Programación sobre Redes

**Trabajo Práctico Teórico**

**1- ¿Qué es una VLAN?**

Una VLAN (Virtual Local Area Network) es un tipo de red de área local virtual que agrupa dispositivos en una misma red lógica, independientemente de su ubicación física. A través de ella, se puede segmentar una red física en varias redes virtuales.

Entre sus características más importantes podemos encontrar la segregación del tráfico, la mejora de seguridad, la mejora del rendimiento, la flexibilidad y la escalabilidad.

Ejemplo: Crear una VLAN para el departamento de Finanzas, otra para el departamento de RRHH, y otra para la red de visitantes. Así, aunque todos los dispositivos estén conectados al mismo switch, se comportarán como si estuvieran en redes separadas.

**2- Qué es una VPN?**

Una VPN (Virtual Private Network), o Red Privada Virtual, es una tecnología que permite crear una conexión segura y cifrada entre tu dispositivo (como una computadora o un celular) y otra red, generalmente a través de internet. Básicamente, una VPN permite navegar por internet de forma más segura y privada, como si estuvieras en una red local, aunque estés en una ubicación remota.

Entre sus características más importantes podemos encontrar la seguridad, privacidad, el acceso remoto, la ocultación de la IP, así como también evitar la censura y el geobloqueo.

Ejemplo: Una empresa tiene empleados trabajando de forma remota, y acceden a la red privada mediante un software VPN.

**3- ¿Qué es una SAN?**

Una SAN (Storage Area Network), o Red de Área de Almacenamiento, es una red dedicada de alta velocidad que conecta servidores con dispositivos de almacenamiento, como discos duros o bibliotecas de cintas, de manera que los datos se gestionen de manera centralizada. Una SAN permite que múltiples servidores accedan a almacenamiento de datos de manera eficiente, como si fuera una unidad de almacenamiento local.

Entre sus características más importantes encontramos el almacenamiento centralizado, acceso rápido y eficiente, escalabilidad, redundancia y disponibilidad. Así como también la facilidad para la administración de datos.

Ejemplo: Una empresa con varios servidores necesita acceder a grandes volúmenes de datos. En lugar de tener discos en cada servidor, la empresa puede instalar una SAN que conecte todos los servidores a un sistema de almacenamiento centralizado. De esta manera, los servidores pueden acceder rápidamente a los datos almacenados en la SAN, y la administración de los datos se realiza de manera centralizada, lo que facilita las copias de seguridad y la recuperación de datos en caso de fallos.

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

Las diferencias entre Hub, Repetidor, Router y Switch se refieren a sus roles y funcionalidades dentro de una red. Cada uno de estos dispositivos cumple una función específica en la transmisión y gestión de datos en redes de comunicación.

Cuadro con las principales diferencias:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Función principal | Inteligencia | Tipo de red que maneja | Uso común |
| Hub | Conectar dispositivos en una red local | Baja (no inteligente) | Red local (LAN) | Conectar dispositivos en una LAN (obsoleto en la mayoría de las redes modernas) |
| Repetidor | Amplificar o regenerar la señal | Baja (no inteligente) | Red local (LAN) | Extender el alcance de una señal en la red |
| Switch | Conectar dispositivos de forma eficiente | Alta (gestión de tráfico) | Red local (LAN) | Gestionar el tráfico en redes locales y mejorar el rendimiento |
| Router | Conectar diferentes redes y dirigir el tráfico | Alta (enrutamiento) | Redes diferentes (LAN, WAN, internet) | Conectar una red local a internet o redes externas |

<https://www.renderforest.com/es/watch-98808908?quality=0>

**5- ¿Qué es un protocolo de comunicaciones?**

Un protocolo de comunicaciones es un conjunto de reglas y estándares que determinan cómo se debe transmitir, recibir e interpretar la información entre dispositivos en una red. Estas reglas definen aspectos como el formato de los datos, el orden en que se envían, cómo se gestionan los errores y cómo se sincronizan las conexiones entre los dispositivos para asegurar que la comunicación se realice de forma correcta y eficiente.

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

TCP/IP (Transmission Control Protocol/Internet Protocol):Es un conjunto de protocolos de comunicación que permite que dispositivos en una red se conecten y se comuniquen entre sí. Está compuesto por dos protocolos principales:

* TCP (Transmission Control Protocol): Es responsable de dividir los datos en paquetes y garantizar que lleguen correctamente y en el orden adecuado. Proporciona control de errores y asegura que los paquetes lleguen a su destino de manera fiable.
* IP (Internet Protocol): Se encarga de dirigir los paquetes de datos a través de la red utilizando direcciones IP (direcciones únicas asignadas a cada dispositivo en la red).

Características:

* TCP/IP es capaz de conectar redes globales y se utiliza en Internet.
* Funciona en un modelo de 4 capas: capa de enlace de datos, capa de red, capa de transporte y capa de aplicación.
* El protocolo TCP asegura que los datos lleguen completos y sin errores, mientras que el IP se encarga de dirigirlos hacia el destino correcto.

NetBIOS (Network Basic Input/Output System): Es una interfaz de programación de aplicaciones (API) que permite que los programas en una red local se comuniquen entre sí. Fue creado inicialmente para ser utilizado en redes de Microsoft. NetBIOS permite que los sistemas operativos se comuniquen a nivel de nombre, sesión y datagrama dentro de una red local (LAN).

