TEMA 3: REDES DE ORDENADORES

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.

Está 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**[1]: 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.

Para saber más

Para ampliar tus conocimientos, y como referencia para los demás puntos a desarrollar en la unidad, te sugerimos que consultes el artículo de la Wikipedia relacionado con las redes de computadoras, te ayudará a estudiar los siguientes apartados. Red de computadoras o red de ordenadores.

[1] Permite que una red vaya creciendo, escalando, sin que su rendimiento se vea seriamente afectado

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.

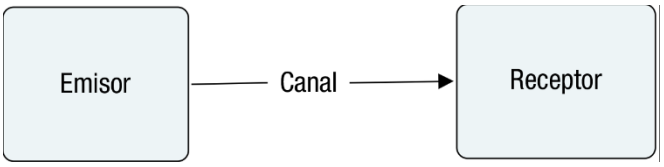
Como podemos deducir, es necesario que emisor y receptor codifiquen la información de forma que ambos se entiendan, por tanto necesitan crear un conjunto de reglas que regulen la comunicación entre ambos, este conjunto de reglas es lo que conocemos por protocolo de comunicación.[2]

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.

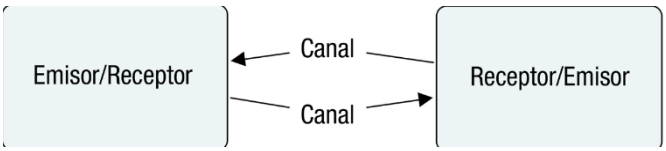
Así podemos clasificar los sistemas de comunicación según diferentes puntos de vista. Si tenemos en cuenta el medio de transmisión, podemos tener **sistemas en línea** o cableados y **sistemas inálambricos**.

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.

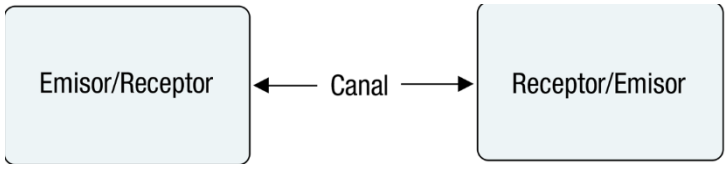


- **Semidúplex** (half duplex): Cuando la comunicación se realiza en los dos sentidos, pero no de forma simultánea. Emisor emite, receptor recibe, receptor pasa a ser emisor, y emisor pasa a ser receptor. **Ejemplo**: Hablar por el walkie-talkie.



[2] Es un conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos.

- **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.



Para saber más

Si quieres conocer más detalles relacionados con los conceptos de simplex, semidúplex y dúplex, te sugerimos que leas el siguiente artículo de la wikipedia. Telecomunicaciones dúplex.

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.

Para saber más

En la presentación que podrás ver al visitar el enlace relacionado, podrás aclarar los conceptos estudiados en este apartado, además de conocer algunos conceptos que desarrollaremos durante este curso. Sistemas de comunicación en redes de telecomunicaciones.

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. Esta 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[3] 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, 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 la misma, seguro que se reducirán costes de implantación y mantenimiento.

[3] Es un sistema informático basado en Internet y centros de datos remotos para gestionar servicios de información y aplicaciones.

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. Un ejemplo típico de red PAN sería una conexión entre dos dispositivos mediante Bluetooth, como por ejemplo dos teléfonos móviles entre sí, o unos auriculares inalámbricos con un ordenador.
- **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 una 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) 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.

Según las **funciones** de sus componentes:

- **Redes de igual a igual** o ente iguales, también conocidas 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 está 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 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.

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.
- **Redes mixtas**: Son redes en las que algunos equipos se conectan de manera cableada, mientras que otros lo hacen de manera inalámbrica.

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

Para saber más

El término Internet lo utilizamos para referirnos a la red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación. Pero sería conveniente que repasaras el artículo de Wikipedia respecto a Internet, para conocer más sobre esta red global. Internet.

1.4. TECNOLOGÍA 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[4] 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[5], o permanecerá si se utiliza una red dedicada [6](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[7] y los circuitos virtuales[8]. Internet es una red de conmutación de paquetes basada en datagramas.

Debes conocer

Es importante que conozcan los conceptos relacionados con la conmutación de paquetes, ya que es la base del funcionamiento de Internet. Para ello debes leer el artículo de wikipedia relacionado con este tema. Conmutación de paquetes.

[4] Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet.
[5] Es el conjunto de elementos constituido por todos los medios de transmisión y conmutación necesarios para enlazar a voluntad dos equipos terminales mediante un circuito físico que se establece específicamente para la comunicación y que desaparece una vez que se ha completado la misma.
[6] Es una denominación que usualmente se reserva para redes de comunicaciones en las cuáles existen un único tipo de tráfico con objetivos de calidad establecidos explícitamente en el contrato entre el operador y el usuario.
[7] Es un fragmento de paquete que es enviado con la suficiente información como para que la red puesta simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes.
[8] Es un sistema de comunicación por el cual los datos de un usuario origen pueden ser transmitidos a otro usuario destino a través de más de un circuito de comunicaciones real durante un cierto periodo de tiempo.

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**, la 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 **UMTS** o telefonía 3G, 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.

Para saber más

Si quieres conocer más sobre las redes WAN recomendamos el siguiente video, donde se hace un somero repaso a todo lo que tiene que ver con la redes WAN. WAN.

2. LA ARQUITECTURA DE RED.

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

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.

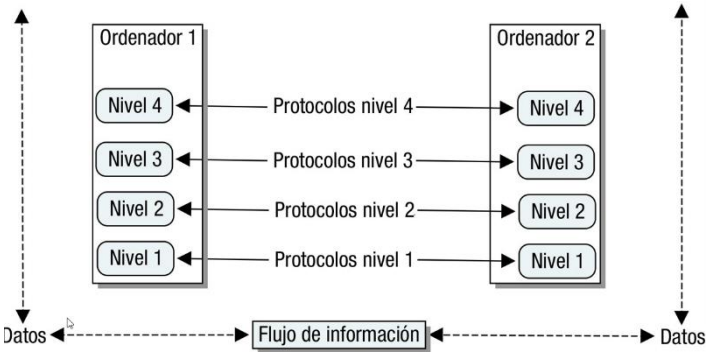
De todo esto podemos concluir que la arquitectura de red tendrá que tener en cuenta al menos tres factores importantes como son:

- La forma como se conectan los nodos de una red, que suele conocerse como **topología**, además de las características físicas de estas conexiones.
- La manera de como 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.

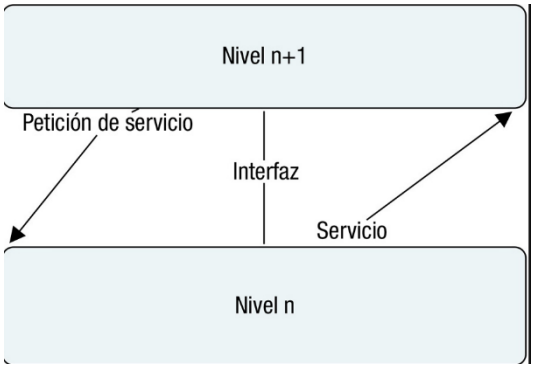


Pero, ¿cómo funciona una arquitectura basada en niveles? Para poder explicar esto utilizaremos diferentes gráficos que creemos que pueden ilustrar mejor la explicación.

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 la comunicaciones entre niveles iguales se hace 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 está 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 está 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 está forma de trabajar cada capa tiene unos servicios asignados, además las capas están jerarquizadas y cada una tiene unas funciones, de está 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 nombre 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.

Como ya hemos visto anteriormente 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 cuales son y en qué nivel se resuelve.
- **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 donde 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.

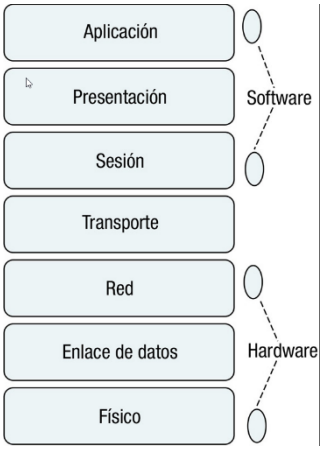
Aunque el modelo OSI no está realmente desarrollado en ningún sistema, si es conveniente conocerlo y aplicarlo, ya que nos sirve para poder entender los procesos de comunicación que se producen en una red, y además puede usarse como referencia para realizar una detección de errores o un plan de mantenimiento.

Los niveles OSI son:

Modelo OSI.

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 este 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 por que los dispositivos y componentes de red, suelen trabajar en los niveles 1 a 3, siendo los programas los que trabajan en los niveles superiores.

Para saber más

Si necesitas ampliar o conocer más sobre el modelo OSI te recomendamos el artículo de la wikipedia que trata sobre el modelo. Modelo OSI.

Es especialmente recomendable que dediques un tiempo al siguiente vídeo donde encontraras una explicación bastante completa de todo el modelo OSI. **Explicación de las capas del modelo OSI y correlación con TCP/IP.**

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.

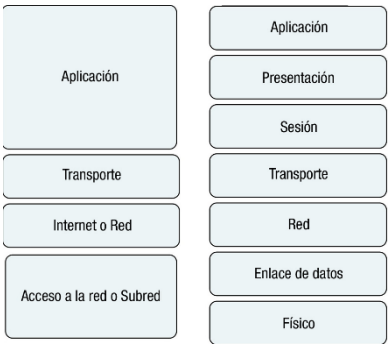
> ***Orientado a conexión***
> Es un modo de comunicación de redes donde se debe establecer una conexión entre el dispositivo emisor y el receptor, antes de transferir datos.

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

Arquitectura TCP/IP.

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 está 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 está 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.



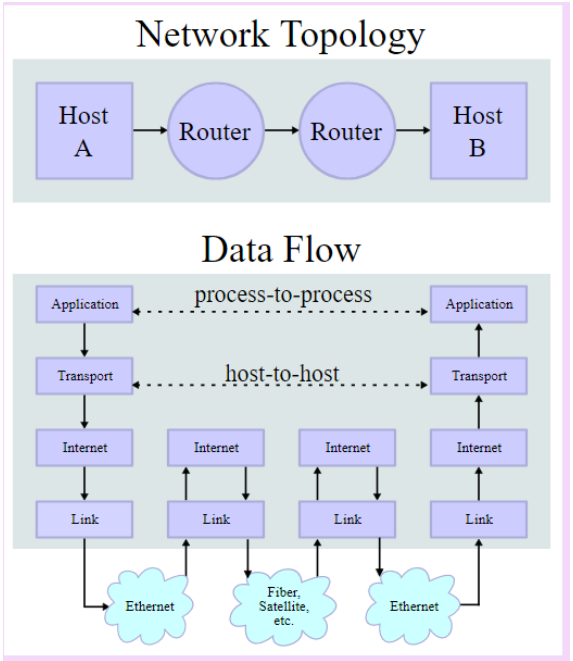
La arquitectura TCP/IP se estructura en capas jerarquizadas y es el utilizado en Internet, por lo que en algunos casos oiréis hablar de Familia de Protocolos de Internet refiriéndose a está arquitectura cuando trabaja en Internet.

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.

Debes conocer

Debes leer el artículo del Modelo TCP/IP de la wikipedia, y prestar especial atención al siguiente gráfico donde se representa la encapsulación de una aplicación de datos a través del modelo, ya que te será necesario para poder entender los siguientes puntos de la unidad. Modelo TCP/IP

Ejemplo de topología de red y flujo de datos en una transmisión de host a host



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

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.

Para saber más

Artículo sobre Ethernet y su evolución al estándar IEEE 802.3. Ethernet.

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:

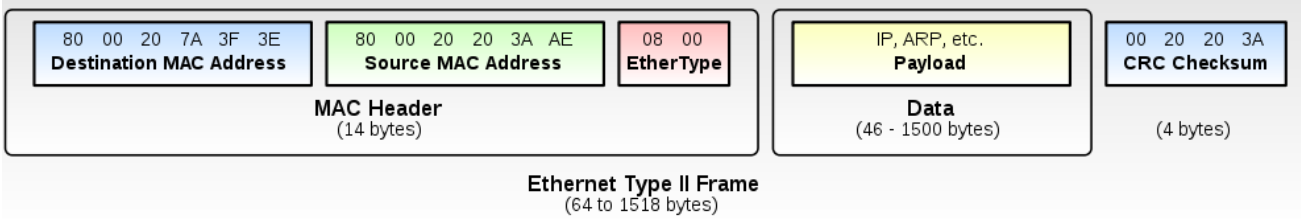
FF:FF:FF:FF:FF:FF

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.

Para saber más

Te será útil cómo conocer la dirección MAC en diferentes sistemas operativos, para ello puede consultar el siguiente enlace. Dirección MAC.

2.6. EL NIVEL DE INTERNET O DE LA 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. Está es una de las principales ventajas de esta arquitectura y por eso es la base de Internet.

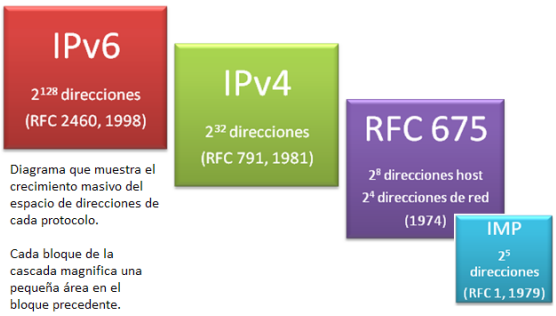


Diagrama que muestra el crecimiento masivo del espacio de direcciones de cada protocolo.

Cada bloque de la cascada magnifica una pequeña área en el bloque precedente.

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 está 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[9] y tracert[10] 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.

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.

Ejemplo de direcciones IP son:

IP versión 4: 192.168.1.11 (Utilizando valores en decimal).

IP versión 6: 2001:0DB8:0000:0000:0000:0000:1428:57AB (Utilizando valores en hexadecimal y puede simplificarse como: 2001:0DB8::1428:57AB)

Para saber más

Como ya hemos mencionado, en la siguiente unidad de trabajo verás más cosas sobre IP, pero sería recomendable que leyeras los artículos relacionados con el protocolo IP para entender mejor algunos conceptos. IP. IPv4. IPv6.

