**Taller #1 Tópicos Especiales II**

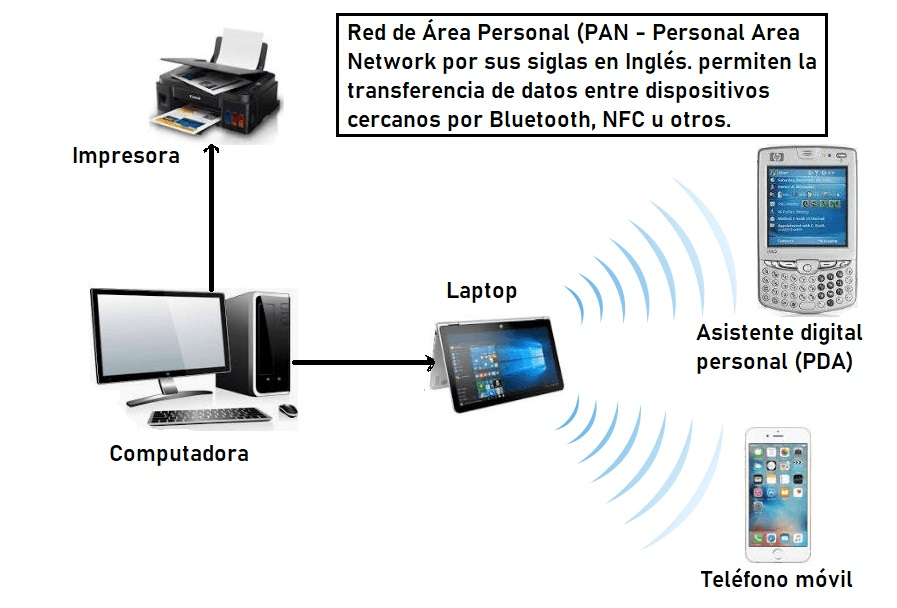
Integrantes: Samantha Abrego

Joy Nelaton

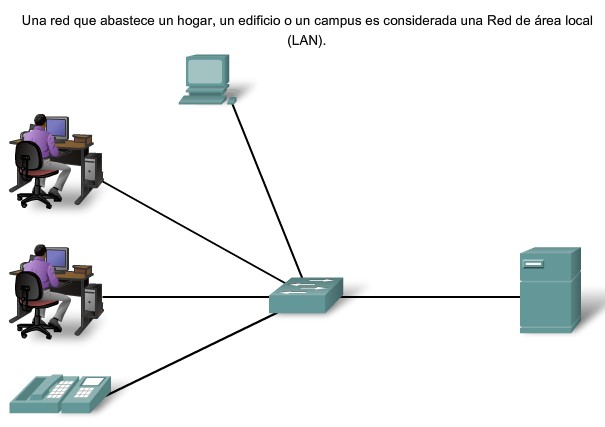
Fecha: 12 de abril del 2024

**I. Diagrame las siguientes topologías. VALOR 10 PUNTOS.**

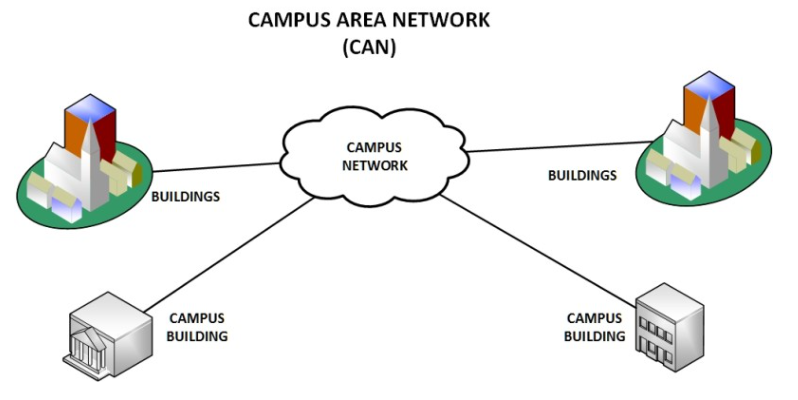
**A). Red de área personal (Personal Área Network, PAN)**



