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 |

**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 dominio (por ejemplo, www.ejemplo.com puede ser un alias de ejemplo.com).