motor red

Analía Romero - Marcos Gonzalez

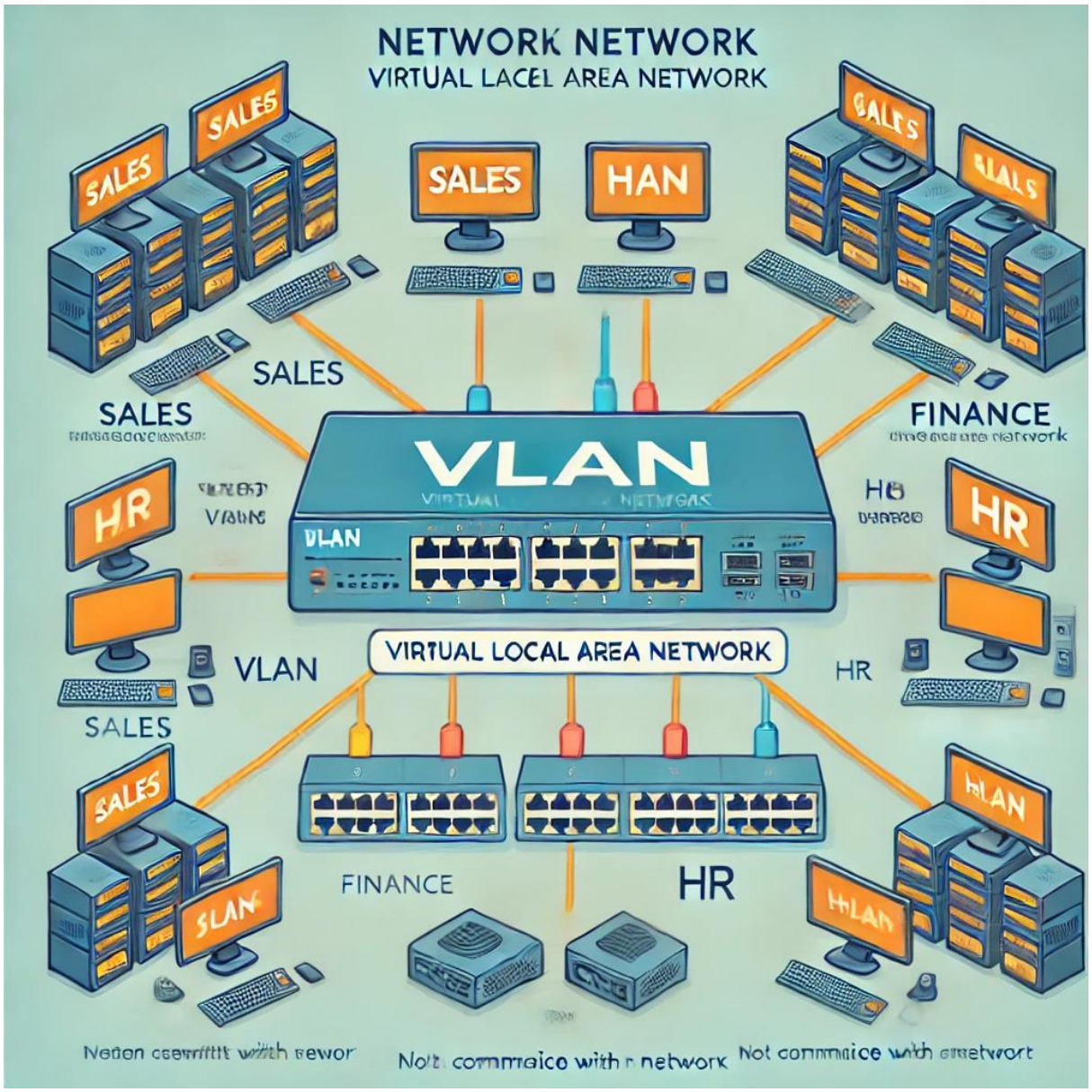
INDICE

1- ¿Qué es una VLAN?

Una **VLAN** (Red de Área Local Virtual, por sus siglas en inglés: **Virtual Local Area Network**) es una tecnología que permite dividir una red física en varias redes lógicas separadas. Aunque todos los dispositivos están conectados al mismo hardware físico (como switches), una VLAN segrega el tráfico de red de manera lógica, lo que significa que los dispositivos dentro de una misma VLAN pueden comunicarse entre sí, pero están aislados de los dispositivos en otras VLANs a menos que se configure una intercomunicación a través de un router.

Beneficios de usar VLAN:

1. **Segmentación**: Permite segmentar una red en subredes más pequeñas y lógicas, mejorando la seguridad y el rendimiento.
2. **Seguridad**: Los datos en una VLAN no pueden ser accedidos por dispositivos en otras VLANs, lo que mejora la privacidad.
3. **Gestión del tráfico**: Reduce la cantidad de tráfico innecesario, lo que puede mejorar el rendimiento de la red.
4. **Flexibilidad**: Facilita la gestión de redes en entornos grandes y complejos sin necesidad de cambios físicos en el cableado.



2- ¿Qué es una VPN?

Una VPN (Red Privada Virtual) es una red privada que se extiende a través de una red pública, como Internet. Esto permite a los usuarios conectarse a una red privada de forma segura, incluso si están utilizando una red pública no segura.

Las VPN se utilizan para una variedad de propósitos, como:

- **Seguridad:** Las VPN pueden ayudar a proteger la privacidad de los usuarios en línea al encriptar su tráfico de Internet. Esto significa que los terceros no pueden ver lo que los usuarios están haciendo en línea.
- **Acceso a contenido bloqueado:** Las VPN pueden ayudar a los usuarios a acceder a contenido bloqueado en su país o región. Esto se debe a que las VPN pueden hacer que parezca que los usuarios están accediendo a Internet desde otro país.
- **Anonimato:** Las VPN pueden ayudar a los usuarios a permanecer anónimos en línea. Esto se debe a que las VPN pueden ocultar la dirección IP de los usuarios.

Si estás interesado en utilizar una VPN, hay muchas opciones disponibles. Es importante elegir una VPN de buena reputación que ofrezca una buena seguridad y privacidad.

Aquí hay algunos consejos para elegir una VPN:

- **Elige una VPN que ofrezca una buena seguridad y privacidad.**
- **Elige una VPN que tenga una buena reputación.**
- **Elige una VPN que ofrezca una buena velocidad.**
- **Elige una VPN que ofrezca un buen servicio al cliente.**

Una vez que hayas elegido una VPN, puedes configurarla en tu computadora, teléfono o tableta. Una vez que esté configurada, podrás conectarte a la VPN y disfrutar de todos sus beneficios.

3- ¿Qué es una SAN?

¿Qué es una SAN?

SAN son las siglas de **Storage Area Network**, que en español se traduce como **Red de Área de Almacenamiento**. Es una red de alta velocidad diseñada específicamente para conectar servidores a dispositivos de almacenamiento masivo, como matrices de discos o cintas.

Imagina una SAN como una autopista exclusiva para datos. Mientras que una red local (LAN) es como una calle de la ciudad donde circulan todo tipo de tráfico (correo electrónico, navegación web, etc.), una SAN es una autopista de alta velocidad donde solo circulan datos de almacenamiento.

¿Por qué usar una SAN?

- **Rendimiento:** Al separar el tráfico de almacenamiento del tráfico de red general, las SAN ofrecen un rendimiento mucho mayor y una latencia más baja, lo que es crucial para aplicaciones que requieren acceso rápido a grandes cantidades de datos, como bases de datos o aplicaciones de virtualización.
- **Disponibilidad:** Las SAN suelen ser altamente redundantes, con múltiples rutas de acceso a los datos y sistemas de respaldo. Esto garantiza una mayor disponibilidad y reduce el riesgo de pérdida de datos en caso de fallo.
- **Escalabilidad:** Las SAN se pueden expandir fácilmente para adaptarse a las necesidades cambiantes de una organización. Es posible agregar nuevos dispositivos de almacenamiento o servidores sin interrumpir las operaciones.
- **Gestión centralizada:** Las SAN permiten administrar y gestionar de forma centralizada todos los dispositivos de almacenamiento de una organización, lo que simplifica las tareas de administración y reduce los costos.

¿Cómo funciona una SAN?

Una SAN típicamente utiliza protocolos de alto rendimiento como Fibre Channel o iSCSI para conectar los servidores a los dispositivos de almacenamiento. Los datos se almacenan en bloques y se presentan a los servidores como discos virtuales.

¿Cuáles son las principales diferencias entre una SAN y un NAS?

Característica	SAN	NAS
Protocolo	Fibre Channel, iSCSI	NFS, SMB
Acceso	Bloque	Archivo
Rendimiento	Muy alto	Alto
Complejidad	Alta	Baja
Uso típico	Entornos empresariales de alta disponibilidad	Pequeñas y medianas empresas, usuarios domésticos

En resumen, una SAN es una solución de almacenamiento de alto rendimiento y escalable ideal para entornos empresariales que requieren un acceso rápido y fiable a grandes cantidades de datos.

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

Diferencias entre Hub, Repetidor, Router y Switch

Estos dispositivos son fundamentales en la construcción de redes, pero cada uno tiene una función específica y se utiliza en diferentes escenarios.

Hub (Concentrador)

- **Función:** Repite todas las señales que recibe en todos sus puertos.
- **Limitaciones:**
  - Baja velocidad.
  - Colisiones frecuentes en redes saturadas.
  - No segmenta la red, lo que puede llevar a un rendimiento reducido.
- **Uso:** Redes muy pequeñas y sencillas, donde el rendimiento no es una prioridad.

Repetidor

- **Función:** Amplía la distancia de una red al regenerar las señales.
- **Diferencia con el Hub:** Aunque ambos repiten señales, el repetidor opera a nivel físico, mientras que el hub opera a nivel de enlace de datos.
- **Uso:** Extender el alcance de una red en distancias cortas.

Switch (Conmutador)

- **Función:** Conecta múltiples dispositivos en una red y reenvía los datos solo al dispositivo de destino.
- **Ventajas:**
  - Mayor velocidad y eficiencia que los hubs.
  - Segmenta la red, lo que reduce colisiones y mejora el rendimiento.
  - Capacidad para manejar tráfico pesado.
- **Uso:** Redes locales (LAN) de tamaño mediano a grande, donde se requiere un alto rendimiento y una buena gestión del tráfico.

Router (Enrutador)

- **Función:** Conecta múltiples redes y enruta los paquetes de datos entre ellas.
- **Ventajas:**
  - Permite la comunicación entre diferentes redes (LAN, WAN).
  - Realiza funciones de enrutamiento, subneteo y NAT.
  - Proporciona seguridad a través de firewalls.
- **Uso:** Conectar redes domésticas a Internet, conectar diferentes edificios de una empresa, crear redes VPN.

Tabla comparativa

Característica	Hub	Repetidor	Switch	Router
Función principal	Repite señales	Amplía distancia	Conmuta datos	Enruta paquetes
Nivel de operación	Físico	Físico	Enlace de datos	Red
Segmentación de red	No	No	Sí	Sí
Rendimiento	Bajo	Bajo	Medio-alto	Alto
Uso típico	Redes muy pequeñas	Extensión de redes	LANs	Conexión entre redes

Resumen

- **Hubs y repetidores:** Son dispositivos más básicos y se utilizan en redes pequeñas o para extender la distancia de una red.
- **Switches:** Son más avanzados y ofrecen un mejor rendimiento y gestión del tráfico.
- **Routers:** Son esenciales para conectar múltiples redes y proporcionar funciones de enrutamiento y seguridad.

