Tema 1: Redes de Ordenadores

1.- Introducción

Lo primero que debemos establecer para abordar el resto de conceptos del tema es la definición de red. En Informática, una red de ordenadores es un conjunto de equipos independientes interconectados entre sí mediante algún medio de transmisión, y que se comunican y transmiten información.
En esta definición aparecen los conceptos de transmisión y comunicación, que son muy similares, pero presentan una sutil diferencia entre sí:

- Transmisión: Implica transportar una señal a través de un medio, sin interpretar los datos ni verificar su validez. Puede utilizar varios medios, como señales eléctricas u ondas inalámbricas.
- Comunicación: Se refiere a transportar información de un lugar a otro. Tanto el emisor como el receptor comprenden el mensaje transmitido. Siempre que hay comunicación, hay transmisión, pero no siempre que hay transmisión, hay comunicación.

Los elementos de un sistema de comunicación presentes en todas las redes son:

- Emisor: Envía la información a través de la red.
- Receptor: Toma la información emitida.
- Canal o medio de transmisión: El medio físico a través del cual se emite la información, como cables u ondas inalámbricas.
- El ruido se define como todas aquellas interferencias o perturbaciones presentes en el medio de transmisión.

El uso de redes en comparación con sistemas aislados presenta ventajas claras y recomendables. Facilita el intercambio y acceso a la información, evitando la duplicación de datos y reduciendo los costos al compartir recursos. Además, mejora la comunicación entre sistemas distantes, permitiendo una interacción efectiva como si estuvieran conectados directamente.

No obstante, el uso de redes plantea desafíos, especialmente en términos de seguridad. Los sistemas conectados a la red son más vulnerables a ataques cibernéticos, lo que puede comprometer la información y permitir el acceso no autorizado al sistema. Por lo tanto, es crucial implementar medidas de protección para minimizar los riesgos de seguridad al operar en entornos de red.

2,.Tipos de redes:

1. **Según nivel de conectividad:**
    - **Sistemas aislados:** Se refiere a sistemas informáticos que operan de forma independiente sin conexión con otros sistemas. No tienen capacidad para compartir información.
    - **Sistemas en red:** Son las redes más comunes en las que los equipos están conectados directa o indirectamente, permitiendo el intercambio de información entre ellos.
    - **Sistemas distribuidos:** Consisten en un grupo de sistemas informáticos interconectados que actúan como una sola unidad, aunque internamente tengan una arquitectura más compleja. Se utilizan para aumentar el rendimiento y la tolerancia a fallos.
2. **Según el tipo de servicios:**
    - **Redes cliente/servidor:** En estas redes, un equipo asume el papel de servidor, ofreciendo servicios a los clientes que solicitan recursos o datos. Los servicios pueden incluir servidores de archivos, web, impresión, DHCP, DNS, entre otros.
    - **Redes entre iguales (P2P):** En este tipo de red, todos los equipos pueden actuar tanto como clientes como servidores. Cada equipo puede ofrecer y solicitar recursos de otros equipos en la red. Este modelo es común en entornos domésticos.
3. **Según quién puede usarlas:**
    - **Redes públicas:** Son redes accesibles para cualquier persona, como Internet. Están formadas por sistemas informáticos interconectados que permiten compartir información y comunicar a usuarios sin importar su ubicación geográfica.
    - **Redes privadas (Intranets):** Estas redes están restringidas a un grupo específico de usuarios y son comunes en entornos empresariales. Contienen recursos puestos a disposición de los usuarios por la organización propietaria de la red.
4. **Según el medio de transmisión:**
    - **Redes cableadas:** Utilizan medios físicos como cables de par trenzado, cables coaxiales o fibra óptica para transmitir información entre los equipos.

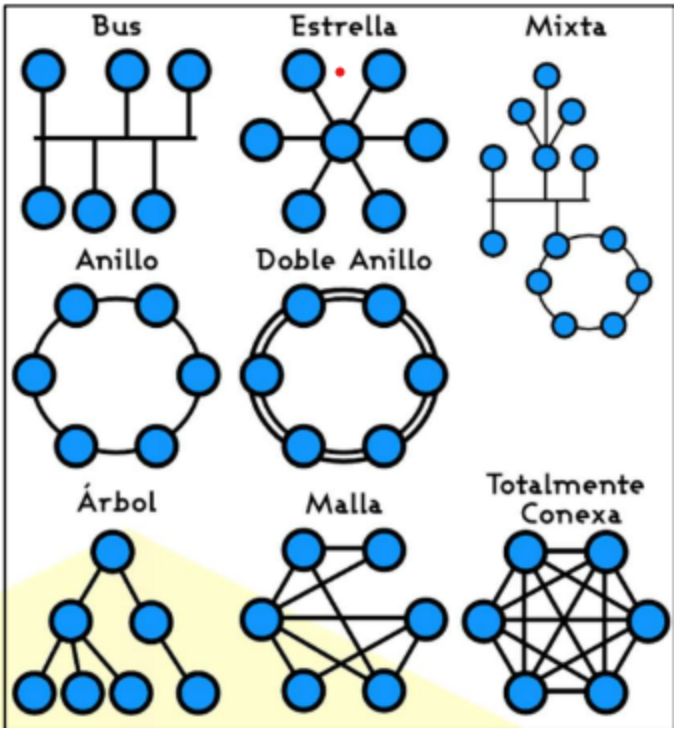
- **Redes inalámbricas:** Emplean ondas electromagnéticas en lugar de medios físicos para la transmisión de información, lo que permite la comunicación sin la necesidad de cables.