[9] Es una utilidad diagnóstica en redes de computadores que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.

[10] Traceroute es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red). Se obtiene además una estadística o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación. Esta herramienta se llama traceroute en UNIX, Mac y GNU/Linux, mientras que en Windows se llama Tracert. Ej: traceroute www.google.es

2.7. EL NIVEL DE TRANSPORTE.

Cumple la función de establecer las reglas necesaria 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.

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.

Para saber más

Es interesante que leas algo más sobre los protocolos más importantes de este nivel, por lo que te proponemos los siguientes enlaces. TCP. UDP.

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)

Para saber más

Durante el desarrollo de este módulo y de otros de este ciclo, necesitaras conocer cuáles son los puertos relacionados con cada una de las aplicaciones, por tanto, te recomendamos el siguiente enlace. Puertos.

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 trasnferencia 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 carios 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[11]) 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

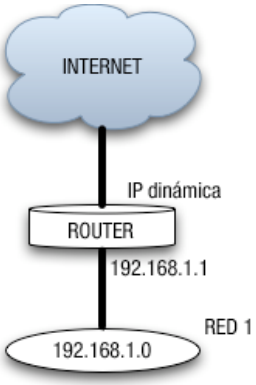
Para saber más

Uno de los protocolos que deberías conocer con mayor profundidad es el protocolo http, por tanto, te recomendamos que leas el siguiente artículo. Protocolo http.

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. Como cada puerto está asociado a una aplicación, podemos decir que no habrá dos conexiones iguales en un mismo instante de tiempo. 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. Este concepto seguro que te será de utilidad más adelante cuando programes servicios web o aplicaciones que utilicen Internet.

[11] En una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor.

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 lógica o esquema lógico, 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 inalámbrico, que son:

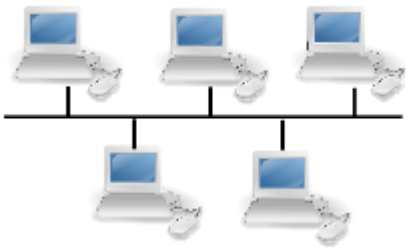
- Modo infraestructura: Suele incluir un punto de acceso.
- Modo ad-hoc: No necesita punto de acceso. Es un tipo de red inalámbrica descentralizada. La red es ad-hoc porque no depende de una infraestructura pre-existente, como routers o puntos de accesos en redes inalámbricas administradas. En lugar de ello, cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red.

Un poco más adelante veremos más detalles sobre estos dos modos de conexión. Sólo comentar que estos modos de conexión se suelen utilizar fundamentalmente en el diseño de redes locales inalámbricas o redes Wi-Fi.[12]

[12] Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica

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. La primeras redes Ethernet utilizaban está 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.

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.

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. Además, es importante que este nodo siempre este activo, ya que si falla toda la red quedaría sin servicio.

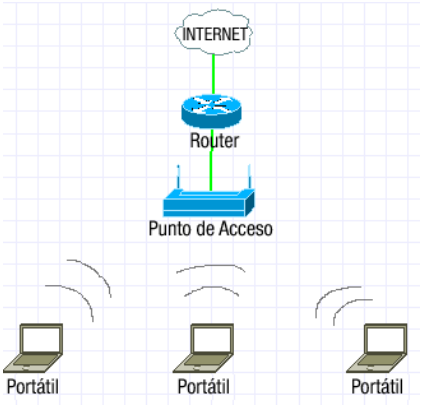
Entre las ventajas de utilizar esta topología tenemos que esta topología es tolerante a fallos ya que si un ordenador se desconecta no perjudica a toda la red, además facilita la incorporación de nuevos ordenadores a la red siempre que el nodo central tenga conexiones, y permite prevenir conflictos de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

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.

3.3. MODO INFRAESTRUCTURA Y MODO AD-HOC.

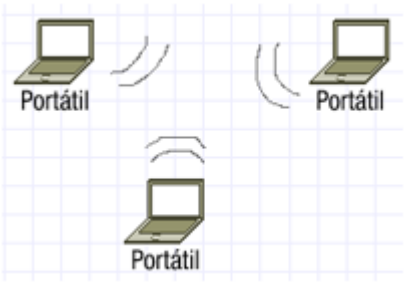


Como hemos visto, existen varias formas de conectar los ordenadores de una red que llamamos topologías, estas topologías, en principio, servirían como base para cualquier tipo de red de área local, ya sea cableada o inalámbrica. Pero en redes inalámbricas que siguen el estándar IEEE 802.11 se introduce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

En las redes inalámbrica 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 está 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 la 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.

Para saber más

Para conocer más detalles de los medios de transmisión y ayudarte a comprender mejor algunos conceptos que vamos a desarrollar más adelante te recomendamos visitar el siguiente enlace: Medio de transmisión

4.2. CABLEADO Y CONECTORES.

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 estándarizada, para que las conexiones de red sean fácilmente reconocibles.

El conector que se utiliza con este cableado es el RJ-45, habiendo macho y hembra.

Debes conocer

Es importante que conozcas las diferentes características de los cables de par trenzado y de los conectores que se utilizan, ya que lo vas a utilizar siempre que trabajes con redes. Por tanto, debes leer los dos artículos que te recomendamos. Par trenzado RJ-45

También se utiliza en las redes de ordenador, el **cable coaxial**. Este cable está compuesto de un hilo conductor, llamado núcleo, y un mallazo externo separados por un dieléctrico o aislante.

Los conectores que se suelen utilizar son el BNC y el tipo N. Dentro del cable coaxial existen diferentes estándares, dependiendo de su uso. 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.

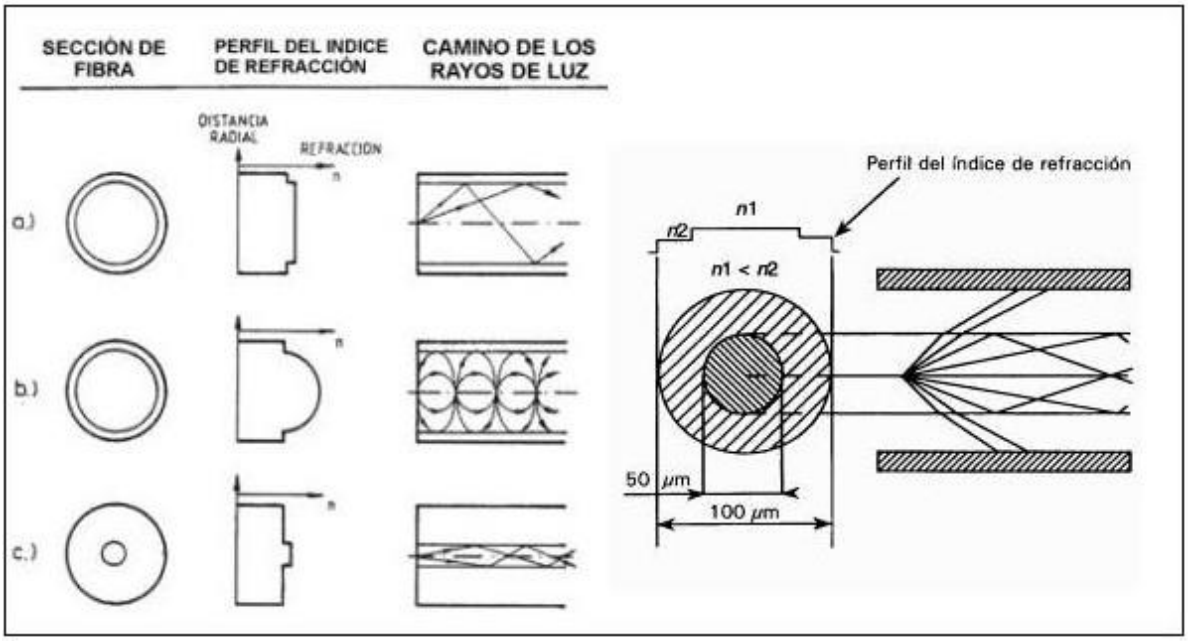
En la distribución de la señal de Internet por cable, el cable coaxial sirve para conectar la central de distribución de Internet que llega a la calle o barrio con la casa del abonado. En este caso se suele utilizar cable de tipo RG6, que permite diferentes configuraciones para incluir acometidas telefónicas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

Si quieres saber algo más sobre el cable coaxial te recomendamos el siguiente enlace. Cable coaxial

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[13], 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**.[14]

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

Para conocer más detalles de la fibra óptica recomendamos el siguiente enlace. Fibra óptica



[13] Un led (del acrónimo inglés LED, light-emitting diode: 'diodo emisor de luz') es un componente optoelectrónico pasivo y, más concretamente, un diodo que emite luz.
[14] Son las principales conexiones troncales de Internet.

4.2.1. CABLEADO ESTRUCTURADO.

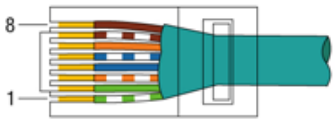
Se llama cableado estructurado a la infraestructura de telecomunicaciones necesaria para conectar un edificio o un conjunto de edificios. En esta infraestructura se incluyen tanto cables, como conducciones, regletas, armarios, dispositivos, espacios específicos, etc.

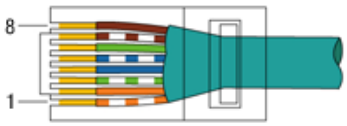
El cableado estructurado define algunos subsistemas para organizar la instalación del cableado. Los subsistemas de cableado estructurado son:

- 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.

Existen estándares de cableado estructurado que especifican cómo organizar la instalación del cableado. Estos estándares especifican el tipo de cable, los conectores, las longitudes máximas de los tramos, la organización de los elementos de interconexión, la ubicación de los dispositivos, etc. Por ejemplo, en el cableado horizontal se recomienda un máximo de 100 metros desde el armario de distribución o rack hasta el área de trabajo.

Otro estándar a tener en cuenta es el ANSI/EIA/TIA 568 A y B, que entre otras cosas define la distribución de colores en la conexión del cable de par trenzado con los conectores RJ-45. Las distribuciones 568 A y B son:





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.

Puedes ampliar la información sobre el cableado estructurado leyendo el siguiente artículo. Cableado estructurado

4.3. 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 direcciones 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. 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.

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 al medio de transmisión.

La mayor parte de las tarjetas tiene los mismos componentes, destacamos:

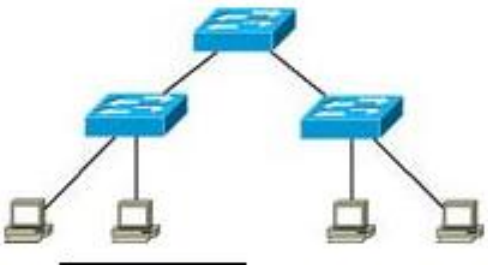
- El procesador principal.
- Un transceptor que es el dispositivo encargado de acceder al medio.
- Un conector wake on LAN que permite el arranque del ordenador desde otro equipo de la red.
- Indicadores de estado para conocer si está conectado y si está enviando o recibiendo datos.
- Dependiendo de si la tarjeta es para redes cableadas o para inalámbricas, tendremos una conexión RJ-45 hembra o una conexión para antena, ya sea interna o externa.

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.

Para saber más

Recomendamos leer el siguiente artículo sobre las tarjetas, ya que te ayudará a conocerlas mejor. Tarjetas de red

4.5. CONMUTADORES.



El conmutador o switch es un elemento de interconexión que trabaja en capa 2 o nivel de enlace de datos, permite conectar dos o más segmentos de red. El conmutador nos permite conectar diferentes ordenadores para que puedan conectarse entre sí, y que éstos tengan acceso a otros segmentos de red.

El conmutador funciona almacenando las direcciones MAC de los ordenadores que están conectados a él y de los dispositivos que se encuentran en cada segmento. Gracias a ello es capaz de conectar un ordenador con otro de forma eficiente, sin necesidad de enviar la información a toda la red.

Esta característica es la que le hace ser el elemento central de conexiones en las redes de área local con topología en estrella.

Usar un conmutador conlleva algunas ventajas como conseguir velocidades altas de conexión y permitir realizar múltiples transmisiones simultáneas, por lo que más de dos ordenadores pueden conectarse al mismo tiempo.

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

Para saber más

Te proponemos dos enlaces interesantes para ampliar la infrmación sobre los conmutadores y las VLAN. Conmutadores VLAN

4.6. ENRUTADORES.

El enrutador o router es el equipo de interconexión de redes que se encarga de conectar dos redes diferentes.

Es un equipo de interconexión de capa 3 o nivel de red. Los enrutadores dirigen el tráfico de red, buscando el mejor camino para llegar al destino. Trabajan con paquetes que contienen la información de las direcciones IP de origen y destino, así como los propios datos del mensaje.

Dada la popularidad del nombre en inglés, usaremos indistintamente router, enrutador o encaminador, para que te sea más fácil familiarizarte con el término.

Hay que destacar que cada puerto o interfaz del router se conectará a una red diferente, por tanto, todos los router deben tener, al menos, dos direcciones IP ya que pertenecerán, al menos, a dos redes diferentes.

Hay que recordar que un router además de las funciones de conectar redes diferentes y de las funciones de enrutamiento, es capaz de realizar filtrados, trasladar direcciones, realizar enlaces y actuar como un conmutador. Para realizar sus funciones un enrutador necesita guardar información de las redes a las que puede acceder, esto lo hace a través de la tabla de enrutamiento, que no es más que una tabla donde se guarda cómo se llega de una red a otra, utilizando qué interfaz.

Los algoritmos de enrutamiento que se utilizan permiten trabajar con rutas estáticas y con rutas dinámicas. Se habla de rutas estáticas cuando en el enrutador se guarda la información de forma permanente y sin cambios de las rutas que pueden seguir los paquetes. Las rutas estáticas son útiles cuando existe una sola forma de conectarse a Internet ya que el paquete siempre seguirá el mismo camino. Las rutas dinámicas serán útiles cuando tengamos varias posibilidades para conectarnos a otra red, en este caso es conveniente que el enrutador pueda recabar información de la red para así, elegir el mejor camino posible.

