Programación sobre Redes

Trabajo Práctico Teórico

Integrantes: Ivana Ebri, Maria Laura Fiege Fava, Melina Joloidovsky

---

Consignas

1- ¿Qué es una VLAN?
2- ¿Qué es una VPN?
3- ¿Qué es una SAN?
4- Diferencias entre un Hub, Repetidor, Router y SWITCH. Explicar las diferencias.
5- ¿Qué es un protocolo de comunicaciones?
6- Explique TCP/IP y NetBios, resuma sus diferencias. (Acá sí explicar cada uno y sus diferencias)
7- ¿Cómo está formado un paquete de datos en TCP/IP? ¿Qué es un “flag” en un paquete de TCP/IP?
8- Defina la red según su geografía. Explicar distintas variantes.
9- Defina una red según su topología. Explicar distintas variantes.
10- Explicar el servicio de DHCP.
11- Explicar el servicio de DNS.
12- Explicar las tecnologías Wireless, y sus estándares.
13- ¿Qué es un Proxy?
14- Explicar el protocolo Spanning tree.
15- Explicar el protocolo de comunicaciones OSPF.
16- Explicar el protocolo ARP.
17- ¿Qué es un Firewall?
18- ¿Qué es una DMZ?
19- ¿Qué es un Gateway?
20- Según Microsoft, ¿qué significa NBL?
21- Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT.
    a. Explique cada uno de estos tipos de enlace.
    b. Agregue dos tipos de enlaces, no mencionados anteriormente.
    c. Ranking de enlaces según lo pedido (de uno a seis, siendo uno el mejor): Por económico, performance, mayor capacidad, mayor o mejor configuración de restricciones, soporte a mayor distancia, menor esfuerzo de configuración.
    d. Elija un tipo de enlace para los siguientes escenarios:
        1 d. Conectividad de varios de call centers con un data center central.
        2 d. Conectar los datos de los pozos petroleros durante 15 minutos por día.
        3 d. Comunicar dos edificios enfrentados en la misma calle.
22- Describir la tecnología LTE.
23- Explique la solución de Microsoft Teams. Si quieren describir otra solución de otra empresa es también válido.
24- ¿Qué significa aplicar calidad en un enlace MPLS?
25- ¿Qué diferencias puede encontrar entre una conexión Coaxial, UTP o Fibra?
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).
27- Explique el modelo OSI.
28- Realizar cuestionario online y copiar el resultado: (1 por cada integrante)
https://es.educaplay.com/es/recursoseducativos/706834/test_de_redes_y_comunicaciones.htm
29- Explicar el estándar IEEE 802.3 regula la red. Cómo se implementa, ventajas y desventajas.
30- Explicar el estándar IEEE 802.4 regula la red.
31- ¿Qué protocolos se usan para enviar y recibir correo?
32- ¿Qué protocolo puede usarse para leer correo recibido?
33- Diferencias entre IPV4 e IPV6
34- (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes?
Ejemplos.: Acceder y configurar el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configuró una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.

1- ¿Qué es una VLAN?

Una VLAN es un *método para crear redes lógicas independientes dentro de una misma red física*. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local. Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo computador, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local. Las VLAN permiten la segmentación de una red para mejorar la seguridad, optimizar el rendimiento y facilitar la gestión de la red al reducir el tráfico innecesario en cada segmento.

2- ¿Qué es una VPN?

Una VPN o red privada virtual *crea una conexión de red privada entre dispositivos a través de Internet*. Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas. Su funcionamiento consiste en ocultar las direcciones IP de los usuarios y cifrar los datos para que nadie que no esté autorizado a recibirlos pueda leerlos. Los servicios de VPN sirven para proteger la privacidad, anonimato y seguridad al enviar los datos por internet. Mediante el cifrado, mantienen segura la información personal, como contraseñas e historial de navegación, especialmente en redes públicas. Ocultan la dirección IP para garantizar el anonimato y usan criptografía para evitar accesos no autorizados, cerrando programas en caso de actividad sospechosa, lo que protege tanto a usuarios individuales como a empresas. Las VPN también pueden permitir el acceso remoto seguro a redes corporativas, facilitando el teletrabajo y la colaboración a distancia.

3- ¿Qué es una SAN?

Las redes de área de almacenamiento (SAN) *son la arquitectura de almacenamiento más utilizada por las empresas debido a su alto rendimiento y baja latencia*, especialmente con el uso de almacenamiento all-flash. Al centralizar el almacenamiento, las SAN permiten la implementación uniforme de seguridad, protección de datos y recuperación de desastres. Basadas en bloques, conectan servidores a unidades lógicas (LUN) de manera eficiente, representando alrededor de dos tercios del mercado de almacenamiento en red. Las SAN están diseñadas para ser altamente disponibles y resilientes, resistiendo múltiples fallos de componentes. Este tipo de red de almacenamiento mejora la eficiencia en el manejo de grandes volúmenes de datos y ofrece opciones avanzadas de recuperación ante desastres.

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

DISPOSITIVO	FUNCIÓN PRINCIPAL	CAPA DEL MODELO OSI	CARACTERÍSTICAS PRINCIPALES	USO COMÚN
HUB	Envía datos a todos los dispositivos conectados, sin discriminar destinatarios	Capa 1 (física)	Repite señales a todos los puertos; no distingue entre direcciones. No administra tráfico, generando colisiones	Pequeñas redes que no requieren gestión avanzada del tráfico.
REPETIDOR	Amplifica y retransmite señales para extender el alcance de la red	Capa 1 (física)	Refuerza las señales debilitadas en redes largas; no modifica los datos.	Extender el alcance de una red en áreas grandes o distantes
ROUTER	Dirige el tráfico entre diferentes redes, como la red local e Internet	Capa 3 (red)	Usa direcciones IP para determinar la mejor ruta para los datos; puede conectar diferentes tipos de redes	Redes domésticas y empresariales para conectar múltiples redes
SWITCH	Envía datos solo al dispositivo destino dentro de una red local	Capa 2	Aprende y almacena direcciones MAC, gestionando eficientemente el tráfico; evita colisiones	Redes locales (LAN) para gestionar el tráfico de datos entre dispositivos conectados

5- ¿Qué es un protocolo de comunicaciones?

En informática y telecomunicación, *un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades* (computadoras, teléfonos celulares, etc.) de un sistema de comunicación *se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física*. Se trata de las reglas y estándares que definen la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Estos protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos. También se define como un conjunto de normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos (paquetes) y la forma en que la información debe procesarse. Los protocolos también pueden definir cómo se maneja el control de flujo y el control de errores durante la transmisión.

6- Explique TCP/IP y NetBios, resuma sus diferencias.

TCP/IP es la identificación de un grupo de protocolos de red que hacen posible la transferencia de datos en redes, entre equipos informáticos e internet. Esta sigla referencia los protocolos:

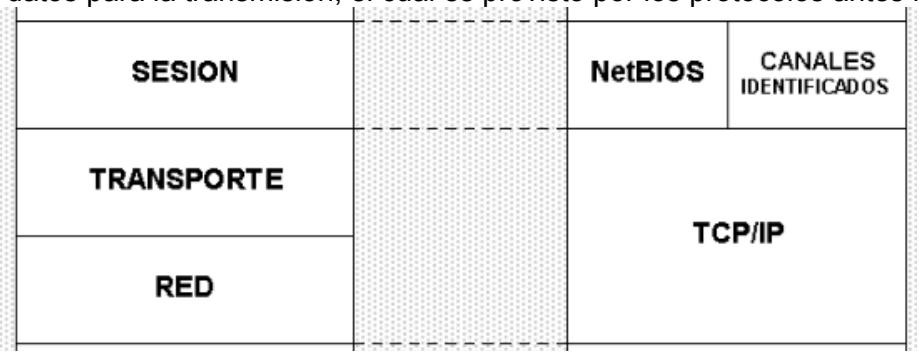
- *TCP* es el Protocolo de Control de Transmisión, el cual permite establecer una conexión y el intercambio de datos entre dos anfitriones. Este protocolo proporciona un transporte fiable de datos.
- *IP* o protocolo de internet, utiliza direcciones series de cuatro octetos con formato de punto decimal (como por ejemplo 11.2.333.44). Este protocolo lleva los datos a otras máquinas de la red.

El modelo TCP/IP permite un intercambio de datos fiable dentro de una red, definiendo los pasos a seguir desde que se envían los datos (en paquetes) hasta que son recibidos.

NetBIOS, Network Basic Input/Output System, provee los servicios de sesión descritos en la capa 5 del modelo OSI. Es un protocolo de aplicación para compartir recursos en red. Se encarga de establecer la sesión y mantener las conexiones. Sin embargo, este protocolo no concreta ningún transporte ni envío de información a otras máquinas por lo que requiere de otros protocolos para cumplir con estas tareas; por sí mismo, no podrá transportar los datos en redes LAN ni WAN, para lo cual debe usar otro mecanismo de transporte (Ej: en redes LAN protocolo NetBEUI, en redes WAN protocolo TCP/IP). Los protocolos que pueden prestar el servicio de transporte a NetBIOS son:

- IPC/IPX
- NetBEUI
- TCP/IP

El hecho de tener que ser transportado por otros protocolos se debe a que al operar en la capa 5 de OSI no provee un formato de datos para la transmisión, el cual es provisto por los protocolos antes mencionados.



La **diferencia** esencial se encuentra en que el protocolo *NetBIOS opera en la capa de sesion del modelo OSI donde se abre la comunicación con otro equipo en la red, lleva a cabo la solicitud, la autorización y mantiene el enlace entre los dispositivos*, sin embargo para recibir requiere de otros protocolos de transporte, como en este caso el *TCP/IP*, *el cual opera en las capas de transporte de datos (TCP, segmenta los datos que se van a compartir, transmite y verifica la correcta recepción) y de red (IP; determina la mejor ruta para enviar los paquetes por la red*, se encarga de que los datos transmitidos salgan y lleguen al destino, con un enrutamiento lógico).