5. **Según el área geográfica:**
    - **PAN (Personal Area Network):** Estas redes tienen un alcance muy limitado, generalmente de unos pocos metros, y conectan dispositivos de usuario cercanos entre sí, como teléfonos móviles, tablets, dispositivos Bluetooth y ordenadores portátiles en entornos domésticos.
    - **LAN (Local Area Network):** Abarcan un área mayor que las PAN, como una planta de un edificio o un edificio completo. Son comunes en entornos empresariales.
    - **WAN (Wide Area Network):** Son redes que unen diferentes LAN y pueden abarcar áreas extensas, como países o continentes. Se utilizan comúnmente en servicios de Internet ofrecidos por proveedores de servicios de Internet.

Topologías de redes:

- **Bus:** En esta topología, todos los equipos están conectados a un mismo medio físico, como un cable principal. Si el bus se rompe, toda la red queda inoperable.
- **Estrella:** Todos los equipos están conectados a un punto central de interconexión, como un switch. Si el elemento central falla, la red puede quedar inoperable, y la saturación del elemento central puede ralentizar el rendimiento de la red.
- **Anillo:** Los equipos están organizados en una estructura de anillo, y la información viaja a través de cada equipo en el anillo para alcanzar su destino. La variante en anillo doble implementa dos anillos independientes para mejorar la tolerancia a fallos y la flexibilidad de la red.
- **Malla:** Todos los elementos están conectados punto a punto con uno o más de los demás elementos de la red, lo que garantiza una ruta de comunicación alternativa en caso de falla en algún segmento de la red.
- **Árbol:** Es una variante de la topología en bus donde múltiples líneas de buses se conectan a un bus central. Intenta brindar mayor tolerancia a fallos en comparación con las redes en bus estándar.
- **Topologías mixtas:** Son redes que incluyen segmentos de al menos dos tipos de topologías, lo que permite combinar las fortalezas de diferentes modelos de

red según los requisitos específicos.



Topologías lógicas de red:

- **Multidifusión (o broadcast):** En esta topología, cada equipo envía sus datos a todos los demás equipos en la red sin discriminar su destino. No hay un orden específico que los equipos deban seguir para utilizar la red.
- **Paso de testigo (o transmisión de tokens):** Esta topología controla el acceso a la red enviando un "testigo" electrónico de manera secuencial a cada equipo. Solo cuando un equipo recibe el testigo puede enviar datos a través de la red. Si el equipo no tiene datos para enviar cuando recibe el testigo, lo pasa al siguiente equipo, repitiendo el proceso.

3.- Arquitectura de una red

La arquitectura de red en informática se refiere a la forma en que los elementos de la red se conectan y se comunican entre sí. Esta arquitectura incluye el acceso al medio, que establece las reglas para el uso del medio físico, y los protocolos de comunicación, que son conjuntos de reglas que regulan aspectos específicos de la comunicación.

Para garantizar una comprensión eficiente y un funcionamiento fluido, la arquitectura de red se divide en capas, donde cada capa se encarga de una función específica en el proceso de comunicación. Estas capas se comunican a través de interfaces

estandarizadas, lo que significa que no necesitan conocer los detalles de las otras capas para operar de manera efectiva.

3.1.-El modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos) propuesto por la ISO, es un modelo teórico que ha influido significativamente en el desarrollo tecnológico de las redes. Se compone de 7 niveles o capas, divididas en niveles orientados a la red y niveles orientados al usuario. La capa de transporte actúa como intermediaria entre las capas inferiores y superiores.

1. **Nivel Físico:** Se encarga de la transmisión de la señal a nivel de bits y maneja los aspectos físicos concretos de la transmisión, como la intensidad de la señal y los tipos de cables.
2. **Nivel de Enlace:** Asegura la transmisión libre de errores dividiendo la información en tramas y solicitando reenvíos de tramas corruptas o duplicadas. Maneja problemas de flujo de datos.
3. **Nivel de Red:** Se ocupa del encaminamiento y establecimiento de rutas óptimas para la transmisión de la información, trabajando a nivel de paquete.
4. **Nivel de Transporte:** Actúa como intermediario entre las capas de red y sesión, fragmentando la información de la capa de sesión para que sea aceptada por la capa de red. Trabaja a nivel de segmentos.
5. **Nivel de Sesión:** Inicia una sesión para cada comunicación establecida y pasa la información hacia las capas inferiores, incluyendo información específica de la comunicación.
6. **Nivel de Presentación:** Se encarga de la sintaxis y semántica de la información, facilitando la comunicación entre las partes al "traducir" la información de manera comprensible.
7. **Nivel de Aplicación:** Define los protocolos utilizados por las aplicaciones y procesos de usuario. Es la capa más cercana al usuario y define los protocolos cruciales para los usuarios que utilizan las redes.

El modelo OSI, al establecer claramente las funciones de cada capa, facilita la comprensión general del funcionamiento de las redes.

