1. Redes
    1.1. Introducción

Es un sistema de interconexión entre dispositivos que permite la comunicación y el intercambio de datos entre ellos. Estas redes pueden abarcar desde conexiones simples entre dos dispositivos, hasta infraestructuras complejas que conectan millones de dispositivos en todo el mundo. Las redes informáticas se basan en la transmisión de datos a través de diversos medios como cables de cobre, fibra óptica o conexiones inalámbricas. Estos datos se transmiten en forma de paquetes de información, que contienen tanto los paquetes que se envían, como la información de control necesaria para dirigirlos a su destino.

Existen diferentes tipos de redes informáticas, como las Redes de Área Local (LAN) que conectan dispositivos dentro de un área geográfica limitada, o una oficina o un hogar, o las Redes de Área Amplia (WAN) que abarcan distancias más grandes y pueden incluir conexiones a través de internet, y las Redes Inalámbricas que utilizan tecnologías como el WiFi para permitir la comunicación sin cables entre dispositivos.

Las Redes Informáticas también pueden clasificarse según su topología, es decir, la forma en que están organizados los dispositivos y las conexiones entre ellos. Algunas topologías comunes incluyen la topología de BUS, en la que todos los dispositivos están conectados a un único cable principal. La topología de estrella, en la que todos los dispositivos están conectados a un punto central como un concentrador o un computador. Y la topología de maya, en la que cada dispositivo está conectado directamente a todos los demás dispositivos de la red.

Las redes informáticas se han convertido en una parte integral de nuestra vida cotidiana y el funcionamiento de numerosas organizaciones y empresas. Permiten compartir recursos como archivos, impresoras y conexiones a internet, así como facilitar la colaboración entre usuarios ubicados en distintos lugares geográficos. Además de las conexiones LAN, WAN y Redes Inalámbricas, existen otros medios de redes especializadas, como las Redes de Área Metropolitana (MAN), que abarcan una ciudad o región, y las Rede de Área Personal (PAN) que conectan dispositivos personales cercanos como teléfonos inteligentes y computadoras portátiles.

Las redes informáticas se rigen por protocolos y estándares como el conjunto protocolos TCP/IP que define cómo se empaquetan, envían y reciben los datos en la red. Estos protocolos aseguran la interoperabilidad entre diferentes dispositivos y sistemas en una red independientemente de su fabricante o tecnología subyacente.

La seguridad de las redes informáticas es una preocupación importante, ya que los datos transmitidos a través de la red, pueden ser sensibles y estar expuestos a amenazas como el acceso no autorizado, el robo de datos y el malware. Por lo tanto, se utilizan diversas técnicas y herramientas como firewalls, cifrado de datos y sistemas de detección de instrucciones, para proteger la integridad y confidencialidad de la información de la red.

El diseño y la administración de redes informáticas requiere conocimientos especializados como la arquitectura de redes, la configuración de dispositivos de red, el direccionamiento IP, la resolución de problemas de conectividad y monitoreo del rendimiento de la red.

Los profesionales de las redes informáticas, como los ingenieros de redes y los administradores de sistemas, desempeñan un papel crucial en la planificación, implementación y mantenimiento de infraestructuras de red robustas y seguras.

1.2. Componentes de una red

- Switch

Un switch es un dispositivo de red que actúa como un centro de conexión para dispositivos en una red local (LAN).

Funciones Principales: Facilita la comunicación entre dispositivos en la misma red al dirigir el tráfico de red de manera eficiente. Permite la transferencia de datos entre múltiples dispositivos de manera simultánea.

Características Importantes: Puertos Ethernet para conectar dispositivos por cable. Tabla de direcciones MAC para dirigir los paquetes de datos a los dispositivos correctos. Gestión de tráfico para optimizar el flujo de datos y evitar congestiones en la red.

Beneficios:

- Mejora el rendimiento de la red al reducir la colisión de datos.
- Permite la segmentación de la red para mejorar la seguridad y el control de acceso.

Escalable:
Se pueden agregar más switches según las necesidades de la red.

- Router:

El router es un componente esencial en cualquier red informática. Actúa como puente entre diferentes redes, dirigiendo el tráfico de datos de manera eficiente. Permite la conexión a Internet y facilita la comunicación entre dispositivos en redes locales y remotas. Utiliza tablas de enrutamiento para determinar la mejor ruta para enviar paquetes de datos. Proporciona funciones de seguridad, como cortafuegos y filtrado de paquetes, para proteger la red contra amenazas externas. Es fundamental para establecer y mantener la conectividad y la comunicación en entornos modernos.

- Repetidores:

Los repetidores desempeñan un papel crucial en la ampliación del alcance de una red y en la mejora de la calidad de la seniat. Estos dispositivos reciben la seniat de red, la amplifican y la retransmiten, lo que permite superar obstáculos físicos y extender la cobertura de la red inalámbrica.

Funciones Principales:

- Amplificación de señal:

Los repetidores aumentan la potencia de la señal, lo que ayuda a superar pérdidas de señal debido a la distancia o a obstáculos físicos.

- Extensión de alcance:

Permiten que la señal de red llegue a áreas que de otro modo serían inaccesibles, lo que es especialmente útil en entornos grandes o con múltiples pisos.

- Mantenimiento de Integridad de la Señal:

Al retransmitir la señal, los repetidores ayudan a mantener su calidad y consistencia, lo que resulta en una comunicación más confiable y sin interrupciones.

