Tema 3

INTRODUCCIÓN A LOS SISTEMAS EN RED

SI | 23-24

Indices

Introducción a los sistemas en red

El objetivo de la unidad es que conozcas los conceptos relacionados con las redes de ordenadores para posteriormente aplicarlos.

Una de las competencias profesionales que debes adquirir es desarrollar aplicaciones capaces de ofrecer servicios en red empleando mecanismos de comunicación. Para esto es necesario que, previamente, conozcas las características de las redes y los conceptos básicos que fundamentan su funcionamiento.

Por tanto, en esta unidad empezarás conociendo las características de las redes de ordenadores, harás un repaso de las arquitecturas de red más importantes, para posteriormente estudiar cómo se pueden conectar ordenadores entre sí, utilizando diferentes topologías y medios de transmisión.

Al finalizar la unidad tendrás los conocimientos suficientes para poder afrontar las unidades siguientes, que se centrarán en la configuración de los equipos que componen una red.

1. Características de las redes de ordenadores.

Las redes están en todas partes, y las redes de ordenadores forman parte de ese sistema de conexión global cada vez más extendido, conocido como Internet. Como futuro profesional del sector de la informática, una de las cosas que debes conocer es: cómo los ordenadores trabajan, y cómo se conectan entre sí para formar sistemas más amplios que, en la mayoría de los casos, utilizan redes de diferentes características.

En esta unidad de trabajo verás los principios de las redes de ordenadores, para posteriormente ser capaz de aplicarlos.

Definimos red informática como dos o más dispositivos conectados para compartir los componentes de su red, y la información que pueda almacenarse en todos ellos.

Si tomamos como referencia la definición dada por Andrew S. Tanenbaum, una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos.

Esta última definición es la que nos va a servir de punto de partida para el desarrollo de la unidad de trabajo, ya que, como irás comprobando, para poder trabajar con las redes

de ordenadores necesitamos conocer los sistemas de comunicación más utilizados, la arquitectura que las hace posible, los protocolos asociados, la forma de conectarlas y sus componentes.

Aunque en el desarrollo de la unidad veremos diferentes características de las redes de ordenadores, y daremos una explicación más amplia, es conveniente empezar citando algunas de las más importantes, y que han contribuido a su generalización:

- **Conectividad**: la posibilidad de conexión de diferentes dispositivos entre sí con la finalidad de compartir recursos propios o ajenos, tanto en entornos locales como en entornos remotos.
- **Escalabilidad**: una red de ordenadores puede ampliar fácilmente sus posibilidades, además esta red puede conectarse con otras redes, y así dar mayores prestaciones.
- **Seguridad**: esta característica es deseable y necesaria, aunque no siempre se cuida lo suficiente. En algunos casos las redes aumentan la seguridad ante pérdidas de datos, ya que duplican información, y en otros casos disminuyen la seguridad de esos datos, ya que están más disponibles. Es conveniente considerar esta característica como una de las más importantes.
- **Optimización de costes**: si podemos compartir recursos, y estos recursos nos dan una mayor productividad, además de facilitarnos el trabajo, estamos optimizando costes y sacando mayor rendimiento a nuestra inversión.

1.1. SISTEMA DE COMUNICACIÓN.

Según el Diccionario de la Lengua Española, sistema, en una de sus acepciones, es el conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí. En este mismo diccionario podemos buscar la palabra comunicación, y encontramos que se puede definir como transmisión de señales mediante un código común al emisor y al receptor.

Por tanto, podemos definir sistema de comunicación como un conjunto de elementos que, siguiendo unas reglas, intervienen en la transmisión de señales, permitiendo el intercambio de información entre un emisor y un receptor.

De esta definición podemos inferir los componentes de un sistema de comunicación, que serán:

- **Emisor:** elemento que transmite la información.
- **Receptor:** elemento que recibe la información.
- **Canal:** medio por el cual se transmite la información, utilizando señales convenientemente codificadas.

Como podemos deducir, es necesario que emisor y receptor codifiquen la información de forma que ambos se entiendan, por tanto, necesitan crear un conjunto de reglas que

regulen la comunicación entre ambos, este conjunto de reglas es lo que conocemos por protocolo de comunicación.

Considerando que la transferencia de la información entre emisor y receptor se lleva a cabo a través del canal de comunicaciones, podemos definir este último como el medio físico por el cual se transporta la información convenientemente codificada, siguiendo unos protocolos establecidos.

Así podemos clasificar los sistemas de comunicación según diferentes puntos de vista. Si tenemos en cuenta el medio de transmisión, podemos tener sistemas en línea o cableados y sistemas inalámbricos.

En cambio, si el criterio que utilizamos es la direccionalidad de la transmisión, los sistemas de comunicación pueden clasificarse en:

- **Simplex**: Cuando la comunicación se efectúa en un sólo sentido. Emisor emite, receptor recibe. Ejemplo: Cuando escuchamos música por la radio, nosotros sólo recibimos.
- **Semidúplex** (half duplex): Cuando la comunicación se realiza en los dos sentidos, pero no de forma simultánea. Emisor emite, receptor recibe, receptor pasa a ser emisor, y emisor pasa a ser receptor. Ejemplo: Hablar por el walkie-talkie.
- **Dúplex** (full duplex): Cuando la comunicación se realiza en ambos sentidos de forma simultánea. Ambos son emisores y receptores a la vez. Ejemplo: Las redes de ordenadores suelen funcionar de esta forma.

Otros criterios que se utilizan para clasificar las comunicaciones son:

- Según la forma de **sincronizar las señales**: así tenemos comunicaciones síncronas y asíncronas.
- Según la **naturaleza de la señal**: este criterio nos lleva a utilizar los términos de comunicaciones **analógicas** y **digitales**. Esta última clasificación es más utilizada en el ámbito de las comunicaciones, por lo que para nosotros será más adecuado hablar de trasmisiones analógicas o digitales. Esto es así porque los ordenadores son sistemas que se basan en el uso de señales digitales.

Además de estos criterios también hay dos conceptos relacionados con las comunicaciones que debemos conocer, uno de ellos es el término Equipo Terminal de Datos (ETD), que serán todos los equipos, ya sean emisores o receptores de información. El otro término es el de Equipo de Comunicación de Datos (ECD) que es cualquier dispositivo que participa en la comunicación pero que no es ni emisor original ni receptor final.

1.2. REDES DE ORDENADORES. VENTAJAS

Red de ordenadores o red informática: es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos.

La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones.

Si conectamos dos ordenadores entre sí ya tenemos una red, si conectamos más ordenadores, le agregamos impresoras, y nos conectamos a dispositivos que permitan salir a Internet, estamos consiguiendo que nuestra red sea cada vez mayor y pueda disponer de mayores recursos, ya que los recursos individuales pueden compartirse. Ésta es la idea principal de las redes, ya que, a medida que conectamos más dispositivos y estos comparten sus recursos, la red será más potente.

Por tanto, las principales **ventajas** de las redes de ordenadores serán:

- La posibilidad de compartir recursos.
- La posibilidad de compartir información.
- Aumentar las posibilidades de colaboración.
- Facilitar la gestión centralizada.
- Reducir costes.

Si analizamos algunas de estas ventajas, está claro que utilizar redes de ordenadores para trabajar es mejor que hacerlo de forma aislada.

Cuando se habla de compartir recursos, la mayoría tenemos en mente la conexión a Internet. Es obvio que una sola conexión a Internet compartida es más barata que tener una conexión para cada ordenador. Éste ha sido uno de los principales motivos por los cuales las redes de ordenadores han tenido tanto éxito. Pero no debemos olvidar otros recursos no menos importantes, como la utilización de periféricos compartidos tales como: impresoras, discos duros de red, escáneres, etc. En este apartado de recursos compartidos, también deberíamos mencionar la posibilidad de compartir software. El software compartido cada vez es mayor, y en algunos entornos de trabajo es indispensable.

Relacionado con la posibilidad de compartir recursos, tenemos la posibilidad de compartir información. De esta manera podremos usar bases de datos compartidas, documentos que pueden leerse, e incluso elaborarse por varios usuarios y usuarias diferentes.

Esto último liga con otra de las ventajas, que es la posibilidad de colaboración. Cuando compartimos recursos e información, las posibilidades de colaboración aumentan. Además, esa colaboración puede darse entre personas que estén en la misma oficina o instituto, pero también se puede dar entre personas que estén tan alejadas que ni siquiera lleguen a conocerse. Esto último está muy de moda; seguro que has oído

hablar del concepto de computación en nube para referirse a la posibilidad de ofrecer servicios informáticos a través de Internet. Este concepto está muy ligado al uso de redes de ordenadores e Internet.

Respecto a la gestión centralizada de los recursos, hay que comentar que mejora la seguridad de los sistemas, suele optimizar las prestaciones de la red y sale más barato.

Para terminar, podemos decir que el principal objetivo de cualquier asociación, corporación o persona es, que cuando haga una inversión, ésta no sea excesiva. Si se hace una buena planificación de la red, y se hace un buen diseño de esta, seguro que se reducirán costes de implantación y mantenimiento.

1.3. CLASIFICACIÓN DE LAS REDES. TIPOS DE REDES.

Las redes se pueden clasificar según diferentes conceptos, nosotros nos centraremos en los conceptos más utilizados.

Por **alcance** o **extensión** tenemos:

- **Red de área personal** o PAN (personal area network) es una red de ordenadores usada para la comunicación entre los dispositivos del ordenador cerca de una persona.
- **Red de área local** o LAN (local area network) es una red que se limita a un área especial, relativamente pequeña, tal como un cuarto, un aula, un solo edificio, una nave, o un avión. Las redes de área local suelen tener las mayores velocidades, además de considerarse como el componente esencial para la creación de redes más grandes.
- **Red de área de campus** o CAN (campus area network) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar. Este término se suele utilizar como extensión del de LAN, ya que realmente lo que se tiene son redes locales conectadas entre sí para abarcar un área más extensa.
- **Red de área metropolitana** o MAN (metropolitan area network) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa. Este concepto se utiliza para definir redes que abarcan extensiones relativamente grandes, y que necesitan recursos adicionales a los que necesitaría una red local.
- **Red de área amplia** o WAN (wide area network) es una red informática que se extiende sobre un área geográfica extensa. Dentro de esta clasificación podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y el propio Internet que puede considerarse como una gigantesca red WAN.

Según las funciones de sus componentes:

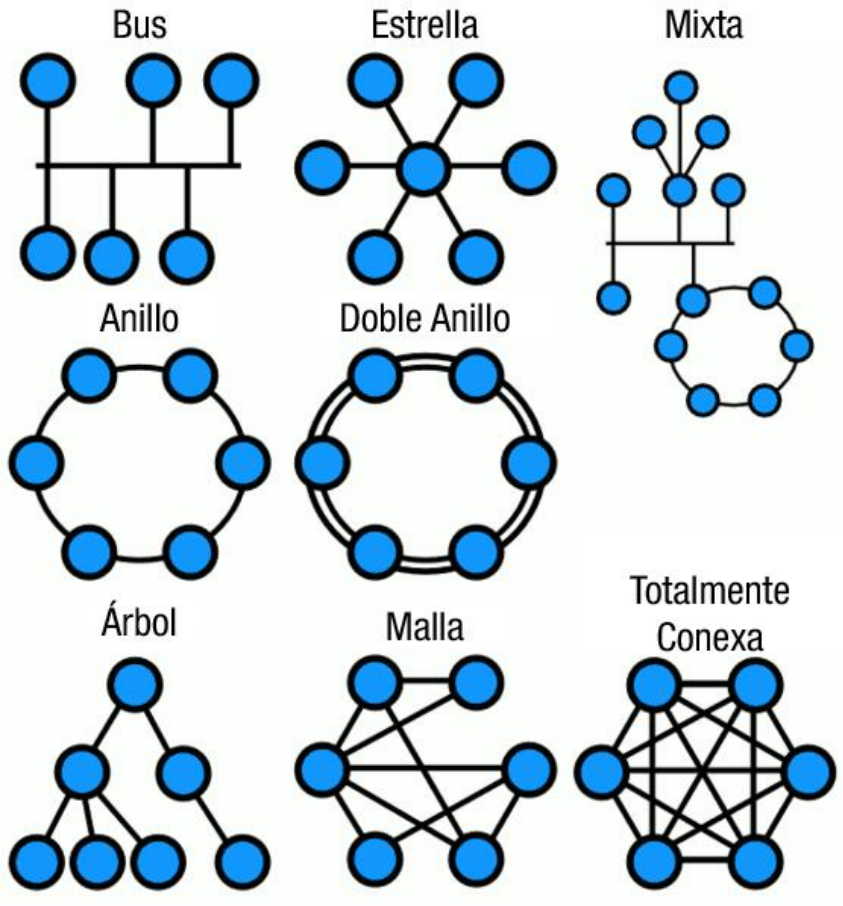
- **Redes de igual a igual** o entes iguales, también conocidos como redes peer-to-peer, son redes donde ningún ordenador está a cargo del

funcionamiento de la red. Cada ordenador controla su propia información y puede funcionar como cliente o servidor según lo necesite. Los sistemas operativos más utilizados incluyen la posibilidad de trabajar de esta manera, y una de sus características más destacadas es que cada usuario controla su propia seguridad.

- **Redes cliente-servidor,** se basan en la existencia de uno o varios servidores, que darán servicio al resto de ordenadores que se consideran clientes. Este tipo de redes facilitan la gestión centralizada. Para crear redes de este tipo necesitamos sistemas operativos de tipo servidor, tales como Windows 2008, 2019 server o GNU-Linux. Cabe destacar que en principio cualquier distribución Linux pueden actuar como servidor, aunque existen distribuciones especialmente recomendadas para este cometido, tales como Debian, Ubuntu server, Red Hat enterprise, etc.

Según su topología:

La forma de conectar los ordenadores nos da otra clasificación muy utilizada, que es lo que se conoce por topología, en este apartado sólo citaremos algunas topologías ya que en esta unidad dedicaremos un apartado para explicarlas con más detalle. Entre las topologías de conexión podemos citar: en bus, en anillo, en estrella, en árbol, en malla, doble anillo, mixta y totalmente conexa.



Según el tipo de conexión podemos tener:

- **Redes cableadas**: En este tipo de redes se utilizan diferentes tipos de cables para conectar los ordenadores, más adelante estudiaremos lo relacionado con los tipos de cables más utilizados.
- **Redes inalámbricas**: Son las redes que no necesitan cables para comunicarse, existen diferentes tecnologías inalámbricas que más adelante estudiaremos.

Otra clasificación interesante es teniendo en cuenta el grado de difusión, en esta clasificación distinguimos dos tipos de redes:

- **Intranet** es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma privada, esto es, que no comparte sus recursos o su información con otras redes, a no ser que autentifiquen, o cumplan unas medidas de seguridad determinadas.
- **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Precisamente

esta característica, es la que ha hecho que el uso de Internet se generalice y que todas las redes funcionen utilizando protocolos TCP/IP.

1.4. TECNOLOGÍAS WAN

Hemos visto que las redes WAN (wide area network) son redes informáticas que se extienden sobre un área geográfica extensa. Dentro de esta clasificación podemos encontrar las redes de telecomunicaciones que permiten el uso de Internet, y el propio Internet que puede considerarse como una gigantesca red WAN.

Las redes WAN son capaces de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería Internet o cualquier red de similares características.

Existen WAN construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de internet (ISP) para proveer de conexión a sus clientes.

Hoy en día, Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente, mientras que las redes privadas virtuales que utilizan cifrado y otras técnicas para hacer esa red dedicada, aumentan continuamente.

Usualmente la WAN es una red punto a punto que utiliza la conmutación de paquetes. Las redes WAN pueden usar sistemas de comunicación vía satélite o de radio.

Las redes WAN basan su funcionamiento en las técnicas de conmutación. Podemos definir las técnicas de conmutación como la forma en que un usuario y otro establecen la comunicación. Estas técnicas son:

- **Conmutación de circuitos**: consiste en el establecimiento de un enlace físico para la transmisión entre dos nodos, que se liberará cuando termine la comunicación en el caso de utilizar una red conmutada, o permanecerá si se utiliza una red dedicada (Ejemplo: transmisión de datos a través de la red telefónica conmutada).
- **Conmutación de mensajes**: es un método basado en el tratamiento de bloques de información, dotados de una dirección de origen y otra de destino, de esta forma la red almacena los mensajes hasta verificar que han llegado correctamente a su destino y proceden a su retransmisión o destrucción. Es una técnica empleada con el servicio télex y en algunas de las aplicaciones de correo electrónico.
- **Conmutación de paquetes**: consiste en dividir el mensaje en paquetes. La comunicación entre dos equipos implica la transmisión de los paquetes. Cada paquete es enviado de un nodo de la red al nodo siguiente. Cuando el nodo receptor recibe completamente el paquete, lo almacena y lo vuelve a emitir al nodo que le sigue. Este proceso se va repitiendo hasta que el paquete llegue al destino final. Para la utilización

de la conmutación de paquetes se han definido dos tipos de técnicas: los datagramas y los circuitos virtuales. Internet es una red de conmutación de paquetes basada en datagramas.

Las redes de área extensa suelen estar soportadas por redes públicas de telecomunicaciones que son las que todos conocemos y que solemos usar para conectarnos a Internet. Ejemplos de estas redes serán:

- La **red telefónica básica** o **red telefónica conmutada** (RTB o RTC) permite que hablemos por teléfono, pero si utilizamos un módem podemos transmitir datos a baja velocidad.
- El **bucle de abonado digital asimétrico**, más conocido como **ADSL**, las operadoras de telefonía ofrecen la posibilidad de utilizar una línea de datos independiente de la línea de teléfono, aprovechando el ancho de banda disponible por encima del requerido por el servicio telefónico hasta el límite permitido por la propia línea.
- Telefonía móvil mediante **t**ecnologías 2G, 3G, 4G o 5G proporcionan la posibilidad de transferir tanto voz y datos (una llamada telefónica o una videollamada) y datos no-voz (como la descarga de programas, intercambio de correo electrónico, y mensajería instantánea).
- **Internet por cable**, usando cable módem o enrutadores, las redes de cable ofrecen la posibilidad de utilizar cable de fibra óptica combinado con cable coaxial, para dar una alta velocidad en el acceso a Internet.

1.4.1. Conmutación de paquetes

La conmutación de paquetes es un método utilizado en las redes de datos, donde la información se divide en unidades más pequeñas llamadas paquetes. Cada paquete contiene un encabezado con la información necesaria para enrutarlo desde el origen hasta el destino (información de control). Los datos en el encabezado son utilizados por el hardware de red para dirigir el paquete a su destino donde la carga útil es extraída y utilizada por el software de la aplicación. Esta forma de conmutación surgió como respuesta a las deficiencias de la conmutación de mensajes en las redes.

En la conmutación de paquetes, los paquetes se transmiten de manera independiente a través de la red y pueden seguir diferentes rutas hacia su destino. Los dispositivos de red intermedios, como los conmutadores, almacenan y reenvían los paquetes según su información de control. Esta forma de conmutación es utilizada en redes corporativas e Internet, ya que es más fácil para los dispositivos de red manejar paquetes de pequeño tamaño y no requiere tantos recursos en la ruta o en la memoria interna.

La principal ventaja de la conmutación de paquetes es la multiplexación estadística, que permite compartir eficientemente los enlaces de comunicación entre paquetes de diferentes orígenes. Esto mejora la eficiencia de la línea y permite que múltiples flujos de datos sean transmitidos simultáneamente. Sin embargo, en caso de congestión de la red, los paquetes pueden experimentar retrasos o incluso ser descartados.

Además, la conmutación de paquetes permite la diferenciación de flujos de datos basados en prioridades. Los paquetes se almacenan y reenvían según su prioridad para garantizar la calidad de servicio. La conmutación de paquetes se ha convertido en la base principal de las comunicaciones de datos en redes informáticas a nivel mundial.

Características:

- Los paquetes forman una cola y se transmiten.
- Permiten la conversión en la velocidad de los datos.
- La red puede seguir aceptando datos, aunque la "Transmisión de datos" sea lenta.
- Existe la posibilidad de manejar prioridades (si un grupo de información es más importante que los otros, será transmitido antes que dichos otros).

La conmutación de paquetes se puede clasificar en conmutación de paquetes sin conexión, también conocida como conmutación de datagramas (UDP), y conmutación de paquetes orientada a la conexión (TCP), también conocida como conmutación de circuitos virtuales.

Modo conmutación de paquetes sin conexión o datagramas (UDP)

En modo sin conexión, cada paquete incluye información de direccionamiento completa. Los paquetes se enrutan individualmente, a veces dando como resultado rutas diferentes y entrega fuera de orden. Cada paquete está etiquetado con una dirección de destino, dirección de origen y números de puerto. También puede etiquetarse con el número de secuencia del paquete. Esto excluye la necesidad de una ruta dedicada para ayudar al paquete a llegar a su destino, pero significa que se necesita mucha más información en el encabezado del paquete, que por lo tanto es más grande, y esta información debe buscarse en un contenido de gran consumo de energía.

El protocolo utilizado para transporte es **UDP** (User Datagram Protocol (Protocolo de Datagramas de Usuario)), es uno de los dos protocolos principales utilizados en la capa

de transporte en redes de computadoras, es un protocolo de comunicación **sin conexión**, lo que significa que no establece una conexión antes de enviar datos y no garantiza la entrega de los mismos ni el orden en que se entregan.

Sus características principales son:

- **Comunicación sin conexión**: A diferencia de TCP, que establece una conexión antes de la transferencia de datos y garantiza la entrega ordenada y confiable de los datos, UDP no establece una conexión. Simplemente toma los datos que se le proporcionan y los envía sin establecer una relación de comunicación permanente.
- **No garantiza la entrega: UDP** no incluye mecanismos para garantizar que los datos sean entregados correctamente al destino. Esto significa que los datos pueden perderse o llegar desordenados, y no se realiza ningún intento automático de reenviar los datos perdidos.
- **Transferencia rápida**: Debido a su falta de mecanismos de control y verificación, UDP tiende a ser más rápido que TCP. Es adecuado para aplicaciones en las que la velocidad es más importante que la integridad de los datos, como la transmisión en tiempo real de audio y video.
- **Encabezado simple:** El encabezado de un datagrama UDP es bastante simple, lo que significa que el protocolo agrega menos sobrecarga de datos a la comunicación en comparación con TCP. El encabezado UDP consta de puertos de origen y destino, longitud y una suma de verificación (checksum) opcional para verificar la integridad de los datos.

Aplicaciones típicas: UDP se utiliza comúnmente en aplicaciones que pueden tolerar cierta pérdida de datos, como transmisiones en vivo por Internet, videojuegos en línea, servicios de voz sobre IP (VoIP) y otras aplicaciones en tiempo real. También se utiliza en situaciones donde la sobrecarga de TCP (como la necesidad de establecer una conexión) podría ser problemática.

Modo conmutación de paquetes orientada a la conexión o conmutación de circuitos virtuales (TCP)

TCP, Transmission Control Protocol (Protocolo de Control de Transmisión), es uno de los protocolos fundamentales de la capa de transporte en redes de computadoras. A diferencia de UDP (User Datagram Protocol), TCP es un protocolo **orientado a la conexión** y proporciona una comunicación confiable y ordenada entre dos dispositivos en una red.

TCP establece una conexión antes de transmitir datos. Esta conexión se conoce como "handshake de tres vías" y asegura que ambos extremos estén listos para la comunicación antes de comenzar la transferencia de datos.