Los enrutadores necesitan configurarse para que funcionen adecuadamente, en la configuración se suele definir las direcciones IP de cada una de las interfaces, se incluye información de las máscaras de subred, se especifica si se va a utilizar alguna puerta de enlace, que servidores DNS se van a utilizar, si se va a dar servicio de asignación de direcciones IP por medio de DHCP, etc. En algunos casos se puede configurar que puertos estarán abiertos, y en el caso de los enrutadores inalámbricos las características de configuración de las redes inalámbricas, que veremos un poco más adelante.

La mayor parte de las veces utilizaremos router para conectarnos a Internet, ya sea por ADSL o por cable. En estos casos los enrutadores suelen venir configurados por los proveedores de servicios de Internet, y nosotros poco tendremos que configurar, estos enrutadores se llaman router ADSL o router de cable

En algunas ocasiones escucharás hablar de **router neutro**, esto es una terminología que se utiliza para diferenciar al router que une dos redes locales del que permite conectar a Internet.

Usualmente, cuando utilices un enrutador como parte de la red de tu casa o de tu trabajo, éste será el que te permita conectarte a Internet, por tanto, en la configuración del ordenador, habrá que poner la dirección del enrutador como puerta de enlace, ya que el ordenador mandará a esta puerta de enlace todos los paquetes que no sean propios de la red y por tanto será la "puerta" para salir a Internet. En estos casos los enrutadores utilizan el mecanismo NAT o de traducción de dirección de red que permite intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Estos conceptos y la configuración de los parámetros necesarios en el sistema operativo los verás en sucesivas unidades de trabajo.

Para ampliar conocimientos puedes leer el siguiente artículo sobre los routers. Enrutadores

4.7. IDS.

En las redes de ordenadores hemos visto que podemos tener diferentes dispositivos para conseguir que funcionen. Además de los equipos de interconexión, podemos tener servidores que realicen diferentes funciones, tal y como hemos comentado anteriormente. Pues bien, todos estos equipos necesitan mantener unas medidas de seguridad, para evitar que usuarios no autorizados puedan hacer uso de la red o conseguir información no permitida.

En mayor o menor medida todos los equipos implementan medidas de seguridad más o menos complejas, pero existe la posibilidad de implementar un sistema de detección de intrusos que cumpla con estas premisas de seguridad.

Precisamente esto es lo que hace **IDS,** ya que IDS son las siglas en inglés de Intrusion Detection System o Sistema de Detección de Intrusos que podemos definirlo como una aplicación usada para la detección de accesos no autorizados en un ordenador o en una red.

Usualmente existen dos tipos de IDS:

- N-IDS: que se encargan de detectar accesos no autorizados de red.
- H-IDS: que se encargan de detectar acceso no autorizados ordenador o host.

Los N-IDS, necesitan un hardware exclusivo ya que necesitan tener la posibilidad de analizar todo el tráfico de red. Una solución es integrar el N-IDS en el cortafuegos, de esta forma el IDS se encarga de detectar los posibles accesos no autorizados y el cortafuegos de impedir su acceso.

Los H-IDS pueden integrarse en el propio sistema del ordenador, y también pueden combinarse con los cortafuegos instalados en cada ordenador.

Es importante establecer las diferencias entre IDS y cortafuegos ya que no son lo mismo. El IDS detecta intrusiones, pero no las evita, y el cortafuegos limita el tráfico para prevenir intrusiones, pero no las detecta, de ahí que la combinación de ambos sea una buena opción para una red.

Este concepto de detección/prevención es el que inspira una tendencia más actual que es la de los llamados IPS. Un IPS es un Sistema de Prevención de Intrusiones, en este caso no sólo se detecta la intrusión si no que se previene que pueda acceder. Existen soluciones software y/o hardware de tipo IDS y de tipo IPS.

Si quieres conocer algo más sobre estos sistemas te sugerimos el siguiente enlace. IDS

5. REDES INALÁMBRICAS 802.11.

Cuando hablamos de redes inalámbricas nos referimos a una red donde los nodos se conectan sin necesidad de una conexión física entre ellos. Está claro que su uso es cada vez mayor, tanto para conectarnos a Internet, utilizando tecnologías como 3G o 4G, como para trabajar en entornos locales.

Es necesario que distingas los distintos tipos de redes inalámbricas según su cobertura, para ello debes leer el artículo de wikipedia que explica las redes inalámbricas. Red inalámbrica

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 actué 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 este 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.

Aunque en otras unidades de trabajo vas a conocer cómo se configuran los sistemas operativos para poder utilizar las redes inalámbricas, te recomendamos el siguiente artículo para ir viendo cómo se puede hacer. Redes inalámbricas en Windows 10

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 infraestrucutra.
- **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.**

Además el estándar define diferentes versiones, nosotros nos centraremos en las más utilizadas:

- **Wi-Fi b** basado en **IEEE 802.11b** (1999): Opera en la banda de 2,4 GHz con una velocidad máxima de 11 Mbps, con velocidades reales de entre 6 y 7 Mbps. Tiene 14 canales separados 5 MHz entre ellos, excepto el 14, que solo se usa en Japón, que tiene una separación de 12 MHz respecto al 13. Los canales tienen una anchura de 22 MHz y pueden usarse tres de ellos sin solapamiento en redes inalámbricas, normalmente los canales 1, 6 y 11 aunque existen otras combinaciones. Esta versión tiene una ventaja con respecto a la 802.11a y es el alcance, ya que puede llegar a dar cobertura a 120 metros en exterior y 60 metros en interior con velocidades adecuadas.

- **Wi-Fi a** basado en **IEEE 802.11a** (1999): Opera en la banda de 5 GHz tiene una velocidad máxima de 54 Mbps, con velocidades reales de aproximadamente 20 Mbps. Tiene 12 canales sin solapamiento, todos ellos pueden usarse para redes inalámbricas en interior y 4 de ellos se pueden usar para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b.

- **Wi-Fi g** basado en **IEEE 802.11g** (2003): Opera en la banda de 2,4 GHz por lo que es compatible con la versión b, pero ofrece las mismas tasas de transferencia que la versión a, por tanto, puede alcanzar una velocidad máxima de 54 Mbps con medias de 20 Mbps. Tiene 14 canales de 20 MHz pudiendo usarse hasta 13 en Europa, teniendo en cuenta que deben ir de 4 en 4 para impedir el solapamiento, para esto hay que cuidar el diseño de la red. Para evitar solapamiento se suelen usar los canales 1, 6 y 11, aunque en Europa es posible usar los canales 1, 5, 9 y 13 sin apenas solapamiento. En cuanto a coberturas, el estándar nos dice que puede alcanzar hasta 75 metros en exterior y 20 metros en interior, pero algunos fabricantes ofrecen dispositivos con mayores coberturas. Hay que resaltar que, aunque la versión b y la g son compatibles se recomienda usar versión g, ya que si un dispositivo versión b se conecta a punto de acceso g, baja la velocidad de toda el área de cobertura, perjudicando a los otros dispositivos.

- **Wi-Fi n**, **Wi-Fi 4**, basado en **IEEE 802.11n** (2009): Puede operar simultáneamente en las bandas de 5 GHz y en la de 2,4 GHz, gracias a esto la versión n es compatible con las otras versiones, incluidas las posteriores Wi-Fi ac y Wi-Fi 6. Además, es útil que trabaje en la banda de 5 GHz con canales de 40 MHz ya que esta banda está menos congestionada y sufre menos interferencias de otros dispositivos. Con una única antena y *spatial stream*[15] puede alcanzar 150 Mbps de velocidad si se usan canales de 40 MHz, permitiendo el estándar un máximo de 600 Mbps cuando se utilizan cuatro antenas y *spatial streams*. En cuanto a cobertura, varía respecto al tipo de dispositivo, antena que utiliza, etc. pero podemos trabajar con coberturas de 250 metros en exterior y unos 80 metros en interior. Al igual que la versión g, si los dispositivos que se conectan son de versiones anteriores, las velocidades y coberturas bajan. Esta versión utiliza tecnología MIMO, que significa múltiples entradas y múltiples salidas, lo que permite usar múltiples antenas transmisoras y receptoras para mejorar la eficiencia del sistema, permitiendo manejar más información que si utilizáramos una sola antena.

- **Wi-Fi ac**, **Wi-Fi 5**, basado en **IEEE 802.11ac** (2013 "oleada 1", 2016 "oleada 2"): Opera en la banda de 5 GHz, aunque la mayoría de dispositivos certificados como Wi-Fi 5 son "dual band" y pueden trabajar también en la banda de 2,4 GHz (en modo Wi-Fi 4). Introduce nuevas tecnologías como MU-MIMO, canales de 80 MHz (obligatorio) y de 160 MHz (opcionalmente), hasta 8 flujos espaciales y todo ello permite alcanzar velocidades combinadas de casi 7 Gbps con múltiples antenas, flujos espaciales y canales de 160 MHz, y de 433 Mbps para un único dispositivo con una antena y canal de 80 MHz (el

[15] Un “spatial stream” o “flujo espacial” representa un camino de comunicación o flujo de información en una transmisión inalámbrica.

uso de canales de 160 MHz en este estándar es posible, pero poco común). Este estándar es muy utilizado en la actualidad.

- **Wi-Fi 6**, basado en **IEEE 802.11ax** (2021): Opera en las bandas de 2,4 y de 5 GHz y existe una designación ampliada Wi-Fi 6E que opera también en la banda de 6 GHz en aquellas zonas del mundo en las que se permite el uso de esta banda. Wi-Fi 6 es el sucesor del Wi-Fi ac, incorpora nuevas mejoras sobre él y mayor ancho de banda individual y combinado. Con un único *spatial stream* puede alcanzar velocidades de 600 Mbps con canales de 80 MHz, y de 1200 Mbps con canales de 160 MHz. Será implantado de manera masiva durante los próximos años.

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 la banda de 2,4 GHz (usada en las versiones IEEE 802.11 b, g, n, ax) 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.

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

Como cada uno de los canales tiene un ancho de banda de 20 o 22 MHz (dependiendo de la técnica de modulación utilizada), 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 competencia por el espacio aéreo, 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 como 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 lo 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.

En el caso de múltiples puntos de acceso transmitiendo en una zona reducida, es recomendable que todos ellos se distribuyan entre los mismos canales, normalmente los canales 1, 6 y 11, ya que, de esta manera, aunque algunos de ellos comparten canal, cuando emiten en el mismo canal se sincronizan entre ellos para ocupar la franja de frecuencia que les corresponde por turnos. En el caso de canales cercanos pero distintos, que se solapan, sí se producen interferencias por solapamiento y los puntos de acceso no acceden al medio de manera ordenada, por lo que el resultado puede ser peor que compartir canal.

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.

Con las versiones de Wi-Fi 5 y Wi-Fi 6, además, se pueden usar en 5 GHz canales de 80 y de 160 MHz, mediante la agrupación de varios canales de 20 MHz contiguos. De nuevo, esto permite mayores anchos de banda, pero al mismo tiempo reduce el número de canales disponibles sin solapamiento.

Lo relacionado con el estándar IEEE 802.11n tiene cierta complejidad, dada las técnicas que utiliza para conseguir mayores velocidades, pero si quieres saber algo más te recomendamos los siguientes enlaces. IEEE 802.11n características. Asociación de canales en IEEE 802.11n

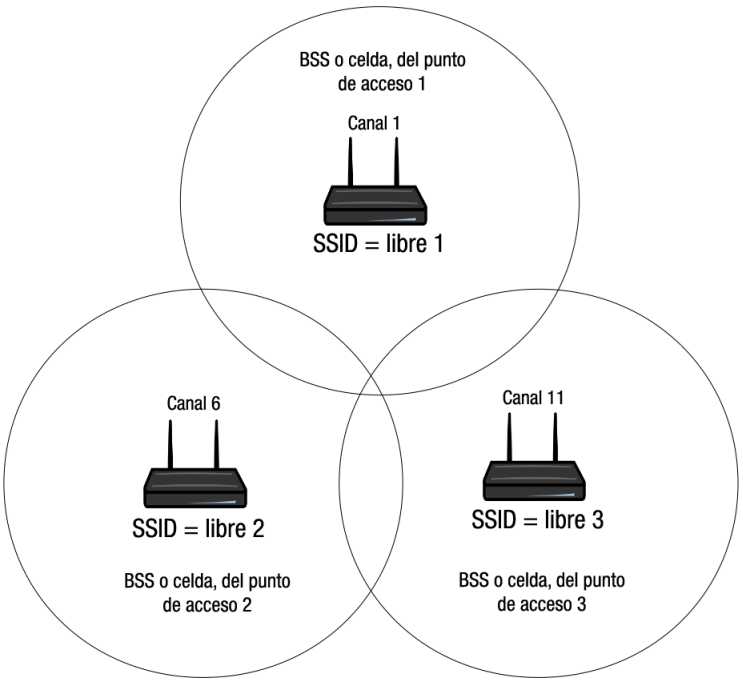
5.3. EL SSID DE UNA RED 802.11.

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 u otros dispositivos 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, 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 sus área de cobertura que se solape con el área de un punto de acceso cercano deberá utilizar canales diferentes, que en el caso de redes en la banda de 2,4 GHz implicará utilizar canales con una diferencia de 5 canales.

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.

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:** Privacidad equivalente a cableado, se encarga de encriptar la información o los datos utilizando claves preconfiguradas para cifrar y descifrar los datos. Puede utilizar claves de 64 bits, 128 bits o 256 bits. Al ser un método bastante débil, ya que es fácilmente descifrable, no es muy recomendable utilizarlo.

- **WPA**: Acceso Wi-Fi protegido, utiliza claves de cifrado de entre 64 y 256 bits. Sin embargo, en WPA se generan claves nuevas de manera dinámica con lo que dificulta su descifrado. WPA tiene una versión mejorada, la **WPA2** que es más robusta y más difícil de descifrar.

Es conveniente destacar que WPA puede utilizar dos tipos de encriptación:

- **WPA-PSK** que utiliza un algoritmo complejo de encriptación, utilizando el protocolo TKIP que es el que cambia la clave dinámicamente. Por lo que WPA-PSK es vulnerable en la primera conexión al punto de acceso que es donde utiliza la clave preestablecida, después va cambiando las claves de forma dinámica.