Características:

* No está diseñado para redes grandes como TCP/IP, sino que se utiliza principalmente en redes locales.
* Aunque originalmente NetBIOS no utilizaba TCP/IP, hoy en día se puede usar sobre TCP/IP como parte de la suite de protocolos SMB (Server Message Block), especialmente para compartir archivos e impresoras en redes de Windows.
* NetBIOS se usa principalmente en redes Windows y sistemas que necesitan compartir recursos como archivos e impresoras.
* Proporciona tres servicios: NetBIOS Name Service (NBNS) para la resolución de nombres, NetBIOS Datagram Service para la comunicación sin conexión, y NetBIOS Session Service para la comunicación orientada a conexión.

|  |  |  |
| --- | --- | --- |
| Característica | TCP/IP | NetBIOS |
| Propósito | Facilitar la comunicación en redes globales, como Internet. | Proporcionar comunicación entre aplicaciones dentro de una red local. |
| Escala | Escalable, usado tanto en redes locales como globales (Internet). | Principalmente utilizado en redes locales (LAN). |
| Protocolo vs. Servicio | Es un conjunto de protocolos de comunicación (TCP y IP). | Es un servicio de comunicación a nivel de red local. |
| Uso principal | Comunicación de datos entre dispositivos a través de una red. | Comunicación de recursos y servicios en redes locales (compartición de archivos, impresoras). |
| Dependencia | No depende de ningún sistema operativo específico, funciona en una variedad de dispositivos y plataformas. | Originalmente asociado con sistemas Windows, aunque también puede funcionar en otros sistemas. |
| Dirección | Utiliza direcciones IP para identificar dispositivos. | Utiliza nombres NetBIOS para identificar dispositivos dentro de la red local. |
| Conexión | Basado en un modelo de conexión de red robusto (orientado a conexión con TCP, sin conexión con UDP). | Proporciona servicios de comunicación sin conexión (datagramas) y con conexión (sesiones). |
| Comunicación | Orientado a la transmisión de datos entre dispositivos a través de una red. | Proporciona funciones para la gestión de entradas/salidas en una red local, con enfoque en la resolución de nombres y el intercambio de información. |
| Protocolo | TCP/IP es un protocolo completo y robusto para la transmisión de datos. | NetBIOS no es un protocolo de transmisión, sino una API que funciona sobre protocolos como TCP/IP. |

**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 una unidad básica de comunicación que transporta la información desde el emisor hasta el receptor a través de una red. Este paquete se estructura de una manera organizada para garantizar que los datos lleguen de forma eficiente y sin errores.

Un paquete TCP/IP se compone de dos partes principales: la cabecera (header) y los datos (payload).

La cabecera contiene información crucial para la entrega, encaminamiento y control del paquete. Dependiendo del protocolo (como TCP o IP), esta cabecera puede variar, pero generalmente incluye varios campos como:

* Dirección IP de origen: La dirección IP del dispositivo que envía el paquete.
* Dirección IP de destino: La dirección IP del dispositivo al que va dirigido el paquete.
* Protocolo: Especifica qué protocolo de capa superior está usando el paquete (por ejemplo, TCP, UDP).
* Número de secuencia: En TCP, se utiliza para asegurarse de que los paquetes sean procesados en el orden correcto.
* Número de puerto de origen y de destino: Estos puertos ayudan a identificar las aplicaciones en los dispositivos de origen y destino.
* Longitud del paquete: Determina el tamaño total del paquete, incluyendo la cabecera y los datos.
* Campo de Control de Error (checksum): Utilizado para detectar errores de transmisión.
* Flags (bandejas): Son indicadores que controlan el comportamiento de la comunicación entre dispositivos. En TCP, los flags son campos especiales que proporcionan información sobre el estado de la conexión.

Datos (Payload): Esta es la parte del paquete que transporta la información real que se está enviando, ya sea una solicitud HTTP, un archivo, o cualquier tipo de datos generados por una aplicación.

Un "flag" (o "bandera") en un paquete TCP/IP es un campo dentro de la cabecera que contiene uno o varios bits específicos utilizados para controlar y gestionar la conexión. Los flags son particularmente importantes en el protocolo TCP, donde ayudan a coordinar la apertura, el cierre y el control de la conexión.

En TCP, los flags más comunes son los siguientes:

* SYN (Synchronize): Utilizado para iniciar una conexión. Este flag se usa en el proceso de establecimiento de conexión (handshake) en TCP.
* ACK (Acknowledgment): Indica que el paquete contiene un acuse de recibo (acknowledgment) para otro paquete recibido. Es crucial en la transmisión confiable de datos.
* FIN (Finish): Indica que el emisor ha terminado de enviar datos y que la conexión puede ser cerrada.
* RST (Reset): Se utiliza para reiniciar una conexión. Puede ser usado si se detecta un error o si se desea restablecer la conexión por alguna razón.
* PSH (Push): Indica que los datos deben ser entregados inmediatamente a la aplicación sin esperar a que se acumulen más datos.
* URG (Urgent): Señala que los datos son urgentes y deben ser procesados antes que otros paquetes.

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

Las redes de computadoras se pueden clasificar según su geografía en función del tamaño y la extensión de la cobertura geográfica que abarcan. Las principales variantes de redes según su geografía son:

Red de Área Personal (PAN - Personal Area Network) es una red que cubre un área muy pequeña, generalmente del tamaño de una persona o un espacio cercano, como una habitación. Su alcance puede llegar hasta los 10 metros aproximadamente.

Características:

o Alta velocidad de comunicación a corta distancia.

o Usualmente, no requiere infraestructura de red compleja.

o Se usa para conectar dispositivos personales como smartphones, tabletas, computadoras portátiles, etc.

Ejemplos: Conexiones Bluetooth entre un teléfono y un auricular, conexiones entre dispositivos mediante Wi-Fi en una oficina pequeña, o dispositivos como relojes inteligentes que se conectan con un teléfono.

Red de Área Local (LAN - Local Area Network) es una red que conecta dispositivos dentro de un área geográfica pequeña, como una oficina, una escuela o un hogar. Su alcance geográfico puede ir desde unos pocos metros hasta unos pocos kilómetros.

