INSTITUTO DE FORMACIÓN TÉCNICA SUPERIOR N° 18

PROGRAMACIÓN SOBRE REDES

Trabajo Práctico Teórico

-GRUPO D-

2do cuatrimestre 2025

Integrantes: **CELIA, Bruno (DNI/Legajo: 41.470.058).-**
Email: brunocelia98@gmail.com

DE LUCA, Leila Giselle (DNI/Legajo: 34.117.783).-
Email: leila.giselle.de.luca@gmail.com

DE SOUZA GOMES, Anna Clara (DNI/Legajo: 95.859.027).-
Email: annaclarag06@gmail.com

MARTINI, Fernando Pablo (DNI/Legajo: 36.724.106).-
Email: fer.martini878@gmail.com

Profesor: **RUSSATTI, Lucas**

1- ¿Qué es una VLAN?

Una VLAN (Red de área local virtual) permite agrupar dispositivos dentro de una red en un mismo dominio de difusión, sin importar su ubicación física. Esto facilita organizar la red según necesidades lógicas (como roles o niveles de acceso) en lugar de basarse en el cableado o la cercanía. Por ejemplo, en una empresa se pueden separar empleados fijos y contratados en VLAN distintas para aplicar diferentes políticas de seguridad.

Las VLAN hacen que la administración de la red sea más flexible, ya que se configuran por software y permiten adaptarse fácilmente a cambios, incorporaciones o reubicaciones. Además, optimizan el tráfico al dirigir los *broadcasts* solo a los equipos de la misma VLAN, reduciendo la carga en los enrutadores y mejorando la eficiencia.

Etiquetado

Para activar VLAN, debe implementar conmutadores compatibles con VLAN en cada sitio. Las interfaces del conmutador insertan etiquetas en la capa 2 del marco de datos que identifican un paquete de red como parte de una VLAN específica. Estas etiquetas, que agregan cuatro bytes extra al encabezado de Ethernet, identifican que el marco pertenece a una VLAN específica. El etiquetado se especifica por el estándar IEEE 802.1Q.Gracias a este sistema, una sola interfaz puede manejar tráfico de varias VLAN mediante enlaces troncales.

La definición de VLAN incluye la disposición de marcos de datos etiquetados y no etiquetados. Debe especificar si la VLAN recibe datos etiquetados, no etiquetados o no recibe datos de cada interfaz activada. Firebox puede insertar etiquetas para paquetes que se envían a un conmutador compatible con VLAN. Su dispositivo también puede eliminar etiquetas de paquetes que se envían a un segmento de red que pertenece a una VLAN que no tiene un conmutador.

De manera predeterminada, la mayoría de los conmutadores asignan sus interfaces a la VLAN 1, lo que puede extender esa VLAN más de lo deseado si no se configura adecuadamente.Lo que puede exponer a la red a vulnerabilidades al mantener toda la comunicación en una única VLAN que no debe usarse para datos. Para mejorar la seguridad, se recomienda mover el tráfico de datos y de administración fuera de la VLAN 1, estableciendo una política de "no utilizar la VLAN 1" para datos y configurando la VLAN nativa en una VLAN separada y no utilizada.

2- ¿Qué es una VPN?

Una VPN, es decir, una red privada virtual, establece una conexión digital entre el equipo y un servidor remoto propiedad de un proveedor de VPN, creando un túnel de punto a punto que cifra los datos personales, enmascara la dirección IP y permite pasar por un lado los firewalls y los bloques de sitios web en Internet. Esto garantiza que la actividad en línea esté protegida y sea privada y más segura.
Por su propia definición, una conexión VPN es:

- Virtual, porque no hay cables físicos implicados en la conexión.
- Privada, porque, a través de esta conexión, nadie más puede ver los datos ni la actividad de navegación.
- En red, porque varios dispositivos (su ordenador y el servidor VPN) funcionan de manera conjunta para mantener el vínculo establecido.

Para cualquier persona que busque una experiencia en línea más fiable, libre y segura, las ventajas de usar una VPN son infinitas. Una VPN protege a los usuarios mediante el cifrado de datos y el enmascaramiento de la dirección IP, lo que deja el historial de exploración y la ubicación sin seguimiento. Este mayor anonimato permite una mayor privacidad, así como mayor libertad para aquellas personas que quieren acceder a contenido bloqueado o enlazado a una región.

Tipos de conexiones VPN

Nombre	Tipo	Método de conexión	Caso de uso
VPN de acceso remoto (también conocida como VPN de cliente a sitio)	Página principal	Conexión a una red privada o a un servidor de terceros a través de SSL/TSL	Para los trabajadores remotos que necesitan acceder a los archivos y recursos de la empresa a través de una conexión privada, o para los usuarios que desean explorar la red pública de Internet a través de una conexión cifrada
VPN de sitio a sitio	Privado	La red se conecta a otra red a través de LAN, WAN	Para organizaciones de gran tamaño que necesitan vincular sus redes internas entre varios sitios en distintas ubicaciones, al tiempo que mantienen una conexión segura
Aplicaciones de VPN	Para dispositivos móviles	Conéctese a una red privada a través de una aplicación VPN en un dispositivo móvil o smartphone	Para los usuarios móviles que deseen aprovechar las ventajas de una VPN mientras se desplazan o mientras experimentan una conexión a Internet inestable

3- ¿Qué es una SAN?

Una red de área de almacenamiento (Storage Area Network) es una red dedicada que se adapta a un entorno específico, que combina servidores, sistemas de almacenamiento, conmutadores de red, software y servicios.Funciona como una red separada y

especializada cuyo único propósito es el almacenamiento de datos a nivel de bloque, no de archivo. Esto significa que los servidores pueden acceder a los datos directamente, como si el almacenamiento estuviera conectado localmente.

La SAN libera el dispositivo de almacenamiento para que no esté en un bus de servidor en concreto. Conecta el almacenamiento directamente a la red, externalizando y distribuyendo funcionalmente el almacenamiento en toda la organización. La SAN también centraliza los dispositivos de almacenamiento y el clustering de servidores, lo que podría lograr una administración centralizada más fácil y económica y reducir el coste total de propiedad

Componentes y funcionamiento

La arquitectura de una SAN se compone principalmente de tres elementos:

- Dispositivos de almacenamiento: Son las matrices de discos duros (como un gran gabinete con muchos discos) que guardan los datos. Estos dispositivos pueden ser de tipo RAID para ofrecer redundancia y alto rendimiento.
- Servidores: Son las computadoras que ejecutan las aplicaciones y que necesitan acceso a los datos almacenados en la SAN. Para conectarse, utilizan una tarjeta de red especial llamada HBA (Host Bus Adapter).
- **"Fabric" de la SAN:** Es la red de interconexión que une los servidores y el almacenamiento. La tecnología más común para esto es **Fibre Channel (FC)**, que ofrece una alta velocidad y baja latencia, ideal para aplicaciones críticas. También existen opciones que usan Ethernet, como iSCSI.

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

Hub: El hub (o concentrador) es un repetidor multi-puerto. También opera en la Capa 1 (Física) y es un dispositivo muy poco eficiente. Cuando recibe un paquete de datos por uno de sus puertos, lo replica y lo envía a todos los demás puertos. Esto crea un "dominio de colisión" grande, ya que todos los dispositivos conectados pueden "escuchar" todo el tráfico de la red, lo que ralentiza la velocidad y genera tráfico innecesario. Los hubs están prácticamente obsoletos hoy en día.

Repetidor: Es el dispositivo más simple. Su única función es recibir una señal de red débil y retransmitirla a la misma potencia que la señal original. Funciona en la Capa 1 (Física) del modelo OSI. Su objetivo es extender el alcance de la red, superando las limitaciones de distancia del cableado. No tiene ninguna inteligencia para filtrar o dirigir el tráfico; simplemente amplifica todo lo que recibe.

Router: El router (o enrutador) es el más sofisticado de los cuatro y opera en la Capa 3 (Red) del modelo OSI. Su función principal es conectar redes diferentes (por ejemplo, tu red doméstica con Internet) y "enrutar" los paquetes de datos entre ellas usando las direcciones IP. El router utiliza tablas de enrutamiento para determinar la mejor ruta para enviar los datos a su destino final, incluso si este se encuentra en una red completamente distinta. Además, los routers modernos suelen incluir funciones como Wi-Fi, servidor DHCP, y un firewall, lo que los convierte en la puerta de enlace a Internet para la mayoría de las redes domésticas y empresariales.