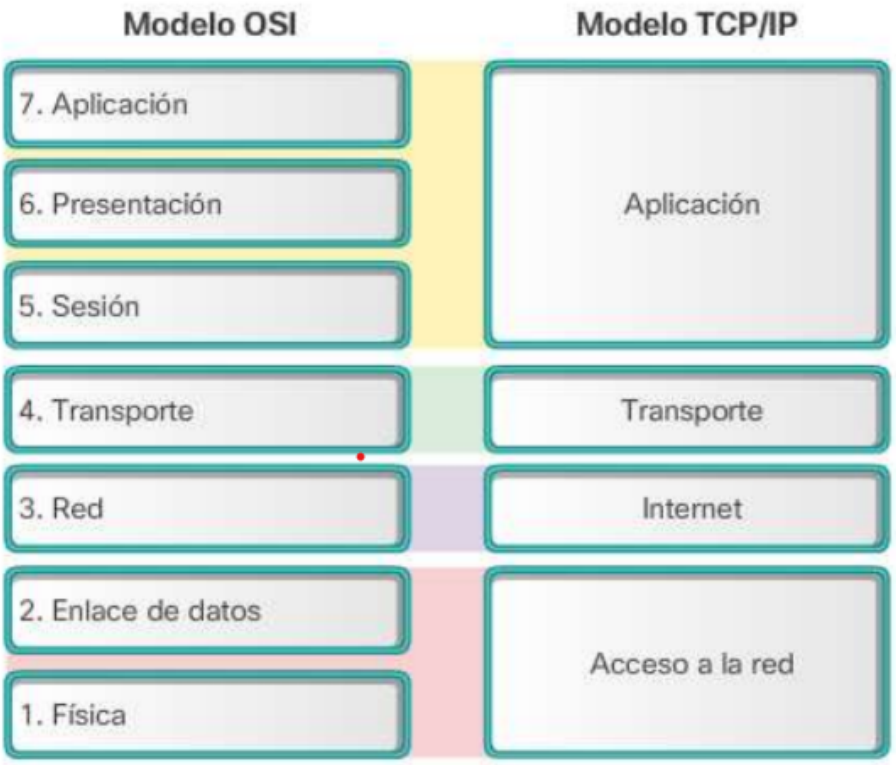
3.2.- modelo TCP/IP

El modelo TCP/IP, desarrollado por Vinton Cerf y Robert Kahn en los años 70 para su uso con ARPANET, la primera WAN de la historia, es la base de las

comunicaciones en Internet y está compuesto por 4 niveles: Capa de Acceso al Medio, Capa de Internet, Capa de Transporte y Capa de Aplicación. Las capas superiores del modelo OSI se corresponden con la capa de aplicación TCP/IP, mientras que las inferiores se relacionan con la capa de Acceso al Medio y la capa de Internet.

- **Capa de Acceso al Medio:** Define las características físicas de los medios de transmisión utilizados en la red, como Ethernet (IEEE 802.3) para redes cableadas y IEEE 802.11 para redes inalámbricas. También incluye soporte para tecnologías LAN y WAN, como Ethernet, ATM y Frame Relay.
- **Capa de Internet:** Ofrece servicios de direccionamiento, empaquetado y enrutamiento. El Protocolo de Internet (IP) es fundamental para proporcionar funciones de direccionamiento, enrutamiento y fragmentación/reensamblado de paquetes. Otros protocolos importantes en esta capa son ARP (Protocolo de Resolución de Direcciones) y ICMP (Protocolo de Mensajes de Control de Internet).
- **Capa de Transporte:** Proporciona servicios de sesión y comunicación de datagramas a la capa de aplicación. Aquí, el Protocolo de Control de Transmisión (TCP) garantiza una conexión fiable punto a punto y recupera paquetes perdidos, mientras que el Protocolo de Datagramas de Usuario (UDP) se utiliza para transferencias no fiables.
- **Capa de Aplicación:** Incluye una amplia variedad de protocolos para los usuarios de las redes, como HTTP para visualizar páginas web, DNS para la traducción de nombres de dominio en direcciones IP, DHCP para asignar direcciones IP automáticamente, SMTP para el envío y recepción de correo electrónico, FTP para la transferencia de archivos, SSH para sesiones de conexión remota segura, y RIP para el enrutamiento eficiente hacia un destino determinado.

Estos protocolos en conjunto permiten el funcionamiento eficiente de las redes y una comunicación efectiva entre los dispositivos conectados.



4.- Capa de Acceso al Medio

En el nivel físico de una red, se establecen los tipos de medios de transmisión, así como sus características generales, como el voltaje necesario para representar valores binarios y la modulación de los datos. Los medios físicos pueden ser guiados, donde la señal se transmite a través de un cable, o no guiados, donde la señal se propaga libremente en el ambiente. A continuación, se describen brevemente los dos tipos de medios:

4.1.1.- Medios guiados:

a) **Cable par trenzado:** Compuesto por hilos de cobre entrelazados, se divide en diferentes tipos como UTP, FTP y STP, que varían en su capacidad de protección contra interferencias externas. Los cables de categoría 5, 5e, 6, 6a y 7 se utilizan en redes de diferentes velocidades, desde 100 Mb/s hasta 10,000 Mb/s.

1. **UTP (Unshielded Twisted Pair):** Se trata de hilos de cobre sin protecciones metálicas. Aunque son los más económicos, también presentan la mayor cantidad de interferencias.
2. **FTP (Foiled Twisted Pair):** Este tipo de cable cuenta con una malla de protección que cubre todos los cables de cobre en bloque, lo que proporciona cierta protección contra interferencias.

3. **STP (Shielded Twisted Pair):** Se distingue por una malla metálica que recubre cada pareja de hilos de cobre. Aunque es más costoso y rígido en comparación con los anteriores, su estructura lo hace menos vulnerable a interferencias externas.

b) **Cable coaxial:** Aunque ha sido reemplazado en gran medida por el par trenzado, sigue siendo utilizado en redes de topología de bus y en la señal de televisión analógica. Está compuesto por un núcleo de cobre recubierto por una malla metálica y un plástico protector.

c) **Fibra óptica:** Emite señales ópticas y no se ve afectada por interferencias electromagnéticas, lo que le permite tener tasas de transferencia de datos elevadas y distancias de cable significativas. Sin embargo, es más costosa y frágil en comparación con otros medios de transmisión.

4.1.2.- Medios no guiados:

En estos medios, la señal se propaga libremente en el ambiente sin un cable que la contenga. Se utilizan en comunicaciones inalámbricas y pueden ser unidireccionales u omnidireccionales. Algunos ejemplos de medios no guiados son las ondas de radio, las transmisiones vía satélite, las comunicaciones infrarrojas, el Bluetooth y las redes locales inalámbricas (Wi-Fi).