- Utilizando servidores de encriptación, usualmente **Radius**. Estos servidores utilizan protocolos de autenticación y autorización, de esta manera es el servidor el que se encarga de distribuir claves diferentes entre los usuarios. Este método es el más seguro, pero también el de mayor coste.

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.

En redes inalámbricas el estándar tiene tres componentes principales:

- El **autenticador**, será el punto de acceso, este 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 público, es utilizar Hotspot, que consiste en utilizar puntos de acceso asociados a servidores Radius, que sólo dan acceso a usuarios previamente configurados. Está 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.

En relación al estándar de seguridad IEEE 802.1x recomendamos una lectura al artículo de Intel, ya que explica el proceso de funcionamiento del estándar. Explicación estándar IEEE 802

6. DIRECCIONAMIENTO IP.

Sin duda alguna Internet se ha convertido en la red más grande y con mayor crecimiento de la historia. Cada vez se ofrecen más servicios a través de Internet como comercio electrónico, banca electrónica, formación, … Por lo que se hace necesario que cualquier empresa disponga de una red y que pueda conectarse a Internet.

Los pasos que hay que realizar para la puesta en marcha de una red son:

- **Creación de la red a nivel físico.** Se crea la infraestructura necesaria para poner la red en funcionamiento. Para ello se instala el cableado de la red y luego se ponen en marcha los dispositivos de interconexión (hub, switch, routers…).
- **Creación de la red a nivel lógico.** Se crean las diferentes redes lógicas y se asignan las direcciones IP a los diferentes equipos de la red.
- **Configuración de los routers.** Se configuran los routers para permitir aceptar o denegar la comunicación que se realizan a través de él.

Además, veremos los conceptos más importantes sobre los servicios más utilizados en las redes de ordenadores e Internet.

Sin duda alguna la red más importante es Internet. En el siguiente enlace podrás ver la Historia de Internet.
Historia de Internet

Para poder trabajar en red, cada interfaz de red de un equipo (host o router) necesita una **dirección IP**, esta dirección identifica al equipo mediante una dirección única de 32 bits. Las direcciones IP se suelen representar por cuatro números decimales separados por puntos, que equivalen al valor de cada uno de los cuatro bytes que componen la dirección. Por ejemplo, una dirección IP válida sería 147.156.23.208.

El direccionamiento IP es la parte encargada de asignar de forma correcta a cada equipo una dirección IP, de forma que los equipos puedan comunicarse correctamente entre sí.

6.1. CLASES DE DIRECCIONES.

Las direcciones IP tienen una estructura jerárquica. Una parte de la dirección corresponde a la red (netid), y la otra al host dentro de la red (hostid). Cuando un router recibe un datagrama (mensaje) por una de sus interfaces compara la parte de red de la dirección con las entradas contenidas en sus tablas (que normalmente sólo contienen direcciones de red, no de host) y envía el datagrama por la interfaz correspondiente.

Dependiendo del número de bits que se utiliza para indicar la red (netid) o el equipo (hostid) se definen varios tipos de direcciones de red. Los diferentes tipos de direcciones IP dan una mayor flexibilidad y permiten definir direcciones IP para grandes, medianas y pequeñas redes, conocidas como redes de clase A, B y C, respectivamente:

- Una red de clase A (que corresponde a las redes originalmente diseñadas) se caracteriza por tener a 0 el primer bit de dirección; el campo red ocupa los 7 bits siguientes y el campo host los últimos 24 bits. Puede haber hasta 126 redes de clase A con 16 millones de hosts cada una.
- Una red de clase B tiene el primer bit a 1 y el segundo a 0; el campo red ocupa los 14 bits siguientes, y el campo host los 16 últimos bits. Puede haber 16382 redes clase B con 65534 hosts cada una.
- Una red clase C tiene los primeros tres bits a 110; el campo red ocupa los siguientes 21 bits, y el campo host los 8 últimos. Puede haber hasta dos millones de redes de clase C con 254 hosts cada una.

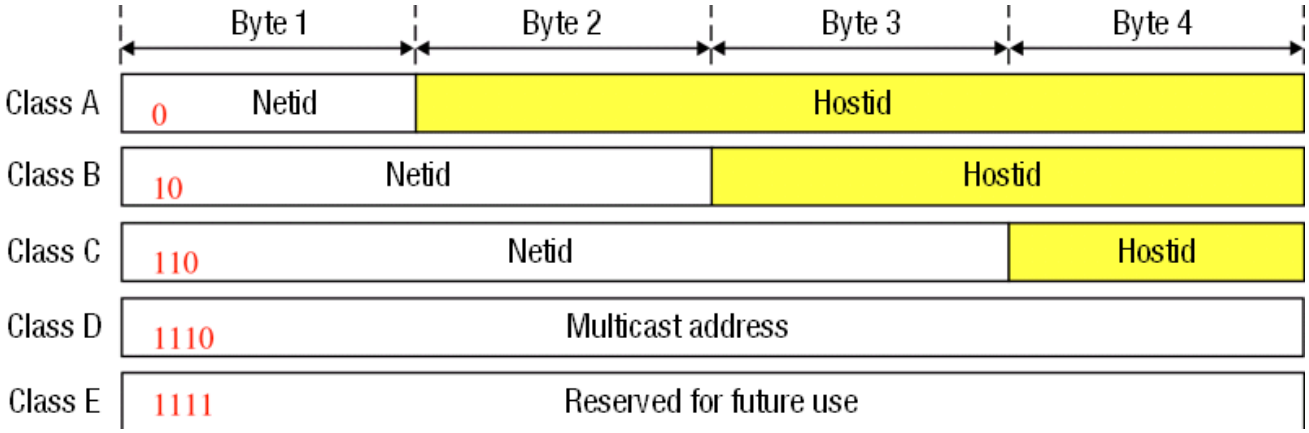
Para indicar qué parte de la dirección corresponde a la red y qué parte al host, se suele utilizar una notación denominada "**máscara de red**", consistente en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden a la parte host. Así, por ejemplo, diremos que una red clase A tiene una máscara 255.0.0.0, lo cual equivale a decir que los ocho primeros bits especifican la red y los 24 restantes el host. Análogamente decimos que una red clase B tiene una máscara 255.255.0.0 y una clase C una máscara 255.255.255.0. Otra notación utilizada en muchos sistemas es expresar de forma conjunta con la dirección IP el número de bits de la máscara de red. Así, por ejemplo, para expresar una dirección de clase A sería 12.15.19.1/8, de clase B 172.16.0.1/16 y de clase C 192.168.1.1/24. Esta notación se llama "notación CIDR" y la estudiaremos en el siguiente apartado.

Además, existen direcciones de clase D (no redes) cuyos primeros cuatro bits valen 1110, que se utilizan para definir grupos multicast (el grupo viene definido por los 28 bits siguientes). Por lo tanto, no se debe utilizar para identificar a ningún host o estación de una red.

Por último, la clase E, que corresponde al valor 11110 en los primeros cinco bits, está reservada para usos futuros por falta de IP's, no obstante, el siguiente paso es la versión 6 del direccionamiento IP, llamado IPv6.

A partir de los valores de los primeros bits de cada una de las clases mencionadas anteriormente, se puede deducir el rango de direcciones que corresponde a cada una de ellas. Así pues, en la práctica es inmediato saber a qué clase pertenece una dirección determinada sin más que leer el primer byte de su dirección. La siguiente tabla resume toda la información esencial sobre los tipos de direcciones de Internet.

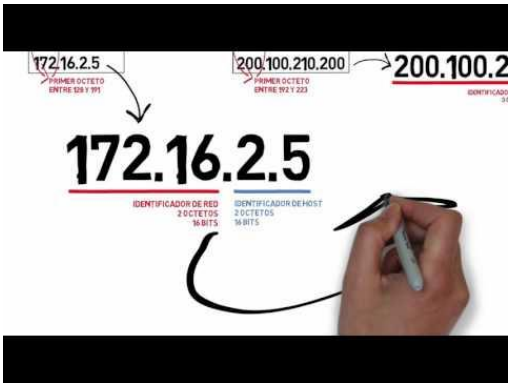
A modo de resumen, a continuación, puedes ver un esquema de las diferentes clases de direcciones y en la tabla puedes ver las características principales de las clases de direcciones.



Características principales de las clases de direcciones.

Clase	Bits Reservados	Bits red/host	Número de redes	Número de ordenadores	Rango	Máscara de Subred por defecto (decimal-binario)
A	0---	7/24	128	16777214	0.0.0.0 - 127.255.255.255	255.0.0.0 -11111111.00000000.00000000.00000000
B	10--	14/16	16384	65534	128.0.0.0 - 191.255.255.255	255.255.0.0 -11111111.11111111.00000000.00000000
C	110-	21/8	2097152	254	192.0.0.0 - 223.255.255.255	255.255.255.0 -11111111.11111111.11111111.00000000
D	1110				224.0.0.0 - 239.255.255.255	
E	11110				240.0.0.0 - 255.255.255.255	

Como sabes los dispositivos electromecánicos de los ordenadores trabajan siempre con dos estados (de tensión, de refracción de la luz, de orientación magnética, etc.) que nosotros los traducimos al sistema de numeración binario (0 y 1).



El protocolo de direccionamiento IPv4, utiliza 32 bits para la dirección de cada dispositivo (host, router, etc.) agrupados en 4 partes de 8 bits cada una que va de 0 (00000000) a 255 (11111111), ya que con 8 bits se pueden representar en binario 2^8=256 combinaciones distintas, que van desde el valor numérico decimal 0 al 255.

Debes conocer

TRANSFORMAR UN NÚMERO ENTERO EXPRESADO EN CUALQUIER BASE DE NUMERACIÓN A DECIMAL.

Para pasar un número que esté en cualquier base de numeración b a la base decimal (10 símbolos distintos) debes aplicar el **Teorema Fundamental de la numeración (TFN)**:

$$\sum_{i=0}^{\infty} b^i * n$$

Ejemplo: El número 532 está expresado en base 8 u octal $532_{8)}$ (este sistema de numeración emplea 8 caracteres para representar cualquier número: del 0 al 7).

Queremos saber su equivalencia en el sistema decimal. Para ello aplicamos el Teorema Fundamental de la Numeración:

Comenzamos tratando el número dígito a dígito de derecha a izquierda, y realizando la sumatoria del TFN= $8^0*2 + 8^1*3 + 8^2*5 = 1*2 + 8*3 + 64*5 = 2 + 24 + 320 = 346$

Podemos afirmar que: $532_{8)} = 346_{10)}$

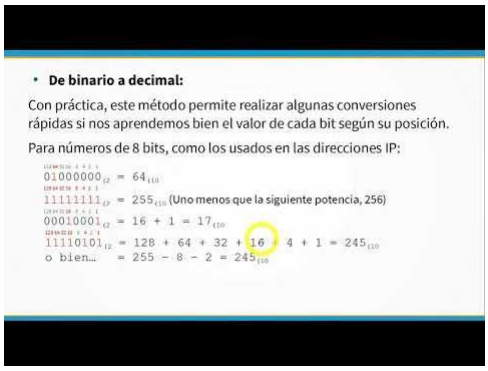
Puedes ver más ejemplos de aplicación del TFN, en el siguiente enlace: Paso de binario a decimal.

TRANSFORMAR UN NÚMERO ENTERO EXPRESADO EN DECIMAL A OTRA BASE DE NUMERACIÓN.

Si queremos hacer el paso inverso, es decir, transformar un número expresado en decimal (base=10) a otra base de numeración (b), el procedimiento consiste en dividir número en decimal y todos sus cocientes hasta que no podamos seguir dividiendo porque el cociente es más pequeño que la base a la que queremos pasar el número. A continuación, se compone el número: El dígito más significativo del nuevo número expresado en la nueva base será el último cociente, como dígito más significativo, y todos los restos de las divisiones que hemos realizado cogidos en orden inverso. Visualiza el siguiente ejemplo, o bien este otro.

EJEMPLOS DE CAMBIOS DE BASE ENTRE DECIMAL Y BINARIO

En el siguiente vídeo puedes observar ejemplos prácticos resueltos de cambios de base entre los sistemas decimal y binario. Estos cambios se realizan a menudo cuando se trabaja con direcciones IP y máscaras de subred.



También puedes descargar la presentación utilizada en el vídeo en formato PDF: Cambios de base entre decimal y binario

6.2. CIDR.

Originalmente, las direcciones de Internet IPv4 se asignaban según redes que seguían el esquema expuesto anteriormente, según redes de clase A, B o C. A este se le llama "*classful networking*" o "redes por clases". Este método era altamente ineficiente, ya que en muchas ocasiones las asignaciones de redes de clase A o B resultaban en que muchas de las direcciones pertenecientes a esas redes quedaban sin ser utilizadas. Por ejemplo, si al asignar una red de tipo B (65.534 hosts posibles) a un proveedor de Internet solamente se utilizaban 10.000 direcciones, esto suponía que se estaban desperdiciando 65.534 - 10.000 = 55.534 direcciones IP. El gran crecimiento de Internet llevó al rápido agotamiento de las direcciones IP, unido al problema del gran crecimiento de las tablas de enrutamiento globales.

Con el objetivo de reducir estos problemas se introdujo en 1993 el método de asignación de direcciones **CIDR**, que significa "enrutamiento entre dominios sin clases". Según este método las direcciones IP se agrupan en "prefijos de red" o "bloques CIDR" de tamaño libre. A las direcciones se les añade un número precedido por una barra '/', lo cual indica el número de bits utilizados para la parte de red de la dirección. Mientras que anteriormente todas las redes tenían un tamaño que era /8 (255.0.0.0) para redes de clase A, /16 (255.255.0.0) para redes de clase B y /24 (255.255.255.0) para redes de clase C, ahora las asignaciones de direcciones se pueden realizar según agrupamientos de otros tamaños.

Por ejemplo: El prefijo 90.74.84.0/22 (máscara equivalente 255.255.252.0) puede ser publicado como tal en las tablas de enrutamiento de Internet, y contiene desde la dirección 90.74.84.0 hasta la 90.74.87.255, lo cual sería equivalente a cuatro redes de tamaño /24 contiguas entre sí. Según el esquema por clases, esta asignación sería solamente una parte de la red 90.0.0.0/8 de clase A. Como se puede comprobar, el sistema CIDR permite que la forma de asignar direcciones IP sea mucho más granular.