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

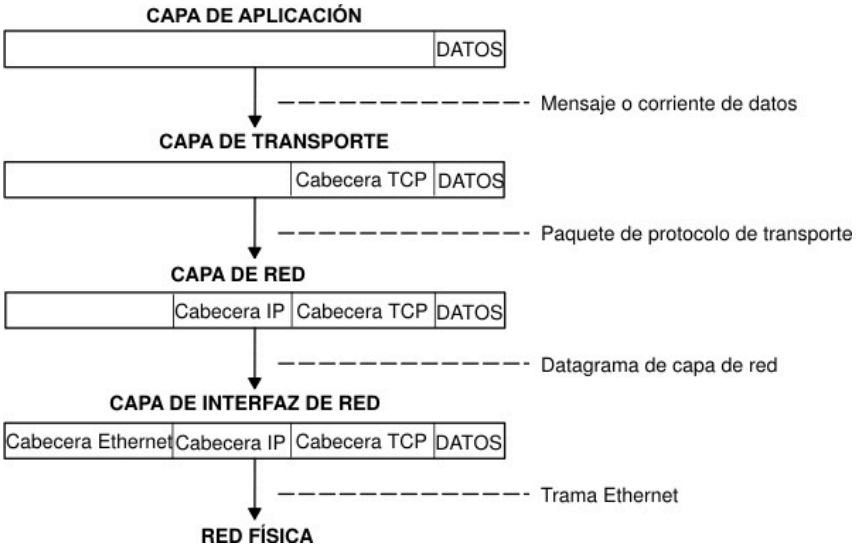
Un paquete de datos en TCP/IP *se compone de varias capas que se corresponden con los niveles del modelo OSI*. El paquete incluye una combinación de encabezados (headers) que contienen la información de control necesaria para la transmisión de datos, así como el propio segmento de datos.

Se compone de las siguientes secciones:

Encabezado de Capa de Interfaz de Red (Enlace de Datos)

Este encabezado depende de la tecnología de red utilizada, incluye:

- Dirección MAC de destino: Identifica el dispositivo de destino en la red local.
- Dirección MAC de origen: Identifica el dispositivo que envía el paquete en la red local.
- Tipo de protocolo: Indica el protocolo de nivel superior, generalmente IP.



Encabezado IP (Capa de Red)

Contiene la información necesaria para enrutar el paquete a través de la red, algunos campos importantes incluyen:

- Versión: Indica la versión del protocolo IP (IPv4 o IPv6).
- Longitud del encabezado: Define el tamaño del encabezado IP.
- Dirección IP de origen: La dirección IP del dispositivo que envía el paquete.
- Dirección IP de destino: La dirección IP del dispositivo al que se envía el paquete.
- Tiempo de vida (TTL): Un contador que indica cuántos saltos de red puede hacer el paquete antes de descartarlo.
- Protocolo: Indica el protocolo de nivel superior que se encuentra en el segmento de datos (por ejemplo, TCP, UDP).

Encabezado TCP (Capa de Transporte)

Este contiene información que asegura una comunicación fiable y ordenada entre dos dispositivos, algunos campos clave son:

- Puerto de origen: El puerto desde el cual se envía el paquete en el dispositivo de origen.
- Puerto de destino: El puerto al cual se envía el paquete en el dispositivo de destino.
- Número de secuencia: Un número que ayuda a ensamblar los datos en el orden correcto.
- Número de acuse de recibo (ACK): Utilizado para confirmar la recepción de datos.
- Longitud del encabezado: Indica el tamaño del encabezado TCP.
- Flags: Bits de control que gestionan la conexión TCP (como SYN, ACK, FIN, etc.).
- Ventana: Define la cantidad de datos que el receptor puede aceptar sin enviar un acuse de recibo.
- Checksum: Usado para verificar la integridad del encabezado y los datos.

Segmento de Datos (Carga Útil)

Finalmente, el segmento de datos contiene la información que realmente se está transmitiendo, como un archivo, un correo electrónico, una página web, etc. Esta es la parte del paquete que será entregada a la aplicación en el dispositivo de destino.

Flag

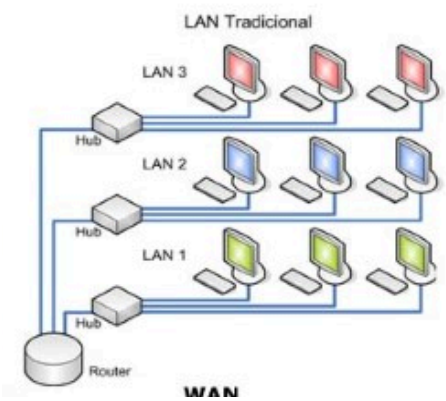
Un **"flag"** es un bit en el encabezado (header) de un paquete TCP que se utiliza para controlar o indicar el estado de la conexión y la transmisión de datos entre dos dispositivos en una red. Cada "flag" tiene un propósito específico y puede activar diferentes acciones en la comunicación entre el emisor y el receptor.

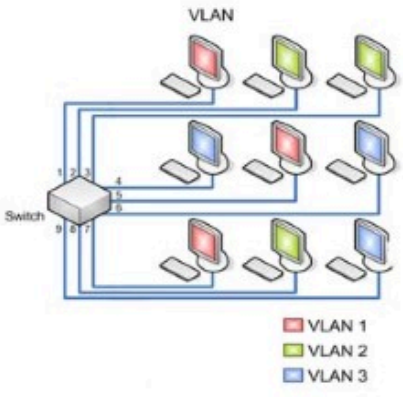
- URG (Urgent): Indica que el contenido del paquete debe ser procesado con prioridad.
- ACK (Acknowledgment): Confirma la recepción de datos por parte del receptor.
- PSH (Push): Solicita al receptor que procese los datos recibidos de inmediato, sin esperar a que se llenen los buffers. Es útil para enviar datos en tiempo real, como teclas presionadas o paquetes de chat.
- RST (Reset): Reinicia la conexión. Este flag se utiliza para cerrar una conexión abruptamente cuando se detecta un error o una condición inesperada.
- SYN (Synchronize): Se utiliza para iniciar una conexión TCP entre dos dispositivos. El flag SYN se establece en el primer paquete enviado durante el proceso de establecimiento de la conexión.
- FIN (Finish): Indica que el remitente ha terminado de enviar datos y desea cerrar la conexión TCP. Se utiliza en el proceso de terminación de la conexión.

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

Personal Area Networks (PAN) o red de área personal

Intercambio de datos *mediante cable* y adoptará la forma de una *Personal Area Network (PAN)* o red de área personal, aunque las técnicas de transmisión más habituales son la *memoria USB* o el conector FireWire. La variante inalámbrica *Wireless Personal Area Network (WPAN)* se basa en técnicas como *Bluetooth, Wireless USB*, Insteon, IrDA, ZigBee o Z-Wave.





Local Area Networks (LAN) o red de área local

Si una red está formada por más de un ordenador, esta recibe el nombre de *Local Area Network (LAN)*. Una red local de tales características puede incluir a dos ordenadores en una vivienda privada o a varios miles de dispositivos en una empresa.

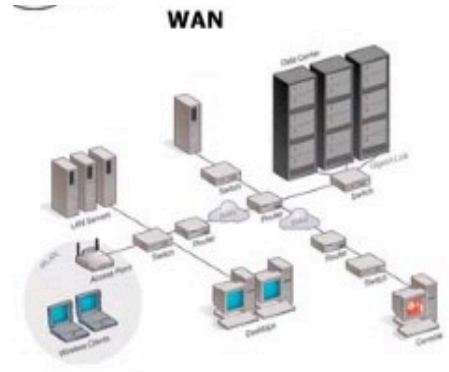
Asimismo, las redes en instituciones públicas como administraciones, colegios o universidades también son redes LAN. Un estándar muy frecuente para redes de área local por *cable es Ethernet.*

Si la red local tiene lugar de manera inalámbrica, se puede hablar en este caso de una *Wireless Local Area Network (WLAN)* o red de área local inalámbrica y los fundamentos básicos de los estándares de la red WLAN quedan definidos por la familia de normas IEEE 802.11. Las redes locales inalámbricas ofrecen la posibilidad de integrar terminales cómodamente en una red doméstica o empresarial y son compatibles con redes LAN Ethernet, aunque el rendimiento es, en este caso, algo menor que el de una conexión Ethernet. Ejemplo: Una red en una oficina corporativa que conecta computadoras e impresoras.

Metropolitan Area Networks (MAN) o red de área metropolitana

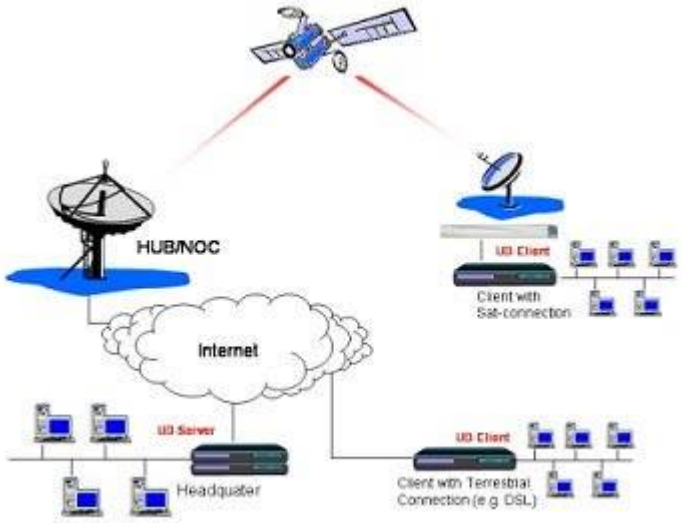
La *Metropolitan Area Network (MAN)* o red de área metropolitana es una *red de telecomunicaciones de banda ancha que comunica varias redes LAN en una zona geográficamente cercana*. Por lo general, se trata de cada una de las sedes de una empresa que se agrupan en una MAN por medio de líneas arrendadas. Para ello, entran en acción routers de alto rendimiento basados en fibra de vidrio, los cuales permiten un rendimiento mayor al de Internet y la velocidad de transmisión entre dos puntos de unión distantes es comparable a la comunicación que tiene lugar en una red LAN. Ejemplo: Una red que conecta varias oficinas de una empresa en una ciudad.