Sus características principales son:

- **Comunicación confiable**: Una de las características más destacadas de TCP es su capacidad para garantizar que los datos se entreguen de manera confiable y en el orden correcto. Utiliza números de secuencia y reconocimientos para asegurarse de que los datos se transmitan y reciban sin errores.
- **Control de flujo:** TCP incluye mecanismos de control de flujo que permiten a los dispositivos emisores ajustar la velocidad de transmisión de datos en función de la capacidad del receptor para procesarlos. Esto evita la congestión en la red y garantiza una transferencia de datos eficiente.
- **Reensamblaje de paquetes:** Cuando los datos se dividen en paquetes más pequeños para su transmisión a través de la red, TCP se encarga de reensamblarlos en el orden correcto en el extremo receptor.
- Detección y corrección de errores: TCP utiliza una suma de verificación (checksum) para detectar errores en los datos transmitidos. Si se detecta un error, TCP solicita la retransmisión de los datos defectuosos.
- **Transmisión bidireccional:** TCP permite la transmisión de datos en ambas direcciones entre dos dispositivos (conocido como un flujo de datos bidireccional o full-duplex). Cada dirección de la comunicación es tratada como una secuencia separada de datos.

TCP es ampliamente utilizado en aplicaciones que requieren una transmisión confiable de datos, como la navegación web, el correo electrónico, la transferencia de archivos (FTP), las bases de datos en línea y muchas otras aplicaciones que dependen de la integridad y la secuencia de los datos transmitidos.

A pesar de su confiabilidad y capacidad para garantizar la integridad de los datos, TCP puede tener un mayor sobrecosto y latencia en comparación con UDP debido al establecimiento de la conexión y la verificación de datos. Por lo tanto, la elección entre TCP y UDP depende de las necesidades específicas de la aplicación.

2. LA ARQUITECTURA DE RED.

¿Cómo comunicamos a los usuarios con las aplicaciones de otros computadores?

Cuando hablamos de arquitectura de red, puede que pensemos en como está construida la red, los cables, los equipos, etc. Pero no es así, el concepto de arquitectura de red es más amplio e incluye cuestiones relacionadas con el hardware y con el software de una red.

Antes de definir el concepto de arquitectura de red, es conveniente que entiendas que uno de los problemas más importantes a la hora de diseñar una red no es que los equipos se conecten entre sí, si no que estos equipos puedan comunicarse, entenderse, compartir recursos, que al fin y al cabo es lo que pretendemos. Para esto ya hemos mencionado que se necesitan unos protocolos de comunicaciones. Debido a la complejidad que acarrea considerar la red como un todo, se consideró oportuno organizar las redes como una serie de capas, donde cada capa se ocuparía de alguna

función. De esta forma se reduciría la complejidad del diseño de la red y de las aplicaciones que en ella se utilicen.

Por tanto, podemos definir arquitectura de red como el conjunto de capas o niveles, junto con los protocolos definidos en cada una de estas capas, que hacen posible que un ordenador se comunique con otro ordenador independientemente de la red en la que se encuentre.

Esta definición implica, que la especificación de una arquitectura de red debe incluir información suficiente para que cuando se desarrolle un programa o se diseñe algún dispositivo, cada capa responda de forma adecuada al protocolo apropiado.

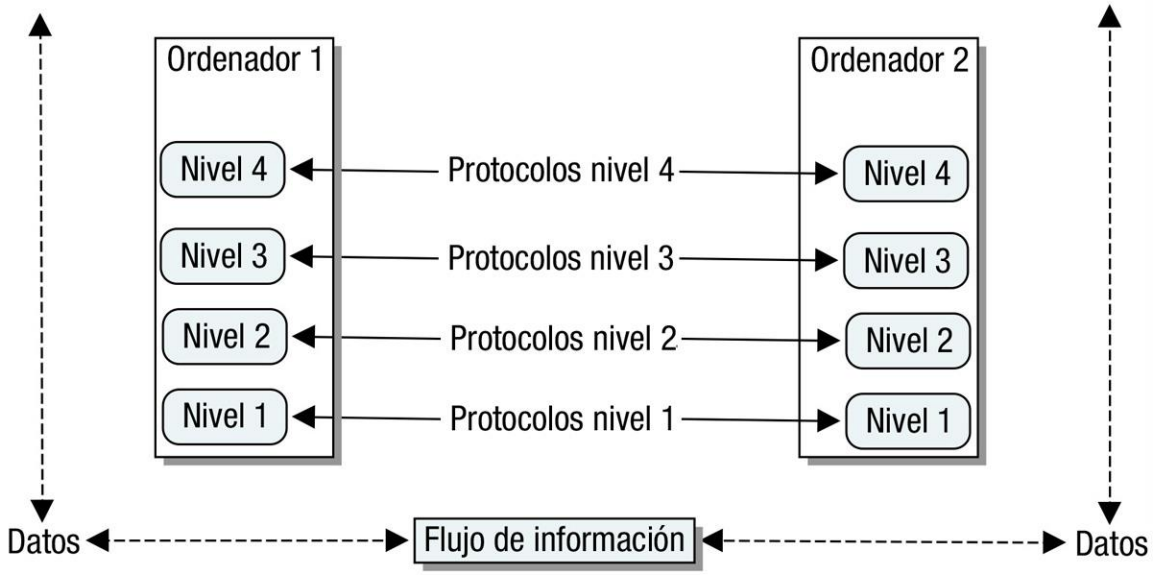
De todo esto podemos concluir que la arquitectura de red tendrá que tener en cuenta al menos tres factores importantes como son:

- La forma en la que se conectan los nodos de una red, que suele conocerse como **topología**, además de las características físicas de estas conexiones.
- La manera de cómo compartir información en la red, que en algunos casos obligará a elegir un **método de acceso a la red** y unas reglas para evitar perdida de información.
- Unas reglas generales que no sólo favorezcan la comunicación, si no que la establezcan, mantengan y permitan la utilización de la información, estás reglas serán los **protocolos de comunicación**.
- A continuación, estudiaremos con más detalle cómo funcionan las arquitecturas basadas en niveles, los protocolos y lo más importante, veremos los dos modelos más importantes en el desarrollo de las redes, el modelo de referencia OSI y la pila de protocolos TCP/IP, que podemos considerarla como la arquitectura base para las comunicaciones por Internet.

2.1. MODELO OSI Y PROTOCOLOS TCP/IP.

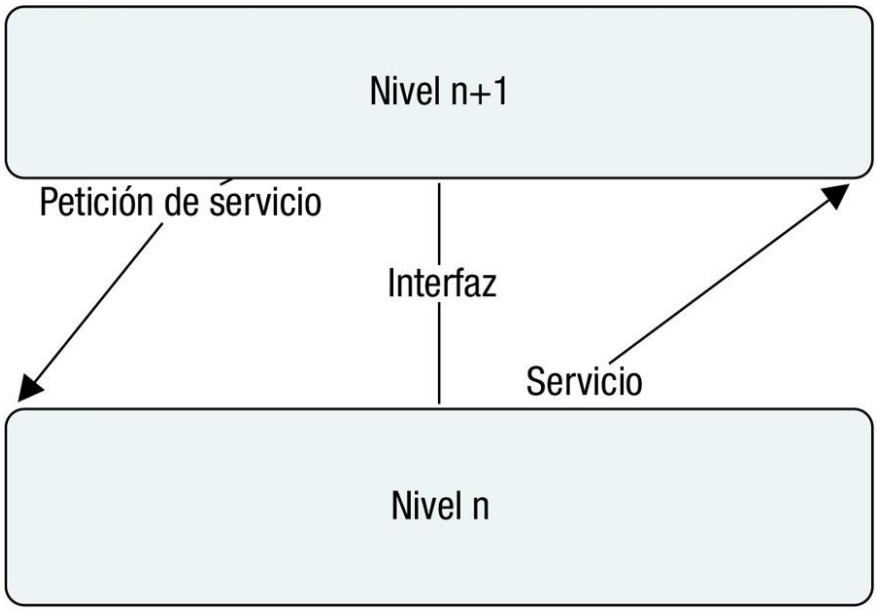
Ya hemos comentado anteriormente, que la arquitectura de red se dividía por niveles o capas para reducir la complejidad de su diseño. Esta división por niveles conlleva que cada uno de estos niveles tenga asociados, uno o varios protocolos que definirán las reglas de comunicación de la capa correspondiente. Por este motivo, también se utiliza el término **pila de protocolos** o **jerarquía de protocolos** para definir a la arquitectura de red que utiliza unos protocolos determinados, esto lo veremos más claramente cuando expliquemos el conjunto de protocolos TCP/IP.

Pero ¿cómo funciona una arquitectura basada en niveles? Para poder explicar esto utilizaremos diferentes gráficos que creemos que pueden ilustrar mejor la explicación.



En el gráfico anterior, podemos ver el esquema de una arquitectura de red de cuatro niveles. Podemos observar dos ordenadores que tendrán implementada la arquitectura, como tenemos cuatro niveles, cada nivel tendrá sus protocolos, por lo que podemos decir que las comunicaciones entre niveles iguales se hacen a través de los protocolos correspondientes. Pero el flujo real de información, con los datos que queremos transmitir irá de un ordenador a otro pasando por cada uno de los niveles. Esto implica que en la realidad los datos no se transfieren directamente de una capa a otra del mismo nivel, si no que cada capa pasa los datos e información de control a la capa adyacente. De esta manera la información pasará por todas las capas, se pasará al medio de transmisión adecuado y posteriormente sucederá lo mismo, pero en sentido contrario, en el otro ordenador. De esta manera la información llegará a su destino y cada nivel sólo se ocupará de los datos y la información de control que necesite, según el protocolo utilizado, sin preocuparse de lo que hagan o necesiten los otros niveles.

Cabe mencionar que con esta forma de trabajar cada capa tiene unos servicios asignados, además las capas están jerarquizadas y cada una tiene unas funciones, de esta forma los niveles son independientes entre sí, aunque se pasan los datos necesarios de una a otra.



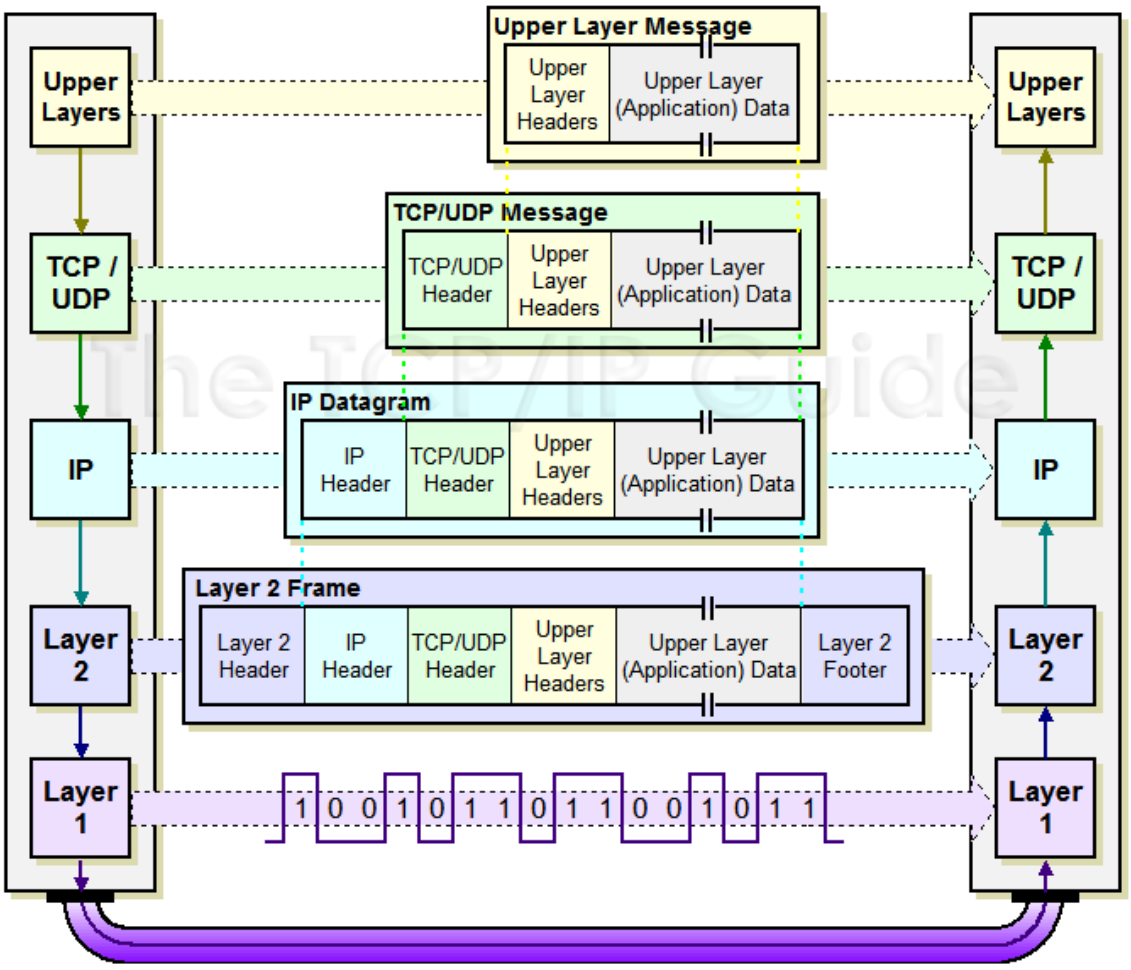
Para poder hacer esto, las capas adyacentes tienen lo que se llama una **interfaz**. En este contexto la interfaz definirá las operaciones y servicios que la capa inferior ofrece a la superior.

Cuando los diseñadores, diseñadoras, o fabricantes quieren fabricar productos compatibles, deben seguir los estándares de la arquitectura de red, para esto es importante definir interfaces claras entre niveles y que cada nivel tenga bien definidos sus servicios.

Todo esto implica que para un buen funcionamiento de la red se deben respetar ciertas reglas, como, por ejemplo: que los servicios se definan mediante protocolos estándares, que cada nivel sólo se comunique con el nivel superior o el inferior y que cada nivel inferior proporcione servicios a su nivel superior.

Hay que comentar que este tipo de arquitectura por niveles conlleva que cada nivel genera su propio conjunto de datos, ya que cada capa pasa los datos originales junto con la información que ella genera, para así poder controlar la comunicación por niveles. Esta información para los niveles inferiores se trata como si fueran datos, ya que sólo la utilizará el nivel correspondiente del ordenador de destino. Más adelante veremos los diferentes nombres que tienen estos datos según la arquitectura que se utilice.

Para terminar, destacar que las arquitecturas de red basadas en capas facilitan las compatibilidades, tanto de software como de hardware, así como las modificaciones futuras, ya que no es necesario cambiar todas las capas cuando queremos mejorar el sistema. Bastaría modificar los protocolos por niveles y podríamos conseguir mejoras en el sistema.



2.2. PROTOCOLO DE COMUNICACIÓN.

Un protocolo de comunicaciones es un **conjunto de reglas normalizadas** para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación.

Entre los protocolos necesarios para poder establecer una comunicación necesitamos protocolos para:

- Identificar el emisor y el receptor.
- Definir el medio o canal que se puede utilizar en la comunicación.
- Definir el lenguaje común a utilizar.
- Definir la forma y estructura de los mensajes.
- Establecer la velocidad y temporización de los mensajes.
- Definir la codificación y encapsulación del mensaje.

Los protocolos usados en las redes están adaptados a las características del emisor, el receptor y el canal, además los protocolos deben definir los detalles de cómo transmitir y entregar un mensaje.

Si nos centramos en las redes de ordenadores, podemos definir algunas cuestiones que los protocolos de redes deben resolver, estas cuestiones serán:

- **El enrutamiento**: En las redes de ordenadores pueden tenerse diferentes rutas para llegar a un mismo destino, por tanto, debe elegirse una de ellas, siendo deseable que siempre se elija la mejor o más rápida. Por tanto, las arquitecturas de red deben tener protocolos que sirvan para este fin, ya veremos cuáles son y en qué nivel se resuelven.
- **El direccionamiento**: Dado que una red se compone de muchos nodos conectados entre sí, debe haber alguna forma de conocer cuál es cual. Para esto necesitamos definir direcciones de red que permitan determinar a qué ordenador me quiero conectar o por dónde debo conectarme para llegar a un destino. Para poder conseguir esto, las arquitecturas de red definen protocolos de direccionamiento, desde un punto de vista lógico y físico, que se definen en niveles adecuados para que la comunicación sea posible, y no se produzcan duplicidades.
- **La necesidad de compartir un medio de comunicaciones**: Puede darse el caso que se comparta un mismo medio para transmitir, por tanto, deben establecerse mecanismos que controlen el acceso al medio y el orden en el que se accede.
- **La saturación**: Los protocolos de cualquier nivel deben ser capaces de evitar que el receptor del mensaje, o los dispositivos intermedios que actúan en la transmisión del mensaje, se saturen. Esto suele ser un problema, y no siempre es fácil de resolver, pero un buen diseño y la adecuación de la red a las necesidades ayudan.
- **El control de errores**: Es deseable que los protocolos de red tengan mecanismos de control de errores. Como veremos cuando analicemos las arquitecturas de red este control se puede hacer desde diferentes puntos de vista y en diferentes niveles.

Hemos citado algunas cuestiones, pero está claro que los protocolos resuelven muchas más, lo importante a tener en cuenta es que gracias a unos protocolos estandarizados, y a un buen diseño de red, podemos conseguir que ordenadores de todo el mundo se comuniquen entre sí.

2.3. FUNCIONAMIENTO DE UNA ARQUITECTURA BASADA EN NIVELES.

El **modelo OSI**, siglas en inglés de Open System Interconnection o traducido, Interconexión de Sistemas Abiertos, es el modelo de red creado por la Organización Internacional para la Normalización (ISO) en el año 1984. Este modelo define un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Hay que destacar que el modelo OSI simplifica las actividades de red,

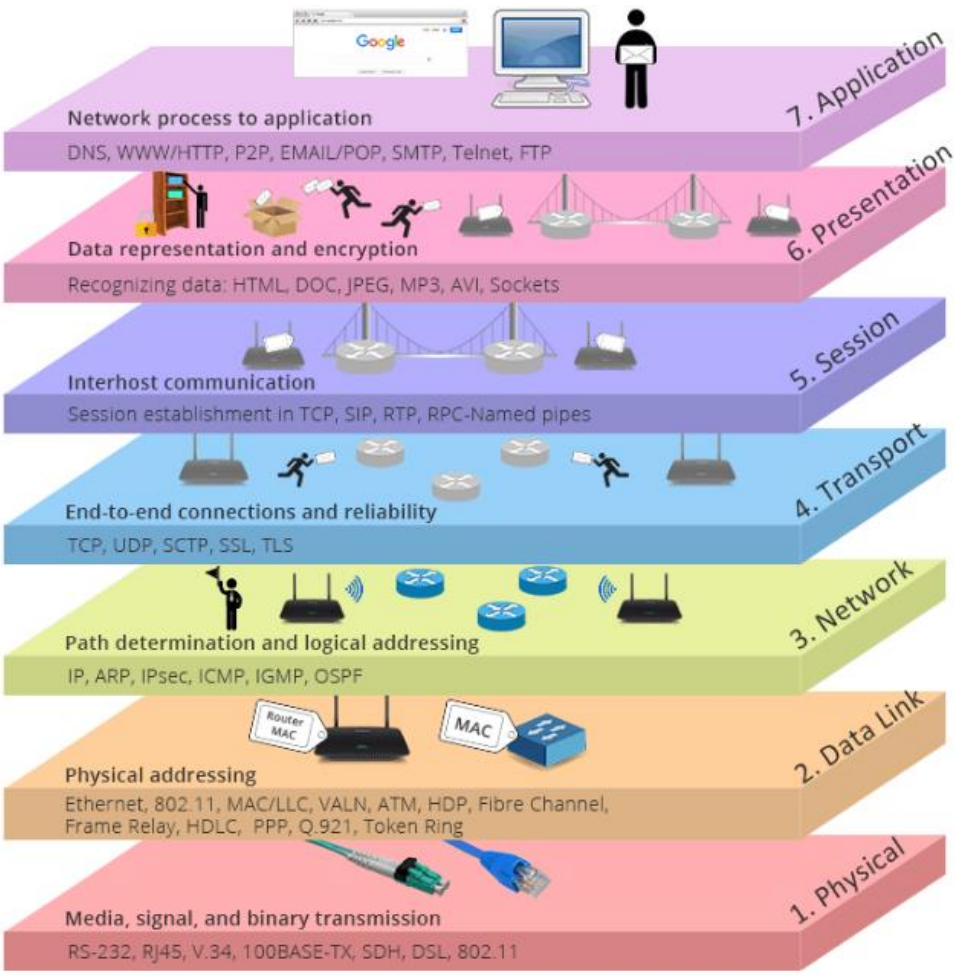
ya que agrupa los procesos de comunicación en siete capas que realizan tareas diferentes. Es conveniente tener en cuenta que el modelo OSI, no es una arquitectura desarrollada en ningún sistema, sino una referencia para desarrollar arquitecturas de red, de forma que los protocolos que se desarrollen puedan ser conocidos por todos.

Aunque el modelo OSI no está realmente desarrollado en ningún sistema, sí es conveniente conocerlo y aplicarlo, ya que nos sirve para poder entender los procesos de comunicación que se producen en una red, y además puede usarse como referencia para realizar una detección de errores o un plan de mantenimiento.

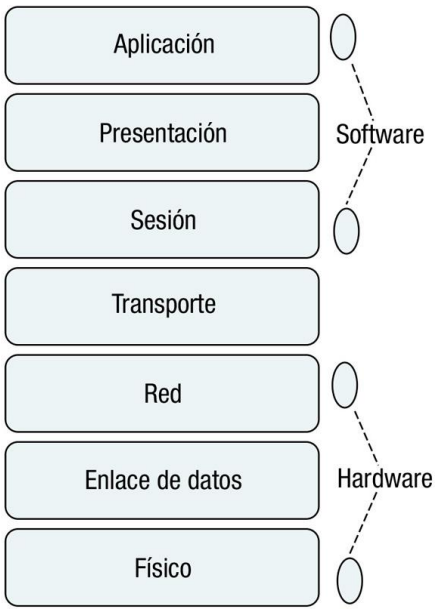
Los niveles OSI son:

Capa	Nombre	Funciones
1	Capa física o nivel físico.	Se encarga de las conexiones físicas, incluyendo el cableado y los componentes necesarios para transmitir la señal.
2	Capa o nivel de enlace de datos.	Empaqueta los datos para transmitirlos a través de la capa física. En esta capa se define el direccionamiento físico utilizando las conocidas direcciones MAC. Además se encarga del acceso al medio, el control de enlace lógico o LLC y de la detección de errores de transmisión, entre otras cosas.
3	Capa o nivel de red.	Separa los datos en paquetes, determina la ruta que tomaran los datos y define el direccionamiento.
4	Capa o nivel de transporte.	Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores.
5	Capa o nivel de sesión.	Mantiene y controla el enlace entre los dos extremos de la comunicación.
6	Capa o nivel de presentación.	Determina el formato de las comunicaciones así como adaptar la información al protocolo que se esté usando.
7	Capa o nivel de aplicación.	Define los protocolos que utilizan cada una de la aplicaciones para poder ser utilizadas en red.

La representación gráfica del modelo OSI, suele hacerse como una pila, donde en lo más alto estaría la capa 7 de aplicación y en lo más bajo la capa 1 o física.



Es conveniente mencionar que en ocasiones se hace referencia a que las capas 1, 2 y 3 del modelo están relacionadas con el hardware y las capas 5, 6 y 7 están relacionadas con el software, siendo la capa 4 una capa intermedia entre hardware y software. Esto suele ser así porque los dispositivos y componentes de red, suelen trabajar en los niveles 1 a 3, siendo los programas los que trabajan en los niveles superiores.



2.4. TCP/IP.

Cuando se habla de protocolos TCP/IP, realmente se suele estar haciendo referencia a la arquitectura de red que incluye varios protocolos de red, de entre los cuales dos de los más destacados son el protocolo TCP (Protocolo de Control de Transmisión) y el protocolo IP (Protocolo de Internet).