Switch: El switch (o conmutador) es una versión inteligente del hub. Funciona en la Capa 2 (Enlace de datos) del modelo OSI. A diferencia del hub, el switch puede aprender y recordar la dirección MAC de los dispositivos conectados a cada uno de sus puertos. Cuando recibe un paquete, lo dirige únicamente al puerto del dispositivo de destino, lo que evita que el tráfico innecesario se transmita a toda la red. Esto reduce las colisiones y mejora enormemente el rendimiento y la seguridad de la red local.

5- ¿Qué es un protocolo de comunicaciones?

Un protocolo de comunicaciones es un conjunto de reglas y procedimientos estandarizados que permiten que dos o más dispositivos en una red se comuniquen entre sí y compartan datos. Piensa en ellos como el "idioma" que hablan las computadoras para entenderse. Sin un protocolo, los dispositivos no sabrían cómo formatear, enviar o recibir la información, lo que haría imposible la comunicación.

Ejemplos de Protocolos de Red

Los protocolos se organizan en capas, donde cada capa tiene una función específica para garantizar que los datos se transmitan de manera eficiente.

- **TCP/IP**: Es el protocolo fundamental de Internet y la mayoría de las redes modernas. El **IP** se encarga del **direccionamiento** (asegurando que los datos lleguen a la dirección IP correcta), mientras que **TCP** gestiona la **fiabilidad** (garantizando que todos los datos lleguen en el orden correcto y sin errores).
- **HTTP/HTTPS**: El **Protocolo de Transferencia de Hipertexto** (HTTP) es la base de la comunicación de la **World Wide Web**. Define cómo se solicitan y se envían las páginas web entre el navegador y el servidor. **HTTPS** es la versión segura de HTTP, que cifra la comunicación para proteger la privacidad de los usuarios.

- **FTP**: El **Protocolo de Transferencia de Archivos** se utiliza para mover archivos entre computadoras.

- **SMTP, POP3, IMAP**: Estos protocolos se usan para el **correo electrónico**. **SMTP** se encarga de enviar los correos, mientras que **POP3** e **IMAP** se usan para recibirlos.
- **DHCP**: El **Protocolo de Configuración Dinámica de Host** asigna automáticamente direcciones IP a los dispositivos en una red, simplificando la administración de la red.

Los protocolos son esenciales porque aseguran la interoperabilidad y la consistencia en las redes. Sin ellos, cada fabricante tendría su propio método de comunicación, creando un caos digital.

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

TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) y **NetBIOS** (Sistema Básico de Entrada/Salida de Red) son dos tecnologías que permiten la comunicación en red, pero operan en diferentes niveles y con propósitos distintos. TCP/IP es el estándar global de facto para las redes modernas, mientras que NetBIOS es un protocolo heredado, enfocado en la resolución de nombres en redes locales.

TCP/IP

TCP/IP es un conjunto de protocolos de comunicación que forma la base de Internet y la mayoría de las redes modernas. Su arquitectura se basa en un modelo de capas que divide la comunicación en tareas específicas, lo que facilita la transmisión de datos a gran escala.

- **IP (Protocolo de Internet)**: Funciona en la **capa de red**. Su principal responsabilidad es el **direccionamiento y enrutamiento** de los paquetes de datos. Cada dispositivo en la red tiene una **dirección IP única** que actúa como su "dirección postal", permitiendo que los datos lleguen a su destino correcto, incluso a través de múltiples redes.
- **TCP (Protocolo de Control de Transmisión)**: Opera en la **capa de transporte**. Su función es garantizar una **transmisión confiable** de los datos. Antes de enviar la información, TCP la divide en paquetes pequeños, los numera y se asegura de que lleguen al destino en el orden correcto y sin errores, solicitando la retransmisión de paquetes perdidos si es necesario.

NetBIOS

NetBIOS es una interfaz de software y una convención de nomenclatura que permite a las aplicaciones comunicarse en una red local. A diferencia de TCP/IP, NetBIOS no es un protocolo de enrutamiento por sí mismo. Su función principal es proporcionar servicios para:

- Nombres: NetBIOS asigna un nombre de 16 caracteres a cada dispositivo en la red local. Esto facilita la comunicación, ya que los usuarios y las aplicaciones pueden referirse a los equipos por su nombre en lugar de una dirección numérica.

- Sesiones: Permite que las aplicaciones establezcan una conexión confiable (orientada a la conexión) para transferir datos.

- Datagramas: Soporta la comunicación sin conexión, enviando paquetes de datos de manera simple a un destino.

En la actualidad, NetBIOS se utiliza principalmente a través de TCP/IP (conocido como NetBT o NetBIOS sobre TCP/IP) para garantizar la compatibilidad con aplicaciones heredadas de Windows, como el intercambio de archivos e impresoras.

Característica	TCP/IP	NetBIOS
Nivel	Conjunto de protocolos de enrutamiento.	Interfaz de software y convención de nombres.
Alcance	Global (Internet y redes extensas).	Principalmente local (LAN).
Direccionamiento	Usa direcciones IP numéricas.	Usa nombres NetBIOS alfanuméricos.
Función	Transmisión de datos, enrutamiento y fiabilidad.	Nomenclatura, sesiones y datagramas.
Estado actual	**Estándar global y actual de las redes.**	**Tecnología heredada, usada para compatibilidad.**

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

Un paquete de datos en TCP/IP es la unidad de información fundamental que se transmite a través de una red. Se crea mediante un proceso de encapsulamiento, donde la información se organiza en diferentes partes a medida que viaja a través de las capas del modelo TCP/IP.

Estructura de un Paquete de Datos TCP/IP

El paquete de datos se compone principalmente de dos partes esenciales: el encabezado (header) y la carga útil (payload), que contiene los datos del usuario. El encabezado, a su vez, se divide en dos secciones principales:

Encabezado IP: Se añade en la Capa de Internet. Contiene la información necesaria para el enrutamiento. Los campos clave incluyen:

- Dirección IP de Origen y de Destino: Las "direcciones postales" de los dispositivos que envían y reciben el paquete.
- Versión de IP: (IPv4 o IPv6).
- Longitud del Encabezado: Indica el tamaño del encabezado IP.
- Protocolo: Identifica el protocolo de la capa de transporte (TCP, UDP, etc.) que se encuentra dentro del paquete.
- Tiempo de Vida (TTL): Un contador que limita el número de saltos que puede dar el paquete para evitar que circule indefinidamente.

Encabezado TCP: Se añade en la Capa de Transporte. Proporciona información para la comunicación fiable, orientada a la conexión. Los campos más importantes son:

- Puertos de Origen y de Destino: Identifican las aplicaciones específicas en el origen y el destino.

- Número de Secuencia: Permite que el receptor reordene los paquetes que podrían haber llegado desordenados.
- Número de Acuse de Recibo: Confirma que el receptor ha recibido un paquete anterior.
- Flags (Banderas): Bits de control para gestionar la comunicación.

Un **"flag"** es un bit de control en el encabezado TCP que actúa como una señal para indicar el estado de la conexión o la naturaleza del paquete. Estos flags son cruciales para el establecimiento, la gestión y la terminación de la conexión. Los más importantes son:

- **SYN (Synchronize)** : Se utiliza para iniciar una conexión TCP. El cliente envía un paquete con el flag SYN activado para solicitar una conexión.
- **ACK (Acknowledge)** : Se usa para reconocer la recepción de un paquete. El receptor envía un paquete con el flag ACK para confirmar que ha recibido los datos.
- **FIN (Finalize)** : Indica que el emisor ha terminado de enviar datos y desea cerrar la conexión de manera ordenada.
- **RST (Reset)** : Se usa para resetear una conexión, generalmente debido a un error o una conexión no válida.
- **PSH (Push)** : Le indica al receptor que los datos deben ser entregados a la aplicación de inmediato, sin esperar a que el búfer se llene.
- **URG (Urgent)** : Señala que hay datos urgentes en el paquete que deben ser procesados con prioridad.