En resumen, la elección del dispositivo dependerá de las necesidades específicas de la red, como el tamaño, el tipo de tráfico y los requisitos de rendimiento.

5- ¿Qué es un protocolo de comunicaciones?

Un protocolo de comunicaciones es un conjunto de reglas, convenciones y estándares que definen la forma en que los dispositivos se comunican entre sí en una red. Es como un idioma que los dispositivos deben hablar para entenderse y transmitir información de manera efectiva.

Imagina una conversación telefónica: existen reglas sobre cómo iniciar y finalizar una llamada, cómo turnarse para hablar y cómo entender el tono de voz. De manera similar, los protocolos de comunicaciones establecen las reglas para que los dispositivos digitales puedan intercambiar datos, desde enviar un correo electrónico hasta transmitir un video en streaming.

¿Por qué son importantes los protocolos de comunicaciones?

- **Estandarización:** Garantizan que diferentes dispositivos, fabricados por distintas empresas, puedan comunicarse entre sí.
- **Eficiencia:** Optimizan el uso de los recursos de la red, asegurando una transmisión de datos rápida y confiable.
- **Seguridad:** Incluyen mecanismos para proteger la información transmitida, evitando accesos no autorizados y garantizando la privacidad.

Ejemplos de protocolos de comunicaciones

- **TCP/IP:** Es uno de los protocolos más utilizados en Internet. Define cómo los datos se dividen en paquetes, cómo se envían y cómo se reensamblan en el destino.
- **HTTP:** Es el protocolo utilizado para la transmisión de información en la World Wide Web. Permite a los navegadores web solicitar y recibir páginas web de servidores.
- **FTP:** Se utiliza para transferir archivos entre computadoras.
- **SMTP:** Es el protocolo utilizado para enviar correos electrónicos.
- **POP3 y IMAP:** Son protocolos utilizados para recibir correos electrónicos.

Niveles de los protocolos de comunicaciones

Los protocolos se organizan en capas, cada una con una función específica:

- **Capa física:** Se encarga de la transmisión de señales eléctricas o ópticas a través del medio físico (cables, fibra óptica, etc.).
- **Capa de enlace de datos:** Se ocupa de la organización de los datos en tramas y de la detección y corrección de errores.
- **Capa de red:** Enruta los paquetes de datos a través de la red.
- **Capa de transporte:** Garantiza la entrega fiable de los datos de una aplicación a otra.
- **Capa de sesión:** Establece, mantiene y termina las conexiones entre aplicaciones.
- **Capa de presentación:** Formatea los datos para que puedan ser interpretados por las aplicaciones.
- **Capa de aplicación:** Proporciona servicios a las aplicaciones de usuario, como HTTP, FTP, SMTP, etc.

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

TCP/IP y NetBIOS: Una Comparativa

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP es la suite de protocolos más utilizada en Internet. Es el lenguaje común que permite a dispositivos de todo el mundo comunicarse entre sí.

- **TCP (Transmission Control Protocol):** Se encarga de la transmisión de datos confiable y ordenada entre dos dispositivos. Divide los datos en paquetes, los numera y los reenvía en caso de pérdida. Garantiza que los datos lleguen al destino en el orden correcto y sin errores.
- **IP (Internet Protocol):** Se encarga del direccionamiento y enrutamiento de los paquetes de datos a través de la red. Cada dispositivo conectado a Internet tiene una dirección IP única que lo identifica.

Características principales de TCP/IP:

- **Orientado a conexión:** Establece una conexión entre dos dispositivos antes de enviar datos.

- **Confiabilidad:** Garantiza la entrega de los datos.
- **Orientado a bytes:** Transmite datos en forma de bytes.
- **Escalabilidad:** Se adapta a diferentes tipos de redes y tamaños.

NetBIOS (Network Basic Input/Output System)

NetBIOS es un protocolo de red diseñado para permitir que las aplicaciones se comuniquen en una red local. Es más antiguo que TCP/IP y tiene algunas limitaciones.

- **Características principales de NetBIOS:**
    - **Orientado a nombre:** Los dispositivos se identifican por nombres en lugar de direcciones IP.
    - **Sin conexión:** No requiere una conexión establecida previamente.
    - **Limitado a redes locales:** No está diseñado para redes de gran escala.
    - **Servicios:** Ofrece servicios de sesión, datagrama y nombre.

Diferencias entre TCP/IP y NetBIOS

Característica	TCP/IP	NetBIOS
Alcance	Global (Internet)	Local (LAN)
Orientación	Conexión	Sin conexión
Direccionamiento	IP	Nombres
Servicios	Transporte, red	Sesión, datagrama, nombre
Escalabilidad	Alta	Baja
Confiabilidad	Alta (TCP)	Baja
Uso actual	Extensamente utilizado en Internet	Menos común, principalmente en redes locales antiguas

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

Estructura de un Paquete de Datos en TCP/IP y los Flags

Estructura General de un Paquete TCP/IP

Un paquete de datos en TCP/IP, también conocido como datagrama, está compuesto por dos partes principales:

1. **Encabezado (Header):** Contiene información de control necesaria para el enrutamiento y la entrega del paquete. Esta información incluye:

    - Dirección IP de origen y destino: Identifica las computadoras que envían y reciben los datos.
    - Protocolo: Indica si el paquete transporta datos TCP, UDP, ICMP, etc.
    - Tiempo de vida (TTL): Limita el número de saltos que puede realizar un paquete para evitar que circule indefinidamente por la red.
    - Suma de comprobación: Permite detectar errores en la transmisión.
    - Fragmentación: Indica si el paquete ha sido dividido en fragmentos más pequeños para adaptarse a las características de la red.
2. **Datos:** Contiene la información real que se está transmitiendo, como el contenido de un correo electrónico, una página web o un archivo.

Los Flags en un Paquete TCP

Los flags son campos de un bit (0 o 1) en el encabezado TCP que proporcionan información adicional sobre el segmento y cómo debe ser procesado por el sistema receptor. Algunos de los flags más comunes son:

- **URG (Urgent):** Indica que parte de los datos en el segmento deben ser entregados lo antes posible.
- **ACK (Acknowledgement):** Confirma la recepción de un segmento.
- **PSH (Push):** Solicita que los datos sean entregados inmediatamente a la aplicación, en lugar de ser almacenados en búferes.
- **RST (Reset):** Restablece una conexión existente o rechaza una solicitud de conexión.
- **SYN (Synchronize):** Se utiliza para iniciar una nueva conexión.
- **FIN (Finish):** Indica que el remitente ha terminado de enviar datos y desea cerrar la conexión.

¿Cómo funcionan los flags?

Los flags trabajan en conjunto para establecer, mantener y finalizar las conexiones TCP. Por ejemplo:

- **Establecimiento de una conexión:** Se intercambian segmentos con los flags SYN y ACK para sincronizar las secuencias y establecer una conexión.
- **Transferencia de datos:** Se utilizan los flags ACK para confirmar la recepción de cada segmento y garantizar la entrega confiable de los datos.
- **Cierre de una conexión:** Se intercambian segmentos con los flags FIN y ACK para finalizar la conexión de manera ordenada.

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

La red, según su geografía, se refiere al alcance físico y la extensión que abarca. Existen varias clasificaciones de redes en función de su cobertura geográfica:

Red de Área Personal (PAN - Personal Area Network):

Cobertura:1 metro a 10 metros

Características:** Es la red más pequeña en términos de cobertura geográfica. Se utiliza para conectar dispositivos personales, como teléfonos móviles, computadoras portátiles, tabletas, auriculares y otros periféricos dentro de un área pequeña. Un ejemplo común es la conexión Bluetooth.

Ejemplo: Conexión entre un teléfono móvil y un auricular Bluetooth.

Red de Área Local (LAN - Local Area Network):

Cobertura: Hasta unos 100 metros (normalmente dentro de un edificio o campus pequeño)

Características:** Es una red limitada a un área geográfica pequeña, como una oficina, un hogar o una escuela. Utiliza cables Ethernet o tecnologías inalámbricas (Wi-Fi). Permite la interconexión de dispositivos como computadoras, impresoras y servidores.

Ejemplo:La red Wi-Fi en una oficina.

Red de Área Metropolitana (MAN - Metropolitan Area Network):

Cobertura: Abarca una ciudad o área metropolitana (varios kilómetros)

Características: Es más grande que una LAN y conecta varias redes LAN en una región geográfica amplia, como una ciudad o un campus universitario grande. Suele ser usada por empresas o instituciones gubernamentales para conectar oficinas o sedes en diferentes partes de una ciudad.

Ejemplo: La red que conecta los campus de una universidad dentro de una ciudad.

Red de Área Amplia (WAN - Wide Area Network):

Cobertura: Abarca países, continentes o incluso todo el mundo.

Características:** Es una red que conecta múltiples redes LAN o MAN a grandes distancias. Utiliza tecnologías como fibra óptica, satélites y cables submarinos para la transmisión de datos. El mejor ejemplo de una WAN es Internet, que conecta redes a nivel global.

Ejemplo: Internet, la red global de comunicaciones.

Red de Área de Campus (CAN - Campus Area Network):

Cobertura: Un grupo de edificios cercanos, como una universidad o un complejo empresarial.

Características: Similar a una LAN, pero abarca un área más amplia, como varios edificios conectados dentro de un campus. Combina redes LAN para permitir la comunicación entre usuarios distribuidos geográficamente en un mismo campus.

Ejemplo:La red interna de una empresa con varias oficinas dentro de un parque tecnológico.

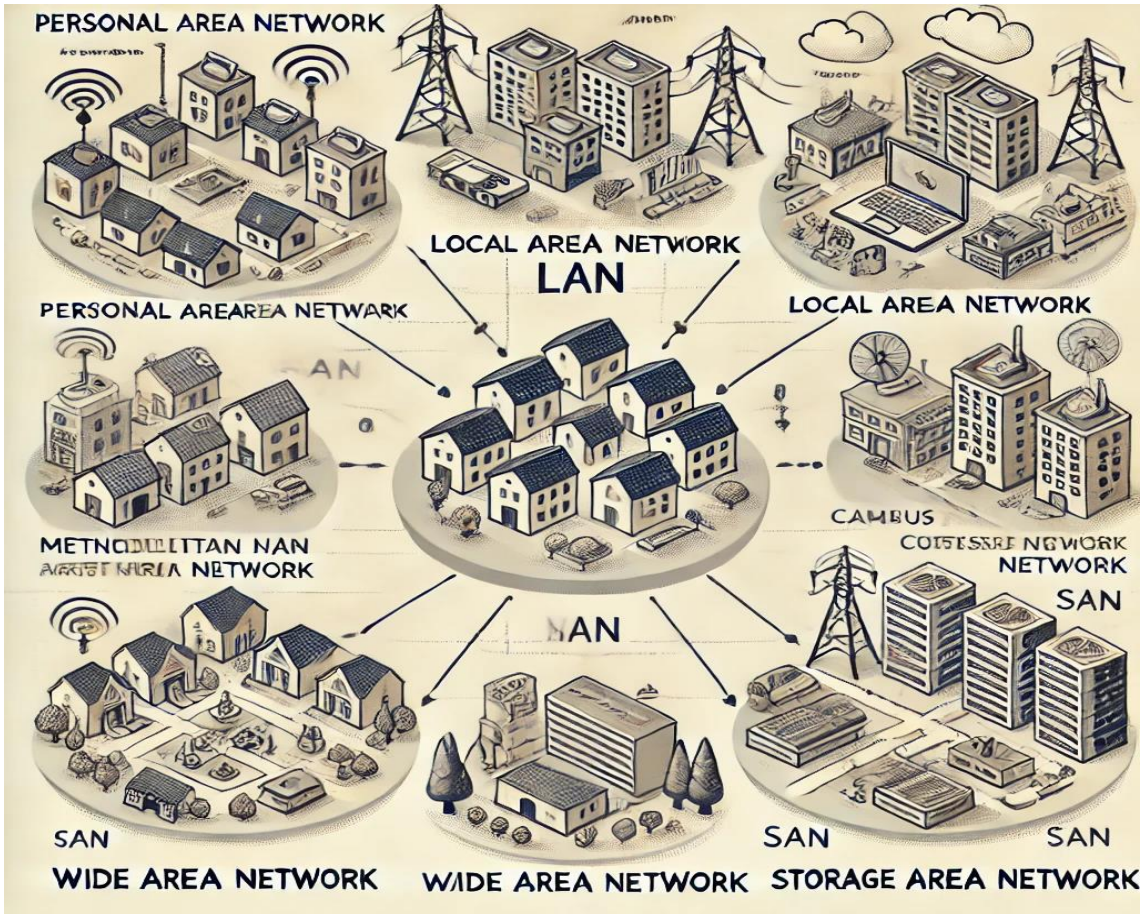
Red de Área de Almacenamiento (SAN - Storage Area Network):

Cobertura Limitada a un entorno empresarial o centro de datos.

