Trabajo Práctico Teórico - Programación sobre Redes

Integrantes: Elida Sandra Seborga Coca

Juan Sebastian Ruiz Martinez

1 - ¿Qué es una VLAN?

Una **VLAN (Virtual Local Area Network)** es una red lógica que permite segmentar una red física en múltiples dominios de broadcast independientes, mejorando la seguridad, el rendimiento y la gestión de tráfico. Las VLANs se configuran en switches y permiten agrupar dispositivos, aunque no estén conectados físicamente al mismo segmento.

2 - ¿Qué es una VPN?

Una **VPN (Virtual Private Network)** es una tecnología que crea una conexión cifrada y segura a través de una red pública (como Internet), permitiendo acceder a recursos de una red privada de forma remota. Se usa para proteger datos, evitar censura y trabajar de manera segura desde ubicaciones externas.

3 - ¿Qué es una SAN?

Una SAN (Storage Area Network) es una red especializada en almacenamiento que conecta servidores con dispositivos de almacenamiento, permitiendo el acceso rápido y seguro a los datos almacenados.

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

Hub: Dispositivo de conexión que reenvía datos a todos los dispositivos conectados sin filtrar el tráfico.

Repetidor: Dispositivo que amplifica la señal de red para extender su alcance.

Router: Dispositivo que dirige paquetes de datos entre redes diferentes, estableciendo rutas óptimas.

Switch: Dispositivo que conecta dispositivos dentro de una misma red y dirige el tráfico de manera eficiente mediante el uso de direcciones MAC.

5 - ¿Qué es un protocolo de comunicaciones?

Un **protocolo de comunicaciones** es un conjunto de reglas y estándares que definen cómo los dispositivos intercambian información en una red. Ejemplos: TCP/IP (Internet), HTTP (web), FTP (transferencia de archivos).

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

TCP/IP: Conjunto de protocolos que rige la comunicación en Internet, estructurado en capas (Aplicación, Transporte, Internet y Red).

NetBIOS: Protocolo utilizado en redes locales para la comunicación entre equipos mediante nombres en lugar de direcciones IP.

Diferencias: TCP/IP se usa en redes grandes y escalables, mientras que NetBIOS es más común en entornos locales y antiguos.

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

Un paquete TCP/IP tiene cabeceras con información sobre origen, destino, control de errores y datos.

Un "flag" es un bit de control dentro de la cabecera TCP que indica el estado de la conexión.

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

- **PAN** (Personal Area Network): Red personal (ej: Bluetooth).
- **LAN** (Local Area Network): Red local (oficina, casa).
- **MAN** (Metropolitan Area Network): Red urbana (ej: fibra óptica municipal).
- **WAN** (Wide Area Network): Red global (Internet).

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

- **Estrella**: Todos los nodos conectados a un central (ej: switch).
- **Bus**: Un único cable compartido (obsoleto).
- **Anillo**: Nodos en círculo (Token Ring).

- **Malla**: Conexiones redundantes (crítico para redundancia).

10 - Explicar el servicio de DHCP.

Protocolo que asigna automáticamente direcciones IP a dispositivos en una red.

DHCP (siglas de **Dynamic Host Configuration Protocol**) es un **protocolo de red** que sirve para **asignar automáticamente** configuraciones IP a los dispositivos (computadoras, teléfonos, impresoras, etc.) que se conectan a una red.

Cuando un dispositivo se conecta a una red que tiene un servidor DHCP, sucede lo siguiente:

El dispositivo envía una solicitud diciendo básicamente: **"Necesito una dirección IP"**.

El servidor DHCP responde asignándole una IP disponible, junto con otros datos importantes como:

- Máscara de subred
- Puerta de enlace predeterminada (gateway)
- Servidores DNS

Esta configuración tiene un **tiempo de validez** (llamado "lease" o arrendamiento). Cuando este tiempo expira, el dispositivo debe renovar su dirección IP o solicitar una nueva.

11 - Explicar el servicio de DNS.

El **DNS (Domain Name System)** es un sistema jerárquico y distribuido que traduce nombres de dominio (ej: google.com) en direcciones IP (ej: 8.8.8.8), permitiendo a los usuarios acceder a sitios web sin memorizar números.

- **Funcionamiento**:
    1. El cliente pregunta al **resolver DNS** (generalmente el ISP o un servidor como Google DNS).
    2. Si no tiene la respuesta, el resolver consulta los **servidores raíz**, luego los **TLD** (.com, .org) y finalmente el **servidor autoritativo** del dominio.
    3. Devuelve la IP al cliente para establecer la conexión.
- **Importancia**: Sin DNS, navegar por Internet requeriría recordar direcciones IP numéricas.

12 - Explicar las tecnologías Wireless, y sus estándares.

Las tecnologías Wireless se refieren a métodos de comunicación que no utilizan cables físicos para transmitir datos. En lugar de eso, emplean ondas de radio, microondas o infrarrojos. Los estándares más comunes para redes inalámbricas de área local (WLAN) son definidos por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) bajo la familia **IEEE 802.11**, conocida popularmente como **Wi-Fi**.

Algunos de los estándares Wi-Fi más relevantes incluyen:

802.11a: Utiliza la banda de 5 GHz, ofrece buenas velocidades pero menor alcance.

802.11b: Opera en la banda de 2.4 GHz, mayor alcance pero menor velocidad y más susceptible a interferencias.

802.11g: También en 2.4 GHz, mejora la velocidad respecto a 802.11b manteniendo el alcance.

802.11n (Wi-Fi 4): Introduce MIMO (Multiple-Input Multiple-Output) para mejorar la velocidad y el alcance en las bandas de 2.4 GHz y 5 GHz.

802.11ac (Wi-Fi 5): Opera exclusivamente en la banda de 5 GHz, ofreciendo velocidades significativamente mayores que 802.11n.

