Instituto de Formación Técnica Superior Nro.18

PROGRAMACIÓN SOBRE REDES

Profesor: Lucas Rusatti

TRABAJO PRÁCTICO TEÓRICO

Integrantes:

Abrahams Nieves

Carlos Daniel Spindler

Ignacio González

José Vera

1 - ¿Qué es una VLAN?

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

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

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

Beneficios de usar VLANs:

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

2 - ¿Qué es una VPN?

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

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

Esto tiene dos efectos principales:

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

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

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

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

3 - ¿Qué es una SAN?

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

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

Las SAN están compuestas principalmente por tres capas:

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

Beneficios de una SAN

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

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

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

1. Repetidor (Repeater)

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

2. Hub

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

3. Switch

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

4. Router

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

Cuadro de diferencias

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

5 - ¿Qué es un protocolo de comunicaciones?

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

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

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

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

Ejemplos de protocolos comunes

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

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

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

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

TCP/IP

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

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

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

NetBIOS

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

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

Resumen de diferencias

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

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

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

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

1. **Encabezado (Header):** Contiene la información de control y direccionamiento necesaria para que el paquete sea entregado correctamente. El encabezado, a su vez, está formado por dos encabezados clave:

    - **Encabezado TCP:** Agregado en la capa de transporte, contiene información para asegurar la fiabilidad de la conexión. Incluye los puertos de origen y destino, el número de secuencia (para reordenar los paquetes), el número de acuse de recibo y los "flags" de control.
    - **Encabezado IP:** Agregado en la capa de red, contiene la dirección IP de origen y destino, lo que permite que el paquete sea enrutado a través de diferentes redes.

2. **Carga útil / Payload:** Es la parte que contiene los datos reales que se están enviando, como un archivo, parte de una página web o un correo electrónico.

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

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

Los flags más importantes son:

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

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

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

1. PAN (Personal Area Network)

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

2. LAN (Local Area Network)

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

3. MAN (Metropolitan Area Network)

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

4. WAN (Wide Area Network)

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

5. GAN (Global Area Network)

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

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

La topología de red describe la forma en que los dispositivos (nodos) y los enlaces (cables o conexiones inalámbricas) están organizados dentro de una red. Es un concepto clave para diseñar, administrar y optimizar redes, ya que permite comprender cómo fluye la información y cómo se interconectan los equipos.

Existen diferentes **tipos de topologías de red**:

- **Punto a punto:** conexión directa entre dos dispositivos.
- **Bus:** todos los dispositivos comparten un único canal de comunicación.
- **Anillo:** los dispositivos están conectados formando un círculo cerrado; los datos viajan en una sola dirección.
- **Estrella:** cada dispositivo se conecta a un nodo central (hub o switch).
- **Árbol:** estructura jerárquica que combina varias estrellas conectadas a un nodo central superior.
- **Malla:** cada dispositivo se conecta directamente a varios otros, formando múltiples caminos posibles.
- **Híbrida:** mezcla dos o más topologías anteriores, adaptándose a necesidades específicas.

Topología de malla.

En esta configuración, los dispositivos se interconectan de forma descentralizada. No dependen de un concentrador central, sino que se conectan directamente entre sí, lo que permite múltiples rutas para la transmisión de datos. Esto mejora la redundancia, la tolerancia a fallos y la escalabilidad de la red.

Existen dos variantes principales:

- **Malla completa:** cada dispositivo está conectado directamente con todos los demás.
- **Malla parcial:** solo algunos dispositivos tienen conexiones directas entre sí; los demás se conectan a través de otros nodos. Es más económica y práctica en redes grandes.

10 Explicar el servicio de DHCP.

El Protocolo de Configuración Dinámica de Host (DHCP) es un sistema para asignar direcciones IP a cada dispositivo de red (conocido como host) en la red de una organización. Un host puede ser una computadora de escritorio, una portátil, una tableta, un dispositivo móvil, un cliente ligero u otros tipos de dispositivos. Cada host debe tener una dirección IP para comunicarse con otros dispositivos a través de internet. El protocolo de red DHCP asigna direcciones automáticamente, sin necesidad de que los administradores de red las asignen manualmente. DHCP también se encarga de asignar automáticamente nuevas direcciones IP cuando los dispositivos se trasladan a nuevas ubicaciones en la red. Además de las direcciones IP, un servicio DHCP asigna parámetros de configuración como direcciones del Sistema de Nombres de Dominio (DNS), máscaras de subred y puertas de enlace predeterminadas, esenciales para las comunicaciones de red.

El protocolo DHCP permite a las organizaciones y administradores de red:

- Optimice la gestión de la red. DHCP reduce la carga de los administradores de red al gestionar de forma eficiente y automática la asignación de direcciones IP. DHCP es especialmente eficaz para dispositivos que requieren actualizaciones frecuentes, como teléfonos móviles que se mueven entre diferentes ubicaciones en una red inalámbrica.
- Optimice las direcciones IP. La posibilidad de reutilizar direcciones IP minimiza el número total de direcciones necesarias para una red.
- Simplifique la gestión de cambios. DHCP permite a las organizaciones cambiar los esquemas de direcciones IP de un rango a otro sin interrumpir a los usuarios finales.
- Minimiza los errores. DHCP centraliza y automatiza la gestión de direcciones IP, minimizando la posibilidad de que dos dispositivos reciban la misma dirección o que un dispositivo reciba una dirección incorrecta.

11 Explicar el servicio de DNS.

El **Protocolo de Configuración Dinámica de Host (DHCP, por sus siglas en inglés)** es un servicio de red que asigna de forma **automática** direcciones IP y otros parámetros de configuración a los dispositivos conectados a una red. De esta manera, los administradores no tienen que asignar manualmente direcciones IP a cada equipo.