Wide Area Networks (WAN) o red de área amplia



Las *Wide Area Networks (WAN)* o redes de área amplia se extienden por zonas geográficas como países o continentes. El número de redes locales o terminales individuales que forman parte de una WAN es, en principio, ilimitado.
En la mayoría de los casos, las Wide Area Networks suelen pertenecer a una organización determinada o a una empresa y se gestionan o alquilan de manera privada. Los proveedores de servicios de Internet también hacen uso de este tipo de redes para conectar las redes corporativas locales y a los consumidores a Internet. Ejemplo: La red que conecta las sucursales de una empresa a nivel nacional o internacional.

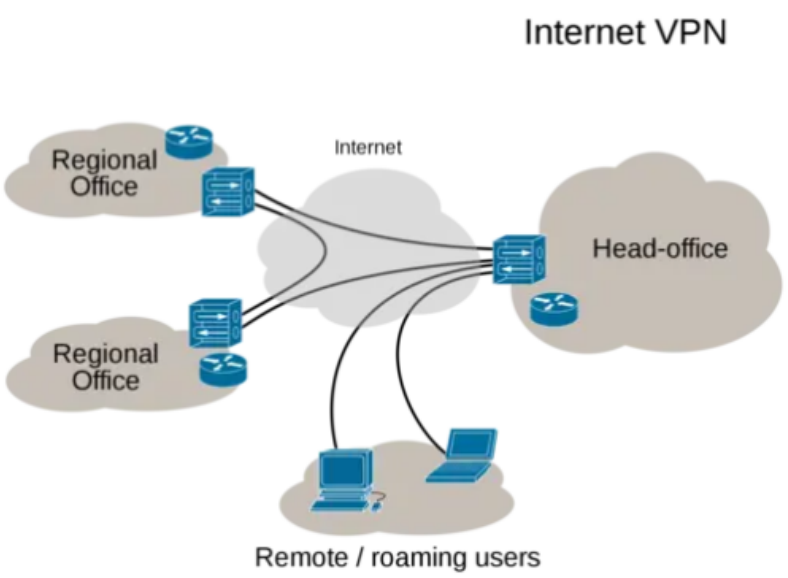
Global Area Networks (GAN) o red de área global



Una red global como Internet recibe el nombre de *Global Area Network (GAN)*, sin embargo no es la única red de ordenadores de esta índole. Las empresas que también son activas a nivel internacional mantienen redes aisladas que comprenden varias redes WAN y que logran, así, la comunicación entre los ordenadores de las empresas a nivel mundial. Las redes GAN utilizan la infraestructura de fibra de vidrio de las redes de área amplia (Wide Area Networks) y las agrupan mediante cables submarinos internacionales o transmisión por satélite. Ejemplo: La red que conecta a todos los usuarios de Internet en todo el mundo.

Virtual Private Network (VPN) o red privada virtual

Una *red privada virtual (VPN)* es una red de comunicación virtual que utiliza la infraestructura de una red física para asociar sistemas informáticos de manera lógica. Lo más común es utilizar Internet como medio de



transporte, ya que este permite establecer la conexión entre todos los ordenadores a nivel mundial, la transferencia de datos tiene lugar dentro de un túnel virtual erigido entre un cliente VPN y un servidor VPN. Si se utiliza la red pública como medio de transporte, las Virtual Private Networks o redes privadas virtuales suelen cifrarse para garantizar la confidencialidad de los datos. Las VPN se emplean para conectar redes LAN en Internet o para hacer posible el acceso remoto a una red o a un único ordenador a través de la conexión pública.

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

Una red según su topología se refiere a la disposición física o lógica de los nodos (dispositivos) que la componen. La topología de red define cómo están conectados los dispositivos y cómo circulan los datos entre ellos. Existen dos tipos principales:

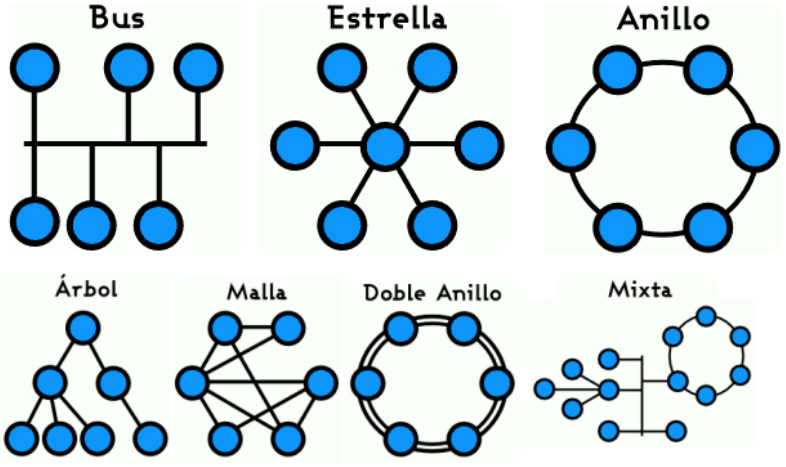
a) Topología física: Es la disposición concreta del cableado y los dispositivos en la red. Describe cómo están interconectados físicamente los nodos.

b) Topología lógica: Se refiere a la forma en que los datos fluyen a través de la red, independientemente de la disposición física de los dispositivos.

Tipología de Redes:

- Bus: Todos los nodos están conectados a un único cable central (bus). Los datos son transmitidos por este cable y recibidos por todos los nodos. Su ventaja es que es simple y tiene un coste reducido. Su desventaja es que la red puede ralentizarse con el aumento de dispositivos, y un fallo en el cable puede afectar a toda la red.
- Estrella: Todos los nodos están conectados a un nodo central que actúa como un intermediario para la comunicación. Su ventaja es la facilidad de gestión y el aislamiento de fallos. Su desventaja es que el fallo del dispositivo central afecta a toda la red.
- Mixta: Combina varias topologías, aprovechando las ventajas de cada una. Su ventaja es su flexibilidad para adaptar la red a necesidades específicas. Su desventaja es que puede ser compleja de diseñar y gestionar.
- Doble Anillo: Es una variante del anillo en la que se utilizan dos anillos en lugar de uno. Normalmente, los datos circulan en direcciones opuestas en cada anillo. Su ventaja es que es ordenada y predecible en términos de tráfico. Su desventaja es que un fallo en un único dispositivo o cable puede interrumpir toda la red.
- Árbol: Combina características de la estrella y bus, formando una estructura jerárquica.
- Malla: Cada nodo se conecta a varios otros, proporcionando múltiples caminos para los datos. Su ventaja es que tiene alta tolerancia a fallos y rendimiento. Su desventaja es que es costosa, compleja de instalar y mantener.

- Totalmente Conexa: Cada nodo está conectado directamente a todos los demás nodos de la red. Esto proporciona la máxima redundancia, ya que hay múltiples caminos para que los datos lleguen a su destino.



10- Explicar el servicio de DHCP.

El servicio DHCP (Protocolo de Configuración Dinámica de Host) es un *protocolo de red que opera bajo una arquitectura cliente-servidor y se encarga de asignar automáticamente direcciones IP y otros parámetros de red a los dispositivos* que se conectan a la red.

Funcionamiento Básico

1. Asignación de direcciones IP: Cuando un dispositivo se conecta a la red, el servidor DHCP le asigna dinámicamente una dirección IP. Esta asignación puede ser de tres tipos:
    - Manual o estática: Se asigna una IP específica a un dispositivo basado en su dirección MAC, que no cambia.
    - Dinámica: Las IPs se asignan y reutilizan de manera temporal según la disponibilidad.
    - Automática: Se asigna una IP disponible que el dispositivo mantendrá hasta que sea liberada.
2. Gestión de IPs: El servidor DHCP mantiene un registro de las direcciones IP asignadas, vinculandolas a las direcciones MAC correspondientes para evitar conflictos (es decir, que dos dispositivos tengan la misma IP).
3. Asignación de parámetros adicionales: Además de la dirección IP, el servidor DHCP también puede proporcionar otros parámetros de configuración, como servidores DNS, puerta de enlace, MTU, y más.

Características Importantes

1. Renovación de IPs: Las direcciones IP asignadas tienen un tiempo de vigencia, tras el cual se pueden reasignar a otros dispositivos si el original ya no las utiliza.
2. APIPA (Automatic Private Internet Protocol Addressing): Si un dispositivo Windows no puede obtener una IP mediante DHCP, se le asigna automáticamente una IP de un rango específico (169.254.x.x) para permitir la comunicación local en la red.

11- Explicar el servicio de DNS.

El Domain Name System (DNS) es un *protocolo de Internet que se encarga de la resolución de nombres de dominio*, es decir, traduce los nombres de dominio en direcciones IP. Cada dominio tiene asignados uno o

más servidores DNS (Nameservers) que permiten convertir el nombre de dominio en la dirección IP correspondiente. Estos servidores DNS suelen tener nombres que se componen de varias partes, como "ns1.ejemplo.com".

Por ejemplo, al escribir “*google.com*” en el navegador, el sistema DNS traduce este nombre de dominio en la dirección IP del servidor donde está alojado el sitio web. Esta traducción es necesaria porque los nombres de dominio son más fáciles de recordar para los humanos, mientras que las direcciones IP son lo que realmente utilizan los dispositivos en la red para localizar y acceder a los sitios web.

Sin el servicio DNS, se tendría que recordar las direcciones IP exactas de los sitios web, lo cual sería mucho más complicado que recordar nombres como “*google.com*”.

12- Explicar las tecnologías Wireless, y sus estándares.

Wireless es un término utilizado para definir la *transmisión de datos entre una variedad de dispositivos, sin conexiones por cables, es decir, de forma inalámbrica, a través de ondas electromagnéticas*.

Este tipo de transmisión de datos se realiza utilizando diferentes tipos de antenas que suelen ser piezas muy pequeñas que se encuentran integradas dentro del hardware de los dispositivos, y son indispensables para recibir un rango específico de espectro de radiación electromagnética. Las redes inalámbricas eliminan la necesidad de disponer de un cableado para conectar diversos equipos.

Wireless sirve eficientemente para transmitir datos entre dispositivos de una forma cómoda y práctica, abaratando costes en mantenimiento y equipos, así mismo, su aplicación se traduce en una optimización del tiempo y los recursos.