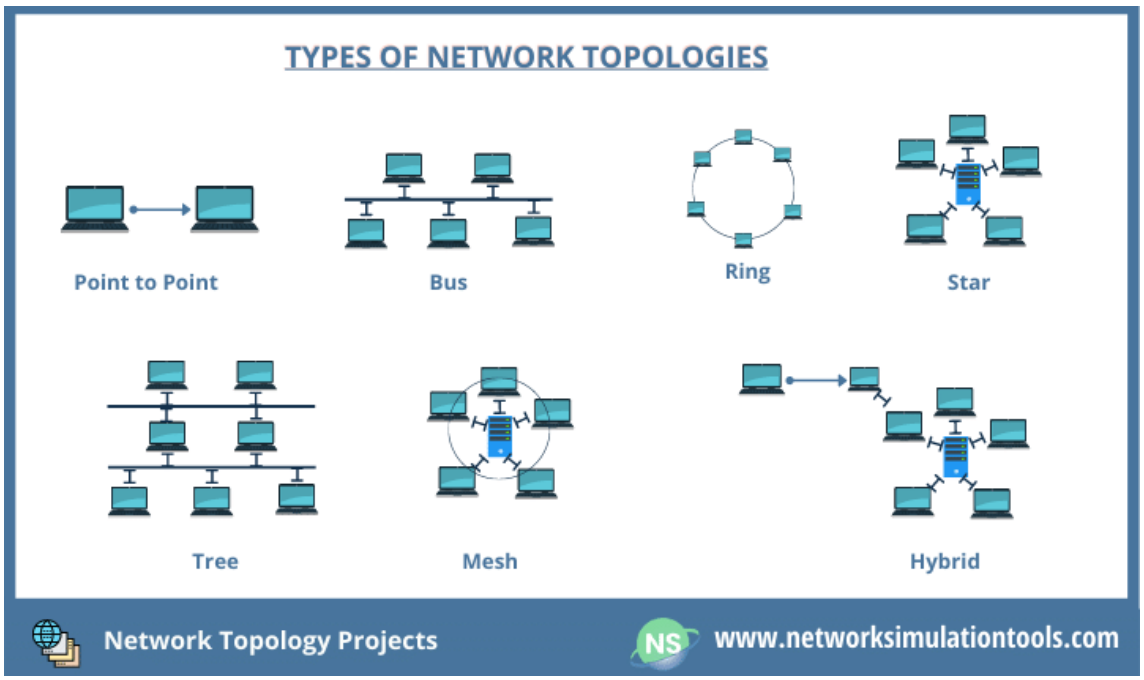
Características: Diseñada específicamente para conectar dispositivos de almacenamiento, como discos duros o servidores, a una red de servidores. Se utiliza principalmente en grandes organizaciones para gestionar el acceso a datos y almacenamiento a alta velocidad.

Ejemplo: La red que conecta los sistemas de almacenamiento en un centro de datos.

Cada una de estas redes tiene características y aplicaciones específicas según el alcance geográfico y los requerimientos de los usuarios o empresas.



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



La **topología de red** describe cómo se organizan y conectan físicamente o lógicamente los dispositivos en una red. Las principales topologías de red incluyen:

1. Topología en Bus:

- **Descripción:** Todos los dispositivos están conectados a un único cable principal o bus, y los datos se transmiten a través de este cable. Cada dispositivo en la red escucha los datos transmitidos, pero solo el destinatario los acepta.
- **Ventajas:** Es económica y fácil de implementar en pequeñas redes.
- **Desventajas:** Si el cable principal falla, toda la red se interrumpe. Además, la eficiencia disminuye a medida que aumenta el tráfico de datos.
- **Ejemplo:** Redes de computadoras en pequeñas oficinas o hogares antiguos.

2. Topología en Estrella (Star):

- **Descripción:** Todos los dispositivos están conectados a un nodo central (como un switch o hub). Los datos se transmiten desde el dispositivo emisor hasta el nodo central, que los reenvía al dispositivo destinatario.
- **Ventajas:** Si un dispositivo falla, no afecta a toda la red. Además, es fácil agregar nuevos dispositivos.
- **Desventajas:** Si el nodo central falla, toda la red deja de funcionar.
- **Ejemplo:** Redes modernas en oficinas o centros educativos.

3. Topología en Anillo (Ring):

- **Descripción:** Cada dispositivo está conectado al siguiente, formando un círculo cerrado. Los datos viajan en un solo sentido (o en ambos en algunas variantes) hasta llegar al dispositivo destinatario.
- **Ventajas:** Todos los dispositivos tienen el mismo acceso al medio de transmisión, lo que puede reducir la colisión de datos.
- **Desventajas:** Si un solo dispositivo o conexión falla, toda la red puede verse afectada.
- **Ejemplo:** Redes Token Ring usadas en algunas redes antiguas.

4. Topología en Malla (Mesh):

- **Descripción:** Cada dispositivo está conectado a múltiples dispositivos, creando múltiples rutas para que los datos lleguen a su destino. Puede ser una malla parcial (algunas conexiones redundantes) o completa (todos los dispositivos están conectados entre sí).
- **Ventajas:** Alta redundancia y confiabilidad, ya que si una conexión falla, los datos pueden tomar una ruta alternativa.
- **Desventajas:** Costosa y difícil de implementar debido a la gran cantidad de cables y conexiones necesarias.
- **Ejemplo:** Redes militares o sistemas de comunicación críticos que requieren alta disponibilidad.

5. Topología en Árbol (Tree):

- **Descripción:** Es una combinación de las topologías en estrella y en bus. Los dispositivos están organizados en una estructura jerárquica, donde pequeños grupos de dispositivos en estrella están conectados a un bus central.
- **Ventajas:** Permite expandir la red de forma sencilla y organizar los dispositivos en grupos.
- **Desventajas:** Si el bus o un nodo principal falla, se puede interrumpir el acceso a varios dispositivos.
- **Ejemplo:** Redes empresariales donde diferentes departamentos están conectados a una red troncal central.

6. Topología Híbrida:

- **Descripción:** Combina dos o más topologías para crear una red que aproveche las ventajas de múltiples configuraciones. Por ejemplo, una red puede utilizar una topología en estrella dentro de un edificio y una topología en anillo para conectar diferentes edificios.
- **Ventajas:** Flexibilidad y optimización, ya que permite diseñar la red según las necesidades específicas.
- **Desventajas:** Puede ser más compleja de administrar y mantener debido a la mezcla de topologías.

- **Ejemplo:** Grandes corporaciones que combinan redes de distintos tipos para adaptarse a diferentes necesidades.

10- Explicar el servicio de DHCP.

DHCP, que significa Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol), es un protocolo de red que automatiza la asignación de direcciones IP a los dispositivos conectados a una red. En lugar de que un administrador de red tenga que configurar manualmente la dirección IP de cada dispositivo, el servidor DHCP se encarga de esta tarea.

DHCP simplifica la gestión de direcciones IP en una red mediante la asignación dinámica de estos parámetros. El proceso básico consta de los siguientes pasos:

Descubrimiento (DHCP Discover):

Cuando un dispositivo (llamado "cliente DHCP") se conecta a una red, envía un mensaje de descubrimiento (broadcast) para encontrar un servidor DHCP. Este mensaje se transmite a todos los dispositivos en la red.

Oferta (DHCP Offer):

El servidor DHCP responde con una oferta que incluye una dirección IP disponible, la máscara de subred, la puerta de enlace (gateway) predeterminada y el tiempo de arrendamiento (lease time). El servidor reserva esta IP para el cliente.

Solicitud (DHCP Request):

El cliente responde al servidor aceptando la oferta de dirección IP enviando un mensaje de solicitud. En este mensaje, el cliente confirma la dirección IP que desea utilizar.

Confirmación (DHCP Acknowledgment):

El servidor DHCP envía un mensaje de confirmación para autorizar el uso de esa dirección IP. A partir de este momento, el cliente puede usar la IP asignada para comunicarse en la red.

Parámetros que el DHCP asigna:

Dirección IP: El número único que identifica al dispositivo en la red.

Máscara de Subred: Define el rango de direcciones IP en la red local.

Puerta de Enlace (Gateway): La dirección IP del router o dispositivo que conecta la red local con otras redes (como Internet).

Servidores DNS: Direcciones IP de los servidores que resuelven nombres de dominio (como "google.com") en direcciones IP.

Tiempo de Arrendamiento (Lease Time): El tiempo que el dispositivo puede usar la dirección IP antes de tener que solicitar una nueva.

Ventajas del DHCP:

Asignación Automática: Facilita la gestión de direcciones IP, eliminando la necesidad de configurar cada dispositivo manualmente.

Eficiencia: Asegura que no haya conflictos de direcciones IP en la red, ya que el servidor se encarga de asignarlas de manera ordenada.

Flexibilidad: Si un dispositivo deja de usar una dirección IP, el servidor DHCP puede reasignarla a otro dispositivo.

Escalabilidad: En redes grandes, el DHCP automatiza la configuración de red, lo que facilita la administración.

Desventajas:

Dependencia del Servidor: Si el servidor DHCP falla, los dispositivos no podrán obtener direcciones IP, lo que puede interrumpir el funcionamiento de la red.

Seguridad: El DHCP no incluye mecanismos de autenticación, por lo que es vulnerable a ciertos ataques (como la suplantación de servidores DHCP, conocido como DHCP spoofing).

Tipos de Asignación DHCP:

Asignación dinámica: Las direcciones IP se otorgan temporalmente (con un lease time) y pueden cambiar tras vencer el tiempo de arrendamiento.

Asignación automática: El servidor asigna direcciones IP de manera permanente, pero el proceso inicial es automático.

Asignación manual o reservada: El administrador reserva una IP específica para un dispositivo basándose en su dirección MAC. Esto es útil para servidores o impresoras que requieren direcciones IP fijas.

11- Explicar el servicio de DNS.

DNS, que significa Sistema de Nombres de Dominio (Domain Name System), es como una guía telefónica gigante para Internet. En lugar de recordar largas secuencias de números (direcciones IP), podemos utilizar nombres fáciles de recordar como www.google.com para acceder a nuestros sitios web favoritos. El DNS se encarga de traducir estos nombres amigables en las direcciones IP que las computadoras entienden.