Cada host (computadora, portátil, tablet, teléfono móvil, impresora, etc.) necesita una dirección IP para comunicarse en la red. El servicio DHCP no solo otorga esta dirección, sino que también puede asignar:

- Máscara de subred
- Puerta de enlace predeterminada (gateway)
- Servidores DNS
- Otros parámetros necesarios para la conectividad de red

Ventajas y funciones del DHCP:

- **Automatización y eficiencia:** simplifica la gestión de la red al asignar direcciones IP de manera dinámica y automática, especialmente útil en redes grandes o con dispositivos móviles.
- **Optimización de direcciones IP:** permite reutilizar direcciones cuando los dispositivos se desconectan o cambian de ubicación, reduciendo el número total necesario.
- **Flexibilidad en cambios:** facilita modificar los rangos de direcciones IP sin interrumpir a los usuarios.
- **Reducción de errores:** al centralizar y automatizar la asignación de direcciones, disminuye el riesgo de conflictos de IP (dos dispositivos con la misma dirección) o configuraciones erróneas.

En resumen, **DHCP** es un protocolo esencial para la administración moderna de redes, ya que automatiza la configuración de los dispositivos y mejora la eficiencia y confiabilidad del entorno de red.

12 Explicar las tecnologías Wireless, y sus estándares.

Las **tecnologías Wireless** (o redes inalámbricas) son redes informáticas que utilizan **radiofrecuencia (RF)** para conectar dispositivos sin necesidad de cables. Son muy comunes en hogares, empresas y redes de telecomunicaciones, ya que permiten movilidad y facilidad de instalación.

Además de las redes **LAN inalámbricas (Wi-Fi)**, existen otros tipos de redes Wireless:

- **PAN (Personal Area Network):** redes de corto alcance para conectar dispositivos personales (por ejemplo, Bluetooth).
- **MAN (Metropolitan Area Network):** redes inalámbricas que cubren ciudades o áreas metropolitanas.
- **WAN (Wide Area Network):** redes que abarcan grandes distancias, incluso países o continentes.

Una red inalámbrica basada en Wi-Fi envía señales mediante ondas de radio (como lo hacen los celulares y las radios, pero en frecuencias y modulaciones distintas).

Estándares Wireless (IEEE 802.11):

El estándar principal para redes inalámbricas es **IEEE 802.11**, que se actualiza de manera continua con enmiendas identificadas por letras. Los más conocidos son:

- **802.11a:** opera en la banda de 5 GHz, hasta 54 Mbps, usando OFDM (multiplexación ortogonal por división de frecuencia).
- **802.11b:** en la banda de 2,4 GHz, hasta 11 Mbps, usando modulación CCK.
- **802.11g:** mejora las velocidades en 2,4 GHz, compatible con 802.11b, usando OFDM.
- **802.11n:** opera en 2,4 y 5 GHz, introduce **MIMO** (múltiples antenas para transmitir y recibir), con mayores velocidades y alcance.
- **802.11ac:** opera en 5 GHz, mejora la velocidad y capacidad respecto a 802.11n.
- **802.11ax (Wi-Fi 6):** unifica especificaciones en todas las bandas disponibles, usa **OFDMA** para mejorar la eficiencia del espectro y es el estándar actual en la mayoría de dispositivos nuevos.

Otros estándares 802.11:

A lo largo de los años se han creado más enmiendas, centradas en mejorar la **seguridad**, **calidad de servicio**, **eficiencia energética** y otras características.

En resumen, las tecnologías **Wireless** permiten la conexión sin cables y, gracias a los distintos estándares, se han ido adaptando a mayores velocidades, mejor rendimiento y más seguridad.

13 ¿Qué es un Proxy?

Un **servidor proxy** es un intermediario entre un cliente (por ejemplo, una computadora) y un servidor de destino. Se encarga de recibir las solicitudes del cliente, reenviarlas al servidor correspondiente y devolver las respuestas al cliente. Esto permite anonimato, mejora de la seguridad, control de acceso y, en algunos casos, aceleración de las conexiones mediante almacenamiento en caché.

En otras palabras, el proxy actúa como **"representante"** o mediador entre dos sistemas informáticos. El cliente no se comunica directamente con el servidor final, sino a través del proxy, que utiliza su propia dirección IP para interactuar con el destino. A menudo, ni el cliente ni el servidor saben que existe un proxy en medio de la comunicación.

Ventajas y usos principales de un servidor proxy:

- **Anonimato y privacidad:** Oculta la dirección IP del usuario, protegiendo su identidad en Internet.
- **Aceleración de carga:** Mediante almacenamiento en caché, reduce el tráfico de datos y mejora los tiempos de respuesta.
- **Balanceo de carga:** Distribuye las solicitudes entre varios servidores para optimizar recursos.
- **Control de acceso:** En empresas y centros educativos se utilizan para restringir o filtrar contenidos.
- **Eludir bloqueos geográficos:** Permite simular la ubicación del usuario para acceder a contenido restringido en determinadas regiones.
- **Seguridad adicional:** Puede bloquear tráfico sospechoso y proteger frente a sitios web potencialmente dañinos.

En resumen, un proxy ofrece **mayor control, seguridad y flexibilidad** en la comunicación entre usuarios y servidores.

14 Explicar el protocolo Spanning tree.

El **Spanning Tree Protocol (STP)** es un protocolo utilizado en redes Ethernet que evita la formación de **tramas duplicadas** y, por lo tanto, previene problemas como **tormentas de broadcast** que pueden saturar o paralizar la red.

El problema que STP aborda surge cuando existen **múltiples rutas simultáneas** entre dos conmutadores. Sin un control, los paquetes podrían circular indefinidamente, generando congestión. STP soluciona esto creando un **árbol lógico** de la red, en el que se determina la **mejor ruta** para la transmisión de datos y se **desactivan temporalmente los puertos redundantes**.

Funcionamiento básico:

- Los conmutadores intercambian **Bridge Protocol Data Units (BPDU)** a intervalos regulares (cada 2 segundos), usando la dirección MAC especial 01-80-C2-00-00-10.
- Gracias a estas BPDU, STP obtiene un **mapa completo de la topología de la red** y elige la conexión más rápida y eficiente.
- Los puertos no utilizados se bloquean hasta que sea necesario reactivar la conexión.