802.11ax (Wi-Fi 6 y Wi-Fi 6E): Mejora la eficiencia y la velocidad en entornos de alta densidad de dispositivos, operando en las bandas de 2.4 GHz, 5 GHz y 6 GHz (para Wi-Fi 6E).

802.11be (Wi-Fi 7): El estándar más reciente, buscando ofrecer velocidades aún mayores y menor latencia.

Existen otras tecnologías inalámbricas como Bluetooth, Zigbee, Z-Wave (para domótica), LTE/5G (comunicaciones móviles), etc., pero cuando se habla de redes inalámbricas en el contexto más común, se suele referir a la familia 802.11 (Wi-Fi).

13 - ¿Qué es un Proxy?

Un servidor proxy actúa como un intermediario entre un cliente (por ejemplo, tu navegador web) y otro servidor (por ejemplo, el servidor de un sitio web). En lugar de que el cliente se conecte directamente al servidor de destino, la solicitud del cliente va primero al servidor proxy, que luego reenvía la solicitud al servidor de destino. La respuesta del servidor de destino regresa al proxy, y el proxy la reenvía al cliente.

Los proxys pueden tener diversas funciones:

Mejorar el rendimiento: Almacenando en caché contenido web visitado frecuentemente.

Seguridad: Filtrando contenido malicioso o controlando el acceso a ciertos sitios.

Privacidad: Ocultando la dirección IP real del cliente al servidor de destino.

Control de acceso: Restringiendo qué sitios web pueden ser visitados por los usuarios en una red.

14 - Explicar el protocolo Spanning tree.

El protocolo Spanning Tree (STP) es un protocolo de red que opera en la capa 2 (Capa de Enlace de Datos) del modelo OSI. Su propósito principal es prevenir bucles en la red cuando existen rutas redundantes entre switches. Los bucles en una red conmutada pueden causar problemas graves como tormentas de broadcast (tráfico que circula sin fin) y múltiples copias de tramas llegando a su destino, lo que degrada severamente el rendimiento de la red.

STP funciona determinando la ruta "óptima" a través de la red y bloqueando lógicamente los enlaces redundantes que podrían crear un bucle. Lo hace seleccionando un switch raíz y luego calculando la ruta de menor costo desde cada otro switch hacia el switch raíz. Los puertos que forman parte de la ruta de menor costo permanecen activos (reenviando tráfico), mientras que los puertos redundantes se ponen en estado de bloqueo (no reenvían tráfico regular). Existen variaciones de STP como RSTP (Rapid Spanning Tree Protocol) que aceleran el proceso de convergencia cuando hay cambios en la topología de la red.

15 - Explicar el protocolo de comunicaciones OSPF.

OSPF son las siglas de **Open Shortest Path First** (Abrir la Ruta Más Corta Primero). Es un protocolo de enrutamiento interno (**IGP - Interior Gateway Protocol**) de estado de enlace que se utiliza para intercambiar información de enrutamiento dentro de un único sistema autónomo (un conjunto de redes bajo una administración común). OSPF es ampliamente utilizado en redes empresariales y de proveedores de servicios.

A diferencia de los protocolos de enrutamiento por vector distancia (como RIP), OSPF construye un mapa completo (o base de datos de estado de enlace) de la topología de la red en cada router que participa en OSPF. Utiliza el algoritmo Dijkstra para calcular la ruta más corta hacia cada destino basado en métricas

(costos) asignadas a los enlaces. OSPF es eficiente, rápido en la convergencia (adaptarse a cambios en la red) y soporta **VLSM (Variable Length Subnet Masking)**. Divide la red en áreas para mejorar la escalabilidad y reducir la cantidad de información de enrutamiento que cada router necesita mantener.

16 - Explicar el protocolo ARP.

ARP son las siglas de **Address Resolution Protocol** (Protocolo de Resolución de Direcciones). Es un protocolo de capa 2 (o a veces considerada capa 2.5) que se utiliza para **mapear direcciones IP (Capa 3) a direcciones MAC (Capa 2)** dentro de una red local (un mismo segmento de red o subred).

Cuando un dispositivo necesita enviar un paquete IP a otro dispositivo en la misma red local, conoce la dirección IP de destino, pero necesita la dirección MAC de destino para poder encapsular el paquete en una trama Ethernet y enviarla físicamente. Si el dispositivo emisor no tiene la dirección MAC correspondiente a la dirección IP de destino en su tabla ARP, envía un mensaje ARP de "broadcast" a todos los dispositivos en la red local preguntando "¿Quién tiene la dirección IP X.X.X.X? Por favor, dígame su dirección MAC". El dispositivo cuya dirección IP coincide con la solicitada responde con un mensaje ARP de "unicast" que contiene su dirección MAC. El dispositivo emisor recibe esta respuesta, actualiza su tabla ARP con el mapeo IP-MAC y luego puede enviar el paquete IP encapsulado en una trama a la dirección MAC correcta.

17 - ¿Qué es un Firewall?

Un firewall es un sistema de seguridad de red que **monitorea y controla el tráfico de red entrante y saliente** [1] basándose en reglas de seguridad preestablecidas. Actúa como una barrera entre una red interna confiable y redes externas no confiables (como Internet).

La función principal de un firewall es permitir o denegar el paso de paquetes de datos basándose en criterios como:

- Direcciones IP de origen y destino.
- Puertos de origen y destino.
- Protocolos de red (TCP, UDP, ICMP, etc.).
- En firewalls más avanzados (Next-Generation Firewalls - NGFW), pueden inspeccionar el contenido del paquete y basar decisiones en aplicaciones o incluso usuarios.