Funcionamiento del DNS:

1. **Resolución de nombres:**
    - Cuando un usuario escribe un nombre de dominio en su navegador, el sistema no puede acceder directamente al dominio porque los sistemas de red funcionan con direcciones IP (como 192.168.1.1).

- El DNS actúa como una "agenda telefónica" de Internet, buscando la dirección IP asociada al nombre de dominio solicitado para conectar al usuario con el sitio o servicio correcto.

2. **Proceso de resolución DNS:** El proceso de resolución de DNS ocurre en varios pasos:

1. **Consulta al DNS Recursivo:**
    - El navegador envía una consulta a un **servidor DNS recursivo**, que normalmente es proporcionado por el ISP (proveedor de servicios de Internet). Este servidor intenta resolver el nombre de dominio.
2. **Consulta al Servidor Raíz:**
    - Si el servidor recursivo no tiene en caché la dirección IP, realiza una consulta a uno de los **servidores raíz** de DNS (hay 13 servidores raíz en todo el mundo). Los servidores raíz no conocen la dirección IP del dominio, pero indican qué **servidor TLD** (Top-Level Domain) debe consultarse.
3. **Consulta al Servidor TLD:**
    - El servidor TLD (que gestiona dominios de nivel superior como .com, .net, .org) dirige al servidor DNS autoritativo que contiene la información exacta del dominio solicitado.
4. **Consulta al Servidor Autoritativo:**
    - El servidor **autoritativo** tiene la dirección IP exacta del nombre de dominio solicitado y la devuelve al servidor recursivo.
5. **Respuesta al Cliente:**
    - El servidor DNS recursivo devuelve la dirección IP al navegador, que la usa para acceder al servidor web del dominio y mostrar la página solicitada.

Componentes del DNS:

1. **Servidores DNS Recursivos:**
    - Reciben la consulta de los usuarios y, si no tienen la información almacenada en caché, la reenvían a otros servidores para obtener la respuesta.
2. **Servidores Raíz:**
    - Son los servidores más altos en la jerarquía DNS y conocen los servidores de los TLD. Actúan como el punto de partida en la búsqueda de la dirección IP.
3. **Servidores TLD (Top-Level Domain):**
    - Administran los dominios de nivel superior, como .com, .net, .org, etc. Estos servidores saben qué servidores autoritativos contienen la información exacta del dominio.
4. **Servidores Autoritativos:**

- Contienen las direcciones IP exactas de los dominios específicos y proporcionan las respuestas definitivas a las consultas DNS.

5. **Registros DNS:**
    - Los servidores autoritativos tienen diferentes tipos de registros que almacenan información relevante para la resolución de dominios. Algunos de los registros más comunes incluyen:
        - **A Record (Address Record):** Asocia un nombre de dominio con una dirección IPv4.
        - **AAAA Record:** Asocia un nombre de dominio con una dirección IPv6.
        - **CNAME Record (Canonical Name Record):** Redirige un dominio a otro dominio.
        - **MX Record (Mail Exchange Record):** Indica el servidor encargado de recibir correos electrónicos para el dominio.
        - **NS Record (Name Server Record):** Indica los servidores que tienen autoridad para el dominio.

Ventajas del DNS:

1. **Facilita la navegación en Internet:**
    - El DNS permite que los usuarios naveguen usando nombres fáciles de recordar en lugar de números de direcciones IP, haciendo la experiencia de usuario más intuitiva.
2. **Escalabilidad:**
    - El sistema DNS es jerárquico y distribuido, lo que significa que no depende de un solo servidor centralizado, haciendo que sea más resistente y escalable para soportar el crecimiento de Internet.
3. **Caché de DNS:**
    - Los servidores DNS y los dispositivos clientes almacenan en caché (temporalmente) las respuestas DNS, lo que acelera las consultas futuras al evitar resolver el mismo dominio repetidamente.

Desventajas y Vulnerabilidades del DNS:

1. **DNS Spoofing (Suplantación DNS):**
    - Es un tipo de ataque en el que un actor malicioso proporciona una dirección IP falsa en respuesta a una consulta DNS, redirigiendo a los usuarios a sitios fraudulentos.
2. **Dependencia de Servidores DNS:**
    - Si un servidor DNS falla o es atacado (por ejemplo, a través de un ataque DDoS), los usuarios pueden experimentar problemas de acceso a sitios web.

Tipos de DNS:

1. **DNS Público:**
    - Algunos proveedores ofrecen servicios DNS públicos (como Google Public DNS o Cloudflare DNS) que son accesibles para cualquier usuario y a menudo mejoran la velocidad y seguridad de la resolución de nombres.
2. **DNS Privado:**
    - Se utiliza dentro de redes privadas, como en empresas o instituciones, para gestionar internamente la resolución de nombres de dominio en su red local.

12- Explicar las tecnologías Wireless, y sus estándares.

Las tecnologías inalámbricas son aquellas que permiten la comunicación entre dispositivos electrónicos sin la necesidad de cables físicos. Utilizan ondas electromagnéticas para transmitir datos a través del aire, lo que brinda una gran flexibilidad y movilidad.

Principales Tecnologías Wireless:

1. **Wi-Fi (Wireless Fidelity):**
    - **Wi-Fi** es una tecnología de red inalámbrica que permite a los dispositivos (como computadoras, smartphones, tablets, etc.) conectarse a Internet o entre sí dentro de un área limitada.
    - Utiliza ondas de radio en las bandas de frecuencia de **2.4 GHz** y **5 GHz** (y recientemente en 6 GHz con Wi-Fi 6E).
    - Wi-Fi es la base de las redes locales inalámbricas (WLANs), comúnmente usadas en hogares, oficinas, y espacios públicos como aeropuertos y cafés.
2. **Bluetooth:**
    - **Bluetooth** es una tecnología de comunicación inalámbrica de corto alcance diseñada para conectar dispositivos de forma directa, como auriculares, impresoras, relojes inteligentes, y altavoces.
    - Funciona principalmente en la banda de **2.4 GHz** y es ideal para la transmisión de datos a corta distancia (hasta unos 100 metros en su versión más reciente).
    - Bluetooth es muy eficiente en términos de consumo de energía, lo que lo hace ideal para dispositivos portátiles.
3. **NFC (Near Field Communication):**
    - **NFC** es una tecnología inalámbrica de corto alcance (aproximadamente 10 cm) que se utiliza principalmente para intercambiar datos entre dispositivos, como smartphones y terminales de pago.
    - Es la base de sistemas de pago sin contacto como **Apple Pay** o **Google Pay**, y se utiliza en tarjetas de transporte o para emparejar rápidamente dispositivos Bluetooth.

4. **LTE (Long Term Evolution) y 5G:**
    - **LTE** y **5G** son tecnologías inalámbricas de banda ancha móvil que permiten la transmisión de datos a alta velocidad en redes celulares.
    - **LTE (4G):** Proporciona velocidades de descarga que van desde los 100 Mbps hasta 1 Gbps, y es la tecnología dominante en las redes móviles actuales.
    - **5G:** Es la evolución de LTE, con velocidades mucho más altas (hasta 10 Gbps), baja latencia, y mayor capacidad de conectividad simultánea, lo que la hace ideal para aplicaciones emergentes como la **Internet de las Cosas (IoT)**, automóviles conectados y la realidad aumentada/virtual.
5. **WiMAX (Worldwide Interoperability for Microwave Access):**
    - **WiMAX** es una tecnología inalámbrica de banda ancha que permite acceso a Internet de alta velocidad en áreas grandes, similar al LTE, pero con un enfoque más fuerte en redes metropolitanas.
    - Utiliza frecuencias entre **2 GHz y 66 GHz** y puede proporcionar cobertura en áreas rurales y urbanas.
6. **Zigbee:**
    - **Zigbee** es una tecnología inalámbrica diseñada para redes de bajo consumo y corta distancia, utilizada comúnmente en sistemas de **Internet de las Cosas (IoT)**, como domótica, sistemas de iluminación inteligentes y sensores.
    - Opera en la banda de **2.4 GHz**, y su principal ventaja es su eficiencia energética, permitiendo que dispositivos funcionen por largos períodos con baterías de bajo consumo.

Estandares de Tecnologías Wireless:

 Wi-Fi (IEEE 802.11): Es el estándar más utilizado para redes locales inalámbricas (WLAN). Permite conectar dispositivos como computadoras, teléfonos inteligentes, tabletas y otros dispositivos a Internet o entre sí. Existen diferentes versiones de Wi-Fi, cada una con mayor velocidad y capacidad.

- **Wi-Fi 4 (802.11n):** Fue el estándar dominante durante muchos años, ofreciendo velocidades de hasta 600 Mbps.
- **Wi-Fi 5 (802.11ac):** Introdujo velocidades de hasta 3.5 Gbps y una mayor eficiencia.
- **Wi-Fi 6 (802.11ax):** Es el estándar más reciente, ofreciendo velocidades aún mayores, menor latencia y una mejor gestión de múltiples dispositivos conectados.

 Bluetooth: Diseñado para conectar dispositivos a corta distancia, como auriculares, teclados, ratones y dispositivos manos libres. Se utiliza en una amplia variedad de dispositivos y ofrece una conexión estable y de bajo consumo de energía.

 Zigbee: Un estándar de bajo consumo de energía utilizado para conectar dispositivos en redes de sensores inalámbricas. Se utiliza en aplicaciones como domótica, control industrial y monitoreo ambiental.

 LoRaWAN: Desarrollado para redes de área amplia de baja potencia (LPWAN), ideal para aplicaciones como sensores remotos, seguimiento de activos y ciudades inteligentes.

 5G: La quinta generación de tecnología móvil, que ofrece velocidades de datos mucho más altas, menor latencia y una mayor capacidad que las redes 4G. 5G se utiliza principalmente para comunicaciones móviles, pero también se está expandiendo a otras áreas como la Internet de las Cosas (IoT).

Name of the Standard	Went Live	Bands	Max Network Bandwidth	Remarks
802.11be (WiFi 7) Extremely High Throughput (EHT)	Currently in works	2.4 GHz, 5 GHz, and new 6 GHz band	30 Gbps (Theoretically)	• Based on draft 802.11be standard drafted in 2021. • The WiFi 7 standard is backward compatible with 2.4 GHz and 5 GHz devices. • The 6 GHz band yields drastically less interference as compared to the 2.4 and 5 GHz bands.
802.11ax (WiFi 6) High-Efficiency Wireless (HEW)	2019		10 Gbps	• Will replace 802.11ac as a de-facto wireless standard. • Uses less power more reliable in congested environments. • Supports better security.
802.11ac (WiFi 5)	2014	5 GHz band	1300 Mbps (5 GHz Band) 450 Mbps (2.4 GHz Band)	• Uses dual-band wireless technology, supporting simultaneous connections on both 2.4 GHz and 5 GHz WiFi devices. • Most wireless routers are compliant with this standard. • Most expensive to implement.
802.11n (WiFi 4)	2009	2.4 GHz, and 5 GHz bands	600 Mbps	• Uses MIMO technology. • Supports a better range over WiFi standards due to its increased signal intensity. • Significant bandwidth improvement over earlier standards. • More expensive to implement over 802.11g (WiFi 3)
802.11g (WiFi 3)	2002-2003	2.4 GHz bands	Up to 54 Mbps	• Uses the 2.4 GHz range. • Combines best of 802.11a and 802.11b. • 802.11g access points work with 802.11b wireless network adaptors and vice versa. • Least expensive. • Supported by all wireless devices.
802.11a (WiFi 2)	1999	5 GHz band	upto 54 Mbps (5 GHz Band)	• 802.11a and 802.11b use different frequencies and hence are incompatible.
802.11b (WiFi 1)	July 1999	2.4 GHz band	2 Mbps (TCP) 3 Mbps (UDP)	• Unregulated. • An issue with interference from microwave ovens and other appliances using the 2.4 GHz range.