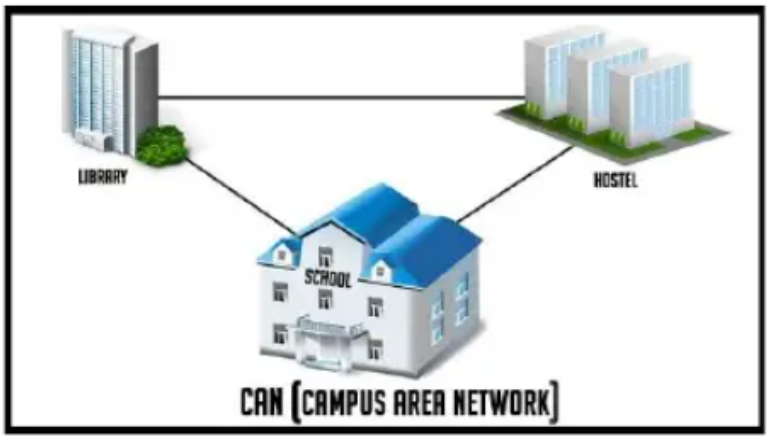
Estos flags son esenciales para el funcionamiento del "handshake de tres vías" de TCP y para el control de flujo y la confiabilidad del protocolo.

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

Red de Área Personal (PAN) : Cubre un área muy pequeña, generalmente alrededor de una persona o un solo dispositivo. Se usa para conectar dispositivos como teléfonos inteligentes, auriculares, impresoras o teclados a una computadora. Las tecnologías comunes incluyen Bluetooth y Wi-Fi Direct.

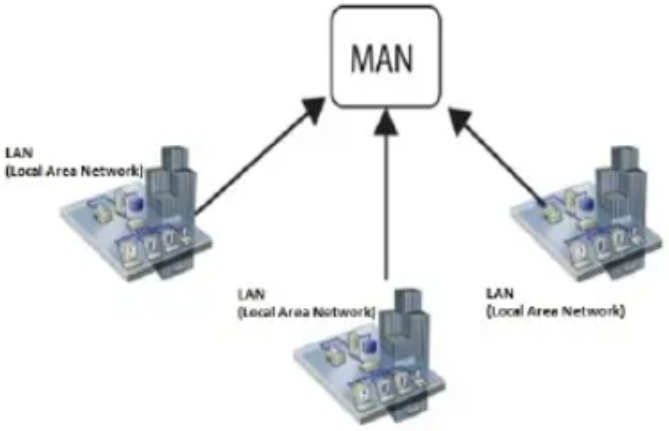
Red de Área Local (LAN) : Conecta computadoras y dispositivos en un área geográfica limitada, como una casa, una oficina, o un solo edificio. Las LAN permiten compartir recursos como impresoras, archivos e Internet. La conexión se realiza típicamente a través de cables Ethernet o de forma inalámbrica (WLAN) usando Wi-Fi. Las LAN son rápidas, seguras y fáciles de gestionar.

Red de Área de Campus (CAN) : Es una red más grande que una LAN, que interconecta múltiples LAN dentro de un área geográfica específica como un campus universitario, un parque industrial o una base militar. La infraestructura de la red es propiedad de la misma

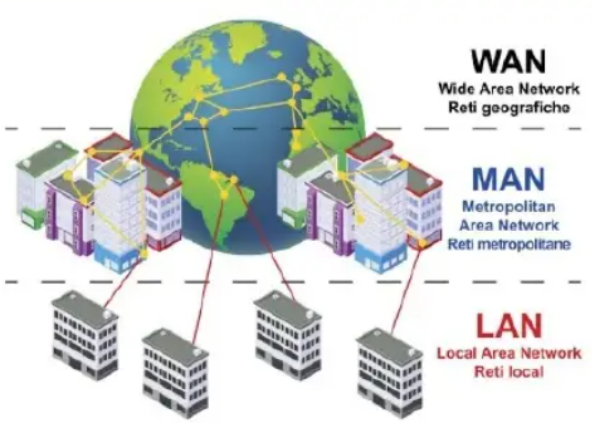


organización, lo que permite un alto rendimiento y una gestión centralizada.

Red de Área Metropolitana (MAN) : Una red que se extiende por una ciudad o un área metropolitana. Una MAN interconecta múltiples LAN y puede ser propiedad de una sola entidad o de un proveedor de servicios que ofrece conectividad a múltiples organizaciones y usuarios. Generalmente se utilizan cables de fibra óptica para lograr altas velocidades de transmisión de datos.



Red de Área Amplia (WAN) : Conecta redes que se encuentran en diferentes ciudades, países o incluso continentes. La WAN más conocida es Internet. Las WANs se construyen a partir de la interconexión de varias LAN y MAN a través de líneas telefónicas, cables de fibra óptica submarinos o enlaces satelitales. Son redes complejas, lentas y costosas, pero permiten la comunicación global.



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

La topología de red describe cómo están interconectados los dispositivos y cómo circula la información.

Según IBM y otros fabricantes, existen varias variantes:

- Bus: un solo canal compartido por todos los nodos; económico pero sensible a fallas.
- Estrella: todos los dispositivos conectan a un punto central (switch/hub). Facilita gestión pero depende del nodo central.
- Anillo: los nodos forman un lazo cerrado. Un fallo interrumpe la red, aunque existen versiones tolerantes.
- Malla: cada nodo tiene múltiples enlaces redundantes. Alta disponibilidad pero costosa.
- Árbol: jerárquica, combina estrellas bajo una estructura ramificada.
- Híbrida: mezcla de varias, según las necesidades.

10- Explicar el servicio de DHCP.

DHCP (Dynamic Host Configuration Protocol) es un protocolo que **asigna automáticamente direcciones IP y otros parámetros de red** a los dispositivos cuando se conectan.

- Sin DHCP: cada IP se asigna manualmente → engorroso y propenso a errores.
- Con DHCP: el servidor entrega automáticamente IP, máscara de subred, gateway y DNS.
- Beneficio: simplifica administración y evita conflictos de IP.

11- Explicar el servicio de DNS.

DNS (Domain Name System) es como la **agenda telefónica de Internet**: traduce los nombres de dominio (ej. `www.google.com`) **en direcciones IP** (ej. `142.250.72.196`) que las computadoras entienden.

- Evita que los usuarios tengan que recordar IPs.
- Es distribuido y jerárquico (servidores raíz, TLD, autoritativos, cachés).
- Ejemplo: al entrar a `chat.openai.com`, tu PC pregunta al DNS cuál es la IP de ese dominio y luego se conecta allí.

12- Explicar las tecnologías Wireless, y sus estándares.

Las tecnologías **wireless** permiten transmitir datos sin cables, usando radiofrecuencia o infrarrojo.

Estándares principales de Wi-Fi (IEEE 802.11):

- **802.11b:** hasta 11 Mbps, 2.4 GHz.
- **802.11g:** hasta 54 Mbps, 2.4 GHz.
- **802.11n:** hasta 600 Mbps, 2.4/5 GHz (MIMO).
- **802.11ac (Wi-Fi 5):** hasta varios Gbps, 5 GHz.
- **802.11ax (Wi-Fi 6):** mejor rendimiento en redes densas, 2.4/5/6 GHz.

Otras tecnologías wireless:

- **Bluetooth:** corto alcance, baja energía, conexión entre dispositivos.
- **LTE / 5G:** tecnologías celulares para Internet móvil.
- **WiMAX:** conexión de banda ancha inalámbrica en grandes distancias.

13- ¿Qué es un Proxy?

Un **Proxy** es un **servidor intermediario** entre el cliente y el recurso al que quiere acceder.

Funciones:

- **Filtrado y control:** bloquear sitios, aplicar políticas de acceso.
- **Anonimato:** oculta la IP real del cliente.
- **Caché:** guarda copias de sitios visitados para mejorar velocidad.
- **Seguridad:** evita accesos directos a la red interna.

Ejemplo: en una empresa, todas las PCs salen a Internet a través del Proxy, que aplica reglas y registra la actividad.

14- Explicar el protocolo Spanning tree.

El **Spanning Tree Protocol (STP)** se usa en redes con **switches** para **evitar bucles**.

- Problema: si hay enlaces redundantes entre switches, los bucles generan tormentas de broadcast.
- Solución: STP detecta enlaces redundantes y los bloquea automáticamente, manteniendo solo una ruta activa.
- Si la ruta principal falla, reconfigura la red y activa un enlace alternativo.
- Esencial en redes empresariales con switches interconectados.