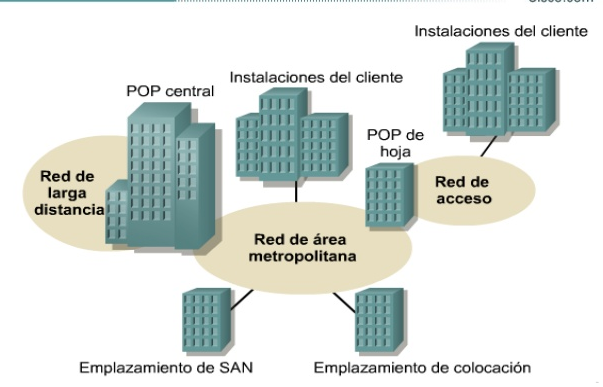
**B). Red de área local (Local Area Network, LAN)**



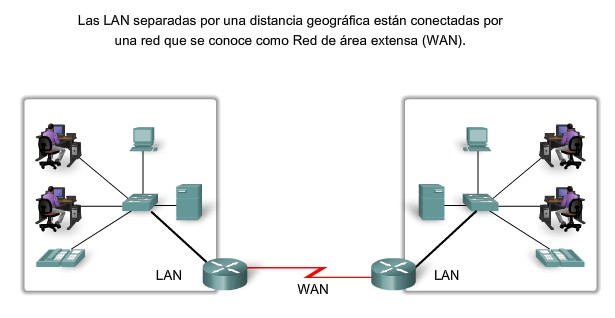
**C). Red de área de campus (Campus Area Network, CAN)**



**D). Red de área metropolitana (Metropolitan Area Network, MAN)**



**E). Red de área amplia (Wide Area Network, WAN)**

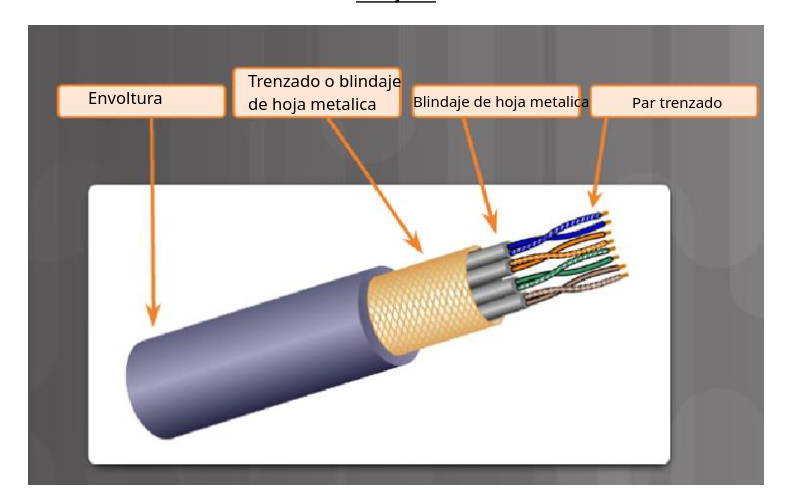


A continuación, la siguiente tabla muestra la cantidad aproximada de usuarios para cada tipo de red, mostrando la variedad en tamaño y cantidad de usuarios que pueden admitir.

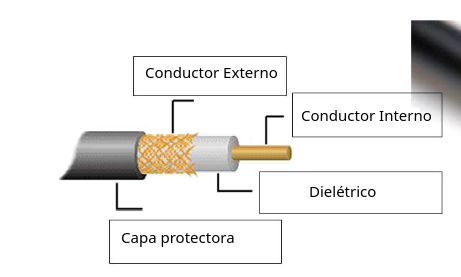
|  |  |  |
| --- | --- | --- |
| **Tipo de Red** | **Ejemplo** | **Número Aproximado de Usuarios** |
| Red PAN | Conexión Bluetooth entre un teléfono y auriculares inalámbricos. | 1-2 |
| Red LAN | Red de área local en una oficina conectando computadoras, impresoras y servidores. | 10-1000 |
| Red MAN | Red que conecta varias redes LAN dentro de una ciudad o área metropolitana. | 100-10000 |
| Red WAN | Internet, conectando dispositivos y redes en diferentes ubicaciones geográficas. | Millones |
| Red CAN | Red de una universidad que conecta todos los edificios dentro del campus. | 1000-10000 |