Cualquier ordenador y dispositivo móvil utilizan esta tecnología para la trasmisión de datos, siendo indispensable distintos puntos de conexión denominados puertos

El funcionamiento de Wireless se realiza por medio de tres ondas principales de transmisión.

- *Microondas terrestres*: funciona con una frecuencia de 1 a 300 GHz abarcando grandes extensiones terrestres.
- *Microondas satelitales*: permite conectar varias estaciones terrestres, pero es necesario que la señal haya ascendido previamente al satélite.
- *Infrarrojo*: funciona con frecuencias que oscilan entre los 300 GHz hasta los 385THz, son poco comunes, debido a que presentan problemas de señal con los obstáculos.

Estándares

Los estándares WiFi son especificaciones técnicas que aseguran la compatibilidad y el correcto funcionamiento de dispositivos en redes inalámbricas. Los principales estándares son:

- IEEE 802.11 (1997): El estándar original, soporta velocidades de hasta 2 Mbps en frecuencias de 2.4 GHz y 5 GHz.
- IEEE 802.11a (1999): Utiliza 5 GHz y ofrece hasta 54 Mbps, pero no es compatible con 802.11.
- IEEE 802.11b (1999): Usa 2.4 GHz, es compatible con 802.11, y ofrece hasta 11 Mbps.
- IEEE 802.11g (2003): También en 2.4 GHz, ofrece hasta 54 Mbps, compatible con 802.11.
- IEEE 802.11n (2009): Opera en 2.4 GHz y 5 GHz, ofrece hasta 600 Mbps, compatible con versiones anteriores.

- IEEE 802.11ac (2013): En 5 GHz, soporta hasta 6.9 Gbps, compatible con 802.11n.
- IEEE 802.11ax (Wi-Fi 6, 2019): Utiliza 2.4 GHz y 5 GHz, ofrece hasta 10 Gbps, con mejoras en eficiencia y capacidad de dispositivos conectados.

13- ¿Qué es un Proxy?

Un proxy es un *servidor que actúa como intermediario entre un dispositivo (como tu ordenador) e Internet*. Cuando se utiliza un proxy, todas las solicitudes de acceso a sitios web pasan primero por el proxy, que luego las envía al destino final. Esto impide la comunicación directa entre tu dispositivo e Internet, lo que puede ayudar a proteger la privacidad al ocultar la dirección IP.

Además de ocultar la IP, los proxys pueden controlar el acceso a sitios web, filtrar contenido, y almacenar en caché páginas visitadas para acelerar el acceso futuro. Existen diferentes tipos de proxys, como el proxy web, que gestiona el tráfico HTTP y HTTPS; el proxy caché, que almacena contenido web para acelerar futuras visitas; el proxy inverso, que protege servidores específicos al filtrar el tráfico entrante; el proxy transparente, que no requiere configuración previa; y el proxy NAT, que oculta la IP del usuario.

14- Explicar el protocolo Spanning tree.

El STP, definido por el *estándar IEEE 802.1d es un protocolo que funciona en el nivel de la capa 2 del modelo OSI y su principal objetivo es controlar los enlaces redundantes, asegurando el rendimiento de una red.*

En términos generales, es un protocolo de red que se utiliza para evitar los bucles de red que pueden ser creados por “enlaces redundantes” en una red de computadoras. Los bucles son perjudiciales para la red y pueden llevar a la propagación sin fin de los paquetes de datos, congestionando y degradando severamente el rendimiento de la red.

El STP trabaja creando una topología de árbol, un “árbol de expansión“, que abarca todos los switches en una red. Este árbol es usado para determinar un camino sin bucles en la red.

La idea es asegurarse de que solo haya un camino activo entre dos nodos de la red. Para hacer esto, STP asigna roles (raíz, designado y bloqueado) a todos los puertos en la red. Estos roles son los siguientes:

- *Puerto raíz:* Este es el puerto que tiene el mejor camino (costo más bajo) desde el switch hasta la raíz.
- *Puerto designado*: Este es el puerto que tiene el mejor camino desde la red hasta la raíz.
- *Puerto bloqueado*: Este puerto no se utiliza en la topología actual. Es un puerto redundante y está en espera en caso de que se produzca una falla en otros puertos.

Los roles se determinan según varios criterios, que incluyen el ID de puente, el ID de puerto y el costo del camino al puente raíz.

El puente raíz es un switch específico seleccionado por el STP para ser la referencia de la red. Este puente es seleccionado según su ID de puente, que incluye un valor de prioridad y la dirección MAC del switch. El switch con el ID de puente más bajo se convierte en el puente raíz. En caso de un empate en la prioridad, se utiliza la dirección MAC para desempatar (la MAC más baja gana).

El proceso de STP se puede resumir en cuatro pasos:

1. Elección del puente raíz
   El proceso comienza con la elección del puente raíz (root bridge), que es esencialmente el switch que actúa como punto de referencia en la red. Todos los caminos en la topología de la red comienzan desde este switch.

2. Selección del puerto raíz
   Después de que se ha elegido el puente raíz, cada switch (que no es el puente raíz) selecciona su puerto raíz, que es el puerto con el menor costo de ruta al puente raíz.
   El costo de ruta se calcula en función de la velocidad de transmisión del enlace. Un enlace más rápido tiene un costo más bajo.

3. Selección del puerto designado
   A continuación, cada segmento de red (dominio de colisión) selecciona un puerto designado. Este es el puerto con el menor costo de ruta desde el segmento de red hasta el puente raíz.
   El switch que tiene este puerto designado se denomina switch designado.

4. Bloqueo de otros puertos
   Todos los demás puertos que no son puertos raíz o designados se bloquean. Se les asigna un estado de bloqueo y no participan en el reenvío de tramas, lo que evita la formación de bucles.

5. Propagación de la información del puente (Bridge Protocol Data Units, BPDUs)
   Los BPDUs se utilizan para intercambiar información entre los switches. Los BPDUs se envían periódicamente (por defecto, cada 2 segundos) desde el puente raíz y los switches designados a todos los otros switches en la red.

6. Cambios en la topología de la red
   Si ocurre un cambio en la topología de la red (por ejemplo, si un enlace falla o se agrega un nuevo switch), el STP recalcula los caminos y puede cambiar el estado de los puertos (bloqueado a designado o raíz, o viceversa) para asegurarse de que no se formen bucles en la nueva topología.

Estos pasos aseguran que se mantenga un árbol de expansión sin bucles en la red y permiten a la red recuperarse de los cambios en la topología.

Variante STP	Descripción	Escenario de uso	Ventajas	Desventajas
STP (IEEE 802.1D)	El original, diseñado para prevenir bucles en la red.	Ideal para redes pequeñas y simples, donde la velocidad de convergencia no es crítica.	Previene bucles de red de manera efectiva.	Tiempo de convergencia lento. Solo permite un camino activo, lo que puede limitar el ancho de banda.
RSTP (IEEE 802.1w)	Mejora de STP con tiempos de convergencia más rápidos.	Adecuado para redes más grandes donde es importante la rapidez en la recuperación de la conectividad tras una interrupción.	Tiempos de convergencia más rápidos en comparación con STP. Mantiene las ventajas de STP.	Aunque es más rápido que STP, aún puede no ser suficientemente rápido para algunas aplicaciones.
MSTP (IEEE 802.1s)	Permite múltiples árboles de expansión, facilitando el balanceo de carga y la adaptación a varias	Óptimo para redes grandes con múltiples VLANs y donde se necesita un balanceo de carga eficaz.	Permite múltiples instancias de STP, lo que puede mejorar el balanceo de carga y el uso del ancho de banda.	Más complejo de configurar y administrar debido a las múltiples instancias de STP.

	configuraciones de red.			
PVST	Variante de Cisco que utiliza un árbol de expansión separado para cada VLAN.	Ideal para redes que utilizan Cisco y tienen múltiples VLANs que requieren configuraciones STP optimizadas individualmente.	Permite una configuración de STP por VLAN, lo que puede optimizar el rendimiento.	Específico de Cisco, por lo que puede no ser compatible con equipos de otros fabricantes.
PVST+	Mejora la interoperabilidad de PVST con STP estándar.	Adecuado para redes con equipos de múltiples proveedores y donde se requiere la optimización individual de VLANs.	Mejora la interoperabilidad con STP estándar en comparación con PVST.	Aunque mejora la interoperabilidad en comparación con PVST, puede seguir habiendo problemas de compatibilidad.
RPVST+	Combina los beneficios de RSTP y PVST+.	Ideal para redes con múltiples VLANs que requieren tanto una rápida convergencia como la optimización individual de VLANs.	Combina las ventajas de RSTP y PVST+. Permite tiempos de convergencia más rápidos y una configuración STP por VLAN.	Específico de Cisco. Es más complejo de configurar y administrar debido a las características adicionales.

15- Explicar el protocolo de comunicaciones OSPF.

El protocolo OSPF (Open Shortest Path First) es un *protocolo de enrutamiento que se usa en redes IP para determinar cuál es el mejor camino para el envío de los datos*. Funciona recopilando y distribuyendo información de estado de los enlaces (links) de red. Para ello, calcula las rutas más cortas empleando un algoritmo denominado SPF (tambien conocido como algoritmo Dijkstra) y crea tablas de enrutamiento. Estas tablas son las que guían la información y los paquetes a través de la red. Además, este protocolo también cuenta con una serie de paquetes que hay que tener en cuenta ya que se usan para el intercambio de información en la red y para el cálculo de las rutas.

OSPF es un protocolo de estado de link. Se puede pensar en un enlace como en una interfaz en un router. El estado del enlace es una descripción de esa interfaz y de su relación con los routers vecinos. Una descripción de la interfaz incluiría, por ejemplo, la dirección IP de la interfaz, la máscara, el tipo de red a la que se conecta, los routers conectados a esa red y así sucesivamente. La recolección de todos estos estados de link formaría una base de datos de estados de link.

OSPF utiliza el algoritmo de la ruta más corta primero para crear y calcular la ruta más corta hacia todos los destinos. La ruta más corta se calcula con el algoritmo Dijkstra.