13- ¿Qué es un Proxy?

Un proxy es como un intermediario en Internet. Imagina que quieres comprar algo en una tienda, pero en lugar de ir directamente, pides a un amigo que vaya por ti. Tu amigo sería el proxy en este caso.

En términos técnicos, un servidor proxy es un servidor que actúa como intermediario entre tu dispositivo (computadora, teléfono, etc.) y los servidores de Internet a los que te conectas. Cuando solicitas una página web, la solicitud pasa primero por el servidor proxy, que luego la reenvía al servidor web y te devuelve la respuesta.

El proceso general del proxy es el siguiente:

1. El cliente (usuario) envía una solicitud para acceder a un recurso en Internet, como una página web.
2. La solicitud se envía al servidor proxy.
3. El proxy evalúa la solicitud y decide si la reenvía al servidor final o la bloquea, según las reglas de configuración.
4. Si el proxy permite la solicitud, reenvía la petición al servidor de destino.
5. El servidor de destino responde al proxy con la información solicitada (como el contenido de una página web).

6. El proxy recibe esta información y la envía al cliente.

14- Explicar el protocolo Spanning tree.

El protocolo **Spanning Tree Protocol (STP)** es un protocolo de red diseñado para evitar **bucles (loops)** en una red de área local (LAN) que tiene múltiples caminos redundantes entre switches o puentes. Estos bucles pueden causar que los paquetes de datos circulen indefinidamente, lo que lleva a una congestión de la red, la duplicación de tramas y otros problemas que degradan el rendimiento de la red. **¿Cómo Funciona STP?**

El protocolo STP utiliza el algoritmo **Spanning Tree Algorithm (STA)** para crear una estructura jerárquica libre de bucles en una red. STP selecciona un **switch raíz (root switch)**, desde el cual se calculan los caminos más cortos a todos los demás switches. Solo se mantienen activos los enlaces necesarios para estos caminos, mientras que los enlaces redundantes se colocan en un estado de bloqueo o espera.

Proceso de STP:

1. **Elección del Switch Raíz (Root Bridge):**
    - STP selecciona un switch como el **Switch Raíz** o **Root Bridge**. Este switch es el centro de la red, y todos los demás switches calculan sus caminos más cortos hacia él.
    - El switch raíz se elige en función de su **Bridge ID**, que está compuesto por dos factores: una prioridad y la dirección MAC. El switch con la prioridad más baja se convierte en el root bridge. Si hay empate en la prioridad, el switch con la dirección MAC más baja es seleccionado.
2. **Elección de los caminos más cortos:**
    - Una vez seleccionado el switch raíz, los otros switches determinan la ruta más corta (en términos de costo) hacia el switch raíz. Esta ruta más corta se denomina **Ruta de Coste Mínimo**.
    - El costo de una ruta se basa en el ancho de banda de los enlaces. Enlaces de mayor ancho de banda tienen un costo más bajo (por ejemplo, un enlace de 10 Mbps tiene un costo más alto que un enlace de 1 Gbps).
3. **Asignación de puertos:**
    - STP clasifica los puertos de los switches en varias categorías:
        - **Puerto Raíz (Root Port):** Es el puerto del switch que tiene el camino más corto hacia el switch raíz.
        - **Puertos Designados (Designated Ports):** Son los puertos en un segmento de red que tienen el mejor camino hacia el switch raíz.
        - **Puertos Bloqueados (Blocked Ports):** Puertos que no se usan para evitar bucles. Estos puertos se mantienen en estado de bloqueo y no envían ni reciben tramas de datos, excepto tramas BPDU (Bridge Protocol Data Unit).

4. **Estados de Puertos en STP:**
    - Los puertos pasan por diferentes estados según el protocolo STP:
        - **Bloqueado (Blocked):** No reenvía tráfico, pero escucha BPDU.
        - **Escuchando (Listening):** Escucha tramas BPDU para decidir si el puerto debe permanecer en el estado bloqueado.
        - **Aprendiendo (Learning):** Comienza a aprender direcciones MAC, pero no reenvía tráfico.
        - **Reenvío (Forwarding):** El puerto está activo y puede reenviar tráfico.
        - **Inactivo (Disabled):** No participa en STP ni reenvía tráfico.

Beneficios del Protocolo STP:

1. **Prevención de bucles:**
    - Al bloquear los caminos redundantes, STP garantiza que no se formen bucles en la red, lo que evitaría problemas como la tormenta de transmisión (broadcast storm).
2. **Redundancia:**
    - Aunque STP bloquea algunos caminos, en caso de que el camino principal falle, activa uno de los enlaces redundantes, lo que proporciona **tolerancia a fallos** en la red.
3. **Compatibilidad y Estandarización:**
    - STP está definido en el estándar IEEE **802.1D**, lo que significa que es ampliamente compatible con la mayoría de los switches Ethernet y redes LAN.

Limitaciones de STP:

- **Convergencia lenta:** El proceso de convergencia de STP (el tiempo que tarda en estabilizar la red después de un cambio en la topología) puede ser relativamente lento. Durante el tiempo de convergencia, algunos puertos pueden no reenviar tráfico, lo que afecta temporalmente el rendimiento de la red.
- **Desempeño en redes grandes:** En redes muy grandes y con muchos switches, STP puede no ser lo suficientemente eficiente, ya que fue diseñado para redes LAN más pequeñas.

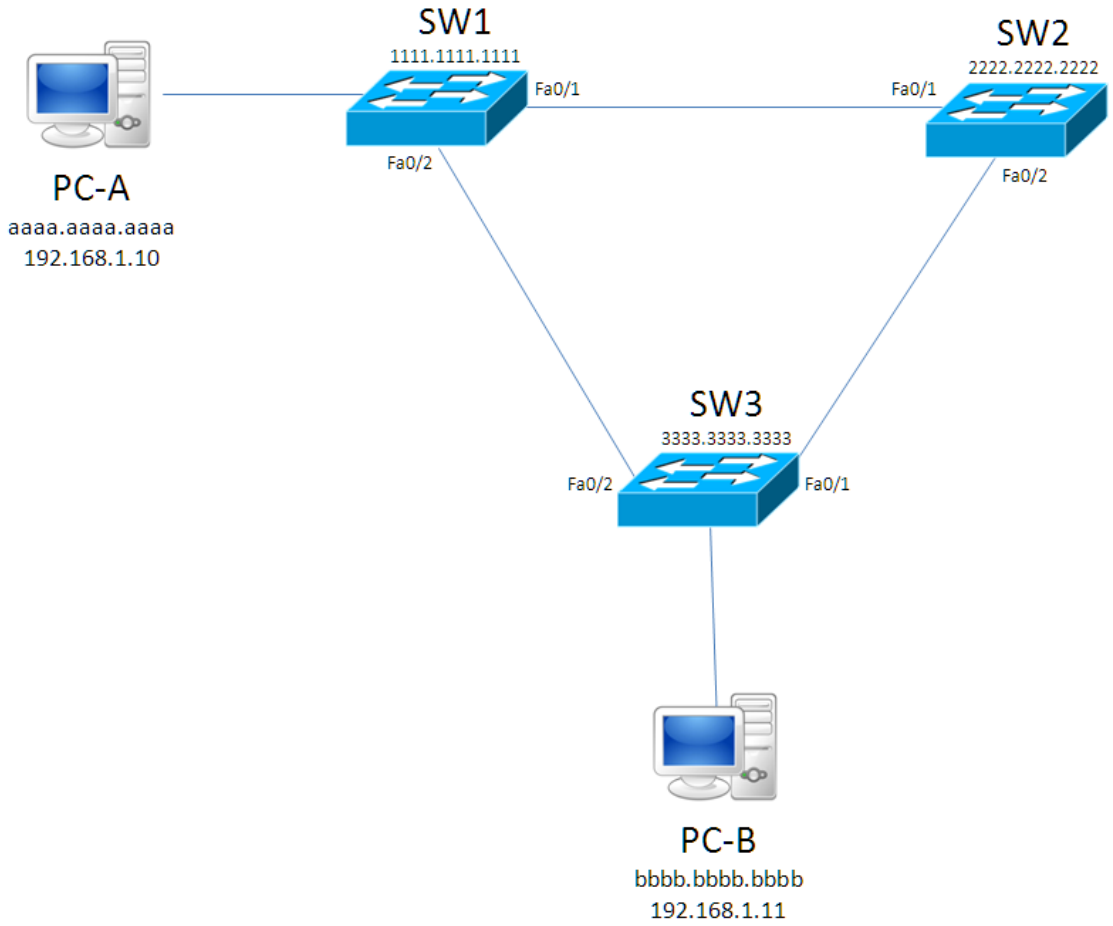
Variantes y Mejoras de STP:

1. **Rapid Spanning Tree Protocol (RSTP) - IEEE 802.1w:**
    - Es una mejora del protocolo STP original que ofrece **convergencia más rápida**. RSTP reduce significativamente el tiempo de convergencia, lo que mejora el rendimiento de la red cuando ocurren fallos o cambios en la topología.
2. **Multiple Spanning Tree Protocol (MSTP) - IEEE 802.1s:**

- Esta variante permite la creación de múltiples árboles de expansión (spanning trees) para diferentes VLANs, lo que mejora el uso de los enlaces en una red con VLANs múltiples.

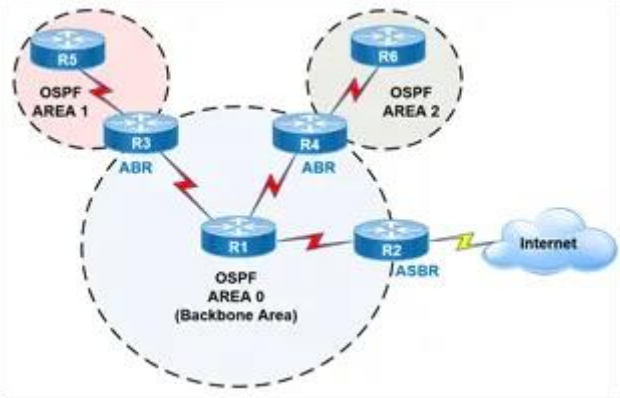
3. **Per VLAN Spanning Tree (PVST):**

- Esta versión del protocolo es específica de Cisco y permite ejecutar un árbol de expansión independiente para cada VLAN, mejorando el uso de los enlaces redundantes.



