TRABAJO PRÁCTICO N° 1
PROXY SOCKS REDES

Profesor:

- *Lucas Rusatti*

Alumnos/as:

- *Mirengo Walter*
- *Kaen Martin*
- *Amado Paula*

Materia: Programación sobre Redes

Año: 2024

ÍNDICE

1 ¿Qué es una VLAN?

Las VLAN (Virtual LAN), es una tecnología de redes que nos permite crear redes lógicas independientes dentro de la misma red física. El objetivo de usar VLAN en un entorno doméstico o profesional, es para segmentar adecuadamente la red y usar cada subred de una forma diferente, además, al segmentar por subredes usando VLANs se puede permitir o denegar el tráfico entre las diferentes VLAN gracias a un dispositivo L3, como un router o un switch multicapa L3.

2 ¿Qué es una VPN?

Es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestion de una red privada, esto se realiza estableciendo una conexión virtual de punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

3 ¿Qué es SAN?

Una red de área de almacenamiento (SAN) es una red dedicada que se adapta a un entorno específico y combina servidores, sistemas de almacenamiento, conmutadores de red, software y servicios.

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

Los tres son dispositivos de hardware que posibilitan la conexión de computadoras a redes.

HUB: Es el dispositivo más sencillo de todos. Un HUB tiene la función de interconectar los ordenadores de una red local. Comparado con el switch y el router, es mucho más simple, ya que solo se dedica a recibir datos procedentes de un ordenador para transmitirlo a los demas. Digamos que se trata de un punto central de conexión en una red. Normalmente son usados para conectar segmentos de una red LAN a través de sus diferentes puertos. Cuando un paquete es recibido en un puerto, es copiado a todos los demas puertos, para que cualquier nodo conectado a la red, pueda verlo, en el momento que esto ocurre, ningún switch puede enviar una señal. Su liberación surge despues que la señal anterior haya sido completamente distribuida.

Los HUBS, se utilizan para la creación de redes locales con topología tipo estrella, en los cuales se interconectan el resto de los equipos, asi como para realizar análisis de redes, ya que al solamente repetir y repartir los mismos datos, se puede analizar fácilmente el tráfico e información que fluye por la red.

SWITCH: El SWITCH es un aparato muy semejante al HUB, pero envía los datos de manera diferente, a través de un switch aquella información proveniente del ordenador de origen es enviada al ordenador de destino, básicamente, los switchs crean una especie de canal de comunicación exclusiva entre el origen y el destino, asi la red no queda "limitada" a un solo equipo en el envio de información, a diferencia del HUB. Está concebido para trabajar en redes con una cantidad de máquinas más elevado que un HUB, esta característica también disminuye errores (colisiones de paquetes de datos, por ejemplo). Asi como en el hub, un switch tiene varios puertos y la cantidad varia de la misma forma, el aparato se encarga de filtrar y reenviar los paquetes entre fragmentos de red LAN. Opera en la capa de enlace, a veces, incluso en la capa de red, por lo tanto soporta cualquier protocolo de paquetes.

ROUTER: El ROUTER es el dispositivo que se encarga de reenviar los paquetes entre distintas redes. Es más "inteligente" que el switch, además de cumplir con la misma función, tiene además la capacidad de escoger la mejor ruta para que un determinado paquete de datos llegue a su destino. Los ROUTERS, son capaces de interconectar varias redes y generalmente trabajan en conjunto con HUBS y SWTICHS. Suelen poseer recursos extras, como firewall, lo que lo hace más seguro. El equipo conecta al menos dos redes, normalmente una red LAN y una conexión WAN hacia tu ISP, usa cabeceras y tablas de enrutamiento para determinar el mejor camino para que el paquete llegue a su destino, usando protocolos como el ICMP para comunicarse con otros routers y asi descubrir el camino más eficiente entre dos nodos. Puede decirse que el router elige la vía menos congestionada para enviar la información.

Mientras que un HUB o SWITCH se encargan de transmitir frames, el trabajo de un router es "enrutar" paquetes a otras redes hasta que llegue a su destino final. Los routers de banda ancha tienen un puerto WAN que permite conectar un cable ADSL.

REPETIDOR: Un REPETIDOR simplemente regenera y amplifica una señal de red que se ha debilitado o distorsionado debido a una atenuación o interferencia. Cuando una señal se transmite a larga distancia, puede debilitarse o distorsionarse debido a diversos factores, como la atenuación del cable, la interferencia electromagnética o los reflejos de una señal.

5 ¿QUÉ ES UN PROTOCOLO DE COMUNICACIONES?

Un protocolo de red es un estándar de comunicaciones. Contiene las reglas necesarias y la información sobre como la computadoras intercambian datos entre sí. Se requiere una interacción de diferente tipo para diversas tareas, como por ejemplo, el simple intercambio de mensajes. Cada uno de los protocolos de comunicación de redes asume entonces una tarea específica en el medio que se requiera.

6 EXPLIQUE TCP/IP Y NETBIOS, RESUMA SUS DIFERENCIAS. (ACA SI EXPLICAR CADA UNO Y SUS DIFERENCIAS)

TCP/IP es un estándar de comunicación que ayuda a que Internet funcione. Es un protocolo de enlace de datos que se usa en Internet para que los ordenadores y otros dispositivos envíen y

reciban datos. TCP/IP son las siglas en ingles de “Transmission Control Protocol/Internet Protocol”, Posibilita que los dispositivos conectados a Internet se comuniquen entre si en varias redes.

NetBIOS: Lo que permite NetBIOS es que las aplicaciones se comuniquen con la red. Un equipo en una red local se comunica con otro a través de una conexión utilizando lo que se conoce como datagramas NetBIOS. Su función es establecer la sesion y mantener las conexiones.

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** está formado por varias capas de información que permiten la transmisión de datos a través de la red. El modelo TCP/IP se basa en cuatro capas principales: Aplicación, Transporte, Red y Enlace. Cada capa añade su propio encabezado al paquete, y la información relevante para cada capa se encapsula dentro de esos encabezados.

7.1.1 Estructura de un paquete de datos TCP/IP:

1. **Capa de enlace** (Enlace de Datos):
   - Aquí se encuentra la dirección física (direcciones MAC) de origen y destino. En esta capa se define el protocolo Ethernet.
   - Encabezado de capa de enlace: Contiene información como la dirección MAC de origen y destino.
2. **Capa de red** (IP):
   - Encabezado IP: Contiene la dirección IP de origen y destino, junto con información sobre el tamaño del paquete, el tiempo de vida (TTL), el tipo de servicio, y más.
   - Datos transportados por IP: El paquete de la capa de transporte (TCP o UDP).
3. **Capa de transporte** (TCP o UDP):
   - **Encabezado TCP** (para conexiones orientadas a conexión): Contiene información como los puertos de origen y destino, números de secuencia, números de acuse de recibo (ack), flags, tamaño de ventana, checksum, y otros parámetros.
   - **Encabezado UDP** (para conexiones no orientadas a conexión): Es más simple, con información sobre los puertos de origen y destino, longitud del paquete y checksum.
   - Datos transportados por TCP o UDP: La carga útil de la aplicación.
4. **Capa de aplicación**:
   - Aquí están los datos que son utilizados por la aplicación final, como el contenido de una página web (HTTP), un archivo transferido (FTP), o un correo electrónico (SMTP).

7.1.2 Flags en un paquete TCP:

Un **"flag"** en un paquete TCP es un bit en el encabezado de la capa de transporte (TCP) que indica el estado o el control de una conexión. Los flags ayudan a coordinar y gestionar la

transmisión de datos, controlando cosas como el establecimiento de una conexión, su finalización, o la solicitud de retransmisiones. Estos flags son cruciales para el proceso de control de flujo y de establecimiento/terminación de conexiones en el protocolo TCP.

Algunos de los **Flags más comunes** en TCP son:

- **SYN** (Synchronize): Se utiliza al inicio de una conexión TCP, para sincronizar los números de secuencia entre las partes.
- **ACK** (Acknowledgment): Indica que el paquete es una respuesta a un paquete recibido, confirmando la recepción de datos.
- **FIN** (Finish): Se utiliza para terminar una conexión TCP de manera ordenada.
- **RST** (Reset): Finaliza una conexión de manera abrupta, sin completar el protocolo de cierre normal.
- **PSH** (Push): Indica que los datos deben ser entregados al proceso de la aplicación lo antes posible.
- **URG** (Urgent): Señala que los datos contenidos son urgentes y deben ser procesados inmediatamente.
- **ECE** (Explicit Congestion Notification Echo): Indica congestión en la red cuando se utiliza con el protocolo ECN.
- **CWR** (Congestion Window Reduced): Señala que la ventana de congestión se ha reducido.

Estos **flags** juegan un papel importante en el **protocolo de control de transmisión (TCP)**, ya que garantiza una entrega confiable y ordenada de datos entre las computadoras en una red.