Puedes ampliar la información acerca del sistema CIDR: CIDR en Wikipedia

Puedes obtener información acerca de tu dirección de Internet y el bloque CIDR al que la misma pertenece en distintos sitios. Por ejemplo, puedes usar la página de estadísticas del RIPE NCC, que es el Registro Regional de Internet de Europa, Oriente Medio y Parte de Asia. En esta página puedes puedes introducir tu IP o tu prefijo (los detecta automáticamente) y obtener información al respecto: Página de estadísticas de RIPE

6.3. DIRECCIONES DE USO ESPECIAL.

Existen unas reglas y convenios en cuanto a determinadas direcciones IP que es importante conocer:

- La dirección broadcast **255.255.255.255** se utiliza para enviar un mensaje a la propia red, cualquiera que sea (y sea del tipo que sea).
- La dirección **0.0.0.0** identifica al host actual. Sólo se puede usar como dirección de origen, no de destino.
- La dirección con el campo **host todo a ceros** se utiliza para indicar la red misma, y por tanto no se utiliza para ningún host. Por ejemplo, la dirección 193.147.7.0 identifica una red de clase C.
- La dirección con el **campo host todo a unos** se utiliza como la dirección broadcast de la red indicada, y por tanto no se utiliza para ningún host. Por ejemplo, para enviar un mensaje broadcast en la red anterior, utilizaríamos la dirección 193.147.7.255.
- La dirección con el **campo red todo a ceros** identifica a un host en la propia red, cualquiera que sea. Al igual que la dirección 0.0.0.0 sólo se puede utilizar como dirección de origen, no de destino, en casos muy específicos.
- La dirección **127.0.0.1** se utiliza para pruebas loopback; todas las implementaciones de IP devuelven a la dirección de origen los datagramas enviados a esta dirección sin intentar enviarlos a ninguna parte.

Como consecuencia de las reglas 3 y 4 siempre hay dos direcciones no asignables a hosts en una red. Por ejemplo, si tenemos la red 200.200.200.0 (clase C) tendremos que reservar la dirección 200.200.200.0 para denotar la red misma, y la dirección 200.200.200.255 para envíos broadcast a toda la red; dispondremos pues de 254 direcciones para hosts, no de 256.

A modo de resumen, en la tabla puedes ver un ejemplo de las diferentes direcciones específicas.

Dirección especial	Netid	Hostid	Ejemplo (193.147.7.32/24)
Dirección de red	Específica	Todo a 0	193.147.7.0
Dirección directa de broadcast	Específica	Todo a 1	193.147.7.255
Dirección broadcast limitada	Todo a 1	Todo a 1	255.255.255.255
Host específico en esta red	Todo a 0	Específica	0.0.0.32
Dirección loopback	127	Cualquiera	127.0.0.1

En el siguiente enlace puedes encontrar información ampliada sobre todo los rangos de direcciones de uso especial. Dichas direcciones no pueden ser utilizadas como direcciones públicas de Internet, ya que se reservan para otros usos. Direcciones de uso especial en IPv4

6.4. DIRECCIONES PRIVADAS.

El RFC 1918 establece que los bloques de direcciones **10/8**, **172.16/12** y **192.168/16** están reservados para redes privadas (intranets). Estos números no se asignan a ninguna dirección válida en Internet y por tanto pueden utilizarse para construir redes privadas. Por ejemplo, detrás de un firewall o cortafuegos[16], sin riesgo de entrar en conflicto de acceso a redes válidas de Internet, que usan direcciones públicas.

Clase	Nombre	Rango	Prefijo	Direcciones disponibles	Número de redes (en notación pre-CIDR)
A	Bloque de 24 bits	10.0.0.0 - 10.255.255.255	10.0.0.0/8	16.777.216	1 red clase A
B	Bloque de 20 bits	172.16.0.0 - 172.31.255.255	172.16.0.0/12	1.048.576	16 redes clase B
C	Bloque de 16 bits	192.168.0.0 - 192.168.255.255	192.168.0.0/16	65.536	256 redes clase C

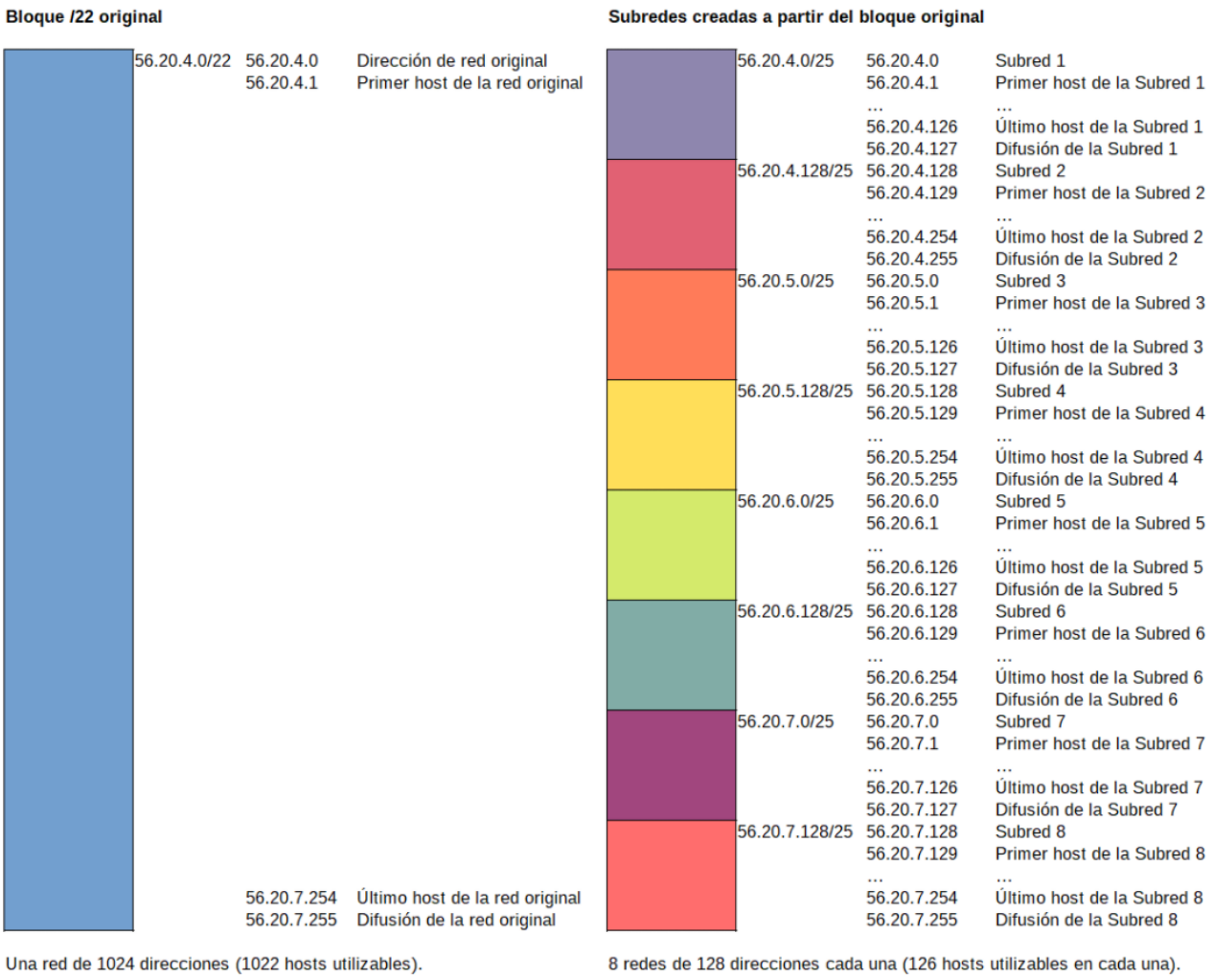
Nótese que, a pesar de que la notación por clases pre-CIDR está obsoleta, sigue siendo común llamar a estos bloques como "direcciones privadas de clase A" (10/8), "de clase B" (172.16/12) y "de clase C" (192.168/16).

Por contraposición, todas las demás direcciones que pueden ser usadas en Internet y que no estén dentro de los rangos privados ni ningún otro rango de direcciones de uso especial se consideran **direcciones públicas**. Por ejemplo: Las direcciones 216.58.211.227 y 8.8.4.4 son direcciones públicas de Internet, la dirección 127.0.0.1 es una dirección reservada para pruebas de *loopback*, y la dirección 172.20.12.48 es una dirección privada perteneciente al bloque 172.16/12.

6.5. SUBREDES.

Cuando se usa el método CIDR los administradores de las redes pueden gestionar el direccionamiento de las mismas, lo cual incluye el poder subdividir las redes en subredes independientes de tamaños inferiores. Por ejemplo, el bloque de direcciones 56.20.4.0/22 puede ser originalmente asignado a un proveedor de Internet. Este bloque comprende las direcciones de la 56.20.4.0 a 56.20.7.255, con un total de 1.024 direcciones IP distintas. El proveedor de Internet puede decidir subdividir este bloque en redes independientes más pequeñas. En la siguiente imagen se puede observar cómo el administrador de la red original la ha subdividido en 8 subredes de 128 direcciones cada una.

[16] Dispositivo hardware o software que se encarga de permitir o bloquear el tráfico a una red o equipo.



Se puede observar que dentro de todas las redes hay dos direcciones IP que no se pueden asignar a hosts. Estas direcciones son la primera y la última de cada red o subred. La primera dirección, que corresponde a aquella en la que la parte del host o "HostID" tiene todos sus bits a 0, es la **dirección de red** de la red o subred, y se usa para identificar a la red. La última dirección, que corresponde a aquella en la que la parte del host tiene todos sus bits a 1, es la dirección **dirección de multidifusión (o difusión, *broadcast* en inglés)** de la red o subred, y se usa para enviar paquetes a todos los hosts que pertenecen a dicha red o subred. Este es el motivo de que en todas las redes el número de hosts disponibles sea igual al número total de direcciones IP de la red menos 2.

En el pasado se recomendaba no utilizar tampoco la primera y última subred creadas al subdividir una red en otras más pequeñas, dado que el uso de estas redes podía crear confusiones y situaciones no deseadas, especialmente en el caso del uso de mensajes de multidifusión en la última subred. En el ejemplo que acabamos de poner esto se traduciría en no utilizar las subredes 1 y 8 con el fin de evitar estas hipotéticas situaciones conflictivas. Esta técnica desperdicia muchas direcciones IP que quedarían sin ser usadas. Aunque en la actualidad es común encontrar bibliografía que hace referencia a esta práctica, está ya está obsoleta y no es necesario aplicarlo. Tanto el hardware como el software de red actuales son capaces de utilizar sin problemas estas dos subredes. Solamente es necesario eliminar dichas redes cuando se trabaja con equipamiento de red muy antiguo.

En el siguiente vídeo se muestra la resolución de este ejemplo: Vídeo.

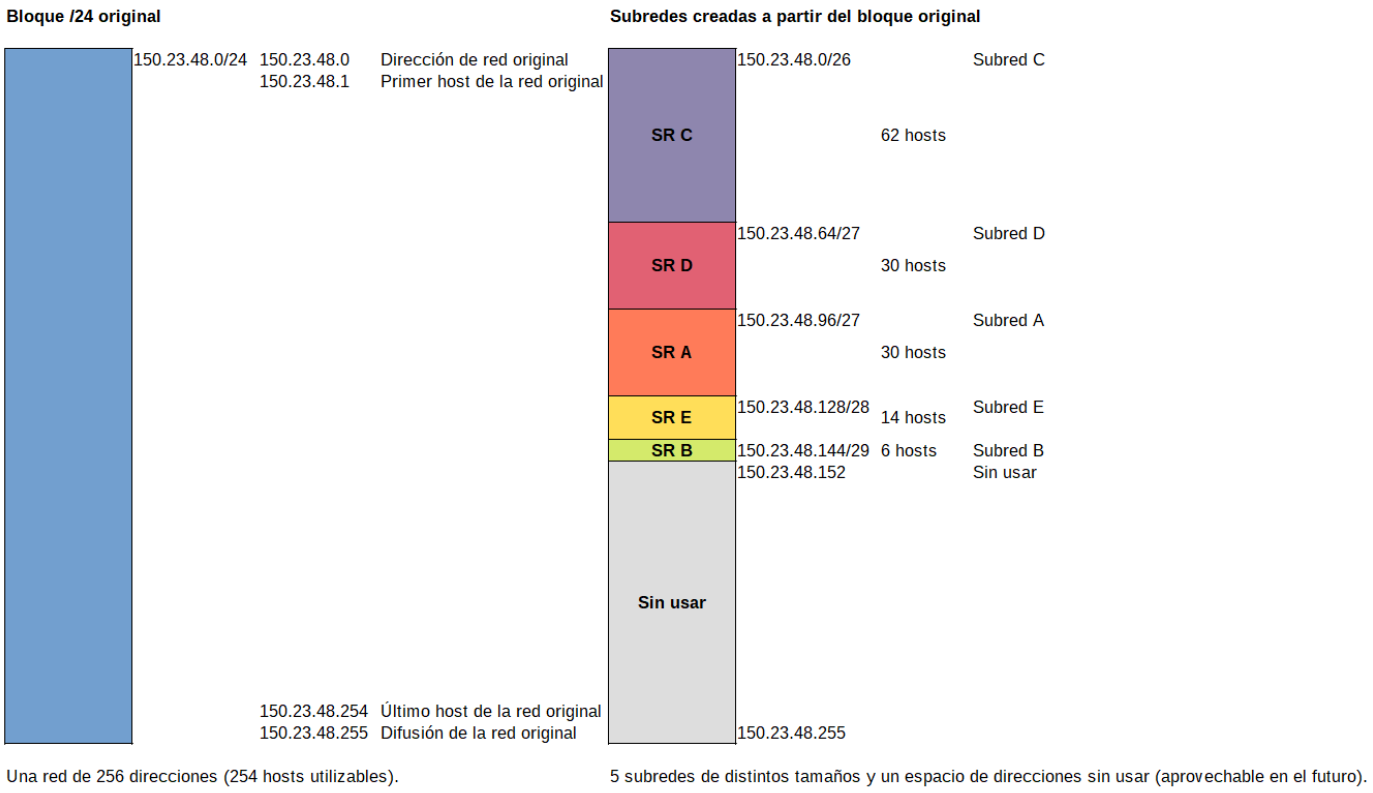
También puedes descargar la versión textual de esta actividad en formato PDF: Ejemplo de *subnetting* sencillo

VLSM: En el ejemplo anterior se ha mostrado un caso simple de subdivisión de un bloque de direcciones en varias subredes del mismo tamaño. El método CIDR permite el uso de VLSM, o "máscaras de subred de tamaño variable". Con VLSM se pueden crear subredes de distinto tamaño a partir de un bloque de direcciones, lo cual permite adaptar el tamaño de las distintas subredes creadas a las necesidades específicas de cada caso.