Los firewalls pueden ser basados en hardware (dispositivos físicos) o software (ejecutándose en un servidor o computadora). Son esenciales para proteger las redes contra accesos no autorizados, ataques maliciosos y la propagación de malware.

18 - ¿Qué es una DMZ?

DMZ son las siglas de **Demilitarized Zone** (Zona Desmilitarizada). En el contexto de redes de computadoras, una DMZ es una **subred física o lógica separada** que se encuentra entre la red interna segura de una organización y la red externa no confiable (Internet).

El propósito de una DMZ es alojar servicios a los que se puede acceder desde Internet (como servidores web, servidores de correo, servidores DNS públicos, VPN gateways) sin exponer directamente la red interna. Un firewall generalmente controla el tráfico entre la DMZ y la red interna, y otro firewall (o reglas diferentes en el mismo firewall) controla el tráfico entre la DMZ e Internet.

De esta manera, si un servidor en la DMZ es comprometido, el atacante solo tendrá acceso a la DMZ y no directamente a la red interna donde se almacenan datos sensibles. Es una capa adicional de seguridad.

19 - ¿Qué es un Gateway?

En redes de computadoras, un gateway (puerta de enlace) es un dispositivo de red que **conecta dos redes diferentes que utilizan protocolos de comunicación distintos**. Su función principal es permitir que los datos fluyan de una red a otra.

El gateway más común en un entorno doméstico o de oficina es el **router**. El Router actúa como gateway entre la red local (tu red doméstica o de oficina) e Internet. Cuando envías tráfico desde tu computadora (en la red local) hacia un destino en Internet, el tráfico se envía primero al gateway (el router), que luego lo dirige hacia su destino en Internet.

En un sentido más amplio, un gateway puede ser cualquier dispositivo que realice una traducción de protocolos o formatos de datos para permitir la comunicación entre redes dispares.

20 - Según Microsoft, ¿qué significa NBL?

Según la documentación de Microsoft, **NBL** significa **NET_BUFFER_LIST**.

NET_BUFFER_LIST es una estructura de datos fundamental utilizada en el **Network Driver Interface Specification (NDIS)** de Microsoft. NDIS es una interfaz de programación de aplicaciones (API) para adaptadores de red que permite que los drivers de red se comuniquen con el sistema operativo.

Una NET_BUFFER_LIST describe una lista vinculada de estructuras NET_BUFFER. Cada estructura NET_BUFFER describe datos de red (una parte de una trama o paquete). Por lo tanto, una NET_BUFFER_LIST puede representar uno o varios paquetes de red que están siendo procesados por los drivers de red. Es una estructura clave para la gestión eficiente del tráfico de red en el kernel de los sistemas operativos Windows.

21 - Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT. a. Explique cada uno de estos 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.

a. Explicación de los tipos de enlace:

1. **MPLS (Multiprotocol Label Switching):**
    - **Concepto:** No es un tipo de medio físico como tal, sino una tecnología de reenvío de paquetes que opera entre la Capa 2 (Enlace de Datos) y la Capa 3 (Red) del modelo OSI. Utiliza "etiquetas" para dirigir el tráfico a través de una red (típicamente la de un proveedor de servicios), en lugar de depender únicamente de las tablas de enrutamiento IP.
    - **Características:** Permite crear rutas virtuales (LSPs - Label Switched Paths), facilita la implementación de Calidad de Servicio (QoS) para priorizar tráfico (como voz o video), soporta redes privadas virtuales (VPNs) de forma nativa y es escalable.
    - **Uso:** Ampliamente utilizado por proveedores de servicios para construir redes troncales (backbones) y ofrecer servicios VPN a empresas que necesitan interconectar múltiples sucursales de forma segura y con garantía de rendimiento.

2. **LAN to LAN:**
    - **Concepto:** Este término se refiere a la **conectividad entre dos redes de área local (LANs) separadas geográficamente**. No describe una tecnología de enlace *específica*, sino la *función* o *aplicación* de interconectar dos LANs. La implementación de un enlace LAN-to-LAN puede hacerse utilizando diversas tecnologías subyacentes, como líneas dedicadas (fibra, cobre), MPLS, o VPNs sobre Internet pública.
    - **Características:** El objetivo es que los dispositivos en una LAN puedan comunicarse de forma transparente con dispositivos en la otra LAN, como si estuvieran en la misma red (aunque a menudo a través de routers o firewalls). Las características de rendimiento, seguridad y costo dependen completamente de la tecnología específica utilizada para realizar la interconexión.
    - **Uso:** Interconexión de sedes, sucursales, centros de datos, etc.
3. **Microonda (Microwave):**
    - **Concepto:** Un tipo de enlace de comunicación inalámbrica que utiliza ondas de radio en el rango de frecuencia de las microondas.
    - **Características:** Requiere línea de vista directa (Line-of-Sight - LOS) entre las antenas transmisora y receptora. Puede ofrecer altas capacidades de ancho de banda (cientos de Mbps a varios Gbps) y tiene una latencia relativamente baja. La instalación es más rápida que la de fibra física, pero es susceptible a condiciones climáticas severas (lluvia, nieve) que pueden degradar la señal (rain fade). El alcance está limitado por la curvatura de la tierra y obstáculos.
    - **Uso:** Conectar edificios cercanos donde el tendido de cable es difícil o costoso, como respaldo de enlaces cableados, o para cubrir la "última milla" en áreas donde la infraestructura alámbrica es limitada.
4. **VSAT (Very Small Aperture Terminal):**
    - **Concepto:** Un sistema de comunicación vía satélite que utiliza antenas parabólicas pequeñas (generalmente de menos de 3 metros de diámetro). Se comunican con un satélite geoestacionario, que a su vez se comunica con una estación terrestre central (teleport) conectada a la red principal (ej. Internet).