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

El termino red hace referencia a un conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión logica de los sistemas. Las redes se configuran con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, bases de datos o impresoras. En función de tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes, se encuentran:

- Personal Area Network (PAN) o red de área local.
- Local Area Networks (LAN) o red de área local.
- Wireless Local Area Network o red de área local inalámbrica.
- Metropolitan Area Networks (MAN) o red de área metropolitana.
- Wide Area Networks (WAN) o red de área amplia.
- Global Area Networks (GAN) o red de área global.

La conexión física en la que se basan estos tipos de redes puede presentarse por medio de cables o llevarse a cabo con tecnológica inalámbrica.

PAN: Es una red pequeña, generalmente utilizada para la comunicación entre dispositivos personales como teléfonos móviles, tablets, computadoras personales y otros dispositivos periféricos como impresoras y auriculares.

LAN: conecta computadoras y otros dispositivos dentro de un área geográfica limitada como una oficina, escuela o campus. Las LAN permiten compartir recursos como archivos, impresoras y conexiones a Internet. La tecnología Ethernet es comúnmente utilizada en las LAN.

WLAN: es una variante LAN que utiliza tecnología inalámbrica, como Wi-Fi, para conectar dispositivos en un área geográfica limitada. Las WLANs permiten a los dispositivos conectarse a la red sin necesidad de cables físicos.

MAN: conecta varias LANs en un área geográfica más amplia, como una ciudad o una gran área urbana. La suelen utilizar organizaciones que tienen oficinas o instalaciones dispersas por toda una ciudad.

WAN: conecta múltiples LANs y MANs a través de grandes distancias geográficas. Internet es el ejemplo más grande y conocido de una WAN, permitiendo la comunicación y transferencia de datos entre usuarios de todo el mundo.

GAN: Es una red que abarca el globo, interconectando múltiples WANs y otras redes de menor escala. Internet puede considerarse una GAN en su forma más extensa.

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

Las topologías de red se refieren a la forma en la que está dispuesta una red, incluyendo sus nodos y las líneas utilizadas para asegurar la transmisión y recepción de datos de manera correcta y segura. En función de esta disposición se pueden evitar cortes innecesarios o incrementar el flujo de la información transmitida. En definitiva, las topologías de red es la forma en la que se organizan los elementos de una red de comunicaciones. Las estructuras de las topologías de red se pueden representar física o lógicamente.

Topología de bus: Tambien se le conoce como topología de red troncal, bus o linea. En esta red todos los dispositivos se conectan directamente a un canal y no existe otro vínculo entre nodos. Los datos fluyen a lo largo del cable a medida que viaja a su destino. Se instala fácilmente, tiene poco cableado y es facil aumentar o disminuir el número de los aparatos que se adjuntan a la red. Alguno inconvenientes son problemas de congestión, colisión y bloqueo, además, si existe en el canal, todos los dispositivos quedaran desconectados.

Topología de anillo: En esta red cerrada los nodos se configuran en un patrón circular con estructuras de anillo. Cada nodo se vincula a uno con los dos contiguos. Al llegar un mensaje a un dispositivo, este comprueba los datos de envio y si no es el receptor, lo pasa al siguiente, y asi sucesivamente hasta que lo recibe el destinatario. Ofrece mejor rendimiento que la de bus, es facil de instalar y localiza pero los nodos no pueden enviar mensajes al mismo tiempo. Es decir que no puede desconectarse ningún dispositivo o se perderá la conexión entre todos.

Topología de estrella: Es el tipo de topología más común, los dispositivos se conectan a un punto central (HUB) que actúa a modo de servidor. Este HUB gestiona la transmisión de datos a través de la red. Permite que todas las estaciones se comuniquen entre sí. Sin embargo si el nodo central tiene algún error, toda la red queda expuesta y puede provocarse desconexión. Existe tambien la topología de estrella extendida que funciona igual pero cada elemento que se conecta al nodo central se convierte en el centro de otra estrella. El cableado es más corto pero se conectan menos dispositivos.

Topologia de árbol: Esta red tiene un punto de enlace troncal y a partir de este se ramifican los demas nodos. El eje central es como el tronco del árbol, las ramas se conectan son los concentradores secundarios o los nodos de control y los dispositivos conectados se conectan a los branches. Puede ser de árbol binario en el que cada nodo se fragmenta en dos enlaces de árbol o backbone, un tronco con un cable principal que lleva información al resto de nodos ramificados. Entre las ventajas de esta tipología esta que no se presentan problemas entre los subsiguientes dispositivos si falla uno, reduce el tráfico de red y es compatible con muchos proveedores de hardware y de software. Es aconsejable para redes de gran tamaño.

Topologia de malla: En esta clase de red informática todos los componentes o nodos están interconectados y enlazados directamente mediante vías separadas. La ventaja es que si una conexión falla, existen caminos alternativos para que la información fluya por varias rutas alternativas. Para ello debe haber una limitada cantidad de dispositivos que unir.

Topologia hibrida: En este caso, se mezclan dos tipologías diferentes de topología. Adapta la estructura a las necesidades físicas del lugar en donde se lleva a cabo la instalación. Seguridad, velocidad e interconexión son los requisitos básicos.

Topología de mixta: Esta topología mezcla dos o más topologías de red diferentes. Adaptar su estructura a las necesidades físicas del lugar en que se realiza la instalación, asi como a los requerimientos de seguridad, velocidad e interconexión. Es fiable porque permite detectar errores y resolver problemas de forma sencilla, es eficaz, escalable y flexible. Sin embargo, es dificil detectar fallas, tiene diseño complejo y dificil, el mantenimiento es caro.

Topologia totalmente conexa: En este caso existe un enlace directo entre todos los pares de sus nodos. Se trata de redes caras de configurar, pero siempre con un alto grado de confiabilidad. Existen muchas rutas para los datos que ofrecen la gran cantidad de enlaces redundantes entre nodos. Esta topología se usa sobre todo para aplicaciones militares.

10 Explicar el servicio DHCP.

El protocolo de configuración dinámica (DHCP) es un protocolo cliente-servidor que proporciona automáticamente un host de protocolo de Internet (IP) con su dirección de IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada.

DHCP se define como un estándar del Grupo de trabajo de ingenieria de Internet (IETF) basado en el protocolo de arranque (BOOTP), con el que DHCP comparte muchos detalles de

implementación. DHCP permite a los hosts obtener la información de configuración TCP/IP necesaria de un servidor DHCP.

11 Explicar el servicio DNS.

El sistema de nombres de dominio (DNS) es el directorio telefónico de Internet. Las personas acceden a la información en linea a través de nombres de dominio como ny.times.com o espn.com. Los navegadores web interactúan mediante direcciones de Protocolo de Internet (IP). El DNS traduce los nombres de dominio a direcciones IP para que los navegadores puedan cargar los recursos de Internet.

Cada dispositivo conectado a Internet tiene una dirección IP única que otros equipos pueden usar para encontrarlo. Los servidores DNS suprimen la necesidad de que los humanos memoricen direcciones IP tales como 192.168.1.1 (en IPv4) o nuevas direcciones IP alfanuméricas más complejas, tales como 2400:cb00:2048:1::c629:d7a2 (en IPv6).

12 Explicar las tecnologías Wireless, y sus estándares.

Las tecnologías Wireless (inalámbricas) permiten la comunicación de dispositivos sin la necesidad de cables físicos, utilizando ondas electromagnéticas. Estas tecnologías se han desarrollado y estandarizado a lo largo del tiempo para asegurar la compatibilidad, rendimiento y seguridad en diversas aplicaciones.

Wi-Fi (Wireless Fidelity):

Es la tecnología inalámbrica más común para redes locales (LAN). Utiliza ondas de radio para transmitir datos entre dispositivos, como teléfonos, laptops y routers.

Estándares Wi-Fi:

IEEE 802.11: Es el conjunto de estándares para Wi-Fi. Se ha actualizado varias veces, con mejoras en velocidad, alcance y seguridad.

- 802.11a (1999): Opera en la banda de 5GHz con velocidades de hasta 54Mbps.
- 802.11b (1999): Utiliza la banda de 2.5GHz, con velocidades de hasta 11Mbps.
- 802.11g (2003): Tambien en 2.4GHz, con velocidades de hasta 54Mbps.
- 802.11n (2009): Opera con las bandas de 2.4Ghz y 5GHz, con velocidades de hasta 600Mbps. Introdujo la tecnología MIMO (Multiple Input Multiple Output), que permite múltiples flujos de datos simultáneos.
- 802.11ac (2014): Banda de 5GHz, con velocidades de hasta 1.3Gbps, utilizando MIMO mejorado.
- 802.11ax (Wi-Fi 6) (2019): Mejora la eficiencia en entornos con muchos dispositivos conectados, velocidades hasta 10Gbps, y funciona tanto en 2.4GHz como en 5GHz.
- 802.11be (Wi-Fi 7): Estándar en desarrollo, se espera que alcance velocidades superiores a 30Gbps.

Bluetooth

Bluetooth es una tecnología diseñada para comunicaciones inalámbricas de corto alcance. Se utiliza principalmente para la conexión entre dispositivos personales como auriculares, teclados, ratones y teléfonos.