- Modems:

Los módems, abreviación de “modulador-demodulador”, son dispositivos esenciales en el mundo de las comunicaciones digitales. Actúan como el enlace crucial entre nuestros dispositivos y el vasto universo de internet. Convertir señales digitales en analógicas para transmitir datos y viceversa, los modems nos permiten acceder a la riqueza de información y servicios en línea.

Funciones Principales:

- Conversión de señales:

Transforman los datos digitales de nuestras computadoras en señales analógicas para ser transmitidas a través de líneas de telecomunicaciones, y viceversa, permitiendo la comunicación bidireccional.

- Acceso a Internet:

Facilitan la conexión a la red mundial de computadoras, permitiendo a los usuarios explorar la web, enviar correos electrónicos, realizar videoconferencias y mucho más.

- Variedad de Tecnologías:

Existen diferentes tipos de módems, como DSL, cable, fibra óptica y móviles, cada uno adaptado a distintos tipos de conexiones y velocidades de transmisión.

1.3. Clasificacion de redes

- Tipos de Redes:

Las redes informáticas se clasifican según diversos criterios, que incluyen su tamaño, topología, método de acceso y uso. Esta clasificación proporciona una comprensión más profunda de cómo están estructuradas y cómo se utilizan en diferentes entornos. A continuación, explicaremos los principales tipos de redes según estos criterios.

- Por Tamaño:

01. **LAN (Red de Área Local)**: Limitada a un área geográfica pequeña, como una casa, oficina o campus.
02. **MAN (Red de Área Metropolitana)**: Cubre un área geográfica más grande, como una ciudad o región metropolitana.
03. **WAN (Red de Área Amplia)**: Se extiende sobre un área geográfica amplia, como un país o continente, a través de enlaces de comunicación públicos.

- Por Topología:

01. **Estrella**: Todos los dispositivos están conectados a un nodo central (como un switch o un router).
02. **Bus**: Todos los dispositivos comparten un solo canal de comunicación.
03. **Anillo**: Cada dispositivo está conectado a otros dos, formando un anillo cerrado de conexiones.

- Por método de acceso:

01. **Ethernet**: Utiliza el protocolo de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD).
02. **Token Ring**: Utiliza un token para controlar el acceso a la red, evitando colisiones.

03. **Wi-Fi**: Utiliza el estándar IEEE 802.11 para redes inalámbricas.

- Por Uso:

01. **Redes de Oficina**: Diseñadas para facilitar la comunicación y compartir recursos dentro de una empresa u organización.
02. **Redes de Hogar**: Conectan dispositivos dentro de una residencia para compartir Internet, archivos y dispositivos.
03. **Redes de Datos**: Utilizadas para transmitir datos entre dispositivos, como en Internet.

- Consideraciones Importantes:
    - **Seguridad**:

Es crucial implementar medidas de seguridad robustas para proteger las redes contra acceso no autorizado, intrusiones y ataques cibernéticos. El uso de firewalls, sistemas de detección de instrucciones (IDS), autenticación de usuarios y encriptación de datos son prácticas fundamentales para garantizar la integridad y confidencialidad de la red.

    - **Escalabilidad**:

Las redes deben diseñarse teniendo en cuenta su capacidad para crecer y adaptarse a las necesidades cambiantes de la organización. La infraestructura de red debe ser escalable, permitiendo la incorporación de nuevos dispositivos, usuarios y servicios sin comprometer el rendimiento ni la seguridad.

    - **Fiabilidad**:

La fiabilidad de la red es esencial para garantizar su disponibilidad y rendimiento continuo. Se deben implementar redundancias y mecanismos de recuperación ante fallos para minimizar el tiempo de inactividad y mantener la productividad de la organización.

1.4. P2P y Cliente-Servidor

- Peer to Peer (P2P):

En una red P2P, cada dispositivo actúa como cliente y servidor al mismo tiempo. Los dispositivos se conectan directamente entre sí, sin necesidad de un servidor centralizado.

Características:

- Igualdad:

Todos los dispositivos tienen roles similares y pueden proporcionar y solicitar recursos.

- Descentralización:

No hay un servidor central que controle la red.

- Escalabilidad:

La red puede crecer fácilmente al agregar nuevos nodos.

- Resiliencia:

No depende de un solo punto de falla.

Ejemplos:

Compartir archivos a través de programas como BitTorrent. Llamadas de voz y video en aplicaciones como Skype. Compartir recursos de impresión o almacenamiento de en red local.

- Cliente-Servidor:

En un modelo cliente-servidor, los dispositivos se dividen en dos categorías: clientes y servidores. Los clientes solicitan recursos o servicios, mientras que los servidores los proporcionan.

Características:

- Centralización:

Los servicios o recursos son controlados y gestionados por servidores dedicados.

- Especialización de Roles:

Los servidores están optimizados para proporcionar servicios específicos, como almacenamiento de datos, gestión de bases de datos, etc.

- Seguridad:

Los servidores pueden implementar medidas de seguridad centralizadas.

- Escalabilidad Limitada:

La adición de nuevos clientes no afecta directamente la capacidad del servidor.

Ejemplos:

Los navegadores actúan como clientes que solicitan páginas web a servidores web. Los clientes de correo electrónico solicitan y envían mensajes a los servidores de correo. Almacenamiento en la nube: Los clientes acceden a sus archivos almacenados en servidores remotos.