Gestión de fallos:

- Si un enlace falla y no se reciben BPDU, el conmutador detecta el fallo y **recalcula la topología** del árbol.
- Las conexiones previamente desactivadas pueden activarse para mantener la comunicación, asegurando **la máxima disponibilidad y velocidad**.
- En configuraciones complejas, este proceso puede tardar más de 30 segundos, dependiendo del tamaño de la red.

Resumen de beneficios:

- Evita **bucles de red** y tormentas de broadcast.
- Garantiza **conectividad redundante** sin interrupciones prolongadas.
- Optimiza la transmisión de datos mediante la selección de la ruta más rápida.

15 Explicar el protocolo de comunicaciones OSPF.

El **OSPF (Open Shortest Path First)** es un **protocolo de enrutamiento interior (IGP)** utilizado para intercambiar información de enrutamiento dentro de redes IP. Fue diseñado para superar las limitaciones de protocolos anteriores como **RIP** y es ampliamente usado en **redes grandes y complejas**.

Características principales:

- **Enrutamiento con estado de enlace:** Cada router conoce la **topología completa** de la red y calcula la mejor ruta para enviar paquetes, considerando el ancho de banda disponible.
- **Algoritmo de camino más corto:** OSPF determina la ruta más eficiente entre dos puntos usando el **algoritmo de Dijkstra**.
- **Estructura por áreas:** La red se divide en **áreas** para limitar la cantidad de información de enrutamiento que se distribuye. Las áreas se conectan mediante un **router de frontera de área (ABR)**, que intercambia información entre ellas.

Aplicaciones y ventajas:

- **Enrutamiento en redes WAN:** Distribuye la información de forma eficiente en redes de gran tamaño.
- **Optimización del tráfico:** Calcula rutas alternativas ante fallas, mejorando eficiencia y disponibilidad.
- **Soporte de múltiples VLAN:** Facilita la administración y monitoreo de redes segmentadas.
- **Integración con otros protocolos:** Compatible con protocolos como **BGP**, para una gestión más eficiente de rutas.
- **Escalabilidad:** Permite agregar nuevas redes sin interrumpir el funcionamiento de la red existente

16 Explicar el protocolo ARP.

El **ARP (Address Resolution Protocol)** es un protocolo que permite **asociar una dirección IP a una dirección física (MAC)** dentro de una red de área local (LAN). Esto es fundamental porque los dispositivos necesitan conocer la dirección MAC del destino para enviar datos correctamente, aunque solo tengan su dirección IP.

Funcionamiento básico:

1. Cuando un dispositivo desea enviar datos a otro en la LAN, verifica su **caché ARP** para ver si ya tiene la correspondencia IP → MAC.
2. Si no la tiene, envía una **solicitud ARP** a la red para obtener la dirección MAC correspondiente a la IP deseada.
3. Una vez recibida la respuesta, se almacena en la caché ARP (dinámica o estática) para futuras comunicaciones.

Caché ARP:

- Mantiene temporalmente las asociaciones IP → MAC.
- Se purga periódicamente para liberar espacio y proteger la privacidad.

Tipos y variantes de ARP:

- **ARP de proxy:** Un dispositivo responde a solicitudes ARP de una red distinta, ofreciendo su propia dirección MAC como destino.
- **ARP gratuito:** Un host anuncia o actualiza su dirección IP a MAC sin que exista una solicitud previa.
- **ARP reverso (RARP):** Permite a un host conocer su propia dirección IP usando su dirección MAC.
- **ARP inverso (IARP):** Permite obtener la dirección IP a partir de una dirección MAC.

Ventajas:

- Facilita la comunicación en redes LAN.
- Automatiza la resolución de direcciones, evitando errores de envío.
- Permite implementaciones avanzadas como proxies o anuncios de dirección.

17 ¿Qué es un Firewall?:

Un firewall es un dispositivo de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas. El propósito principal de un firewall es establecer una barrera entre una red interna confiable y redes externas no confiables.

Los firewalls vienen en formas de hardware y software, y funcionan inspeccionando paquetes de datos y determinando si los permiten o bloquean en función de un conjunto de reglas. Las organizaciones pueden configurar estas reglas para permitir o denegar el tráfico en función de varios criterios, como direcciones IP de origen y destino, números de puerto y tipo de protocolo.

Los firewalls son la base de la seguridad de la red, protegiendo la red del acceso no autorizado. Evitan que los actores maliciosos, piratas informáticos, bots y otras amenazas, sobrecarguen o se infiltren en una red privada para robar datos sensibles.

Afortunadamente, las tecnologías de firewall de vanguardia con servicios impulsados por IA están acelerando la seguridad de la red. Combinando las fortalezas de las herramientas tradicionales con las capacidades innovadoras de las nuevas soluciones, los proveedores de firewall modernos ayudan a las organizaciones a defenderse incluso contra las estrategias de ataque más complejas.

Los firewalls regulan el tráfico entrante y saliente, protegiendo la red de:

- **Amenazas externas** como virus, puertas traseras, correos electrónicos de suplantación de identidad y ataques de denegación de servicio (DoS). Los firewalls filtran los flujos de tráfico entrantes, evitando el acceso no autorizado a datos sensibles y frustrando posibles infecciones de malware.

- **Amenazas internas** como actores maliciosos conocidos o aplicaciones riesgosas. Un firewall puede aplicar reglas y políticas para restringir ciertos tipos de tráfico saliente, lo que ayuda a identificar actividades sospechosas y mitigar la exfiltración de datos.

Fuente [https://www.fortinet.com/lat/resources/cyberglossary/firewall]

18 ¿Qué es una DMZ?

Una DMZ o zona desmilitarizada es una red perimetral que protege y agrega una capa adicional de seguridad a la red de área local interna de una organización del tráfico no confiable.

El objetivo final de una red de zona desmilitarizada es permitir que una organización acceda a redes no confiables, como Internet, mientras garantiza que su red privada o LAN permanezca segura. Por lo general, las organizaciones almacenan servicios y recursos externos, así como servidores para el Sistema de nombres de dominio (DNS), el Protocolo de transferencia de archivos (FTP), correo, proxy, el Protocolo de voz sobre Internet (VoIP) y los servidores web, en la DMZ.