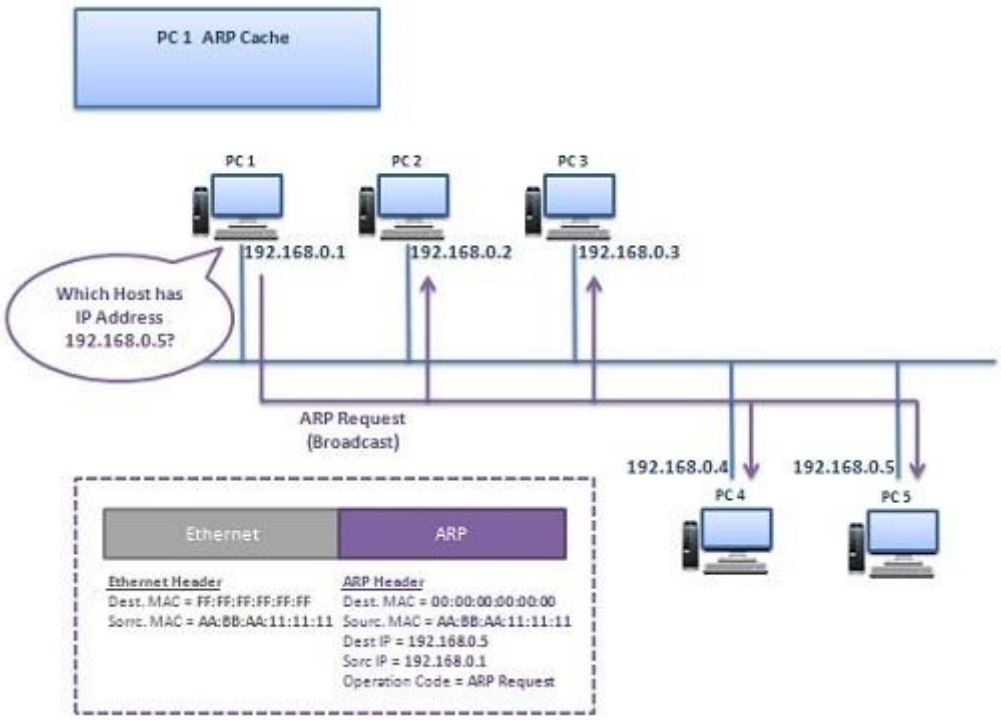
15- Explicar el protocolo de comunicaciones OSPF.

OSPF, que significa *Open Shortest Path First* o "Abrir el camino más corto primero" en español, es un protocolo de enrutamiento de estado de enlace, lo que significa que cada router comparte información detallada sobre sus enlaces con todos los demás routers de la red. Esto permite que los routers calculen la ruta más corta hacia cualquier destino, lo que resulta en una red más eficiente y robusta.



16- Explicar el protocolo ARP.

ARP, o *Address Resolution Protocol*, es un protocolo de comunicaciones de la capa de enlace de datos que se encarga de **traducir direcciones IP a direcciones MAC**.



¿Cómo Funciona ARP?

1. **Solicitud ARP (ARP Request)**:
    - Cuando un dispositivo necesita comunicarse con otro en la misma red local, primero verifica su tabla ARP para ver si ya tiene la dirección MAC correspondiente a la dirección IP del destino.
    - Si no la tiene, envía una solicitud ARP en forma de un paquete broadcast (difusión) a todos los dispositivos en la red. Esta solicitud incluye la dirección IP de destino y la dirección IP y MAC del solicitante.
2. **Respuesta ARP (ARP Reply)**:
    - Todos los dispositivos en la red reciben la solicitud, pero solo el dispositivo cuya dirección IP coincide con la solicitada responderá.

    - Este dispositivo envía una respuesta ARP de vuelta al solicitante, que incluye su dirección MAC.

3. **Actualización de la tabla ARP**:
    - Una vez que el dispositivo solicitante recibe la respuesta, actualiza su tabla ARP con la dirección IP y la dirección MAC del dispositivo de destino, lo que le permite comunicarse directamente en el futuro sin necesidad de volver a hacer una solicitud ARP.

Importancia de ARP

- **Conectividad**: ARP es esencial para que los dispositivos en una red local puedan encontrar y comunicarse entre sí.
- **Eficiencia**: Permite la resolución de direcciones de manera rápida y eficiente, minimizando el tráfico de red innecesario.

Consideraciones de Seguridad

ARP no tiene mecanismos de autenticación, lo que lo hace vulnerable a ataques como el "ARP spoofing", donde un atacante puede enviar respuestas ARP falsas para interceptar el tráfico entre dos dispositivos.

17- ¿Qué es un Firewall?

Un firewall, o cortafuegos, es una herramienta de seguridad de red que actúa como un filtro entre una red interna confiable y redes externas no confiables, como Internet. Su propósito principal es monitorizar y controlar el tráfico de datos entrante y saliente, permitiendo o bloqueando el tráfico según un conjunto de reglas de seguridad predefinidas.

Funcionamiento

 Inspección de paquetes: Examina cada paquete de datos que intenta entrar o salir de tu red.

 Filtrado de tráfico: Permite el paso de tráfico seguro y bloquea el tráfico sospechoso o dañino.

 Aplicación de reglas: Utiliza reglas de seguridad predefinidas para determinar qué tipo de tráfico es permitido o bloqueado.

Tipos de Firewalls:

- **Firewall de hardware:** Un dispositivo físico que se instala en la red.
- **Firewall de software:** Un programa que se ejecuta en tu computadora o dispositivo.
- **Firewall de próxima generación:** Ofrece características avanzadas como la inspección profunda de paquetes y la prevención de intrusiones.

18- ¿Qué es una DMZ?

DMZ (Zona Desmilitarizada) en el contexto de redes es una subred que actúa como una zona intermedia entre una red interna segura y una red externa no confiable, como Internet. Su objetivo principal es aumentar la seguridad de la red al proporcionar una capa adicional de defensa.

1. **Aislamiento**: Los servidores en la DMZ están separados de la red interna, lo que significa que, incluso si un atacante logra comprometer uno de esos servidores, no tiene acceso directo a la red interna.
2. **Servidores públicos**: Comúnmente, en una DMZ se alojan servicios accesibles al público, como servidores web, servidores de correo electrónico y servidores FTP. Esto permite a los usuarios externos interactuar con estos servicios sin exponer la red interna.
3. **Control de acceso**: Se implementan firewalls y otras medidas de seguridad para controlar el tráfico entre la DMZ, la red interna y la red externa. Esto ayuda a filtrar y monitorizar las comunicaciones.
4. **Facilidad de gestión**: Permite una gestión más sencilla de los servidores expuestos a Internet, facilitando actualizaciones y mantenimiento sin afectar la seguridad de la red interna.

Beneficios de una DMZ:

- **Seguridad mejorada**: Al separar los recursos públicos de los privados, se reduce el riesgo de acceso no autorizado.
- **Control granular**: Se pueden aplicar políticas de seguridad más estrictas a la DMZ en comparación con la red interna.
- **Detección de intrusiones**: Puede facilitar la implementación de sistemas de detección y prevención de intrusiones para monitorizar el tráfico que pasa por la DMZ.

19- ¿Qué es un Gateway?

Gateway, o puerta de enlace, es un dispositivo de red que actúa como un punto de acceso entre dos redes diferentes, permitiendo la comunicación y el intercambio de datos entre ellas. Puede ser considerado como un traductor que convierte los protocolos de comunicación de una red a otro.

Características de un Gateway:

1. **Interconexión de redes**: Permite la conexión entre redes que utilizan diferentes protocolos o arquitecturas, como una red local (LAN) y una red amplia (WAN).
2. **Protocolos de comunicación**: Puede traducir diferentes protocolos de comunicación, lo que facilita la interoperabilidad entre sistemas y aplicaciones.
3. **Enrutamiento de datos**: Dirige el tráfico de datos entre las redes, determinando la mejor ruta para la transmisión de información.

4. **Seguridad**: A menudo, los gateways pueden incluir características de seguridad, como firewalls o sistemas de detección de intrusiones, para proteger las redes conectadas.
5. **Funciones adicionales**: Algunos gateways también pueden realizar funciones adicionales, como la conversión de direcciones (por ejemplo, de direcciones IP a direcciones MAC) o la traducción de formatos de datos.

20- Según Microsoft, ¿qué significa NBL?

Según Microsoft, NBL significa "Network Boundary Layer". Es un término que se refiere a una capa de seguridad que define y controla el tráfico entre diferentes redes o segmentos dentro de una arquitectura de red.

Características clave de NLB:

- **Alta disponibilidad:** Al distribuir la carga entre múltiples servidores, se reduce el riesgo de que un fallo en un solo servidor afecte a todos los usuarios.
- **Escalabilidad:** Permite agregar o quitar servidores del clúster para ajustar la capacidad según las necesidades.
- **Fácil configuración:** La configuración de NLB se realiza a través de una interfaz gráfica de usuario o línea de comandos.
- **Compatibilidad con protocolos TCP y UDP:** NLB puede balancear el tráfico de ambos protocolos.

2. NET_BUFFER_LIST:

En el ámbito de los controladores de red de Windows, NBL se refiere a una estructura de datos llamada NET_BUFFER_LIST. Esta estructura contiene información sobre una lista de búferes de red que se utilizan para transportar datos a través de la pila de protocolos de red.

La extensión !ndiskd.nbl en el depurador de Windows permite examinar el contenido de una estructura NBL, lo que puede ser útil para diagnosticar problemas de red.

21- Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT. a. Explique cada uno deestos tipos de enlace. b. Agregue dos tipos de enlaces, no mencionados

anteriormente. c. Ranking de enlaces según lo pedido (de uno a seis, siendo uno

el mejor): Por económico, performance, mayor capacidad, mayor o mejor

configuración de restricciones, soporte a mayor distancia, menor esfuerzo de

configuración. d. Elija un tipo de enlace para los siguientes escenarios: 1 d.

Conectividad de varios de call centers con un data center central. 2 d. Conectar

los datos de los pozos petroleros durante 15 minutos por día. 3 d. Comunicar dos

edificios enfrentados en la misma calle.

Tipos de enlace:

1. **MPLS (Multiprotocol Label Switching)**:
    - Es una técnica de conmutación de paquetes que dirige datos de un nodo a otro basado en etiquetas en lugar de direcciones IP. Permite crear rutas predefinidas y optimizar el tráfico en la red, lo que mejora la velocidad y la eficiencia.
2. **LAN to LAN (Red de Área Local a Red de Área Local)**:
    - Se refiere a la conexión de dos o más redes de área local. Esto puede hacerse a través de enlaces físicos como cables Ethernet o conexiones de fibra óptica, permitiendo la comunicación directa entre dispositivos en diferentes ubicaciones.
3. **Microondas**:
    - Este tipo de enlace utiliza ondas de radio en la banda de microondas para transmitir datos. Es ideal para comunicaciones a larga distancia y se usa frecuentemente en enlaces de comunicación entre torres. Sin embargo, puede ser afectado por obstáculos físicos y condiciones climáticas.

4. **VSAT (Very Small Aperture Terminal)**:
    - Se refiere a estaciones de terminales de muy pequeña apertura que utilizan satélites para transmitir y recibir datos. Se utilizan en áreas remotas donde las conexiones terrestres son inviables. Ofrecen cobertura global, pero la latencia puede ser un problema.

b. Dos tipos de enlaces adicionales:

5. **Fibra óptica**:
    - Utiliza fibras de vidrio o plástico para transmitir datos como pulsos de luz. Ofrece alta capacidad de ancho de banda y es ideal para largas distancias, con baja atenuación y sin interferencias electromagnéticas.
6. **Wi-Fi (Red Inalámbrica)**:
    - Proporciona conectividad inalámbrica a dispositivos dentro de un área determinada. Es conveniente y fácil de implementar, pero tiene limitaciones en alcance y seguridad en comparación con enlaces físicos.

Ranking de enlaces:

Criterio	MPLS	Fibra óptica	Microondas	VSAT	LAN to LAN	Wi-Fi
Económico	4	3	2	5	1	1
Performance	2	1	3	5	4	6
Mayor capacidad	2	1	3	5	4	6
Mejor configuración de restricciones	1	2	3	5	4	6
Soporte a mayor distancia	2	1	3	4	5	6
Menor esfuerzo de configuración	3	5	4	6	1	1

d. Elección de enlace para escenarios:

1. **Conectividad de varios call centers con un data center central**:
    - **Tipo de enlace**: MPLS. Permite una conexión eficiente y segura entre múltiples sitios con calidad de servicio garantizada.
2. **Conectar los datos de los pozos petroleros durante 15 minutos por día**:
    - **Tipo de enlace**: VSAT. Ideal para ubicaciones remotas donde la infraestructura terrestre es limitada.
3. **Comunicar dos edificios enfrentados en la misma calle**:
    - **Tipo de enlace**: Fibra óptica o Microondas. Ambos proporcionan alta capacidad y velocidad para enlaces cortos, pero la fibra óptica ofrece mejor rendimiento y menor interferencia.