1.5. Medios de transmisión de datos

- ¿Qué son los Medios de Transmisión?

Los medios de transmisión son los conductos físicos o inalámbricos a través de los cuales se transmiten datos entre dispositivos en una red.

- Tipos de Medios de Transmisión:
  - **Cableado**:

Utiliza cables físicos para transmitir señales eléctricas. Proporciona una conexión confiable y segura.
Ejemplos: cable de par trenzado, cable coaxial, fibra óptica.

  - **Inalámbrico**:

Transmite datos a través de ondas electromagnéticas sin la necesidad de cables físicos. Ofrece flexibilidad y movilidad.
Ejemplos: Wi-Fi, Bluetooth, infrarrojos, tecnologías celulares (4G, 5G).

- Factores a Considerar:
  - **Velocidad**:

Los diferentes medios de transmisión tienen velocidades de transmisión distintas.

  - Seguridad:

Algunos medios pueden ser más seguros que otros, especialmente en entornos inalámbricos.

  - **Costo**:

El costo de implementación y mantenimiento varía entre los diferentes medios de transmisión.

- **Entorno**:

Factores como la distancia, la interferencia y las obstrucciones pueden afectar la elección del medio de transmisión.

1.6. Ancho de banda, frecuencia de transmisión y alcances

- ¿Qué es el Ancho de Banda?

El ancho de banda se refiere a la cantidad de datos que pueden transmitirse en un periodo de tiempo dado a través de un medio de comunicación.

- ¿Qué es la Frecuencia de Transmisión?

La frecuencia de transmisión es la cantidad de veces que una señal completa un ciclo en un segundo, medida en hercios (Hz).

- ¿Cómo se Relacionan?

El ancho de banda y la frecuencia de transmisión están relacionados de manera (Inversa o Directa?) inversa: a mayor frecuencia, mayor ancho de banda disponible.

- Ancho de Banda y Frecuencia de Transmisión:

Ancho de Banda vs Frecuencia:
Cuanto mayor sea la frecuencia de transmisión, mayor será el ancho de banda disponible para transmitir datos.

Ejemplo:
En redes de fibra óptica, diferentes longitudes de onda (frecuencias) se utilizan para transmitir múltiples canales de datos simultáneamente, lo que aumenta el ancho de banda total disponible.

Efectos de la Frecuencia:
Frecuencias más altas pueden transportar más datos en menos tiempo, pero pueden verse afectadas por una atenuación más rápida y una menor distancia de transmisión.
Frecuencias más bajas pueden viajar distancias más largas, pero tienen un ancho de banda limitado.

- Alcance de la Transmisión:

Alcance de las Transmisiones Inalámbricas:
Las transmisiones inalámbricas pueden variar en alcance dependiendo de factores como la potencia de la señal, la frecuencia utilizada y las obstrucciones en el entorno.
Por ejemplo, las redes Wi-Fi en la banda de 2.4 GHz suelen tener un alcance mayor que las redes en la banda de 5 GHz debido a la mayor capacidad de penetración de las ondas de radio de menor frecuencia.

Alcance de las Transmisiones Cableadas:
Las transmisiones a través de medios cableados, como cables de par trenzado o fibra óptica, pueden alcanzar distancias mucho mayores con menos degradación de la señal en comparación con las transmisiones inalámbricas.
Las redes de fibra óptica pueden transmitir datos a distancias de hasta varios kilómetros sin pérdida significativa de señal.

- Consideraciones Importantes:

La elección del ancho de banda, la frecuencia de transmisión y el medio de transmisión adecuados depende de factores como la distancia de transmisión, la velocidad requerida y el entorno de implementación. Es importante equilibrar la velocidad y la distancia de transmisión con la estabilidad y la fiabilidad de la conexión.

2. Protocolos de Internet - (Inicial)

2.1. Introducción

Protocolo de internet: es una serie de reglas que permite la comunicación entre dispositivos dentro de una red informática. Estos protocolos se dividen en capas, cada una encargada de funciones específicas para facilitar la transmisión de datos de un extremo a otro de la red.

En la capa de aplicación, se encuentran los protocolos que permiten a las aplicaciones comunicarse entre sí a través de la red. Algunos ejemplos son HTTP para la web, SMTP para el correo electrónico, FTP para la transferencia de archivos y DNS para la resolución de nombres de dominio.

La capa de transporte es donde opera el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). El TCP proporciona una conexión orientada a la fiabilidad, mientras que el UDP es más ligero y se utiliza cuando la velocidad es más importante que la fiabilidad, como la transmisión de videos en tiempo real. Fiabilidad se refiere a que TCP claramente va a intentar transmitir información lo más prolijamente posible, que no se pierda ningún dato ni paquete, en cambio UDP va a priorizar el tema de que se siga transmitiendo, como por ejemplo un video de streaming.

En la capa de red, se encuentra el protocolo IP (Internet Protocol), que asigna direcciones únicas a cada dispositivo en la red y determina cómo se deben enviar los datos de un dispositivo a otro.

La capa de enlace de datos define los protocolos para la transferencia confiable de datos entre dispositivos directamente conectados. Incluye protocolos como ethernet y Wi-Fi.

La capa física es la capa más baja, encargada de la transmisión física de bits a través de medios de comunicación, sea por cable-cobre, fibra óptica o señales de radio.

Estos protocolos de internet son fundamentales para el funcionamiento de internet y son la base de todas las comunicaciones de las redes modernas desde la navegación web hasta las llamadas de voz por IP.