Estos servidores y recursos están aislados y tienen acceso limitado a la LAN para garantizar que se pueda acceder a ellos a través de Internet, pero la LAN interna no puede hacerlo. Como resultado, un enfoque de DMZ hace que sea más difícil para un hacker obtener acceso directo a los datos y servidores internos de una organización a través de Internet.

Las empresas con un sitio web público que utilizan los clientes deben hacer que su servidor web sea accesible a Internet. Para proteger la red de área local corporativa, el servidor web se instala en una computadora separada de los recursos internos. La DMZ permite la comunicación entre recursos comerciales protegidos, como bases de datos internas y tráfico calificado de Internet.

Una DMZ permite que los visitantes del sitio web obtengan ciertos servicios mientras proporcionan un búfer entre ellos y la red privada de la organización. Como resultado, ofrece también beneficios de seguridad adicionales, tales como:

1. Habilitación del control de acceso: Las empresas pueden proporcionar a los usuarios acceso a servicios fuera de los perímetros de su red a través de Internet pública. La DMZ permite el acceso a estos servicios mientras implementa la *segmentación de red* para hacer que sea más difícil para un usuario no autorizado llegar a la red privada.
2. Prevenir el reconocimiento de la red: Al proporcionar un búfer entre Internet y una red privada, una DMZ evita que los atacantes realicen el trabajo de reconocimiento que realizan en la búsqueda de posibles objetivos. Los servidores dentro de la DMZ están expuestos públicamente, pero un firewall ofrece otra capa de seguridad que evita que un atacante pueda ver dentro de la red interna.
3. Bloqueo de la falsificación de protocolo de Internet (IP): los atacantes intentan encontrar formas de obtener acceso a los sistemas falsificando una dirección IP y suplantando un dispositivo aprobado

que inició sesión en una red. Una DMZ puede descubrir y detener estos intentos de suplantación de identidad, ya que otro servicio verifica la legitimidad de la dirección IP.

Los servicios de una DMZ incluyen:

- Servidores DNS
- Servidores FTP
- Servidores de correo
- Servidores proxy
- Servidores web

Fuente[https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz]

19 ¿Qué es un Gateway?

Un Gateway actúa como un enlace entre dos redes, permitiendo que los dispositivos de una red se comuniquen con los de otra. La presencia de Gateways es fundamental para acceder a Internet, facilitando la comunicación y transferencia de datos entre diferentes redes. Estas pasarelas pueden ser implementadas completamente a través de software**,** hardware o una combinación de ambos. Dado que las pasarelas de red suelen situarse en el extremo de una red, su funcionalidad se extiende para integrar capacidades como cortafuegos y servidores proxy.

Un Gateway tiene tarjetas de interfaz de red (NICs – Network Interface Cards), entradas y salidas (generalmente Ethernet), junto con software para traducir protocolos de red entre las diferentes redes que interconecta. Las funciones del Gateway también pueden implementarse mediante software. Cada vez más se están integrando en routers y otros equipos físicos.

En base a las funcionalidades que habilita, puede haber una gran variedad de Gateways, entre los que destacan los siguientes:

- **Gateway de red**: Es el más común y sirve de interfaz entre dos redes que usan protocolos diferentes. Cuando solo se menciona Gateway, nos solemos estar refiriendo a este tipo.
- **Gateway de almacenamiento en cloud**: Este tipo de Gateway funciona como un intermediario entre las solicitudes de almacenamiento API SOAP o REST y los servicios de almacenamiento en la nube. Su función esencial radica en facilitar la integración del almacenamiento privado en la nube en las aplicaciones existentes sin requerir la migración de estas aplicaciones a una nube pública. Esto simplifica la transferencia de datos y la comunicación, asegurando una mejor interoperabilidad.
- **Gateway IoT**: Conecta dispositivos IoT locales a la red, permitiendo la recopilación, procesamiento y transmisión de datos entre los dispositivos y la nube o sistemas centrales.
- **Gateway de seguridad:** Protege una red interna de amenazas externas, como ataques cibernéticos, filtrando el tráfico no autorizado y aplicando políticas de seguridad.
- **Gateway de voz:** Facilita la comunicación de voz sobre protocolos de Internet (VoIP), convirtiendo señales de voz analógicas en datos digitales para su transmisión a través de redes IP.

- **Gateway de mensajería:** Sirve como intermediario entre diferentes protocolos de mensajería, como SMS, correo electrónico y mensajes instantáneos, para facilitar la comunicación entre ellos.
- **Gateway de servicios web:** Permite la interoperabilidad entre aplicaciones y servicios web al traducir solicitudes y respuestas entre diferentes protocolos y formatos de datos.
- **Gateway de API:** Facilita el acceso y la integración de servicios y datos de aplicaciones a través de interfaces de programación de aplicaciones (API), permitiendo la comunicación entre sistemas heterogéneos.

Fuente[https://conectividadiot.telefonicatech.com/gateway/]

20 Según Microsoft, ¿qué significa NBL?

El NBL (Network Load Balancing) o Equilibrio de carga de red mejora la disponibilidad y escalabilidad de las aplicaciones de servidor de Internet tales como las usadas en servidores web, servidores FTP, servidores firewall, servidores proxy, servidores de redes privadas virtuales (VPN) y otros servidores con una importancia decisiva.

La característica de equilibrio de carga de red (NLB) distribuye el tráfico por distintos servidores mediante el protocolo de red TCP/IP. Al combinar en un solo clúster virtual dos o más equipos que ejecutan aplicaciones, NLB ofrece confiabilidad y rendimiento para los servidores web y otros servidores con una importancia decisiva.

Los servidores de un clúster NLB se denominan *hosts* y cada host ejecuta una copia independiente de las aplicaciones de servidor. NLB distribuye las solicitudes de cliente entrantes entre los hosts que forman el clúster. Se puede configurar la carga que administrará cada host. También se pueden agregar hosts de manera dinámica al clúster para administrar los aumentos de carga. NLB también puede dirigir todo el tráfico a un host único designado, que se denomina *host predeterminado*.

NLB permite que todos los equipos del clúster se dirijan al mismo conjunto de direcciones IP y mantiene un conjunto de direcciones IP exclusivas y dedicadas para cada host.