Características:

o Generalmente se usa tecnología Ethernet (cableada) o Wi-Fi (inalámbrica).

o Alta velocidad de transmisión de datos.

o Permite compartir recursos como impresoras, archivos y acceso a Internet.

o Requiere poca infraestructura, pero puede ser bastante compleja dependiendo de la configuración y el número de dispositivos.

Ejemplos: Redes de computadoras en una oficina, en una universidad, o en una casa donde varios dispositivos están conectados a través de un router o switches.

Red de Área Metropolitana (MAN - Metropolitan Area Network) es una red que cubre un área más grande que una LAN, típicamente en el rango de una ciudad o un área metropolitana. Su alcance puede abarcar hasta 50 kilómetros aproximadamente.

Características:

o Utiliza tecnologías de conexión de alta velocidad como fibra óptica, conexiones de microondas o enlaces de radio.

o Puede ser operada por una empresa privada o una entidad pública.

o Ofrece una mayor capacidad de ancho de banda que una LAN, y puede conectar varias LAN dentro de una misma área geográfica.

o Puede ser utilizada para conectar diferentes sucursales de una empresa dentro de la misma ciudad o región.

Ejemplos: Conexiones entre diferentes edificios o sucursales de una empresa en una ciudad, o incluso la red de una ciudad que conecta diversos servicios públicos o redes de comunicación.

Red de Área Amplia (WAN - Wide Area Network) es una red que cubre un área geográfica mucho más amplia, como un país o incluso el mundo. Puede tener un alcance que va desde decenas de kilómetros hasta conexiones internacionales.

Características:

o Utiliza diversas tecnologías de conexión a larga distancia, como líneas arrendadas, satélites, fibra óptica y conexiones de microondas.

o Se necesita infraestructura mucho más compleja para gestionar la interconexión de redes a gran escala.

o Permite la comunicación de datos a través de distancias muy largas, entre ciudades, países y continentes.

o Requiere proveedores de servicios (ISP, operadores de telecomunicaciones) para gestionar la conectividad.

Ejemplos: Internet es el ejemplo más común de una WAN, donde millones de redes locales (LAN) y redes metropolitanas (MAN) están interconectadas globalmente.

Red de Área Global (GAN - Global Area Network) es una red que abarca un área geográfica a nivel global, generalmente a través de múltiples países o continentes.

Características:

o Implica una infraestructura extremadamente compleja y costosa.

o Los datos viajan a través de redes WAN, subredes y enlaces internacionales.

o La capacidad de la red varía dependiendo de las conexiones y la infraestructura de telecomunicaciones disponible.

Ejemplos: Internet es también un ejemplo de una GAN, ya que permite la interconexión de redes a nivel mundial.

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

La topología de red se refiere a la disposición física o lógica de los dispositivos y cables que conforman una red de computadoras. Describe cómo están interconectados los dispositivos dentro de la red y cómo fluye la información entre ellos. La topología afecta el rendimiento, la escalabilidad y la fiabilidad de la red.

Topología de Bus: en una topología de bus, todos los dispositivos están conectados a un único cable común (llamado bus), que actúa como el canal de comunicación. Este cable transmite la información a todos los dispositivos, pero solo el que tenga la dirección correcta procesará la información.

Características:

o Simple y económica.

o El cable único es el punto central de falla. Si se corta o daña, toda la red puede caerse.

o Escalabilidad limitada, ya que añadir más dispositivos puede ralentizar la red.

o Usada principalmente en redes pequeñas o en la época temprana de las redes.

Ventajas:

o Fácil de instalar y configurar.

o Requiere menos cableado.

Desventajas:

o Si el cable principal falla, la red entera se interrumpe.

o Puede experimentar colisiones si muchos dispositivos transmiten simultáneamente.

Topología de Estrella:en una topología de estrella, todos los dispositivos están conectados a un dispositivo central (como un hub o switch). El dispositivo central actúa como un concentrador de comunicaciones, gestionando el tráfico entre los dispositivos.

Características:

o El hub o switch se convierte en el punto de control.

o Si un dispositivo falla, solo se interrumpe ese dispositivo, no la red completa.

o La red puede ser fácilmente escalada añadiendo más dispositivos.

Ventajas:

o Fácil de configurar y mantener.

o Alta tolerancia a fallos: si un dispositivo o conexión falla, no afecta a los demás.

o Buen rendimiento y gestión de tráfico.

Desventajas:

o Depende del dispositivo central (hub o switch); si este falla, la red entera se interrumpe.

o Requiere más cableado que en la topología de bus.

Topología de Anillo: en una topología de anillo, cada dispositivo está conectado a otros dos, formando un anillo cerrado. Los datos viajan en una sola dirección (o en algunas variantes, en ambas direcciones) alrededor del anillo hasta llegar a su destino.

Características:

o Los datos pasan de un dispositivo a otro en un único sentido (en algunos casos, bidireccional).

o Cada dispositivo tiene un token (un mensaje de control) que autoriza su envío de datos.

o Si un dispositivo o conexión se cae, puede afectar a toda la red, aunque existen métodos para hacerla tolerante a fallos (como el uso de un anillo doble).

Ventajas:

o La transmisión de datos es ordenada y eficiente.

o No hay colisiones de tráfico.

Desventajas:

o Si un dispositivo o cable falla, puede afectar a toda la red (a menos que se use un anillo doble).

o Añadir o quitar dispositivos puede ser complicado.

o El rendimiento puede verse afectado si la red crece mucho.

Topología de Malla: en una topología de malla, cada dispositivo está directamente conectado a todos los demás dispositivos de la red. Esto crea múltiples rutas para los datos, lo que garantiza que siempre haya una vía alternativa disponible si una de ellas falla.