2.2. Dirección MAC y direcciones IP (IPv4/IPv6/fijas y dinámicas)

- Dirección MAC (Media Access Control):

Es un identificador único asignado a cada dispositivo de red. Está grabado en el hardware de la tarjeta de red y no puede cambiarse. Tiene una longitud de 48 bits (6 bytes) y se representa típicamente en formato hexadecimal.

Función: Identifica de manera única a un dispositivo en una red local. Se utiliza para el direccionamiento en la capa de enlace de datos del modelo OSI.

Ejemplo de dirección MAC: 00:1A:2B:3C:4D:5E

- Dirección IP (IPv4 e IPv6):

IPv4 (Protocolo de internet versión 4): Utiliza direcciones de 32 bits, representadas en formato decimal separado por puntos (por ejemplo: 192.168.0.1).
Debido a la creciente demanda de direcciones, IPv4 ha alcanzado su límite y se han introducido soluciones como la traducción de direcciones de red (NAT) para conservar direcciones.

Ejemplo de direccion IPv4: 192.168.1.100

IPv6 (protocolo de internet versión 6): Utiliza direcciones de 128 bits, representadas en formato hexadecimal separado por dos puntos (por ejemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
Ofrece un espacio de direcciones mucho más grande que IPv4, lo que permite un número casi ilimitado de dispositivos conectados a internet.

Ejemplo de dirección IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

- Direcciones IP: Fijas y Dinámicas:

Fijas:
Asignadas manualmente a un dispositivo y permanecen constantes.
Son útiles para servidores, dispositivos de red críticos y dispositivos que necesitan ser fácilmente identificables en una red.

Dinámicas:
Asignadas automáticamente a un dispositivo por un servidor DHCP (Protocolo de Configuración Dinámica de Host).
Son temporales y pueden cambiar cada vez que el dispositivo se conecta a la red.
Son útiles para dispositivos cliente y en redes donde se necesita flexibilidad en las asignaciones de direcciones IP.

- Consideraciones Importantes:

Las direcciones MAC son únicas a nivel mundial y sirven para identificar de manera exclusiva un dispositivo de red.

Las direcciones IP permiten la comunicación entre dispositivos en una red y se utilizan para enrutar paquetes de datos.

Tanto las direcciones IP fijas como las dinámicas tienen sus propias aplicaciones y consideraciones de seguridad.

2.3. Máscara de subred

- ¿Qué es la máscara de subred?

La máscara de subred es un número binario que se utiliza para dividir una red IP en subredes más pequeñas.

Define que parte de una dirección IP pertenece a la red y que parte pertenece a los hosts dentro de esa red.

- Notación de la Máscara de Subred:

La máscara de subred se representa en forma de una dirección IP.

Consiste en una serie de unos (1) seguidos de una serie de ceros (0), indicando la porción de red y la porción de host, respectivamente.

Ejemplo de notacion de mascara de subred: 255.255.255.0

- Máscara de Subred en Acción:

Divisores de Redes:
La máscara de ubres divide una dirección IP en dos partes: la red y el host.

Por ejemplo, en una máscara de subred 255.255.255.0, los primeros 24 bits representan la red y los últimos 8 bits representan el host.

Determinación de la Subred:
Al aplicar la máscara de subred a una dirección IP, se puede determinar a qué subred pertenece esa dirección.

Por ejemplo, si la dirección IP es 192.168.1.100 y la máscara de subred es 255.255.255.0, la subred sería 192.168.1.0

- Clases de Direcciones IP y Máscaras de Subred

Clases de Direcciones IP:
Las direcciones IP se dividen en cinco clases: A, B, C, D, y E.

Las clases A, B y C se utilizan para redes, mientras que las clases D y E se reservan para otros propósitos, como multidifusión (streaming) o para usos futuros.

Máscaras de Subred por Defecto:
Cada clase de dirección IP tiene una máscara de subred predeterminada asociada.

Por ejemplo:
Clase A: 255.0.0.0
Clase B: 255.255.0.0
Clase C: 255.255.255.0

- Importancia de la Máscara de Subred

La máscara de subred es fundamental para la segmentación y la organización de redes IP.

Permite la optimización del tráfico de red al limitar la difusión de paquetes solo a los hosts dentro de la misma subred.

Facilita la implementación de políticas de seguridad y el control del acceso a recursos de red.

2.4. Enrutamiento

- ¿Qué es el Enrutamiento?:

El enrutamiento es el proceso de seleccionar el mejor camino para que los datos viajen desde el origen hasta el destino en una red de computadoras.

- Importancia del Enrutamiento:

Permite la comunicación efectiva entre dispositivos en redes complejas.

Optimiza el flujo de datos al dirigirlos por la ruta más eficiente disponible.

Es esencial para el funcionamiento de Internet y otras redes de gran escala.

- Componentes del Enrutamiento:

01. **Router**:

El router es el dispositivo principal responsable de la toma de decisiones de enrutamiento. Examina las direcciones IP de destino de los paquetes de datos y los envía al mejor camino posible hacia su destino.

02. **Tabla de Enrutamiento**:

La tabla de enrutamiento es una lista de destinos conocidos y las rutas asociadas a ellos. Se basa en información recopilada a través de protocolos de enrutamiento y configuración manual.