Por tanto, sería conveniente considerar este modelo como una arquitectura en sí, siendo la más utilizada, ya que es la base de las comunicaciones de Internet y de los sistemas operativos modernos.

Cuando nos referimos a la arquitectura TCP/IP o modelo TCP/IP, nos estamos refiriendo a un conjunto de reglas generales de diseño e implementación de protocolos de red, que permiten la comunicación de los ordenadores. Como veremos con más detalle durante esta unidad, existen protocolos para los diferentes tipos de servicios de red.

La arquitectura TCP/IP está compuesta de cuatro capas o niveles que son:

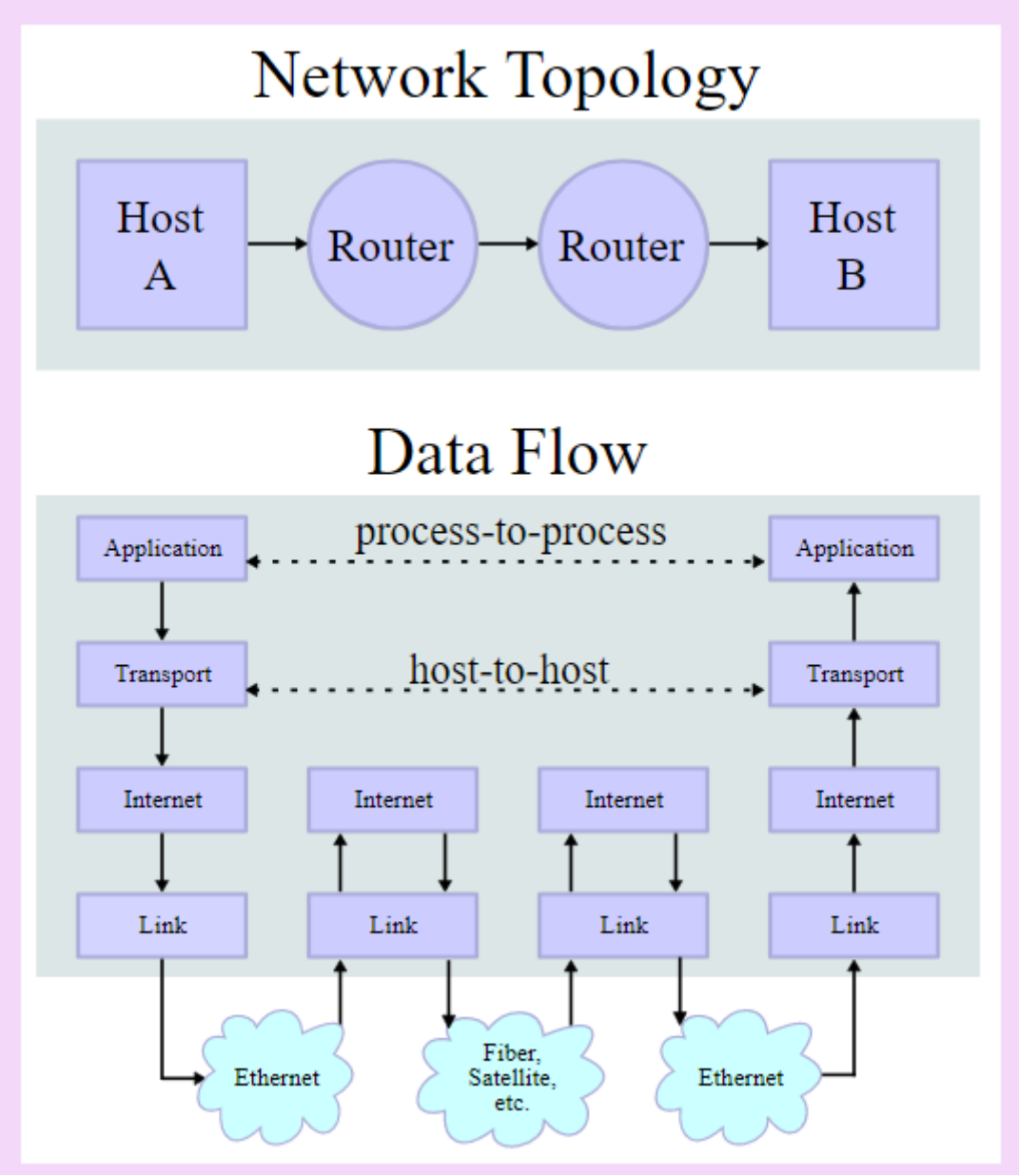
Capa	Nombre	Funciones
1	Capa o nivel de acceso a la red, de enlace o también llamado de subred.	Se encarga del acceso al medio de transmisión, es asimilable a los niveles 1 y 2 del modelo OSI, y sólo especifica que deben usarse protocolos que permitan la conexiones entre ordenadores de la red. Hay que tener en cuenta que esta arquitectura está pensada para conectar ordenadores diferentes en redes diferentes, por lo que las cuestiones de nivel físico no se tratan, y se dejan lo suficientemente abiertas para que se pueda utilizan cualquier estándar de conexión. Permite y define el uso de direcciones físicas utilizando las direcciones MAC.
2	Capa o nivel de red también llamada de Internet.	Al igual que la capa de red del modelo OSI, esta capa se encarga de estructurar la información en paquetes, determina la ruta que tomaran los paquetes y define el direccionamiento. En esta arquitectura los paquetes pueden viajar hasta el destino de forma independiente, pudiendo atravesar redes diferentes y llegar desordenados, sin que la ordenación de los paquetes sea responsabilidad de esta capa, por tanto tampoco se encarga de los errores. El protocolo más significativo de esta capa es el protocolo IP, y entre sus funciones está la de dar una dirección lógica a todos los nodos de la red.
3	Capa o nivel de transporte.	Es igual al nivel de transporte del modelo OSI. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores. Los protocolos más importantes de esta capa son: TCP y UDP. El protocolo TCP es un protocolo orientado a conexión y fiable, y el protocolo UDP es un protocolo no orientado a conexión y no fiable.
4	Capa o nivel de aplicación.	Esta capa englobaría conceptos de las capas de sesión, presentación y aplicación del modelo OSI. Incluye todos los protocolos de alto nivel relacionados con las aplicaciones que se utilizan en Internet.

Una comparativa de esta arquitectura con el modelo OSI podemos verla en el siguiente gráfico.

Capas según el modelo OSI		Capas según el modelo TCP/IP	
7	Aplicación *Application*	4	Aplicación *Process*
6	Presentación *Presentation*		
5	Sesión *Session*		
4	Transporte *Transport*	3	Transporte *Host-to-Host*
3	Red *Network*	2	Internet *Network*
2	Enlace de datos *Data Link*	1	Acceso al medio *Media*
1	Física *Physical*		

La arquitectura TCP/IP se estructura en capas jerarquizadas y es el utilizado en Internet, por lo que en algunos casos oiréis hablar de Familia de Protocolos de Internet refiriéndose a está arquitectura cuando trabaja en Internet.

Es conveniente recordar que en algunos casos se divide la capa de acceso a la red, en capa de hardware o física y enlace de datos, con lo que la arquitectura tendría cinco niveles en vez de cuatro. Esto suele hacerse en referencia al modelo OSI. En realidad, esto se puede hacer y no cambiaría la estructura de la arquitectura.



2.5.EL NIVEL DE ACCESO A LA RED

La arquitectura TCP/IP en su estandarización original no se preocupaba demasiado del nivel físico en sí, de hecho, en un principio sólo se preocupó de estandarizar los protocolos relacionados con el enlace de datos, de ahí el nombre de este nivel.

Posteriormente con el auge de las redes de todo tipo, se vio que los estándares que ya existían desde un punto de vista físico, cada vez se tenían que tener más en cuenta, y por esto algunos autores, desarrolladores y diseñadores consideran que la arquitectura TCP/IP realmente consta de cinco capas, siendo la primera la capa física o de hardware y la segunda la de enlace de datos, tal y como recomienda el modelo OSI.

Para nosotros nos basta con considerarla como una sola, tal y como viene referido en el RFC 1122, documento que define el modelo TCP/IP.

La principal función de este nivel es convertir la información suministrada por el nivel de red, en señales que puedan ser transmitidas por el medio físico. La función inversa es convertir las señales que llegan por el medio físico en paquetes de información manejables por el nivel de red.

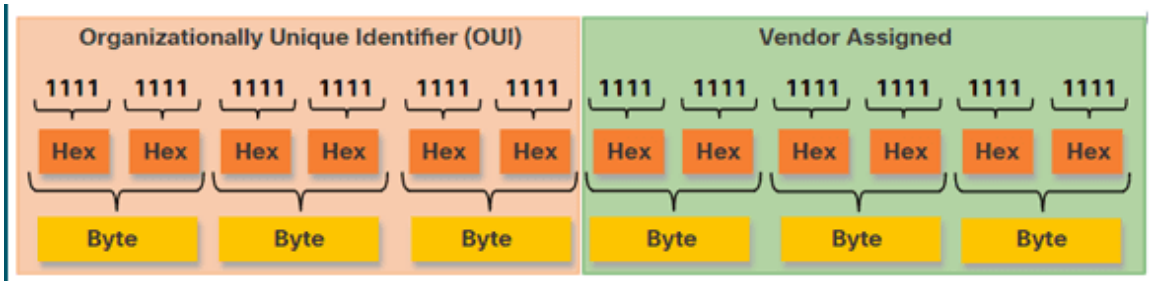
En este nivel se deben tener en cuenta las cuestiones relacionadas con las conexiones físicas, que en las redes locales vienen definidas por el estándar Ethernet. Este estándar define las características de cableado y señalización de nivel físico, y los formatos de las tramas de datos del nivel de enlace de datos. Ethernet es la base para el estándar **IEEE 802.3**, que es un estándar internacional que tiene posibilidades de uso tanto en redes locales como en redes de área amplia.

Otro aspecto importante de este nivel es lo relacionado con el direccionamiento físico. Este concepto viene de lo que se considera una subcapa del nivel de enlace de datos, y que se llama control de acceso al medio, cuyas siglas en inglés, MAC, se utilizan para definir lo que se conoce como direcciones MAC.

La dirección MAC es un identificador de 48 bits, que suele representarse en forma de números hexadecimales, en un formato de 6 bloques de dos números hexadecimales, divididos por dos puntos. El formato es el siguiente:

FF:FF:FF:FF:FF:FF

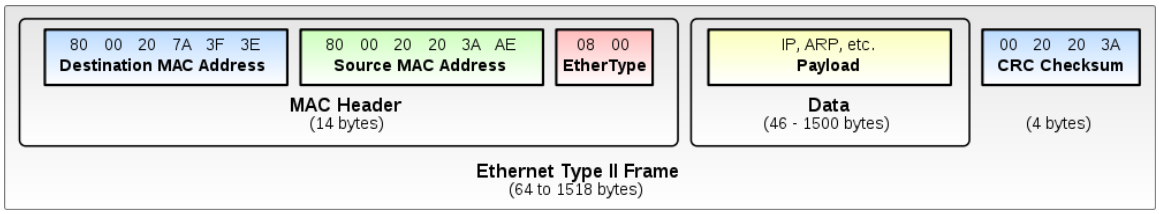
Los 24 bits más significativos (los de la izquierda) determinan el fabricante y se les conoce como Identificador Único de Organización y los 24 bits menos significativos (los de la derecha), identifican una interfaz concreta. De esta forma ninguna tarjeta de red tiene la misma dirección física.



En este nivel hay un protocolo relacionado con el direccionamiento físico. Este protocolo es el **ARP**.

ARP son las siglas en inglés del **protocolo de resolución de direcciones**, este protocolo trabaja a nivel de enlace de datos y se encarga de encontrar la dirección física o MAC que tiene relación con la correspondiente dirección lógica, que, como veremos en el siguiente apartado, se corresponde con la dirección IP. Lo que hace ARP es traducir direcciones lógicas (IP) a direcciones físicas (MAC). Existe su inverso el RARP que son las siglas en inglés del protocolo de resolución de direcciones inverso, hace la función inversa del protocolo ARP, pero no es tan utilizado.

Para terminar, mostramos el formato de la unidad de información de este nivel. Cada nivel tendrá una unidad de información, en este nivel se llama **TRAMA,** y tiene un formato determinado.



Sólo destacaremos que en la trama tenemos los datos que recibimos de las capas superiores, y que la capa de enlace le agrega una cabecera, con las direcciones MAC origen y destino, junto con el tipo de trama Ethernet que se utiliza, y una cola donde se agrega información para el control de errores.

2.5.1. Obtención de MAC en distintos sistemas operativos

Windows 2000/XP/Vista/7/8/10/11

En el entorno Windows la Dirección MAC se conoce como «dirección física». La manera más sencilla es abrir una terminal de línea de comandos («cmd» desde Inicio>Ejecutar) y allí usar la instrucción: `ipconfig /all`, o también se puede usar el comando `getmac`.

UNIX, GNU/Linux y Mac OS X

En el entorno de familia *nix (Mac Os X está basado en UNIX), habrá que abrir un terminal y ejecutar el comando: **ifconfig**. Esto nos muestra las interfaces seguidas de sus respectivas direcciones MAC en el epígrafe ether. (Nota: para ejecutar "ifconfig" algunas distribuciones requieren que se tengan privilegios de root: "sudo ifconfig").

Usando el paquete iproute2, es posible obtener las direcciones MAC de todas las tarjetas ethernet: "ip link list".

Tanto en Mac OS X 10.5, 10.7 o 10.9, para saber la dirección MAC basta con ir a Preferencias del Sistema > Red y dentro del apartado Wi-FI darle al botón Avanzado... En la ventana que saldrá, abajo del todo vendrá la dirección Wifi correspondiente a nuestro ordenador.

2.6. EL NIVEL DE INTERNET O DE RED.

El nivel de red del modelo TCP/IP se considera el nivel de la arquitectura más importante, ya que permite que las estaciones envíen información a la red en forma de paquetes. Estos paquetes viajan por la red de forma independiente, pudiendo atravesar diferentes redes y sin un orden establecido. Ésta es una de las principales ventajas de esta arquitectura y por eso es la base de Internet.

El objetivo principal del nivel de red será encaminar los paquetes desde el nodo origen hasta el nodo destino.

En la arquitectura TCP/IP la capa de red es casi totalmente asimilable a la capa de red del modelo OSI, pero en el caso de la arquitectura TCP/IP la capa de red no se preocupa de las tareas de ordenación de los paquetes cuando llegan a su destino. Esto es lo que se conoce como servicio no orientado a conexión. Cuando los paquetes se tratan de forma independiente, conteniendo cada uno la dirección de destino, se dice que se usa la técnica de datagrama, por tanto, Internet es una red de conmutación de paquetes basada en datagramas.

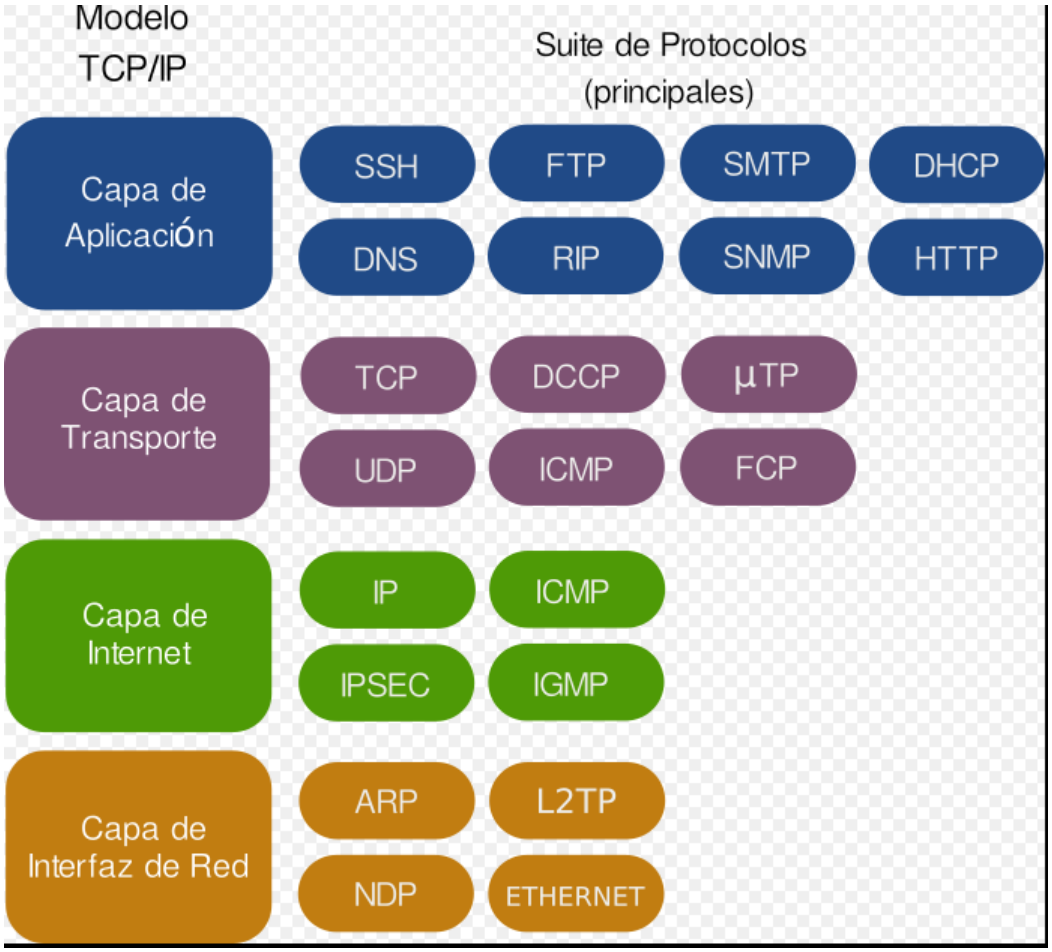
Entre las funciones de la capa de red se encuentra:

- **El direccionamiento:** Permite identificar de forma única cada nodo de la red. Cuando se habla de direccionamiento en este nivel, se está hablando de direccionamiento lógico, para distinguirlo del direccionamiento físico que ya hemos visto anteriormente.
- **La conectividad:** Conseguir que los nodos de una red se conecten, independientemente de la red a la que pertenezcan.
- **El enrutamiento:** También llamado encaminamiento, los protocolos de esta capa deben ser capaces de encontrar el mejor camino entre dos nodos.
- **El control de la congestión:** Es conveniente realizar un control del tráfico, ya que si un nodo recibe más información de la que puede procesar, se produce una saturación y este problema puede extenderse a toda la red.

Para realizar todas estas funciones el nivel de red utiliza diferentes protocolos, entre los protocolos más destacados de este nivel tenemos:

- **IP:** Internet Protocol, o Protocolo de Internet proporciona un enrutamiento de paquetes no orientado a conexión y es usado tanto por el origen como por el destino para la comunicación de datos.
- **ARP y RARP:** También se utilizan en la capa de enlace de datos y sirven para relacionar direcciones IP con direcciones MAC y viceversa.
- **ICMP:** Protocolo de mensajes de control en Internet, suministra capacidades de control y envío de mensajes. También se considera protocolo del nivel de transporte, y herramientas tales como ping y tracert lo utilizan para poder funcionar.

- **OSPF:** Es un protocolo de enrutamiento que busca el camino más corto entre dos nodos de la red.
- **RIP:** Protocolo de enrutamiento de información, al igual que OSPF, también busca el camino más corto, pero utilizando otras técnicas de enrutamiento.



2.6.1. IP (Internet Protocol)

Como se puede comprobar este nivel tiene varias funciones, y varios protocolos, pero podemos decir que el más importante de todos, de hecho, da nombre a la arquitectura, es el protocolo IP.

El protocolo IP, además de lo mencionado anteriormente, también proporciona las direcciones IP. Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz dentro de una red que utilice el protocolo de Internet. Más adelante conocerás más sobre el direccionamiento IP, pero ahora es conveniente que conozcas que existen dos versiones IPv4 (IP versión 4) e IPv6 (IP versión 6). Se diferencian en el número de bits que utilizan, versión 4 utiliza direcciones de 32 bits y la versión 6 utiliza direcciones de 128 bits.

El Protocolo de Internet (IP) es un componente fundamental de las redes de comunicación, incluyendo Internet. IP es un conjunto de reglas y protocolos que rigen la forma en que los datos se envían, enrutados y recibidos en una red de computadoras.

En el corazón del Protocolo de Internet se encuentran las direcciones IP. Estas son etiquetas numéricas únicas que se asignan a cada dispositivo conectado a una red IP. Existen dos versiones principales de direcciones IP: IPv4 (Protocolo de Internet versión 4) y IPv6 (Protocolo de Internet versión 6).

- **IPv4:** Utiliza direcciones de 32 bits y se representa en formato decimal separado por puntos, como 192.168.1.1. IPv4 es ampliamente utilizado, pero el número limitado de direcciones disponibles ha llevado a problemas de agotamiento de direcciones.

- **IPv6:** Utiliza direcciones de 128 bits y se representa en un formato hexadecimal, como 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 se ha desarrollado para abordar la escasez de direcciones IPv4 y proporcionar un espacio de direcciones mucho más amplio.

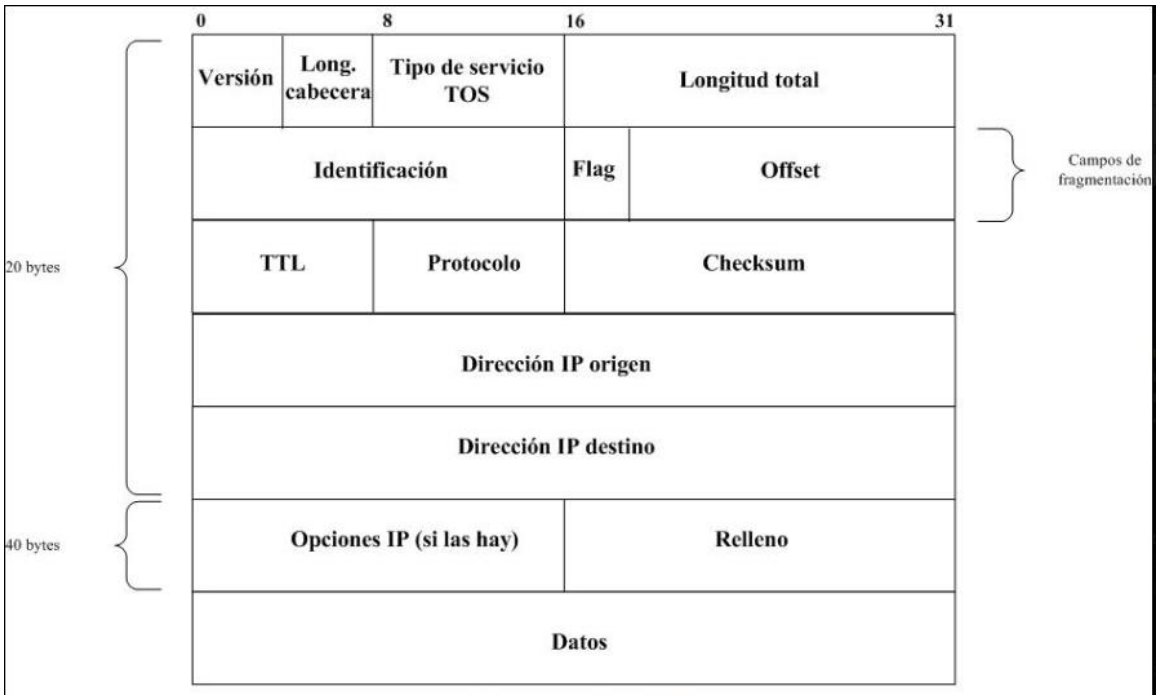
IP es esencial para el **enrutamiento de paquetes** en una red. Cada vez que un dispositivo envía datos a otro, esos datos se dividen en pequeños paquetes llamados "datagramas". Cada datagrama incluye la dirección IP del dispositivo de origen y del dispositivo de destino. Los enrutadores y conmutadores en la red utilizan esta información para transmitir los datagramas de un nodo a otro a través de la red, siguiendo la mejor ruta disponible.