Estándares bluetooth:

- Bluetooth 1.0 y 1.1: Las primeras versiones, con una velocidad máxima de 721kbps.
- Bluetooth 2.0 + EDR: Introdujo la “Enhaced Data Rate”, con velocidades de hasta 3Mbps.
- Bluetooth 3.0 + HS: Agrego un modo de alta velocidad, usando Wi-Fi para transferencias rápidas (hasta 24 Mbps).
- Bluetooth 4.0: Introdujo Bluetooth Low Energy (BLE), diseñado para dispositivos de bajo consumo como wearables y sensores.
- Bluetooth 5.0: Mejoro el alcance y la velocidad (hasta 2Mbps) y permite conexiones más robustas.
- Bluetooth 5.1 y 5.2: Introducen mejoras en la localización de dispositivos y optimizaciones en la transmisión de audio y eficiencia energética.

NFC (Near Field Communication)

Es una tecnología de comunicación de corto alcance, generalmente de unos pocos centímetros. Se utiliza en pagos móviles, intercambio de información entre dispositivos y tarjetas inteligentes.

Estándares NFC:

- **ISO/IEC 18092**: Define la comunicación entre dispositivos NFC.
- **ISO/IEC 14443**: Define los estándares para las tarjetas inteligentes sin contacto que se usan con NFC.
- **NFC-A, NFC-B y NFC-F**: Diferentes modos de operación, que ofrecen compatibilidad con varias tecnologías de tarjetas y dispositivos.

LTE/5G (Long Term Evolution / 5G)

LTE y 5G son estándares para comunicaciones móviles, diseñados para ofrecer conectividad de banda ancha móvil.

Estándares LTE y 5G:

- **LTE (4G)**: Proporciona velocidades de descarga de hasta 1 Gbps en condiciones ideales. Utiliza diversas bandas de frecuencia, y soporta MIMO y técnicas de agregación de portadoras.

- **5G**: Es el estándar más reciente para redes móviles, con velocidades teóricas de hasta 20 Gbps y baja latencia. Utiliza frecuencias en el espectro de sub-6 GHz y mmWave (ondas milimétricas), ofreciendo un mayor ancho de banda.

Cada una de estas tecnologías tiene aplicaciones específicas y se adaptan a diferentes necesidades de comunicación. Wi-Fi es predominante en redes locales, Bluetooth en dispositivos personales, NFC para pagos y comunicaciones de corto alcance, y tecnologías como LTE/5G para comunicaciones de larga distancia en redes móviles. Los estándares juegan un rol importante en asegurar que los dispositivos puedan interactuar de manera eficiente y segura.

13 ¿Qué es un proxy?

Un servidor proxy es una tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet). Generalmente se trata de un dispositivo u ordenador intermedio que nos permite conectarnos a Internet de manera indirecta.

Cuando utilizamos un servidor proxy, toda la información pasa primero por él, este es el encargado de enviarlo al lugar de destino, impidiendo toda comunicación directa entre nuestro ordenador destino e Internet (u otro ordenador).

14 Explicar el protocolo Spanning tree.

Es un protocolo de red de capa 2 del **modelo OSI (capa de enlace de datos).** Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles. STP es transparente a las estaciones de usuario.

15 Explicar el protocolo de comunicaciones OSPF

OSPF (Open Shortest Path First) es un protocolo de enrutamiento dinámico que se utiliza en redes IP. Es un protocolo de enrutamiento de **estado de enlace (link-state)** y es parte de los protocolos de enrutamiento interior (Interior Gateway Protocol - IGP). Fue diseñado para trabajar dentro de un sistema autónomo (AS, Autonomous System) y es uno de los protocolos más comunes en redes empresariales y de operadores.

16 Explicar el protocolo ARP.

ARP (Address Resolution Protocol) es un protocolo de red utilizado para mapear direcciones IP (de la capa de red) a direcciones físicas o MAC (de la capa de enlace de datos) dentro de una red local (LAN). Este mapeo es necesario porque mientras que las direcciones IP se usan para

identificar dispositivos en una red a nivel lógico, las direcciones MAC son las que permiten la comunicación a nivel físico dentro de una red local.

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 basado en reglas de seguridad predeterminadas. Su principal función es actuar como una barrera entre una red confiable (por ejemplo, una red local) y una red no confiable (como Internet), bloqueando el acceso no autorizado y permitiendo el tráfico autorizado.

18 ¿Qué es un DMZ?

Una **DMZ (Demilitarized Zone)**, o zona desmilitarizada en el contexto de redes, es una subred física o lógica que se encuentra entre una red interna segura (como la red local de una empresa) y una red externa no confiable (como Internet). Su propósito es agregar una capa adicional de seguridad entre la red interna y externa, proporcionando un área controlada donde se colocan servidores que necesitan interactuar tanto con usuarios externos como con los sistemas internos.

19 ¿Qué es un Gateway?

Un **gateway** (puerta de enlace) es un dispositivo de red que actúa como un punto de acceso o interfaz entre dos redes diferentes, permitiendo que se comuniquen y transfieran datos. Es responsable de traducir, convertir o enrutarse entre protocolos y arquitecturas de red diferentes. Los gateways son esenciales en la comunicación entre redes que utilizan protocolos diferentes, ya que permiten que los datos fluyan entre ellas sin problemas.

20 Según Microsoft, ¿Qué significa NBL?

En el contexto de Microsoft, "NBL" suele significar "Non-Business Line." Se refiere a aplicaciones, servicios o actividades que no están directamente relacionadas con los procesos comerciales o de negocio principales de una empresa. Este término puede usarse para diferenciar entre las operaciones comerciales principales y las actividades que están fuera de ese ámbito, como proyectos experimentales o servicios no centrales.

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- Conectividad de varios de call centers con un data center central.
   2- Conectar los datos de los pozos petroleros durante 15 minutos por día.
   3- Comunicar dos edificios enfrentados en la misma calle.

Tipos de enlace:

1. **MPLS (Multiprotocol Label Switching)**:

   - **Descripción**: MPLS es una técnica de conmutación de datos que utiliza etiquetas para dirigir los paquetes a través de una red de manera eficiente. Las etiquetas se agregan a los paquetes para determinar su ruta a través de la red, lo que permite la creación de caminos predefinidos para el tráfico.
   - **Ventajas**: Mejora el rendimiento, la escalabilidad y el control del tráfico en redes grandes. Es ideal para redes empresariales y de telecomunicaciones que necesitan soporte para VPNs y QoS (Quality of Service).

2. **LAN to LAN**:

   - **Descripción**: Se refiere a la conexión directa entre dos redes locales (LANs) mediante enlaces físicos o virtuales. Esto puede lograrse a través de conexiones por cable, como fibra óptica o Ethernet, o mediante VPNs.
   - **Ventajas**: Proporciona alta velocidad y baja latencia debido a la conexión directa. Ideal para interconectar redes dentro de una misma área geográfica.

3. **Microonda**:

   - **Descripción**: La tecnología de microondas utiliza ondas electromagnéticas para transmitir datos a través del aire. Los enlaces de microondas requieren una línea de vista directa entre las antenas emisora y receptora.
   - **Ventajas**: Buena opción para conectar sitios que están a distancias moderadas y donde no se puede instalar cableado. Es más rápida de desplegar en áreas remotas.

4. **VSAT (Very Small Aperture Terminal)**:

   - **Descripción**: VSAT es una tecnología de comunicación por satélite que utiliza pequeñas antenas parabólicas para enviar y recibir datos a través de satélites en órbita. Es útil para áreas geográficas extensas.
   - **Ventajas**: Permite la conectividad en áreas remotas y rurales donde las otras opciones no están disponibles. Es independiente de la infraestructura terrestre.

Dos tipos de enlaces adicionales

1. **Fibra óptica**:

    - **Descripción**: Utiliza cables de fibra óptica para transmitir datos como pulsos de luz a alta velocidad. Es ideal para largas distancias y grandes volúmenes de datos.
    - **Ventajas**: Alta capacidad de transmisión, baja atenuación y baja latencia. Ideal para conexiones de alta velocidad a larga distancia.

2. **Ethernet**:

    - **Descripción**: Es una tecnología de red local que utiliza cables de cobre o fibra óptica para la transmisión de datos en redes LAN. Existen diferentes velocidades como 10/100/1000 Mbps y 10 Gbps.
    - **Ventajas**: Fácil de implementar, económico para redes locales y tiene alta velocidad y bajo costo en distancias cortas.