4.2.- Nivel de enlace

El nivel de enlace se divide en dos subniveles: el de enlace lógico (LLC) y el de acceso al medio (MAC). Ambos subniveles proporcionan servicios a la capa superior, realizan el entramado de tramas, controlan errores y gestionan el flujo de datos. El estándar más común en este nivel es el IEEE 802.2 para el subnivel LLC, mientras que en el subnivel MAC, varía según el tipo de red.

El nivel de enlace se encarga de diversas funciones:

- **Ofrecer servicios a la capa superior:** Puede ofrecer servicios orientados a conexión que establecen un vínculo con el receptor para intercambiar información sobre el estado de la transmisión, o servicios no orientados a conexión que son más rápidos pero menos confiables, especialmente en redes con baja tasa de errores.
- **Entramado:** Agrupa los bits del subnivel físico en bloques llamados tramas, con un formato específico conocido por el emisor y el receptor. Además, delimita las tramas para que el receptor identifique su inicio y fin.
- **Control de errores:** Implementa mecanismos para detectar errores en las tramas recibidas, como chequeos de paridad o códigos de redundancia cíclica

(CRC). También facilita la retransmisión de tramas perdidas o dañadas.

- **Control de flujo:** Regula la velocidad de transmisión de tramas para evitar que un emisor rápido sature a un receptor más lento, asegurando un flujo de datos equilibrado.

En el contexto de las redes Ethernet, basadas en el estándar IEEE 802.3, el cable de par trenzado es el medio de transmisión principal, aunque también se emplea la fibra óptica para velocidades más altas. Estas redes generalmente siguen una topología de estrella, con un dispositivo central como un switch o un router coordinando las transmisiones. Anteriormente, se utilizaba el protocolo CSMA/CD para evitar colisiones, pero con el control inteligente de tráfico de los switches modernos, este protocolo ha quedado obsoleto en gran medida.

Las tramas Ethernet tienen un formato específico que incluye:

- **Preámbulo:** Una secuencia de 56 bits alternando unos y ceros para sincronizar los relojes de los dispositivos de la red.
- **Delimitador de inicio:** Indicador del comienzo de la trama, correspondiente a la secuencia 10101011 en binario.
- **MAC de destino/origen:** Direcciones físicas de los dispositivos receptor y emisor de la trama.
- **802.1Q:** Campo opcional que se utiliza para redes VLAN y contiene la información correspondiente.
- **Protocolo:** Indica a qué protocolo pertenece la información encapsulada en la trama.
- **Datos:** La carga útil de la trama, correspondiente a la información que se transmite, con un tamaño variable de hasta 1500 Bytes.
- **FCS (Frame Check Sequence):** Una secuencia de comprobación de trama que se utiliza para detectar errores en la trama recibida.
- **Espacio entre tramas:** Un tiempo de reposo en la línea de comunicaciones para permitir que el receptor se prepare para otra trama o facilitar la sincronización de la siguiente trama.

Durante la autonegociación al inicio de la transmisión, el emisor y el receptor intercambian información sobre el modo de transmisión, los protocolos a utilizar y la velocidad.

- IEEE 802.3 (Ethernet). Sobre todo para LAN en estrella con pable de car trenzado, aunque también tiene versiones con fibra óptica.
- IEEE 802.11 (Wi-Fi). Para LAN inalámbricas.
- IEEE 802.15 (Bluetooth). Para redes de área personal inalámbricas.

4.2.2 sobre LAN inalámbricas (Wi-Fi):

Las redes inalámbricas son populares debido a su fácil instalación y menor costo, a pesar de tener velocidades de transmisión más lentas que las redes cableadas. Sin embargo, la seguridad es un desafío, ya que son más vulnerables a intrusiones. Las redes Wi-Fi operan en diferentes rangos de frecuencia, como 2,4 GHz y 5 GHz, con múltiples canales que buscan reducir interferencias y mejorar la calidad de la señal.

El estándar para las redes WLAN (Wireless LAN) es el IEEE 802.11. Este estándar ha ido presentando constantes evoluciones en sus protocolos, entre las cuales destacaremos las siguientes:

1. IEEE 802.11b: Primer estándar Wi-Fi con un ancho de banda de 11 Mbps, publicado en 1999.
2. IEEE 802.11g: Mejora significativa del protocolo con una velocidad de hasta 54 Mbps utilizando la misma banda que 802.11b, publicado en 2003.
3. IEEE 802.11n: Aumenta la velocidad de transmisión hasta 600 Mbps con una duplicación de la frecuencia de transmisión para encapsular múltiples transmisiones simultáneas, publicado en 2009.
4. IEEE 802.11ac: Mejoras en la banda de 5 GHz permiten alcanzar velocidades de 1.3 Gbps, compatible con estándares anteriores de la familia 802.11, publicado en 2014.
5. IEEE 802.11ax: Introduce el uso de señales de 6 GHz para mejorar el rendimiento de la señal con una velocidad típica de 3.5 Gbps y una velocidad pico teórica de hasta 14 Gbps, aún en desarrollo con pocos dispositivos que lo admiten completamente, con la especificación final publicada en 2021.
6. Otros estándares: Destacando IEEE 802.11be, o Wi-Fi7, desarrollado a partir de 802.11ax y aún en desarrollo.

En las redes inalámbricas, se utiliza el protocolo CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, Acceso múltiple con detección de portadora y prevención de colisiones) como un método de acceso al medio. A diferencia de CSMA/CD utilizado en Ethernet, en las redes inalámbricas no se pueden detectar

todas las colisiones, lo que resulta en un enfoque menos estricto y un mayor número de retransmisiones de tramas. Esto se debe a la incapacidad de siempre detectar si otros nodos de la red están transmitiendo, ya que podrían estar demasiado lejos del emisor, y a las interferencias propias del medio de transmisión.