Ejemplo: Supongamos que disponemos del bloque 150.23.48.0/24 y debemos dividirlo en cinco subredes más pequeñas que deben dar cabida como mínimo al siguiente número de hosts:

- Subred A: 15 hosts.
- Subred B: 6 hosts.
- Subred C: 40 hosts.
- Subred D: 20 hosts.
- Subred E: 13 hosts.

Utilizando VLSM, la división de la red podría quedar así:



En el siguiente vídeo se muestra la resolución de este ejemplo: vídeo

También puedes descargar la versión textual de esta actividad en formato PDF: Ejemplo de *subnetting* usando VLSM

¿Cómo determinar si dos equipos pertenecen a la misma red?

Para que dos equipos puedan comunicarse entre ellos de manera directa deben pertenecer a la misma red o subred. Esta comunicación tiene lugar a nivel 2 (nivel de enlace de datos) del modelo OSI. Dos equipos que pertenezcan a redes o subredes distintas pueden comunicarse entre sí si existe un mecanismo de enrutamiento que permita el tráfico entre dichas redes. Esta comunicación tiene lugar a nivel 3 (nivel de red) del modelo OSI.

Para saber si dos equipos pertenecen a la misma red o subred se utilizan sus direcciones IP y sus máscaras de red. Se aplica la operación "Y lógica" entre las direcciones IP y las máscaras, y esto determina las redes a las que pertenecen las direcciones. Veamos un ejemplo:

Host A	Host B
IP: 198.10.62.7 Máscara: 255.255.248.0 (equivalente a /21)	IP: 198.10.58.39 Máscara: 255.255.248.0 (equivalente a /21)

- Para obtener la dirección de red del Host A:

```
  198.10.62.7 → 11000110.00001010.00111110.00000111
255.255.248.0 → 11111111.11111111.11111000.00000000 Y lógico
                ------------------------------------
                11000110.00001010.00111000.00000000 → 198.10.56.0
```

198.10.56.0 es la dirección de la red a la que pertenece el Host A.

- Para obtener la dirección de red del Host B:

```
 198.10.58.39 → 11000110.00001010.00111010.00100111
255.255.248.0 → 11111111.11111111.11111000.00000000 Y lógico
                ------------------------------------
                11000110.00001010.00111000.00000000 → 198.10.56.0
```

198.10.56.0 es la dirección de la red a la que pertenece el Host B.

En este ejemplo ambos hosts, A y B, pertenecen a la misma red y por tanto se podrían comunicar entre ellos de manera directa sin necesidad de enrutamiento entre redes.

7. SEGURIDAD.

Uno de los aspectos más importantes a la hora de asegurar la red correctamente es la arquitectura de red. Una arquitectura de red es el diseño de la red en el que se emplean unos determinados componentes, cuya finalidad es la de canalizar, permitir o denegar el tráfico con los elementos apropiados.

Existen varias arquitecturas de red, desde la más sencilla, que utiliza simplemente un router, hasta otras más complejas, basadas en varios routers, proxys y redes perimetrales (o zonas neutras[17]).

Antes de entrar en detalle con las arquitecturas de cortafuegos[18], se van a describir tres elementos básicos que intervienen en ella:

- **Router**. Equipo que permite o deniega las comunicaciones entre dos o más redes. Al ser el intermediario entre varias redes debe estar especialmente protegido ya que puede ser objeto de un ataque. Un router puede ser un dispositivo específico o un servidor[19] que actúe como router.
- **Red interna**. Es la red interna de la empresa y, por lo tanto, es donde se encuentran los equipos y servidores internos. Dependiendo del nivel de seguridad que necesite la red interna se puede dividir en varias redes para permitir o denegar el tráfico de una red a otra.

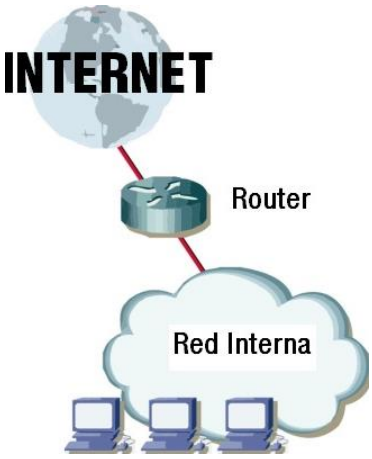
[17] Es una red independiente que permite aislar el tráfico de la red interna y de Internet. Además de asilar redes, la zona neutra se utiliza para alojar los servidores externos de la empresa.
[18] Es la manera en que se configuran los elementos de una red (P.e router, servidores) para que el sistema funcione correctamente y de una forma segura.
[19] Equipo que ofrece unos determinados servicios. Normalmente los servidores están adoptados de un hardware preparados para trabajar de forma ininterrumpida.

- **Zona neutra (o red perimetral).** Red añadida entre dos redes para proporcionar mayor protección a una de ellas. En esta red suelen estar ubicados los servidores de la empresa. Su principal objetivo es que ante una posible intrusión en unos de los servidores, se aísle la intrusión y no se permita el acceso a la red interna de la empresa.

A continuación, se va a ver el esquema de red básico que se puede utilizar cuando desea crear una red interna pero no hay servidores que ofrezcan servicios a Internet. En el caso de tener servidores públicos entonces se recomienda tener una zona neutral.

A partir del esquema de red con una zona neutra se pueden realizar todas las modificaciones que estimes oportunas dependiendo de la seguridad que quieras tener en la red interna, si quieres más zonas neutras, varias conexiones a Internet, etcétera. En este caso lo importante es adaptar el esquema de red a las necesidades de la empresa.

7.1. ESQUEMA DE RED BÁSICO.

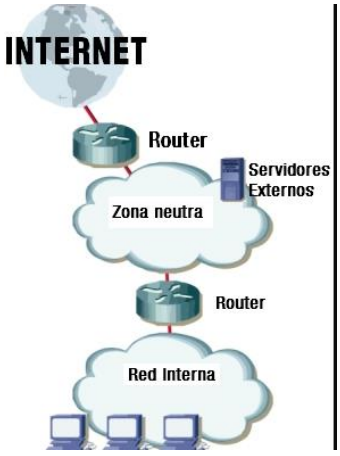


Es la configuración más simple y consiste en el empleo de un router para comunicar la red interna de la empresa con Internet. Como el router es el encargado de comunicar ambas redes es ideal para permitir o denegar el tráfico.

Esta arquitectura de red, aunque es la más sencilla de configurar es la más insegura de todas ya que toda la seguridad reside en un único punto: el router. En caso de que se produzca un fallo de seguridad en el router el atacante tiene acceso a toda la red interna.

Otro aspecto muy importante es que si se desea tener un servidor que ofrezca servicios a Internet hay que ubicarlo en la red interna. Es peligroso poner el servidor en la red interna ya que el router permite el tráfico al servidor y, en el caso de que se produzca un fallo de seguridad el atacante tiene acceso completo a la red interna. Para solucionar este problema se añade una nueva red a la empresa que se denomina **zona neutra o zona demilitarizada.**

7.2. ESQUEMA DE RED CON ZONA NEUTRA.



Este esquema de red es considerado como el esquema base cuando quiere ofrecer servicios a Internet manteniendo un nivel adecuado de seguridad en la red interna. Como puede verse en la siguiente figura, esta arquitectura utiliza dos routers que permiten crear un perímetro de seguridad (red perimetral o zona neutra), en la que se pueden ubicar los servidores accesibles desde el exterior, protegiendo así a la red local de los atacantes externos.

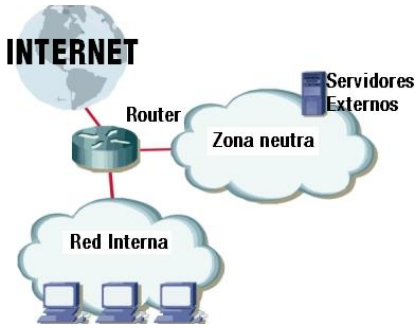
Esquema de red con una zona neutra y una red interna

Al tener dos redes independientes se puede indicar a través de los routers el tráfico que se permite entre Internet y la zona neutra, o el tráfico entre la zona neutra y la red interna. Lo normal es que el router exterior esté configurado para permitir el acceso desde Internet a los servidores de la zona neutra, especificando los puertos utilizados, mientras que el router interior permite únicamente el tráfico saliente de la red interna al

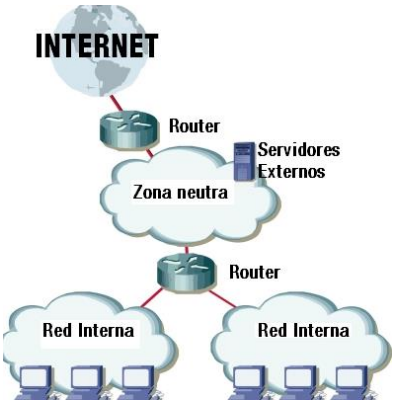
exterior. De esta forma si se produce un fallo de seguridad y se accede a los servidores de la zona neutra, el atacante nunca podrá tener acceso a la red interna de la empresa.

A partir del esquema de red con una red interna y una zona neutra puedes realizar las modificaciones que estimes oportunas para adaptarlo a tus necesidades. A continuación, a modo de ejemplo, se muestran algunas de las configuraciones más utilizadas:

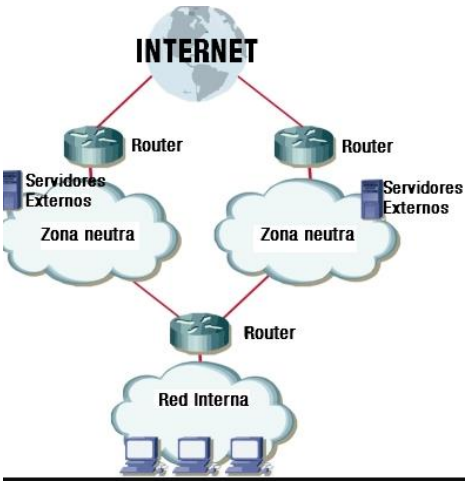
- **Esquema de red con una zona neutra y una red interna utilizando un único router.** Aunque lo recomendable es utilizar dos routers para separar las redes también se puede crear el esquema de red con un único router. En este caso el router tiene tres interfaces de red que le permiten crear la red interna, la zona neutra y conectarse a Internet. Aunque este esquema no es tan fiable como el anterior resulta más aconsejable que el modelo básico que no tiene ninguna zona neutra.



- **Esquema de red con una zona neutra y varias redes internas.** En los esquemas de red anteriores se ha creado una única red interna y por lo tanto todos los equipos y servidores internos están en la misma red dificultando así su seguridad. En el caso de que se tengan equipos con diferentes tipos de seguridad o servidores internos, resulta aconsejable crear varias redes internas para mejorar así la seguridad de la red. En la siguiente figura puede ver un esquema de red que tiene dos redes internas.



- **Esquema de red con varias zonas neutras.** En el caso de que la empresa necesite dar servicios bien diferenciados al exterior puede optar por tener dos zonas neutras, o incluso dos salidas diferentes a Internet. Por ejemplo, en el esquema de red de la figura tiene dos zonas neutras y dos salidas a Internet. En este caso una de las zonas neutras se puede utilizar para ubicar los servidores públicos (por ejemplo, un servidor web o ftp) y la otra zona neutra se puede utilizar para que los clientes se conecten por VPN a la red interna de la empresa. De esta forma, los clientes en la VPN estarán en una zona neutra que se encuentra aislada de la red de servidores públicos y la red interna.



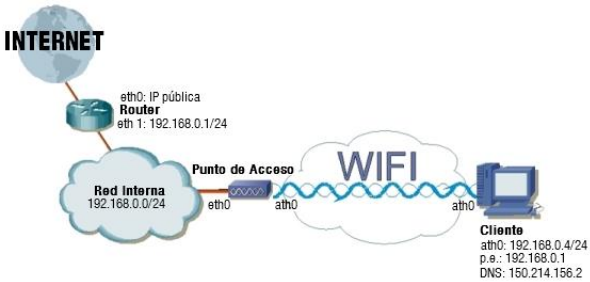
7.3. REDES INALÁMBRICAS.

Las redes de área local inalámbricas (WLAN, Wireless Local Area Networks) permiten que varios dispositivos puedan transmitir información entre ellos a través de ondas de radio sin necesidad de cables. Las ventajas saltan a la vista. La principal es la libertad que proporcionan a los usuarios de red, que pueden llevar su ordenador (especialmente si es portátil) a cualquier sitio sin perder la conexión a Internet.

El acceso sin necesidad de cables es la razón por la que son tan populares las redes inalámbricas, y es a la vez el problema más grande de este tipo de redes en cuanto a la seguridad se refiere. Cualquier equipo que se encuentre cerca del punto de acceso[20] podrá tener acceso a la red inalámbrica.