22- Describir la tecnología LTE.

LTE (Long-Term Evolution) es una tecnología de telecomunicaciones móviles de cuarta generación (4G) que mejora significativamente la velocidad y eficiencia de las comunicaciones en comparación con las generaciones anteriores (2G y 3G). Diseñada para ofrecer acceso rápido a Internet y servicios multimedia, LTE ha transformado la manera en que los usuarios interactúan con sus dispositivos móviles.

Principales Características de LTE

1. **Alta Velocidad de Datos**:
    - LTE puede alcanzar velocidades de descarga de hasta 300 Mbps y velocidades de subida de hasta 75 Mbps en condiciones óptimas. Esto permite una experiencia fluida en la transmisión de video, navegación web y uso de aplicaciones que requieren gran ancho de banda.
2. **Baja Latencia**:
    - LTE ofrece una latencia reducida, generalmente inferior a 10 ms, lo que mejora la respuesta en aplicaciones en tiempo real, como videoconferencias y juegos en línea.
3. **Eficiencia Espectral**:
    - Utiliza técnicas avanzadas como OFDMA (Orthogonal Frequency Division Multiple Access) para la transmisión de datos en el enlace descendente y SC-FDMA (Single Carrier Frequency Division Multiple Access) en el enlace ascendente, lo que maximiza la utilización del espectro radioeléctrico.
4. **Soporte para Voz sobre LTE (VoLTE)**:
    - LTE permite la transmisión de voz a través de la misma red que los datos, ofreciendo una mejor calidad de llamadas y reduciendo la necesidad de redes separadas para voz.
5. **Compatibilidad con Redes Anteriores**:
    - LTE está diseñado para coexistir con tecnologías de generaciones anteriores, lo que facilita la transición para operadores y usuarios.

23- Explique la solución de Microsoft Teams. Si quieren describir otra solución de otra empresa es también válido.

Microsoft Teams es una plataforma de colaboración y comunicación desarrollada por Microsoft que forma parte de la suite de productividad Microsoft 365. Diseñada para facilitar el trabajo en equipo, Teams combina chat, videoconferencias, almacenamiento de archivos y colaboración en documentos en un solo lugar.

Características Principales

1. **Chat y Mensajería**:
    - Permite conversaciones en tiempo real, tanto en chats individuales como en grupos. Los usuarios pueden enviar mensajes de texto, emojis, GIFs y archivos.
2. **Videoconferencias y Reuniones**:
    - Ofrece capacidades de videoconferencia con soporte para reuniones grandes, presentaciones y grabaciones. También incluye características como compartir pantalla y fondos virtuales.
3. **Integración con Microsoft 365**:
    - Se integra con aplicaciones como Word, Excel, PowerPoint y OneNote, permitiendo la colaboración en documentos en tiempo real sin salir de la plataforma.
4. **Canales y Equipos**:
    - Los usuarios pueden crear equipos y canales dedicados a proyectos específicos, facilitando la organización de conversaciones y recursos.
5. **Aplicaciones y Bots**:
    - Teams permite la integración de aplicaciones de terceros y bots que pueden automatizar tareas y mejorar la productividad.
6. **Seguridad y Cumplimiento**:
    - Ofrece características de seguridad avanzadas, incluyendo autenticación multifactor y cumplimiento de normativas, lo que lo hace adecuado para entornos empresariales.

Beneficios de Microsoft Teams

- **Colaboración Efectiva**: Facilita el trabajo en equipo al centralizar las herramientas de comunicación y colaboración.
- **Flexibilidad**: Permite a los equipos trabajar desde cualquier lugar, lo que es especialmente valioso en entornos de trabajo remoto.
- **Mejora de la Productividad**: La integración con otras herramientas de Microsoft 365 permite a los usuarios realizar múltiples tareas sin cambiar de aplicación.

24- ¿Qué significa aplicar calidad en un enlace MPLS?

Aplicar calidad en un enlace MPLS (Multiprotocol Label Switching) se refiere a la implementación de mecanismos y políticas que aseguran un nivel adecuado de rendimiento y fiabilidad en la transmisión de datos a través de la red. Esto es especialmente importante en entornos donde se manejan aplicaciones críticas que requieren un servicio continuo y de alta calidad.

Aspectos Clave de la Calidad en un Enlace MPLS

1. **Calidad de Servicio (QoS)**:
    - MPLS permite la implementación de políticas de QoS, que clasifican y priorizan el tráfico según su tipo y requisitos. Esto garantiza que aplicaciones sensibles a la latencia, como VoIP o video en tiempo real, reciban el ancho de banda necesario y un tratamiento preferencial.
2. **Control de Congestión**:
    - Se utilizan mecanismos de control para gestionar el tráfico en caso de congestión, evitando la pérdida de paquetes y garantizando que el rendimiento de las aplicaciones críticas no se vea afectado.
3. **Ingeniería de Tráfico**:
    - MPLS permite redirigir el tráfico por rutas optimizadas, evitando enlaces congestionados y equilibrando la carga en la red. Esto contribuye a un uso más eficiente de los recursos de red y mejora la calidad de la conexión.
4. **Monitoreo y Gestión del Rendimiento**:
    - Herramientas de monitoreo permiten evaluar el rendimiento del enlace MPLS en tiempo real, facilitando la identificación y resolución de problemas antes de que afecten a los usuarios.
5. **Segmentación del Tráfico**:
    - La capacidad de crear "flujos" de tráfico diferenciados en MPLS permite segmentar el tráfico por tipos de aplicaciones, usuarios o servicios, lo que contribuye a un mejor control y gestión de la calidad.

Beneficios de Aplicar Calidad en un Enlace MPLS

- **Mejora de la Experiencia del Usuario**: Al garantizar un rendimiento constante, se mejora la satisfacción del usuario final en aplicaciones críticas.
- **Mayor Fiabilidad**: La implementación de QoS y gestión de tráfico reduce la probabilidad de interrupciones y pérdidas de datos.
- **Optimización de Recursos**: Permite una mejor utilización del ancho de banda disponible, evitando el desperdicio y maximizando la eficiencia de la red.

25- ¿Qué diferencias puede encontrar entre una conexión Coaxial, UTP o Fibra?

Diferencias entre Conexiones Coaxial, UTP y Fibra Óptica

Cada tipo de conexión de red tiene sus propias características y se adapta mejor a diferentes escenarios. A continuación, te presento un resumen de las principales diferencias entre las conexiones coaxial, UTP y fibra óptica:

Cable Coaxial

- **Estructura:** Un conductor central de cobre rodeado por un aislante y una malla metálica.
- **Uso:** Originalmente utilizado para televisión por cable, pero también se ha empleado en redes de datos.
- **Ventajas:** Resistente a interferencias, fácil de instalar.
- **Desventajas:** Ancho de banda limitado comparado con otras tecnologías, susceptible a interferencias de alta frecuencia, distancias máximas relativamente cortas.

Cable UTP (Par Trenzado no Blindado)

- **Estructura:** Pares de hilos de cobre trenzados para reducir interferencias.
- **Uso:** Muy común en redes locales (LAN), como Ethernet.
- **Ventajas:** Fácil de instalar, económico, flexible.
- **Desventajas:** Susceptible a interferencias electromagnéticas, distancias máximas limitadas, menor ancho de banda que la fibra óptica.

Fibra Óptica

- **Estructura:** Un núcleo de vidrio o plástico por el que se transmiten pulsos de luz.
- **Uso:** Redes de alta velocidad, largas distancias, aplicaciones que requieren alta seguridad y ancho de banda.
- **Ventajas:** Inmune a interferencias electromagnéticas, alta velocidad, largas distancias, baja atenuación de la señal.
- **Desventajas:** Costo más elevado, instalación más compleja, requiere equipos especializados.

26- Según Cisco, ¿qué significa CCENT, CCNA y CCNP? Descripción breve del Track

1. CCENT (Cisco Certified Entry Networking Technician)

- **Descripción**: CCENT es la certificación inicial de Cisco, diseñada para validar los conocimientos básicos en redes. Es el primer paso para aquellos que buscan desarrollar una carrera en el campo de la tecnología de redes.
- **Enfoque**: La certificación cubre temas fundamentales como el funcionamiento de redes, configuración básica de dispositivos de red y resolución de problemas en redes pequeñas.
- **Track**: CCENT sirve como un trampolín hacia certificaciones más avanzadas, como CCNA.

2. CCNA (Cisco Certified Network Associate)

- **Descripción**: CCNA es una certificación intermedia que demuestra habilidades en la instalación, configuración y resolución de problemas de redes en un entorno empresarial. Es una de las certificaciones más reconocidas en el ámbito de redes.
- **Enfoque**: CCNA cubre temas como redes LAN y WAN, protocolos de enrutamiento y conmutación, seguridad de red y acceso a redes inalámbricas. También se introduce el concepto de redes definidas por software (SDN).
- **Track**: CCNA es un requisito previo para certificaciones más avanzadas, como CCNP, y es ideal para profesionales que buscan roles de nivel medio en redes.

3. CCNP (Cisco Certified Network Professional)

- **Descripción**: CCNP es una certificación avanzada que valida la capacidad de un profesional para planificar, implementar y verificar redes de tamaño mediano a grande. Es un reconocimiento importante para quienes buscan especializarse en tecnologías de red.
- **Enfoque**: La certificación abarca temas avanzados, como enrutamiento, conmutación, soluciones de red seguras y conectividad a través de redes WAN. También incluye aspectos de automatización y programación de redes.
- **Track**: CCNP permite a los profesionales especializarse en diversas áreas, como seguridad, colaboración o servicios en la nube, y es altamente valorada en el sector de TI.

 CCENT: Introducción a las redes, conocimientos básicos.

 CCNA: Fundamentos intermedios, preparación para el entorno empresarial.

 CCNP: Especialización avanzada en redes, preparación para roles profesionales en diseño y gestión de redes complejas.

Routing & Switching y de algún otro a elección (ej. Wireless, Security, Cloud, etc).

1. Routing (Enrutamiento)

- **Descripción**: El enrutamiento es el proceso de dirigir paquetes de datos a través de una red desde el origen hasta el destino, utilizando dispositivos llamados routers. Estos dispositivos determinan la mejor ruta para el tráfico de datos basándose en diversas métricas, como el costo, la latencia y el ancho de banda.
- **Protocolos Comunes**: Algunos protocolos de enrutamiento populares incluyen RIP (Routing Information Protocol), OSPF (Open Shortest Path First) y BGP (Border Gateway Protocol).

2. Switching (Conmutación)

- **Descripción**: La conmutación se refiere al proceso de recibir, procesar y enviar tramas de datos entre dispositivos en una misma red local (LAN). Los switches utilizan

direcciones MAC para filtrar y dirigir el tráfico de manera eficiente, asegurando que los datos lleguen solo al dispositivo de destino.

- **Tipos de Switches**: Existen varios tipos de switches, como switches gestionados (que permiten configuraciones avanzadas) y no gestionados (que funcionan con configuraciones predeterminadas).

Seguridad (Security)

La **Seguridad** en redes se refiere a las prácticas, herramientas y políticas diseñadas para proteger la infraestructura de red y los datos transmitidos de accesos no autorizados, ataques y amenazas.