03. **Protocolos de Enrutamiento**:

Los protocolos de enrutamiento son conjuntos de reglas y algoritmos utilizados por los routers para intercambiar información de enrutamiento y tomar decisiones. Ejemplos de protocolos de enrutamiento: RIP (Protocolo de Información de Enrutamiento), OSPF (Protocolo de Estado de Enlace), BGP (Protocolo de Puerta de Enlace Exterior).

- Tipos de Enrutamiento:

Enrutamiento Estático:

Las rutas se configuran manualmente por un administrador de red.

Es adecuado para redes pequeñas y estables donde los cambios en la topología de la red son poco frecuentes.

Enrutamiento Dinamico:

Las rutas se determinan automáticamente por los routers utilizando protocolos de enrutamiento.

Es más flexible y adaptable a cambios en la red, pero requiere un mayor uso de recursos de procesamiento y ancho de banda.

- Estrategias de Enrutamiento:

Enrutamiento por Vector de Distancia:
Cada router mantiene una tabla de enrutamiento que contiene el mejor camino conocido hacia cada destino.

Los routers intercambian información de enrutamiento con sus vecinos y actualizan sus tablas en función de la distancia y el número de saltos.

Enrutamiento por Estado de Enlace:
Cada router mantiene una base de datos de la topología de la red completa.

Utiliza algoritmos para calcular la ruta más corta hacia cada destino basándose en la calidad de las conexiones y la latencia.

- Consideraciones Importantes:

La eficacia del enrutamiento depende de una buena planificación de la red, incluyendo la segmentación de subredes y la selección de protocolos de enrutamiento adecuados.

La seguridad es una preocupación importante en el enrutamiento, y se deben implementar medidas para proteger las tablas de enrutamiento y evitar ataques de envenenamiento de enrutamiento.

3. Protocolos de Internet - (Intermedio)
   3.1. Modelo OSI

- ¿Qué es el Modelo OSI?:

El Modelo OSI (Open Systems Interconnection) es un marco conceptual que describe las funciones de una red de computadoras en términos de siete capas lógicas.

- Importancia del Modelo OSI:

Proporciona una estructura clara y modular para diseñar, implementar y gestionar redes de computadoras.

Facilita la interoperabilidad entre sistemas de diferentes fabricantes al estandarizar las funciones de red en capas separadas.

- Las Siete Capas del Modelo OSI:

01. **Capa Física**:

Define los medios físicos y eléctricos utilizados para transmitir datos entre dispositivos. Ejemplos de dispositivos: cables, conectores, concentradores (hubs).

02. **Capa de Enlace de Datos**:

Controla el acceso al medio y proporciona la detección y corrección de errores en la capa física. Empleos de dispositivos: switches, bridges.

03. **Capa de Red**:

Se encarga del enrutamiento y la conmutación de datos a través de la red. Ejemplos de dispositivos: routers, gateways.

04. **Capa de Transporte**:
Proporciona servicios de extremo a extremo para el transporte de datos, como la segmentación y el control del flujo. Ejemplos de protocolos: TCP (Control de Transmisión), UDP (Datagrama de Usuario).

05. **Capa de Sesión**:
Establece, mantiene y termina las conexiones entre aplicaciones en diferentes dispositivos. Administra el diálogo entre los procesos de aplicación.

06. **Capa de Presentación**:
Se encarga de la representación de datos, como la codificación, la comprensión y el cifrado. Proporciona interoperabilidad entre sistemas con diferentes formatos de datos.

07. **Capa de Aplicación**:
Proporciona servicios de red a las aplicaciones y usuarios finales. Ejemplos de protocolos: HTTP (Protocolo de Transferencia de Hipertexto), FTP (Protocolo de Transferencia de Archivos), SMTP (Protocolo de Transferencia de Correo Simple).

- Interacción entre Capas:

Las capas del Modelo OSI interactúan entre sí mediante interfaces bien definidas. Cada capa realiza sus funciones específicas y se comunica con las capas adyacentes a través de unidades de datos específicas (PDU).

- Ventajas de Modelo OSI:

01. **Modularidad**:
Permite cambios y actualizaciones en una capa sin afectar a las demás capas. Facilita el diseño y la implementación de nuevas tecnologías de red.

02. **Estandarización**:
Proporciona un marco de referencia común para el diseño de redes y la interoperabilidad entre sistemas.

03. **Resolución de Problemas**:
Divide las funciones de red en capas más manejables, lo que facilita la localización y corrección de problemas.

3.2. Fragmentación y Reensamblado

- ¿Qué es la Fragmentación?

La fragmentación es el proceso de dividir un paquete de datos en fragmentos más pequeños para que pueda ser transmitido a través de una red con un tamaño máximo de unidad de transmisión (MTU) más pequeño que el tamaño del paquete original.

- Importancia de la Fragmentación:

Permite la transmisión de datos a través de redes con diferentes capacidades de transmisión y restricciones de tamaño de paquete.

Optimiza el uso del ancho de banda al ajustar dinámicamente el tamaño de los paquetes según las condiciones de la red.

- Proceso de Fragmentación:

01. **Determinación del Tamaño del Paquete**:

Antes de enviar un paquete de datos, el dispositivo emisor verifica el tamaño del paquete y compara con el MTU de la red de destino.

02. **División del Paquete**:

Si el tamaño del paquete excede el MTU de la red, el dispositivo emisor divide el paquete en fragmentos más pequeños, cada uno con una longitud que se ajuste al MTU.