15- Explicar el protocolo de comunicaciones OSPF.

OSPF (Open Shortest Path First) es un protocolo de enrutamiento interno (IGP) basado en el algoritmo de **estado de enlace**.

Según IBM, cada router mantiene una base de datos de la topología y usa el algoritmo de Dijkstra para calcular la ruta más corta. Es rápido ante cambios, escalable y soporta áreas jerárquicas, lo que lo hace ideal para redes grandes.

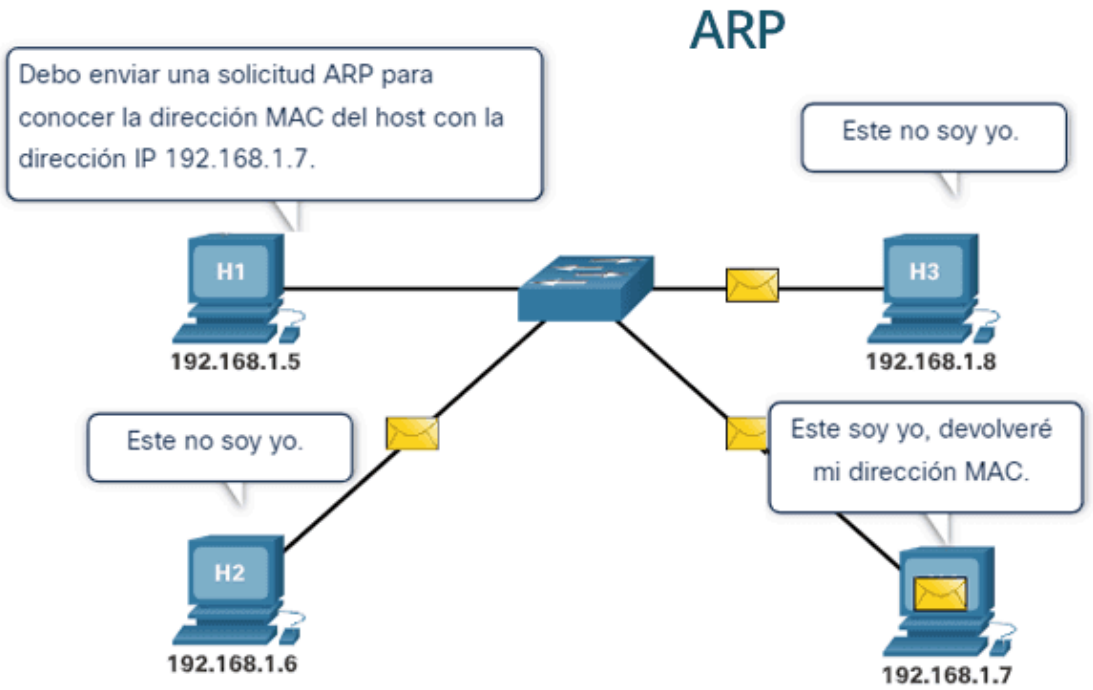
16- Explicar el protocolo ARP.

ARP (Address Resolution Protocol) se usa para **traducir direcciones IP en direcciones MAC** dentro de una red local.

- La IP identifica al dispositivo en la red.
- La MAC identifica al dispositivo físicamente en la LAN.

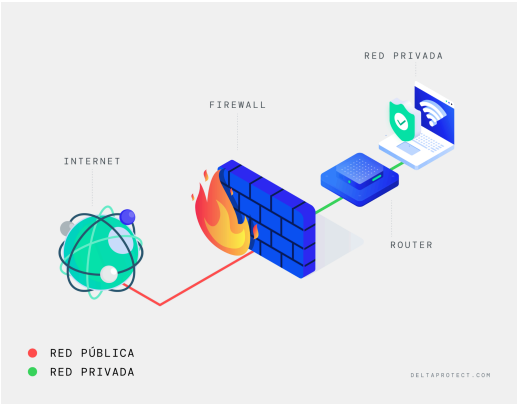
- Ejemplo: si tu PC quiere enviar un paquete a `192.168.1.5`, pregunta por la red: *"¿Quién tiene esta IP?"*. El dispositivo responde con su MAC y la comunicación se establece.

Problema: ataques de **ARP spoofing/poisoning**, donde un atacante responde con una MAC falsa para interceptar tráfico.



17- ¿Qué es un Firewall?

Un firewall es un **sistema de seguridad que controla y filtra el tráfico de datos** entre redes. Su función principal es analizar las comunicaciones para **detectar posibles amenazas** y prevenir accesos no autorizados, actuando como una barrera entre una red interna confiable y redes externas como internet.



Tipos de firewall:

De red: controla el tráfico de entrada y salida en el perímetro de la red, protegiendo contra accesos no deseados etre las conexiones internas y externas.

De aplicaciones Web (WAF)**:** Protege servidores y aplicaciones web de ataques comunes (como inyecciones SQL), funcionando como un escudo especializado para servicios en línea.

De próxima generación (NGFW)**:** combina funciones de los firewalls tradicionales con capacidades avanzadas, como inspección profunda de paquetes, prevención de intrusiones y control de aplicaciones.

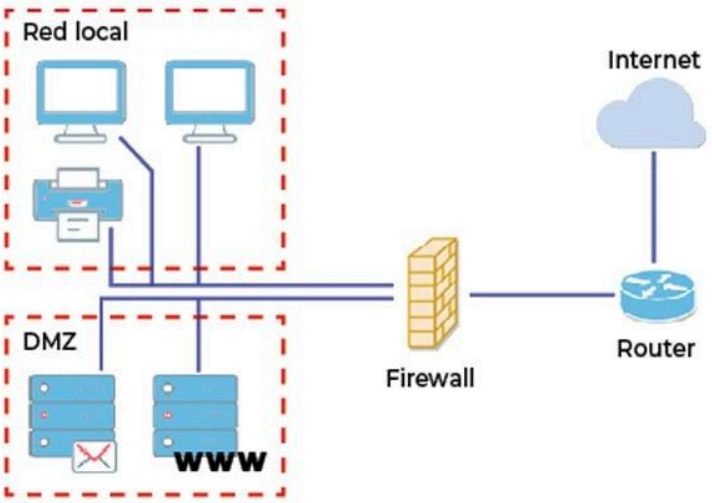
Basado en la nube: Se implementa como un servicio en la nube, ofreciendo escalabilidad, flexibilidad y adaptación rápida a la infraestructura de cada organización.

18- ¿Qué es una DMZ?

Un DMZ o Zona Desmilitarizada es una **subred que se ubica entre una red interna confiable y una red externa no confiable (internet).**

Su objetivo principal es actuar como una zona de amortiguación que aísla y protege la red interna. Al colocar los servicios que deben ser accesibles desde internet en la DMZ, se invita que un atacante que hackee estos servicios pueda acceder directamente a los datos sensibles de la red interna como por ejemplo las bases de datos.

Es una zona de “alto riesgo controlado” donde se ubican los servidores que necesitan interactuar con el exterior. Se asume que van a ser atacados, por lo que se endurece la seguridad.



¿Cómo funciona?

Se controlan los accesos mediante firewalls que aplican reglas de seguridad:

Tráfico desde Internet: Solo se permite el tráfico dirigido a los puertos específicos de los servicios en la DMZ, el resto se bloquea.

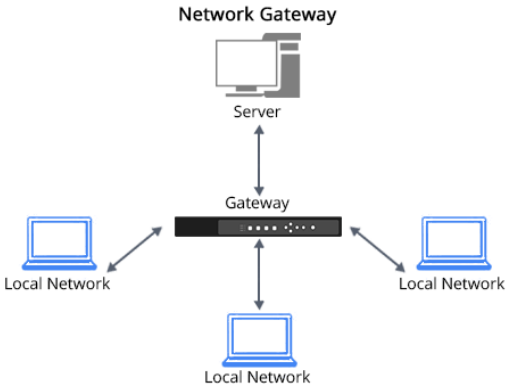
Tráfico desde la DMZ a la red interna: Generalmente, se prohíbe por completo o se restringe extremadamente. Si un servidor en la DMZ es hackeado, el atacante encontrará un “muro” entre la DMZ y la red interna.

Trafico desde la red interna a la DMZ: suele estar permitido para que los administradores gestionen los servidores.