NLB se instala como un componente estándar del controlador de redes de Windows Server. Sus operaciones son transparentes para la pila de redes TCP/IP.

Fuente:
[https://learn.microsoft.com/es-es/windows-server/networking/technologies/network-load-balancing]

21 Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT.

a. Explique cada uno de estos tipos de enlace.

MPLS:

El switching de etiquetas multiprotocolo (MPLS) es un protocolo diseñado para llevar paquetes de datos a sus destinos de manera rápida y eficiente. Debido a que envía datos directamente a su destino, es superior al enrutamiento regular del protocolo de Internet (IP), que rebota datos por Internet antes de enviarlos finalmente a su destino final.

"Multiprotocolo" significa que el sistema no depende de ningún protocolo en particular para operar. Es una superposición, que le permite reenviar una variedad de diferentes tipos de datos, independientemente del protocolo utilizado para organizarlos.

Ventajas:

- Mejor rendimiento
- Mejor administración del trafico
- Seguridad mejorada

Desventajas:

- Dependencia de un operador
- Gasto
- Falta de cobertura integral

Fuente [https://www.fortinet.com/lat/resources/cyberglossary/mpls]

LAN TO LAN:

Es un servicio de transmisión de datos punto a punto basado en protocolo IP que permite interconectar dos o más redes de área local. Está diseñada específicamente para comunicar dos ubicaciones mediante una conexión privada entre ellas sin necesidad de pasar por internet. En esencia, una LAN puede enlazarse a otra igual para formar una red LAN to LAN, creando una conexión entre dos sitios distintos de manera privada y dedicada.

Esta conexión permite que los equipos como impresoras, laptops y computadoras de escritorio que trabajan en diferentes oficinas funcionen como si

estuvieran en un mismo espacio físico.

Al ser una conexión exclusiva, toda la capacidad es únicamente para la empresa, lo que evita la congestión de tráfico. Resulta más segura, pues para interceptarla se necesitaría violar la infraestructura física. Los datos no viajan por internet público sino por una línea dedicada, proporcionando mayor confidencialidad. Cuando un colaborador comparte información, ésta no sale de manera abierta, sino que viaja por la red privada del negocio.

Las arquitecturas de las redes LAN to LAN pueden configurarse en diferentes topologías según las necesidades:

Punto a punto: conecta directamente dos ubicaciones, creando un enlace exclusivo entre ellas.

Punto-multipunto: permite que una ubicación central se conecte con múltiples sitios remotos.

Malla: interconecta todos los puntos entre sí, ofreciendo mayor redundancia.

Fuente: [https://www.servnet.mx/blog/redes-lan-to-lan-que-es-funcionamiento]

MICROONDAS:

Un enlace de microondas es un sistema de comunicaciones que utiliza un haz de ondas de radio en el rango de frecuencia de microondas para transmitir información entre dos puntos fijos en la Tierra. Son cruciales para muchas formas de comunicación e impactan en una amplia gama de industrias:

- Los proveedores de servicios de internet inalámbrico utilizan enlaces de microondas para proporcionar a sus clientes acceso a internet de alta velocidad sin necesidad de conexiones por cable.
- Las empresas y los organismos gubernamentales los utilizan para proporcionar redes de comunicaciones entre instalaciones cercanas dentro de una organización, como una empresa con varios edificios en una ciudad.

Una de las razones por las que los enlaces de microondas son tan adaptables es su banda ancha. Esto significa que pueden transmitir grandes cantidades de información a alta velocidad. Otra cualidad importante de los enlaces de microondas es que no requieren equipos ni instalaciones entre los dos puntos terminales, por lo que instalar un enlace de microondas suele ser más rápido y económico que una conexión por cable. Finalmente, se pueden utilizar prácticamente en cualquier lugar, siempre que la distancia a cubrir esté dentro del alcance operativo del equipo y haya una ruta despejada (es decir, sin obstáculos sólidos) entre las ubicaciones. Las

microondas también pueden atravesar la lluvia, la niebla y la nieve, lo que significa que el mal tiempo no interrumpe la transmisión.

Un enlace de microondas unidireccional simple incluye cuatro elementos principales: un transmisor, un receptor, líneas de transmisión y antenas. Estos componentes básicos existen en todos los sistemas de radiocomunicaciones, incluyendo teléfonos celulares, radios bidireccionales, redes inalámbricas y radiodifusión comercial.

Fuente [https://ethw.org/Microwave_Link_Networks]

VSAT:

Los sistemas **VSAT** (Very Small Aperture Terminal), son redes de comunicación por satélite que, empleando antenas de pequeñas dimensiones, permiten el establecimiento de una gran variedad de servicios de comunicaciones entre un gran número de puntos o estaciones remotas, pudiendo estar supervisadas por una estación principal llamada Hub, NOC o Telepuerto.

Gracias a su flexibilidad, rápida implementación y bajos costos de instalación y operación, la tecnología VSAT se utiliza cada vez más en el despliegue de redes para aplicaciones privadas, públicas/gubernamentales y corporativas.

En todos los sectores del mercado que requieren tareas cruciales y un sistema de comunicación altamente confiable, se utiliza la tecnología VSAT. Las redes basadas en tecnología VSAT se dividen en dos categorías principales: servicios dedicados y compartidos. Los servicios compartidos (TDMA) permiten que varias estaciones remotas compartan la misma red por división de tiempo. Los servicios dedicados se comunican entre sí sin necesidad de un concentrador y con una sola portadora por canal.

Ventajas:

- Facilidad y rapidez para la puesta en operación y la incorporación de nuevas terminales
- Acceso a lugares donde no está disponible otra infraestructura terrestre, por razones físicas o económicas
- Salvan prácticamente la totalidad de los obstáculos geográficos
- Alta calidad y disponibilidad de los enlaces
- Gestión centralizada y dependencia de un único Operador de Servicios
- Coste de terminales a la baja

Fuentes:[https://satcomdefensa.com/que-es-vsat/|
https://www.icarusnet.it/en/vsat-technology/]

b. Agregue dos tipos de enlaces, no mencionados anteriormente.