Ranking de enlaces

	Económico	**Performance**	**+ Capacidad**
1	Ethernet	Fibra Óptica	Fibra Óptica
2	LAN to LAN	Ethernet	Ethernet
3	VSAT	MPLS	MPLS
4	Microonda	Microonda	Microonda
5	MPLS	LAN to LAN	LAN to LAN
6	Fibra Óptica	VSAT	VSAT

	Soporte a Distancia	**Menor esfuerzo de configuración**	**Soporte a Distancia**	**+Restricciones**
1	Fibra Óptica	Ethernet	Fibra Óptica	MPLS
2	VSAT	LAN to LAN	VSAT	Fibra Óptica
3	Microonda	VSAT	Microonda	Ethernet

4	MPLS	MPLS	MPLS	Microonda
5	Ethernet	Microonda	Ethernet	LAN to LAN
6	LAN to LAN	Fibra Óptica	LAN to LAN	VSAT

Elección de tipo de enlace para escenarios

1. **Conectividad de varios call centers con un data center central**:
   - **Elección**: **MPLS**
   - **Razón**: MPLS proporciona una red privada virtual segura y escalable, ideal para conectar múltiples sitios y garantizar la calidad del servicio para aplicaciones críticas.
2. **Conectar los datos de los pozos petroleros durante 15 minutos por día**:
   - **Elección**: **VSAT**
   - **Razón**: VSAT permite la conectividad en áreas remotas y puede ser una solución adecuada para transmitir datos en intervalos específicos desde ubicaciones geográficas extensas.
3. **Comunicar dos edificios enfrentados en la misma calle**:
   - **Elección**: **Microonda**
   - **Razón**: La tecnología de microondas puede proporcionar una conexión rápida y eficiente entre dos edificios cercanos sin necesidad de instalar cables subterráneos o aéreos.

22 Describir la tecnología LTE

LTE (Long-Term Evolution) es una tecnología de comunicación móvil de cuarta generación (4G) que mejora significativamente la velocidad y la eficiencia en comparación con sus predecesores, como 3G.

Características Clave de LTE:

1. **Velocidades de datos**:
   - **Descarga**: LTE ofrece velocidades teóricas de descarga que pueden alcanzar hasta 300 Mbps en redes LTE-Advanced. En implementaciones típicas, las velocidades de descarga son generalmente entre 10 y 100 Mbps.
   - **Subida**: Las velocidades teóricas de subida pueden llegar a 75 Mbps, con velocidades típicas en el rango de 5 a 50 Mbps.
2. **Arquitectura de red**:
   - **Evolución de la red**: LTE es parte de la evolución de la red celular y se basa en una arquitectura IP (Internet Protocol), lo que facilita la integración con servicios de datos y multimedia.
   - **EPC (Evolved Packet Core)**: LTE utiliza el EPC para gestionar el tráfico de datos y proporcionar una transición fluida entre diferentes tipos de red.

3. **Ancho de banda y espectro**:
    - **Ancho de banda**: LTE soporta una amplia gama de anchos de banda, desde 1.4 MHz hasta 20 MHz en un solo canal, permitiendo a los operadores ajustar la red según la disponibilidad del espectro y las necesidades de la demanda.
    - **Frecuencias**: LTE puede operar en diferentes bandas de frecuencia, lo que permite a los operadores elegir las bandas más adecuadas para sus redes.
4. **Modulación y tecnología**:
    - **Modulación**: LTE utiliza modulación OFDM (Orthogonal Frequency-Division Multiplexing) para las transmisiones en el enlace descendente (downlink) y SC-FDMA (Single Carrier Frequency Division Multiple Access) para el enlace ascendente (uplink), lo que mejora la eficiencia del espectro y reduce la interferencia.
    - **MIMO (Multiple Input Multiple Output)**: LTE utiliza técnicas de MIMO para mejorar la capacidad y la cobertura de la red, permitiendo que múltiples antenas transmitan y reciban señales simultáneamente.
5. **Latencia**:
    - **Baja latencia**: LTE ofrece una latencia significativamente menor en comparación con las tecnologías anteriores, típicamente en el rango de 30 a 50 ms, lo que mejora la experiencia del usuario en aplicaciones que requieren respuesta rápida.
6. **Calidad de servicio (QoS)**:
    - **Gestión de tráfico**: LTE proporciona mecanismos para garantizar la calidad del servicio, permitiendo a los operadores priorizar el tráfico y gestionar el ancho de banda de manera eficiente para aplicaciones como video en alta definición, juegos en línea y servicios en tiempo real.
7. **Interoperabilidad y compatibilidad**:
    - **Compatibilidad**: LTE está diseñado para ser compatible con las redes 3G y 2G existentes, facilitando la transición y la coexistencia con tecnologías anteriores.
    - **Roaming**: Los dispositivos LTE pueden hacer roaming en redes 3G y 2G, asegurando la conectividad incluso cuando no hay cobertura LTE disponible.
8. **Seguridad**:
    - **Encriptación**: LTE proporciona mecanismos de seguridad robustos, incluyendo encriptación de datos y autenticación, para proteger la integridad y la confidencialidad de las comunicaciones.

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

Microsoft Teams es una solución de colaboración y comunicación desarrollada por Microsoft que está diseñada para mejorar la productividad y la eficiencia en el lugar de trabajo. Forma parte del conjunto de herramientas de Microsoft 365 (anteriormente Office 365) y está integrada con otras aplicaciones y servicios de Microsoft.

Beneficios de Microsoft Teams

- **Centralización de la Comunicación**: Agrupa todos los aspectos de la comunicación y colaboración en una sola plataforma, eliminando la necesidad de múltiples herramientas.
- **Mejora de la Productividad**: Facilita la colaboración en tiempo real y la gestión eficiente de proyectos y tareas.
- **Flexibilidad y Accesibilidad**: Disponible en diversas plataformas, incluyendo aplicaciones de escritorio, móviles y web, permitiendo a los usuarios trabajar desde cualquier lugar.
- **Integración con Microsoft 365**: Ofrece una integración fluida con otras herramientas de Microsoft, mejorando la eficiencia y la cohesión en el entorno de trabajo.

Alternativa de otra empresa: Slack

- **Slack** es una solución de colaboración y comunicación que también ofrece características similares a las de Microsoft Teams. Se centra en la comunicación en canales, la integración con una amplia gama de aplicaciones y servicios de terceros, y la facilidad de uso. Al igual que Teams, Slack soporta mensajes directos, conversaciones en grupo, llamadas y videoconferencias, y la integración con herramientas de productividad.

24 ¿QUÉ SIGNIFICA APLICAR CALIDAD EN UN ENLACE MPLS?

Aplicar calidad en un enlace MPLS (Multiprotocol Label Switching) se refiere a implementar técnicas y mecanismos para garantizar un rendimiento óptimo y predecible del tráfico de datos a través de la red MPLS. Esto abarca varias prácticas y tecnologías para asegurar que el enlace cumpla con los requisitos de calidad del servicio (QoS) y que los datos se transmitan de manera eficiente y confiable.

1. Calidad de servicio (QoS)

- **Priorización del tráfico**: En un enlace MPLS, la QoS se aplica para clasificar y priorizar diferentes tipos de tráfico. Esto garantiza que las aplicaciones críticas, como VoIP (voz sobre IP) o video en tiempo real, reciban un tratamiento preferencial en términos de ancho de banda y baja latencia.
- **Etiquetas MPLS y QoS**: MPLS utiliza etiquetas para dirigir el tráfico a través de la red. Los mecanismos de QoS en MPLS permiten asignar diferentes niveles de prioridad a los paquetes según su etiqueta, asegurando que el tráfico sensible al tiempo tenga prioridad sobre el tráfico menos crítico.

2. Control de Congestión

- **Gestión de recursos**: Para evitar la congestión y mantener un rendimiento estable, se implementan políticas de gestión de recursos en los enlaces MPLS. Esto incluye la

asignación adecuada de ancho de banda y el control del tráfico para evitar la saturación de los enlaces.
- **Colas y planificación**: Los enlaces MPLS pueden utilizar mecanismos de planificación y gestión de colas para manejar el tráfico de manera eficiente. Esto ayuda a minimizar la pérdida de paquetes y a reducir la latencia.

3. Reserva de ancho de banda

- **Reserva de recursos**: MPLS permite la reserva de ancho de banda para flujos de tráfico específicos utilizando técnicas como RSVP (Resource Reservation Protocol). Esto asegura que se asignen los recursos necesarios para mantener la calidad del servicio para aplicaciones críticas.
- **LSP (Label Switched Paths)**: Los LSP en MPLS pueden ser configurados para reservar ancho de banda específico, garantizando que el tráfico que sigue un LSP determinado tenga suficiente capacidad disponible.

4. Monitoreo y mantenimiento

- **Monitoreo del rendimiento**: La calidad de un enlace MPLS también implica monitorear el rendimiento de la red para identificar problemas como pérdida de paquetes, latencia y jitter (variabilidad en el tiempo de llegada de los paquetes). Las herramientas de monitoreo y análisis pueden ayudar a detectar y resolver problemas de calidad.
- **Mantenimiento proactivo**: Realizar mantenimiento regular y ajustes en la configuración del enlace MPLS para adaptarse a los cambios en el tráfico y en las necesidades de los usuarios es esencial para mantener una alta calidad de servicio.