03. **Encabezado de Fragmentación**:

Cada fragmento incluye un encabezado de fragmentación que contiene información sobre la posición del fragmento en el paquete original y un identificador de fragmento único.

04. **Envío de Fragmentos**:

Los fragmentos se envían individualmente a través de la red al destino.

- ¿Qué es el Reensamblado?

El reensamblado es el proceso de reconstruir el paquete original a partir de los fragmentos recibidos en el destino.

- Importancia del Reensamblado:

Garantiza la entrega completa y precisa de los datos al destino final, incluso cuando los paquetes se dividen durante la transmisión.

Permite que los dispositivos de destino reconstruyan los datos originales y procesen la información correctamente.

- Proceso de Reensamblado:

01. **Recepción de Fragmentos**:

El dispositivo de destino recibe los fragmentos de datos individualmente a través de la red.

02. **Reensamblado de Fragmentos**:

El dispositivo de destino utiliza la información de los encabezados de fragmentación para reensamblar los fragmentos en el orden correcto y reconstruir el paquete original.

03. **Verificación de Integridad**:

Se verifica la integridad de los datos reensamblados para detectar y corregir errores de transmisión.

04. **Entrega al Destino Final**:

Una vez que el paquete original ha sido reensamblado correctamente, se entrega a la aplicación o proceso de destino para su procesamiento.

- Consideraciones Importantes:

La fragmentación y el reensamblado introducen sobrecarga adicional en los dispositivos de red y pueden afectar el rendimiento en redes de alta carga.

Es importante configurar adecuadamente los parámetros de fragmentación y reensamblado para garantizar un rendimiento óptimo y una comunicación confiable.

3.3. Protocolos de Internet

- ¿Qué son los Protocolos de Internet?:

Los Protocolos de Internet son conjuntos de reglas y estándares que permiten la comunicación entre dispositivos en redes de computadoras.

- Importancia de los Protocolos de Internet:

Facilitan la transmisión de datos de manera eficiente y confiable en redes de cualquier tamaño.

Establecen reglas para la identificación, el direccionamiento, el enrutamiento y la entrega de paquetes de datos a través de la red.

- Protocolos Fundamentales de Internet:

01. **Protocolo de Internet (IP)**:

El protocolo IP es el principal protocolo de la capa de red del modelo OSI. Proporciona direccionamiento y enrutamiento de paquetes a través de la red. IPv4 e IPv6 son las versiones más comunes del protocolo IP utilizadas en la actualidad.

02. **Protocolo de Control de Transmisión (TCP)**:

TCP es un protocolo de la capa de transporte del modelo OSI. Proporciona una comunicación orientada a la conexión y garantiza la entrega ordenada y confiable de datos. Utilizado en aplicaciones que requieren transferencia de datos segura y sin pérdidas, como la navegación web y el correo electrónico.

03. **Protocolo de Datagrama de usuario (UDP)**:

UDP es otro protocolo de la capa de transporte del modelo OSI. Proporciona una comunicación sin conexión y no garantiza la entrega de datos ni el orden de los paquetes. Utilizado en aplicaciones que requieren transmisión rápida de datos, como la transmisión de audio y video en tiempo real.

- Otros Protocolos Importantes:

01. **Protocolo de Control de Acceso al Medio (MAC)**:

MAC es un protocolo de la capa de enlace de datos que se utiliza para controlar el acceso al medio de transmisión compartido, como Ethernet. Define reglas para la detección de colisiones y la asignación de direcciones MAC únicas a dispositivos de red.

02. **Protocolo de Resolución de Direcciones (ARP)**:

ARP es un protocolo utilizado para mapear direcciones IP a direcciones MAC en una red local. Permite a los dispositivos encontrar la dirección MAC asociada a una dirección IP específica antes de enviar un paquete de datos.

03. **Protocolo de Control de Internet (ICMP)**:

ICMP es un protocolo utilizado para enviar mensajes de control y error entre dispositivos en una red IP. Utilizado para el diagnóstico de problemas de red y la comunicación de errores, como el famoso “ping” para probar la conectividad.

- Evolución y Futuro de los Protocolos de Internet:

Los protocolos de internet están en constante evolución para adaptarse a las necesidades cambiantes de las redes modernas.

La transición de IPv4 a IPv6 está en marcha para abordar la escasez de direcciones IP y proporcionar un espacio de direcciones más grandes y eficientes.

3.4. Puertos

- ¿Qué son los Puertos?

Los puertos son puntos de acceso numerados que permiten a los dispositivos de red comunicarse entre sí a través de una red de computadoras.
Cada servicio o aplicación utiliza un puerto específico para enviar y recibir datos.

- Importancia de los Puertos:

Facilitan la comunicación entre aplicaciones y servicios en una red.
Permiten que múltiples servicios se ejecuten simultáneamente en un mismo dispositivo sin interferir entre sí.

- Puertos Bien Conocidos:

Puertos Bien Conocidos (Well-Known Ports): Van del puerto 0 al puerto 1023.
Reservados para servicios estándar y ampliamente utilizados.
Ejemplos:
Puerto 80: HTTP (Protocolo de Transferencia de Hipertexto).
Puerto 443: HTTPS (HTTP Seguro).
Puerto 21: FTP (Protocolo de Transferencia de Archivos).
Puerto 22: SSH (Protocolo de Shell Seguro).