Fibra Óptica:

Un enlace de fibra óptica suele ser parte de un sistema de comunicaciones de fibra óptica que proporciona una conexión de datos entre dos puntos (*conexión punto a punto*). Consiste esencialmente en un transmisor de datos, una fibra de transmisión y un receptor. Incluso para distancias de transmisión muy largas, se pueden alcanzar velocidades de datos extremadamente altas, de muchos Gbit/s o incluso varios Tbit/s.

La capacidad de manejo de grandes cantidades de datos, el evitar el ruido asociado y el aislamiento eléctrico son sólo pocas de las características que hacen que la tecnología de la fibra óptica se ideal para usarse en los sistemas industriales y comerciales.

Fuentes [https://microcompbajio.com/enlaces-de-fibra-optica/ | https://www.rp-photonics.com/fiber_optic_links.html]

Wifi Punto a Punto:

Se utilizan antenas direccionales para establecer una conexión inalámbrica de alta velocidad y baja latencia entre dos dispositivos. Estos enlaces pueden emplearse para conectar edificios, redes, dispositivos móviles, zonas rurales, entre otros.

En general, los enlaces punto a punto son una solución efectiva para conectar dispositivos y redes en diferentes entornos, ya que ofrecen una comunicación directa y eficiente sin la necesidad de dispositivos intermedios, lo que puede mejorar la velocidad y la fiabilidad de la conexión.

Una de las principales aplicaciones de los enlaces Wifi punto a punto es conectar dos edificios separados por una distancia considerable. Esto se utiliza comúnmente en instalaciones industriales, campus universitarios, áreas rurales, entre otros. Al conectar los edificios a través de un enlace Wifi punto a punto, es posible compartir información y recursos, así como comunicarse entre ellos sin la necesidad de instalar cableado adicional.

Los enlaces Wifi punto a punto también se utilizan en la implementación de sistemas de vigilancia y seguridad. Por ejemplo, se pueden conectar cámaras de seguridad ubicadas en diferentes puntos de un campus universitario o una instalación industrial para monitorear la seguridad de una zona en particular. De esta manera, se puede compartir información de manera rápida y eficiente y mejorar la respuesta ante posibles amenazas.

Fuente:

[https://eltecnic.net/redes/que-es-un-enlace-punto-a-punto/?srsltid=AfmBOopTcTNyiLIDkblyiB7WLW-it7QL4Gt2RmvuphgdAoTmpIc4eLMB]

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.

Ranking por categorías:

1. Económico (menor costo de implementación y operación)

1. Wi-Fi punto a punto (equipos baratos, poca infraestructura).
2. LAN to LAN (si ya hay cableado, solo se requiere interconexión).
3. Microonda (costo medio, depende de las torres).
4. Fibra Óptica (infraestructura cara de instalar).
5. MPLS (servicio contratado a un proveedor, no suele ser barato).
6. VSAT (carísimo por uso de satélite y mantenimiento).

---

2. Performance (latencia y estabilidad)

1. Fibra Óptica (mejor latencia y estabilidad).
2. LAN to LAN (muy estable en entornos locales).
3. MPLS (bueno, pero depende del proveedor).
4. Microonda (puede verse afectado por el clima).
5. Wi-Fi punto a punto (estable, pero menos robusto que microonda).
6. VSAT (latencia muy alta por la distancia al satélite GEO).

---

3. Mayor capacidad (ancho de banda soportado)

1. Fibra Óptica (terabits por segundo).
2. LAN to LAN (limitado al estándar Ethernet, pero muy alto).
3. MPLS (depende del contrato, pero muy capaz).
4. Microonda (varios Gbps, pero limitado por espectro).
5. Wi-Fi punto a punto (cientos de Mbps, máximo Gbps en casos).
6. VSAT (muy limitado en capacidad).

---

4. Mayor o mejor configuración de restricciones (QoS, priorización, seguridad)

1. MPLS (soporta QoS, priorización, VPNs).
2. Fibra Óptica (gran flexibilidad de configuración, especialmente en enlaces dedicados).
3. LAN to LAN (seguro y configurable en redes privadas).
4. Microonda (depende del proveedor/equipo, configurable).
5. Wi-Fi punto a punto (configurable, pero con más limitaciones).
6. VSAT (muy limitado en QoS por latencia y compartición).

---

5. Soporte a mayor distancia

1. VSAT (cubre miles de km, incluso zonas remotas).
2. Microonda (decenas de km por salto, se puede encadenar).
3. MPLS (depende del proveedor, puede abarcar ciudades/países).
4. Fibra Óptica (puede recorrer grandes distancias con repetidores, pero es caro).
5. Wi-Fi punto a punto (hasta decenas de km en condiciones ideales).
6. LAN to LAN (muy limitado, solo dentro de una misma red o con cableado físico).

---

6. Menor esfuerzo de configuración (fácil de instalar y operar)

1. LAN to LAN (prácticamente plug-and-play en la misma red).
2. Wi-Fi punto a punto (configuración inicial sencilla).
3. MPLS (proveedor lo entrega ya configurado).
4. Fibra Óptica (requiere instalación, pero después es estable).
5. Microonda (alineación de antenas y permisos, más complejo).
6. VSAT (requiere instalación, alineación al satélite y soporte técnico).

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

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

MPLS:

Porque permite conectar múltiples sedes a un mismo centro de datos

con calidad de servicio (priorización de voz/datos), seguridad y gestión centralizada.

2 d. Conectar los datos de los pozos petroleros durante 15 minutos por día.

VSAT:

Ideal para zonas alejadas donde no llega fibra, microonda ni móvil. Aunque tiene alta latencia y costo, es perfecto para transmitir datos de forma puntual en lugares inhóspitos.

3 d. Comunicar dos edificios enfrentados en la misma calle.

Wi-Fi punto a punto:

Económico, fácil de instalar, y suficiente para distancias cortas. Alternativamente se podría usar **Fibra Óptica** si se busca algo más robusto, pero wifi es la solución más práctica.