19- ¿Qué es un Gateway?

Un Gateway o puerta de enlace es un dispositivo de la red(como un router) o software que actúa como un **punto de acceso obligatorio entre dos redes que utilizan protocolos diferentes.**

Su función principal es **traducir protocolos y permitir la comunicación entre redes** que, de otro mod, serían incompatibles.



Funciones y Características:

Conectividad entre redes diferentes: Esta es su función principal, no solo conecta una red local con internet, sino que puede interconectar cualquier tipo de red, por ejemplo, una red corporativa con una red cloud.

Punto de salida a Internet: En una red Doméstica o empresarial, el gateway predeterminado es casi siempre el router. Todos los dispositivos de tu red envían el tráfico destinado a Internet hacia la IP del gateway (el router), que se encarga de enrutarlo hacia el exterior.

Traducción de protocolos: Es lo que lo diferencia de un simple router, Un gateway puede entender y convertir la información de un protocolo a otro para que las redes puedan entenderse.

20- Según Microsoft, ¿qué significa NBL?

Según Microsoft, NBL significa Lista de Bloqueos de red. Este término está r**elacionado con la seguridad en entornos cloud y de red,** especialmente en servicios como Azure o Office 365. La NBL es una lista utilizada para bloquear direcciones IP o rangos de IP considerados maliciosos o no deseados, impidiendo que acceda a recursos de la red de Microsoft. Ayuda a mitigar amenazas como ataques DDoS, spam o intentos de intrusión.

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- MPLS: Es una técnica de transporte de datos de alto rendimiento que dirige los paquetes de información entre nodos, utilizando etiquetas en lugar de direcciones de red complejas. Funciona entre la capa 2 y la capa 3 del modelo OSI.

Características:

- Etiquetado de paquetes: cada paquete recibe una etiqueta que determina su ruta predefinida.
- Calidad de servicio: Permite priorizar tráfico crítico sobre otros datos.
- Escalabilidad: Ideal para redes grandes y complejas.
- Seguridad: Aísla el tráfico entre clientes en redes compartidas.

Usos Típicos:

- Conectividad entre sedes corporativas.
- Servicios de red privada para empresas.
- Soporte para complicaciones sensibles a la latencia.

LAN to LAN: es un enlace que conecta dos o más redes de área local geográficamente separadas, generalmente a través de Internet o de una red privada, formando una red privada virtual (VPN).

Características:

- Cifrado: Los datos se cifran para garantizar confidencialidad.
- Coste reducido: Utiliza Internet como medio de transporte, evitando costosos enlaces dedicados.
- Flexibilidad: Se puede implementar sobre cualquier conexión a Internet.
- Configuración: Requiere dispositivos VPN en ambos extremos.

Usos Típicos:

- Conexión segura entre oficinas de una misma organización.
- Extensión de la red corporativa a sucursales remotas.

MICROONDAS: Es un enlace inalámbrico que utiliza ondas electromagnéticas de alta frecuencia para transmitir datos entre dos puntos fijos con línea de vista directa.

Características:

- Línea de vista: Requiere antenas alineadas visualmente sin obstrucciones.
- Ancho de banda alto: Capaz de transmitir grandes volúmenes de datos.
- Baja LAtencia: Ideal para aplicaciones en tiempo real.
- Vulnerabilidad a interferencias: El clima puede afectar la señal.

Usos Típicos:

- Enlaces urbanos para ISPs
- Conexión entre edificios en campus.

VSAT: Es una tecnología de comunicación por satélite que utiliza antenas de pequeño diámetro para establecer enlaces de datos bidireccionales con un satélite geoestacionario.

Características:

- Cobertura global: Funciona en zonas remotas sin infraestructura terrestre.
- Costo moderado: Relativamente económico para áreas de difícil acceso.
- Latencia alta: Debido a la distancia entre la Tierra y el satélite.
- Ancho de banda limitado:Comparado con enlaces terrestres, ofrece menos capacidad.

Usos Típicos:

- Comunicación en zonas rurales.
- Telemedicina y educación a distancia en áreas remotas.
- Sistemas de punto de venta para comercios en locaciones aisladas.
- Backup para enlaces terrestres.

B- FIBRA ÓPTICA: Es un enlace que utiliza fibras de vidrio o plástico transparente para transmitir datos mediante pulsos de luz. Es el medio de transmiipon por excelencia para backbone de redes y conexiones de alta demanda.

Características:

- Ancho de banda extremadamente alto: Capaz de soportar velocidades de múltiples terabyte por segundo.
- Inmunidad electromagnética: al no usar señales eléctricas, es inmune a interferencias.
- Baja atenuación: La señal puede viajar largas distancias sin necesidad de repetidores.
- Seguridad: es muy difícil interceptar la señal sin ser detectado, ya que requiere acceso físico al cable.
- Coste: La instalación inicial es costosa, pero el costo por bit transmitido es muy bajo.

Usos Típicos:

- Conexión troncal de proveedores de internet.
- Conexión de ultima milla para usuarios residenciales y empresas.
- Campus universitarios o empresariales.
- Conexiones submarinas.

5G/LTE: Son enlaces inalámbricos que utilizan torres de telefonía celular para proporcionar conectividad de banda ancha a dispositivos móviles y fijos.

El 5G es la evolución del LTE (4G), diseñado para ofrecer mayor velocidad, menos latencia y conectar un masivo número de dispositivos.

Características:

- Alta movilidad: diseñado para usuarios en movimiento.
- Baja latencia: el 5G promete latencias ultra-bajas de hasta 1ms.
- Segmentación de red:El 5G permite crear “redes virtuales” dedicadas para aplicaciones específicas.
- Cobertura variable: La calidad de la señal depende de la proximidad a la celda y la congestión de la red.

Usos Típicos:

- Conexión a internet para smartphones.
- Competencia directa para el cable y la fibra óptica en los hogares.
- Conectividad para sensores, y ciudades inteligentes.
- Vehículos autónomos, telemedicina, realidad virtual.

C-

	Económico	performance	mayor capacidad	configuración de restricciones	soporte a mayor distancia	menor esfuerzo de configuración
MPLS	6	3	3	1	2	6
LAN to LAN	1	5	5	3	4	1
MICROONDAS	3	2	2	5	5	3
VSAT	5	6	6	6	1	4
FIBRA ÓPTICA	4	1	1	2	6	5
5G/LTE	2	4	4	4	3	2

D-

1d- El enlace elegido es **MPLS** ya que es el estándar de la industria para este tipo de escenarios. Tiene la seguridad y el performance que requiere una operación de call centers.

2d- El enlace perfecto es **VSAT** debido a que es la única tecnología que cumple con los requisitos fundamentales para llevar a cabo la operaciones una ubicación remota sin infraestructura.

3d- El enlace ideal es **MICROONDA** porque es rápida de instalar, extremadamente económica a corto y largo plazo y ofrece un performance comparable al de un cable de fibra.

22- Describir la tecnología LTE.

Tecnología LTE (Long Term Evolution)

Es una tecnología de comunicación móvil de cuarta generación (4G), diseñada para mejorar la velocidad, capacidad y eficiencia de las redes celulares en comparación con 2G y 3G.

Características principales:

- Alta velocidad: Permite velocidades de descarga de hasta 100Mbps y de subida de 50 MBps.
- Basada en IP: Todo tráfico viaja en forma de paquetes IP, lo que hace la red más eficiente.

- Uso de OFDMA: divide el espectro de múltiples subcanales, optimizando el uso del ancho de banda.
- Compatibilidad con MIMO (Multiple Input, Multiple Output): permite el uso de múltiples antenas en transmisión y recepción, mejorando la cobertura de velocidad.

Ventajas:

- Mayor cobertura y velocidad que 3G.
- Mejor experiencia de usuario para aplicaciones de streaming, navegación y descargas pesadas.
- Red optimizada para servicios multimedia.