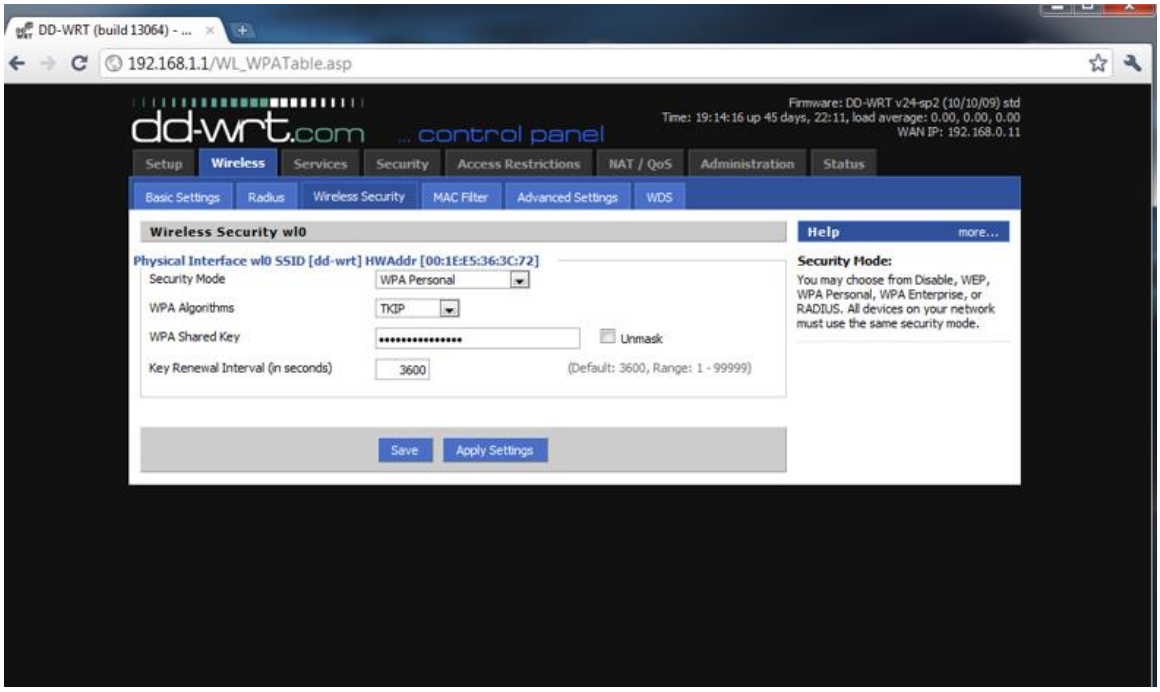
Para poder considerar una red inalámbrica como segura debería cumplir los siguientes requisitos:

- **Aislar la red inalámbrica de la red interna de la empresa creando una zona neutra**. Al utilizar una zona neutra es posible limitar el acceso desde la red inalámbrica a los servicios y/o equipos que estime oportunos. Por ejemplo, una opción muy útil es permitir el acceso de la red inalámbrica únicamente a Internet o algún determinado servicio de la red interna.

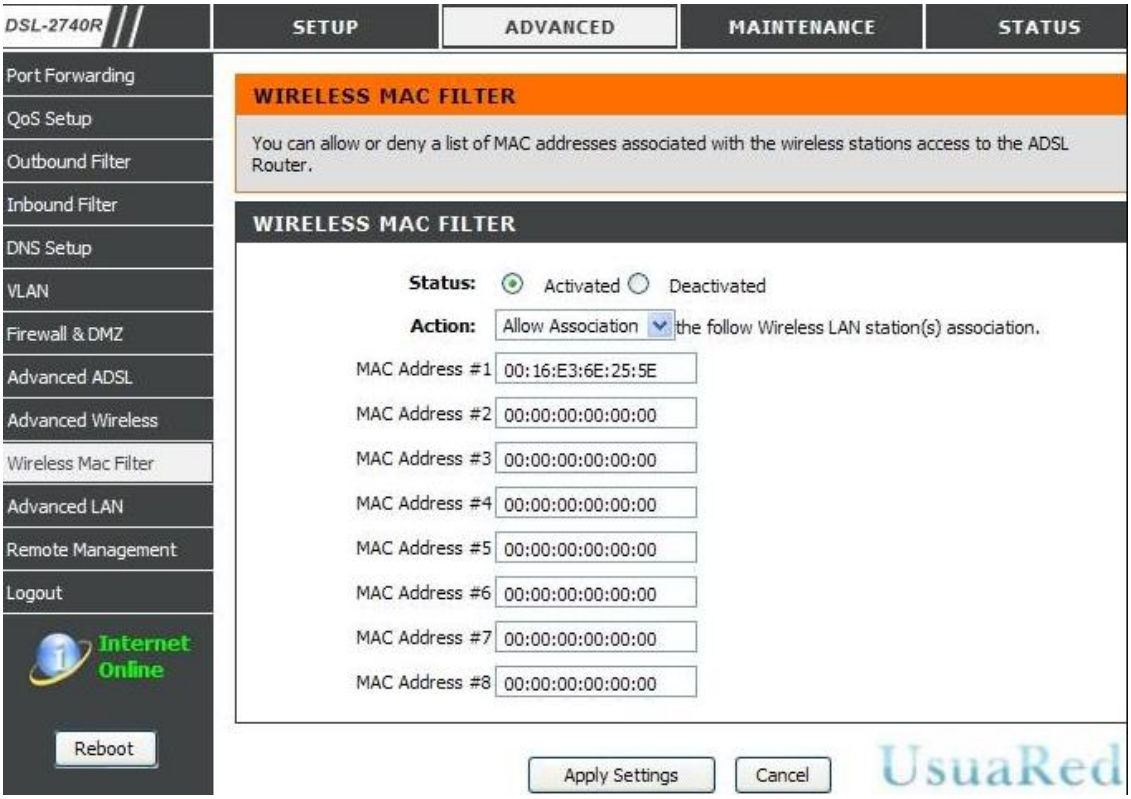


- Las ondas de radio deben confinarse tanto como sea posible.
- Los datos deben viajar cifrados para impedir que sean capturados por otro equipo. Los protocolos más utilizados son:
    - **WEP (Wired Equivalent Privacy)**. WEP fue el primer protocolo de encriptación introducido en el primer estándar 802.11 en el año 1999. Está basado en algoritmo RC4 con una clave secreta de 40 ó 104 bits, combinado con un vector de inicialización (IV:initialization vector) de 24 bits.
    - **WPA (WiFi Protected Access)**. Es un estándar creado para corregir los fallos de seguridad del protocolo WEP. Fue diseñado para utilizar un servidor de autentificación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK: Pre-Shared Key). La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits.
    - **WPA2 (Wi-Fi Protected Access 2).** WPA2 es la evolución de protocolo WPA y surge para corregir sus fallos de seguridad.

[20] Dispositivo que permite crear una red inhalámbrica e interconectarla con una red cableada.



- Debe existir algún mecanismo de autentificación en doble vía que permita al cliente conectarse realmente a su punto de acceso, y que permita verificar que al punto de acceso sólo se conectan los clientes legítimos. Para permitir la autentificación de los clientes es posible utilizar un servidor de autentificación Radius.
- **Filtrado de dirección MAC**. Un mecanismo adicional de seguridad es permitir el acceso a la red inalámbrica únicamente a unos determinados equipos. Para indicar los equipos que pueden acceder a la red inalámbrica se utiliza la dirección física (MAC) del adaptador de red.



8. CONFIGURACIÓN DE ROUTERS.

Como hemos visto anteriormente, un router es un dispositivo de interconexión que permite regular el tráfico que pasa entre varias redes. Un router es muy útil a la hora de defendernos de posibles intrusiones o ataques externos. Pero como desventaja es que un router no se configura por sí sólo. Mientras que un router bien configurado puede ser muy útil, un router mal configurado no nos proporciona ningún tipo de protección o, simplemente, no llega a comunicar dos redes.

Si quieres obtener más información, puedes consultar la correspondiente entrada de la wikipedia.Enrutador

8.1. TABLAS DE ENROUTADO.

Para configurar un router debemos crear lo que se denomina "tabla de enrutado" o "directivas de firewall[21]". En ella se guardan las acciones que hay que realizar sobre los mensajes que recibe el router para redirigirlos a su destino. Existen dos tipos de encaminamiento: **encaminamiento clásico y encaminamiento regulado.**

Con el **encaminamiento clásico**, las reglas utilizadas para encaminar los paquetes se basan, exclusivamente, en la dirección destino que aparece en la cabecera del paquete. Así se distinguen las siguientes reglas:

- Permitir un equipo de nuestra red.
- Permitir cualquier equipo de nuestra red.
- Permitir un equipo de otra red.
- Permitir cualquier equipo de otra red.

La última regla (por defecto) se aplica en el caso de que no se cumpla ninguna de las anteriores y se suele utilizar para poder enviar los mensajes a la puerta de enlace de la red.
Sin embargo, en la actualidad, con la explosión del uso de Internet y la llegada del concepto de calidad de servicio (QoS) y la seguridad, los routers utilizan el llamado **encaminamiento regulado,** con el que, a la hora de escribir la tabla de enrutado, se pueden utilizar los siguientes elementos:

- **Interfaz**: interfaz de red por donde se recibe la información.
- **Origen / Destino:** origen y destino del mensaje. Normalmente el origen y el destino de un mensaje es una dirección IP, pero algunos routers permiten utilizar como dirección origen y destino usuarios o grupos de usuarios.
- **Protocolo:** permitir o denegar el acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto para que un cliente (que inicia la conexión) pueda conectarse. Por ejemplo, un servidor web trabaja en el puerto 80, un servidor de FTP en el puerto 21, etcétera.
- **Seguimiento:** indica si el router debe de realizar un seguimiento de los lugares por los que pasa un mensaje.
- **Tiempo:** espacio temporal en el que es válida la regla.
- **Autentificación de usuarios:** indica si el usuario debe de estar autentificado para utilizar la regla.
- **Acción:** especifica la acción que debe realizar el router. Un router puede realizar las siguientes acciones:
    - **Aceptar:** dejar pasar la información.
    - **Denegar:** no deja pasar la información.
    - **Reenviar:** envía el paquete a una determinada dirección IP.

[21] Reglas del cortafuegos que permiten indicar el tráfico que puede o no puede pasar.

```
[root@redhatserver root]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  10.0.0.0/24          anywhere            tcp dpt:http
ACCEPT     udp  --  10.0.0.0/24          anywhere            udp dpt:domain
ACCEPT     all  --  anywhere             anywhere            state ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
[root@redhatserver root]#
```

Si quieres obtener más información, puedes consultar los siguientes enlaces: Tablas de enrutamiento (wikipedia) Tablas de enrutamiento (MSDN)

8.2. ELEMENTOS DE CONFIGURACIÓN DE UN ROUTER.

Existen diferentes tipos de routers por lo que en un principio podemos caer en la tentación de pensar que el proceso de configuración para cada router es totalmente diferente a los demás. Pero entre los routers más utilizados, ya sean hardware o software, tenemos:

- FireWall 1 de CheckPoint.
- Private Internet Exchange (PIX) de Cisco System.
- IOS Firewall Feature Set de Cisco System.
- Firewall del núcleo de Linux, Iptables.
- Enterprise Firewall de Symantec.
- Internet Security and Acelerador (ISA Server) de Microsoft.

Si se comparan los elementos que utilizan los diferentes routers (ver tabla) puede ver cómo los más utilizados a la hora de realizar una tabla de enrutado son la **interfaz**, la **dirección origen** y **destino**, el **puerto** y la **acción** que debe realizar el router.

Comparativa sobre los elementos de las tablas de enrutado.

Modelo	Interfaz	Origen/destino	Protocolo	Seguimiento	Tiempo	Autentificación de usuarios	Acción
FireWall 1	√	√**	√	√	√		√
PIX	√	√	√*				√
IOS Firewall	√	√	√				√
Firewall Linux	√	√	√				√
Enterprise Firewall	√	√**	√		√	√	√
ISA Server	√	√**	√*		√	√	√

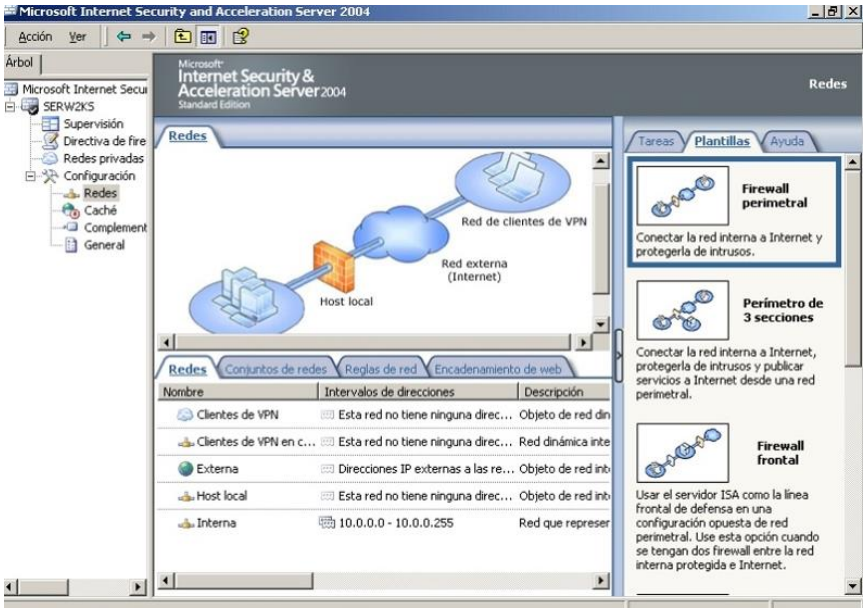
*Distingue entre puerto de origen y destino.

**Permiten especificar como origen o destino direcciones IPs o usuarios.

A la hora de indicar la **dirección de origen** o la **dirección de destino** es importante utilizar la máscara de red para indicar un mayor o menor número de ordenadores. Así por ejemplo, si en la dirección destino utiliza la dirección de clase B 142.165.2.0/16 se hace referencia a todas las direcciones IP del tipo 142.165.x.x. Si utiliza la dirección de clase C 192.165.2.0/24, hace referencia a las direcciones del tipo 192.165.2.x. Por lo tanto, si aumentamos la máscara de red, estamos disminuyendo el número de direcciones IP a las que se hace referencia y si disminuimos la máscara de red, entonces se hace referencia a un mayor número de direcciones IP. En la tabla siguiente, puedes ver algunas de las posibilidades más habituales.