- **Características:** Ofrece cobertura en áreas remotas donde otras infraestructuras de comunicación no existen o son poco fiables. Sin embargo, generalmente ofrece ancho de banda limitado, tiene una latencia muy alta (debido a la gran distancia a la que se encuentran los satélites geoestacionarios) y es susceptible a las condiciones climáticas.
- **Uso:** Conectividad en ubicaciones rurales o aisladas (plataformas petrolíferas, minas, bases remotas), comunicaciones de emergencia, respaldo para enlaces terrestres.

b. Dos tipos de enlaces adicionales:

1. **Fibra Óptica (Fiber Optic):**
   - **Concepto:** Un medio de transmisión física que utiliza hilos finos de vidrio o plástico (fibras) para transmitir datos en forma de pulsos de luz.
   - **Características:** Ofrece el mayor ancho de banda potencial y permite la transmisión de datos a muy altas velocidades (desde cientos de Mbps hasta Terabits por segundo). Tiene baja latencia, es inmune a la interferencia electromagnética y permite la transmisión a distancias muy largas (varios kilómetros sin necesidad de repetidores, y mucho más con ellos). La principal desventaja es el costo y la dificultad de la instalación física (excavación, tendido, terminación).
   - **Uso:** Redes troncales (backbones), enlaces de larga distancia, conexiones de alta capacidad entre centros de datos, conectividad de alta velocidad para empresas y hogares (FTTH).
2. **Celular (LTE/5G):**
   - **Concepto:** Utiliza la infraestructura de redes de telefonía móvil para proporcionar conectividad a Internet (LTE, 5G).
   - **Características:** Es inalámbrico, relativamente fácil de desplegar (si hay cobertura), y ofrece movilidad. Las velocidades varían enormemente dependiendo de la generación de la tecnología (LTE es 4G, 5G es más rápido), la calidad de la señal, la distancia a la torre y la congestión de la red. La latencia es generalmente mayor que la de enlaces cableados. Opera bajo un modelo de suscripción.

- **Uso:** Conectividad para dispositivos móviles, respaldo para enlaces fijos, conectividad en ubicaciones temporales o de difícil acceso para infraestructura fija, IoT (Internet de las Cosas).

c. Ranking de enlaces (1 a 6, siendo 1 el mejor):

Ranking general basado en las características típicas de cada tipo de enlace. Es importante notar que el "mejor" puede variar mucho según las necesidades específicas (costo vs. rendimiento vs. distancia).

Criterio	1 (Mejor)	2	3	4	5	6 (Peor)
Económico (Costo Total)	**Celular**	**LAN to LAN***	**VSAT**	**MPLS**	**Microonda**	**Fibra Óptica**
Performance	**Fibra Óptica**	**Microonda**	**LAN to LAN***	**MPLS**	**Celular**	**VSAT**
Mayor Capacidad	**Fibra Óptica**	**Microonda**	**LAN to LAN***	**MPLS**	**Celular**	**VSAT**
Mejor Configuración Restricciones	**MPLS**	**LAN to LAN***	**Fibra Óptica**	**Microonda**	**Celular**	**VSAT**
Mayor Distancia	**VSAT**	**MPLS**	**Celular**	**LAN to LAN***	**Fibra Óptica**	**Microonda**
Menor Esfuerzo Configuración	**Celular**	**VSAT**	**LAN to LAN***	**MPLS**	**Microonda**	**Fibra Óptica**

*Nota sobre LAN to LAN: Su ranking exacto depende de la tecnología subyacente utilizada para implementarlo (fibra, cobre, etc.). Aquí se asume una conexión dedicada punto a punto típica.

Justificación del Ranking:

- **Económico:** Celular puede ser el más barato para bajo uso. VSAT y Microonda tienen altos costos iniciales pero variables de operación. Fibra tiene un costo de instalación muy alto si no está presente, pero el costo por bit puede ser bajo a gran escala. MPLS y Dedicated LAN-to-LAN son servicios gestionados, su costo depende del ancho de banda y SLA.

- **Performance/Capacidad:** Fibra lidera en potencial de ancho de banda y baja latencia. Microonda le sigue de cerca pero con limitaciones de LOS y clima. Dedicated/MPLS ofrecen rendimiento garantizado pero limitado por la capa física subyacente. Celular y VSAT son generalmente inferiores en performance y capacidad, con VSAT teniendo la peor latencia.
- **Configuración de Restricciones:** MPLS está diseñado para políticas de tráfico y QoS. Los demás enlaces son principalmente medios de transporte; la configuración de restricciones se realiza en los equipos terminales (routers, firewalls).
- **Distancia:** VSAT tiene alcance global. MPLS y los servicios de carrier (como los usados en LAN-to-LAN dedicado) cubren grandes distancias. Celular cubre áreas con infraestructura. Fibra y Microonda tienen limitaciones físicas de distancia para enlaces punto a punto (aunque la fibra puede extenderse con repetidores en redes de carrier).
- **Esfuerzo de Configuración:** Celular requiere mínima configuración del usuario. VSAT a menudo es gestionado por el proveedor. Dedicated y MPLS requieren configurar equipos de borde. Microonda y Fibra requieren instalación física y alineación/terminación precisa.

d. Elección de tipo de enlace para escenarios:

1. **Conectividad de varios call centers con un data center central:**
    - **Elección: MPLS**.
    - **Justificación:** MPLS es ideal para interconectar múltiples sitios (los call centers) a un punto central (el data center). Permite implementar QoS de manera efectiva para priorizar el tráfico de voz (VoIP) y datos sensibles de los call centers, garantizando un rendimiento predecible y seguro sobre la red del proveedor.
2. **Conectar los datos de los pozos petroleros durante 15 minutos por día:**
    - **Elección: VSAT** o **Celular**.
    - **Justificación:** Los pozos petroleros suelen estar en ubicaciones muy remotas donde la infraestructura cableada es inexistente. **VSAT** es una solución fiable para ubicaciones aisladas, aunque su latencia es alta, para una transmisión de datos diaria de 15 minutos, es aceptable. **Celular** es una alternativa viable y potencialmente más económica *si y solo si* hay cobertura de red móvil suficiente en la ubicación del pozo y el plan de datos soporta el volumen de información a transmitir. Dada la naturaleza

remota, VSAT es a menudo la opción por defecto, pero Celular debe evaluarse si la cobertura lo permite.