Limitaciones:

- Requiere dispositivos compatibles con LTE.
- La velocidad real depende de la congestión, cobertura y calidad de la red.
- En zonas rurales puede ser menos estable que en entornos urbanos

Arquitectura de Red:

Es más plana y simple que sus predecesoras.Sus elementos principales son:

- eNodeB(Evolved Node B): Es más inteligente que las de generaciones anteriores ya que se comunica directamente con otros eNodeBs.
- EPC (Evolved Packet Core): El núcleo de red.
- MME (Mobility Management Entity): Gestiona la movilidad y las sesiones de los usuarios.
- S-GW (Serving Gateway): El punto de anclaje para la movilidad.
- P-GW(Packet Data Network Gateway): Conecta la red LTE a Internet y otros servicios de datos.
- HSS (Home Subscriber Server): La base de datos centralizada que contiene la información de los suscriptores.

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

Microsoft Teams es una plataforma de colaboración y comunicación unificada que forma parte del ecosistema Microsoft 365. Es un centro de trabajo digital que integra chat, videollamadas, almacenamiento de archivos e integración con aplicaciones de Office en un solo lugar.

Características Principales:

- **Chat y conversaciones**: posee canales que son espacios organizados por temas, proyectos o departamentos dentro de un equipo. Chats privados y grupales, para conversaciones uno a uno o en grupos más pequeños fuera de los canales. Menciones para alertar a un usuario o a todo el equipo.
- **Reuniones y videoconferencias:** Integración total con el calendario de Outlook, se puede compartir pantalla, tiene una pizarra digital, fondos virtuales, salas para reuniones más pequeñas y grabación automática en la nube. Se realizan eventos en vivo con capacidad para hasta 10.000 participantes.
- **Llamadas de Voz:** Puede reemplazar a un central telefónico tradicional con números directos, menús de voz y transferencias de llamadas.
- **Almacenamiento y colaboración en archivos:** Integración con SharePoint y OneDrive, cada canal tiene automáticamente una carpeta en SharePoint donde se almacenan todos los archivos compartidos de ese canal, se puede editar en simultáneo documentos de Word, Excel, PowerPoint sin salir de Teams.
- **Integraciones:** La integración con Office es nativa y perfecta, con App Store también permite agregar cientos de aplicaciones de terceros como trello, Salesforce, ETC. directamente dentro del canal. y admite bots y automatizaciones.
- **Seguridad y Cumplimiento:** tiene Datos encriptados en tránsito y en reposo.

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

Aplicar calidad a un enlace MPLS significa poder ofrecer garantías de Servicio (Service Level Agreements) sobre parámetros claves de rendimiento:

- **Ancho de banda:** Reservar una cantidad minia (y a veces máxima) de capacidad para una aplicación.
- **Latencia (Delay):** Asegurar que el retraso para una aplicación sensible (como la voz) se mantenga por debajo de un umbral crítico.
- **Variación de la latencia (Jitter):** Mantener la latencia consistente, crucial para voz y video.

- **Pérdida de Paquetes (Packet Loss):** Minimizar la cantidad de paquetes que se descartan, lo que es vital para cualquier aplicación en tiempo real.

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

	COAXIAL	UTP	FIBRA ÓPTICA
Definición	Un cable coaxial es un tipo de cable que transmite señales eléctricas de alta frecuencia. Su nombre se debe a que tiene dos conductores que comparten el mismo eje (o "coaxial").	Un cable UTP (Unshielded Twisted Pair - Par Trenzado No Apantallado) es el cable de red más común, el que normalmente se usa para conectar computadoras a routers.	Un cable de fibra óptica es un medio de transmisión de datos que utiliza hilos delgados de vidrio o plástico para enviar información a través de pulsos de luz. Es la tecnología más avanzada y la más rápida disponible para uso comercial.
Medio	Núcleo de cobre y malla	Hilos de cobre trenzados	Hilos de vidrio o plástico
Señal	Impulsos eléctricos	Impulsos eléctricos	Pulsos de luz
Velocidad	Hasta 1 Gbps	Hasta 10 Gbps	10 Gbps o más
Costo	Económico	Muy económico	Costo de instalación alto
Alcance	Medio	Corto (100 metros)	Muy largo (kilómetros)
Interferencia	Moderada	Alta	Inmune a interferencias
Uso Común	Televisión por cable, internet	Redes locales (hogares, oficinas)	Internet de alta velocidad, centros de 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).

Según Cisco, CCENT (Cisco Certified Entry Networking Technician), CCNA (Cisco Certified Network Associate) y CCNP (Cisco Certified Network Professional) son certificaciones que validan las habilidades y el conocimiento en redes. Forman parte de una ruta de aprendizaje (o *track*) progresiva que permite avanzar en la carrera profesional.

CCENT (Cisco Certified Entry Networking Technician):
Era el primer paso en la ruta de certificaciones de Cisco. Certificaba el conocimiento básico sobre la instalación, operación y resolución de problemas en una red de sucursal de una empresa, incluyendo la seguridad de la red. Esta certificación fue retirada por Cisco en el año 2020.

CCNA (Cisco Certified Network Associate)*:*
Certificación básica ampliamente reconocida que valida la capacidad de una persona para instalar, configurar, operar y solucionar problemas en redes enrutadas y conmutadas de tamaño mediano. Al obtener la certificación CCNA, los profesionales demuestran su experiencia en los fundamentos de redes, seguridad y automatización.

CCNP (Cisco Certified Network Professional):
Certificación de nivel avanzado que valida la capacidad de un profesional para planificar, implementar y resolver problemas de soluciones de red complejas. Se basa en los conocimientos básicos adquiridos con la certificación CCNA, demostrando experiencia en áreas como enrutamiento, conmutación, seguridad y administración de redes.
Para obtenerla se deben aprobar dos exámenes, uno básico de tecnología y otro de concentración y especialización que se elige de entre una serie de dominios, los que se pueden elegir (CCNP Enterprise, Colaboración CCNP, Centro de datos CCNP, Seguridad CCNP, Proveedor de servicios CCNP).

El Track Routing & Switching de Cisco es un programa de certificación que valida habilidades para diseñar, implementar, operar y solucionar problemas en redes enrutadas y conmutadas, es decir, aquellas que permiten la comunicación entre diferentes redes y la conexión de dispositivos en una misma red local, respectivamente. Este track histórico es fundamental para la carrera de especialistas en redes. En la actualidad, estos conocimientos han sido consolidados en el CCNP Enterprise y abarca una gama más amplia de temas; incluyendo redes inalámbricas, automatización y virtualización, lo que lo hace más relevante para las redes modernas.

El Track de Cisco Security se enfoca en proteger las redes, sistemas y datos. Los profesionales de esta área se especializan en la implementación de soluciones de seguridad como firewalls, VPNs y sistemas de prevención de intrusiones. Es importante destacar que no es un producto o servicio específico, sino que hace alusión a soluciones y capacidades de seguridad que ofrece Cisco para proteger redes, nubes, terminales y correos electrónicos contra ciberamenazas.

27- Explique el modelo OSI.

El modelo OSI (Open Systems Interconnection) es un marco de referencia conceptual creado por la Organización Internacional de Normalización (ISO). Su objetivo principal es estandarizar cómo se comunican los sistemas informáticos entre sí, sin importar el hardware o software que usen.
El modelo divide el proceso de comunicación en siete capas distintas, cada una con una función específica:

- *Capa 7 (Aplicación):* Es la capa con la que se interactúa directamente.
- *Capa 6 (Presentación):* Traduce el formato de los datos.

- *Capa 5 (Sesión):* Establece, gestiona y termina la conexión entre las aplicaciones.
- *Capa 4 (Transporte):* Se encarga de la entrega de los datos.
- *Capa 3 (Red):* Maneja el direccionamiento y el enrutamiento.
- *Capa 2 (Enlace de Datos):* Gestiona la transferencia de datos entre dos dispositivos conectados directamente.
- *Capa 1 (Física):* Se encarga de la transmisión de datos sin procesar a través de un medio físico (cables, ondas, etc.).

Cada capa se comunica solo con la capa directamente superior e inferior, lo que permite que el sistema sea modular y flexible.

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

El estandar IEEE 802.3 es el conjunto de estándares desarrollados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que define la tecnología Ethernet para redes de área local (LAN) y metropolitana (MAN). Estos estándares especifican cómo se implementan la capa física y la capa de control de acceso al medio (MAC) en las redes cableadas. Cubren aspectos como la velocidad de transmisión, los medios físicos (cobre o fibra), el método de acceso a la red como el CSMA/CD, y el formato de la trama Ethernet.
Es el estándar más común para la comunicación de redes locales (LAN) y es fundamental en el mundo de las redes informáticas.