5. Seguridad y Fiabilidad

- **Protección contra fallos**: Implementar mecanismos de redundancia y recuperación ante desastres para asegurar la fiabilidad del enlace MPLS. Esto incluye el uso de rutas alternativas y mecanismos de conmutación por error para minimizar el impacto de fallos en la red.
- **Seguridad de datos**: Asegurar que el tráfico en la red MPLS esté protegido contra accesos no autorizados y amenazas de seguridad. Esto puede incluir el cifrado del tráfico y el control de acceso a la red.

6. Configuración y políticas de enlace

- **Configuración adecuada**: Asegurarse de que el enlace MPLS esté configurado correctamente según los requisitos de QoS y las políticas de tráfico de la red. Esto incluye la correcta asignación de etiquetas, la configuración de LSP y la aplicación de políticas de QoS.
- **Políticas de tráfico**: Definir y aplicar políticas de tráfico para gestionar cómo se maneja el tráfico en el enlace MPLS, garantizando que se cumplan los acuerdos de nivel de servicio (SLA) y los requisitos de rendimiento.

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

Las conexiones Coaxial, UTP (Unshielded Twisted Pair) y Fibra Óptica son tres tipos de cables utilizados para la transmisión de datos, cada uno con características y aplicaciones específicas.

1. Cable coaxial

Descripción:

- **Estructura**: Un cable coaxial consiste en un conductor central de cobre o aluminio, rodeado por un aislamiento dieléctrico, una capa de malla de cobre (blindaje) y una cubierta exterior. El blindaje protege contra interferencias electromagnéticas (EMI).

Características:

- **Velocidad y ancho de banda**: Ofrece buenas velocidades de transmisión y anchos de banda adecuados para aplicaciones de televisión por cable y conexiones de Internet de banda ancha.
- **Distancia**: Adecuado para distancias moderadas. A medida que aumenta la distancia, la calidad de la señal puede degradarse, a menos que se utilicen amplificadores.
- **Interferencia**: Menos susceptible a interferencias externas debido al blindaje. Sin embargo, puede haber pérdida de señal si el cable está dañado o mal instalado.
- **Aplicaciones**: Comúnmente utilizado para la televisión por cable, conexiones de banda ancha en hogares y redes de televisión.

2. Cable UTP (Unshielded Twisted Pair)

Descripción:

- **Estructura**: El cable UTP está compuesto por pares de cables de cobre trenzados, sin blindaje adicional. Los pares están trenzados para reducir la interferencia electromagnética y mejorar la calidad de la señal.

Características:

- **Velocidad y ancho de banda**: Varía según la categoría del cable (Cat5e, Cat6, Cat6a, Cat7, Cat8). Los cables más avanzados pueden ofrecer velocidades de hasta 10 Gbps y mayores anchos de banda.
- **Distancia**: Adecuado para distancias cortas a medianas. Los cables UTP de categoría superior pueden soportar distancias de hasta 100 metros para redes Ethernet de alta velocidad.
- **Interferencia**: Menos protección contra interferencias externas en comparación con los cables blindados. La calidad de la señal puede verse afectada por interferencias y ruido.

- **Aplicaciones**: Utilizado principalmente en redes Ethernet para redes locales (LAN), conexiones de computadoras y sistemas telefónicos.

3. Cable de Fibra Óptica

Descripción:

- **Estructura**: Consiste en un núcleo de vidrio o plástico por el que viaja la luz, rodeado por una capa de revestimiento que refleja la luz dentro del núcleo, una capa de refuerzo y una cubierta exterior.

Características:

- **Velocidad y ancho de banda**: Ofrece las mayores velocidades de transmisión y anchos de banda, soportando velocidades que van desde 1 Gbps hasta varios Tbps. Ideal para aplicaciones que requieren alta capacidad y velocidad.
- **Distancia**: Soporta distancias mucho mayores en comparación con los cables coaxiales y UTP. La fibra óptica puede transmitir datos a distancias de varios kilómetros sin pérdida significativa de calidad.
- **Interferencia**: Totalmente inmune a interferencias electromagnéticas y radiofrecuencias, ya que transmite datos en forma de luz.
- **Aplicaciones**: Utilizado en redes de telecomunicaciones, conexiones de datos de alta velocidad, redes de área extensa (WAN), y conexiones entre centros de datos y proveedores de servicios de Internet.

Comparación y aplicaciones

1. Velocidad y ancho de banda:

- **Fibra óptica**: Mejor rendimiento en términos de velocidad y ancho de banda.
- **Coaxial**: Menor ancho de banda y velocidad en comparación con la fibra óptica.
- **UTP**: Velocidad y ancho de banda dependen de la categoría del cable. Los cables de categoría más alta ofrecen mejor rendimiento.

2. Distancia:

- **Fibra óptica**: Soporta distancias mucho mayores sin degradación significativa de la señal.
- **Coaxial**: Adecuado para distancias moderadas; la señal puede degradarse en distancias largas.
- **UTP**: Mejor para distancias cortas a medianas; la calidad de la señal disminuye con la distancia.

3. Interferencia:

- **Fibra óptica**: Inmune a interferencias electromagnéticas y radiofrecuencias.

- **Coaxial**: Menos susceptible a interferencias debido al blindaje, pero puede haber pérdida de señal si el cable está dañado.
- **UTP**: Más susceptible a interferencias y ruido, especialmente en cables sin blindaje.

4. Aplicaciones:

- **Fibra óptica**: Ideal para redes de alta velocidad y largas distancias, conexiones entre centros de datos, y telecomunicaciones.
- **Coaxial**: Usado para televisión por cable y conexiones de banda ancha en el hogar.
- **UTP**: Común en redes LAN, conexiones Ethernet y sistemas telefónicos.

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).

Certificaciones Cisco

1. **CCENT (Cisco Certified Entry Networking Technician)**:
   - **Descripción**: La certificación CCENT es la certificación inicial de Cisco para aquellos que buscan comenzar una carrera en redes. Proporciona una base sólida en los conceptos básicos de redes y la configuración de dispositivos de red.
   - **Contenido**: Incluye fundamentos de redes, configuración y verificación de dispositivos de red básicos, y resolución de problemas de conectividad.
2. **CCNA (Cisco Certified Network Associate)**:
   - **Descripción**: La certificación CCNA es una certificación más avanzada que cubre una gama más amplia de conceptos de redes y tecnologías. Es un requisito común para profesionales de redes y técnicos que buscan roles en administración de redes.
   - **Contenido**: Abarca temas como la configuración y operación de redes pequeñas a medianas, IPv4 e IPv6, conmutación y enrutamiento, y conceptos básicos de seguridad y redes inalámbricas.
3. **CCNP (Cisco Certified Network Professional)**:
   - **Descripción**: La certificación CCNP es un nivel avanzado que requiere un conocimiento profundo de redes y habilidades de configuración. Está diseñada para profesionales de redes que desean demostrar su capacidad para implementar, verificar y solucionar problemas en redes empresariales complejas.
   - **Contenido**: Incluye temas avanzados en enrutamiento y conmutación, tales como la implementación de soluciones de red más grandes y complejas, la optimización del rendimiento y la resolución de problemas en redes empresariales.

Tracks de certificación cisco

Track Routing & Switching

- **Descripción**: Este track de certificación se enfoca en las habilidades necesarias para diseñar, configurar y mantener redes de conmutación y enrutamiento. Es uno de los tracks más fundamentales y abarca desde conceptos básicos hasta avanzados.
- **Certificaciones Incluidas**:
    - **CCNA Routing & Switching**: Proporciona conocimientos básicos de redes, configuración de dispositivos de red y resolución de problemas.
    - **CCNP Routing & Switching**: Ofrece un conocimiento más profundo en la implementación, operación y solución de problemas de redes grandes y complejas.
- **Temas Clave**:
    - **Enrutamiento**: Protocolos de enrutamiento, como OSPF, EIGRP y BGP.
    - **Conmutación**: VLANs, STP, y la configuración de switches.
    - **Redes WAN**: Tecnologías y protocolos de redes de área amplia.
    - **Resolución de Problemas**: Herramientas y técnicas para identificar y solucionar problemas de red.

Track Wireless

- **Descripción**: El track Wireless se centra en la planificación, diseño, implementación y solución de problemas en redes inalámbricas. Es crucial para las organizaciones que implementan redes Wi-Fi y otras tecnologías inalámbricas.
- **Certificaciones incluidas**:
    - **CCNA Wireless**: Introducción a la configuración y administración de redes inalámbricas.
    - **CCNP Wireless**: Habilidades avanzadas para implementar y solucionar problemas en redes inalámbricas empresariales.
- **Temas Clave**:
    - **Diseño de redes inalámbricas**: Planificación de la cobertura, análisis de sitios y diseño de redes.
    - **Configuración de equipos**: Implementación de puntos de acceso y controladores de red inalámbrica.
    - **Seguridad inalámbrica**: Protocolo de seguridad, autenticación y cifrado de datos.