3. **Comunicar dos edificios enfrentados en la misma calle:**
    - **Elección: Fibra Óptica** o **Microonda**.
    - **Justificación:** Para una distancia tan corta, ambas son excelentes opciones para proporcionar alto ancho de banda. **Fibra Óptica** es ideal si se necesita la máxima capacidad y menor latencia, y si es factible tender el cable bajo la calle. **Microonda** es una excelente alternativa si tender fibra es prohibitivamente costoso o complicado (ej. permisos difíciles), siempre y cuando haya línea de vista clara entre los edificios. Una conexión **LAN to LAN dedicada** (usando fibra o cobre si es una distancia muy corta) a través de un carrier también es una opción, pero directa Fibra/Microonda puede ofrecer más control y/o ser más económica a esta distancia.

22 - Describir la tecnología LTE.

LTE (Long-Term Evolution) es un estándar de comunicación inalámbrica de banda ancha para dispositivos móviles. Aunque a menudo se comercializa como "4G LTE", técnicamente representa una evolución significativa sobre las tecnologías 3G anteriores y sirve como un paso intermedio hacia 5G.

Sus características principales incluyen:

- **Mayor Velocidad:** Ofrece velocidades de descarga y subida considerablemente más altas que 3G, permitiendo una mejor experiencia para navegación web, streaming de video, descargas rápidas, etc.
- **Menor Latencia:** Reduce el tiempo de retardo en la comunicación, lo que mejora el rendimiento de aplicaciones en tiempo real como juegos online o videollamadas.
- **Red Totalmente IP:** A diferencia de las redes 3G que aún tenían componentes basados en circuitos, la arquitectura de red de LTE es completamente basada en Protocolo de Internet (IP), lo que simplifica la infraestructura y soporta mejor la convergencia de servicios.
- **Uso Eficiente del Espectro:** Utiliza técnicas de modulación avanzadas como OFDMA (Orthogonal Frequency-Division Multiple Access) y SC-

FDMA (Single-Carrier Frequency-Division Multiple Access) para hacer un uso más eficiente del espectro radioeléctrico disponible.

- **Soporte a la Movilidad:** Está diseñado para mantener la conectividad de alta velocidad incluso cuando el dispositivo se mueve a velocidades considerables.

En resumen, LTE es la tecnología que hizo posible la era moderna del smartphone con acceso rápido a datos, video de alta definición y una variedad de aplicaciones online que requieren buen ancho de banda y baja latencia en movilidad.

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 unificada** desarrollada por Microsoft. Está diseñada para ser el centro de trabajo en equipo, integrando diversas herramientas y servicios en una sola aplicación.

Sus funcionalidades clave incluyen:

- **Chat Persistente:** Permite conversaciones de texto en tiempo real, tanto individuales como en grupos (llamados "equipos" o "canales"). El historial del chat es persistente, lo que facilita seguir conversaciones.
- **Videoconferencias y Llamadas de Voz:** Permite realizar reuniones de video y llamadas de voz, tanto programadas como instantáneas, con funcionalidades como compartir pantalla, fondos virtuales, grabación, etc.
- **Almacenamiento y Colaboración de Archivos:** Cada equipo y canal tiene un espacio de almacenamiento integrado (basado en SharePoint y OneDrive) donde los miembros pueden subir, compartir y co-editar documentos de forma simultánea utilizando las aplicaciones de Microsoft 365 (Word, Excel, PowerPoint).
- **Integración de Aplicaciones:** Permite integrar una amplia variedad de aplicaciones de Microsoft y de terceros directamente en la interfaz de Teams, lo que centraliza el flujo de trabajo (ej. Planner para gestión de tareas, Trello, Asana, etc.).
- **Reuniones Grandes y Seminarios Web:** Soporta reuniones con un gran número de participantes y funcionalidades específicas para seminarios web (webinars).

Teams busca reemplazar o complementar otras herramientas como el correo electrónico para conversaciones rápidas y compartir archivos, y ofrecer una alternativa a otras plataformas de videoconferencia. Es una solución central para la comunicación y la productividad en entornos empresariales y educativos.

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

Aplicar calidad en un enlace MPLS se refiere a implementar **Calidad de Servicio (QoS - Quality of Service)** sobre la red MPLS. Significa configurar la red para **priorizar ciertos tipos de tráfico** sobre otros y **garantizar un nivel de rendimiento predecible** para las aplicaciones críticas.

En una red MPLS, el tráfico de diferentes aplicaciones (voz, video, datos transaccionales, navegación web, backups) puede viajar a través de los mismos enlaces. Sin QoS, todo el tráfico recibe el mismo tratamiento y, en momentos de congestión, aplicaciones sensibles como la voz o el video pueden experimentar problemas (interrupciones, eco, pixelación) debido a la latencia, el jitter (variación de la latencia) y la pérdida de paquetes.

Con QoS en MPLS:

1. El tráfico se **clasifica** en diferentes categorías (ej. Tráfico de voz, tráfico de video, tráfico de datos prioritario, tráfico de datos estándar).
2. A cada categoría se le asigna un **nivel de prioridad** y, potencialmente, un **ancho de banda garantizado** o preferencial.
3. Los routers (Label Switching Routers - LSRs) dentro de la red MPLS utilizan las etiquetas MPLS (o campos de encabezado como DSCP) para identificar la categoría de tráfico.
4. En caso de congestión, los routers **priorizan el reenvío** del tráfico de alta prioridad sobre el de baja prioridad, y pueden utilizar mecanismos de cola y modelado de tráfico para asegurar que cada categoría reciba el tratamiento configurado.