22 Describir la tecnología LTE.

Long-Term Evolution o LTE es un estándar inalámbrico de cuarta generación **(4G)** que proporciona mayor capacidad de red y velocidad para teléfonos móviles y otros dispositivos celulares en comparación con la tercera generación (3G), pero con menor rendimiento (velocidad, retardo de propagación, etc.) que la tecnología 4G pura.

LTE ofrece velocidades máximas de transferencia de datos de hasta 100 Mbps de bajada y 30 Mbps de subida. Proporciona latencia reducida, capacidad de ancho de banda escalable y compatibilidad con versiones anteriores de la tecnología existente del Sistema Global para Comunicaciones Móviles (GSM) y del Servicio Universal de Telecomunicaciones Móviles (UMTS). La evolución LTE-Advanced (LTE-A) consigue tasas de hasta 300 Mbps.

LTE es una tecnología muy buena y estable con tres características clave: permite altas tasas de bits con baja latencia, es barato y fácil de desplegar por los operadores, y evita la fragmentación por el tipo de duplexación.

TE ofrece a los usuarios varias funcionalidades que los estándares anteriores como 2G y 3G no son capaces de ofrecer:

1. **Transmisión de audio y vídeo:** LTE tiene velocidades de descarga y subida más rápidas que 2G y 3G.
2. **Conexión en tiempo real a los servicios:** con voz sobre LTE, los usuarios pueden hablar con otras personas sin experimentar retrasos ni fluctuaciones
3. **Velocidades aún más rápidas con LTE-Advanced:** las velocidades de descarga y subida son dos o tres veces más rápidas que las del LTE estándar. Todos los dispositivos LTE-Advanced son compatibles con versiones anteriores del LTE estándar.
4. **Agregación de portadoras de frecuencia:** esta característica de LTE-Advanced mejoró la capacidad de la red, agregando un ancho de banda de hasta 100 MHz en cinco portadoras (bandas) con un ancho de banda de 20 MHz cada una. Los teléfonos LTE-A combinan frecuencias de múltiples portadoras para mejorar la señal, la velocidad y la confiabilidad.

Fuentes [https://www.unir.net/revista/ingenieria/lte-que-es/ | https://www.xataka.com/moviles/que-es-lte | https://es.digi.com/blog/post/what-is-lte]

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

Microsoft Teams es la aplicación más sofisticada de mensajería para su organización. Se trata de un espacio de trabajo pensado para la colaboración en tiempo real y la comunicación, las reuniones, el uso compartido de archivos y aplicaciones, e incluso para los ocasionales emojis. Todo en un único lugar, en equipo, y con todo a disposición de todos.

En su forma más básica, Microsoft Teams es una forma para que las organizaciones agilicen sus actividades, abran las líneas de comunicación, protejan sus datos confidenciales y, en última instancia, operen a una mayor capacidad.

Fuentes:
[https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-microsoft-teams-3de4d369-0167-8def-b93b-0eb5286d7a29
https://antares.solutions/what-we-do/modern-workplace-solutions/microsoft-teams-solution/]

24 ¿Qué significa aplicar calidad en un enlace MPLS?

Aplicar calidad a un enlace MPLS significa utilizar la tecnología para garantizar un rendimiento predecible y optimizado, priorizando el tráfico sensible como la voz o el video para reducir latencia y jitter (fluctuación de la señal), asignando diferentes clases de servicio (CoS) y ancho de banda según la importancia de la aplicación. Esto se logra mediante la implementación de mecanismos de Calidad de Servicio (QoS) que clasifican el tráfico y lo enrutan por rutas predefinidas y con recursos asignados, asegurando una experiencia consistente para los usuarios.

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

Las principales diferencias entre estos tipos de conexión de red radican en su material, método de transmisión y rendimiento.

Coaxial: Utiliza un cable con un conductor central de cobre y un blindaje metálico. Su diseño lo hace resistente a las interferencias electromagnéticas. Históricamente fue usado en redes de computadoras (Ethernet) y es común hoy en día en redes de televisión por cable.

UTP (Par Trenzado No Blindado): Consiste en pares de hilos de cobre trenzados, pero no tiene blindaje adicional. Es el tipo de cable más común en las redes de área local (LAN) debido a su bajo costo, flexibilidad y facilidad de instalación. Sin embargo, es más susceptible a las interferencias que el cable coaxial o la fibra óptica.

Fibra Óptica: Transmite datos a través de pulsos de luz que viajan por finos hilos de vidrio o plástico. Ofrece la mayor velocidad y capacidad de transmisión, con una mínima atenuación de la señal, lo que la hace ideal para redes de alta velocidad y largas distancias. Su principal desventaja es el costo y la complejidad de su instalación.

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

Cisco ofrece un programa de certificaciones que valida los conocimientos y habilidades en redes.

CCENT (Cisco Certified Entry Networking Technician): Era una certificación de nivel inicial descontinuada por Cisco. Proporcionaba un conocimiento básico sobre redes y era un paso previo para la certificación CCNA.

CCNA (Cisco Certified Network Associate): Es una certificación de nivel asociado que cubre un amplio rango de fundamentos de redes, incluyendo enrutamiento, conmutación, seguridad y redes inalámbricas.

CCNP (Cisco Certified Network Professional): Es una certificación de nivel profesional. Se enfoca en la implementación y la solución avanzada de problemas de redes. Para obtenerla, se requiere aprobar varios exámenes.

Track Routing & Switching: Es el pilar fundamental de las redes de datos.

Routing (Enrutamiento): Es el proceso de seleccionar el mejor camino para enviar datos entre diferentes redes, utilizando direcciones IP. Los routers son los dispositivos que realizan esta función.

Switching (Conmutación): Es el proceso de dirigir el tráfico de datos dentro de una misma red local, utilizando direcciones MAC. Los switches son los dispositivos que realizan esta función.

Track Wireless (Inalámbrico): Este track se enfoca en redes que utilizan ondas electromagnéticas para transmitir datos, eliminando la necesidad de cables. La principal tecnología en este ámbito es Wi-Fi. Estas redes se clasifican según su alcance:

WLAN (Wireless Local Area Network): Redes inalámbricas de área local (hogares, oficinas).

WWAN (Wireless Wide Area Network): Redes de área amplia (redes móviles 3G, 4G, 5G).