Track Security

- **Descripción**: Este track está orientado a la implementación y administración de soluciones de seguridad en redes empresariales. Cubre desde la protección básica hasta las soluciones avanzadas de seguridad.
- **Certificaciones incluidas**:
    - **CCNA Security**: Introducción a los conceptos de seguridad en redes, incluyendo la protección de redes contra amenazas comunes.
    - **CCNP Security**: Enfoque en la implementación de políticas de seguridad avanzadas y la gestión de dispositivos de seguridad.

- **Temas clave**:
  - **Seguridad de redes**: Firewalls, VPNs y tecnologías de protección de redes.
  - **Amenazas y vulnerabilidades**: Identificación y mitigación de amenazas.
  - **Cumplimiento y políticas**: Implementación de políticas de seguridad y cumplimiento normativo.

Track Cloud

- **Descripción**: Este track se enfoca en el diseño, implementación y gestión de soluciones de nube, tanto públicas como privadas. Es esencial para organizaciones que adoptan o gestionan servicios en la nube.
- **Certificaciones incluidas**:
  - **CCNA Cloud**: Fundamentos de los conceptos y tecnologías en la nube.
  - **CCNP Cloud**: Habilidades avanzadas para la implementación y administración de soluciones en la nube.
- **Temas clave**:
  - **Servicios en la nube**: Infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS).
  - **Gestión de nube**: Implementación de soluciones en la nube, administración de recursos y monitoreo de servicios.
  - **Seguridad en la nube**: Implementación de medidas de seguridad y gestión de riesgos en entornos de nube.

27 EXPLIQUE EL MODELO OSI

El modelo OSI (Open Systems Interconnection) es un marco conceptual que estandariza las funciones de comunicación de un sistema de red en siete capas distintas. Fue desarrollado por la Organización Internacional de Normalización (ISO) para promover la interoperabilidad entre diferentes sistemas de red y asegurar una comunicación efectiva entre ellos.

1. Capa Física (Physical Layer)

- **Descripción**: La capa física se encarga de la transmisión y recepción de datos sin procesar a través de un medio físico, como cables, fibra óptica o radiofrecuencia.
- **Funciones**:
  - Definir las características eléctricas y mecánicas de los dispositivos de transmisión.
  - Determinar cómo se codifican y decodifican los datos en señales físicas.
  - Establecer la velocidad de transmisión y los tipos de conectores utilizados.

2. Capa de Enlace de Datos (Data Link Layer)

- **Descripción**: La capa de enlace de datos proporciona una comunicación libre de errores entre dos dispositivos conectados directamente. Asegura que los datos sean enviados sin errores y en el orden correcto.
- **Funciones**:

- Controlar el acceso al medio de transmisión (por ejemplo, mediante protocolos de acceso al medio como CSMA/CD).
- Detectar y corregir errores en la capa física.
- Segmentar los datos en tramas y añadir direcciones físicas (MAC) para el direccionamiento de dispositivos en la red local.

3. Capa de red (Network Layer)

- **Descripción**: La capa de red es responsable del enrutamiento de datos entre diferentes redes y la determinación de la mejor ruta para el envío de paquetes.
- **Funciones**:
  - Encaminamiento (routing) de paquetes a través de múltiples redes.
  - Asignación y gestión de direcciones lógicas (como direcciones IP).
  - Fragmentación y reensamblaje de paquetes para ajustarse a los tamaños de trama de las redes físicas.

4. Capa de transporte (Transport Layer)

- **Descripción**: La capa de transporte asegura la entrega fiable y ordenada de datos entre sistemas finales. Proporciona control de flujo y corrección de errores para garantizar la integridad de la comunicación.
- **Funciones**:
  - Establecer, mantener y finalizar conexiones entre aplicaciones.
  - Proporcionar control de flujo para evitar la sobrecarga del receptor.
  - Garantizar la entrega correcta de datos mediante el uso de protocolos como TCP (Transmission Control Protocol) para comunicación orientada a conexión y UDP (User Datagram Protocol) para comunicación no orientada a conexión.

5. Capa de sesión (Session Layer)

- **Descripción**: La capa de sesión gestiona la apertura, el mantenimiento y el cierre de sesiones entre aplicaciones. Se encarga de establecer, mantener y terminar las conexiones entre aplicaciones de red.
- **Funciones**:
  - Coordinar y controlar el diálogo entre aplicaciones (por ejemplo, mediante el uso de protocolos de sesión).
  - Sincronización y recuperación de sesiones en caso de fallos.
  - Manejo de la comunicación en diferentes direcciones (de una aplicación a otra).

6. Capa de presentación (Presentation Layer)

- **Descripción**: La capa de presentación se encarga de la representación y la codificación de datos para que puedan ser entendidos por la capa de aplicación. Actúa como un traductor entre el formato de los datos y el formato de presentación.
- **Funciones**:

- Traducción de datos entre diferentes formatos y codificaciones (por ejemplo, ASCII a EBCDIC).
- Cifrado y descifrado de datos para asegurar la privacidad (como en el caso de HTTPS).
- Compresión y descompresión de datos para mejorar la eficiencia en la transmisión.

7. Capa de aplicación (Application Layer)

- **Descripción**: La capa de aplicación es la capa más cercana al usuario final y proporciona servicios de red a las aplicaciones. Es donde se ejecutan los programas que utilizan la red.
- **Funciones**:
  - Proporcionar servicios de red a las aplicaciones del usuario final (por ejemplo, correo electrónico, navegación web).
  - Definir protocolos de comunicación para aplicaciones específicas (como HTTP, FTP, SMTP).
  - Interactuar con los usuarios y proporcionar la interfaz para las aplicaciones.

El modelo OSI proporciona un marco estructural para entender y diseñar redes, permitiendo la interoperabilidad entre sistemas de diferentes fabricantes. Cada capa del modelo OSI tiene responsabilidades específicas y se basa en la capa inferior para ofrecer servicios a la capa superior. Esto facilita la comprensión y el diagnóstico de problemas de red, y proporciona una base para el desarrollo de protocolos y tecnologías de red.

28 REALIZAR CUESTIONARIO ONLINE Y COPIAR EL RESULTADO: (1 POR CADA INTEGRANTE)

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

Walter Mirengo, Martin Kaen, Gabriela Amado

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

El estándar IEEE 802.3 es una parte fundamental de la familia de estándares IEEE 802 que regula las redes Ethernet.

Estándar IEEE 802.3

Descripción:

- El estándar IEEE 802.3 define las especificaciones para las redes Ethernet en términos de la capa de enlace de datos (capa 2 del modelo OSI) y la capa física. Ethernet es una tecnología de red de área local (LAN) que utiliza tramas para transmitir datos a través de una red.
- El estándar 802.3 abarca varios tipos de Ethernet, incluyendo Ethernet de 10 Mbps (10Base-T), 100 Mbps (100Base-TX), 1 Gbps (1000Base-T), y 10 Gbps (10GBase-T), entre otros.

Regulación de la red

1. **Capa de enlace de datos**:

- **Dirección MAC**: Define el formato de las direcciones físicas (MAC) y cómo se utilizan para identificar y direccionar los dispositivos en la red.
- **Formato de trama**: Especifica la estructura de las tramas Ethernet, que incluye el encabezado, el campo de datos y el campo de verificación de errores (FCS).

2. **Capa física**:

- **Medios de transmisión**: Define los tipos de cables y medios de transmisión utilizados, como cables de par trenzado (UTP), fibra óptica y cables coaxiales.
- **Codificación de datos**: Establece las técnicas de codificación y modulación utilizadas para transmitir datos a través de los medios físicos.

3. **Acceso al medio**:

- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**: En las versiones antiguas de Ethernet (como 10Base-T y 100Base-TX), se utiliza CSMA/CD para gestionar el acceso al medio compartido y evitar colisiones de datos. Aunque este método no es necesario en las versiones modernas de Ethernet que usan switches, sigue siendo parte del estándar.

Implementación

1. **Equipos de red**:

- **Switches y Hubs**: Los switches Ethernet dirigen las tramas a los dispositivos de destino en función de sus direcciones MAC. Los hubs, aunque menos eficientes, también se usan para conectar dispositivos en una red Ethernet.
- **Tarjetas de red**: Las tarjetas de red (NIC) en los dispositivos finales (como computadoras y servidores) se encargan de enviar y recibir tramas Ethernet.

2. **Cabling**:

- **Cables ethernet**: Los cables de par trenzado (como Cat5e, Cat6, Cat6a) y cables de fibra óptica se utilizan para conectar dispositivos y transmitir datos según las especificaciones del estándar IEEE 802.3.

3. **Configuración de red**:

- **VLANs y redes**: Los switches Ethernet pueden configurar VLANs (Virtual LANs) para segmentar el tráfico y mejorar el rendimiento y la seguridad de la red.

Ventajas

1. **Amplia compatibilidad**:
   - Ethernet, basado en el estándar IEEE 802.3, es ampliamente compatible con una variedad de equipos y tecnologías, lo que facilita la interoperabilidad.
2. **Escalabilidad**:
   - Permite la escalabilidad a diferentes velocidades y capacidades (de 10 Mbps a 10 Gbps y más), adaptándose a las necesidades cambiantes de la red.
3. **Costo-Efectividad**:
   - La infraestructura de Ethernet es generalmente más económica en comparación con otras tecnologías de red, como las redes de fibra óptica de alto nivel.
4. **Simplicidad y facilidad de implementación**:
   - La tecnología Ethernet es relativamente fácil de implementar y configurar, con estándares bien definidos y equipos disponibles a bajo costo.