El Protocolo de Internet es un protocolo **sin estado y sin conexión**, lo que significa que no mantiene un estado de conexión persistente entre los dispositivos. Cada datagrama se enruta de manera independiente, lo que permite una comunicación eficiente y escalable.

IP es un protocolo global que permite la comunicación a nivel mundial. Cada dispositivo en Internet tiene una dirección IP única, lo que facilita la identificación y la comunicación en la red global.

El Protocolo de Internet se utiliza en una amplia gama de aplicaciones, desde navegación web y correo electrónico hasta servicios en la nube, videoconferencias, juegos en línea, dispositivos de Internet de las cosas (IoT) y mucho más.

IPv4



IPv6

Los primeros 40 bytes (320 bits) son la cabecera del paquete y contiene los siguientes campos:

Offset del octeto		0								1								2								3							
	Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Versión				Clase de tráfico								Etiqueta de flujo																			
4	32	Longitud del campo de datos																Cabecera siguiente								Límite de saltos							
8	64	Dirección de origen																															
C	96																																
10	128																																
14	160																																
18	192	Dirección de destino																															
1C	224																																
20	256																																
24	288																																

- Direcciones de origen (128 bits)
- Direcciones de destino (128 bits)
- Versión del protocolo IP (4 bits)

- Clase de tráfico (8 bits, Prioridad del Paquete)
- Etiqueta de flujo (20 bits, manejo de la Calidad de Servicio)
- Longitud del campo de datos (16 bits)
- Cabecera siguiente (8 bits)
- Límite de saltos (8 bits, Tiempo de Vida).

2.7.EL NIVEL DE TRANSPORTE

Cumple la función de establecer las reglas necesarias para establecer una conexión entre dos dispositivos remotos. Al igual que las capas anteriores, la información que maneja esta capa tiene su propio nombre y se llama **segmento**.

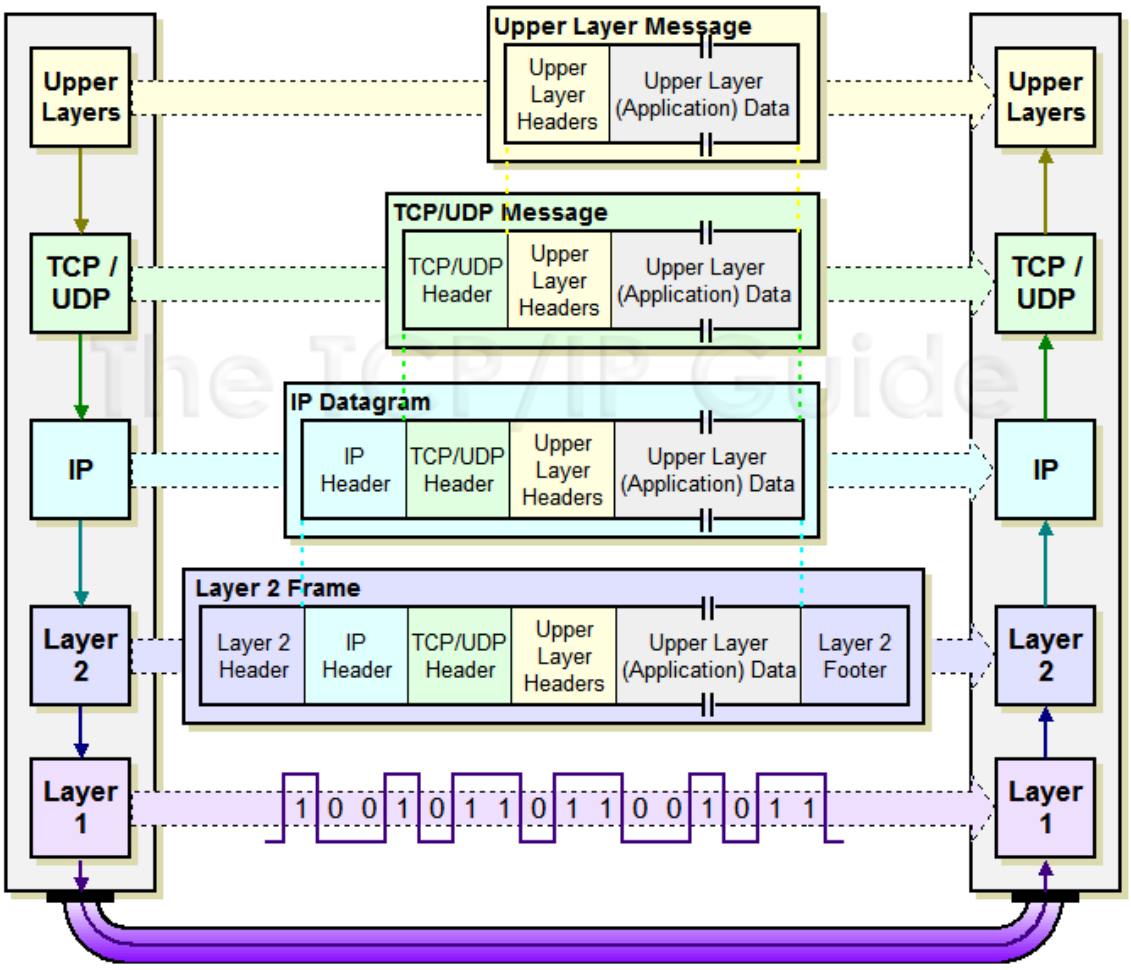
Por tanto, la capa de transporte se debe de encargar de unir múltiples segmentos del mismo flujo de datos. Como la capa de red en la arquitectura TCP/IP no se preocupa del orden de los paquetes ni de los errores, es en esta capa donde se deben cuidar estos detalles.

El nivel de transporte de la arquitectura de TCP/IP es totalmente asimilable al nivel de transporte del modelo OSI, por tanto, podemos decir que este nivel es el encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. La tarea de este nivel es proporcionar un transporte de datos confiable de la máquina de origen a la máquina destino, independientemente de la red física.

En este nivel trabajan varios protocolos, pero los dos más importantes son el **TCP** y el **UDP**. Como vimos anteriormente:

- **TCP es un protocolo orientado a conexión y fiable,** se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de redes no fiables. Por eso es tan útil en Internet, ya que a diferencia del tráfico en una sola red donde conoceremos sus características, las redes que configuran Internet podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete, etc. Pero TCP tiene un diseño que se adapta de manera dinámica a las propiedades de estas redes y permite la conexión en muchos tipos de situaciones.

- **UDP es un protocolo no orientado a conexión y no fiable,** este protocolo proporciona todo lo necesario para que las aplicaciones envíen datagramas IP encapsulados sin tener una conexión establecida. Uno de sus usos es en la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.



Cuando un proceso de aplicación quiere establecer comunicación con otro proceso de aplicación remoto, debe especificar a cuál se conectará. El método que normalmente se emplea es el de definir direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexión. Estos puntos terminales se llaman **puertos**.

Por tanto, un puerto serán las direcciones de transporte en las que los procesos pueden estar a la escucha de solicitudes de conexión. El termino puerto se utiliza en Internet, el termino genérico es el de **Punto de Acceso al Servicio de Transporte**, cuyas siglas en inglés son TSAP.

Los números de puertos son utilizados por TCP y UDP para identificar las sesiones que establecen las distintas aplicaciones. Algunos puertos son:

- 20: datos de FTP (Protocolo de transferencia de ficheros).
- 21: control de FTP.
- 53: DNS (Servicio de nombres de dominio).
- 80: http (Protocolo utilizado para servir y descargar páginas web).

Puertos: Service Name and Transport Protocol Port Number Registry (iana.org)

2.8. EL NIVEL DE APLICACIÓN

El nivel aplicación contiene los programas de usuario (aplicaciones) que hace que nuestro ordenador pueda crear textos, chatear, leer correo, visitar páginas web, etc.

En este nivel se incluyen todos los protocolos de alto nivel que utilizan los programas para comunicarse.

En la arquitectura TCP/IP este nivel incluye a los niveles de sesión, presentación y aplicación del modelo OSI.

Algunos de los protocolos de la capa de aplicación son:

- **FTP**: Protocolo utilizado en la transferencia de ficheros entre un ordenador y otro.
- **DNS:** Servicio de nombres de dominio, es el sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones de red.
- **SMTP**: Protocolo simple de transferencia de correo, basado en texto y utilizado para el intercambio de mensajes de correo. Está basado en el concepto cliente-servidor, donde un cliente envía un mensaje a uno o varios servidores.
- **POP**: Protocolo de oficina de correo, se utiliza en los clientes de correo para obtener los mensajes de correo almacenados en un servidor.
- **SNMP**: Protocolo de administración de redes, permite monitorizar y controlar los dispositivos de red y de administrar configuraciones y seguridad.
- **HTTP**: Protocolo de transferencia de hipertexto, es el protocolo utilizado en las transacciones de páginas web. Define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Tiene una versión segura que es el HTTPS.

2.9. Socket

Una vez que conocemos los diferentes niveles de la arquitectura podemos definir el concepto de socket. Un socket, es una conexión que está formada por la unión de la dirección IP más el puerto que se utiliza para la conexión.

Un socket se utiliza para establecer conexiones de red, enviar y recibir datos, y permite que las aplicaciones se comuniquen entre sí, ya sea en la misma máquina o a través de una red, como Internet.

Un socket actúa como un punto de comunicación que permite que dos dispositivos, como computadoras, se conecten y se comuniquen entre sí a través de una red. Cada socket tiene una dirección única que consiste en una dirección IP y un número de

puerto. Ejemplo: 192.168.1.11:80, esto significa que el ordenador cuya dirección es 192.168.1.11 está utilizando el puerto 80, que está asociado al protocolo http del nivel de aplicación, por tanto, esto puede significar que el ordenador está visitando una página web o sirviendo una página web

Los sockets se utilizan en aplicaciones de red que utilizan protocolos de comunicación como TCP (Protocolo de Control de Transmisión) o UDP (Protocolo de Datagramas de Usuario). Estos protocolos definen cómo se establece, se mantiene y se cierra una conexión, así como cómo se envían y reciben los datos.

Los sockets pueden ser de varios tipos, incluyendo sockets de escucha (listening sockets) y sockets de conexión (connected sockets). Los sockets de escucha se utilizan para esperar nuevas conexiones entrantes, mientras que los sockets de conexión se utilizan para transmitir datos una vez que se ha establecido una conexión.

Cada socket está asociado con una dirección IP y un número de puerto. La dirección IP identifica el dispositivo o servidor en la red, mientras que el número de puerto identifica una aplicación o servicio específico en ese dispositivo. Esto permite que **múltiples aplicaciones se comuniquen en un solo dispositivo utilizando diferentes números de puerto.**

Los sockets permiten la comunicación bidireccional, lo que significa que tanto el emisor como el receptor pueden enviar y recibir datos a través del socket. Esto permite la interacción y el intercambio de información entre las aplicaciones en dos extremos de la conexión.

Los sockets se utilizan en una amplia variedad de aplicaciones, desde navegadores web que se conectan a servidores para cargar páginas web (utilizando sockets TCP) hasta aplicaciones de mensajería instantánea y juegos en línea que utilizan sockets UDP para transmitir datos en tiempo real.

En resumen, un socket es un mecanismo esencial para permitir la comunicación entre dispositivos a través de una red utilizando protocolos de comunicación como TCP o UDP. Permite que las aplicaciones se conecten, envíen y reciban datos de manera eficiente, lo que es fundamental para la programación de redes y la comunicación en aplicaciones distribuidas.

Este concepto seguro que te será de utilidad más adelante cuando programes servicios web o aplicaciones que utilicen Internet.

3. TOPOLOGÍAS DE RED Y MODOS DE CONEXIÓN.

La topología de red se define como la cadena de comunicación usada por los nodos que conforman una red para comunicarse. La topología puede referirse, tanto al camino físico como al lógico. Usualmente usaremos topología desde el punto de vista físico y por tanto lo consideraremos como la forma en que se conectan los ordenadores de una red. Entre las topologías de conexión podemos citar: en bus, en anillo, en estrella, en árbol o jerárquica, en malla, doble anillo, mixta y totalmente conexa.

Cuando se hace una instalación de red es conveniente realizar un esquema de red donde se muestre la ubicación de cada ordenador, cada equipo de interconexión e incluso del cableado. Esto suele hacerse utilizando los planos del edificio o planta, donde está ubicada la red y es una herramienta útil a la hora del mantenimiento y actualización.

La topología o esquema lógicos, nos muestra el uso de la red, el nombre de los ordenadores, las direcciones, las aplicaciones, etc. En estos esquemas un grupo de ordenadores puede estar representado con un sólo icono. En la siguiente unidad utilizarás este tipo de esquemas.

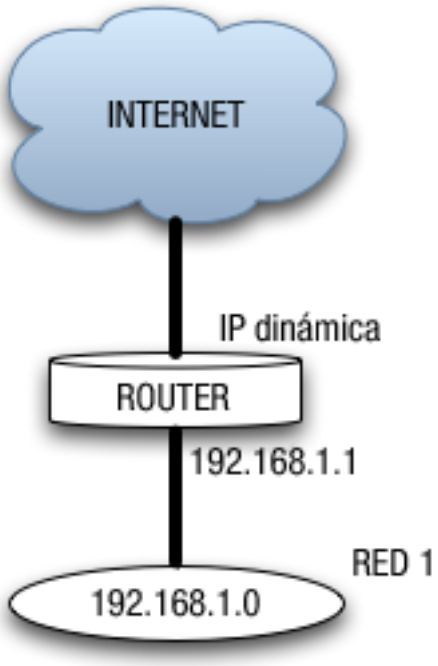
Como ejemplo te mostramos un gráfico donde se muestra una red de ordenadores que tendrá conexión a Internet gracias a un router. La red se representa con un óvalo donde dentro tiene la dirección de red y fuera el nombre de la red. Este tipo de esquemas lógicos pueden ser más o menos complejos, pero sirven para hacernos una idea de cómo está conectada una red. Existen programas que permiten realizar estos esquemas, pero pueden hacerse utilizando cualquier programa de dibujo, siempre y cuando se dejen claros todos los elementos que se representan en el gráfico.

Si tenemos en cuenta las topologías físicas, también pueden tener más o menos detalle en su representación, pero la idea fundamental es mostrar cómo están conectados los dispositivos desde un punto de vista físico, tal y como analizaremos más adelante.

Otro concepto relacionado con la forma de conectar los ordenadores en red es el de modo de conexión, este concepto está relacionado con las redes inalámbricas, representa cómo se pueden conectar ordenadores en red de forma inalámbrica. Se definen dos modos de conexión inalámbrica, que son:

- **Modo infraestructura:** Suele incluir un punto de acceso.
- **Modo ad-hoc**: No necesita punto de acceso.

Un poco más adelante veremos más detalles sobre estos dos modos de conexión. Sólo hay que comentar que estos modos de conexión se suelen utilizar fundamentalmente en el diseño de redes locales inalámbricas o redes Wi-Fi.

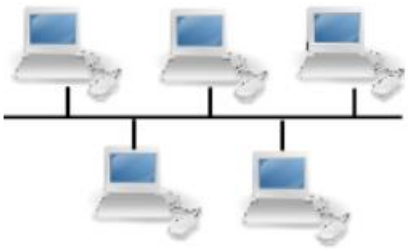


3.1. BUS Y ANILLO

La topología en bus utiliza un único cable troncal con terminaciones en los extremos, de tal forma que los ordenadores de la red se conectan directamente a la red troncal. Las primeras redes Ethernet utilizaban esta topología usando cable coaxial.

Actualmente se emplean variantes de la topología en bus en las redes de televisión por cable, en la conexión troncal de las redes de fibra óptica, y en la instalación y operación de máquinas y equipamientos industriales utilizados en procesos de producción.

Esquema de la topología en bus:



La topología en anillo conecta cada ordenador o nodo con el siguiente y el último con el primero, creando un anillo físico de conexión. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación. En este tipo de red la comunicación se da por el paso de un testigo, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. Las redes locales Token-ring emplean una topología en anillo aunque la conexión física sea en estrella.

Existen topologías de anillo doble donde dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos).

Esta topología se utiliza en las redes FDDI o Fiber Distributed Data Interface, en español Interfaz de datos distribuidos por fibra, que puede usarse como parte de una red troncal que distribuye datos por fibra óptica. En algunas configuraciones de servidores también se utiliza este tipo de topología.

Esquema de la topología en anillo:

3.2. ESTRELLA

La topología en estrella conecta todos los ordenadores a un nodo central, que puede ser: un router, un conmutador o switch, o, un concentrador o hub. Las redes de área local modernas basadas en el estándar IEEE 802.3 utilizan esta topología.

El equipo de interconexión central canaliza toda la información y por él pasan todos los paquetes de usuarios. Este nodo central realizará funciones de distribución, conmutación y control. Es importante que este nodo siempre esté activo, ya que si falla toda la red queda sin servicio.

Entre las ventajas de utilizar esta topología tenemos que esta topología es tolerante a fallos ya que si un ordenador se desconecta no perjudica a toda la red, además facilita la incorporación de nuevos ordenadores a la red siempre que el nodo central tenga conexiones, y permite prevenir conflictos de uso.

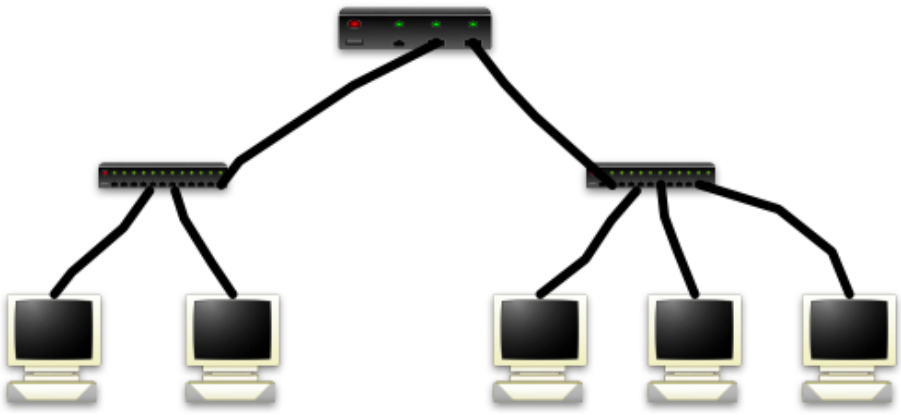
Un esquema de la topología es:

Una ampliación de la topología en estrella es la estrella extendida o árbol donde las redes en estrella se conectan entre sí.

Cuando la estrella extendida tiene un elemento de donde se parte, hablaremos de la topología en estrella jerárquica, donde a partir de redes conectadas en estrella conseguimos una red más amplia y que mantiene una jerarquía de conexiones, ya que tenemos un nodo que es el inicio de la jerarquía. Este nodo suele ser un router y a partir de él se crea una red de área local que permite dar servicios a redes de área locales más pequeñas.

Este tipo de topologías es muy típico en redes de área local donde el principio de la jerarquía será el router que conecta a Internet, usualmente el que nos pone la compañía de telecomunicaciones, y el resto son los switches que dan servicio a diferentes aulas, salas de ordenadores, despachos, etc.

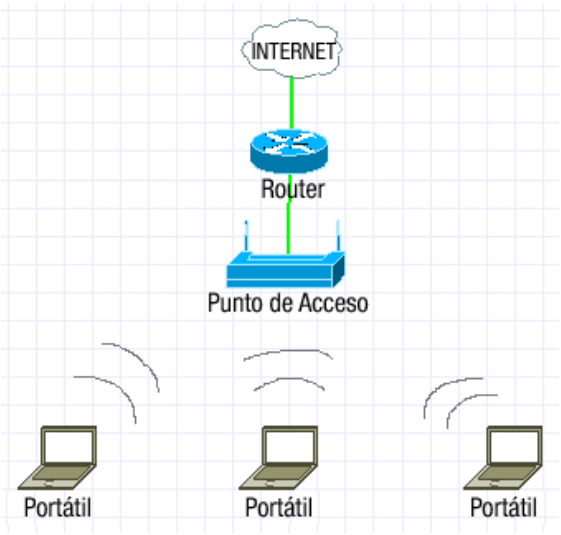
Un esquema de la topología jerárquica es:



Esta topología tiene la ventaja que, a partir de una única conexión a Internet, por ejemplo, podemos dar servicio a varias redes o subredes locales, con lo que ahorramos costes. Su principal desventaja está precisamente en la jerarquía, si el equipo de interconexión de mayor jerarquía falla, la red ya no presta los servicios para los cuales fue diseñada.

3.3. MODO INFRAESTRUCTURA Y MODO AD-HOC.

Como hemos visto, existen varias formas de conectar los ordenadores de una red que llamamos topologías, estas topologías, en principio, servirían como base para cualquier tipo de red de área local, ya sea cableada o inalámbrica. Pero en redes inalámbricas que siguen el estándar IEEE 802.11 se introduce un concepto diferente que es el de modo de conexión.



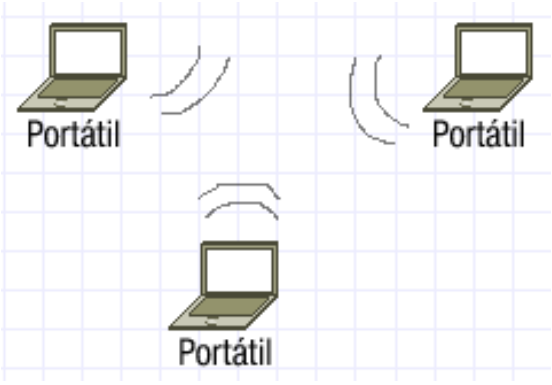
En las redes inalámbricas con estándar IEEE 802.11, también llamadas redes Wi-Fi se especifican dos modos de conexión, que son el modo infraestructura y el modo ad-hoc. Cabe mencionar, que algunas veces oiréis hablar de modo de conexión o topología de conexión en referencia a la forma de conectar los dispositivos inalámbricos, y modo de funcionamiento refiriéndose al funcionamiento del equipo. En nuestro caso preferimos utilizar el término modo de conexión.

El modo infraestructura se suele utilizar para conectar equipos inalámbricos a una red cableada ya existente. Su principal característica es que utiliza un equipo de interconexión como puente entre la red inalámbrica y la cableada. Este equipo de interconexión se denomina **Punto de Acceso** y puede ser un equipo especialmente diseñado para ello que sólo haga esta función, o puede ser un router con características de punto de acceso. Usualmente se suele utilizar como punto de acceso a la infraestructura de cable que permite la conexión a Internet, el router inalámbrico que instala la compañía de telecomunicaciones.

En el modo infraestructura todo el tráfico de la red inalámbrica se canaliza a través del punto de acceso, y todos los dispositivos inalámbricos deben estar dentro de la zona de cobertura del punto de acceso, para poder establecer una comunicación entre ellos.

El modo ad-hoc permite conectar dispositivos inalámbricos entre sí, sin necesidad de utilizar ningún equipo como punto de acceso. De esta forma cada dispositivo de la red forma parte de una red de igual a igual (Peer to Peer).

Este tipo de conexión permite que se pueda compartir información entre equipos que se encuentren en un lugar determinado de forma puntual, por ejemplo una reunión, también se puede utilizar para conectar dispositivos de juegos para jugar unos con otros.