Características:

o Cada dispositivo tiene múltiples conexiones, lo que permite una alta redundancia.

o Utilizada principalmente en redes de misión crítica, como centros de datos o redes de telecomunicaciones.

Ventajas:

o Alta redundancia: si un enlace falla, los datos pueden ser dirigidos por una ruta alternativa.

o Excelente fiabilidad y resistencia.

Desventajas:

o Requiere mucho cableado y es costosa de implementar.

o La gestión de la red puede ser complicada debido al gran número de conexiones.

Topología de Árbol (o Jerárquica): es una combinación de la topología de estrella y la topología de bus. En una topología de árbol, varios dispositivos de una red de estrella están conectados a un dispositivo central (el "tronco" del árbol), y esos dispositivos centrales están conectados a otros dispositivos de la misma forma.

Características:

o A menudo se usa en redes grandes, como en una empresa, donde cada departamento está conectado a un dispositivo central y luego al dispositivo principal de la red.

o El diseño jerárquico permite una fácil expansión y organización de la red.

Ventajas:

o Fácil de expandir y organizar.

o Puede ser utilizada para crear grandes redes distribuidas.

Desventajas:

o Dependencia de los dispositivos centrales: si un dispositivo central falla, puede afectar a la sección de la red que depende de él.

o Requiere más cableado que una topología de estrella simple.

Topología Híbrida: es una combinación de dos o más topologías básicas. Se emplea cuando se requiere lo mejor de diferentes topologías para adaptarse a las necesidades de la red.

Características:

o Por ejemplo, una red puede usar una topología de estrella para conectar departamentos, pero dentro de esos departamentos usar una topología de bus.

o Su flexibilidad permite adaptarse a diferentes requerimientos de tamaño, rendimiento y redundancia.

Ventajas:

o Flexibilidad: se pueden combinar las ventajas de varias topologías.

o Puede ser adaptada según las necesidades específicas de la red.

Desventajas:

o Más compleja de implementar y gestionar.

o Puede ser costosa dependiendo de las topologías combinadas.

**10- Explicar el servicio de DHCP.**

El DHCP (Dynamic Host Configuration Protocol), o Protocolo de Configuración de Host en español, es un protocolo de red utilizado para asignar automáticamente direcciones IP a dispositivos en una red. Este servicio permite que los dispositivos (como computadores, impresoras, smartphones, etc.) se conecten a una red sin necesidad de configurar manualmente la dirección IP en cada uno de ellos.

Funcionamiento:

Cuando un dispositivo (cliente) se conecta a la red, envía un mensaje de solicitud de IP (DHCP Discover) a través de la red para encontrar un servidor DHCP disponible.

Los servidores DHCP que están disponibles responden al cliente con una oferta (DHCP Offer), que incluye una dirección IP disponible para el dispositivo, la máscara de subred, el gateway predeterminado y otros parámetros de configuración.

El cliente responde aceptando una de las ofertas que ha recibido, enviando un mensaje de solicitud (DHCP Request) al servidor seleccionado.

El servidor DHCP confirma la asignación de la dirección IP al cliente enviando un mensaje de confirmación (DHCP Acknowledgment). En este momento, el cliente ya tiene asignada una dirección IP válida para su uso en la red.

Como características importantes cuenta con asignación de IP dinámica, automatización y configuración adicional, por ejemplo, de la Gateway, el servidor DNS y del tiempo de arrendamiento.  
  
Por arrendamiento se conoce al período de tiempo durante el cual se le asigna a un cliente una dirección IP dinámica en una red, antes de que deba renovar el arrendamiento para seguir utilizando esa IP, o, en algunos casos, recibir una nueva dirección IP. El servidor DHCP gestiona este proceso y, si el arrendamiento no se renueva, la IP asignada puede ser liberada y puesta nuevamente a disposición para otros dispositivos.

Los beneficios de este servicio son la eficiencia ya que simplifica la asignación y gestión de direcciones IP, especialmente en redes grandes. La flexibilidad ya que permite que dispositivos nuevos o móviles obtengan configuraciones automáticamente. Y la reducción de errores ya que minimiza la posibilidad de errores humanos al configurar las IP manualmente.

**11- Explicar el servicio de DNS.**

El DNS (Domain Name System), o Sistema de Nombres de Dominio en español, es un sistema que se utiliza para traducir los nombres de dominio legibles por los humanos, como [www.ejemplo.com](http://www.ejemplo.com), en direcciones IP númericas, como 192.168.1.1, que son utilizadas por los dispositivos para identificarse y comunicarse a través de redes, como internet.

Funcionamiento:

Cuando un usuario ingresa una dirección web en el navegador, por ejemplo, www.ejemplo.com, el navegador necesita saber cuál es la dirección IP correspondiente para poder conectarse al servidor que aloja esa página web.

El dispositivo del usuario (como su computadora o teléfono) hace una consulta a un servidor DNS para obtener la dirección IP asociada con el nombre de dominio www.ejemplo.com.

El servidor DNS busca la dirección IP correspondiente al dominio solicitado. Si el servidor DNS no tiene la dirección IP en su base de datos, puede consultar otros servidores DNS en la jerarquía del sistema para obtener la información.

Una vez que el servidor DNS encuentra la dirección IP, se la devuelve al dispositivo del usuario. Con esta dirección IP, el navegador puede conectarse al servidor web y cargar la página solicitada.