En resumen, aplicar calidad en un enlace MPLS significa usar las capacidades de la tecnología MPLS (etiquetas, gestión de rutas, mecanismos de QoS) para asegurar que las aplicaciones más importantes (como la voz o las aplicaciones críticas de negocio) tengan el rendimiento (baja latencia, bajo jitter, ancho de banda suficiente) que necesitan, incluso cuando la red está congestionada.

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

Las principales diferencias radican en el material conductor, el método de transmisión, el rendimiento (ancho de banda y distancia), el costo y la inmunidad a interferencias:

Característica	Cable Coaxial	Cable UTP (Par Trenzado No Blindado)	Fibra Óptica
Material Conductor	Cobre (conductor central) y Cobre/Aluminio (malla)	Cobre	Vidrio o Plástico (fibras)
Método Transmisión	Señales Eléctricas	Señales Eléctricas	Pulsos de Luz
Ancho de Banda	Moderado (depende del tipo, ej. cientos de Mbps)	Variable (depende de la Categoría, ej. 100 Mbps a 40 Gbps)	Muy Alto (desde Gbps hasta Terabits por segundo)
Distancia Típica	Decenas/Cientos de metros (para redes)	Hasta 100 metros para altas velocidades	Cientos de metros a Kilómetros (depende del tipo y equipo)
Inmunidad a EMI/RFI	Moderada (por el blindaje)	Baja a Moderada (depende del trenzado y categoría)	Muy Alta (Inmune)
Costo del Cable	Moderado	Bajo (especialmente Cat 5e/6)	Alto
Costo del Equipamiento	Moderado	Bajo	Alto (transceptores ópticos)
Facilidad de Instalación	Moderada	Alta (flexible, conectores RJ45 comunes)	Baja (rígido, conectores y terminación especializada)
Usos Comunes	Cable TV, Redes antiguas (ThinNet/ThickNet)	Redes Ethernet cableadas (LANs), Telefonía	Redes troncales, Larga distancia, Alta velocidad, FTTH

- **UTP** es el más común y económico para redes locales hasta 100m, usando señales eléctricas.
- **Coaxial** es menos común ahora en LANs pero usado para TV por cable, ofrece algo de blindaje.
- **Fibra Óptica** es la mejor en rendimiento (velocidad, distancia, inmunidad), pero la más cara y difícil de instalar, usando luz para transmitir datos.

26 - Según Cisco, ¿qué significa CCENT, CCNA y CCNP? Descripción breve del Track Routing & Switching y de algún otro a elección (ej. Wireless, Security, Cloud, etc).

Cisco Systems tiene un programa de certificaciones reconocido globalmente para profesionales de redes. Las siglas que mencionas corresponden a diferentes niveles dentro de este programa.

- **CCENT (Cisco Certified Entry Networking Technician):** (Certificación Retirada por Cisco). Era el nivel de entrada. Validaba conocimientos básicos sobre instalación, operación y soporte de una pequeña red de sucursal, incluyendo seguridad de red básica. Era a menudo el primer paso hacia la certificación CCNA.
- **CCNA (Cisco Certified Network Associate):** Nivel Asociado. Es una certificación fundamental que valida conocimientos y habilidades más amplios sobre tecnologías de red, incluyendo fundamentos de red, acceso a red, conectividad IP, servicios IP, fundamentos de seguridad, automatización y programabilidad. Desde 2020, hay un solo examen CCNA que cubre un rango más amplio de temas que los CCNA anteriores específicos de tecnología.
- **CCNP (Cisco Certified Network Professional):** Nivel Profesional. Es un nivel más avanzado que valida habilidades y conocimientos profundos en un área de tecnología de red específica. Para obtener un CCNP, generalmente se debe pasar un examen "Core" (central) y un examen de "Concentración" (especialista) dentro de una tecnología determinada.

Descripción de Tracks (Enfoques Tecnológicos):

- **Track Routing & Switching (Enfoque Clásico, ahora parte de Enterprise):** Históricamente, este era el track central y más popular. Se enfocaba en profundidad en la configuración, verificación y troubleshooting de protocolos de enrutamiento IP (como OSPF, EIGRP, BGP) y tecnologías de switching de Capa 2 (como VLANs, STP, VTP) en

redes empresariales. Cubría WANs y servicios de red asociados. En la estructura de certificación actual de Cisco (post-2020), gran parte de este contenido se encuentra integrado dentro del track **CCNP Enterprise**.

- **Track Security:** Este track se enfoca en la seguridad de redes utilizando productos y soluciones de Cisco. Los temas incluyen la implementación de seguridad de acceso a la red, VPNs, firewalls (ej. Cisco ASA, Firepower), sistemas de prevención de intrusiones (IPS), seguridad de contenido (web y email), y gestión de identidades. Un CCNP Security demuestra habilidades para diseñar, implementar y solucionar problemas de soluciones de seguridad para proteger redes.

27 - Explique el modelo OSI.

El **Modelo OSI (Open Systems Interconnection)** es un **modelo de referencia conceptual** que divide el proceso de comunicación de red en siete capas distintas y ordenadas. Fue desarrollado por la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (ITU) para promover la interoperabilidad entre diferentes sistemas de hardware y software de red.

Cada capa tiene una función específica y se comunica solo con la capa inmediatamente superior o inferior. La idea es que los protocolos y tecnologías de red puedan ser desarrollados y estandarizados por separado para cada capa.