Una vista general de los diversos pasos del algoritmo:

1. En la inicialización y debido a cualquier cambio en la información de ruteo, un router genera un anuncio de estado de link. Este anuncio representa la colección de todos los estados de link en ese router.

2. Todos los routers intercambian estados de enlace a través de saturaciones. Cada router que recibe una actualización del estado de enlace debe almacenar una copia en su base de datos de estados de enlace y, luego, propagar la actualización a otros routers.

3. Una vez que la base de datos de cada router está completa, el router calcula un árbol de trayectoria más corta a todos los destinos. El router utiliza el algoritmo Dijkstra para calcular el árbol de la ruta más corta, los destinos, el costo asociado y el siguiente salto para llegar a esos destinos desde la tabla de routing IP.

4. Cuando no ocurren cambios en la red de OSPF, como el costo de un enlace o el agregado o eliminación de una red, OSPF permanece en silencio. Los cambios se comunican a través de paquetes de estado de enlace y el algoritmo Dijkstra se vuelve a calcular para encontrar la ruta más corta.

El algoritmo coloca cada router en la raíz de un árbol y calcula la trayectoria más corta a cada destino basándose en el costo acumulativo necesario para alcanzar ese destino.

Cada router tiene su propia vista de la topología, a pesar de que todos los routers crean un árbol de ruta más corta que usa la misma base de datos de estados de enlace. Estas secciones indican qué comprende la creación de un árbol de ruta más corta.

16- Explicar el protocolo ARP.

El protocolo ARP es una parte integral del conjunto de protocolos de Internet (TCP/IP). Su función principal radica en *mapear direcciones IP a direcciones físicas de hardware, como las direcciones MAC en redes locales*. En términos sencillos, ARP se encarga de encontrar la dirección física asociada a una dirección IP específica.

El protocolo de resolución de direcciones (Address Resolution Protocol, ARP) es un protocolo o procedimiento que conecta una dirección de protocolo de Internet (IP) en constante cambio a una dirección de máquina física fija, también conocida como dirección de control de acceso a medios (media access control, MAC), en una red de área local (local-area network, LAN).

Cuando un dispositivo en una red local necesita comunicarse con otro dispositivo dentro de la misma red, utiliza el protocolo ARP para determinar la dirección física correspondiente a la dirección IP de destino. El proceso implica los siguientes pasos:

1. Solicitud ARP (ARP Request): El dispositivo origen, conocido como host A, envía una solicitud ARP broadcast preguntando quién posee la dirección IP de destino que busca.

2. Respuesta ARP (ARP Reply): El dispositivo destino, host B, que posee la dirección IP buscada, responde directamente a host A con su dirección MAC.

3. Almacenamiento en caché (Caching): Una vez que host A recibe la respuesta, almacena temporalmente la relación entre la dirección IP y la dirección MAC en una tabla de caché ARP. Esto optimiza futuras comunicaciones, ya que no es necesario repetir el proceso completo cada vez que se necesita la información.

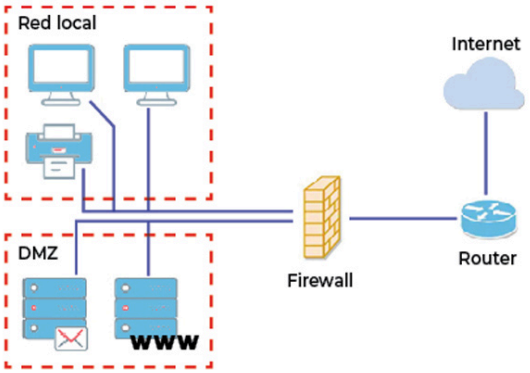
En entornos donde varios dispositivos comparten la misma red, el protocolo ARP se convierte en un componente crítico para el flujo de datos. Cada dispositivo mantiene su propia tabla de caché ARP para optimizar la eficiencia y minimizar la necesidad de realizar solicitudes ARP frecuentes.

17- ¿Qué es un Firewall?

Un firewall es un *sistema de seguridad que supervisa y controla el tráfico de la red según un conjunto de reglas*. Actúa como una barrera entre una red confiable (como la red de una oficina) y una red no confiable (como Internet). Su función principal es decidir si permite o bloquea el tráfico entrante y saliente, protegiendo así la red de amenazas en línea.

Los firewalls pueden ser tanto hardware como software, o una combinación de ambos. Su propósito principal es interceptar el tráfico malicioso antes de que llegue a la red y evitar que la información sensible sensible salga de la misma. Además, pueden filtrar contenido, bloquear sitios web específicos y mantener un registro de las conexiones abiertas para analizar el tráfico con mayor contexto.

18- ¿Qué es una DMZ?



Una zona desmilitarizada (DMZ) es una *red perimetral que protege la red de área local (LAN) interna contra el tráfico no confiable*.

Un significado común para una DMZ es una subred que se encuentra entre la Internet pública y las redes privadas. Expone los servicios externos a redes no confiables y agrega una capa adicional de seguridad para proteger los datos confidenciales almacenados en redes internas, utilizando firewalls para filtrar el tráfico.

El objetivo final de una DMZ es permitir que una organización acceda a redes no confiables, como Internet, a la vez que garantiza que su red privada o LAN permanecen seguras.

Una red DMZ proporciona un búfer entre Internet y la red privada de una organización. La DMZ está aislada por una puerta de enlace de seguridad, como un firewall, que filtra el tráfico entre la DMZ y una LAN. Está protegida por otra puerta de enlace de seguridad que filtra el tráfico entrante de redes externas.

Idealmente se la ubica entre dos firewalls, y la configuración del firewall de la DMZ garantiza que un firewall u otras herramientas de seguridad observen los paquetes de red entrantes antes de que lleguen a los servidores alojados en la DMZ. Esto significa que incluso si un atacante sofisticado puede atravesar el primer firewall, también debe acceder a los servicios reforzados de la DMZ antes de que pueda causarle daño a una empresa.

Si un atacante puede penetrar el firewall externo y poner en peligro a un sistema en la DMZ, también deberá pasar por un firewall interno antes de obtener acceso a datos corporativos confidenciales. Un malhechor altamente calificado puede ser capaz de violar una DMZ segura, pero los recursos que esta contiene deberían activar alarmas que adviertan con mucha antelación que se está cometiendo una infracción.

19- ¿Qué es un Gateway?

Un gateway es un *dispositivo o nodo que actúa como punto de acceso o salida entre dos redes o sistemas que operan utilizando protocolos de comunicación distintos*. Su función primordial reside en la tarea de traducir los datos entre los formatos compatibles con cada una de las redes, posibilitando la fluida transferencia de información entre ellas.

Un gateway incluye tarjetas de interfaz de red (NIC), entradas y salidas (generalmente Ethernet) y software para traducir protocolos de red. Las funciones del gateway también se pueden definir, implementar y controlar mediante software y cada vez más se integran en enrutadores y otros equipos.

Normalmente se utiliza una puerta de enlace en la capa de red del modelo de interconexión de sistemas abiertos (OSI), pero podría implementarse en cualquiera de las capas OSI. Se pueden colocar gateways independientes o virtuales en cualquier lugar de una red donde se necesite traducción. Pueden ser unidireccionales o bidireccionales.

Como punto de entrada o salida de datos, un gateway se puede utilizar en una variedad de procesos de seguridad, como un firewall para escanear y filtrar datos o un servidor proxy para mantener el acceso restringido a ciertas aplicaciones o activos.

20- Según Microsoft, ¿qué significa NBL?

El equilibrio de carga de red (NLB) de Windows Server proporciona *distribución de tráfico mediante TCP o IP y se puede usar con la característica de configuración compartida de IIS (Internet Information Services) para crear una granja de servidores web que proporcione redundancia y tolerancia a errores*. NLB funciona mediante el equilibrio del tráfico entre los nodos de una granja de servidores web o un clúster. Los servidores emiten una señal intermitente a otros hosts del clúster y escuchan la señal de otros hosts. Si se produce un error en un host, los hosts restantes ajustan y redistribuyen la carga de trabajo.

NLB no supervisa el estado de la aplicación. En su lugar, permite al desarrollador de aplicaciones determinar el estado de una aplicación con carga equilibrada. Dado que cada aplicación tiene su propia definición de carga y estado, la mejor manera de medir y supervisar estas cantidades es por medio de la propia aplicación. Mediante el uso de medidas recopiladas de la aplicación y el proveedor de WMI (Windows Management Instrumentation) público de NLB, agregar seguimiento de carga y estado a la aplicación con equilibrio de carga es una tarea relativamente sencilla.

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

a. Enlaces MPLS, LAN to LAN, microonda, VSAT

MPLS

Son las siglas de Multiprotocol Label Switching (conmutación de etiquetas multiprotocolo), una técnica que unifica la transferencia de diferentes tipos de datos a través de una misma red, para superar las limitaciones de velocidad y mejorar el flujo de trabajo de Internet.

Técnica de encaminamiento utilizada en redes de alta velocidad que permite gestionar de manera eficiente los flujos de datos. Los paquetes reciben etiquetas en lugar de ser enrutados de manera tradicional, lo que permite una conmutación más rápida.

Ventajas:

- Mayor eficiencia en el uso del ancho de banda.
- Rutas predefinidas para una mejor calidad de servicio (QoS).
- Reducción de la latencia.

Usos: Es común en redes de proveedores de servicios de telecomunicaciones para interconectar varias sucursales de una empresa, priorizando el tráfico crítico, como voz y video.

LAN to LAN

Es un servicio de transmisión de datos punto a punto basado en protocolo IP. Permite conectar fácilmente dos sedes de un mismo cliente sin necesidad de convertir protocolos o medios, tiene la posibilidad de integrar sedes remotas de un cliente a muy bajo costo.

Este tipo de enlace conecta dos redes locales (Local Area Networks, LAN) ubicadas en diferentes lugares a través de una red externa, como una red privada o Internet. Se utiliza para extender la conectividad entre dos ubicaciones geográficamente dispersas.

Ventajas:

- Conectividad segura y eficiente entre sedes remotas.
- Fácil administración si se implementa con VPN (Virtual Private Network).

Usos: Conectar oficinas o sucursales que están en diferentes ubicaciones geográficas, asegurando que puedan compartir recursos de red como si estuvieran en la misma ubicación física.