Desventajas

1. **Colisiones en redes Hubs**:

- En redes basadas en hubs (en las que todos los dispositivos comparten el mismo medio), las colisiones de datos pueden ocurrir, lo que puede afectar el rendimiento. Esto se minimiza con el uso de switches modernos.

2. **Limitaciones de distancia**:
   - Las versiones de Ethernet sobre cables de par trenzado tienen limitaciones de distancia (por ejemplo, 100 metros para 100Base-TX y 1000Base-T), lo que puede requerir el uso de repetidores o switches adicionales para redes extensas.
3. **Interferencia electromagnética**:
   - Los cables de par, trenzado y coaxiales pueden ser susceptibles a interferencias electromagnéticas, aunque las versiones más recientes de Ethernet utilizan técnicas de blindaje para minimizar estos problemas.
4. **Velocidades superiores**:
   - Para velocidades superiores a 1 Gbps, Ethernet puede requerir el uso de cables de fibra óptica o de cobre de categorías avanzadas (como Cat6a o Cat7), lo que puede incrementar los costos.

30 Explicar el estándar IEEE 802.4 regula la red

El estándar IEEE 802.4, aunque no es tan comúnmente discutido como otros estándares de la serie IEEE 802, proporciona especificaciones para un tipo de red en particular.

Estándar IEEE 802.4

Descripción general:

- **IEEE 802.4** es un estándar para redes de área local (LAN) que define el uso de **Token Bus**. Se diseñó para proporcionar un método de acceso al medio de red basado en el paso de un token o permiso de acceso entre dispositivos de red.

Características del Token Bus:

1. **Topología de red**:
   - **Topología de Bus**: En el estándar IEEE 802.4, los dispositivos están conectados en una topología de bus utilizando un cable coaxial. Los dispositivos están conectados a lo largo de un único cable coaxial que actúa como el medio de transmisión compartido.
2. **Método de acceso**:
   - **Token Bus**: Utiliza un mecanismo de **Token Passing** para controlar el acceso al medio. En este método, un token (un paquete especial de datos) circula por la red, y solo el dispositivo que posee el token puede transmitir datos. Esto ayuda a evitar colisiones y garantiza que cada dispositivo tenga una oportunidad de acceder al medio.
3. **Operación**:
   - **Pasaje del token**: El token se mueve de un dispositivo a otro en un orden específico. Cuando un dispositivo desea enviar datos, debe esperar a que el

token llegue a él. Una vez que recibe el token, el dispositivo puede transmitir sus datos y luego pasa el token al siguiente dispositivo en la secuencia.

4. **Direccionamiento**:
    - **Dirección MAC**: Los dispositivos en una red Token Bus utilizan direcciones MAC para identificar y direccionar los datos enviados a través de la red.

Implementación

1. **Medios de transmisión**:
    - **Coaxial**: El estándar IEEE 802.4 utiliza cables coaxiales como medio de transmisión, aunque también se pueden emplear otros medios de transmisión.
2. **Equipos de red**:
    - **Adaptadores de red**: Los dispositivos de la red Token Bus están equipados con adaptadores de red que gestionan la comunicación basada en el paso del token.
3. **Configuración de red**:
    - **Configuración Física**: La red se configura con un cable coaxial que conecta todos los dispositivos en la topología de bus. Se requiere una terminación adecuada en ambos extremos del cable para evitar reflexiones de señales.

Ventajas

1. **Control de Acceso Eficiente**:
    - El método de token passing evita colisiones y permite un acceso justo al medio, ya que cada dispositivo tiene una oportunidad de transmitir.
2. **Determinismo**:
    - Ofrece un acceso determinista al medio, lo que es útil en aplicaciones que requieren una entrega predecible de datos.
3. **Simpleza en la Gestión de Colisiones**:
    - Debido a que solo un dispositivo puede transmitir a la vez, el estándar reduce la probabilidad de colisiones en comparación con métodos de acceso como CSMA/CD.

Desventajas

1. **Topología de Bus**:
    - La topología de bus puede ser menos flexible y más difícil de gestionar en comparación con topologías más modernas, como las de estrella utilizadas en Ethernet.
2. **Costo de Implementación**:
    - Puede ser costoso implementar una red Token Bus debido al hardware especializado necesario y los cables coaxiales.
3. **Escalabilidad Limitada**:
    - Las redes basadas en Token Bus tienen limitaciones en términos de escalabilidad y pueden no ser tan efectivas en redes grandes o de alto tráfico.
4. **Menor Adopción**:

- El estándar IEEE 802.4 ha sido menos adoptado en comparación con otros estándares de redes, como Ethernet (IEEE 802.3) y ha sido en gran parte reemplazado por tecnologías más modernas.

31 ¿QUÉ PROTOCOLOS SE USAN PARA ENVIAR Y RECIBIR CORREO?

Protocolos para Enviar Correo

1. **SMTP (Simple Mail Transfer Protocol)**
   - **Descripción**: SMTP es el protocolo estándar para enviar correos electrónicos desde un cliente de correo (como Outlook o Thunderbird) a un servidor de correo, o entre servidores de correo.
   - **Puerto**: Normalmente opera en el puerto **25**, aunque también puede usar el puerto **587** para conexiones seguras.
   - **Función**: Encargado de la transmisión de correos electrónicos y la comunicación entre servidores para entregar los mensajes a su destino final.

Protocolos para Recibir Correo

1. **POP3 (Post Office Protocol version 3)**
   - **Descripción**: POP3 es un protocolo utilizado para recuperar correos electrónicos desde un servidor de correo. Los correos descargados se almacenan localmente en el dispositivo del usuario y generalmente se eliminan del servidor.
   - **Puerto**: Opera en el puerto **110**, aunque también puede usar el puerto **995** para conexiones seguras (POP3S).
   - **Función**: Permite al usuario descargar correos electrónicos del servidor y gestionarlos localmente en su cliente de correo.
2. **IMAP (Internet Message Access Protocol)**
   - **Descripción**: IMAP es otro protocolo para recibir correos electrónicos. A diferencia de POP3, IMAP mantiene los correos electrónicos en el servidor, permitiendo a los usuarios acceder a sus mensajes desde múltiples dispositivos y sincronizar carpetas.
   - **Puerto**: Opera en el puerto **143**, aunque también puede usar el puerto **993** para conexiones seguras (IMAPS).
   - **Función**: Facilita la gestión de correos electrónicos en el servidor, incluyendo la sincronización y organización en carpetas, y permite a los usuarios acceder a sus correos desde diferentes ubicaciones y dispositivos.

Protocolos Adicionales

1. **MIME (Multipurpose Internet Mail Extensions)**
   - **Descripción**: MIME no es un protocolo en sí mismo, sino una extensión de los protocolos de correo que permite enviar mensajes con diferentes tipos de contenido, como texto enriquecido, imágenes y archivos adjuntos.

- **Función**: Permite la codificación de mensajes en formatos distintos al texto plano, facilitando la inclusión de archivos y formatos multimedia en los correos electrónicos.

2. **STARTTLS**
   - **Descripción**: STARTTLS es una extensión que permite a los protocolos SMTP, POP3 e IMAP operar sobre una conexión cifrada utilizando TLS (Transport Layer Security).
   - **Función**: Mejora la seguridad de la comunicación de correos electrónicos al cifrar los datos en tránsito, protegiendo contra la interceptación y el espionaje.
3. **Para Enviar correos**: **SMTP** es el protocolo principal utilizado.
4. **Para Recibir correos**: Se utilizan **POP3** para descargar correos y almacenarlos localmente, e **IMAP** para acceder y gestionar correos directamente en el servidor.
5. **Para seguridad**: **STARTTLS** proporciona cifrado para las comunicaciones de correo electrónico.

31 ¿QUÉ PROTOCOLO PUEDE USARSE PARA LEER CORREO RECIBIDO?

Para leer correo recibido, los protocolos más comunes son **POP3 (Post Office Protocol version 3)** y **IMAP (Internet Message Access Protocol)**. Ambos protocolos permiten acceder y gestionar los correos electrónicos almacenados en un servidor, pero tienen diferencias clave en cómo manejan los mensajes:

1. POP3 (Post Office Protocol version 3)

- **Descripción**: POP3 es un protocolo utilizado para descargar correos electrónicos desde un servidor de correo a un cliente de correo local. Una vez descargados, los correos se almacenan en el dispositivo del usuario y generalmente se eliminan del servidor.
- **Puerto**: Opera en el puerto **110** para conexiones estándar y en el puerto **995** para conexiones seguras (POP3S).
- **Características**:
  - **Descarga y almacenamiento local**: Los correos se descargan al dispositivo local y se eliminan del servidor (aunque algunas configuraciones permiten mantener una copia en el servidor).
  - **Acceso desde un solo dispositivo**: Dado que los correos se almacenan localmente, generalmente solo se pueden acceder desde el dispositivo donde se descargaron.