Jerarquías del DNS:

El sistema DNS tiene una estructura jerárquica de servidores. La jerarquía va desde los servidores de raíz hasta los servidores autoritativos de dominio específico:

* Servidores raíz: Son los servidores de nivel superior en la jerarquía del DNS. Existen unos pocos servidores raíz en todo el mundo y dirigen las consultas a los servidores adecuados para resolver los nombres de dominio.
* Servidores de nombres de dominio de nivel superior (TLD): Estos servidores resuelven dominios de nivel superior como .com, .org, .net, y otros.
* Servidores autoritativos: Son los servidores que contienen la información final sobre un dominio específico, como ejemplo.com. Este servidor tiene la IP exacta del servidor web correspondiente.

Tipos de registros DNS:

Cuando se realiza una consulta DNS, el servidor DNS responde con diferentes tipos de registros. Algunos de los más comunes son:

* A (Address Record): Mapea un nombre de dominio a una dirección IPv4.
* AAAA (IPv6 Address Record): Mapea un nombre de dominio a una dirección IPv6.

CNAME (Canonical Name): Es un alias de un dominio que apunta a otro

**12- Explicar las tecnologías Wireless, y sus estándares.**

Las tecnologías Wireless o inalámbricas son aquellas que permiten la transmisión de datos sin necesidad de cables o conexiones físicas. Estas tecnologías usan ondas de radio, microondas, infrarrojas u otras frecuencias electromagnéticas para enviar y recibir información entre dispositivos. Las redes inalámbricas se utilizan en una amplia gama de aplicaciones, desde comunicaciones personales (como Wi-Fi y Bluetooth) hasta conexiones móviles (como 4G y 5G).

Algunas de las principales tecnologías inalámbricas y sus estándares:

### 1. Wi-Fi (Wireless Fidelity)

El Wi-Fi es una tecnología inalámbrica que permite la conexión de dispositivos a Internet y a redes locales sin cables, utilizando ondas de radio. Es la tecnología más común para acceder a Internet en hogares, oficinas y lugares públicos.

#### Estándares de Wi-Fi:

* IEEE 802.11a/b/g/n/ac/ax (Wi-Fi 6): Varían en velocidad, frecuencia y eficiencia, siendo el más reciente Wi-Fi 6 (802.11ax), qué ofrece velocidades de hasta 9.6 Gbps, mayor eficiencia y mejor rendimiento en áreas con muchos dispositivos conectados.

### 2. Bluetooth

Bluetooth es una tecnología inalámbrica de corto alcance, diseñada para la transmisión de datos entre dispositivos cercanos, como teléfonos, computadoras, auriculares y dispositivos de IoT (Internet de las cosas). Es muy utilizada para la conexión de dispositivos periféricos (teclados, ratones, auriculares) y en sistemas de automóviles, por ejemplo.

#### Estándares de Bluetooth:

* Bluetooth 4.0: Introdujo el Bluetooth Low Energy (BLE), optimizado para dispositivos de bajo consumo, como sensores o wearables.
* Bluetooth 5.0/5.1/5.2: Mejoró la velocidad (hasta 2 Mbps), el alcance (hasta 240 metros) y las capacidades de conectividad, ideal para dispositivos IoT y audio de alta calidad

### 3. LTE (Long-Term Evolution) y 4G

LTE es una tecnología de comunicación móvil de alta velocidad, conocida comúnmente como 4G, que permite la transmisión de datos y voz a través de redes celulares. LTE ofrece velocidades mucho mayores que las tecnologías anteriores como 3G.

#### Estándares de LTE:

* LTE: Ofrece velocidades de hasta 100 Mbps de descarga y 50 Mbps de carga en condiciones ideales.
* LTE-Advanced: Mejora el LTE con velocidades de hasta 1 Gbps utilizando técnicas como la agregación de canales.

### 4. 5G (Quinta Generación)

5G es la próxima generación de tecnología móvil, que ofrece velocidades de transferencia de datos significativamente más rápidas que 4G, menor latencia y una mayor capacidad para conectar más dispositivos simultáneamente. Está diseñada para satisfacer las necesidades de aplicaciones avanzadas como vehículos autónomos, ciudades inteligentes, y más.

#### Estándares de 5G:

* 5G NR (New Radio): La especificación técnica de 5G que soporta velocidades de hasta 10 Gbps, latencia de menos de 1 milisegundo y una mayor densidad de dispositivos conectados por km². Utiliza frecuencias más altas (mmWave) y técnicas avanzadas de modulación y antenas.

### 5. Zigbee

Zigbee es una tecnología inalámbrica de bajo consumo diseñada para aplicaciones de automatización del hogar, como luces inteligentes, termostatos, y sensores de movimiento. Se utiliza en redes de Internet de las cosas (IoT) donde los dispositivos necesitan estar interconectados sin requerir un alto ancho de banda.

#### Estándares de Zigbee:

* IEEE 802.15.4: Este es el estándar base en el que se basa Zigbee. Define las capas físicas (PHY) y de enlace de datos (MAC) de la comunicación, asegurando que los dispositivos Zigbee puedan comunicarse de forma eficiente con bajo consumo de energía.

**13- ¿Qué es un Proxy?**

Un proxy es un servidor que actúa como intermediario entre un cliente (como una computadora o un dispositivo) y otro servidor (generalmente un servidor web). Su función principal es recibir las solicitudes que un cliente hace a un servidor y luego reenviarlas al servidor correspondiente, actuando como un "puente" entre ambos.

### Funcionamiento:

1. El cliente realiza una solicitud: Un usuario intenta acceder a un recurso en Internet (por ejemplo, visitar un sitio web).
2. La solicitud pasa por el proxy: En lugar de que la solicitud se envíe directamente al servidor web, se envía primero al proxy.
3. El proxy procesa la solicitud: El proxy recibe la solicitud, la examina y, si es necesario, la modifica o filtra según las reglas configuradas. Luego, el proxy reenvía la solicitud al servidor web.
4. El servidor responde al proxy: El servidor web envía la respuesta (como la página web solicitada) de vuelta al proxy.
5. El proxy envía la respuesta al cliente: Finalmente, el proxy pasa la respuesta del servidor web al cliente.