Microonda

Enlace que funciona a través de la transmisión de datos o voz por medio de radiofrecuencias con longitudes de onda en la región de frecuencias de microondas. Para este fin son utilizadas un par de antenas, una del lado del cliente, que deberá ser alineada a otra antena del lado del proveedor. Puede ser analógico o digital y la conexión de estos terminales pueden ser punto a punto o punto multipunto.

Ventajas:

- Rápida implementación, ya que no requiere cables físicos.
- Útil en áreas rurales o lugares donde es difícil instalar cables.

Usos: Se utiliza comúnmente en telecomunicaciones, transmisión de datos entre torres, estaciones base de telefonía móvil y en situaciones donde el tendido de cables no es viable.

VSAT

La tecnología satelital VSAT, usa un tipo de antena que recibe y transmite datos y que por su sigla en inglés significa Terminal de Apertura Muy Pequeña. Esta antena consta de pequeños terminales que se pueden instalar en sitios dispersos y conectarse a un Hub central gracias a un satélite.

Es una tecnología de comunicación satelital que utiliza antenas parabólicas pequeñas para transmitir y recibir datos de un satélite en órbita geoestacionaria.

Ventajas:

- Cobertura global, incluyendo áreas remotas.
- Independencia de la infraestructura terrestre.

Usos: Ideal para ubicaciones remotas o rurales sin acceso a redes terrestres, como en barcos, minería, petróleo, o lugares de difícil acceso. También se utiliza para garantizar comunicaciones de respaldo.

b. Dos tipos de enlaces no mencionados anteriormente

Fibra Óptica

Los enlaces de fibra óptica utilizan hilos de vidrio o plástico para transmitir datos en forma de pulsos de luz. La fibra óptica es extremadamente rápida y tiene una gran capacidad para transmitir grandes cantidades de datos a largas distancias con muy baja atenuación.

Ventajas:

- Alta velocidad de transmisión de datos (hasta varios terabits por segundo).
- Baja latencia y menor interferencia electromagnética.
- Capacidad para cubrir largas distancias sin degradación significativa de la señal.

Usos: Se utiliza en redes troncales de telecomunicaciones, conexiones a Internet de alta velocidad, redes de proveedores de servicios (ISP), y en infraestructuras de redes metropolitanas (MAN) y redes locales de gran tamaño (LAN).

LTE (Long Term Evolution)

Es una tecnología de comunicación móvil de banda ancha que permite la transmisión de datos a alta velocidad a través de redes celulares. Es ampliamente utilizada en redes 4G y 5G.

Ventajas:

- Conexión rápida a Internet sin necesidad de cables.
- Cobertura amplia a través de redes móviles.
- Facilidad de despliegue para usuarios móviles o en áreas rurales donde la infraestructura de fibra o cable no está disponible.

Usos: Conexiones móviles a Internet, puntos de acceso inalámbricos en áreas sin infraestructura terrestre, conexiones de respaldo en empresas, y en soluciones de Internet fijo en zonas donde no llega la fibra óptica.

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.

Económico		Performance (Rendimiento)	
1	LAN to LAN (con VPN)	**1**	Fibra óptica
2	Microonda	**2**	MPLS
3	LTE	**3**	LAN to LAN
4	VSAT	**4**	Microonda
5	MPLS	**5**	LTE
6	Fibra óptica	**6**	VSAT
Los enlaces de LAN to LAN y microondas son generalmente más económicos porque requieren menos infraestructura costosa. LTE es relativamente accesible, mientras que los enlaces de fibra óptica y MPLS son más caros debido a su infraestructura especializada. VSAT tiene costos elevados debido a la tecnología satelital.		La fibra óptica y MPLS ofrecen el mejor rendimiento en términos de velocidad y fiabilidad. LAN to LAN también puede ser muy eficiente, mientras que LTE y VSAT tienden a ser más lentos, con latencias más altas.	

Mayor Capacidad (Ancho de Banda)		Mayor o Mejor Configuración de Restricciones (QoS y Control de Tráfico)	
1	Fibra óptica	**1**	MPLS
2	MPLS	**2**	Fibra óptica
3	LAN to LAN	**3**	LAN to LAN (VPN)
4	Microonda	**4**	LTE
5	LTE	**5**	Microonda
6	VSAT	**6**	VSAT
La fibra óptica tiene la mayor capacidad para transmitir datos, seguida de MPLS. Las tecnologías inalámbricas como LTE, microondas y VSAT tienen limitaciones de ancho de banda en comparación.		MPLS se destaca en el control de calidad del servicio (QoS) y las rutas predefinidas. La fibra óptica y LAN to LAN también permiten un buen control, mientras que las opciones inalámbricas tienen menos capacidad para configurar restricciones complejas.	

Soporte a Mayor Distancia		Menor Esfuerzo de Configuración	
1	VSAT	**1**	LTE
2	Fibra óptica	**2**	VSAT
3	Microonda	**3**	Microonda
4	MPLS	**4**	LAN to LAN (VPN)

5	LTE	**5**	Fibra óptica
6	LAN to LAN	**6**	MPLS
VSAT tiene cobertura global debido a los satélites. La fibra óptica puede cubrir distancias muy largas, mientras que las microondas requieren línea de vista. Las redes como MPLS y LTE dependen de la infraestructura de torres o puntos intermedios.		LTE y VSAT son fáciles de configurar, ya que son plug-and-play en su mayoría. Los enlaces de microondas requieren alineación, pero su implementación es más sencilla que la instalación de fibra óptica o la configuración avanzada de MPLS, que puede ser compleja.	

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

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

MPLS es ideal para conectar múltiples sitios como call centers con un data center central, ya que permite un alto nivel de control sobre la calidad del servicio (QoS), garantizando que el tráfico crítico, como voz y datos en tiempo real, sea priorizado. También ofrece baja latencia y alta fiabilidad, lo cual es clave para la continuidad operativa de los call centers.

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

VSAT es la mejor opción para ubicaciones remotas como pozos petroleros, donde no hay acceso a infraestructura terrestre. Dado que los datos solo se necesitan transmitir durante 15 minutos al día, la tecnología satelital puede proporcionar cobertura incluso en áreas inhóspitas. La conectividad por satélite garantiza que se pueda transmitir información sin la necesidad de líneas físicas.

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

Un enlace de *microondas* es adecuado para conectar dos edificios cercanos, ya que se puede implementar rápidamente y no requiere cavar o instalar cables entre los edificios. Si los edificios tienen línea de vista, la transmisión es eficiente y estable, ofreciendo una alternativa económica y rápida a soluciones más complejas como la fibra óptica.

22- Describir la tecnología LTE.

LTE significa "Long Term Evolution" (evolución a largo plazo) y se utiliza más comúnmente en relación con 4G, el estándar de comunicación inalámbrica global de cuarta generación.

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.

LTE es un rediseño del estándar 3G para satisfacer la demanda de transmisión de datos de baja latencia. El rediseño incluye:

- Una red central basada en direcciones IP
- Una arquitectura de red simplificada
- Una nueva interfaz de radio
- Un nuevo método de modulación
- Radios de entrada y salida múltiple (MIMO) para todos los dispositivos

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

Microsoft Teams es una plataforma de colaboración en línea que utiliza las redes de datos como su infraestructura principal para habilitar la comunicación y el trabajo en equipo a través de Internet o redes privadas corporativas.

Características:

1. **Dependencia de las redes para la comunicación**: Microsoft Teams depende de una conexión a la red para permitir la mensajería instantánea, videollamadas, reuniones y la colaboración en tiempo real sobre archivos. Para asegurar que estas funciones sean posibles, Teams utiliza varios elementos de redes, tales como:
    - **Protocolos de comunicación**: Usa TCP/IP para la transferencia de datos y UDP en algunos casos, como en videollamadas para mejorar el rendimiento en la transmisión en tiempo real.
    - **Ancho de banda**: El rendimiento de Teams, especialmente en videollamadas o compartición de archivos, depende del ancho de banda disponible en la red de los usuarios.
2. **Optimización de recursos de red**: Teams gestiona el tráfico de red de manera eficiente mediante tecnologías como:
    - **QoS (Quality of Service)**: Permite priorizar el tráfico crítico como la voz o el video sobre otros tipos de tráfico en la red, lo que es esencial para una buena calidad en las videollamadas y reuniones.
    - **Uso de servidores distribuidos (CDN)**: Para mejorar la velocidad y reducir la latencia, Teams aprovecha redes de distribución de contenido (CDN), lo que permite que los datos y archivos se descarguen desde servidores más cercanos geográficamente a los usuarios.
3. **Seguridad en las redes**:
    - Utiliza **VPN** y otras tecnologías de seguridad para cifrar las comunicaciones y proteger los datos cuando los usuarios acceden desde ubicaciones remotas o redes inseguras.
    - **Cifrado**: Todos los datos transmitidos entre usuarios de Teams están cifrados, lo cual asegura que la información sensible esté protegida a medida que viaja por la red.
4. **Escalabilidad en redes empresariales**: En grandes organizaciones con múltiples oficinas o trabajadores remotos, Teams se conecta a través de redes WAN, MPLS o redes privadas para permitir una comunicación segura y eficiente entre los empleados sin importar dónde se encuentren.

Teams facilita la **comunicación distribuida** en redes complejas, ayudando a conectar a trabajadores en distintas ubicaciones. Resuelve problemas de latencia, conectividad y disponibilidad al aprovechar tecnologías como redes en la nube, distribución geográfica de servidores y calidad de servicio (QoS) para optimizar el uso de la red en la transmisión de datos.

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

MPLS son las siglas de Multiprotocol Label Switching (conmutación de etiquetas multiprotocolo), una *técnica que unifica la transferencia de diferentes tipos de datos a través de una misma red*, para superar las limitaciones de velocidad y mejorar el flujo de trabajo de Internet.

Aplicar calidad en un enlace MPLS significa utilizar las tecnologías y técnicas de QoS disponibles para clasificar, evitar la congestión y gestionar el tráfico de manera que se cumplan los requisitos de rendimiento y se garantice que las aplicaciones críticas operen con la calidad necesaria. Esto se logra mediante el uso de funciones como CAR, WRED y WFQ, que permiten a los administradores de red priorizar y gestionar el tráfico de forma efectiva en una red MPLS.