Una tercera posibilidad es combinar ambos modos de conexión, para aprovechar las ventajas de ambos.

4. Componentes de una red informática.

En este punto daremos un repaso a algunos de los componentes más importantes, de los que componen una red informática. Como ya hemos visto, una **red de ordenadores** o **red informática** es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos y ofrecer servicios. Este término también engloba aquellos medios técnicos que permiten compartir la información.

Por tanto, podemos considerar componentes de la red a los propios ordenadores con sus sistemas operativos que permiten utilizarla, y a todo el hardware y el software que ayuda a que la red funcione. En este punto nosotros nos centraremos en el hardware, ya que el software lo vas a estudiar en siguientes unidades.

Algunos de estos componentes serán:

- El **cableado de red** y sus **conectores**, que permite la transmisión de la señal.
- El **rack** o armario de conexiones, es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- Los **patch panel**, paneles de conexión que sirven de terminadores del cableado y ayudan a organizarlo.
- Las **tarjetas de red**, que permitirán la conexión del ordenador, bien por cable o de forma inalámbrica.

- Los **conmutadores** o switch, que permiten la conexión de diferentes ordenadores entre sí y de segmentos de red entre sí.
- Los **enrutadores** o router, también conocidos como encaminadores, que permiten conectar redes diferentes, como por ejemplo una red de área local con Internet.
- Los **puntos de acceso**, que permiten la interconexión de dispositivos inalámbricos entre sí, y/o la conexión de dispositivos cableados con los inalámbricos.
- Los **cortafuegos**, que pueden ser dispositivos hardware con un software específico para bloquear acceso no autorizados a la red, o software específico que se instale en los ordenadores y/o servidores para evitar los accesos no autorizados.
- Los **servidores**, que no son más que ordenadores con un sistema operativo específico para actuar como servidor, o con sistemas operativos no servidores, pero con software de servidor.

Además de estos componentes, también consideramos como parte de la red a los ordenadores que trabajarán en red, que en muchos casos se les llama **estaciones de trabajo.** Cualquier dispositivo que se pueda conectar a la red para prestar algún servicio, tales como impresoras, discos duros de red, o cualquier periférico que esté conectado a algún ordenador de la red, es también un componente de la red y se les suele denominar **nodos de red**.

Antes de desarrollar alguno de los conceptos explicados, cabe mencionar que entre los servidores de red que prestarán servicio a la red, podemos encontrar: servidores de archivos, de correo, de páginas web, de impresión, etc.

4.1. CLASIFICACIÓN DE LOS MEDIOS DE TRANSMISIÓN.

El medio de transmisión constituye el canal que permite la transmisión de información entre dos terminales en un sistema de transmisión. Por tanto, en las redes de ordenadores serán los canales que transmiten la información entre los nodos de la red, ya sean ordenadores, servidores, etc. Las transmisiones se realizan habitualmente empleando ondas electromagnéticas que se propagan a través del canal.

A veces el canal es un medio físico y otras veces no, ya que las ondas electromagnéticas son susceptibles de ser transmitidas por el vacío. Por esto podemos clasificar los medios de transmisión como:

- **Medios guiados:** conducen las ondas electromagnéticas a través de un camino físico.
- **Medios no guiados:** proporcionan un soporte para que las ondas se transmitan, pero no las dirigen.

Por tanto, cuando hablemos de medios guiados nos estaremos refiriendo a los distintos tipos de cables que se pueden utilizar. Entre los tipos de cables más utilizados

encontramos el par trenzado, el coaxial y la fibra óptica. Más adelante daremos más detalles sobre ellos.

Cuando nos referimos a medios no guiados nos estamos refiriendo a la posibilidad de transmitir ondas electromagnéticas, a través del aire o del vacío. Esta particularidad permite montar redes inalámbricas y tener sistemas de telecomunicaciones sin cable, como por ejemplo el teléfono móvil o la conexión a Internet a través del móvil.

4.2. Principales medios de transmisión:

Medios de transmisión por cable o guiados:

a. Cable de cobre:

- **Cable de par trenzado:** Este es el tipo de cable más común utilizado en redes locales (LAN) y telefonía. Consiste en pares de cables de cobre trenzados entre sí para reducir la interferencia electromagnética. Hay dos categorías principales: UTP (par trenzado sin blindaje) y STP (par trenzado apantallado).
- **Cable coaxial:** Se utiliza en aplicaciones de banda ancha, como la transmisión de señales de televisión por cable. Consta de un núcleo conductor central rodeado de un escudo metálico y una cubierta aislante.

b. Fibra óptica:

La fibra óptica utiliza pulsos de luz para transmitir datos a través de fibras de vidrio o plástico. Ofrece numerosas ventajas, como alta velocidad de transmisión, inmunidad a interferencias electromagnéticas y capacidad para transmitir datos a largas distancias. Hay dos tipos principales: monomodo (utilizada para distancias largas) y multimodo (usada para distancias más cortas).

Medios de transmisión inalámbricos o no guiados:

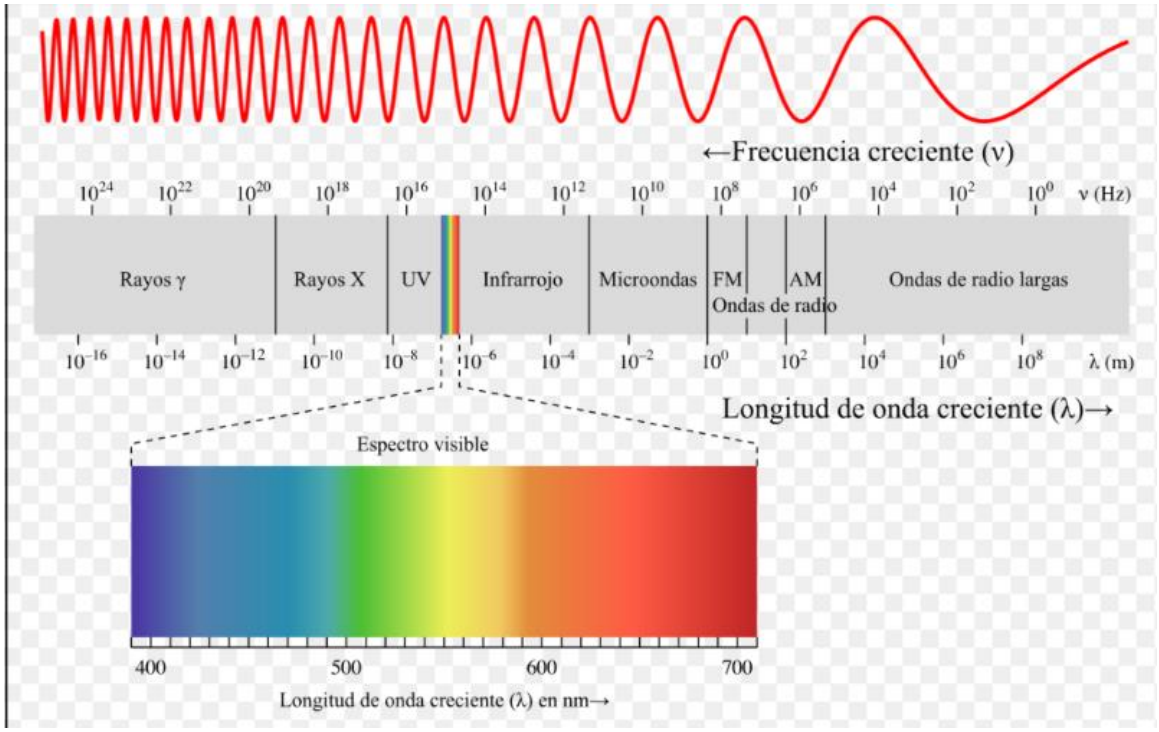
En este tipo de medios, la transmisión y la recepción de información se lleva a cabo a través de antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario, en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

Para las transmisiones no guiadas, la configuración puede ser:

- **Direccional,** en la que la antena transmisora emite la energía electromagnética concentrándola en un haz, por lo que las antenas emisora y receptora deben estar alineadas; y
- **Omnidireccional,** en la que la radiación se hace de manera dispersa, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas.

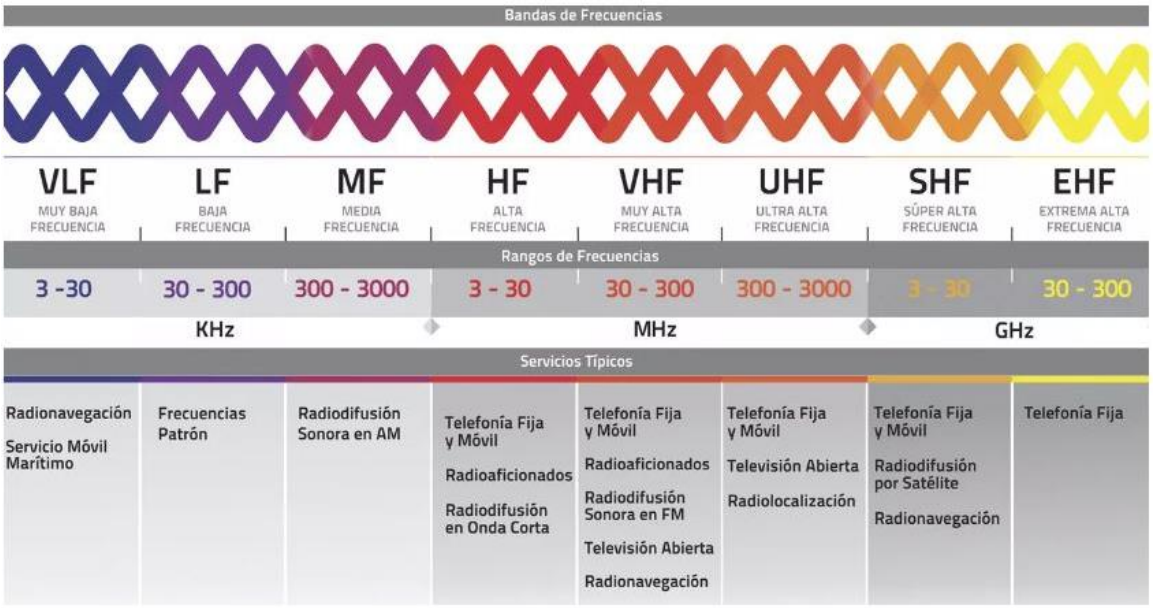
Generalmente, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

La transmisión de datos a través de medios no guiados añade problemas adicionales, provocados por la reflexión que sufre la señal en los distintos obstáculos existentes en el medio. Resultando más importante el **espectro de frecuencias** de la señal transmitida que el propio medio de transmisión en sí mismo.



Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos:

- Radiofrecuencia u ondas de radio
- Microondas
  - terrestres
  - satelitales
- Luz
  - infrarroja
  - láser



a. Ondas de radio:

Las ondas de radio se utilizan en una variedad de aplicaciones, como redes Wi-Fi, comunicaciones celulares y radio. Operan en el espectro de radiofrecuencia y pueden transmitir datos a través del aire.

En radiocomunicaciones, aunque se emplea la palabra “radio”, las transmisiones de televisión, radio (radiofonía o radiodifusión), radar y telefonía móvil están incluidas en esta clase de emisiones de radiofrecuencia. Otros usos son audio, video, radionavegación, servicios de emergencia y transmisión de datos por radio digital; tanto en el ámbito civil como militar. También son usadas por los radioaficionados.

b. Microondas:

Además de su aplicación en hornos microondas, las microondas permiten transmisiones tanto con antenas terrestres como con satélites. Dada sus frecuencias, del orden de 1 a 10 Ghz, las microondas son muy direccionales y solo se pueden emplear en situaciones en que existe una línea visual entre emisor y receptor. Los enlaces de microondas permiten grandes velocidades de transmisión, del orden de 10 Mbps. es lo más relevante acerca de los microondas...

Las microondas se utilizan para comunicaciones de punto a punto a larga distancia, como las enlaces entre torres de telecomunicaciones. Utilizan señales de alta frecuencia en el rango de las microondas para transmitir datos.

c. Infrarrojos:

La radiación infrarroja, o radiación IR es un tipo de radiación electromagnética, de mayor longitud de onda que la luz visible, pero menor que la de los microondas. Por

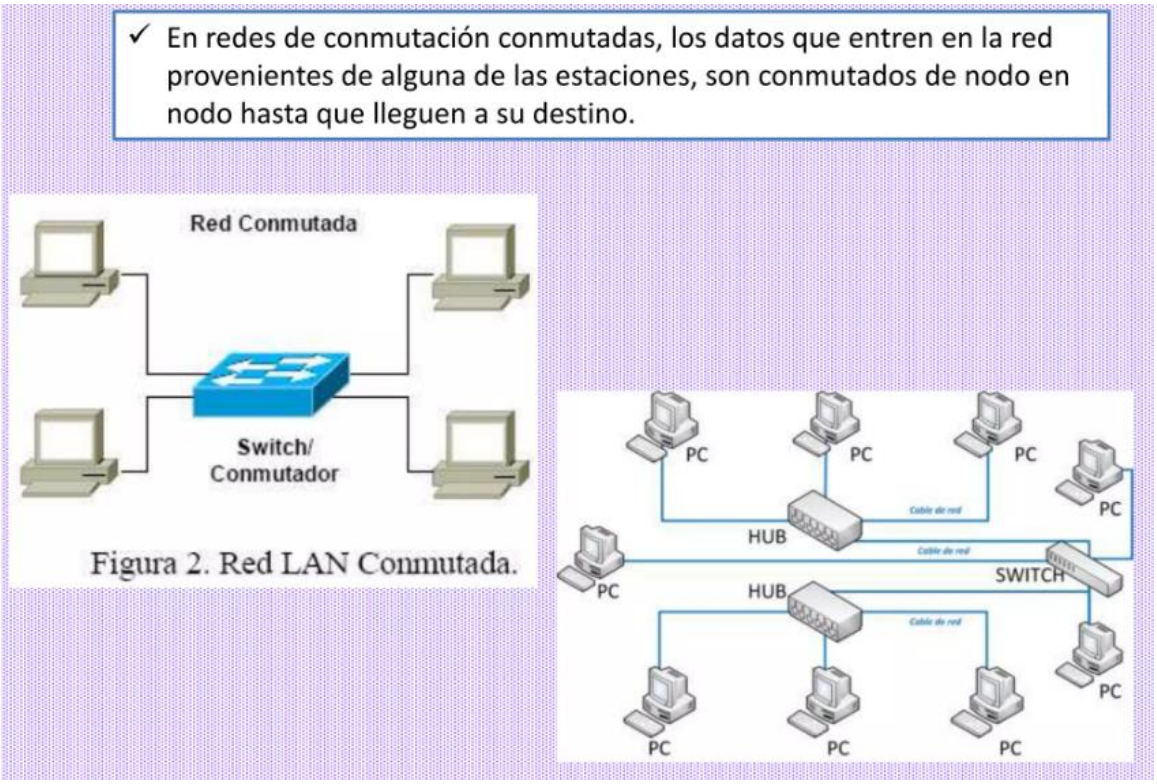
ello, tiene menor frecuencia que la luz visible y mayor que las microondas. Su rango de longitudes de onda va desde unos 0,7 hasta los 1000 micrómetros.1 La radiación infrarroja es emitida por cualquier cuerpo cuya temperatura sea mayor que 0 Kelvin, es decir, −273,15 grados Celsius (cero absoluto).

Por tanto, es invisible para el ojo humano. Por lo general, se entiende que el IR abarca longitudes de onda desde el borde nominal del rojo del espectro visible, alrededor de 700 nanómetros (frecuencia 430 THz), hasta 1 milímetro (300 GHz)2 (aunque las longitudes de onda IR más largas suelen designarse más bien como radiación de terahercios). La radiación del cuerpo negro de los objetos cercanos a la temperatura ambiente es casi toda de longitud de onda infrarroja. Como forma de radiación electromagnética, la radiación infrarroja propaga energía y momento, con propiedades que corresponden a la dualidad onda-partícula de una onda y de una partícula, el fotón. Los dispositivos de control remoto utilizan señales infrarrojas para transmitir comandos a equipos como televisores y equipos de audio. El alcance es limitado y requiere línea de visión directa.

Medios de transmisión en red:

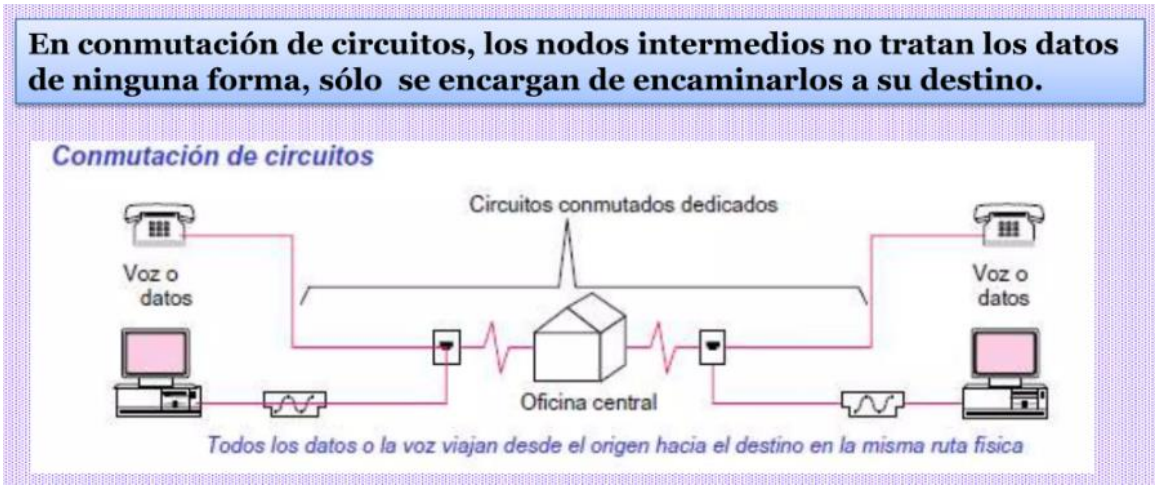
a. Red de conmutación de paquetes:

En una red de conmutación de paquetes, los datos se dividen en paquetes que se transmiten de manera independiente a través de la red. Los protocolos IP (Internet Protocol) son un ejemplo común de este tipo de red, utilizada en Internet y muchas redes de datos.



b. Red de conmutación de circuitos:

En una red de conmutación de circuitos, se establece una conexión dedicada y reservada durante la duración de la comunicación. Esto se utiliza en las llamadas telefónicas tradicionales, donde se reserva un circuito para la llamada.



4.3.CABLEADO Y CONECTORES

En este punto vamos a hacer un resumen de los tipos de cables más utilizados en la conexión de redes de ordenadores y los conectores más utilizados.

4.3.1.PAR TRENZADO

El cable más utilizado en redes de área local es el **par trenzado** de ocho hilos. Consta de ocho hilos con colores diferentes y se utiliza en redes de ordenadores bajo el estándar IEEE 802.3 (Ethernet).

Los colores son: blanco-naranja, naranja, blanco-verde, verde, blanco-azul, azul, blanco-marrón y marrón. La distribución de estos colores cuando se conectan en el conector viene estandarizada, para que las conexiones de red sean fácilmente reconocibles.

Existen dos tipos principales de cables de par trenzado:

- **Par trenzado no apantallado (UTP):** Este tipo de cable se utiliza comúnmente en redes Ethernet y es ampliamente utilizado en aplicaciones de redes locales (LAN) y en sistemas de telefonía. Los cables UTP no tienen una capa de blindaje adicional y se dividen en diferentes categorías, como Cat 5e, Cat 6, Cat 6a y Cat 7, según su capacidad de transmisión y velocidad.
- **Par trenzado apantallado (STP):** Los cables STP incluyen una capa de blindaje que rodea los pares de cables trenzados. Este blindaje ayuda a proteger la señal de interferencias electromagnéticas y es más común en entornos donde la interferencia es un problema, como entornos

industriales. Los cables STP también se utilizan en ciertas aplicaciones de redes.

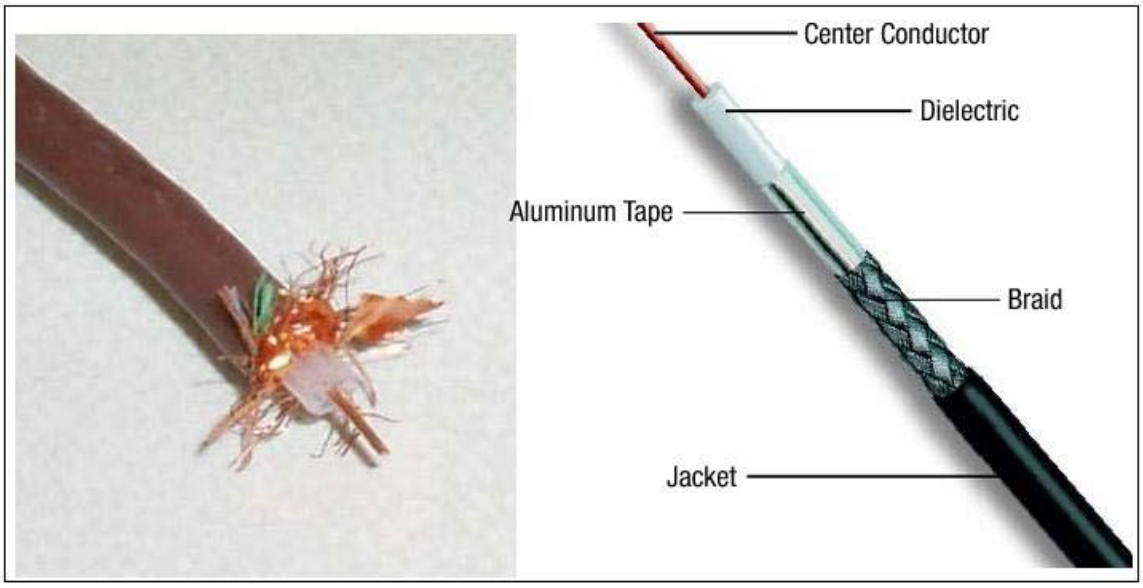
Los conectores para cable de par trenzado son componentes esenciales en las redes de comunicación y se utilizan para conectar cables de par trenzado a dispositivos, como computadoras, switches, enrutadores, cámaras de red, teléfonos, entre otros. Los conectores se utilizan para establecer conexiones seguras y confiables en sistemas de cableado estructurado, como Ethernet. Aquí tienes algunos de los conectores más comunes utilizados con cables de par trenzado:

- RJ-45: Este es el conector más comúnmente utilizado en redes Ethernet. Es un conector modular de 8 pines que se usa para conectar cables de par trenzado a dispositivos de red, como computadoras, switches y enrutadores.
- RJ-11: Aunque se parece al RJ-45, es más pequeño y se utiliza comúnmente en conexiones de telefonía y líneas DSL. Es un conector modular de 6 pines.
- RJ-12: Similar al RJ-11, es un conector modular de 6 pines, pero se utiliza en aplicaciones que requieren más conductores, como algunas líneas de telefonía y sistemas de control.
- Conector BNC: Estos conectores se utilizan en aplicaciones de redes de video y algunas redes de datos. Son más comunes en aplicaciones de video analógico.
- Conector de 8P8C: Este es un conector de 8 pines y 8 contactos que se utiliza en aplicaciones de redes Ethernet. Es funcionalmente equivalente al RJ-45 y se usa en muchos cables Ethernet.
- Conector modular de 4P4C: Estos conectores tienen 4 pines y 4 contactos y se utilizan comúnmente en cables telefónicos o cables de consola.
- Conector modular de 6P6C: Este es un conector de 6 pines y 6 contactos que se usa en aplicaciones diversas, como algunos sistemas de control y comunicaciones de datos.
- Conector modular de 10P10C: Estos conectores tienen 10 pines y 10 contactos y se utilizan en aplicaciones específicas que requieren más conductores, como algunos sistemas telefónicos y de datos.