Su implementación se realiza a través de la tecnología Ethernet, que funciona en las capas 1 (Física) y 2 (Enlace de Datos) del modelo OSI y requiere tanto hardware físico como protocolos de software.

El hardware se encarga de la infraestructura física por donde viajan los datos.

- Medios de Transmisión: Se usan cables de red, siendo el UTP el más común, aunque también se usa fibra óptica para mayores distancias. El estándar especifica la forma y el tamaño de los conectores y cables.
- Tarjetas de Interfaz de Red (NIC): Cada dispositivo (computadora, servidor) necesita una NIC. Este es el hardware que se conecta al cable y que es capaz de procesar las señales eléctricas o de luz para transmitir y recibir datos.
- Dispositivos de Conmutación: Switches, que conectan múltiples dispositivos y dirigen el tráfico de datos de manera eficiente.

El protocolo define cómo los dispositivos organizan y gestionan el flujo de datos.

- Trama de Ethernet: Los datos que vienen de la capa de red (como los paquetes IP) se empaquetan en una "trama" de Ethernet. Esta trama tiene un formato específico que incluye la dirección MAC de origen y destino para identificar los dispositivos.
- CSMA/CD: Este protocolo es la regla de control de acceso al medio. Antes de transmitir, un dispositivo "escucha" el medio para ver si está libre. Si detecta una colisión (dos dispositivos transmitiendo al mismo tiempo), detiene la transmisión, espera un tiempo aleatorio y lo intenta de nuevo.

VENTAJAS	DESVENTAJAS
Interoperabilidad: Es un estándar universal que garantiza que los dispositivos de diferentes fabricantes funcionen juntos sin problemas.	**Distancia Limitada:** Los cables de cobre UTP (el tipo más común) tienen un límite de 100 metros.
Escalabilidad: Se ha adaptado para soportar velocidades muy altas, desde 10 Mbps hasta 100 Gbps o más.	**Vulnerabilidad a Interferencias:** Los cables de cobre son susceptibles a las interferencias electromagnéticas, lo que puede afectar el rendimiento.
Costo: La infraestructura de hardware es relativamente económica y su implementación es accesible para redes de cualquier tamaño.	**Manejo del Cableado:** Las redes grandes pueden volverse complejas y difíciles de gestionar si no hay una buena organización del cableado.
Fiabilidad: Es una tecnología robusta y probada que ofrece conexiones estables y seguras.	**Topología de red:** Aunque flexible, su configuración puede ser un desafío en entornos muy grandes o complejos sin el equipo adecuado.

29- Explicar el estándar IEEE 802.4 regula la red.

IEEE 802.4, también conocido como el estándar Token Bus, es un protocolo de red definido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

Este estándar fue desarrollado para proporcionar un medio confiable de comunicación en redes de área local (LAN) que operan en entornos industriales y de automatización.

Este estándar se centra en la transmisión de datos de manera determinista y predecible, lo que lo hace especialmente adecuado para aplicaciones que requieren tiempos de respuesta consistentes y controlados.

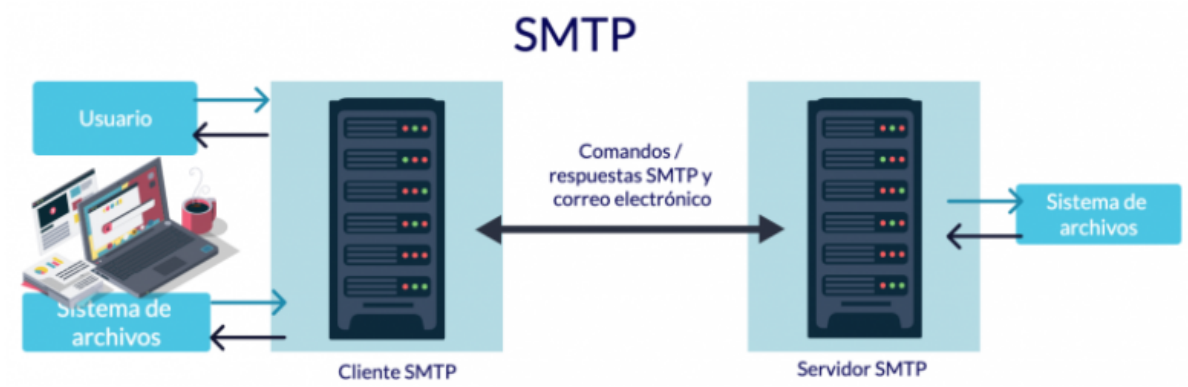
El estándar IEEE 802.4 funciona usando un método de acceso al medio llamado *token passing*, en una topología de bus lógico, aunque la topología física sea un bus.

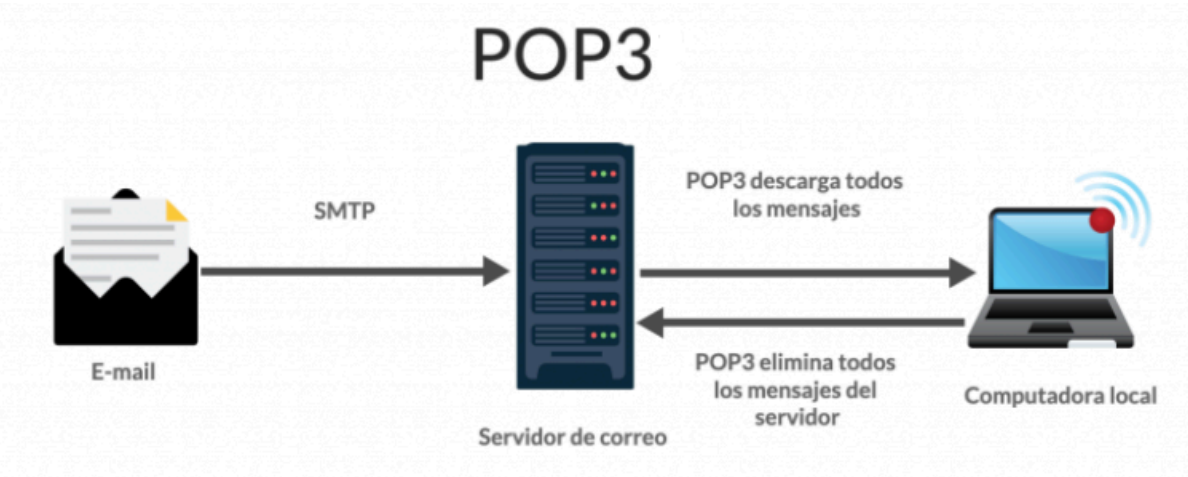
- *Testigo (token):* Hay un mensaje especial, el "testigo", que circula por la red en un orden predefinido.
- *Transmisión de datos:* Solo el nodo (computadora, dispositivo) que tiene el testigo puede transmitir datos. Si un nodo quiere enviar información, espera hasta recibir el testigo.
- *Liberación del testigo:* Una vez que el nodo ha terminado de transmitir sus datos, libera el testigo, que pasa al siguiente nodo en la secuencia preestablecida.
- *Control:* Si un nodo recibe el testigo pero no tiene datos para enviar, simplemente lo pasa al siguiente en la secuencia, asegurando que todos los nodos tengan una oportunidad de acceso.

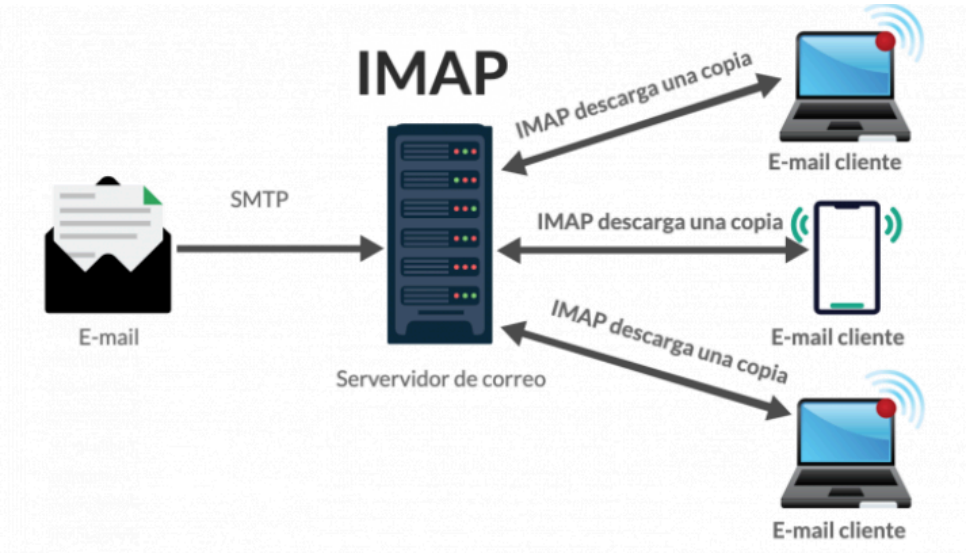
Este método garantiza que ningún nodo sea excluido de la red y ofrece un rendimiento predecible, lo cual fue útil para redes industriales que necesitaban un control estricto del tiempo de transmisión.