Las siete capas del modelo OSI, de abajo hacia arriba, son:

1. **Capa 1: Física (Physical Layer):** Es la capa más baja. Se encarga de la transmisión de bits crudos sobre el medio físico. Define las especificaciones eléctricas, mecánicas, procedimentales y funcionales para activar, mantener y desactivar enlaces físicos. (Ejemplos: cables (UTP, fibra), conectores (RJ45, SFP), niveles de voltaje, tasas de datos, señales de radio en Wi-Fi).
2. **Capa 2: Enlace de Datos (Data Link Layer):** Se encarga de la comunicación de nodo a nodo a través de un enlace físico. Proporciona direccionamiento físico (direcciones MAC), detección y corrección de errores en la transmisión entre nodos adyacentes, y control de flujo. Divide los datos en "tramas" (frames). Se divide a su vez en dos subcapas: Control de Enlace Lógico (LLC) y Control de Acceso al Medio (MAC). (Ejemplos: Ethernet, Wi-Fi (802.11), PPP).
3. **Capa 3: Red (Network Layer):** Se encarga del enrutamiento de paquetes a través de múltiples redes (interconexión de redes).

Proporciona direccionamiento lógico (direcciones IP) y determina la mejor ruta para que los paquetes lleguen a su destino final, que puede estar en una red diferente. (Ejemplos: IP (Internet Protocol), routers).

4. **Capa 4: Transporte (Transport Layer):** Se encarga de la comunicación de extremo a extremo entre procesos en diferentes hosts. Divide los datos de la capa superior en segmentos o datagramas, maneja la entrega fiable (con protocolos como TCP) o no fiable (con protocolos como UDP), control de flujo y control de errores a nivel de segmento. (Ejemplos: TCP (Transmission Control Protocol), UDP (User Datagram Protocol)).
5. **Capa 5: Sesión (Session Layer):** Establece, gestiona y termina las sesiones de comunicación entre aplicaciones en diferentes hosts. Sincroniza el diálogo entre las capas de presentación de los dos hosts y gestiona el intercambio de datos. (Ejemplos: NetBIOS, algunos aspectos de RPC).
6. **Capa 6: Presentación (Presentation Layer):** Se encarga de la representación de los datos, es decir, traduce los datos de la capa de aplicación a un formato que la capa de sesión pueda entender y viceversa. Maneja la codificación/decodificación, cifrado/descifrado y compresión/descompresión de datos. (Ejemplos: Formatos de datos como JPEG, ASCII; cifrado como SSL/TLS a veces se ubica aquí).
7. **Capa 7: Aplicación (Application Layer):** Es la capa superior y la más cercana al usuario. Proporciona servicios de red directamente a las aplicaciones de software que utiliza el usuario. Permite que las aplicaciones accedan a la red. (Ejemplos: HTTP (Web), FTP (Transferencia de Archivos), SMTP (Correo Electrónico), DNS (Resolución de Nombres), SSH (Acceso Remoto Seguro)).

Aunque el modelo OSI es un marco teórico útil para entender y diseñar redes, en la práctica, el modelo TCP/IP (con menos capas) es el que se implementa predominantemente en Internet.

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

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

El estándar IEEE 802.3 es el conjunto de normas que definen la tecnología **Ethernet** para redes de área local (LAN) cableadas. Opera principalmente en las capas Física y de Enlace de Datos (específicamente la subcapa MAC - Control de Acceso al Medio) del modelo OSI. Su objetivo es definir cómo los

dispositivos se conectan físicamente y cómo acceden al medio de transmisión para enviar datos en una red compartida o conmutada.

Cómo se implementa: Se implementa mediante:

- **Medios Físicos:** Define el tipo de cableado (pares trenzados de cobre como UTP Categoría 5e, 6, etc., o fibra óptica) y los conectores (como RJ45 para cobre).
- **Señalización:** Especifica cómo se codifican y transmiten los bits a través del medio.
- **Formato de Trama:** Define la estructura del paquete de datos (la "trama Ethernet"), incluyendo direcciones MAC de origen y destino, información de control, y la carga útil (los datos).
- **Método de Acceso al Medio:** Históricamente usaba CSMA/CD (Carrier Sense Multiple Access with Collision Detection) para redes compartidas (hubs). En las redes modernas conmutadas (switches) se utiliza principalmente el modo full-duplex, donde no hay colisiones y los dispositivos pueden transmitir y recibir simultáneamente.

La implementación más común se ve en las tarjetas de red (NICs) de computadoras y servidores, y en dispositivos de red como switches y routers, que tienen puertos conformes a los estándares 802.3 (ej. 100BASE-TX, 1000BASE-T, 10GBASE-SR).

Ventajas:

- **Ampliamente Adoptado:** Es el estándar de facto para redes cableadas en todo el mundo, lo que garantiza compatibilidad entre equipos de diferentes fabricantes.
- **Altas Velocidades:** Soporta un rango muy amplio de velocidades, desde 10 Mbps hasta 400 Gbps y más en sus versiones más recientes.
- **Costo Relativamente Bajo:** Especialmente el cableado de cobre (UTP) y el hardware de red asociado (switches) son muy económicos para la velocidad que ofrecen.
- **Fiabilidad:** Las conexiones cableadas son generalmente más estables y menos susceptibles a interferencias que las inalámbricas.
- **Seguridad:** Inherente mayor seguridad física comparado con redes inalámbricas, ya que requiere acceso físico al cable.

Desventajas:

- **Requiere Cableado Físico:** La instalación puede ser costosa, compleja y requiere planificación, especialmente en edificios existentes. Limita la movilidad.
- **Distancia Limitada:** Los cables de cobre tienen limitaciones de distancia (generalmente 100 metros para altas velocidades) antes de necesitar repetidores o switches.
- **Susceptible a Daños Físicos:** Los cables pueden ser dañados, lo que interrumpe la conectividad.
- **Menos Flexible:** Cambiar la disposición de la red o añadir nuevos dispositivos requiere modificar la infraestructura de cableado.