**II. DE ACUERDO CON EL DIBUJO PRESENTADO. SEÑALE EL NOMBRE CORRECO DEL COMPONENTE QUE LO CONFORMA. 20 PTS**

**Dibujo #1**



**Dibujo #2**

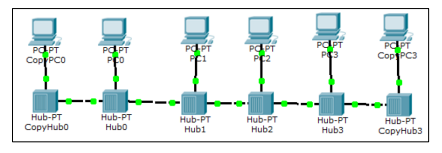


**III. DEFINA LOS SIGUIENTES CONCEPTOS. 55 PTS**

**1. Mencione, defina y diagrame gráficamente los tipos de redes, de acuerdo con su topología física. 30 pts.**

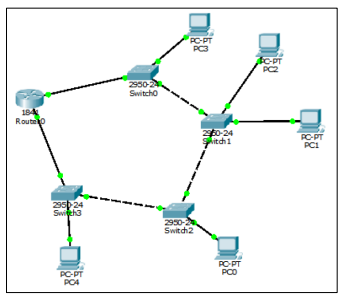
**a. Topología en bus**

La topología bus es un tipo de red en la que todos los dispositivos están conectados a un cable central llamado bus o backbone.



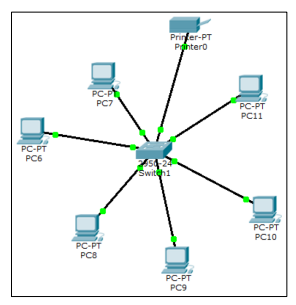
**b. Topología en Anillo**

La topología de red de anillo es cuando todos los dispositivos están conectados en un bucle cerrado, de manera que cada dispositivo está conectado directamente a otros dos dispositivos en cada lado.



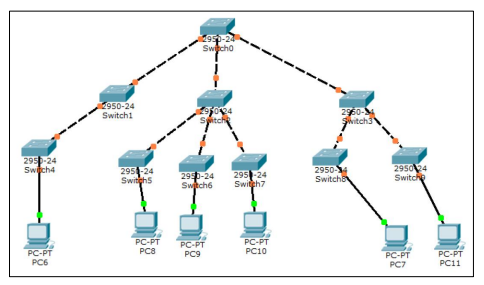
**c. Topología en estrella**

La topología en estrella es un tipo de red donde todos los dispositivos están conectados a un centro llamado hub. Los dispositivos se comunican entre sí a través del hub.



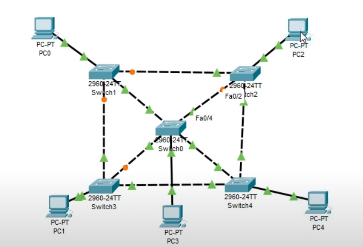
**d. Topología en árbol**

La topología de red bus-star es una combinación de dos tipos de topologías: la estrella y la línea de bus. Se conectan en un bus o línea central y los dispositivos se vinculan a dicho bus mediante una conexión en estrella.



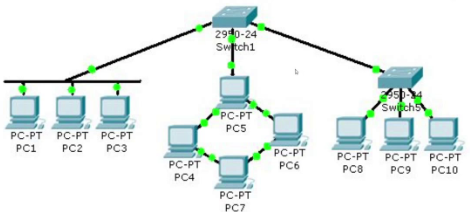
**e. Topología en malla**

La topología en malla es un tipo de conexión de red en la que todos los dispositivos están conectados entre sí para asegurar una conexión constante y directa. Cada dispositivo tiene una conexión con todos los demás en la red.



**f. Topología mixta**

La topología mixta es un tipo de topología de red que utiliza dos o más topologías de red diferentes. Esta topología contiene una combinación de la topología de bus, topología de malla, topología de anillo y topología de estrella.



A continuacion se detalla en la siguiente tabla una comparativa entre las topologías:

|  |  |  |  |
| --- | --- | --- | --- |
| **Topología** | **Descripción** | **Ventajas** | **Desventajas** |
| Bus | Todos los dispositivos en un cable común | Fácil implementación | Vulnerable a fallos y baja escalabilidad |
| Anillo | Dispositivos conectados en un anillo | Bueno para tráfico unidireccional | Fallo de un dispositivo afecta a toda la red |
| Estrella | Todos los dispositivos conectados a un nodo central | Fácil gestión, fallos aislados | Punto único de fallo, costo de infraestructura |
| Árbol | Topología en forma de árbol con múltiples niveles | Escalable, fallos aislados | Complejidad de diseño, costoso |
| Malla | Todos los dispositivos conectados entre sí | Alta fiabilidad, rendimiento alto | Costoso y complejo de implementar y mantener |
| Mixta | Combinación de múltiples topologías | Adaptabilidad a necesidades específicas | Mayor complejidad y coste de mantenimiento |