- Puertos Registrados y Puertos Dinámicos o Privados:

Puertos Registrados (Registered Ports):
Van del puerto 1024 al puerto 49151.
Asignados a aplicaciones específicas o servicios por la IANA (Autoridad de Números Asignados por Internet).

Puertos Dinámicos o Privados (Dynamic or Private Ports):
Van del puerto (49152 al puerto 65535).
Utilizados por aplicaciones cliente para establecer conexiones efímeras con servicios en puertos bien conocidos y registrados.

- Asociación Puerto-Servicio:

Cada puerto está asociado a un servicio o aplicación específica. Esta asociación se define en la IANA y se mantiene en un registro público de números de puertos asignados.

- Gestión de Puertos en un Firewall:

Los firewalls utilizan reglas de filtrado para permitir o bloquear el tráfico de red en función del puerto y otros criterios.
Las reglas de firewall pueden configurarse para permitir el acceso a servicios específicos solo a trajes de determinados puertos.

- Seguridad de Puertos:

Algunos puertos están asociados con servicios vulnerables y pueden ser un objetivo para ataques de seguridad, como escaneos de puertos y ataques de denegación de servicio (DoS).
Es importante asegurar y monitorear los puertos para proteger la red contra posibles amenazas.

4. Protocolos de Internet - (Avanzado)
    4.1. Proxy

- ¿Qué es un Proxy?:

Un proxy es un servidor intermediario que actúa como un punto de contacto entre los clientes y los servidores en una red.
Los clientes se conectan al proxy en lugar de conectarse directamente al servidor final.

- Importancia del Proxy:

Mejora el rendimiento al cachear contenido frecuentemente solicitado.
Aumenta la seguridad al filtrar y bloquear el tráfico no deseado.
Facilita el acceso a recursos restringidos por ubicación geográfica.

- Tipos de Proxy:

01. **Proxy Web**:

Utilizado para interceptar y gestionar el tráfico web. Puede filtrar contenido, realizar caché de páginas web y proteger contra amenazas en línea.

02. **Proxy de Reenvío**:

Actúa como intermediario entre los clientes y los servidores, enviando solicitudes en nombre de los clientes y reenviando respuestas a los clientes.

03. **Proxy Inverso**:

Utilizado para mejorar el rendimiento y la seguridad de los servidores web. Sirve como punto de entrada para los clientes y distribuye las solicitudes a servidores backend.

- Funcionamiento del Proxy:

01. **Solicitud del Cliente**:

Un cliente realiza una solicitud de conexión a través del proxy.

02. **Intermediación del Proxy**:

El proxy intercepta la solicitud y la reenvía al servidor correspondiente en nombre del cliente.

03. **Procesamiento en el Servidor**:

El servidor procesa la solicitud y envía una respuesta al proxy.

04. **Reenvío al Cliente**:

El proxy reenvía la respuesta al cliente original.

- Ventajas del Uso de Proxy:

01. **Caché de Contenido**:

Reduce el tiempo de carga de páginas web al almacenar en caché contenido estático y dinámico.

02. **Filtrado de Contenido**:

Bloquea el acceso a sitios web maliciosos o inapropiados mediante la configuración de reglas de filtrado.

03. **Anonimato en la Web**:

Oculta la dirección IP real del cliente al reenviar solicitudes a través del proxy, proporcionando anonimato en línea.

04. **Control de Acceso**:

Permite administrar el acceso a recursos de red al requerir autenticación para establecer conexiones a través del proxy.

- Implementación de Proxy:

01. **Software de Proxy**:

Se ejecuta en un servidor dedicado y proporciona funcionalidades de proxy, como Squid, Nginx y Apache.

02. **Appliances de Proxy**:

Dispositivos dedicados que se implementan en la red para gestionar el tráfico proxy, como hardware de firewall y balanceadores de carga

03. **Servicios de Proxy en la Nube**:

Ofrecen proxy como servicio en la nube para empresas y usuarios individuales, proporcionando acceso seguro y anonimato en línea.

- Consideraciones de Seguridad:

Es importante configurar el proxy correctamente para evitar posibles vulnerabilidades, como ataques de denegación de servicio (doS) y fuga de información.
Se deben implementar políticas de seguridad para controlar el acceso y la autenticación de usuarios en el proxy.

4.2. Virtual Private Network (VPN)

- ¿Qué es una VPN?:

Una Virtual Private Network (VPN) es una red privada virtual que permite a los usuarios enviar y recibir datos a través de una red pública como si estuvieran conectados directamente a una red privada.

- Importancia de las VPN:

Proporcionan seguridad y privacidad al cifrar el tráfico de red y ocultar la dirección IP del usuario.
Permiten el acceso seguro a recursos de red privados desde ubicaciones remotas o redes públicas.

- Tipos de VPN:

01. **VPN de Acceso Remoto**:

Permite a usuarios individuales o dispositivos remotos conectarse a una red privada desde ubicaciones externas, como el hogar o un café.

02. **VPN de Sitio a Sitio**:

Conecta dos o más redes privadas geográficamente separadas a través de una red pública, como Internet.

03. **VPN de Acceso de Usuario**:

Permite a los usuarios acceder a recursos de red privados mediante autenticación de usuario, independientemente de su ubicación.

- Funcionamiento de una VPN:

01. **Inicio de Sesión en la VPN**:

El usuario inicia sesión en la VPN utilizando credenciales de autenticación proporcionadas por el proveedor de VPN.