30 - Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4 define la tecnología **Token Bus**. Era un método de acceso al medio para redes de área local (LANs) que utiliza una **topología lógica de anillo** sobre un **medio físico de bus**.

En una red Token Bus, los dispositivos están conectados a un cable común (bus), pero operan en un orden lógico predeterminado. Se pasa un "token" (una trama de control) entre los dispositivos en este orden lógico. **Solo el dispositivo que posee el token tiene permiso para transmitir datos** durante un tiempo limitado. Una vez que termina de transmitir o se agota su tiempo, pasa el token al siguiente dispositivo en el orden lógico.

Estado Actual: Token Bus fue uno de los tres principales estándares LAN en las primeras etapas del desarrollo de redes (junto con 802.3 Ethernet y 802.5 Token Ring). Sin embargo, **Ethernet (802.3) se convirtió en la tecnología dominante** debido a su simplicidad, escalabilidad y coste más bajo a medida que evolucionaba. El estándar IEEE 802.4 **está en gran parte obsoleto** para redes de propósito general y no se utiliza comúnmente en la actualidad. Tuvo algunas aplicaciones en entornos industriales con requisitos estrictos de tiempo (ej. Manufacturing Automation Protocol - MAP).

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

Para el **envío** y **transferencia** de correo electrónico (desde el cliente de correo hacia el servidor, y entre servidores de correo), el protocolo principal es **SMTP (Simple Mail Transfer Protocol)**.

Cuando envías un correo electrónico desde tu cliente (como Outlook o Gmail), este se conecta al servidor SMTP saliente configurado y utiliza SMTP para

transferir el mensaje al servidor. Luego, los servidores SMTP se comunican entre sí utilizando SMTP para enrutar el correo hasta el servidor de correo del destinatario.

Para la **recepción** de correo en el sentido de que un servidor recibe un correo de otro servidor, también se utiliza **SMTP**. Sin embargo, si te refieres a la **recepción** de correo en el sentido de que un cliente de correo **descarga o accede** a los correos que están almacenados en un servidor de correo, se utilizan otros protocolos (ver la siguiente pregunta).

En resumen, para el envío y la transferencia entre servidores: SMTP.

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

Para **leer** o **acceder** a los correos electrónicos que ya han sido recibidos por el servidor de correo de destino y están almacenados en la bandeja de entrada de un usuario, los protocolos utilizados por los clientes de correo son principalmente dos:

1. **POP3 (Post Office Protocol version 3):**
    - Funciona como una "oficina de correos". El cliente se conecta al servidor, **descarga** los correos a la computadora local y, por defecto, los **elimina** del servidor (aunque se puede configurar para que deje una copia). Una vez descargados, los correos se gestionan localmente.
2. **IMAP (Internet Message Access Protocol):**
    - Permite al cliente **acceder y gestionar** los correos electrónicos directamente **en el servidor**. Los correos permanecen en el servidor. Esto es ideal si accedes a tu correo desde múltiples dispositivos (computadora, teléfono, tablet), ya que todos ven el mismo estado de los correos (leído, no leído, carpetas, etc.).

Aunque técnicamente se podría usar un navegador web para acceder a un cliente webmail (como Gmail, Outlook.com) que a su vez interactúa con el servidor usando protocolos internos o APIs, cuando se habla de protocolos estándar para que un cliente de escritorio o móvil "lea" correo, se refiere a **POP3** o **IMAP**. IMAP es el más utilizado actualmente.

33 - Diferencias entre IPV4 e IPV6

IPv4 (Internet Protocol version 4) e IPv6 (Internet Protocol version 6) son las dos versiones del Protocolo de Internet que se utilizan para identificar dispositivos en una red y enrutar el tráfico entre ellos. La principal motivación para el desarrollo de IPv6 fue el agotamiento **de direcciones IPv4**.

Estas son las diferencias clave:

Característica	IPv4	IPv6
Tamaño de la Dirección	32 bits	128 bits
Formato de la Dirección	Notación decimal con puntos (ej. 192.168.1.1)	Notación hexadecimal con dos puntos (ej. 2001:0db8:85a3::8a2e:0370:7344)
Número de Direcciones	~4.3 mil millones (agotadas globalmente)	2128 (aproximadamente 3.4×1038, prácticamente ilimitado)
Encabezado (Header)	Más pequeño (20 bytes fijo + opciones)	Más grande (40 bytes fijo + encabezados de extensión opcionales)
Checksum del Encabezado	Presente (calculado en cada salto)	No presente (se basa en la comprobación de errores de capas inferiores)
Fragmentación	Manejada por routers y host de origen	Manejada solo por el host de origen
Configuración Auto.	Requiere DHCP	Soporte nativo para Autoconfiguración de Direcciones sin Estado (SLAAC) y DHCPv6
Seguridad (IPsec)	Opcional	Integrado en el estándar (aunque la implementación puede ser opcional)
Movilidad	Requiere Mobile IP	Funcionalidad de movilidad mejorada (Mobile IPv6)
Soporte QoS	Marcadores (ToS, DSCP)	Campo Flow Label nativo para manejo de flujos de tráfico

34- (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes? Ejemplos.: Accedo y configuro el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configuro una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.

Juan Ruiz: Tengo acceso al router de casa y lo configuro, también en mi antigua casa que era un hotel familiar logre configuran un modem principal y 2 router debido a que era muy grande y eran muchos equipos conectados, cada uno estaba en una planta, me gustan mucho las redes y trato de aprender cada día lo que mas se puede.

Elida Seborga Coca: No tengo ninguna experiencia.