5.- Capa de Internet

En el modelo TCP/IP, la capa de Internet tiene tres funciones fundamentales:

- Para los paquetes recibidos, recabar su información y pasarlos a la capa de transporte si procede
- Para los paquetes emitidos, decidir cuál es el siguiente “salto” en su camino hacia el dispositivo destino (encaminamiento)
- Proporcionar capacidad de diagnóstico y detectar errores en la red
  En este nivel, la unidad de información ya no es la trama, sino el paquete.

En el protocolo IP, que es el que se utiliza en el modelo TCP/IP, los paquetes IP también se denominan datagramas.

5.1protocolo IP

El **protocolo IP** es el protocolo más importante de la capa de Internet. Se encarga de enviar paquetes a través de la red utilizando direcciones IP para identificar al emisor y receptor. Con su función de encaminamiento, permite que los paquetes salten de una red a otra, lo que en la práctica es lo que permite el funcionamiento de Internet. En la actualidad, la cuarta versión del protocolo, **IPv4**, es la que domina el tráfico en Internet, aunque la sexta versión, **IPv6**, lleva años implantada en numerosas redes y acabará sustituyendo a IPv4 debido sobre todo a la falta de direcciones IPv4 disponibles en la actualidad1.

El protocolo IP direcciona a los equipos de la red mediante las direcciones IP, encapsula datos procedentes de otras capas en datagramas IP, y también los fragmenta y reensambla si su tamaño es excesivo para poder transmitirse a través de la red. Por si esto fuera poco, también decide la ruta que deben seguir los datagramas para llegar a su destino mediante tablas de enrutamiento, que están también expresadas en función de direcciones IP. Como los datagramas pueden llegar desordenados si han seguido rutas diferentes, IPv4 también tiene la capacidad de recomponer los datagramas fragmentados aunque no lleguen en orden. Una de las grandes ventajas de IP es su flexibilidad, capaz de adaptarse a condiciones cambiantes en una red, donde a cada instante pueden desconectarse

nodos o conectarse otros nuevos. El protocolo IP es “no fiable”, lo cual significa que no se comprueba que los datagramas llegan a su destino con éxito; esta labor se deja a los protocolos de capas superiores1.

5.1.1 direcciones IP

Las **direcciones IP** son identificadores de cada interfaz de red emisor o receptor en el nivel de Internet. Cada dispositivo tendrá un número diferente para evitar ambigüedades. La dirección IP de un dispositivo puede modificarse o ir variando por las necesidades de la red, o porque nos conectemos a redes diferentes. Esto las diferencia de las direcciones MAC, de nivel inferior, que siempre se mantienen fijas.

En la versión **IPv4** del protocolo, las direcciones tienen 32 bits, presentados como 4 grupos de 8 bits separados por un punto. Algunas direcciones IP están reservadas para propósitos específicos y por tanto no pueden utilizarse para nombrar dispositivos. Algunas de ellas son:

- **127.X.X.X**: También conocida como dirección de bucle local o loopback, direcciona al propio dispositivo que emite o recibe la transmisión.
- **Dirección de broadcast**: Es una dirección especial que sirve para identificar a todos los equipos de la red.
- **0.0.0.0**: Esta dirección está reservada y representa una convención en las tablas de enrutamiento.
- **Direcciones privadas**: El principal problema de las direcciones IPv4 es su escasez; hay tantos dispositivos que no es posible tener.

o 10.X.X.X
o Desde 172.16.0.0 hasta 172.31.255.255
o 192.168.X.X
o 169.254.X.X Este grupo de direcciones está reservado para fallos en un protocolo llamado DHCP, que mencionaremos en el apartado 7 de este mismo tema.

- Direcciones reservadas. Aparte de las ya mencionadas, muchas direcciones IP están reservadas para usos futuros o fines especiales.

Las direcciones IPv4 están cerca de agotarse desde hace tiempo. Se han utilizado estrategias como NAT o CIDR para prolongar la vida del direccionamiento IPv4, pero antes o después tendrá que ser sustituido. En la versión 6 del protocolo IP, IPv6, las direcciones IP tienen 128 bits, lo cual da un total de aproximadamente 3,4 · 10^28 direcciones posibles. Es un número inmenso y más si lo comparamos con los 4300

millones de direcciones diferentes que pueden usarse con IPv4. Las direcciones IPv6 se suelen presentar como 8 grupos de 4 dígitos hexadecimales. Un ejemplo de dirección IPv6 sería algo como FDE9:BA98:0074:3210:001F:0077:0000:FFB1. Como salta a la vista, son bastante más complejas y difíciles de manejar que las direcciones IPv4.

El problema de IPv6 es que aún no está extendido en todas las redes, si bien su penetración crece año tras año. La mayor complejidad del direccionamiento IPv6 con las dificultades para el trabajo de los administradores de red que ello conlleva, así como el coste de la transición al nuevo modelo son las principales causas de esta (relativa) falta de implantación. A pesar de ello, ya existen numerosos mecanismos de transición en marcha para adaptar redes que sólo usan IPv4 y permitir que funcionen en entornos IPv6, y viceversa. De este modo, mucho del tráfico que circula por las redes WAN ya es IPv6, incluso si en origen la comunicación está utilizando direcciones IPv4. El tiempo dirá si finalmente IPv6 hace desaparecer a las direcciones IPv4, aunque no parece que vaya a suceder próximamente.