La funcionalidad CoS en MPLS permite a los administradores de red proporcionar servicios diferenciados en toda la red MPLS, especificando la clase de servicio aplicable a cada paquete IP transmitido. Esto se logra

estableciendo diferentes clases de servicio mediante la configuración del bit de precedencia IP en el encabezado de cada paquete.

Servicios Diferenciados en MPLS:

- Clasificación de Paquetes (Packet Classification): Utilizando CAR, los paquetes se clasifican en el borde de la red antes de que se asignen etiquetas. Esto permite controlar el tráfico que entra o sale de la red, asegurando que se gestione adecuadamente según sus requisitos de transmisión.
- Evitación de Congestión (Congestion Avoidance): WRED se utiliza para anticipar y prevenir la congestión en la red, descartando selectivamente el tráfico de menor prioridad cuando una interfaz se congestiona. Esto ayuda a mantener el rendimiento de la red al evitar la saturación de la misma.
- Gestión de Congestión (Congestion Management): WFQ asegura una asignación justa del ancho de banda a todo el tráfico de la red, utilizando pesos (prioridades) para determinar cuánta banda ancha se asigna a cada clase de tráfico. Esto es esencial para mantener la eficiencia y la equidad en la red.

MPLS, CoS y QoS en Dispositivos MPLS:

La funcionalidad CoS en MPLS permite replicar lo más fielmente posible las características de CoS de IP (Capa 3) en dispositivos MPLS, asegurando que las funciones de QoS sean consistentes en toda la red.

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

A.Velocidad, ancho de banda y distancia

El cable coaxial y el cable de par trenzado (UTP) son cables de cobre o basados en cobre rodeados de aislamiento con otros materiales Ambos pueden transmitir televisión, teléfono y datos con señales eléctricas. Sin embargo, el cable de fibra óptica puede entregar los mismos tipos de señales con un ancho de banda mucho más amplio, mayor velocidad y frecuencias más altas. Este cable está compuesto por tubos de vidrio o plástico muy finos y flexibles.

Tipo de cable	Velocidad	Máximo ancho de banda	Distancia
Cables de fibra óptica	10/100/1000Mbps, 10/40/100/200Gbps	Fibra multimodo OM5: 3500 MHz·km sobre 850 nm	Hasta 80km
Cable de par trenzado	Hasta 10Gbps	Cat 8 2000MHz	Hasta 100m
Cable coaxial	—	750MHz (defecto)	Hasta 500m

B. Instalación

Aunque el cable de fibra óptica ofrece un gran beneficio en términos de flexibilidad de ancho de banda y fiabilidad, no está tan generalizado como el cable coaxial o el cable de par trenzado. Además, los cables de fibra son frágiles y más delgados que los cables de par trenzado y los cables coaxiales, haciendo así que su instalación, operación y manutención requiera de más cuidados. En comparación con el cable de par trenzado, el cable coaxial puede alcanzar una distancia mayor. Sin embargo, el cable coaxial es difícil de instalar y mantener debido a su aislante dieléctrico alrededor del núcleo de cobre.

C. Aplicación

Los cables de fibra óptica no solo se instalan para soportar conexiones de larga distancia entre ciudades y países, sino también en vecindarios suburbanos para acceso directo como FTTH, FTTP, FTTB, FTTC, etc., lo que se denomina instalaciones de "última milla". Estos cables son ampliamente utilizados en centros de datos donde se necesita transmitir un gran volumen de datos.

Los cables de par trenzado son utilizados principalmente en redes telefónicas, redes de datos y blindaje de cables. Las aplicaciones del cable coaxial incluyen: líneas de alimentación que conectan transmisores y receptores de radio con sus antenas; conexiones de red informática (Internet); audio digital (Formato de Interfaz Digital Sony/Philips, S/PDIF por sus siglas en inglés); distribución de señales de televisión por cable y conexiones de interfaz de medios de alta definición.

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).

Las *certificaciones de Cisco son reconocidas a nivel global para la formación en redes y telecomunicaciones*. A continuación se describen las certificaciones CCENT, CCNA y CCNP:

- **CCENT (Cisco Certified Entry Networking Technician)**: Esta es una certificación de nivel básico que valida habilidades esenciales para instalar, operar y solucionar problemas en redes pequeñas. Es el primer paso hacia certificaciones más avanzadas.
- **CCNA (Cisco Certified Network Associate)**: Esta certificación es de nivel intermedio y cubre habilidades fundamentales en redes, como la instalación, configuración, operación y resolución de problemas en redes de tamaño medio. Prepara a los profesionales para manejar redes con switches y routers, con énfasis en la conectividad WAN (Wide Area Network).
- **CCNP (Cisco Certified Network Professional)**: Es una certificación de nivel avanzado que requiere mayor experiencia y profundiza en redes complejas. Se enfoca en áreas más especializadas como la implementación, configuración y resolución de problemas avanzados de redes LAN (Local Area Network) y WAN.

El **track de Routing & Switching** se centra en la instalación, operación y resolución de problemas de redes empresariales que involucran routers y switches. Los profesionales con esta certificación adquieren conocimientos para configurar redes LAN y WAN, optimizar el tráfico de red, implementar seguridad básica en las redes y gestionar infraestructuras de red.

El **track de Security** se enfoca en proteger infraestructuras de red contra amenazas, incluyendo ataques y vulnerabilidades. Los temas incluyen tecnologías de firewall, VPNs, control de acceso a redes (NAC), y la implementación de políticas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información en las redes empresariales.

27- Explique el modelo OSI.

El modelo de interconexión de sistemas abiertos (Open Systems Interconnection, OSI) es un *marco conceptual que divide las funciones de comunicaciones de red en siete capas.*

El modelo de interconexión de sistemas abiertos (OSI) fue desarrollado por la Organización Internacional de Normalización y otros a fines de la década de 1970. Se publicó en su primera versión en 1984 como ISO 7498 y la versión actual es ISO/IEC 7498-1:1994. A continuación se muestran las siete capas del modelo.

Capa física

La capa física se refiere al *medio de comunicación físico y a las tecnologías para transmitir datos a través de ese medio*. En esencia, la comunicación de datos es la transferencia de señales digitales y electrónicas a través de varios canales físicos, como cables de fibra óptica, cableado de cobre y aire. La capa física incluye estándares para tecnologías y métricas estrechamente relacionadas con los canales, como Bluetooth, NFC y velocidades de transmisión de datos.

Capa de enlace de datos

La capa de enlace de datos se refiere a las *tecnologías utilizadas para conectar dos máquinas a través de una red* donde la capa física ya existe. Gestiona los marcos de datos, que son señales digitales encapsuladas en paquetes de datos. El control del flujo y el control de errores de los datos suelen ser los enfoques clave de la capa de enlace de datos. Ethernet es un ejemplo de un estándar a este nivel. La capa de enlace de datos a menudo se divide en dos subcapas: la capa de control de acceso a los medios (MAC) y la capa de control de enlace lógico (LLC).

Capa de red

La capa de red se ocupa de *conceptos como el enrutamiento, el reenvío y el direccionamiento a través de una red dispersa o de múltiples redes conectadas de nodos o máquinas*. La capa de red también puede gestionar el control de flujo. En Internet, el Protocolo de Internet v4 (IPv4) y el IPv6 se utilizan como protocolos de capa de red principales.

Capa de transporte

El objetivo principal de la capa de transporte es g*arantizar que los paquetes de datos lleguen en el orden correcto, sin pérdidas ni errores, o que se puedan recuperar sin problemas si es necesario*. El control del flujo, junto con el control de errores, suele ser un objetivo en la capa de transporte. En esta capa, los protocolos de uso común incluyen el Protocolo de Control de Transmisión (TCP), un protocolo basado en conexiones casi sin pérdidas y el Protocolo de datagramas de usuario (UDP), un protocolo sin conexiones con pérdidas. TCP se suele utilizar cuando todos los datos deben estar intactos (por ejemplo, cuando se comparten archivos), mientras que UDP se utiliza cuando retener todos los paquetes es menos crítico (por ejemplo, streaming de vídeo).

Capa de sesión

La capa de sesión es responsable de la *coordinación de la red entre dos aplicaciones independientes en una sesión. Una sesión gestiona el inicio y el final de los conflictos de sincronización y conexión* de una aplicación uno a uno. Network File System (NFS) y Server Message Block (SMB) son protocolos de uso común en la capa de sesión.

Capa de presentación

La capa de presentación *se ocupa principalmente de la sintaxis de los datos en sí para que las aplicaciones los envíen y consuman*. Por ejemplo, el lenguaje de marcas de hipertexto (HTML), la notación de objetos

JavaScript (JSON) y los valores separados por comas (CSV) son lenguajes de modelado para describir la estructura de los datos en la capa de presentación.

Capa de aplicación

La capa de aplicación se refiere al *tipo específico de aplicación en sí y a sus métodos de comunicación estandarizados.* Por ejemplo, los navegadores pueden comunicarse mediante el Protocolo seguro de transferencia de hipertexto (HTTPS) y los clientes de correo electrónico y HTTP pueden comunicarse mediante POP3 (Protocolo de oficina de correo versión 3) y SMTP (Protocolo simple de transferencia de correo).

No todos los sistemas que utilizan el modelo OSI implementan todas las capas.

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

María:

Ivana:

Melina:

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

El estándar **IEEE 802.3,** también conocido como **Ethernet**, permite la *transferencia eficiente de datos entre diferentes dispositivos mediante la definición de una interfaz de comunicación estandarizada*. El estándar define la capa física de la arquitectura de red, incluido el cableado, los conectores y los medios de transmisión. Ethernet se basa en el modelo OSI y cubre principalmente las capas 1 y 2. Admite varios tipos y velocidades de cables, desde cables de par trenzado hasta cables de fibra óptica.

Este protocolo Ethernet utiliza un método especial llamado Acceso múltiple con detección de operador con detección de colisiones (CSMA/CD) para garantizar que varios dispositivos puedan acceder a la red simultáneamente sin causar colisiones. Esto significa que cada dispositivo comprueba si la red está libre o no antes de transmitir.