4.3.2. COAXIAL

También se utiliza en las redes de ordenadores, el **cable coaxial**. El cable coaxial es un tipo de cable de transmisión utilizado en aplicaciones de comunicación para transmitir señales eléctricas, como señales de televisión por cable, transmisiones de radio, transmisiones de datos y redes de banda ancha, entre otros. Está compuesto por varios componentes clave que lo hacen adecuado para estas aplicaciones:

- **Conductor central:** En el centro del cable coaxial se encuentra un conductor central, generalmente hecho de cobre o aluminio, que transporta la señal eléctrica.
- **Aislamiento dieléctrico:** Alrededor del conductor central hay una capa de aislamiento dieléctrico que mantiene separado el conductor central del blindaje exterior. El aislamiento dieléctrico puede estar hecho de materiales como polietileno o polipropileno.
- **Blindaje**: El aislamiento dieléctrico está rodeado por una capa de blindaje metálico, que puede ser una malla de alambre o una lámina de metal. El blindaje tiene varias funciones, incluyendo la protección de la señal contra interferencias electromagnéticas externas y la prevención de fugas de señal.
- **Cubierta protectora:** En la parte exterior, el cable coaxial tiene una cubierta protectora, generalmente de plástico o PVC, que protege el cable y proporciona resistencia mecánica.



El cable coaxial es conocido por su capacidad para transportar señales de alta frecuencia a lo largo de distancias relativamente largas. Las características eléctricas del cable coaxial, como la impedancia característica, varían según el tipo de cable. Los tipos de cable coaxial más comunes incluyen:

- **RG-6:** Se utiliza comúnmente en la transmisión de señales de televisión por cable y satélite, así como en aplicaciones de banda ancha.
- **RG-59:** Anteriormente utilizado en transmisiones de señales de televisión analógica, todavía se encuentra en algunas instalaciones, pero ha sido reemplazado en gran medida por RG-6.

- **RG-11:** Es un cable coaxial más grueso y se utiliza para aplicaciones de transmisión de señales de larga distancia, como transmisiones de cable de alta potencia.

Los conectores utilizados con cables coaxiales varían según la aplicación y el tipo de cable coaxial. Algunos de los conectores más comunes para cables coaxiales incluyen:

- **Conector tipo F:** Este conector es comúnmente utilizado en aplicaciones de televisión por cable y satélite, así como en sistemas de distribución de señal de video. Es fácil de instalar y tiene una rosca que asegura una conexión firme. Los conectores tipo F son comunes en cables RG-6 y RG-59.
- **Conector BNC (Bayonet Neill-Concelman):** Los conectores BNC son populares en aplicaciones de vídeo y datos, y son conocidos por su facilidad de conexión y desconexión con un giro de bayoneta. Son ampliamente utilizados en equipos de vídeo profesional y sistemas de seguridad, así como en algunas aplicaciones de redes.
- **Conector N:** Los conectores N son utilizados en aplicaciones de radiofrecuencia y comunicaciones de alta potencia. Proporcionan una conexión segura y están diseñados para minimizar las pérdidas de señal a frecuencias más altas. Son comunes en aplicaciones como antenas y equipos de radioaficionados.
- **Conector SMA (SubMiniature version A):** Los conectores SMA son utilizados en aplicaciones de alta frecuencia, como equipos de radio, antenas GPS y equipos de comunicación inalámbrica. Vienen en versiones SMA macho y SMA hembra.
- **Conector TNC (Threaded Neill-Concelman):** Los conectores TNC son similares a los BNC, pero cuentan con una rosca en lugar de un giro de bayoneta para asegurar la conexión. Son utilizados en aplicaciones de alta frecuencia y radiofrecuencia.
- **Conector BNC de doble pila:** Este tipo de conector permite conectar dos cables coaxiales BNC juntos, creando una extensión de señal. Es útil en aplicaciones donde se necesita unir dos cables BNC para lograr la longitud adecuada.
- **Conector SMB (SubMiniature version B):** Estos conectores son utilizados en aplicaciones de comunicación de alta frecuencia, como en sistemas de posicionamiento global (GPS) y equipos de comunicación inalámbrica.
- **Conector UHF (Ultra High Frequency):** A pesar de su nombre, se utilizan en aplicaciones de radiofrecuencia de baja a media frecuencia, como en sistemas de radio de dos vías.

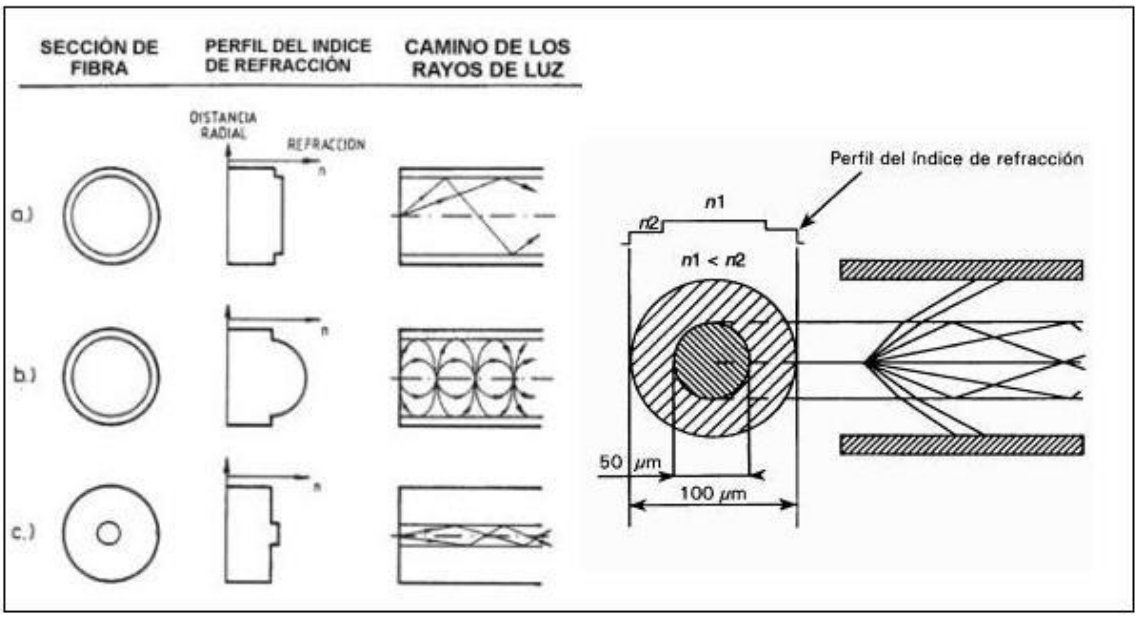
Actualmente el cable coaxial no se utiliza para montar redes de ordenadores, si no para la distribución de las señales de Televisión, Internet por cable, etc.

En la distribución de la señal de Internet por cable, el cable coaxial sirve para conectar la central de distribución de Internet que llega a la calle o barrio con la casa del abonado. En este caso se suele utilizar cable de tipo RG6, que permite diferentes configuraciones para incluir acometidas telefónicas y transmisión de datos.

4.3.3. FIBRA ÓPTICA

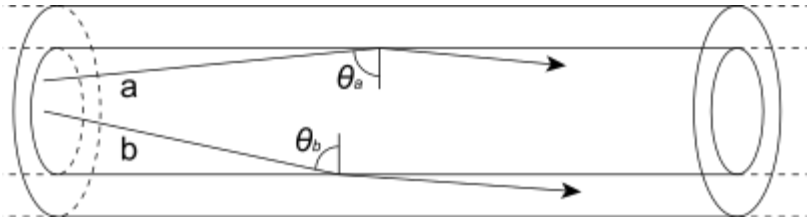
La **fibra óptica** es otro tipo de cable que se utiliza para la transmisión de datos. La fibra óptica es un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. La fuente de luz puede ser láser o un led, en las redes de ordenadores se suele utilizar el láser. Permite transmitir gran cantidad de datos a una gran distancia, a una velocidad adecuada, y al ser inmune a las interferencias electromagnéticas es muy fiable. Es utilizado en la distribución de señales de telecomunicaciones a largas distancias y en las redes locales, constituye la infraestructura de distribución de la señal que permite conectar redes entre sí, por ejemplo, en un mismo edificio. Esto último es conocido como **backbone**.

Tenemos dos tipos de fibra óptica, el multimodo y la monomodo. Como conectores se pueden utilizar de tipo FC y FDDI, entre otros.



Los principios básicos de su funcionamiento se justifican aplicando las leyes de la óptica geométrica, principalmente, la ley de la refracción (principio de reflexión interna total) y la ley de Snell (La ley de Snell-Descarte es una fórmula utilizada para calcular el ángulo de refracción de la luz al atravesar la superficie de separación entre dos medios de propagación de la luz (o cualquier onda electromagnética) con índice de refracción distinto).

Su funcionamiento se basa en transmitir por el núcleo de la fibra un haz de luz, tal que este no atraviese el revestimiento, sino que se refleje y se siga propagando. Esto se consigue si el índice de refracción del núcleo es mayor al índice de refracción del revestimiento, y también si el ángulo de incidencia es superior al ángulo límite.



Representación de dos rayos de luz propagándose dentro de una fibra óptica. En esta imagen se percibe el fenómeno de reflexión total en el haz de luz "a".

Tipos de Fibra Optica

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.

Fibra multimodo

Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 2 km, es simple de diseñar y económico.

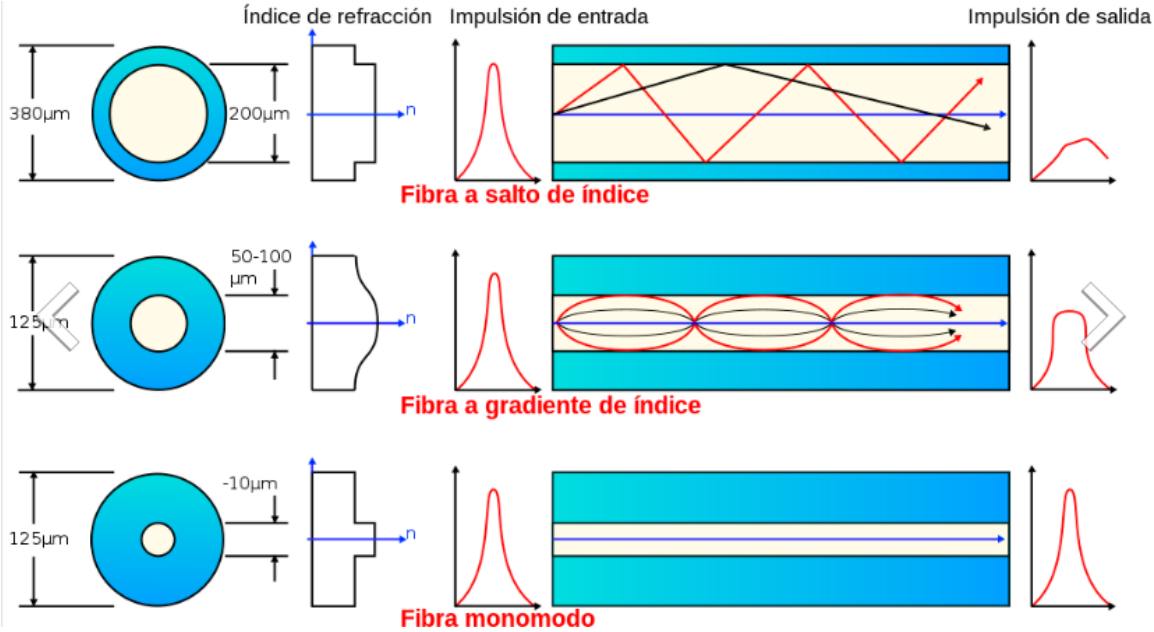
El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión.

Dependiendo del tipo de índice de refracción del núcleo, tenemos dos tipos de fibra multimodo:

- **Índice escalonado:** en este tipo de fibra, el núcleo tiene un índice de refracción constante en toda la sección cilíndrica, tiene alta dispersión modal.
- **Índice gradual:** mientras en este tipo, el índice de refracción no es constante, tiene menor dispersión modal y el núcleo se constituye de distintos materiales.

Fibra monomodo

Una fibra monomodo es una fibra óptica en la que solo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que solo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (10 Gbit/s)



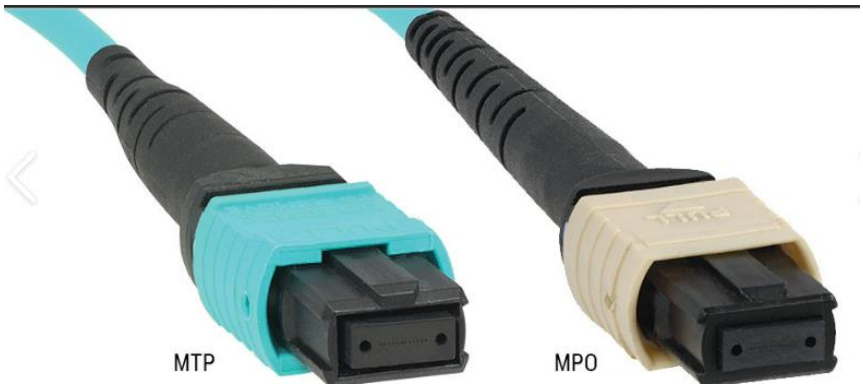
Los conectores de fibra óptica son componentes esenciales en sistemas de comunicación por fibra óptica, ya que permiten conectar y desconectar cables de fibra óptica de manera segura y confiable. Estos conectores están diseñados para alinear de manera precisa las fibras ópticas para garantizar la transmisión eficiente de señales de luz a través de ellas. Aquí tienes algunos de los conectores de fibra óptica más comunes:

- **Conector SC (Subscriber Connector):** El conector SC es uno de los conectores más utilizados en redes de fibra óptica. Es un conector de enganche que proporciona una conexión segura y confiable. Tiene un diseño cuadrado y utiliza un conector push-pull para la conexión y desconexión.

- **Conector LC (Lucent Connector):** El conector LC es otro conector de enganche que es ampliamente utilizado en aplicaciones de fibra óptica, especialmente en redes de área local (LAN) y sistemas de telecomunicaciones. Tiene un diseño pequeño y es conocido por su alta densidad de puertos.

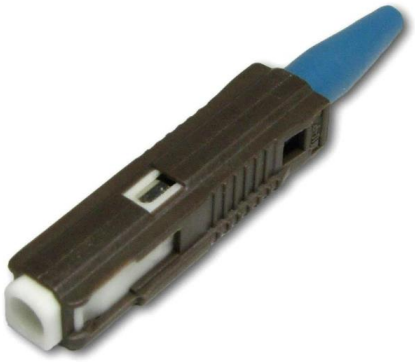
- **Conector ST (Straight Tip):** El conector ST es un conector de rosca que se utiliza comúnmente en redes de fibra óptica. Requiere una alineación precisa y una rotación para conectarse y desconectarse.

- **Conector MTP/MPO (Multi-Fiber Push-On):** Estos conectores están diseñados para aplicaciones de alta densidad y se utilizan para conectar múltiples fibras ópticas a la vez. Son comunes en centros de datos y aplicaciones de alta velocidad, como redes 40G y 100G.



- **Conector DIN (Deutsches Institut für Normung):** Los conectores DIN son populares en Europa y se utilizan en aplicaciones de telecomunicaciones y redes de fibra óptica. Tienen una carcasa redonda y un diseño de enganche.

- **Conector MU (Miniature Unit):** El conector MU es un conector pequeño y se utiliza en aplicaciones donde el espacio es limitado. Es similar en diseño al conector LC.



- **Conector E2000 (LC Duplex):** El conector E2000 es un conector de alto rendimiento con un mecanismo de bloqueo y desbloqueo. Ofrece una conexión segura y es común en aplicaciones de alta velocidad.

- **Conector SMA (SubMiniature version A):** Este conector se utiliza en aplicaciones de fibra óptica de alta precisión, como la instrumentación y la investigación científica.

4.3.4. CABLEADO ESTRUCTURADO.

Se llama cableado estructurado a la infraestructura de telecomunicaciones necesaria para conectar un edificio o un conjunto de edificios. En esta infraestructura se incluyen tanto cables, como conducciones, regletas, armarios, dispositivos, espacios específicos, etc.

El cableado estructurado define algunos subsistemas para organizar la instalación del cableado. Los subsistemas de cableado estructurado son:

- Cableado de campus o de interconexión de edificios.
- Entrada de edificio, punto por donde se conectan los cables exteriores con los interiores.
- Sala de equipamiento, sala donde se distribuyen todas las conexiones del edificio.
- Cableado troncal o backbone, cableado vertical de distribución entre plantas.
- Armarios de distribución, donde confluyen los cables y donde se montan los equipos de interconexión, utilizando rack y paneles de parcheo.
- Cableado horizontal, el cableado de planta.
- Área de trabajo.

Los estándares para cableado estructurado son un conjunto de normas y especificaciones técnicas que se utilizan para diseñar, implementar y mantener sistemas de cableado que soportan una variedad de servicios de comunicación, como voz, datos, vídeo y otros servicios. Estos estándares aseguran la interoperabilidad y el rendimiento óptimo en las redes de telecomunicaciones y de tecnología de la información en edificios y campus. El estándar más comúnmente utilizado para cableado estructurado es el estándar TIA/EIA-568 (o simplemente ANSI/TIA-568), que ha sido desarrollado por la Telecommunications Industry Association (TIA) y la Electronic Industries Alliance (EIA) en los Estados Unidos.

Aquí hay algunas de las especificaciones más importantes dentro del estándar TIA/EIA-568:

- **TIA/EIA-568-A y TIA/EIA-568-B:** Estas son las dos versiones principales del estándar. La versión B reemplazó a la versión A y se considera el estándar actual. Define las especificaciones para el cableado de telecomunicaciones en edificios comerciales, incluyendo categorías de cables de par trenzado, configuraciones de cableado, conectores y sistemas de gestión de cableado.
- **Categorías de cables:** El estándar TIA/EIA-568 especifica diferentes categorías de cables de par trenzado, como Cat 5e, Cat 6, Cat 6a y Cat 7. Cada categoría tiene características específicas de rendimiento y ancho de banda.
- **Topología de cableado:** Define la topología de estrella como la más comúnmente utilizada, en la que todos los cables se conectan a un punto central (generalmente un patch panel). También se mencionan otras topologías, como el bus y el anillo, aunque son menos comunes.
- **Conectores:** Establece los estándares para conectores RJ-45 (conectores Ethernet) y otros conectores utilizados en redes de cableado estructurado.
- **Distancias y requisitos de longitud:** Define las distancias máximas permitidas para el cableado y las limitaciones de longitud para asegurar un rendimiento adecuado.
- **Gestión del cableado:** Incluye pautas para la gestión del cableado, como el uso de canaletas, bandejas de cableado y organizadores para mantener el cableado ordenado y accesible.
- **Certificación y pruebas:** Establece pautas para la certificación y pruebas de los sistemas de cableado para garantizar que cumplan con los requisitos de rendimiento.

Existen otros estándares y normas regionales, como **ISO/IEC 11801** en Europa, que son similares en su enfoque y objetivos.

Conexiones 568A y 568B

Pin	568-A	568-B
1	blanco-verde	blanco-naranja
2	verde	naranja
3	blanco-naranja	blanco-verde
4	azul	azul
5	blanco-azul	blanco-azul
6	naranja	verde
7	blanco-marrón	blanco-marrón
8	marrón	marrón

En las conexiones de red usaremos **cables directos**, que significa que los dos extremos tendrán la misma norma. Se recomienda usar la 568B. En caso de querer hacer un **cable cruzado** usaremos la norma 568A en un extremo y la norma 568B en el otro. Los cables cruzados se usan para conectar dos equipos del mismo tipo, por ejemplo, ordenador con ordenador.

4.4. ELEMENTOS DE INTERCONEXIÓN

Cuando hablamos de elementos de interconexión nos referimos a todos los elementos que permiten conectar equipos en red. Normalmente nos referiremos a los elementos de interconexión de una red de área local, aunque los elementos de interconexión pueden pertenecer a cualquier tipo de red.

Una forma de clasificar a los equipos de interconexión es teniendo en cuenta el nivel en el que trabajan tomando como referencia el modelo OSI. Por tanto vamos a hacer una clasificación tomando este modelo como referencia.

En el nivel físico tenemos:

- **Tarjetas de red:** pueden ser cableadas o inalámbricas. Las tarjetas de red permiten conectar los equipos a la red.
- **Concentradores también conocidos como hubs:** permiten distribuir la señal a diferentes ordenadores sin discriminar entre ello.
- **Repetidores:** pueden ser locales o remotos, y su función es repetir la señal para regenerarla y/o amplificarla.

En el nivel de enlace de datos tenemos:

- **Conmutadores o switch:** se encargan de conectar segmentos de red y ordenadores entre sí pero de forma más eficaz que un concentrador, ya que sólo envía la información al ordenador que la necesita.
- **Puentes o bridges:** conectan subredes, transmitiendo de una a otra el tráfico generado no local.
- **Puntos de acceso:** pueden considerarse como elementos de nivel de enlace de datos, se encargan de conectar elementos inalámbricos entre sí, y de permitir el acceso de dispositivos inalámbricos a redes cableadas.

En el nivel de red:

- **Encaminador o router:** se encarga de conectar redes diferentes. Su principal uso está en la conexión a Internet, ya que permite que redes de área local puedan conectarse a Internet. Se basa en el uso del protocolo IP, por lo que necesita tener asignadas al menos dos dirección IP, una para Internet y otra para la red local. También maneja protocolos de enrutamiento y de control de red. Puede dar servicio inalámbrico y por tanto dar servicio de punto de acceso.

En los niveles superiores:

- **Pasarelas**: suele denominarse pasarelas a los equipos de interconexión que trabajan en los niveles superiores del modelo OSI. Existen diferentes tipos de pasarelas, podemos tener las que se encargan de conectar redes con tecnologías diferentes, las que facilitan el control de acceso a

una red, la que controlan los accesos no autorizados. Según su función pueden también ser servidores, cortafuegos, etc.

Es conveniente recordar que un equipo que trabaja en un nivel suele ser capaz de dar servicio a los niveles inferiores, un ejemplo bastante conocido es el caso del router. Un router trabaja a nivel de red, pero puede actuar como un switch ya que tiene incorporadas varias conexiones RJ-45 y dar servicio a varios ordenadores, y en caso de ser inalámbrico, puede actuar como punto de acceso para que los ordenadores inalámbricos tengan conexión a Internet a través suyo.

4.4.1. TARJETAS DE RED Y DIRECCIONAMIENTO MAC

Ya hemos explicado algo sobre las tarjetas de red, ahora explicaremos algunas de sus características más importantes.

Una tarjeta de red o adaptador de red permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más ordenadores. A las tarjetas de red también se les llama NIC del inglés network interface card o en español tarjeta de interfaz de red.

Su función principal es la de permitir la conexión del ordenador a la red, en la tarjeta se graban los protocolos necesarios para que esto suceda. Todas las tarjetas de red tienen grabada la dirección MAC correspondiente. Como ya hemos visto, la dirección MAC está compuesta de 48 bits y permite identificar a la tarjeta a nivel de enlace de datos. Esta dirección se la conoce como dirección física y es única.

Se observa una tarjeta de red, con sus circuitos y su conector externo.

Las tarjetas de red pueden conectarse al equipo utilizando uno de los buses internos, como el PCI, utilizando el bus externo USB, o estar integradas en la placa.

La tarjeta debe determinar la velocidad de la transmisión, la cantidad de información a transmitir, que protocolos utilizar, y todos los parámetros físicos de la transmisión. Una vez que hace eso, debe transformar la información que le llega a través de la conexión con el ordenador, para poder ser transmitida, esto lo hace convirtiendo la información en una secuencia en serie de bits, convenientemente codificada, para formar una señal eléctrica adecuada.