2. IMAP (Internet Message Access Protocol)

- **Descripción**: IMAP es un protocolo para acceder y gestionar correos electrónicos en el servidor. Los correos permanecen en el servidor, lo que permite la sincronización y el acceso desde múltiples dispositivos.
- **Puerto**: Opera en el puerto **143** para conexiones estándar y en el puerto **993** para conexiones seguras (IMAPS).
- **Características**:

- **Sincronización**: Los correos se mantienen en el servidor y se sincronizan con el cliente de correo. Las acciones realizadas en un dispositivo (como leer, mover o eliminar mensajes) se reflejan en todos los dispositivos.
- **Acceso desde múltiples dispositivos**: Permite acceder a los correos desde varios dispositivos, ya que los mensajes permanecen en el servidor.

Comparación entre POP3 e IMAP

- **POP3**:
  - **Ventajas**: Simple y eficiente para el almacenamiento local. Ideal si solo se usa un dispositivo para acceder al correo.
  - **Desventajas**: No permite la sincronización entre múltiples dispositivos. Los correos se eliminan del servidor (a menos que se configure para mantener una copia).
- **IMAP**:
  - **Ventajas**: Permite la sincronización entre múltiples dispositivos y mantiene los correos en el servidor, facilitando el acceso desde cualquier lugar.
  - **Desventajas**: Dependencia de la conexión a Internet y del espacio en el servidor.

32 DIFERENCIAS ENTRE IPV4 E IPV6

IPv4 e **IPv6** son dos versiones del Protocolo de Internet (IP) utilizados para identificar y localizar dispositivos en una red. Aunque ambos cumplen la función de direccionamiento y enrutamiento en redes, tienen diferencias significativas en cuanto a su estructura, capacidad y características. A continuación se detallan las principales diferencias entre IPv4 e IPv6:

1. Espacio de Direccionamiento

- **IPv4**:
  - **Dirección**: Utiliza direcciones de 32 bits, lo que proporciona aproximadamente **4.3 mil millones** de direcciones únicas.
  - **Formato**: Las direcciones se representan en formato decimal punteado, por ejemplo, 192.168.1.1.
- **IPv6**:
  - **Dirección**: Utiliza direcciones de 128 bits, ofreciendo un espacio de direccionamiento mucho mayor, aproximadamente **340 undecillones** (3.4 x 10^38) de direcciones únicas.
  - **Formato**: Las direcciones se representan en formato hexadecimal separado por dos puntos, por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

2. Estructura de la Dirección

- **IPv4**:

  - **Longitud**: 32 bits (4 bytes).
  - **Formato**: Dividida en 4 octetos (8 bits cada uno) separados por puntos.
  - **Ejemplo**: 192.168.0.1
- **IPv6**:
  - **Longitud**: 128 bits (16 bytes).
  - **Formato**: Dividida en 8 bloques de 16 bits, cada uno representado en hexadecimal y separado por dos puntos.
  - **Ejemplo**: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

3. Encabezado

- **IPv4**:
  - **Encabezado**: Tiene un encabezado de 20 a 60 bytes de longitud, dependiendo de las opciones.
  - **Campos**: Contiene campos como Dirección IP de origen y destino, Longitud del encabezado, y más.
- **IPv6**:
  - **Encabezado**: Tiene un encabezado fijo de 40 bytes, simplificado en comparación con IPv4.
  - **Campos**: Contiene campos como Dirección IP de origen y destino, y una sección llamada Next Header que señala a los encabezados de extensión.

4. Configuración y Asignación

- **IPv4**:
  - **Configuración**: Puede requerir configuración manual o automática a través de DHCP (Dynamic Host Configuration Protocol).
  - **NAT (Network Address Translation)**: Utilizado para conservar el espacio de direcciones mediante la traducción de direcciones privadas a direcciones públicas.
- **IPv6**:
  - **Configuración**: Soporta la autoconfiguración sin estado (SLAAC) y configuración automática a través de DHCPv6.
  - **NAT**: Generalmente no se utiliza, ya que el amplio espacio de direcciones de IPv6 elimina la necesidad de NAT.

5. Seguridad

- **IPv4**:
  - **Seguridad**: La seguridad no está integrada en el protocolo. IPsec (Internet Protocol Security) puede ser utilizado para añadir seguridad, pero no es obligatorio.
- **IPv6**:
  - **Seguridad**: IPsec está integrado en el protocolo y es un componente obligatorio, proporcionando cifrado y autenticación.

6. Soporte para Multicast y broadcast

- **IPv4**:
  - **Multicast**: Soportado, permitiendo la transmisión de datos a múltiples destinatarios.
  - **Broadcast**: Soportado, permitiendo la transmisión de datos a todos los dispositivos en una red.
- **IPv6**:
  - **Multicast**: Soportado, pero el broadcast no se utiliza. En su lugar, se emplean otras técnicas como el multicast y la transmisión a grupos específicos.

7. Fragmentación

- **IPv4**:
  - **Fragmentación**: Realizada tanto por el remitente como por los routers en el camino para adaptar los paquetes a las limitaciones del enlace.
- **IPv6**:
  - **Fragmentación**: Solo realizada por el remitente. Los routers no fragmentan los paquetes; deben ser capaces de manejar el tamaño máximo del paquete o rechazarlo si es demasiado grande.

8. Compatibilidad y Coexistencia

- **IPv4**:
  - **Compatibilidad**: No es compatible de forma nativa con IPv6. Los dos protocolos deben coexistir en redes que soporten ambos.
- **IPv6**:
  - **Compatibilidad**: Diseñado para coexistir con IPv4 durante la transición. Existen mecanismos como el túnel y la traducción para permitir la interoperabilidad entre IPv4 e IPv6.

Resumen

- **IPv4**: Usa direcciones de 32 bits, con un espacio limitado y encabezados más complejos. Configuración a través de DHCP y uso de NAT.
- **IPv6**: Usa direcciones de 128 bits, con un espacio casi ilimitado y encabezados simplificados. Soporta autoconfiguración y tiene seguridad integrada con IPsec.

IPv6 fue diseñado para superar las limitaciones de IPv4 y soportar la creciente demanda de direcciones IP a medida que Internet sigue expandiéndose.

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.

Walter Mirengo: Cuando era chico (8 u 9 años), mi hermano solía conectar las PC de mi casa para jugar en red entre sí, de ahí aprendi las palabras TCP/IP, lo que era una LAN local y ciertos conceptos básicos, como las IP y demás… aunque no entendia nada jajaja. Ya mas de adulto, no, ninguna salvo configurar los dispositivos de mi casa.

Paula Gabriela Amado: mi experiencia en redes es limitada, pero he tenido la oportunidad de familiarizarme con algunos conceptos mientras estudiaba tecnologías en la nube. En ese contexto, trabajé con redes virtuales, entendiendo cómo funcionan las conexiones entre servidores y servicios en plataformas como AWS o Azure.

Martin Kaen: En mi caso si bien no tengo experiencia directa trabajando con redes, siempre tuvo un lugar importante en mi vida y lo sigue teniendo en muchas formas. Mi viejo tenía un cybercafé en Catamarca y toda la red la hizo mi hermano (en ese momento él tenía unos 15 años y yo 10). Así que aunque poco podía entender, me encantaba que mi hermano me muestre los switches con todos los cables. Un poco más grande, de adolescente, siempre era yo el que armaba las LAN para jugar con amigos al Age of Empires (solo usábamos un switch y era todo local).

Después de más grande, ya trabajando como developer, como siempre fui del ámbito Linux me interesó mucho la parte de despliegue. También trabajé 2 años en una empresa de Cloud Hosting donde aprendí bastante del tema servidores. En mi trabajo actual tengo que ver temas de deploy, pero no está enfocado en eso.

Por último, la experiencia de redes que me pareció más interesante, es haber ido a conocer el data center de Arsat, nos hicieron un recorrido, vimos un montón de infra, los sistemas de seguridad y anti incendio. Todo fue muy interesante.

34 FUENTE

- https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/
- https://www.redeszone.net/tutoriales/redes-cable/desactivar-netbios-windows/
- https://www.ibm.com/es-es/topics/storage-area-network
- https://www.proydesa.org/portal/noticias/1576-hub-switch-y-router-cuales-son-sus-diferencias
- https://autmix.com/blog/que-es-protocolo-red
- https://www.avg.com/es/signal/what-is-tcp-ip
- https://www.tokioschool.com/noticias/topologias-red/
- https://learn.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top
- https://www.cloudflare.com/es-es/learning/dns/what-is-dns/
- https://nsrc.org/wrc/trac/wirelessu/raw-attachment/wiki/WALC2009/02_es_estandares-inalambricos_guia_v02[1].pdf
- https://www.mcafee.com/blogs/es-es/privacy-identity-protection/que-es-un-proxy//