### Tipos de Proxy:

* Proxy Directo: Redirige las solicitudes de los clientes a un servidor sin modificar el contenido, simplemente actuando como intermediario.
* Proxy Reverso: A diferencia del proxy directo, el proxy reverso actúa en el lado del servidor. En lugar de que el cliente se conecte directamente al servidor, se conecta al proxy, que luego se encarga de enviar la solicitud al servidor adecuado. Es comúnmente usado para distribuir cargas entre varios servidores.
* Proxy Web: Específicamente diseñado para navegar por Internet, redirigiendo el tráfico HTTP. Se utiliza para bloquear contenido, mantener el anonimato o acceder a sitios web restringidos.
* Proxy Transparente: No requiere configuración especial por parte del cliente. Este tipo de proxy intercepta las solicitudes y las responde sin que el cliente lo sepa.
* Proxy Anónimo: Proporciona anonimato al cliente al ocultar su dirección IP real cuando accede a Internet, permitiendo una navegación más privada.

### Usos comunes de los Proxies:

* Anónimo y privacidad: Muchos usuarios emplean proxies para ocultar su dirección IP y navegar de forma más privada, sin revelar su ubicación o identidad.
* Filtrado de contenido: En empresas o escuelas, los proxies se usan para bloquear el acceso a ciertos sitios web o contenido, permitiendo o restringiendo el acceso según políticas específicas.
* Optimización de la red: Los proxies pueden almacenar en caché (guardar) las respuestas de los servidores web para que los usuarios puedan acceder a contenido más rápidamente sin tener que hacer una nueva solicitud al servidor original.
* Acceso a contenido restringido: Los proxies pueden permitir el acceso a sitios web o servicios bloqueados en ciertas regiones o redes, como cuando un servicio está restringido por geolocalización.
* Balanceo de carga: En los proxies reversos, se puede distribuir el tráfico entre varios servidores para optimizar la carga y mejorar la disponibilidad de los servicios.

### Ventajas de usar un Proxy:

* Mejora la seguridad: Al ocultar la dirección IP real del cliente, el proxy puede proteger contra ataques o accesos no autorizados.
* Control de tráfico: Los administradores pueden controlar el acceso a Internet, filtrar contenido y limitar el uso de ciertos recursos.
* Aumento de velocidad: Al almacenar en caché las respuestas, los proxies pueden reducir los tiempos de carga y mejorar la eficiencia de la red.
* Acceso remoto: Los proxies permiten a los usuarios conectarse a redes privadas de forma segura, incluso cuando están fuera de la oficina o en una red pública.

**14- Explicar el protocolo Spanning tree.**

El Protocolo Spanning Tree (STP) es utilizado en redes Ethernet para evitar bucles de red en topologías con enlaces redundantes. Un bucle puede causar congestión y fallos en la red, pero STP asegura que solo exista un camino activo para el tráfico de datos, bloqueando los enlaces redundantes cuando no son necesarios.

### Funcionamiento:

1. Elección del puente raíz (Root Bridge): El switch con el identificador más bajo se elige como el centro de la red.
2. Determinación de puertos:
   * Root Port: El puerto más cercano al puente raíz.
   * Designated Port: El puerto designado para enviar tráfico en cada segmento de red.
3. Bloqueo de puertos redundantes: Los puertos no necesarios se bloquean para evitar bucles.

### Estados de los puertos:

* Forwarding: El puerto transmite datos.
* Blocking: El puerto está inactivo para evitar bucles.
* Learning y Listening: El puerto está aprendiendo direcciones MAC o esperando para cambiar a estado Forwarding.

<https://www.canva.com/design/DAGknRlokMA/i3fhvtZWtov2NbLQCR2dfQ/edit?utm_content=DAGknRlokMA&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton>

**15- Explicar el protocolo de comunicaciones OSPF.**

OSPF (Open Shortest Path First) es un protocolo de enrutamiento utilizado en redes IP para encontrar la ruta más corta entre los routers, basándose en el estado de los enlaces. Es un protocolo link-state, lo que significa que los routers comparten información sobre sus conexiones para construir una topología de red.

### Características clave:

* Basado en el estado de los enlaces: Los routers intercambian información sobre sus conexiones (LSA) para construir una base de datos de la red.
* Áreas OSPF: La red se divide en áreas para mejorar la eficiencia.
* Algoritmo de Dijkstra: Se usa para calcular la ruta más corta a cada destino.
* Convergencia rápida: OSPF se adapta rápidamente a cambios en la red, como enlaces caídos.

### Ventajas:

* Escalable: Ideal para redes grandes.
* Convergencia rápida: Se adapta rápidamente a los cambios.
* Soporta VLSM: Usa direcciones IP sin clases, permitiendo una mejor distribución de direcciones.

**16- Explicar el protocolo ARP.**

El protocolo ARP (Address Resolution Protocol, por sus siglas en inglés) es un protocolo de red utilizado para mapear una dirección IP (protocolo de capa de red) a una dirección MAC (Media Access Control, en la capa de enlace de datos) en una red local (como Ethernet).

El ARP funciona en un proceso que hay que dividir en dos partes: solicitud y respuesta.

* Solicitud ARP (ARP Request): Cuando un dispositivo (por ejemplo, una computadora o un router) necesita enviar datos a otro dispositivo dentro de la misma red local, primero debe conocer la dirección MAC del dispositivo de destino. Si solo tiene la dirección IP de destino, debe utilizar ARP para encontrar la dirección MAC correspondiente.

