3. Switch

Un switch es una versión más "inteligente" del hub, y opera en la **capa 2 (enlace de datos)** del modelo OSI. A diferencia del hub, un switch aprende y almacena las **direcciones MAC** de los dispositivos conectados a cada uno de sus puertos. Cuando recibe un paquete de datos, lo dirige de manera inteligente solo al puerto del dispositivo de destino, en lugar de enviarlo a todos los puertos. Esto reduce el tráfico innecesario, minimiza las colisiones y mejora significativamente el rendimiento de la red.

4. Router

Un router es un dispositivo mucho más complejo que opera en la **capa 3 (red)** del modelo OSI. Su función principal es interconectar **diferentes redes** (como una red local con internet) y dirigir el tráfico entre ellas. Para hacer esto, utiliza **direcciones IP** y tablas de enrutamiento para determinar la mejor ruta para que los paquetes de datos lleguen a su destino. Los routers son esenciales para conectar tu red doméstica o de oficina a Internet y a otras redes externas, y a menudo incluyen funciones de seguridad como firewalls.

Cuadro de diferencias

Dispositivo	Capa OSI	Función principal	¿Cómo dirige el tráfico?
Repetidor	Capa 1 (Física)	Regenerar la señal	No dirige; simplemente amplifica y retransmite
Hub	Capa 1 (Física)	Conectar dispositivos	Envía datos a todos los puertos
Switch	Capa 2 (Enlace de datos)	Conectar dispositivos	Dirige datos al puerto correcto (usando direcciones MAC)
Router	Capa 3 (Red)	Conectar redes diferentes	Dirige datos a través de redes (usando direcciones IP)

5 - ¿Qué es un protocolo de comunicaciones?

Un protocolo de comunicaciones es un conjunto de reglas y estándares que permiten que dos o más dispositivos o sistemas se comuniquen entre sí, intercambiando información de manera ordenada y comprensible. Es el "idioma común" que utilizan los dispositivos para entenderse en una red. Sin estos protocolos, la comunicación entre ordenadores, servidores, routers y otros equipos sería imposible, ya que cada uno usaría su propio método para enviar y recibir datos.

Los protocolos definen todos los aspectos de la comunicación, incluyendo:

- **Formato de los datos:** Cómo se deben estructurar los datos antes de ser enviados (por ejemplo, en paquetes de datos).
- **Métodos de transmisión:** Cómo se envían los datos a través de la red (por cable, de forma inalámbrica, etc.).
- **Procedimientos para la conexión:** Cómo se inician, mantienen y finalizan las sesiones de comunicación.
- **Manejo de errores:** Cómo se detectan y corrigen los errores que pueden ocurrir durante la transmisión.

Los protocolos son como las reglas de un juego. Para que todos los jugadores entiendan lo que sucede, deben seguir las mismas reglas. En el mundo de las redes, si un dispositivo envía datos siguiendo un protocolo (por ejemplo, el protocolo HTTP para una página web) y el receptor no conoce esas reglas, no podrá interpretar la información.

Ejemplos de protocolos comunes

Existen muchos protocolos diferentes, cada uno diseñado para un propósito específico. Algunos de los más conocidos son:

- **TCP/IP:** Es el conjunto de protocolos fundamental de Internet. **TCP** (Protocolo de Control de Transmisión) se encarga de dividir los datos en paquetes y asegurarse de que lleguen de forma correcta y en el orden adecuado. **IP** (Protocolo de Internet) se encarga de direccionar esos paquetes para que viajen a través de la red hasta su destino final.
- **HTTP:** (Protocolo de Transferencia de Hipertexto) Es el protocolo que usan los navegadores y servidores web para transferir documentos y datos en la World Wide Web.
- **FTP:** (Protocolo de Transferencia de Archivos) Se utiliza para la transferencia de archivos entre un cliente y un servidor.
- **SMTP:** (Protocolo Simple de Transferencia de Correo) Es el protocolo para el envío de correos electrónicos.

6 - Explique TCP/IP y NetBios, resuma sus diferencias. (Acá sí explicar cada uno y sus diferencias)

TCP/IP (Transmission Control Protocol/Internet Protocol) y NetBIOS (Network Basic Input/Output System) son protocolos que permiten la comunicación en red, pero operan en diferentes niveles y con propósitos distintos. TCP/IP es el estándar global para Internet y redes modernas, mientras que NetBIOS es un protocolo de sesión más antiguo, diseñado para redes locales.

TCP/IP

TCP/IP es el conjunto de protocolos de red que es la base de Internet. Opera en las capas 3 y 4 del modelo OSI. Se divide en dos componentes principales:

- **IP (Internet Protocol):** Se encarga de direccionar y enrutar los paquetes de datos a través de la red. Utiliza direcciones IP para identificar de manera única cada dispositivo conectado. Su función principal es asegurar que los datos viajen desde el origen hasta el destino, eligiendo la mejor ruta posible.
- **TCP (Transmission Control Protocol):** Funciona en un nivel superior al de IP y garantiza que la entrega de los datos sea confiable. Se encarga de dividir los datos en paquetes, reensamblarlos en el destino y verificar que no se pierda nada. Si un paquete no llega, solicita su reenvío.

TCP/IP es jerárquico, escalable y enrutable, lo que significa que puede usarse para redes pequeñas y locales, así como para la vasta red de Internet.

NetBIOS

NetBIOS es un protocolo de sesión que se usa para establecer una conexión de comunicación entre dos ordenadores en una red local. Funciona en la capa 5 (sesión) del modelo OSI. Su función principal es el descubrimiento y nombramiento de recursos en una red, permitiendo que los ordenadores se encuentren entre sí por nombre en lugar de por dirección numérica. Aunque NetBIOS es antiguo, todavía se usa en redes Windows para funciones como la resolución de nombres y el intercambio de archivos.