**2. ¿Diferencia entre la tecnología LIFI y WIFI? 5 pts.**

La principal diferencia entre LiFi y Wi-Fi es el medio de transmisión utilizado: LiFi usa luz visible o infrarroja, mientras que Wi-Fi usa ondas de radio. Esta diferencia fundamental tiene implicaciones importantes en términos de velocidad de transmisión, resistencia a las interferencias, seguridad y alcance, lo que hace que cada tecnología se adapte mejor a diferentes aplicaciones y entornos específicos.

|  |  |  |
| --- | --- | --- |
| **Aspecto** | **LiFi** | **WiFi** |
| Medio de Transmisión | Luz visible o infrarroja | Ondas de radio |
| Velocidad de Transmisión | Potencialmente más alta en ambientes cerrados | Generalmente menor que LiFi en ambientes cerrado |
| Interferencia | Menos susceptible a interferencias | Puede experimentar interferencias |
| Seguridad | Potencialmente más seguro | Vulnerable a ataques de piratería |
| Alcance | Más limitado | Más amplio |

**3. En cuanto a seguridad de redes se refiere ¿Qué son ataques DDOS? Explique**

**con sus palabras. 5 pts.**

Los ataques distribuidos de denegación de servicio (DDoS) son un tipo de ciberataque en el que se utilizan múltiples sistemas informáticos infectados con virus, también conocidos como "bots" o "zombis", para inundar una red con grandes cantidades de tráfico malicioso hacia un objetivo específico.

El objetivo de este ataque es sobrecargar los recursos del sistema objetivo, como servidores web, redes o servicios en línea, haciéndolos no disponibles para usuarios legítimos. Este tipo de ataque puede causar una interrupción significativa de los servicios en línea, lo que afecta negativamente la disponibilidad y el rendimiento de los sistemas afectados.

Los ataques DDoS pueden ser difíciles de mitigar debido a la distribución de los sistemas de ataque y el gran volumen de tráfico generado, lo que puede requerir medidas de seguridad adicionales para combatirlos de manera efectiva.

Un ejemplo típico de un ataque DDoS es cuando un grupo de atacantes coordina una serie de computadoras comprometidas, también conocidas como "botnet", para inundar los servidores de una empresa de comercio electrónico con una cantidad demasiado grande de solicitudes de conexión simultáneas. Esta cantidad de tráfico malicioso mantiene al servidor tan ocupado procesando solicitudes fraudulentas que no puede procesar solicitudes legítimas de clientes reales que intentan visitar el sitio para realizar una compra. Como resultado, el sitio web de la empresa quedó inaccesible durante el ataque, lo que provocó pérdidas financieras y daños a la reputación de la empresa.

**4. ¿Qué es SCANDISK y para qué sirve?, 5 pts.**

En el campo de las redes, Scandisk no es una herramienta especializada para diagnosticar y mantener dispositivos de red. Sin embargo, en entornos que utilizan almacenamiento conectado a la red (NAS) o servidores de archivos compartidos, la integridad del sistema de archivos en el dispositivo de almacenamiento es fundamental para garantizar operaciones de red fluidas.

Se requieren herramientas equivalentes como CHKDSK en Windows o fsck en Unix/Linux para realizar el mantenimiento preventivo y correctivo en los dispositivos de almacenamiento en red. Estas herramientas ayudan a identificar y corregir errores del sistema de archivos, protegiendo así los datos almacenados en la red de posibles errores, al tiempo que garantizan la disponibilidad e integridad de los recursos de almacenamiento de la red para los usuarios y dispositivos conectados.

**5. ¿Explique el concepto de Dominios de Broadcast?, 10 pts**

Los dominios de difusión son áreas de la red donde se envían mensajes de difusión a todos los dispositivos. Pueden ser físicos, limitados por la infraestructura de la red, o lógicos, determinados por la configuración y el enrutamiento de la red. Para evitar la congestión de la red y optimizar el rendimiento, es importante comprender los dominios de transmisión.

Por ejemplo, en una red con múltiples conmutadores interconectados, cada segmento de conmutador es un dominio de transmisión físico, mientras que, en una red con múltiples subredes separadas por enrutadores, cada sub puede ser un dominio de transmisión lógico. Esto ayuda a evitar que los mensajes difundidos se propaguen innecesariamente por la red, mejorando así el rendimiento y la eficiencia generales.