Para ello, el dispositivo emisor envía una solicitud ARP en forma de paquete broadcast (es decir, dirigido a todos los dispositivos de la red) preguntando: "¿Quién tiene esta dirección IP?".

La solicitud ARP se envía a través de la red y todos los dispositivos la reciben.

* Respuesta ARP (ARP Reply): El dispositivo que tiene la dirección IP solicitada responde con un paquete ARP indicando su dirección MAC.

Esta respuesta es enviada directamente al dispositivo que realizó la solicitud (no como un broadcast), permitiendo que este último obtenga la dirección MAC correspondiente a la IP.

Para evitar tener que realizar solicitudes ARP de manera constante, los dispositivos mantienen una tabla ARP (también conocida como caché ARP) en la que se almacenan las correspondencias entre direcciones IP y MAC.

Esta tabla tiene un tiempo de vida limitado, y cuando un dispositivo no utiliza una dirección IP durante un cierto período de tiempo, esa entrada en la tabla ARP se elimina.

**17- ¿Qué es un Firewall?**

Los firewalls pueden considerarse fronteras o puertas que administran el flujo de la actividad web que se permite o prohíbe en una red privada. El término proviene del concepto de paredes físicas que actúan como barreras para ralentizar la propagación del fuego hasta que los servicios de emergencia pueden extinguirlo. En comparación, los firewalls de seguridad de red sirven para la administración del tráfico web y normalmente están destinados a ralentizar la propagación de las amenazas web.

Los firewalls crean “cuellos de botella” para canalizar el tráfico web. En esos puntos, se realiza una revisión según un conjunto de parámetros programados y se actúa en consecuencia. Algunos firewalls también realizan un seguimiento del tráfico y las conexiones en los registros de auditoría para consultar lo que se ha permitido o bloqueado.

Normalmente, los firewalls se utilizan para delimitar las fronteras de una red privada o sus dispositivos host. Así, los firewalls son una herramienta de seguridad que se incluye en la amplia categoría del control de acceso de los usuarios. Estas barreras por lo general se encuentran en dos ubicaciones: en computadoras específicas en la red o en las computadoras del usuario y en otros puntos de conexión (hosts).

**18- ¿Qué es una DMZ?**

Una zona desmilitarizada (demilitarized zone, DMZ) es una red perimetral que protege la red de área local (local-area network, 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. En la DMZ, las organizaciones normalmente almacenan servicios y recursos externos así como servidores para el sistema de nombres de dominio (Domain Name System, DNS), el protocolo de transferencia de archivos (File Transfer Protocol, FTP), correo, proxy, protocolo de voz sobre Internet (Voice over Internet Protocol, VoIP) y servidores web.

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 DMZ hace que sea más difícil para un pirata informático obtener acceso directo a los datos de una organización y a los servidores internos a través de Internet.

**19- ¿Qué es un Gateway?**

Un gateway (puerta de enlace en español) es un dispositivo o software de red que sirve como un punto de acceso entre dos redes diferentes, permitiendo la comunicación entre ellas.

Aunque las funciones de los gateways varían según su categoría y su propósito, es posible identificar algunas características comunes que caracterizan su operación:

· Enrutamiento y Conversión de Direcciones: En el caso de los gateways de red, su papel se extiende más allá de la simple conexión, incluyendo tareas de enrutamiento y conversiones de direcciones. Estas acciones garantizan que los datos lleguen con precisión a su destino en una red más amplia.

· Traducción de Protocolos: En la esfera de los gateways de protocolo, la traducción de datos de un formato a otro emerge como un aspecto fundamental. Esto posibilita la comunicación sin fricciones entre dispositivos y sistemas que operan con protocolos diferentes.

· Integración de Aplicaciones: Los gateways de API desempeñan un papel esencial al facilitar la integración entre aplicaciones que utilizan interfaces de programación diversas. Esta funcionalidad impulsa la automatización de procesos y el flujo de datos eficiente entre sistemas.

**20- Según Microsoft, ¿qué significa NBL?**

En el ámbito de Microsoft, NBL se refiere a NET\_BUFFER\_LIST. Una NET\_BUFFER\_LIST es una estructura de datos utilizada en la programación de controladores de red en sistemas operativos Windows. Esta estructura gestiona y representa los paquetes de datos que se transmiten o reciben a través de la red.

Microsoft proporciona herramientas y extensiones, como !ndiskd.nbl, que permiten a los desarrolladores y técnicos obtener información detallada sobre las NET\_BUFFER\_LIST durante el proceso de depuración de controladores de red. Estas herramientas facilitan el análisis y la resolución de problemas relacionados con el manejo de datos en la red.

Además, en el contexto de Windows, existe un encabezado denominado nbl.h que define las estructuras y funciones asociadas con las NET\_BUFFER\_LIST, proporcionando las interfaces necesarias para su manejo en el desarrollo de controladores de red.

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

**a. Explique cada uno de estos tipos de enlace.**

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

**c. Ranking de enlaces según lo pedido (de uno a seis, siendo uno el mejor): Por económico, performance, mayor capacidad, mayor o mejor configuración de restricciones, soporte a mayor distancia, menor esfuerzo de configuración.**