Sin embargo, NetBIOS no es enrutable por sí mismo, por lo que requiere un protocolo de transporte como TCP/IP o IPX/SPX para enviar datos a través de diferentes redes. Por esta razón, su implementación más común hoy en día es NetBIOS sobre TCP/IP, conocido como NBT (NetBIOS over TCP/IP), que permite que NetBIOS funcione en redes más grandes y en Internet.

Resumen de diferencias

Característica	TCP/IP	NetBIOS
Función principal	Enrutamiento de paquetes y comunicación de extremo a extremo.	Nombramiento de recursos y establecimiento de sesiones en redes locales.
Capas OSI	Capa 3 (Red) y Capa 4 (Transporte).	Capa 5 (Sesión).
Alcance	Global (Internet) y redes locales.	Redes locales (requiere un protocolo de transporte para enrutamiento).
Mecanismo de identificación	Direcciones IP.	Nombres de NetBIOS.
Uso actual	El estándar para redes modernas e Internet.	Principalmente en redes locales de Windows para compatibilidad heredada (a través de NBT).

7 - ¿Cómo está formado un paquete de datos en TCP/IP? ¿Qué es un “flag” en un paquete de TCP/IP?

Un paquete de datos en TCP/IP es la unidad de información fundamental que se transmite a través de una red. Se forma mediante un proceso de **encapsulamiento** a medida que los datos viajan desde la capa de aplicación hasta la capa de red.

Un paquete TCP/IP se compone de dos partes principales:

1. **Encabezado (Header):** Contiene la información de control y direccionamiento necesaria para que el paquete sea entregado correctamente. El encabezado, a su vez, está formado por dos encabezados clave:
    - **Encabezado TCP:** Agregado en la capa de transporte, contiene información para asegurar la fiabilidad de la conexión. Incluye los puertos de origen y destino, el número de secuencia (para reordenar los paquetes), el número de acuse de recibo y los "flags" de control.
    - **Encabezado IP:** Agregado en la capa de red, contiene la dirección IP de origen y destino, lo que permite que el paquete sea enrutado a través de diferentes redes.
2. **Carga útil / Payload:** Es la parte que contiene los datos reales que se están enviando, como un archivo, parte de una página web o un correo electrónico.

¿Qué es un "flag" en un paquete de TCP?

En un paquete TCP, los **flags** (o banderas) son bits de control que se encuentran en el encabezado TCP. Sirven para indicar el estado de una conexión o para controlar el flujo de la comunicación. Son como interruptores que están "encendidos" o "apagados" para señalar el propósito del paquete.

Los flags más importantes son:

- **SYN (Synchronize):** Se usa para iniciar una conexión. Es el primer paso en el "apretón de manos de tres vías" (three-way handshake) que establece una conexión TCP.
- **ACK (Acknowledgment):** Se usa para acusar recibo de un paquete. Se envía para confirmar que el receptor ha recibido correctamente los datos.
- **FIN (Finish):** Se usa para terminar una conexión de forma ordenada y controlada.
- **RST (Reset):** Se usa para abortar una conexión de forma abrupta e inmediata, generalmente en caso de un error.

8 - Defina la red según su geografía. Explicar distintas variantes.

Una red según su geografía se define por el área que cubre. Esto va desde redes muy pequeñas que conectan dispositivos en un solo edificio hasta redes masivas que se extienden por continentes enteros. Aquí están las variantes principales:

1. PAN (Personal Area Network)

Una PAN es la red más pequeña, diseñada para conectar dispositivos que usa una persona, como un teléfono, una tablet, auriculares y una computadora. Su alcance es muy corto, generalmente de unos pocos metros. Un ejemplo común es la conexión por Bluetooth para unos auriculares inalámbricos.

2. LAN (Local Area Network)

Una LAN conecta dispositivos en un área geográficamente limitada, como una casa, una oficina, un edificio o un campus universitario. Las redes LAN suelen ser propiedad de la organización que las usa. Permiten que los dispositivos se comuniquen entre sí, compartan archivos e impresoras. Las tecnologías más comunes para una LAN son Ethernet y Wi-Fi.

3. MAN (Metropolitan Area Network)

Una MAN es una red más grande que una LAN, ya que cubre el área de una ciudad o un área metropolitana. A menudo conecta varias LAN dentro de una ciudad o en un área grande, como un campus corporativo o un grupo de edificios del gobierno. Es común que las MAN usen fibra óptica para lograr una alta velocidad de transmisión de datos.

4. WAN (Wide Area Network)

Una WAN es una red que se extiende por un área geográfica grande, como una región, un país o incluso continentes. **Internet** podría considerarse un ejemplo de WAN. Estas redes conectan varias LAN y MAN entre sí y suelen ser gestionadas por un proveedor de servicios de telecomunicaciones.

5. GAN (Global Area Network)

Una GAN es una red que se extiende a nivel global. Internet también podría incluirse como un ejemplo de GAN ya que conecta redes en todo el mundo. Las GAN pueden estar compuestas por WANs interconectadas.

33 - ¿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.

Tuve experiencia en redes hace algunos años. En el secundario técnico tuve materias vinculadas a redes y en los primeros años después de la secundaria realicé algunos trabajos de instalación de redes pequeñas para hogares y comercios, principalmente para conexión entre equipos y disponibilización de redes WIFI. En ese contexto tuve experiencia en armado de cables ethernet.

También he realizado algunas configuraciones para conexión entre computadoras para poder jugar en red con algunos amigos, a veces realizando conexiones directas entre los equipos y en otros casos utilizando Switches o Routers.

El último acercamiento que tuve con redes fue hace unos 6 años aproximadamente cuando hice un curso básico de redes en Educación IT.