Existen una gran variedad de tipos de tarjeta de red, algunos son:

- **Tarjetas de red internas:** Estas tarjetas se instalan directamente en una ranura de expansión de la placa base de una computadora. Son comunes en computadoras de escritorio y servidores. Las tarjetas de red internas pueden ser Ethernet (cableadas) o inalámbricas (Wi-Fi).
    - **Tarjetas de red Ethernet:** Las tarjetas de red Ethernet se utilizan para conectarse a redes cableadas. Pueden ser Gigabit Ethernet, 10 Gigabit Ethernet y más, dependiendo de la velocidad de

conexión deseada. Son comunes en entornos empresariales y hogareños.
    - **Tarjetas de red inalámbrica (Wi-Fi):** Estas tarjetas permiten la conexión a redes Wi-Fi y son comunes en computadoras portátiles, dispositivos móviles y otros dispositivos que requieren conectividad inalámbrica.
- **Tarjetas de red externas**: Estas tarjetas de red se conectan a través de puertos USB o Thunderbolt y son utilizadas comúnmente en computadoras portátiles y dispositivos móviles. Proporcionan conectividad adicional o mejorada, como adaptadores Ethernet USB o dongles Wi-Fi.
- **Tarjetas de red Bluetooth:** Estas tarjetas permiten la conectividad Bluetooth, que se utiliza para conectar dispositivos inalámbricos, como auriculares, teclados y ratones, a una computadora.
- **Tarjetas de red de fibra óptica:** Estas tarjetas permiten la conexión a redes de fibra óptica, que se utilizan en entornos de alta velocidad y larga distancia, como en centros de datos y redes de telecomunicaciones.
- **Tarjetas de red virtual (VMNIC):** Estas tarjetas son utilizadas en entornos de virtualización, como máquinas virtuales, para proporcionar conectividad de red a las máquinas virtuales.
- **Tarjetas de red de alto rendimiento:** Algunas tarjetas de red están diseñadas para aplicaciones de alto rendimiento, como juegos, transmisión de medios o edición de video. Estas tarjetas pueden ofrecer características avanzadas como priorización de tráfico y reducción de latencia.

La instalación y configuración de la tarjeta dependerá del sistema operativo, pero en general, necesitaremos que tenga configurada una dirección IP, que se configure una máscara de red y que se defina una puerta de enlace. Esto lo podrás practicar en las siguientes unidades del módulo.

4.4.2. CONMUTADORES

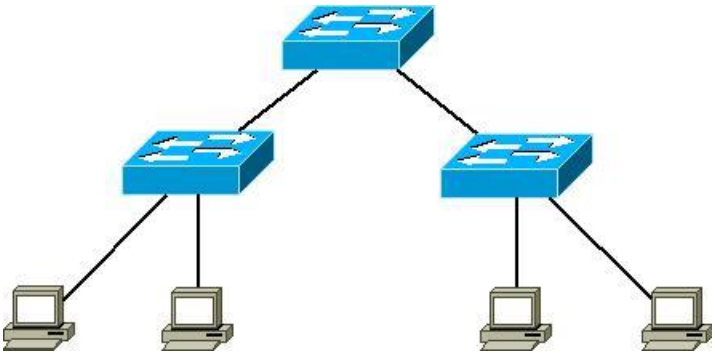
Los switches, en el contexto de las redes de computadoras, son dispositivos esenciales que se utilizan para conectar varios dispositivos en una red local (LAN) y dirigir el tráfico de datos de manera eficiente. Estos dispositivos operan en la capa 2 (capa de enlace de datos) del modelo OSI y son cruciales para el funcionamiento de las redes modernas. Aquí tienes una descripción general de los switches y sus principales características:

- **Conmutador de red:** Un switch se utiliza para conectar dispositivos, como computadoras, impresoras, servidores y otros dispositivos de red, en una red local. Cuando un dispositivo envía datos a otro, el switch determina el camino más eficiente para que los datos lleguen a su destino, reduciendo la congestión y mejorando el rendimiento de la red.

- **Dirección MAC:** Los switches utilizan direcciones MAC (Media Access Control) para identificar los dispositivos en la red. Cada dispositivo tiene una dirección MAC única, lo que permite al switch aprender la ubicación de cada dispositivo en la red.
- **Tabla de direcciones MAC:** El switch mantiene una tabla de direcciones MAC que registra la relación entre las direcciones MAC de los dispositivos y los puertos del switch a los que están conectados. Esto ayuda al switch a determinar la ruta correcta para enviar paquetes de datos.
- **Conexiones de puertos:** Los switches vienen en diferentes tamaños, desde switches de 5 o 8 puertos para uso doméstico hasta switches empresariales con cientos de puertos. Los dispositivos se conectan a los puertos del switch para formar una red.
- **Tráfico de datos eficiente:** Los switches operan en modo de conmutación y, por lo tanto, solo envían datos al puerto de destino específico en lugar de transmitir datos a todos los puertos, lo que reduce la congestión y aumenta la eficiencia de la red.
- **Gestión y configuración:** Los switches gestionables permiten a los administradores de red configurar y supervisar el comportamiento del switch. Esto incluye la capacidad de crear VLAN (redes virtuales), implementar políticas de calidad de servicio (QoS) y realizar un seguimiento del rendimiento de la red.
- **PoE (Power over Ethernet):** Algunos switches ofrecen la capacidad de proporcionar energía a dispositivos conectados, como cámaras IP, teléfonos VoIP y puntos de acceso inalámbrico, a través de los cables Ethernet. Esto simplifica la instalación y alimentación de dispositivos.
- **Resiliencia y redundancia:** En entornos críticos, se utilizan switches con capacidades de resiliencia y redundancia para garantizar la continuidad del servicio en caso de fallas. Esto se logra mediante la configuración de enlaces troncales (trunking) y la configuración de switches en clústeres.
- **Seguridad:** Los switches pueden implementar características de seguridad, como listas de control de acceso (ACL), para controlar el acceso a la red y protegerla contra amenazas.

El inconveniente que se tiene utilizando conmutadores es que sólo pueden conectar redes con la misma topología, aunque pueden trabajar a diferentes velocidades.

Un ejemplo de conexión de segmentos se puede ver en la siguiente imagen:



Existen los conmutadores de nivel 3 o switch de nivel 3, que tienen las ventajas de los conmutadores en cuanto a velocidad y además pueden escoger la mejor ruta entre distintos dispositivos. Una de las aplicaciones más importantes de los conmutadores de nivel 3 es la posibilidad de definir redes de área local virtuales o VLAN. Las VLAN son redes lógicamente independientes dentro de una misma red física.

VLAN

Una VLAN, que significa "Virtual LAN" o "Red de Área Local Virtual", es una técnica de segmentación de redes que permite dividir una red local (LAN) física en múltiples redes lógicas separadas. Esto se logra al asignar grupos de dispositivos a diferentes segmentos lógicos sin importar su ubicación física en la red. Las VLAN ofrecen varios beneficios, como mejorar la seguridad, la administración y la eficiencia en el tráfico de datos. A continuación, se presentan los conceptos clave y ventajas de las VLAN:

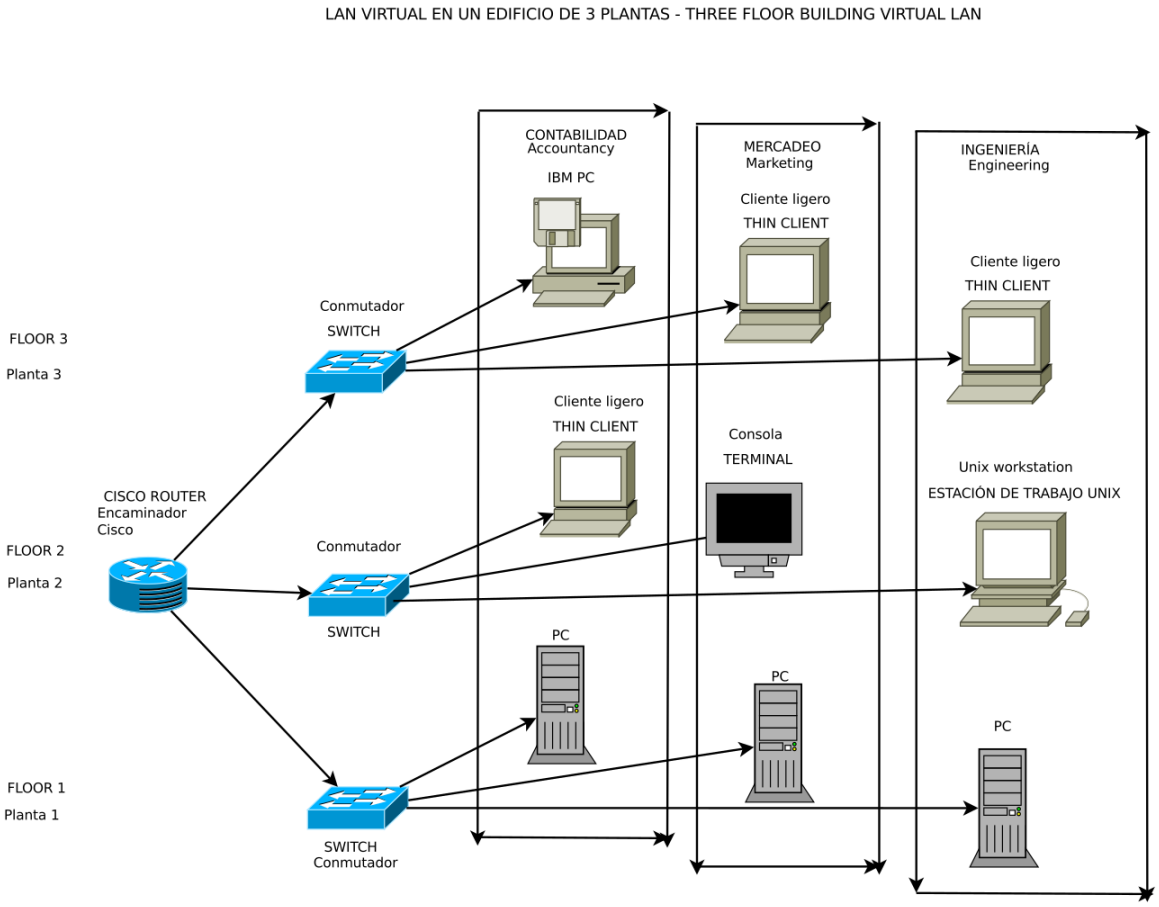
- **ID de VLAN:** Cada VLAN se identifica mediante un número único conocido como ID de VLAN. Los dispositivos en la misma VLAN comparten el mismo ID de VLAN y se comunican entre sí como si estuvieran en la misma red, incluso si están ubicados en diferentes partes de la LAN física.
- **Segmentación:** La segmentación de redes es el proceso de dividir la red en segmentos virtuales. Cada segmento se asocia con una VLAN específica y funciona como una red independiente.
- **Troncal (Trunk):** Para permitir que múltiples VLANs se comuniquen a través de un solo enlace o puerto en un switch, se utiliza un enlace de troncal o trunk. Esto permite que los paquetes de diferentes VLANs se transmitan a través del mismo enlace.

Ventajas de las VLAN:

- **Mejora de la seguridad:** Las VLAN pueden aislar el tráfico entre diferentes grupos de dispositivos, lo que ayuda a evitar el acceso no autorizado a recursos de red. Por ejemplo, los dispositivos en una VLAN de invitados pueden estar separados de los dispositivos en una VLAN de empleados.

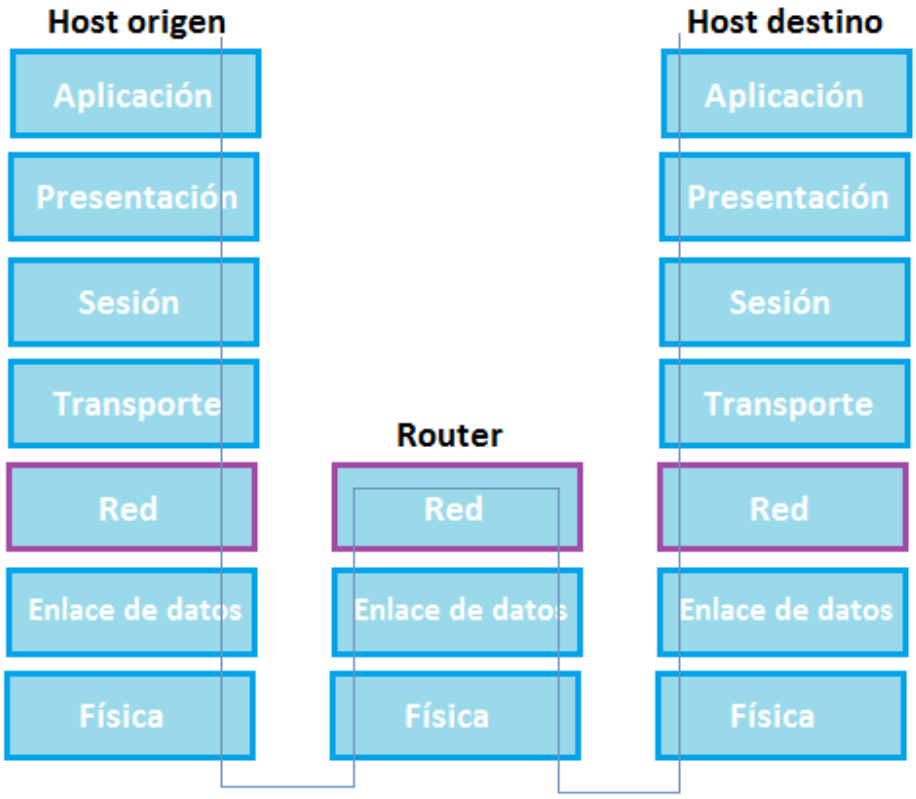
- **Optimización del rendimiento:** Las VLAN permiten controlar y priorizar el tráfico de red, lo que es especialmente útil en entornos donde es crucial garantizar un alto rendimiento para ciertas aplicaciones.
- **Facilita la administración:** Las VLAN hacen que la administración de la red sea más eficiente al agrupar dispositivos relacionados y simplificar la configuración y el mantenimiento de la red.
- **Flexibilidad:** Las VLAN permiten a las organizaciones adaptar su red a las necesidades cambiantes sin necesidad de modificar la infraestructura física. Es más fácil reorganizar dispositivos y recursos según sea necesario.
- **Ahorro de costos:** Al reducir la necesidad de hardware físico adicional, como switches separados, se pueden reducir los costos de implementación y mantenimiento.
- **Mejora de la escalabilidad:** Las VLAN facilitan la expansión de la red sin la necesidad de agregar más cables o switches físicos.
- **Aplicaciones específicas:** Las VLAN son útiles en aplicaciones donde es importante el aislamiento de tráfico, como en la telefonía IP, redes de datos de alta velocidad y entornos de servidores.

Para implementar VLANs, se requiere hardware de red compatible, como switches gestionables que permitan configurar y asignar dispositivos a diferentes VLANs. También es importante diseñar un esquema de VLAN adecuado, asignando dispositivos a las VLANs de acuerdo con los requisitos específicos de la organización. La configuración de las VLAN se realiza a través del software de gestión del switch.



4.4.3. ROUTERS

Un router es un dispositivo de hardware o software que conecta diferentes redes de computadoras y se utiliza para enrutar paquetes de datos entre ellas. Su función principal es determinar la mejor ruta para que los datos viajen desde su origen hasta su destino a través de una red interconectada. Los routers operan en la capa 3 (capa de red) del modelo OSI y utilizan tablas de enrutamiento para tomar decisiones sobre cómo reenviar paquetes.



Funciones principales de un router:

- **Enrutamiento:** El enrutamiento es la función principal de un router. Cuando recibe un paquete de datos, el router determina la ruta más eficiente para enviarlo a su destino basándose en la dirección IP de destino y la información contenida en su tabla de enrutamiento. Esto implica tomar decisiones sobre el siguiente salto en la ruta.
- **Tabla de enrutamiento:** El router mantiene una tabla de enrutamiento que contiene información sobre las redes conectadas y las rutas posibles para llegar a otras redes. Estas tablas se actualizan dinámicamente a medida que cambia la topología de la red.
- **NAT (Network Address Translation):** Los routers a menudo realizan NAT, que permite que múltiples dispositivos en una red privada compartan una única dirección IP pública para acceder a Internet. Esto mejora la seguridad y conserva direcciones IP públicas.
- **Firewall:** Muchos routers incluyen funciones de firewall para proteger la red contra amenazas y ataques. Pueden filtrar y bloquear ciertos tipos de tráfico no autorizado.
- **Gestión de tráfico:** Los routers pueden priorizar y gestionar el tráfico de red, garantizando que las aplicaciones críticas tengan prioridad y que el ancho de banda se utilice eficientemente.

- **Conectividad a Internet:** Los routers son comunes en la conexión a Internet en hogares y empresas. Establecen la conexión con el ISP (proveedor de servicios de Internet) y distribuyen el tráfico entre los dispositivos de la red local.
- **VPN (Red Privada Virtual):** Algunos routers ofrecen soporte para configurar conexiones VPN, lo que permite conexiones seguras a través de Internet y la interconexión de redes remotas.
- **Calidad de servicio (QoS):** Los routers pueden implementar QoS para priorizar ciertos tipos de tráfico, como voz y video, para garantizar una experiencia de usuario óptima.
- **Gestión y configuración:** Los routers gestionables permiten la configuración y supervisión avanzadas a través de una interfaz web o una línea de comandos.

En un enrutador se pueden identificar cuatro componentes:

- **Puertos de entrada:** realiza las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un encaminador; realiza las funciones de la capa de enlace de datos necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada; realiza también una función de búsqueda y reenvío de modo que un paquete reenviado dentro del entramado de conmutación del encaminador emerge en el puerto de salida apropiado.
- **Entrada de conmutación:** conecta los puertos de entrada del enrutador a sus puertos de salida.
- **Puertos de salida:** almacena los paquetes que le han sido reenviados a través del puerto de conmutación y los transmite al enlace de salida. Realiza entonces la función inversa de la capa física y de la capa de enlace que el puerto de entrada.
- **Procesador de encaminamiento:** ejecuta los protocolos de ip encaminamiento, mantiene la información de encaminamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del enrutador.

Los routers son vitales en la infraestructura de red y se utilizan en diversas configuraciones, desde redes domésticas y pequeñas empresas hasta redes empresariales y de proveedores de servicios de Internet. La elección del router adecuado depende de las necesidades específicas de la red y de su capacidad para gestionar el tráfico, garantizar la seguridad y proporcionar servicios adicionales, como VPN y QoS.

5. REDES INALÁMBRICAS

Las redes inalámbricas, en un sentido más amplio, se refieren a cualquier sistema de comunicación que utilice conexiones inalámbricas, ya sea para dispositivos móviles o no

móviles. Esto incluye conexiones Wi-Fi en hogares, empresas o lugares públicos, así como tecnologías de comunicación inalámbrica utilizadas en aplicaciones no móviles, como redes de sensores, automatización del hogar, comunicaciones de máquina a máquina (M2M) y más.

Ejemplos de tecnologías inalámbricas: Wi-Fi (802.11), Bluetooth, Zigbee y tecnologías de comunicación de campo cercano (NFC) son ejemplos de tecnologías inalámbricas utilizadas para conectar dispositivos en una variedad de contextos.

Aplicaciones: Las redes inalámbricas se utilizan en una amplia gama de aplicaciones, incluyendo la conectividad a Internet en hogares y empresas, la comunicación entre dispositivos inteligentes en el Internet de las cosas (IoT), la comunicación en entornos empresariales y más. No se limitan a dispositivos móviles.

Las redes móviles se centran en proporcionar conectividad a dispositivos móviles, como teléfonos celulares y tabletas, y se desarrollan a través de generaciones como 2G, 3G, 4G y 5G. Por otro lado, las redes inalámbricas son un término más amplio que incluye cualquier comunicación inalámbrica, y pueden abarcar desde conexiones Wi-Fi en el hogar hasta tecnologías de comunicación inalámbrica utilizadas en aplicaciones específicas, independientemente de si los dispositivos son móviles o no.

Nosotros nos centraremos en las redes de área local inalámbricas (WLAN), que basan su funcionamiento en el estándar IEEE 802.11 usualmente conocidas como redes Wi-Fi.

Es conveniente saber que Wi-Fi es una marca de la Wi-Fi Alliance, organización comercial de fabricantes que adopta, prueba y certifica que los equipos cumplen los estándares 802.11. Lo que significa que los dispositivos que llevan el sello Wi-Fi cumplen el estándar IEEE 802.11.

El funcionamiento de una red Wi-Fi es similar al funcionamiento de una red de área local cableada, ya que el estándar define el formato de trama, que es ligeramente diferente en las redes Wi-Fi, el uso de la MAC, la forma de acceder al medio, las frecuencias de uso, etc.

Como ya hemos visto anteriormente, las redes inalámbricas pueden estar formadas por ordenadores que se comuniquen entre sí formando una red de tipo ad-hoc, esto permite conectarse entre sí, pero a velocidades bajas y con una seguridad mínima.

Para paliar este inconveniente se suele utilizar el otro modo de conexión que es el modo infraestructura, que como ya sabemos, consiste en utilizar un punto de acceso para que actúe como canalizador de todas las conexiones dentro de la infraestructura de la red Wi-Fi. Este modo de conexión mejora la velocidad y la seguridad, y permite que diferentes dispositivos se conecten entre sí. Es usual que el punto de acceso se conecte a una red de área local a través de un cable, con la idea de poder dar acceso a Internet. Una configuración muy típica es utilizar un router Wi-Fi, que se conecte a una red local o que esté directamente conectado a Internet, para de esta forma dar servicio de Internet a la red inalámbrica.

Algunas ventajas de las redes Wi-Fi son:

- **Movilidad:** se pueden conectar dispositivos estáticos y móviles.
- **Escalabilidad:** son relativamente fáciles de ampliar, tanto en usuarios como en cobertura.
- **Flexibilidad:** se puede conseguir un alto grado de conectividad.
- **Menor tiempo de instalación:** instalando un punto de acceso se puede conseguir rápidamente conectividad.

Las mayores desventajas son:

- **La seguridad:** es difícil conseguir un alto grado de seguridad.
- **Interferencias**: al trabajar en rangos de frecuencias compartidos por otros dispositivos se pueden tener muchas interferencias.

5.1. TIPOS DE REDES 802.11. CARACTERÍSTICAS.

El estándar IEEE 802.11 define el uso del nivel físico y del nivel de enlace de datos del modelo OSI, por parte de las redes de área local inalámbricas, y como hemos visto anteriormente, los dispositivos que usan este estándar se certifican por el sello Wi-Fi.

Dentro del estándar se definen los conceptos de:

- **Estación:** Ordenadores y elementos de interconexión.
- **Medio:** Usualmente radiofrecuencia. Las redes Wi-Fi trabajan en las bandas de 2,4 GHz y 5 GHz, estos rangos están en el rango de las microondas.
- **Punto de acceso**
- **Sistema de distribución**
- **Conjunto de servicio básico** o como lo conocemos nosotros, modo de conexión: ad-hoc e infraestructura.
- **Conjunto de servicio extendido**: la unión de varios modos de conexión o de varias infraestructuras.
- **Área de servicio básico:** la zona donde se comunican las estaciones.
- **Movilidad**
- **Cobertura**

Descripción general de algunos de los estándares más importantes en la familia 802.11:

- **802.11:** Este fue el primer estándar de la familia, lanzado en 1997. Operaba en la banda de frecuencia de 2.4 GHz y proporcionaba velocidades de hasta 2 Mbps.
- **802.11b:** Introducido en 1999, 802.11b operaba en la misma banda de 2.4 GHz y ofrecía una velocidad máxima de 11 Mbps. Fue ampliamente adoptado y popularizó el uso de Wi-Fi en hogares y empresas.