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

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

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

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

a. Tipos de enlace

* MPLS (Multiprotocol Label Switching): Es una tecnología de red que permite dirigir el tráfico de datos en función de etiquetas en lugar de direcciones de red, lo que permite un enrutamiento más eficiente y flexible. MPLS es utilizado principalmente en redes de área amplia (WAN), permitiendo priorizar el tráfico (QoS) y mejorar la eficiencia. Entre sus características se incluyen alta fiabilidad, escalabilidad, soporte para VPNs, y permite un control del tráfico de datos más eficiente.
* LAN to LAN: Este tipo de enlace conecta dos redes de área local (LAN) a través de una infraestructura de red privada o pública. Esto puede realizarse mediante enlaces dedicados o utilizando tecnologías como VPN (Virtual Private Network) para extender la red de una empresa entre varias ubicaciones. Se destaca por ofrecer conectividad directa entre dos redes locales, con latencias reducidas y sin necesidad de intervención externa para el intercambio de datos.
* Microonda (Enlace por microondas): Es una tecnología de transmisión de datos a través de ondas electromagnéticas de alta frecuencia, generalmente entre dos puntos fijos en línea de vista (LoS). Se utiliza para conectar áreas que no están cubiertas por cables, y es común en enlaces de transmisión de datos a larga distancia. Posee una gran capacidad de transmisión, aunque depende de la línea de visión entre los puntos de transmisión y es sensible a condiciones climáticas adversas.
* VSAT (Very Small Aperture Terminal): Es una tecnología de comunicación satelital que utiliza antenas pequeñas para enviar y recibir datos a través de satélites en órbita. Se usa comúnmente para conectar lugares remotos, como áreas rurales o plataformas marítimas. Se distingue por su cobertura global, ideal para lugares sin infraestructura terrestre, aunque suele tener mayores latencias y costos comparados con otras tecnologías terrestres.

b. Dos tipos de enlaces no mencionados anteriormente

* Fibra óptica: Utiliza cables de fibra de vidrio o plástico para transmitir señales de luz, lo que permite altas velocidades de transmisión y grandes capacidades. Es ampliamente usada para enlaces de largo alcance, como en redes de telecomunicaciones o conexiones entre centros de datos. Entre sus características se incluyen una alta velocidad de transmisión, una gran capacidad, bajo nivel de interferencia y su idoneidad para enlaces a larga distancia.
* Enlace ADSL (Asymmetric Digital Subscriber Line): Es una tecnología de acceso a internet de alta velocidad que utiliza las líneas telefónicas convencionales. Permite navegar por internet y realizar llamadas telefónicas al mismo tiempo, sin interferencias. Es una conexión asimétrica, lo que significa que la velocidad de descarga es mayor que la de subida. Una de sus principales características es que opera sobre infraestructuras telefónicas existentes. Las velocidades de conexión varían según la distancia entre el usuario y la central telefónica. Utiliza la modulación DMT (Discrete Multitone Modulation), que permite la transmisión simultánea de datos y voz, optimizando el uso de la línea.

c. Ranking de enlaces

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Criterio | MPLS | LAN to LAN | Microonda | VSAT | Fibra óptica | ADSL |
| Más económico | 6 | 4 | 3 | 2 | 1 | 5 |
| Mejor performance | 1 | 3 | 4 | 5 | 2 | 6 |
| Mayor capacidad | 2 | 5 | 3 | 4 | 1 | 6 |
| Mejor configuración de restricciones | 1 | 3 | 4 | 5 | 2 | 6 |
| Mejor soporte a mayor distancia | 2 | 5 | 1 | 3 | 4 | 6 |
| Menor esfuerzo de configuración | 6 | 4 | 3 | 2 | 1 | 5 |

d. Elección de tipo de enlace para los escenarios propuestos:

1. Conectividad de varios call centers con un data center central: MPLS es ideal para redes privadas y garantiza un rendimiento confiable y seguro entre varios sitios distantes, como call centers y un data center central. Su capacidad para manejar tráfico de voz, datos y video lo hace adecuado para este tipo de conectividad empresarial.
2. Conectar los datos de los pozos petroleros durante 15 minutos por día: Los pozos petroleros a menudo se encuentran en ubicaciones remotas donde las opciones de infraestructura son limitadas. VSAT ofrece conectividad satelital eficiente y es ideal para situaciones con tiempos de transmisión limitados y en lugares sin acceso a redes terrestres.
3. Comunicar dos edificios enfrentados en la misma calle: La comunicación por microondas es adecuada para edificios cercanos que necesitan una conexión punto a punto rápida y confiable. Considerando que están enfrentados, las estaciones de microondas pueden instalarse en los techos de ambos edificios, proporcionando una conexión directa sin la necesidad de cableado físico.

**22- Describir la tecnología LTE.**

Long-Term Evolution (LTE) es un estándar de cuarta generación (4G) para redes inalámbricas, que ofrece mayor capacidad y velocidad en comparación con 3G, aunque con un rendimiento inferior al de 4G puro. LTE permite velocidades de hasta 100 Mbps en descarga y 30 Mbps en subida, con baja latencia y una capacidad de ancho de banda escalable. Además, es compatible con tecnologías previas como GSM y UMTS. La evolución LTE-Advanced (LTE-A) alcanza hasta 300 Mbps. Aunque se le llama comúnmente 4G LTE, en realidad, LTE es más lento que el 4G real y se considera más cercano a un 3.95G.

LTE utiliza OFDMA (Acceso Múltiple por División de Frecuencia Ortogonal) para transmitir datos en el enlace descendente, lo que mejora la velocidad y eficiencia espectral en comparación con 3G. En el enlace ascendente, usa FDMA de portadora única, lo que reduce la potencia de transmisión y mejora el consumo de batería del dispositivo móvil. LTE se basa en el protocolo TCP/IP, lo que permite una red completamente basada en IP, ideal para la transmisión de datos de voz, video y mensajería.

En su versión LTE-Advanced (LTE-A), se emplean técnicas como MIMO y OFDM para mejorar la calidad de la señal, cobertura, velocidad y eficiencia energética, especialmente en áreas urbanas densas, similares a las redes Wi-Fi de última generación. Además, al ser una red basada en IP, la exposición a ciberamenazas es mayor, por lo que se requiere protección adecuada para mitigar los riesgos de seguridad.