27 Explique el modelo OSI.

El modelo OSI (Open Systems Interconnection) es un marco conceptual que divide la comunicación de red en siete capas. Cada capa tiene una función específica y se basa en la anterior, lo que facilita el diseño, la implementación y la solución de problemas en las redes.

Capa 7 - Aplicación: Es la más cercana al usuario final. Permite la interacción con aplicaciones de red (navegadores, clientes de correo electrónico).

Capa 6 - Presentación: Formatea, comprime y cifra los datos para que puedan ser comprendidos por la capa de aplicación.

Capa 5 - Sesión: Crea y mantiene la comunicación entre dispositivos, asegurando que la conexión permanezca abierta el tiempo necesario.

Capa 4 - Transporte: Divide los datos en segmentos y los reensambla. Se asegura de que la entrega sea completa (usando protocolos como TCP) o de que sea rápida (usando UDP).

Capa 3 - Red: Se encarga del enrutamiento. Los routers operan en esta capa para determinar la ruta óptima para enviar los datos a su destino, usando direcciones IP.

Capa 2 - Enlace de Datos: Organiza los datos en "tramas" y facilita la transferencia entre dispositivos en una misma red.

Capa 1 - Física: Se encarga de la transmisión de datos a nivel de bits (unos y ceros) a través de un medio físico, como cables o señales inalámbricas.

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

El estándar IEEE 802.3, conocido como Ethernet, define las reglas para las redes de área local (LAN). Es el estándar más utilizado en la actualidad.

Implementación**:** Se basa en un método llamado CSMA/CD (Acceso Múltiple con Detección de Señal Portadora y Detección de Colisiones), que permite a los dispositivos competir por el uso del medio de transmisión. Si se detecta una colisión de datos, la transmisión se detiene y se reintenta después de un breve periodo aleatorio.

Ventajas:

- Alta velocidad: Ha evolucionado para soportar velocidades de hasta 100 Gbps o más.
- Flexibilidad: Es compatible con diferentes tipos de medios de transmisión (cobre, fibra óptica) y diversas topologías de red (estrella, bus).
- Estandarización: Su reconocimiento como estándar internacional garantiza la compatibilidad entre equipos de distintos fabricantes.

Desventajas:

- Colisiones: En redes más antiguas o con mucho tráfico, el método CSMA/CD puede provocar colisiones que reducen el rendimiento.

29 Explicar el estándar IEEE 802.4 regula la red.

El estándar IEEE 802.4, conocido como Token Bus, fue un protocolo de red histórico utilizado en entornos industriales. Implementaba una red lógica en anillo sobre una red física de bus, usando un "testigo" (token) para controlar el acceso al medio de transmisión.

En una red Token Bus, solo el dispositivo que posee el testigo puede transmitir datos. Una vez que termina, pasa el testigo al siguiente dispositivo en el anillo lógico. Este método evitaba las colisiones y garantizaba tiempos de respuesta predecibles, lo que era crucial para aplicaciones industriales en tiempo real. Sin embargo, con el tiempo, fue superado por la popularidad de Ethernet.

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

Los protocolos de correo electrónico son conjuntos de reglas que rigen la transferencia de mensajes.

SMTP (Simple Mail Transfer Protocol): Se utiliza para enviar correos electrónicos. Maneja la transmisión de mensajes entre clientes y servidores, y entre servidores de correo.

POP3 (Post Office Protocol versión 3): Se usa para recibir correos electrónicos. Al conectarse al servidor, este protocolo descarga los mensajes a tu dispositivo local y, por defecto, los elimina del servidor. Es ideal si solo accedes a tu correo desde un único dispositivo.

IMAP (Internet Message Access Protocol): Se usa para recibir correos electrónicos. A diferencia de POP3, IMAP te permite acceder y gestionar los mensajes directamente en el servidor. Esto significa que los mensajes permanecen en el servidor y se sincronizan en todos los dispositivos que utilices, lo que facilita la lectura y gestión del correo desde múltiples ubicaciones.

31 ¿Qué protocolo puede usarse para leer correo recibido?

Para leer correo recibido se utilizan principalmente dos protocolos:

IMAP (Internet Message Access Protocol): Permite acceder y sincronizar los correos directamente en el servidor. Los mensajes no se descargan por defecto y pueden ser leídos desde cualquier dispositivo.

POP3 (Post Office Protocol versión 3): Descarga los correos del servidor a un dispositivo local y los elimina del servidor. Los mensajes solo se pueden leer en el dispositivo donde fueron descargados.

32 Diferencias entre IPV4 e IPV6

IPv4 e IPv6 son dos versiones del Protocolo de Internet que permiten la comunicación entre dispositivos en una red. La principal diferencia radica en su estructura y sus capacidades.

Direcciones:

IPv4: Utiliza direcciones de 32 bits, lo que limita el número de direcciones únicas a aproximadamente 4.3 mil millones. Se representan en formato decimal (ej: 192.168.1.1).

IPv6: Utiliza direcciones de 128 bits, proporcionando un número de direcciones virtualmente ilimitado. Se representan en formato hexadecimal (ej: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Seguridad: IPv6 incluye IPsec como una característica obligatoria y nativa, lo que mejora la seguridad de las comunicaciones al proporcionar autenticación y cifrado. En IPv4, IPsec es opcional.

Configuración: IPv6 permite la autoconfiguración de direcciones (SLAAC), eliminando la necesidad de un servidor DHCP en muchos casos. También elimina el uso de NAT (Network Address Translation), lo que permite una conectividad más eficiente de extremo a extremo.

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

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

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

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

José Vera: No tengo experiencia técnica previa en redes ni he realizado configuraciones avanzadas. Mi conocimiento se limita al uso doméstico de las redes

Abrahams Nieves: En lo personal, no tengo experiencia con redes. Mis únicos acercamientos fueron en el tercer cuatrimestre de la carrera, donde vimos un poco de redes, en la materia ‘TIC’ y luego esta materia de ‘Programación sobre redes’.

Spindler Carlos Daniel: No tengo ninguna experiencia en redes. Tampoco la tengo en TIC.