Si dos o más dispositivos intentan acceder a la red al mismo tiempo y se produce una colisión, el protocolo lo detecta mediante un mecanismo llamado detección de colisiones. Cuando se detecta una colisión, ambos dispositivos involucrados detienen inmediatamente sus transmisiones y esperan un breve tiempo antes de volver a intentarlo.

El tamaño máximo del paquete en el protocolo Ethernet suele ser de 1500 bytes más Encabezamiento-Información. Si es necesario enviar paquetes más grandes, se dividen en fragmentos más pequeños y luego se transmiten individualmente.

Ventajas de IEEE 802.3

1. Estándar consolidado: Es uno de los estándares de red más utilizados en el mundo, lo que garantiza una gran interoperabilidad entre dispositivos de diferentes fabricantes.
2. Escalabilidad: Las redes Ethernet basadas en 802.3 pueden escalar desde pequeñas redes domésticas hasta grandes redes empresariales, con velocidades que pueden variar desde 10 Mbps hasta más de 100 Gbps.
3. Bajo costo: La infraestructura Ethernet es relativamente económica, tanto en términos de cableado (UTP) como de dispositivos como switches y tarjetas de red.
4. Fiabilidad: Ethernet es conocido por su alta estabilidad y fiabilidad en entornos de red, lo que lo hace ideal para la mayoría de las aplicaciones empresariales.
5. Compatibilidad con tecnologías modernas: Las versiones recientes de IEEE 802.3 han incorporado soporte para redes virtuales (VLANs), calidad de servicio (QoS), y mayor seguridad, lo que lo convierte en una tecnología robusta y versátil.

Desventajas de IEEE 802.3

1. Limitaciones de distancia: Aunque las velocidades son muy altas, el cableado de cobre Ethernet tiene limitaciones en cuanto a la distancia máxima sin necesidad de repetidores o switches (hasta 100 metros para cables de cobre). Las versiones de fibra óptica superan esta limitación, pero son más costosas.
2. Control de colisiones: Aunque el control de colisiones mediante CSMA/CD era adecuado para redes compartidas, con la introducción de switches (que segmentan la red), esta tecnología se ha vuelto menos eficiente y ha sido prácticamente eliminada en redes modernas.
3. Latencia en redes grandes: Aunque las velocidades de transmisión han aumentado, en redes Ethernet muy grandes la latencia puede ser un problema si no se gestionan adecuadamente los cuellos de botella.
4. Complejidad en entornos muy grandes: A medida que las redes crecen en tamaño y complejidad, la gestión de redes Ethernet puede volverse más desafiante, requiriendo una planificación más cuidadosa para evitar problemas de tráfico, latencia y congestión.

30- Explicar el estándar IEEE 802.4 regula la red.

IEEE 802.4 es un estándar que define la **red Token Bus**, utilizado principalmente en entornos de automatización industrial y en la industria de manufactura. Este estándar se originó a partir del Protocolo de Automatización de Manufactura (MAP), diseñado para *proporcionar comunicaciones confiables y de gran ancho de banda entre máquinas y dispositivos en procesos de producción automatizada.*

En el esquema de Token Bus, las estaciones están conectadas físicamente a un medio compartido, como un cable lineal o en forma de árbol, pero están organizadas lógicamente en un anillo lógico. En este anillo lógico,

cada estación conoce la dirección de la estación a su izquierda y a su derecha, lo que no depende de su disposición física, sino de un orden lógico predefinido.

La comunicación entre las estaciones se realiza mediante el método de token-passing. El token es un mensaje especial que circula entre las estaciones de la red. Solo la estación que tiene el token puede transmitir datos, lo que garantiza que no haya colisiones. Una vez que una estación termina de transmitir, pasa el token a la siguiente estación en el anillo lógico. Si una estación no tiene datos para transmitir, simplemente pasa el token sin transmitir.

Funcionamiento

1. Inicialización del anillo lógico: Al iniciar la red, la estación con el número más alto es la que envía la primera trama. Posteriormente, el token se pasa a su vecino según el anillo lógico.
2. Token-passing: El token viaja de estación en estación, permitiendo que solo una estación a la vez transmita datos. Esto asegura una transmisión ordenada sin colisiones, lo que es crítico en entornos industriales donde la confiabilidad y el tiempo de respuesta son esenciales.
3. Control de acceso: Como solo la estación con el token tiene permiso para transmitir, se elimina la posibilidad de colisiones, que es un problema en otras redes como Ethernet (donde se usa CSMA/CD). Esto garantiza un acceso al medio más eficiente en redes con alta demanda de datos y tiempo real.

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

Protocolo SMTP (Simple Mail Transfer Protocol)

- Función principal: SMTP es un protocolo que se utiliza solo para enviar correos electrónicos, no para recibirlos; se complementa con POP3 o IMAP para descargar los mensajes desde el servidor.
- Uso: SMTP permite que el cliente de correo envíe correos al servidor de correo y también facilita la transmisión de correos entre servidores.
- Limitación: SMTP no está diseñado para la recepción de correos en el cliente de correo del usuario.

Protocolo POP3 (Post Office Protocol 3)

- Función: POP3 es utilizado para recibir y descargar correos electrónicos desde el servidor hacia el cliente de correo del usuario. Normalmente, los correos se eliminan del servidor después de ser descargados.
- Ventaja: Permite la lectura del correo sin conexión, ya que se almacena localmente.
- Desventaja: No sincroniza el correo entre múltiples dispositivos.

Protocolo IMAP (Internet Message Access Protocol)

- Función: IMAP es utilizado también para recibir correos electrónicos, pero a diferencia de POP3, permite que los mensajes permanezcan en el servidor y se sincronicen en múltiples dispositivos.
- Ventaja: Ofrece una mejor sincronización entre dispositivos, permitiendo acceder a los correos desde cualquier lugar sin eliminarlos del servidor.

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

IMAP (Internet Message Access Protocol):

Permite leer correos electrónicos manteniéndolos almacenados en el servidor. IMAP es ideal para usuarios que acceden a su correo desde varios dispositivos (como computadoras, teléfonos y tablets) ya que mantiene los mensajes sincronizados en todos los dispositivos. Es mejor para acceder y leer correos en varios dispositivos, ya que los mensajes se mantienen en el servidor. Los correos permanecen en el servidor, lo que

permite gestionarlos y leerlos desde cualquier lugar con conexión a Internet. Además, se pueden organizar carpetas de manera remota.

Puerto: El puerto estándar es el 143 y el 993 para conexiones seguras (SSL/TLS).

POP3 (Post Office Protocol 3):

OP3 descarga los correos electrónicos desde el servidor al dispositivo del usuario. Después de la descarga, los correos normalmente se eliminan del servidor (aunque esto puede configurarse para mantener una copia).

Ventaja: Una vez descargados, los correos pueden leerse sin conexión a Internet. Este protocolo es adecuado si solo se accede al correo desde un dispositivo.

Puerto: El puerto estándar es el 110 y el 995 para conexiones seguras (SSL).

33- Diferencias entre IPV4 e IPV6

1. Espacio de Direcciones

IPv4 tiene 32 bits (≈4.3 mil millones de direcciones), mientras que IPv6 tiene 128 bits (≈340 undecillones de direcciones).

- IPv4:
  - Tamaño: Utiliza direcciones de 32 bits, lo que permite un total de 2^{32} o 4,294,967,296 direcciones únicas.
  - Agotamiento: Debido al crecimiento explosivo de dispositivos conectados a Internet, el espacio de direcciones IPv4 se agotó, y se han utilizado técnicas como la Traducción de Direcciones de Red (NAT) para extender el uso de las direcciones disponibles.
- IPv6:
  - Tamaño: Utiliza direcciones de 128 bits, proporcionando un espacio de direcciones de 2^{128} o aproximadamente 340 undecillones (340,282,366,920,938,463,463,374,607,431,768,211,456) direcciones únicas.
  - Espacio de direcciones: El espacio es vasto y se considera prácticamente inagotable, lo que elimina la necesidad de NAT y facilita la asignación directa de direcciones a dispositivos.

2. Nomenclatura de Direcciones

IPv4 usa notación decimal punteada, mientras que IPv6 usa notación hexadecimal con dos puntos.

- IPv4:
  - Formato: Las direcciones se representan en formato decimal punteado, con cuatro octetos separados por puntos. Cada octeto es un número de 8 bits (0-255). Ejemplo: `192.168.1.1`
- IPv6:
  - Formato: Las direcciones se representan en formato hexadecimal, con ocho grupos de cuatro dígitos hexadecimales separados por dos puntos. Cada grupo representa 16 bits. Ejemplo: `2600:1400:d:5a3::3bd4`
  - Compresión: Los ceros consecutivos en la dirección IPv6 pueden ser comprimidos usando `::` para simplificar la notación.

3. Tipos de Comunicación

IPv4 usa unicast, broadcast y multicast, mientras que IPv6 usa unicast, multicast y anycast, eliminando el broadcast.

- IPv4:
  Direcciones: Soporta tres tipos principales de direccionamiento:
  - Unicast (uno a uno): Comunicación entre un solo remitente y un solo receptor.

    - Broadcast (uno a todos): Comunicación de un solo remitente a todos los dispositivos en la red.
    - Multicast (uno a muchos): Comunicación de un solo remitente a un grupo específico de receptores.
- IPv6:
  Direcciones: Admite tres tipos de direccionamiento:
    - Unicast (uno a uno): Similar a IPv4, permite la comunicación entre un único remitente y un único receptor.
    - Anycast (uno a varios, el más cercano): Los paquetes se envían a la instancia más cercana (en términos de costo de enrutamiento) dentro de un grupo de direcciones.
    - Multicast (uno a muchos): Similar a IPv4, permite la comunicación a un grupo de receptores.
    - Broadcast: IPv6 no soporta broadcast. En su lugar, se utilizan direcciones multicast y anycast para lograr efectos similares.

34- (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes?

Ejemplos: Acceder y configurar el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configurar una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.

María: No tengo ninguna experiencia.

Ivana: No tengo ninguna experiencia.

Melina: No tengo ninguna experiencia.