1. Seguridad de la Red

- **Descripción**: Implica proteger la red y sus dispositivos contra intrusiones y ataques. Esto incluye el uso de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y VPNs (Virtual Private Networks).
- **Mecanismos de Seguridad**: Los firewalls filtran el tráfico entrante y saliente según reglas predefinidas, mientras que las VPNs permiten conexiones seguras y encriptadas a través de redes públicas.

2. Seguridad de Datos

- **Descripción**: Abarca la protección de datos en reposo y en tránsito, utilizando técnicas como cifrado y autenticación. Esto asegura que la información sensible no sea accesible por personas no autorizadas.
- **Prácticas Comunes**: Implementación de políticas de acceso, encriptación de datos y capacitación en concienciación sobre seguridad para los empleados.

27- Explique el modelo OSI.

El **Modelo OSI (Open Systems Interconnection)**, o Modelo de Interconexión de Sistemas Abiertos, es un modelo conceptual que divide la comunicación de datos en redes en siete capas distintas. Cada capa tiene una función específica y se encarga de un aspecto particular del proceso de comunicación.

Las 7 Capas del Modelo OSI:

1. **Capa Física:**
    - Se encarga de la transmisión de bits a través del medio físico (cables, fibra óptica, etc.).
    - Define características eléctricas, mecánicas y funcionales de la conexión física.
    - Ejemplos: conectores, tarjetas de red.
2. **Capa de Enlace de Datos:**
    - Organiza los datos en tramas y se encarga de la transmisión de datos a nivel de enlace.

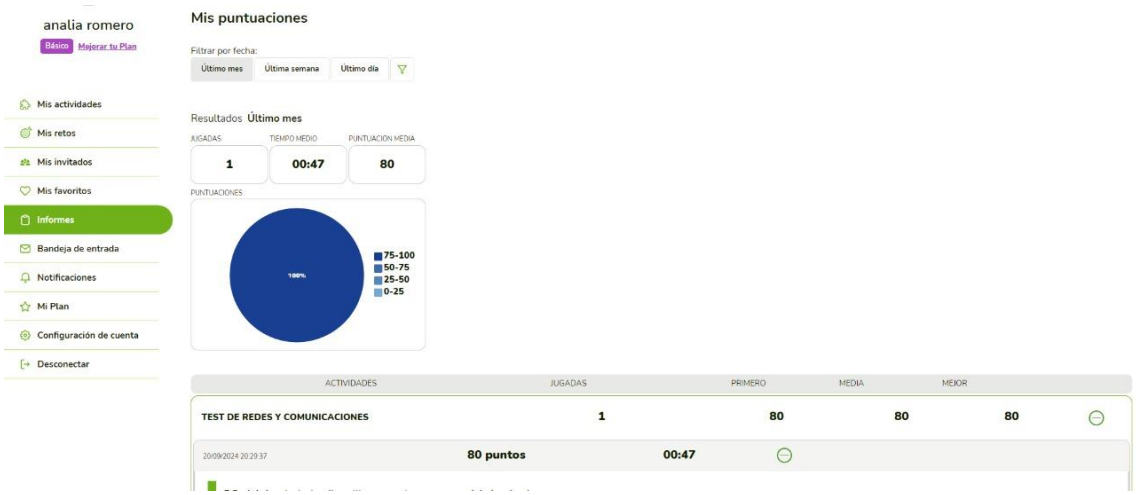
- Detecta y corrige errores en la transmisión.
- Ejemplos: protocolos Ethernet, PPP.

3. **Capa de Red:**
   - Enruta los paquetes de datos a través de la red.
   - Asigna direcciones IP a los dispositivos.
   - Ejemplos: protocolos IP, ICMP.
4. **Capa de Transporte:**
   - Establece, mantiene y termina las conexiones entre los dispositivos.
   - Garantiza la entrega fiable de los datos.
   - Ejemplos: protocolos TCP, UDP.
5. **Capa de Sesión:**
   - Establece, gestiona y termina las sesiones entre aplicaciones.
   - Sincroniza la comunicación y controla el flujo de datos.
   - Ejemplo: protocolo NFS.
6. **Capa de Presentación:**
   - Formatea los datos para que sean comprensibles por la aplicación.
   - Codifica y decodifica los datos.
   - Ejemplos: compresión de datos, cifrado.
7. **Capa de Aplicación:**
   - Proporciona servicios a las aplicaciones del usuario.
   - Define protocolos específicos para diferentes aplicaciones.
   - Ejemplos: HTTP, FTP, SMTP.

28- Realizar cuestionario online y copiar el resultado: (1 por cada integrante)

https://es.educaplay.com/es/recursoseducativos/706834/test_de_redes_y_comunicaciones.htm

Analía Romero



Marcos Gonzalez

29- Explicar el estándar IEEE 802.3 regula la red. Cómo se implementa, ventajas y desventajas.

El estándar IEEE 802.3 define las especificaciones técnicas para las redes Ethernet. Este conjunto de normas establece los protocolos y los medios físicos necesarios para la comunicación entre dispositivos en una red local (LAN).

Ventajas del estándar IEEE 802.3

- **Universalidad:** Es el estándar más utilizado en redes locales, lo que garantiza la interoperabilidad entre equipos de diferentes fabricantes.
- **Flexibilidad:** El estándar ha evolucionado a lo largo de los años para adaptarse a las nuevas tecnologías y ofrecer mayores velocidades de transmisión.

- **Fiabilidad:** Los protocolos Ethernet son robustos y ofrecen una alta fiabilidad en la transmisión de datos.
- **Escalabilidad:** Las redes Ethernet pueden escalarse fácilmente para adaptarse a las necesidades cambiantes de una organización.

Desventajas del estándar IEEE 802.3

- **Complejidad:** El estándar es muy extenso y complejo, lo que puede dificultar su comprensión y configuración para usuarios no especializados.
- **Limitaciones en grandes distancias:** Aunque se han desarrollado tecnologías para extender las distancias de las redes Ethernet, estas pueden tener limitaciones en comparación con otras tecnologías como la fibra óptica.

30- Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4 define la tecnología **Token Bus**, un protocolo de acceso al medio que se utiliza en redes locales (LAN). A diferencia del más común Ethernet (IEEE 802.3), que utiliza un método de acceso al medio basado en colisiones, Token Bus emplea un sistema de token (testigo) para controlar el acceso al medio de transmisión.

Ventajas del Token Bus

- **Sin colisiones:** Al utilizar un token, se evita que múltiples dispositivos intenten transmitir al mismo tiempo, lo que elimina las colisiones típicas de Ethernet.
- **Determinismo:** El tiempo de respuesta es más predecible, ya que cada dispositivo tiene un turno garantizado para transmitir.
- **Eficiencia:** El token asegura que el medio de transmisión se utilice de manera eficiente, evitando tiempos de inactividad.

Desventajas del Token Bus

- **Complejidad:** La implementación y gestión de una red Token Bus es más compleja que una red Ethernet.
- **Costo:** El hardware y software necesarios para implementar Token Bus suelen ser más costosos.
- **Menor popularidad:** Ethernet ha superado en popularidad a Token Bus debido a su simplicidad y mayor flexibilidad.

31- ¿Qué protocolos se usan para enviar y recibir correo?

Para enviar y recibir correos electrónicos, se utilizan varios protocolos que trabajan en conjunto para garantizar la entrega de mensajes a través de Internet. Estos protocolos son fundamentales para el funcionamiento del correo electrónico y se encargan de diferentes aspectos de la comunicación.

Principales Protocolos de Correo Electrónico

- **SMTP (Simple Mail Transfer Protocol):**
    - **Función:** Se utiliza exclusivamente para **enviar** correos electrónicos.
    - **Proceso:** Establece una conexión entre el servidor de correo del remitente y el servidor de correo del destinatario, transfiere el mensaje y luego cierra la conexión.
    - **Características:**
        - Es un protocolo de texto plano.
        - Utiliza comandos como HELO, MAIL FROM, RCPT TO y DATA para indicar el remitente, destinatario y el cuerpo del mensaje.
        - No almacena los mensajes en el servidor de destino.
- **POP3 (Post Office Protocol version 3):**
    - **Función:** Se utiliza para **recibir** correos electrónicos y descargarlos al dispositivo del usuario.
    - **Proceso:** El cliente de correo se conecta al servidor de correo, descarga los mensajes y los elimina del servidor (por defecto).
    - **Características:**
        - Cada mensaje se descarga una sola vez.
        - No permite acceder a los correos desde múltiples dispositivos de forma simultánea.
- **IMAP (Internet Message Access Protocol):**
    - **Función:** También se utiliza para **recibir** correos electrónicos, pero ofrece más funcionalidades que POP3.
    - **Proceso:** Permite acceder a los correos electrónicos desde múltiples dispositivos y sincronizar los cambios entre ellos.
    - **Características:**
        - Los mensajes se almacenan en el servidor de correo.
        - Permite marcar mensajes como leídos, no leídos, eliminados, etc., y estas acciones se sincronizan en todos los dispositivos.
        - Ofrece mayor flexibilidad y control sobre los mensajes.

32- ¿Qué protocolo puede usarse para leer correo recibido?

Los protocolos principales que se utilizan para leer correos electrónicos recibidos son:

- **POP3 (Post Office Protocol version 3):**
    - **Funcionamiento:** Descarga los correos electrónicos del servidor al dispositivo del usuario.
    - **Características:**
        - Los correos se eliminan del servidor una vez descargados, a menos que se configure de otra manera.
        - Ideal para usuarios que desean leer sus correos desde un solo dispositivo y no necesitan acceder a ellos desde múltiples lugares.
- **IMAP (Internet Message Access Protocol):**
    - **Funcionamiento:** Permite acceder a los correos electrónicos almacenados en el servidor desde múltiples dispositivos.
    - **Características:**
        - Los correos se almacenan en el servidor, lo que permite acceder a ellos desde cualquier lugar.
        - Ofrece opciones para marcar correos como leídos, no leídos, eliminados, etc., y sincronizar estos cambios entre dispositivos.
        - Es más flexible y permite una mejor gestión del correo electrónico.

33- Diferencias entre IPV4 e IPV6

IPv4 e **IPv6** son los dos principales protocolos de Internet utilizados para asignar direcciones únicas a dispositivos conectados a una red. Aunque ambos sirven para el mismo propósito, existen diferencias significativas entre ellos, principalmente en términos de tamaño de dirección y capacidad.

Tamaño de la Dirección

- **IPv4:** Utiliza direcciones de 32 bits, lo que se traduce en un número limitado de direcciones IP disponibles (alrededor de 4.300 millones).
- **IPv6:** Emplea direcciones de 128 bits, lo que proporciona un número prácticamente ilimitado de direcciones IP.

Estructura de la Dirección

- **IPv4:** Utiliza una notación decimal con puntos (por ejemplo, 192.168.1.1).
- **IPv6:** Utiliza una notación hexadecimal con dos puntos (por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Resumen

- **Dirección**: IPv4 usa 32 bits, IPv6 usa 128 bits.
- **Exhaustividad**: IPv4 tiene un número limitado de direcciones, IPv6 tiene una cantidad prácticamente ilimitada.

- **Configuración**: IPv4 puede requerir configuración manual; IPv6 permite autoconfiguración.
- **Encabezado**: IPv4 tiene un encabezado más complejo, IPv6 es más simplificado.
- **Seguridad**: IPv4 no integra seguridad por defecto, IPv6 incluye IPsec.
- **Multicast**: IPv4 tiene soporte limitado; IPv6 tiene soporte mejorado.