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

Los protocolos de correo electrónico son un conjunto de reglas que rigen cómo se envían, reciben y almacenan los correos electrónicos. Los principales protocolos son SMTP para enviar correos, y POP3 e IMAP para recibir correos: SMTP maneja la transmisión de correo entre servidores, mientras que POP3 descarga los correos electrónicos a un dispositivo e IMAP sincroniza los correos electrónicos en múltiples dispositivos.







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

POP3 e IMAP manejan los correos entrantes y funcionan de diferentes maneras para recuperar o acceder a los mensajes de email. Por lo tanto, se consideran protocolos de acceso al correo.

Mientras que el protocolo POP3 asume que se accede a tu email solo desde una aplicación, IMAP permite el acceso simultáneo por varios clientes.

IMAP es más adecuado si se accede al email desde diferentes ubicaciones o si los mensajes son administrados por múltiples usuarios.

POP3, en cambio, descarga los correos a la computadora local, eliminándolos del servidor. Por lo tanto, reduce el espacio que usa la cuenta de correo electrónico en el servidor web.

32- Diferencias entre IPV4 e IPV6

	IPV4	**IPV6**
Longitud de la dirección	32 bits	128 bits
Formato	Cuatro números decimales, separados por puntos (ej: `192.168.1.1`)	Ocho grupos de cuatro dígitos hexadecimales, separados por dos puntos (ej: `2001:0db8::8a2e:0370:7334`)
Número de direcciones	Aproximadamente 4.3 mil millones (escaso)	Cantidad virtualmente ilimitada (340 sextillones)
Configuración	Requiere configuración manual o DHCP para asignar direcciones.	Soporta autoconfiguración (SLAAC) sin necesidad de un servidor DHCP.
Seguridad	IPsec es opcional y no está integrado por defecto.	IPsec está integrado en el protocolo, ofreciendo seguridad nativa.
Rendimiento	La cabecera del paquete es más grande y requiere más procesamiento.	La cabecera del paquete es más simple, lo que mejora la eficiencia de enrutamiento y el rendimiento.

33- (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.

- **CELIA, BRUNO:**
  Tengo un poco de experiencia en redes, en mi casa tengo configurados algunos artefactos Smart, puse en Bridge dos routers para bypassear el DNS de Fibertel y que use el de Cloudflare (1.1.1.1). De chico me gustaba abrir servidores para jugar con mis amigos por lo que he hosteado mi propio servidor de Counter Strike (para lo cual tuve que abrir puertos UDP como el 27015 y exponerlo) para lo cual tuve que instalar un firmware moddeado ya que Arnet no te lo permitía hacer, también servidores de Minecraft y de MU Online, pero este último en un hosting subiendo los archivos del juego por FTP. También he configurado algún nginx para hostear un docker en una VPS por SSH, darle un certificado SSL a una página y configurar los DNS en Cloudflare. Aparte de eso, en mi trabajo de Full Stack hago lateralmente algunas tareas de DevOps como configurar pipelines en AWS o configurar el API Gateway para darle acceso a ciertos roles ciertos servicios.

- **DE LUCA, LEILA GISELLE:**
  No tengo ninguna experiencia en redes.

- **DE SOUZA GOMES, ANNA CLARA:**
  No tengo ninguna experiencia en redes

- **MARTINI, FERNANDO PABLO:**
  No tengo ninguna experiencia en redes.

Bibliografía:

- **Aprendiendo Ciberseguridad. (2024). *Flags de TCP (El nivel de Transporte) – Aprendiendo Ciberseguridad paso a paso #66* [Vídeo]. YouTube. https://www.youtube.com/watch?v=qAALjYLaG3c**

- **CCNA Desde Cero. (s.f.). *Protocolo de Resolución de Direcciones o ARP*. Recuperado el 20 de septiembre de 2025, de https://ccnadesdecero.es/protocolo-resolucion-direcciones-arp/**

- **Cisco Systems, Inc. (2025). *Certificación CCNP Enterprise*. Recuperado el 20 de septiembre de 2025, de https://www.cisco.com/site/us/en/learn/training-certifications/certifications/enterprise/ccnp-enterprise/index.html**
    -
- **Cisco Systems, Inc. (s.f.). *Protocolo Spanning Tree*. Recuperado el 20 de septiembre de 2025, de https://www.cisco.com/c/es_mx/tech/lan-switching/spanning-tree-protocol/index.html**

- **Cloudflare. (s.f.). *¿Qué es el modelo OSI?*. Recuperado el 15 de septiembre de 2025, de https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/**

- **Duò, M. (2023, 12 de septiembre). *IPv4 vs IPv6: ¿Cuál es la diferencia entre los dos protocolos?* Kinsta. Recuperado de https://kinsta.com/es/blog/ipv4-vs-ipv6/**

- **EcuRed. (s.f.). *Estándares IEEE 802.3*. Recuperado el 15 de septiembre de 2025, de https://www.ecured.cu/Est%C3%A1ndares_IEEE_802.3**

- **Firewall.cx. (s.f.). *The IEEE 802.3 Frame Format*. Recuperado el 15 de septiembre de 2025, de https://www.firewall.cx/networking/ethernet/ieee-8023-frame.html**

- **FP Informática. (s.f.). *¿Qué es la certificación CCNA Routing and Switching de Cisco?* Recuperado el 15 de septiembre de 2025, de https://www.fp-informatica.com/que-es-la-certificacion-ccna-routing-and-switching-de-cisco/**

- **Hernández, J. (2025). *¿Qué es el protocolo IEEE 802.4? TOKEN BUS.* SaberPunto. Recuperado de https://saberpunto.com/tecnologia/que-es-el-protocolo-ieee-8024-autobus-simbolico/**

- **IBM. (s.f.). *Protocolo de configuración dinámica de host (DHCP) en IBM i*. Recuperado el 20 de septiembre de 2025, de https://www.ibm.com/docs/es/i/7.5.0?topic=protocol-dhcp-concepts**

- **IBM. (2021). *Redes de área local virtuales (VLAN).* En IBM Knowledge Center. Recuperado de https://www.ibm.com/docs/es/aix/7.1.0?topic=cards-virtual-local-area-networks**

- **IBM. (2025). *¿Qué es una red de área de almacenamiento (SAN)?* In *IBM Think Topics: Storage Area Network*. Recuperado de https://www.ibm.com/es-es/think/topics/storage-area-network**

- **Microsoft. (2025).** ***¿Qué es una red privada virtual o VPN? ¿Por qué debería usar una red privada virtual o VPN?*** **In** ***Azure Cloud Computing Dictionary*****. Recuperado de** https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-vpn

- **Sacco, L. (2024, 21 de febrero).** ***Arquitectura TCP/IP: La Espina Dorsal de la Conectividad en la Era Digital.*** **Peritos Informáticos. Recuperado de** https://peritosinformaticos.ar/arquitectura-tcp-ip/?srsltid=AfmBOopLOFcKrAVx5lX2Wwafs1GSTUdw9-OCHPqYhckMtaIHC5RNw7od

- **Sharma, V. (2024, 20 de septiembre).** ***CCNA vs CCNP: Diferencia entre ambas certificaciones de Cisco*****. UniNets. Recuperado de** https://www.uninets.com/blog/ccna-vs-ccnp-certification

- **WatchGuard Technologies.** ***Acerca de Redes Virtuales de Área Local (VLAN).*** **En Fireware Help (v. 12). Recuperado de** https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/networksetup/vlans_about_c.html