02. **Establecimiento de Conexión**:

La aplicación de VPN establece una conexión segura con un servidor VPN remoto utilizando un túnel cifrado.

03. **Transmisión de Datos**:
Todos los datos transmitidos entre el dispositivo del usuario y el servidor VPN se cifran y encapsulan dentro del túnel VPN.

04. **Salida a Internet**:
El servidor VPN reenvía las solicitudes de salida a Internet en nombre del usuario, ocultando su dirección IP real.

- Protocolos de VPN y Ventajas de las VPN:

Ventajas de las VPN:
Seguridad: Cifrado de extremo a extremo protege los datos contra el acceso no autorizado.
Privacidad: Oculta la dirección IP del usuario y protege su privacidad en línea.
Acceso Remoto: Permite a los usuarios acceder a recursos de red privados desde cualquier lugar con conexión a Internet.

Protocolos de VPN:
OpenVPN: Protocolo de código abierto que ofrece un equilibrio entre velocidad, seguridad y compatibilidad multiplataforma.
IPsec (Protocolo de Seguridad de Internet): Protocolo estándar para implementar VPNs seguras en redes IP.
L2TP/IPsec (Túnel de Capa 2/Protocolo de Seguridad de Internet): Combina las ventajas de L2TP e IPsec para proporcionar una conexión VPN segura y confiable.

- Consideraciones de Seguridad:

Es importante elegir un proveedor de VPN confiable que garantice la seguridad y privacidad de los datos del usuario.
Se deben implementar políticas de seguridad adicionales, como la autenticación de dos factores y el uso de contraseñas seguras.

4.3. Práctica VPN

ProtonVPN.

4.4. TOR, Surface web, Deep web y Dark net

- Introducción a TOR:

TOR (The Onion Router) es una red anónima que permite a los usuarios navegar por internet de forma segura y privada al enrutar el tráfico a través de una serie de servidores voluntarios en todo el mundo.

- Características de TOR:

Enmascara la dirección IP del usuario y cifra el tráfico de Internet, proporcionando anonimato en línea.
Permite acceder a recursos en la Surface Web, Deep Web, y Dark Net de manera anónima.

- Surface Web:

La surface Web es la parte de Internet que es accesible mediante motores de búsqueda convencionales y navegadores web estándar.
Incluye sitios web de uso común, como redes sociales, tiendas en línea, noticias y blogs.

- Características de la Surface Web:

La mayoría de los sitios web en la Surface Web son indexados por motores de búsqueda y están disponibles públicamente.
Los usuarios pueden acceder a estos sitios web sin necesidad de herramientas especiales de navegación.

- Deep Web:

La Deep Web es la parte de Internet que no está indexada por motores de búsqueda convencionales y no es fácilmente accesible para el público en general.
Incluye contenido protegido por contraseñas, bases de datos, archivos privados y otros recursos no indexados.

- Características de la Deep Web:

Requiere credenciales de acceso, como nombres de usuario y contraseñas, para acceder a la información.
Los usuarios pueden encontrar contenido en la Deep Web utilizando servicios de búsqueda especializados o navegadores TOR.

- Dark Net:

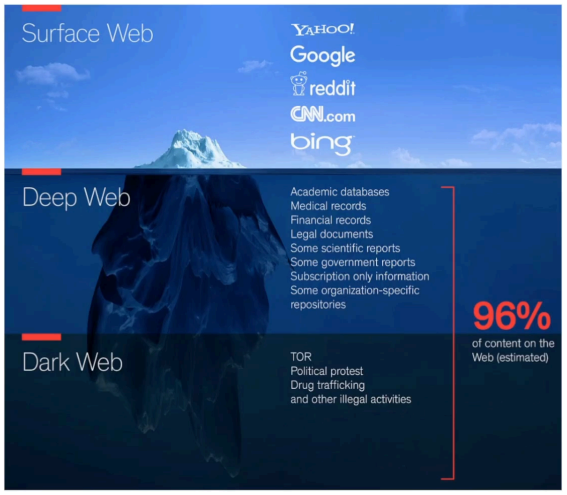
La Dark Net es una parte específica de la Deep Web que se utiliza para actividades ilícitas y anónimas.
Incluye mercados de drogas, foros de hacking, servicios de asesinato a sueldo y otras actividades criminales aún peor.

- Características de la Dark Net:

Los usuarios acceden a la Dark Net utilizando redes privadas y protocolos de anonimato, como TOR.
El contenido de la Dark Net es anónimo y no se puede rastrear fácilmente hasta su origen.

- Uso Responsable de TOR y las Profundidades de Internet:

TOR y las profundidades de Internet pueden ser herramientas poderosas para proteger la privacidad y la seguridad en línea.
Sin embargo, también pueden ser utilizadas para actividades ilegales y peligrosas.
Es importante utilizar estas herramientas de manera responsable y ética, respetando las leyes y normativas locales.



5. Checkpoints de contenidos
   - ¿Cuál es un componente esencial en cualquier red de computadoras?

Un router

   - ¿Qué tipo de red se caracteriza por no tener servidores ni clientes fijos, donde cada nodo puede actuar como cliente o servidor?

Red Peer-To-Peer (P2P)

   - ¿Qué término describe la capacidad máxima de datos que puede transmitir una red?

Ancho de Banda

   - En el contexto del modelo OSI, ¿qué capa se encarga del enrutamiento de paquetes a través de diferentes redes?

Capa de Red