5.1.2 datagrama IP

El datagrama es la unidad de información que se transmite en el nivel de protocolo IP. Está compuesto por una cabecera y los datos propiamente dichos. El formato del encabezado de un datagrama IPv4 consta de 14 campos, donde el campo de "Opciones" es opcional. A continuación se detallan las funciones de cada uno de estos campos:

1. **Versión:** Indica la versión del protocolo IP que se está utilizando.
2. **IHL (Internet Header Length):** Representa la longitud de la cabecera de Internet. Dado que la longitud de la cabecera del datagrama puede variar, este campo es necesario para conocer el tamaño específico del datagrama.
3. **Tipo de servicio:** Se refiere a los servicios diferenciados que garantizan la calidad de las prestaciones en redes grandes como Internet. Este campo especifica parámetros de esos servicios.
4. **Longitud del paquete:** Indica el tamaño total del datagrama, incluyendo la cabecera y los datos.
5. **Identificación:** Es un número que identifica al datagrama y se utiliza cuando se necesita fragmentar el datagrama a través de la red. Ayuda a identificar a qué datagrama pertenece cada fragmento recibido.

6. **Flags:** Son bits utilizados para manejar los datagramas fragmentados y determinar, por ejemplo, si el datagrama no permite fragmentación o si es un fragmento de un datagrama más grande. En IPv6, estos campos no son necesarios ya que los datagramas no se fragmentan.
7. **Desplazamiento de fragmentos:** Indica la posición que ocupa el fragmento dentro del datagrama completo. Ayuda a recomponer un datagrama fragmentado en su orden original.
8. **Tiempo de vida (TTL, Time to Live):** Indica el número máximo de saltos que el paquete puede realizar a través de la red. Se decrementa en uno cada vez que el datagrama pasa por un enrutador hacia su destino. Si llega a 0, el paquete se descarta para evitar bucles infinitos.
9. **Protocolo:** Indica el protocolo de nivel superior al que corresponde el contenido del datagrama.
10. **Checksum del encabezado:** Sirve para verificar que la cabecera se ha recibido sin errores. Consiste en una suma de verificación de la cabecera completa que el receptor realizará para verificar la integridad del datagrama.
11. **Dirección de origen:** Representa la dirección IP desde la que parte el datagrama.
12. **Dirección de destino:** Representa la dirección IP a la que debe llegar el datagrama.
13. **Opciones:** Campo opcional que suele contener parámetros específicos sobre los datagramas, como opciones de enrutamiento.
14. **Relleno:** Si es necesario, se incluyen bits al final de la cabecera para que su tamaño sea un múltiplo de 32 y sea más fácil de manejar.

5.1.3 enrutamiento IP

El enrutamiento IP implica determinar la ruta adecuada para enviar un datagrama a su destino. Este proceso se basa en tablas de enrutamiento que indican la puerta de enlace para destinos específicos y una ruta predeterminada para paquetes fuera de la red local. Se utilizan diversos protocolos de enrutamiento como RIP, EGP y el más común en Internet, BGP. El enrutamiento IP es fundamental para garantizar un envío eficiente y seguro de datos a través de redes complejas.

5.2 otros protocolos

1. **ICMP (Internet Control Message Protocol):** Protocolo para enviar mensajes de error o información sobre el estado de la red, como confirmaciones de conectividad y notificaciones de errores como la inaccesibilidad del destino de un paquete.
2. **IGMP (Internet Group Management Protocol):** Protocolo para la gestión de mensajes en modo de multidifusión (broadcast), útil para administrar grupos en la red, especialmente en aplicaciones de streaming de audio/vídeo y comunicaciones de grupo.
3. **IPsec (IP Security):** Conjunto de protocolos de encriptación y autenticación de datagramas IP que aseguran las comunicaciones en redes públicas como Internet. Se utiliza especialmente en redes privadas virtuales (VPN) para establecer conexiones seguras punto a punto entre emisores y receptores.

6.- Capa de Transporte

Comunicaciones orientadas a conexión: Establecimiento de una conexión entre emisor y receptor para el intercambio de datos de manera continua y secuencial.

1. **Comunicaciones fiables:** Garantía de la entrega exitosa de datos mediante la retransmisión de segmentos con errores o la solicitud de retransmisión de segmentos perdidos.
2. **Entrega en orden:** Asegurar que los segmentos se reciben en el orden correcto, evitando la entrega desordenada de datos al nivel de aplicación.
3. **Control de congestión:** Implementación de mecanismos para evitar la sobrecarga de nodos congestionados en la red, asegurando una transmisión fluida.
4. **Control de flujo:** Ajuste de la velocidad de envío de segmentos para que coincida con la capacidad del receptor, evitando la congestión de la red y el rechazo de segmentos.
5. **Multiplexación:** Uso de puertos para establecer múltiples conexiones con el mismo origen/destino, permitiendo el uso de varios servicios del nivel de aplicación simultáneamente.

En cuanto a los protocolos de transporte, TCP y UDP son los más comunes en Internet, aunque para el futuro estándar de la World Wide Web, HTTP/3, se implementará el protocolo de transporte QUIC (Quick UDP Internet Connections) en lugar de TCP. Este cambio ha sido impulsado por Google para mejorar la velocidad y la seguridad de las conexiones en Internet.

6.1.- Protocolo TCP

TCP (Transmission Control Protocol) es el protocolo de transporte más utilizado en Internet, proporcionando comunicación confiable y orientada a la conexión. Asegura que los segmentos lleguen en orden, pero su enfoque en la confiabilidad puede ralentizar la transmisión en comparación con otros protocolos. Establece conexiones utilizando puertos y direcciones IP, utiliza temporizadores y retransmisiones para garantizar una transmisión segura y fiable, y su cabecera contiene información esencial como direcciones IP de origen y destino, puertos, y mensajes específicos del protocolo.