- **802.11a:** También lanzado en 1999, 802.11a operaba en la banda de 5 GHz y ofrecía velocidades de hasta 54 Mbps. Aunque menos común que 802.11b, proporcionaba un mayor rendimiento**.**
- **802.11g:** Lanzado en 2003, 802.11g operaba en la banda de 2.4 GHz y ofrecía velocidades de hasta 54 Mbps. Fue ampliamente adoptado y mejoró la compatibilidad con 802.11b.
- **802.11n:** Introducido en 2009, 802.11n operaba tanto en las bandas de 2.4 GHz como en las de 5 GHz y ofrecía velocidades de hasta 600 Mbps. También introdujo tecnologías como **MIMO** (Multiple Input, Multiple Output) para mejorar el rendimiento y la cobertura.
- **802.11ac:** Lanzado en 2013, 802.11ac opera en la banda de 5 GHz y ofrece velocidades de hasta varios gigabits por segundo. Utiliza técnicas avanzadas como canales más amplios y MIMO para proporcionar un rendimiento de alta velocidad.
- **802.11ax (Wi-Fi 6):** Lanzado en 2019, 802.11ax es la última revisión de la familia 802.11. Opera en ambas bandas de 2.4 GHz y 5 GHz y ofrece mejoras significativas en la eficiencia y el rendimiento, lo que permite velocidades más altas y un manejo más eficiente de múltiples dispositivos.
- **802.11ay:** Este estándar, lanzado en 2020, es una extensión de 802.11ad y opera en la banda de 60 GHz, ofreciendo velocidades muy altas para aplicaciones de corto alcance, como transmisiones de video en alta definición.

5.2.EL CANAL DE UNA RED 802.11.

Las frecuencias utilizadas por las redes Wi-Fi están comprendidas en las bandas de 2,4 Ghz o 5 Ghz y están subdividas en canales. Estos canales pueden variar según las leyes de cada país, por lo que el número de canales que se pueden utilizar puede variar de un país a otro.

Ya hemos visto con anterioridad que existe un número de canales estándar y, según las leyes del uso de las ondas electromagnéticas o el tipo de dispositivo, podemos utilizar más o menos canales.

En las versiones IEEE 802.11 b y g, podemos tener un máximo de 14 canales, y en Europa se definen 13 canales en el estándar, siendo la separación entre canales de 5 MHz, por lo que empezando por la frecuencia del canal 1 tendríamos:

- Canal 1 a 2,412 GHz.
- Canal 2 a 2,417 GHz.
- Canal 3 a 2,422 Ghz.
- Etc.

Así sucesivamente hasta el Canal 13 que emitiría a 2,472 GHz. En el caso de usar el Canal 14, éste emitiría a 2,484 GHz.

Como cada uno de los canales tiene un ancho de banda de 22 MHz, que es superior a la separación entre canales, se pueden producir interferencias si se utilizan canales contiguos. Por tanto, cuando se usen varios puntos de acceso o routers inalámbricos, se recomienda utilizar canales no solapados para evitar interferencias. La idea es que haya 5 canales de diferencia entre dos puntos de acceso que estén próximos. En caso de necesidad, podría haber sólo 4 canales de diferencia.

Pongamos un ejemplo de situación, que seguro te ha pasado:

En tu casa tienes un router Wi-Fi que emite en el canal 1, de repente un día notas como la velocidad baja o las conexiones van y vienen. Tú sabes que tu vecino se ha comprado un router y, como te llevas bien con él, le preguntas en que canal emite, lo comprobáis y véis que también emite en el canal 1, por tanto, estáis teniendo un problema de interferencia, ya que dos routers, que prácticamente están uno al lado del otro, emiten en el mismo canal. La solución en este caso es fácil ya que sois amigos. Os ponéis de acuerdo y configuráis los routers para que uno emita en el canal 1, y el otro en el 6. De esta forma los dos podéis usar las redes Wi-Fi sin interferencias.

En este ejemplo la solución es relativamente fácil, pero no siempre será así, ya que sólo eran dos routers los que interferían, y los dos podían configurarse sabiendo cómo estaba el otro. En la mayoría de los casos os encontraréis con más de dos puntos de acceso interfiriendo, y que no siempre podréis poneros de acuerdo para elegir canales lo suficientemente separados.

En los casos donde haya muchos puntos de acceso cercanos y se necesiten varios de ellos trabajando, se puede utilizar distancias de 4 canales entre puntos de acceso cercanos, y entre los que no se ven, se utilizan los otros canales. Por ejemplo, canales 1, 5 y 10, si hay que poner más puntos de acceso se intenta que no estén cerca del grupo anterior para evitar interferir, y se usan los canales 2, 7 y 12. Así se puede ir haciendo una infraestructura de puntos de acceso para atender las demandas de conexión.

Estos ejemplos los hemos hecho con las versiones b y g, con la versión IEEE 802.11n también se debe hacer así, pero con la salvedad de que además existe la posibilidad de utilizar la banda de frecuencias de 5 GHz.

La banda de 5 GHz está mucho menos saturada, y en la versión n permite trabajar con canales de 40 MHz asociando dos canales de 20 MHz. Esto permite un mayor ancho de banda del canal y por consiguiente una mayor velocidad. Aunque con estas asociaciones tenemos canales más "anchos", podemos usar más canales, ya que la separación entre ellos es mayor y no siempre la misma. Sólo comentaremos que, si se trabaja con versión IEEE 802.11n, se pueden utilizar 8 canales sin problemas de solapamiento.

5.2.1. MULTIPLEXACIÓN ESPACIAL: MIMO

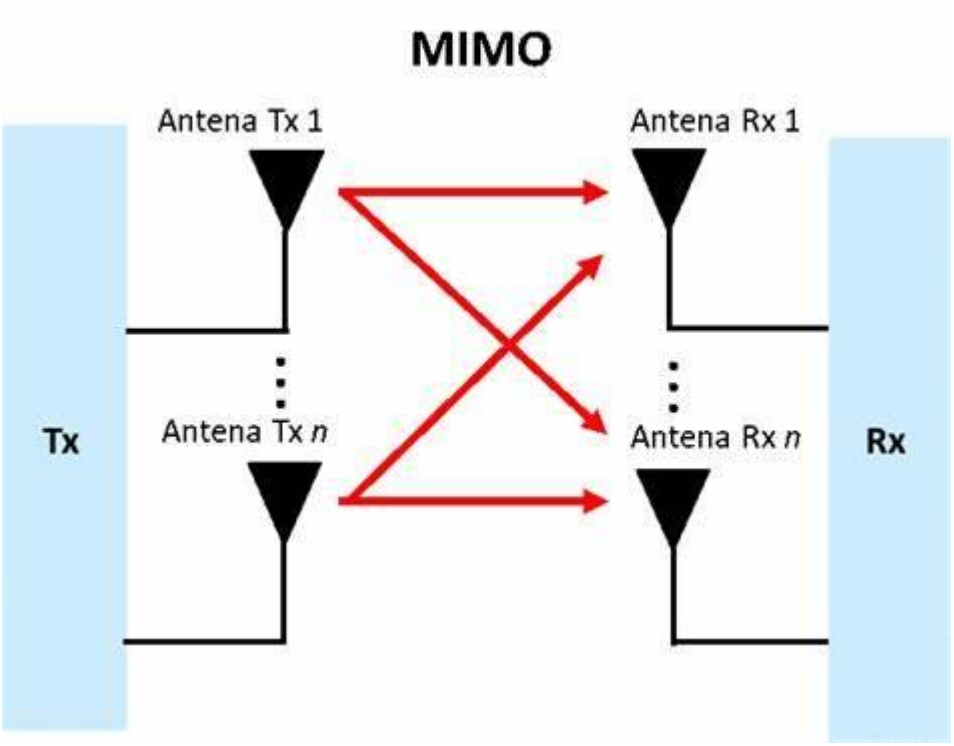
La multiplexación espacial se refiere a una técnica utilizada en comunicaciones inalámbricas y sistemas de transmisión de datos para mejorar la capacidad y la calidad de la transmisión. MIMO, que significa "Multiple Input, Multiple Output" (Múltiples Entradas, Múltiples Salidas), es una de las tecnologías más destacadas en el campo de la multiplexación espacial.

MIMO aprovecha múltiples antenas tanto en el transmisor como en el receptor para transmitir y recibir datos de manera más eficiente. La idea básica detrás de MIMO es que, al utilizar múltiples antenas, se pueden crear múltiples caminos o canales de comunicación entre el transmisor y el receptor. Esto permite una transmisión de datos más rápida y robusta.

Algunos de los beneficios clave de la tecnología MIMO incluyen:

- **Mayor capacidad:** MIMO permite transmitir múltiples flujos de datos simultáneamente a través de diferentes antenas, lo que aumenta significativamente la capacidad del sistema de comunicación.
- **Mayor velocidad:** Al aprovechar los caminos de señal múltiple, MIMO puede aumentar la velocidad de transmisión de datos sin necesidad de un ancho de banda adicional.
- **Mejora de la calidad de la señal:** MIMO ayuda a superar problemas de atenuación y distorsión de la señal, lo que conduce a una comunicación más confiable y de mayor calidad, especialmente en entornos con interferencias y reflexiones.
- **Mayor alcance:** MIMO puede mejorar la cobertura y el alcance de las comunicaciones inalámbricas al hacer un uso más eficiente de la energía y superar obstáculos.
- **Reducción de la interferencia:** MIMO puede ayudar a reducir la interferencia de señales de otras fuentes, lo que mejora la coexistencia de múltiples dispositivos en un entorno inalámbrico.

En resumen, MIMO es una tecnología de multiplexación espacial que utiliza múltiples antenas en el transmisor y el receptor para mejorar la capacidad, velocidad y calidad de las comunicaciones inalámbricas. Es ampliamente utilizado en tecnologías inalámbricas modernas, como Wi-Fi, 4G LTE, 5G y sistemas de comunicación de largo alcance.



5.3. EL SSID DE UNA RED 802.11.

Una vez que ya sabemos cómo funcionan los canales vamos a explicar el término SSID de una red inalámbrica. Cuando se instala una red inalámbrica es conveniente asegurarnos de que los ordenadores se conectan con la red apropiada, esto se hace utilizando un SSID, que son las siglas en ingles de **Identificador de Conjunto de Servicio**. El SSID es una cadena alfanumérica de 32 caracteres de longitud, donde se distinguen las mayúsculas de las minúsculas, y sirve para identificar a la red. Este identificador se emplea para informar a los dispositivos inalámbricos de a qué red pertenecen y con qué otros dispositivos se pueden comunicar.

Tanto si la red inalámbrica es tipo ad-hoc, como si es de tipo infraestructura, es necesario que todos los dispositivos inalámbricos de la misma red se configuren con el mismo SSID. Cuando la red es tipo ad-hoc el SSID se configura en cada ordenador. Si la red es de tipo infraestructura el SSID se configura en el punto de acceso, para que así los ordenadores se puedan conectar a la red.

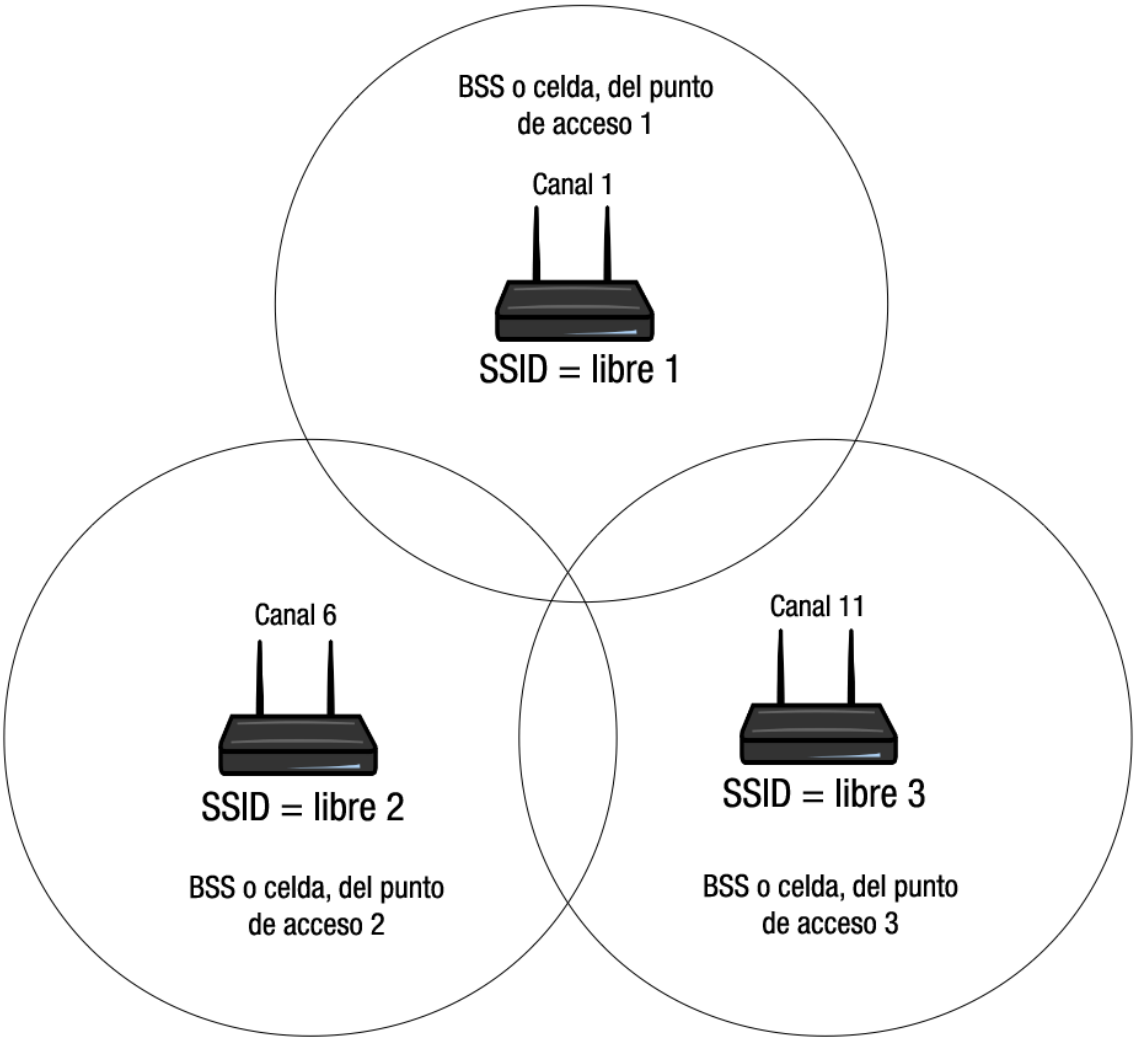
En el caso de las redes ad-hoc se utiliza el **BSSID** (Basic Service Set Identifier) o SSID básico; mientras que en las redes de tipos infraestructura que incorporan un punto de acceso, se utiliza el **ESSID** (Extended Service Set Identifier) o SSID extendido.

Cuando hablamos de redes ad-hoc (ed de malla o red peer-to-peer, es un tipo de red inalámbrica en la que los dispositivos se comunican directamente entre sí sin necesidad de un punto de acceso central o una infraestructura de red. En una red ad-hoc, todos los dispositivos se consideran iguales y tienen la capacidad de actuar como nodos de

retransmisión para transmitir datos a otros dispositivos en la red. Estas redes son autónomas y se organizan de manera dinámica.), el área cubierta por la red se le llama conjunto de servicios básicos independientes cuyas siglas en inglés son **IBSS**. En el caso de una red en modo infraestructura el área cubierta por un punto de acceso se le llama conjunto de servicios básicos, cuyas siglas en inglés son **BSS**. También se le puede llamar celda o área de cobertura, ya que será el área de cobertura del punto de acceso.

Como hemos visto anteriormente, cada punto de acceso que tenga su área de cobertura que se solape con el área de un punto de acceso cercano deberá utilizar canales diferentes, que en el caso del estándar IEEE 802.11b/g, implicará utilizar canales con una diferencia de 5.

A modo de ejemplo se muestra el siguiente gráfico, donde se pueden observar tres puntos de acceso, cada uno con su SSID, el canal que utiliza y el BSS o área de cobertura.



Si por necesidades de cobertura necesitamos conectar múltiples **BSS** entre sí, podemos formar un **ESS** o conjunto de servicios extendidos. Un conjunto de servicios extendidos o ESS, no es más que varios puntos de acceso, conectados entre sí, preferiblemente con cable. Cada punto de acceso utilizará un canal diferente, pero el SSID será el mismo. Como ejemplo podemos imaginarnos el mismo esquema de la figura, pero con los puntos de acceso conectados por cable y con el mismo nombre de SSID.

El **SSID** es un campo obligatorio en los paquetes de administración enviados por un punto de acceso (AP) o un enrutador inalámbrico, y también se muestra en la lista de redes disponibles en los dispositivos de los usuarios. Los usuarios pueden ver una lista de redes WiFi-disponibles y seleccionar la red a la que desean conectarse a través del SSID.

Es importante destacar que el SSID no es una medida de seguridad por sí mismo. A menudo, los administradores de redes configuran un SSID para que sea fácilmente identificable, como "Casa de Juan" o "Oficina Principal". Sin embargo, también se puede ocultar el SSID, lo que significa que la red no se mostrará en la lista de redes disponibles, a menos que el usuario conozca el nombre exacto y lo introduzca manualmente.

La seguridad en una red inalámbrica se basa principalmente en la configuración de autenticación y cifrado, como **WPA2** o **WPA3**, y no en la ocultación del SSID. Por lo tanto, ocultar el SSID no es una medida de seguridad efectiva, ya que todavía es posible para un atacante determinado descubrir el nombre de la red oculta.

5.4. SEGURIDAD EN 802.11.

Existen varias formas de mantener la seguridad en una red Wi-Fi, nosotros citaremos algunas de las más usuales.

Hay que tener en cuenta que las redes Wi-Fi son muy vulnerables a la interceptación de paquetes, a los ataques o simplemente a que usuarios no autorizados se aprovechen de la conexión, por tanto, es conveniente implementar medidas de seguridad que prevengan un uso indebido de la red.

Empecemos comentando una medida que no proporciona ningún tipo de seguridad, pero dificulta a los clientes el conectarse, está medida es ocultar el SSID. Desde los puntos de acceso se difunde el SSID, para que ordenadores que estén dentro de la cobertura, puedan conectarse, esto se hace mediante broadcast o emisión del SSID, si esa función se desactiva los ordenadores deben configurar manualmente el SSID, por tanto, aquellos que no lo conozcan, puede que no detecten la red. Esto es fácilmente salvable ya que existen herramientas que detectan el SSID oculto, pero es un primer paso.

Otras medidas un poco más eficaces, consisten en encriptar o codificar la información que de la red. Para ello se pueden usar distintos tipos de cifrado:

- **WEP (Wired Equivalent Privacy):** WEP fue uno de los primeros protocolos de cifrado utilizados en redes inalámbricas, pero es considerado como inseguro en la actualidad debido a sus debilidades. Es susceptible a ataques de fuerza bruta y no proporciona una protección sólida de datos.
- **WPA (Wi-Fi Protected Access):** WPA fue desarrollado como una mejora de WEP. Proporciona un cifrado más fuerte y una autenticación más segura mediante el uso de TKIP (Temporal Key Integrity Protocol). WPA es un paso adelante en términos de seguridad en comparación con WEP, pero ha sido reemplazado por protocolos más seguros.
- **WPA2 (Wi-Fi Protected Access 2):** WPA2 es un protocolo de seguridad más avanzado que utiliza el cifrado AES (Advanced Encryption Standard) en lugar de TKIP. Es ampliamente considerado como seguro y se recomienda para la mayoría de las redes inalámbricas. Sin embargo, a medida que pasa el tiempo, se han descubierto vulnerabilidades, y se recomienda migrar a WPA3.
- **WPA3 (Wi-Fi Protected Access 3):** WPA3 es la versión más reciente y segura de los protocolos de seguridad Wi-Fi. Proporciona una mayor protección contra ataques de fuerza bruta y mejora la seguridad de las contraseñas. También ofrece cifrado más sólido y protección de datos.
- **AES (Advanced Encryption Standard):** AES es un cifrado fuerte utilizado en WPA2 y WPA3 para proteger los datos transmitidos en una red inalámbrica. AES es altamente resistente a los ataques y se considera uno de los algoritmos de cifrado más seguros disponibles.
- **Open (Redes Abiertas):** Las redes abiertas no utilizan cifrado y no requieren autenticación. Son inseguras y se deben evitar en la mayoría de los casos, a menos que se utilicen en situaciones muy específicas, como redes de invitados con acceso limitado.
- **Cifrado de capa de enlace (Link Layer Encryption):** Además de los protocolos de seguridad anteriores, algunos dispositivos y aplicaciones pueden utilizar cifrado de capa de enlace adicional para proteger sus comunicaciones. Esto puede incluir el uso de VPNs (Redes Privadas Virtuales) u otras tecnologías de cifrado específicas.

La elección del tipo de cifrado y protocolo de seguridad dependerá de tus necesidades y del nivel de seguridad requerido. En general, se recomienda utilizar WPA3 o WPA2 con AES para redes inalámbricas domésticas y empresariales, y evitar el uso de redes abiertas sin cifrado. También es importante mantener el firmware y las contraseñas de los dispositivos actualizados para mantener la seguridad de la red.

El filtrado de direcciones MAC es una medida de seguridad adicional y se recomienda utilizarla como complemento de algunos de los métodos de encriptación. Consiste en configurar el punto de acceso o router de tal forma que tenga un listado de direcciones MAC de los equipos autorizados a conectarse a la red inalámbrica, para que aquellos equipos que no estén en la lista no puedan conectarse.

Hay que tener en cuenta que todo lo relacionado con la seguridad en redes inalámbricas viene establecido en el estándar **IEEE 802.1x**. Originalmente este estándar era para redes cableadas, pero se modificó para poder ser utilizado en redes inalámbricas. Consiste en el control de los puertos de acceso a la red, de forma que sólo se abrirá el puerto y la conexión, si el usuario está autentificado y autorizado en base a la información guardada en una base de datos alojada en un servidor Radius (Un servidor RADIUS (Remote Authentication Dial-In User Service) es un servidor de autenticación, autorización y contabilidad utilizado en redes de comunicaciones para gestionar el acceso de usuarios a la red. Este protocolo de red es ampliamente utilizado en una variedad de entornos, incluyendo redes inalámbricas, redes VPN (Redes Privadas Virtuales) y redes cableadas, para garantizar la seguridad y el control del acceso).

En redes inalámbricas el estándar tiene tres componentes principales:

- El **autenticador**, será el punto de acceso, éste recibirá la información del cliente y la traslada al servidor Radius.
- El **solicitante**, será el software del cliente que dará la información de las claves y permisos para mandarla al autenticador.
- El **servidor de autenticación** será el servidor RADIUS que debe verificar los permisos y claves de los usuarios.

Una solución interesante de seguridad, sobre todo en sitios públicos, es utilizar Hotspot, que consiste en utilizar puntos de acceso asociados a servidores Radius, que sólo dan acceso a usuarios previamente configurados. Ésta es una buena medida de seguridad ya que establece conexiones punto a punto entre el usuario y el punto de acceso, además de permitir el control de acceso, el cobro de las conexiones, etc. Es muy utilizado en hoteles, aeropuertos, etc.

En resumen, mantener la seguridad completa en una red inalámbrica, es difícil y costoso, pero combinando las técnicas descritas, es posible tener un alto grado de seguridad sin necesidad de un gasto excesivo.