La cabecera de un segmento TCP contiene varios elementos esenciales para su funcionamiento, que incluyen:

1. **Puerto de origen/destino:** Identifica el número de puerto de la transmisión.
2. **Número de secuencia:** Utilizado para ordenar los segmentos y garantizar la entrega en orden.
3. **Número de acuse de recibo:** Indica hasta qué segmento se han confirmado como recibidos en el destino de la transmisión.
4. **HLEN (Longitud de la cabecera):** Especifica el tamaño de la cabecera, que puede variar.
5. **Reservado:** Espacio para posibles usos futuros, aunque en la práctica no se utiliza.
6. **Bits de control o bits de código:** Identifican segmentos especiales necesarios para operaciones específicas relacionadas con el protocolo.
7. **Tamaño de ventana:** Indica cuánta información está dispuesto a aceptar el receptor, lo que ayuda en el control de flujo de datos.
8. **Suma de verificación (Checksum):** Se utiliza para verificar la integridad de la cabecera y asegurar que no ha llegado con errores.
9. **Puntero de urgencia:** Activado si el contenido del segmento se marca como urgente.
10. **Opciones:** Almacena parámetros específicos de la transmisión, aunque no siempre están presentes.
11. **Relleno:** Se agregan ceros al final del segmento para que el tamaño de la cabecera sea un múltiplo de 32 bits, lo que facilita su manejo.

6.2.- Protocolo UDP

UDP, o Protocolo de Datagrama de Usuario (User Datagram Protocol), se desarrolló como un complemento de TCP para atender a protocolos en niveles superiores donde la velocidad de transmisión es más crítica que la precisión. A diferencia de TCP, UDP no es orientado a conexión, lo que significa que no se dedica tiempo a establecer conexiones y negociar características, lo que ahorra tráfico. Sin embargo, no se verifica si los segmentos llegan a su destino, si hay errores en los datos o si llegan en orden.

Este protocolo es mucho más simple que TCP, proporcionando menos servicios a la capa superior para evitar la sobrecarga de información de control que requiere TCP, sacrificando su confiabilidad. Se utiliza en entornos donde la confiabilidad de la red subyacente es alta o donde es esencial que los segmentos lleguen a su destino, aunque pueda haber pérdida de calidad, como en sistemas de tiempo real o transmisiones de multimedia en directo (streaming). Algunos protocolos que emplean UDP son DNS y DHCP.

A diferencia de TCP, UDP no garantiza la entrega en orden ni tiene control de congestión, pero ofrece funciones de broadcast y multicast, lo que lo hace ideal para transmisiones en tiempo real. La cabecera de un segmento UDP es más simple que la de TCP, lo que permite una transmisión más rápida debido a su tamaño más reducido.

7.- Capa de Aplicación

La capa de aplicación en el modelo TCP/IP es el nivel superior que contiene una variedad de protocolos para satisfacer las necesidades de los usuarios y aplicaciones. Aprovecha la fiabilidad de la capa de transporte TCP y se enfoca en los detalles específicos de cada protocolo de comunicación. Aunque hay una gran cantidad de protocolos en esta capa, nos centraremos en los más importantes y ampliamente utilizados para diversos servicios y aplicaciones.

7.1.- Protocolo HTTP

HTTP (Protocolo de Transferencia de Hipertexto) es el protocolo que permite la visualización de páginas web en Internet, operando en un modelo cliente/servidor. Utiliza el puerto TCP 80 para las comunicaciones estándar y consiste en intercambios de mensajes sencillos entre el cliente y el servidor para proporcionar contenido web.

La versión segura de HTTP, llamada HTTPS, permite la transferencia de datos de manera cifrada, lo que impide que terceros puedan interpretar los mensajes. En

HTTPS, los mensajes se encriptan durante la transmisión y se descifran en el destino, asegurando que solo el emisor y el receptor puedan interpretarlos. Las comunicaciones HTTPS generalmente utilizan el puerto TCP 443.

7.2.- Protocolo DNS

El protocolo DNS (Sistema de Nombres de Dominio) traduce direcciones IP a nombres de dominio para facilitar la accesibilidad en Internet. Funciona como una base de datos distribuida que almacena nombres de dominio junto con sus direcciones IP correspondientes. Los servidores DNS resuelven las peticiones de los usuarios para establecer conexiones, y cada proveedor de servicios de Internet proporciona servidores DNS a sus usuarios para facilitar la navegación web.

El sistema DNS opera de manera jerárquica, con servidores raíz y niveles superiores que gestionan las consultas de nombres de dominio. Los servidores raíz, ampliamente distribuidos y replicados, garantizan la seguridad del sistema. El protocolo DNS utiliza los puertos TCP y UDP con el número 53, aunque la mayoría de las operaciones se realizan a través del puerto UDP.

7.3.- Protocolo DHCP

El protocolo DHCP (Dynamic Host Control Protocol) asigna automáticamente direcciones IP y otros parámetros de red a equipos en una red local. Funciona como un protocolo cliente/servidor, asignando direcciones IP dinámicas de un pool o depósito de direcciones asignables. También registra las direcciones MAC de los equipos a los que asigna direcciones y puede incluir periodos de concesión para mantener las asignaciones de direcciones IP.

Los equipos configurados para obtener direcciones IP automáticamente se conectan al servidor durante el arranque para obtener los parámetros de configuración de red. Aunque DHCP no garantiza la misma dirección para un mismo equipo, los administradores pueden configurar direcciones estáticas para mantener la consistencia, especialmente para servidores cuyas direcciones deben ser conocidas por los clientes.

El cliente DHCP utiliza el puerto UDP 68, mientras que el servidor emplea el puerto UDP 67.

7.4.- Protocolo FTP

FTP (Protocolo de Transferencia de Archivos) es utilizado para transferir archivos entre un equipo cliente y un equipo servidor. Los clientes se conectan al servidor proporcionando credenciales de autenticación, lo que les permite descargar archivos

del servidor o cargar archivos en su espacio de almacenamiento. FTP utiliza el puerto TCP 21 para la conexión al servidor y autenticación, y el puerto TCP 20 para la transferencia de archivos.

Una desventaja principal de FTP es que las comunicaciones no están encriptadas, lo que podría permitir a terceros acceder a los archivos intercambiados al monitorear el tráfico de red. Para solucionar este problema, se recomienda el uso de otros métodos de transferencia, como SCP o SFTP, ambos basados en SSH y que proporcionan un nivel de seguridad adicional.

7.5.- Protocolo SSH

SSH (Secure Shell) es un protocolo utilizado para acceder de forma remota a equipos, proporcionando un canal seguro en el que toda la información transmitida está cifrada. Esto garantiza que terceros que monitorean la red no puedan acceder a la comunicación entre el emisor y el receptor.

SSH utiliza criptografía de clave pública para las comunicaciones, empleando dos claves: una pública y otra privada. La clave pública se utiliza para cifrar el mensaje y la clave privada para descifrarlo, lo que asegura que solo el destinatario del mensaje pueda acceder a su contenido.

Por defecto, SSH utiliza el puerto TCP 22 y tiene diversas aplicaciones, incluida la transferencia segura de archivos con SFTP o SCP, así como la capacidad de abrir un terminal en una máquina remota siempre que se tengan las credenciales adecuadas.

7.6.- Protocolos SMTP, POP3 e IMAP

Estos tres protocolos, SMTP, POP3 e IMAP, se utilizan para el envío y recepción de correos electrónicos. Inicialmente, solo se usaba SMTP, pero sus limitaciones llevaron a la adición de otros protocolos para complementarlo.

SMTP (Simple Mail Transfer Protocol) se utiliza para enviar y recibir correos electrónicos y usa el puerto TCP 25 en la especificación original, y los puertos TCP 587 y 465 en versiones posteriores.

Por otro lado, POP (Post Office Protocol) e IMAP (Internet Message Access Protocol) permiten una gestión más eficiente de los buzones de correo de los usuarios, manejando la bandeja de entrada y ofreciendo servicios adicionales. La versión más popular actualmente es POP3, que utiliza los puertos TCP 110 y 995 para conexiones seguras. IMAP, por su parte, emplea los puertos TCP 143 para conexiones no seguras y 993 para conexiones cifradas.

7.7.- Protocolos para streaming

En el ámbito del streaming, destacan varios protocolos importantes:

- RTMP (Real-Time Messaging Protocol): Desarrollado por Adobe para Flash, sigue presente en la transmisión en vivo con especificaciones originales que usan TCP en el puerto 1935 y una versión alternativa, RTMFP, que utiliza UDP. Aunque tiene baja latencia, no es ideal para transmisiones masivas y no es altamente escalable.
- HLS (HTTP Live Streaming): Ampliamente utilizado y adaptable, HLS ajusta la calidad del video según el ancho de banda del receptor. Utiliza HTTP como soporte con TCP en el puerto 80. Aunque tiene mayor latencia, versiones modificadas como LL-HLS mejoran las prestaciones.
- SRT (Secure Reliable Transport): Una alternativa de código abierto que utiliza UDP en el puerto 9710. Ofrece baja latencia y tráfico encriptado, con mecanismos ligeros para confirmar y retransmitir datos perdidos, mejorando la calidad de la transmisión.

8.- Dispositivos Hardware de red

a) Dispositivos del nivel físico:

- Módem: Un módem modula y demodula señales para permitir la transmisión de datos a través de medios físicos específicos, como cables de fibra óptica o líneas ADSL. Ayuda a adaptar las señales a las características del medio de transmisión.
- Repetidor: Los repetidores amplifican y restauran las señales de transmisión para evitar su atenuación, permitiendo la transmisión de datos a larga distancia sin pérdida de información.
- Hub: Los hubs, también conocidos como repetidores multipuerto o concentradores, reenvían la información recibida en un puerto a todos los demás puertos de la red. Son útiles para la creación de redes locales sencillas con topología de estrella y pueden ser activos, amplificando y regenerando la señal, o pasivos, simplemente repitiendo la señal.

b) Dispositivos del nivel de enlace:

- Tarjeta de red: Las tarjetas de red o NIC (Network Interface Card) permiten la conexión de un dispositivo, como un ordenador, al medio físico de una red. Existen diferentes tipos de tarjetas de red según el tipo de arquitectura o cableado de la red.

- Puente: Los puentes se utilizan para conectar redes que utilizan diferentes topologías o protocolos. Facilitan el paso de datos de una red a otra y proporcionan un control de tráfico en la red al permitir el cruce de paquetes específicos.
- Puntos de Acceso: Los puntos de acceso, presentes en redes inalámbricas, interconectan dispositivos inalámbricos para formar una red que conecta dispositivos móviles o tarjetas de red inalámbricas. Además, pueden conectarse a una red cableada y transmitir datos entre dispositivos conectados a ambas redes.
- Conmutadores: Los conmutadores, también conocidos como switches, conectan redes a nivel de enlace de datos con un único protocolo. Son selectivos y solo reenvían la información al puerto de destino correspondiente, evitando tráfico innecesario en la LAN. Aprenden la configuración de la red a medida que se producen transacciones entre dispositivos, utilizando el protocolo ARP para identificar las direcciones MAC correspondientes a las direcciones IP de destino.

c) Dispositivos de nivel de red:

- Router: Los routers conectan una red a otras redes y permiten el paso de información solo cuando va dirigida a un equipo en una red diferente a la del emisor. También localizan la ruta óptima hacia el destino, considerando factores como la longitud, congestión y seguridad de la ruta.