Ejemplos de utilización de la máscara de red en la configuración de routers

Ejemplo	Comentario
192.165.2.23/32	Representa a un único ordenador (por ejemplo, un servidor web)
192.165.2.0./24	Representa a todas las direcciones IP del tipo 192.165.2.X
192.165.0.0/16	Representa a todas las direcciones IP del tipo 192.165.X.X
192.0.0.0/8	Representa a todas las direcciones IP del tipo 192.X.X.X
0.0.0.0/0	Representa a todas las direcciones IP del tipo X.X.X.X



Durante el filtrado de paquetes se aplica la regla de “coincidencia total”. Todos los criterios de la regla tienen que coincidir con el paquete entrante; en caso contrario, no se aplica la regla. Esto no significa que se rechace el paquete o que se elimine, sino que la regla no entra en vigor. Normalmente, las reglas se aplican en orden secuencial, de arriba hacia abajo. Aunque hay varias estrategias para implementar filtros de paquetes, las dos que se describen a continuación son las más utilizadas por los especialistas de seguridad:

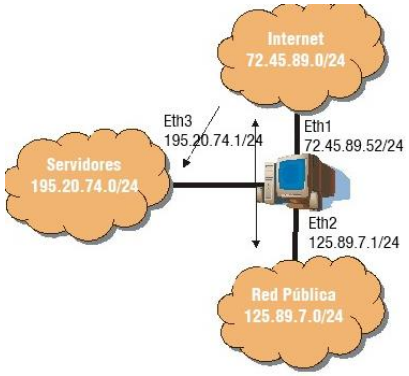
- **Construir reglas desde la más específica a la más general.** Esto se hace así para que una regla general no "omita" a otra más específica, pero conflictiva, que entra dentro del ámbito de la regla general.
- **Las reglas deberían ordenarse de tal forma que las que más se utilizan estén en la parte superior de la lista.** Esto se hace por cuestiones de rendimiento. Normalmente un router detiene el procesamiento de una lista cuando encuentra una coincidencia total.

8.3. EJEMPLO DE CREACIÓN DE UNA TABLA DE ENRUTADO.

La figura muestra un router conectado a tres redes diferentes. Debemos crear el conjunto de reglas para permitir que: la red pública se conecte a Internet y que los servidores sean accesibles desde Internet; el servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.

La tabla de enrutado representa el conjunto de reglas que actúan como medida de seguridad para determinar si se permite que un paquete pase o no.

El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes. Las notas acerca de la implementación se incluyen siguiendo la descripción de cada línea del conjunto de reglas.



Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.

Tabla de enrutamiento

Reglas	Interfaz	Origen	Destino	Puerto	Acción
1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.7/32	25, 110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

- **Regla 1.** Esta regla permite el acceso entrante en el puerto 80, que normalmente se utiliza para el tráfico http. El host que está en 195.20.74.5 es el servidor web. La organización no puede predecir quién va a tener acceso a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.
- **Regla 2**. Esta regla permite el acceso entrante a los puertos 25 y 110, que normalmente se utiliza para correo electrónico (el puerto 25 es el servidor smtpo correo saliente y el puerto 110 es el servidor pop3 o correo entrante). El servidor de correo está en la dirección 195.20.74.7. Al igual que en la regla anterior, como no se puede predecir quién va a tener acceso al servidor de correo no se restringen las direcciones IP de origen.
- **Regla 3**. Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como las reglas 1 y 2 se ejecutan antes, sí se permite el tráfico que va dirigido a los servidores web y correo electrónico. Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a ningún servidor.
- **Reglas 4 y 5.** La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y la quinta regla deja pasar el tráfico que va desde la red pública a la red de Internet.
- **Regla 6.** Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría de los casos, permite registrar los paquetes que coinciden con ella. Esto es útil por motivos jurídicos y administrativos.

9. SERVICIOS DE RED.

Aunque los servicios más conocidos en Internet son el servidor Web y el de correo electrónico, también existen otros servicios necesarios y menos conocidos que permiten crear la infraestructura de una red. Estos servicios son los siguientes:

- **Encaminamiento.** Permite a un servidor actuar como router para permitir la comunicación entre dos o más redes. Es un servicio por el cual un router enruta (o envía) el tráfico entre varias redes.
- **Servidor DHCP.** Permite asignar automáticamente la configuración IP de los equipos clientes de la red. Este servicio es muy importante ya que facilita la conexión de los equipos a la red. Por ejemplo, cuando un portátil se conecta a una red obtiene su configuración IP a través de un servidor DHCP.
- **Servidor DNS.** Permite mantener una equivalencia entre un nombre y su dirección IP. Por ejemplo, el nombre www.adminso.es equivale a 150.214.150.30.

Además de los servicios ya comentados existen otros muchos servicios como, por ejemplo, compartir datos, acceso remoto a sistema, monitorización de equipos, etcétera. A continuación, se van a ver los servicios más utilizados.

Posteriormente, veremos los dominios de Internet y los servicios de Internet más importantes.

Si quieres obtener más información, puedes ver el siguiente enlace

Servicios de red (wikipedia)

9.1. SERVICIO DHCP.

El mantenimiento y la configuración de la red de los equipos de una red pequeña es relativamente fácil. Sin embargo, cuando se dispone de una red grande con equipos heterogéneos, la administración y asignación de direcciones IPs, así como la configuración de los equipos, se convierte en una tarea compleja de difícil mantenimiento y gestión. Cualquier cambio en la configuración de red, el servidor de nombres, la dirección IP asignada, la puerta de enlace… conlleva un excesivo tiempo para ejecutar la tarea.

Por otra parte, en entornos con equipos móviles, la gestión y asignación de direcciones supone una tarea compleja que, aunque puede resolverse con la asignación de direcciones IP estáticas, conlleva la asociación fija de una dirección IP al mismo equipo, para evitar conflictos, y la imposibilidad de su reutilización si un portátil no está conectado a la red local en un momento determinado.

Éste es el mismo problema que se presenta en el entorno de trabajo de un ISP; o se dispone de un sistema de asignación dinámica y flexible que permita reutilizar las direcciones de tal forma que sólo los equipos conectados en un momento determinado a la red tienen asignada una dirección IP, o se dispone de una dirección IP distinta por cada cliente que tenemos, algo inviable con el número de usuario conectados a Internet. El servidor DHCP surge ante la necesidad de realizar la asignación dinámica y automática de las direcciones IP de una red.

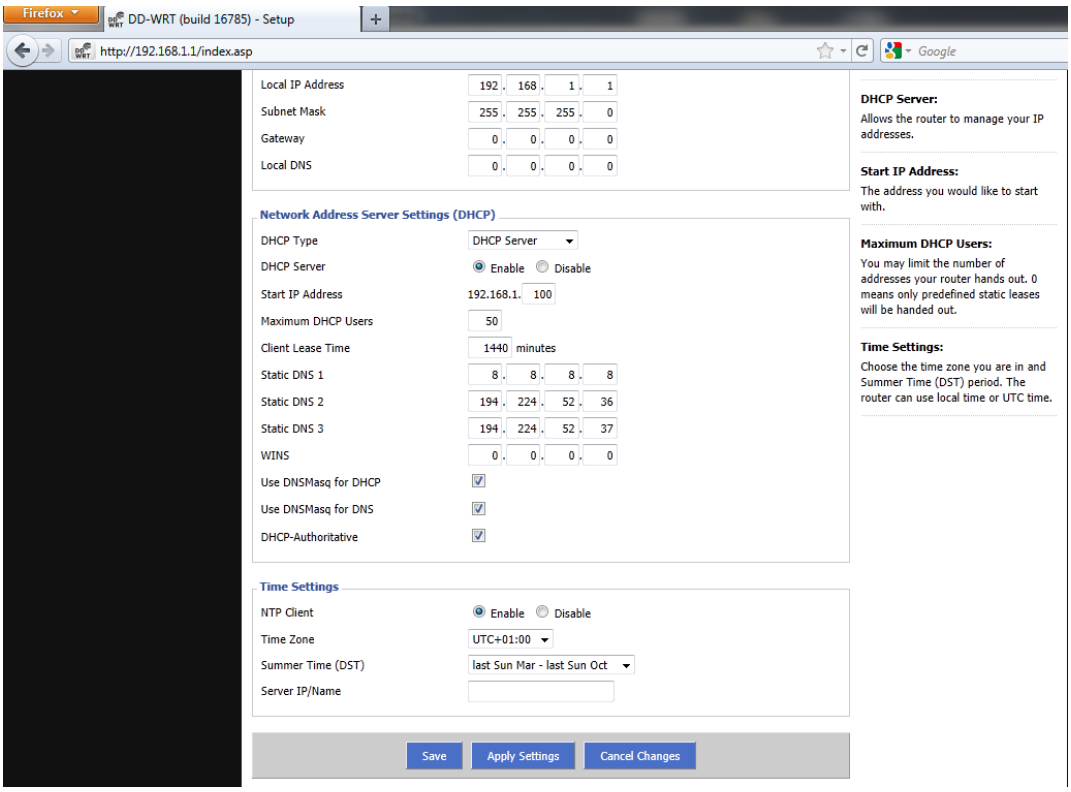
El servidor DHCP se encarga de gestionar la asignación de direcciones IP y de la información de configuración de la red en general. Para ello, necesita de un proceso (**dhcpd**) y un fichero de configuración **(/etc/dhcpd.conf)** Los datos mínimos que un servidor de DHCP proporciona a un cliente son:

- Dirección IP.
- Máscara de red.
- Puerta de enlace o gateway. Un Gateway o puerta de enlace es un equipo que permite a los equipos de una red local conectarse a una red exterior.
- Dirección IP del servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

- **Asignación dinámica.** Asigna direcciones IPs libres de un rango de direcciones establecido por el administrador en el fichero**/etc/dhcpd.conf**. Es el único método que permite la reutilización dinámica de las direcciones IP.
- **Reserva por dirección IP[22].** Si queremos que un dispositivo o equipo tenga siempre la misma dirección IP entonces la mejor forma es establecer una reserva. Para ello, en el fichero de configuración, para una determinada dirección MAC, se asignará una dirección IP. Este método es muy útil para aquellos dispositivos que no queramos que cambien de dirección IP. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP deberemos configurar nuevamente la impresora en todos los equipos clientes que la utilicen.

[22] Es un proceso por el cual un servidor DHCP reserva siempre la misma dirección IP al mismo equipo a través de su usario MAC.



Si quieres obtener más información, puedes ver más información sobre el servicio DHCP. Dynamic Host Configuration Protocol (wikipedia)

9.2. SERVICIO DNS.

Los equipos informáticos se comunican entre sí mediante una dirección IP como 193.147.0.29. Sin embargo nosotros preferimos utilizar nombres como www.mec.es porque son más fáciles de recordar y porque ofrecen la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él.

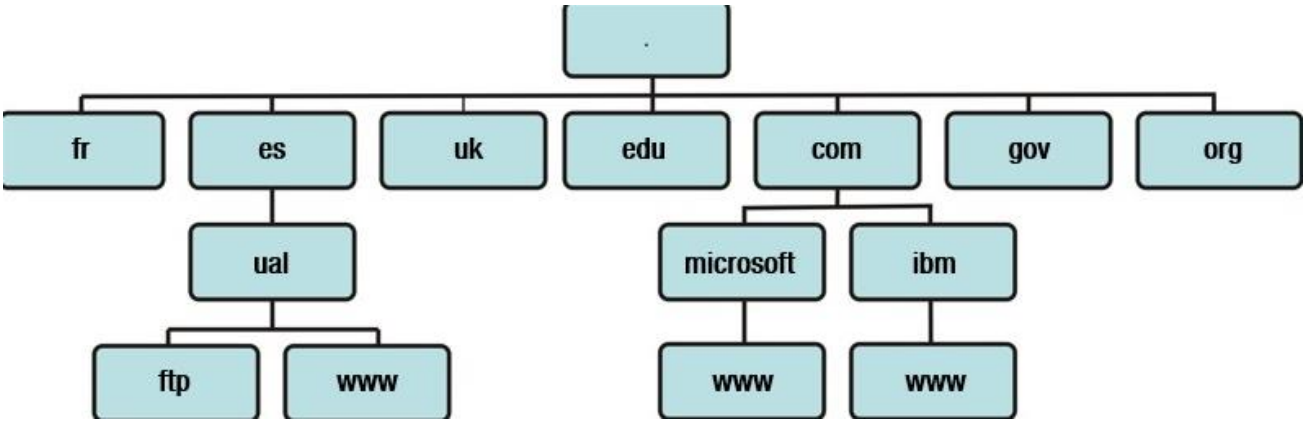
Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba de forma local a través del fichero **/etc/hosts** (Linux) o **\winnt\system32\driver\etc\hosts** (Windows) en los que se guarda cada nombre junto a su respectiva dirección IP. Con todo, esta opción presenta varios problemas.

Por un lado, todos los equipos de la red están obligados a conocer cualquier cambio para actualizar sus ficheros apropiadamente. Es decir, ante, por ejemplo, la inserción de un nuevo elemento en la red, debe añadirse en los ficheros locales de cada equipo los datos referentes a su nombre y dirección IP. Este hecho indica la poca escalabilidad y manejabilidad de esta opción, sobre todo si hablamos de Internet o, sin llegar a este extremo, de cualquier red local que tenga, por ejemplo, más de veinte ordenadores. Además, el mantenimiento tan descentralizado y dependiente de ficheros locales conlleva un alto riesgo de falta de sincronización y descoordinación entre los equipos de la red y, por tanto, de la información que manejan.

Para paliar estos problemas se ideó el sistema de resolución de nombres (DNS) basado en dominios, en el que se dispone de uno o más servidores encargados de resolver los nombres de los equipos pertenecientes a su ámbito, consiguiendo, por un lado, la centralización necesaria para la correcta sincronización de los equipos, un sistema jerárquico que permite una administración focalizada y, también, descentralizada y un mecanismo de resolución eficiente.

9.2.1. ESPACIO DE NOMBRES DE DOMINIO.

Al igual que los sistemas de ficheros se organizan en árboles jerárquicos y el nombre absoluto de un fichero es el formado por los distintos directorios que recorremos hasta encontrar el fichero, separados por el carácter '/' (o '\' en sistemas Windows), el sistema de nombres de dominios también se estructura con un árbol jerárquico en el que las distintas ramas que encontramos reciben el nombre de dominio. Así el nombre completo de un equipo (el equivalente al nombre de un fichero) o FQDN (path absoluto) es el nombre resultante de recorrer todos los dominios por los que pasamos, desde las hojas hasta la raíz del árbol utilizando, en este caso, el carácter '.' (punto) como separador.

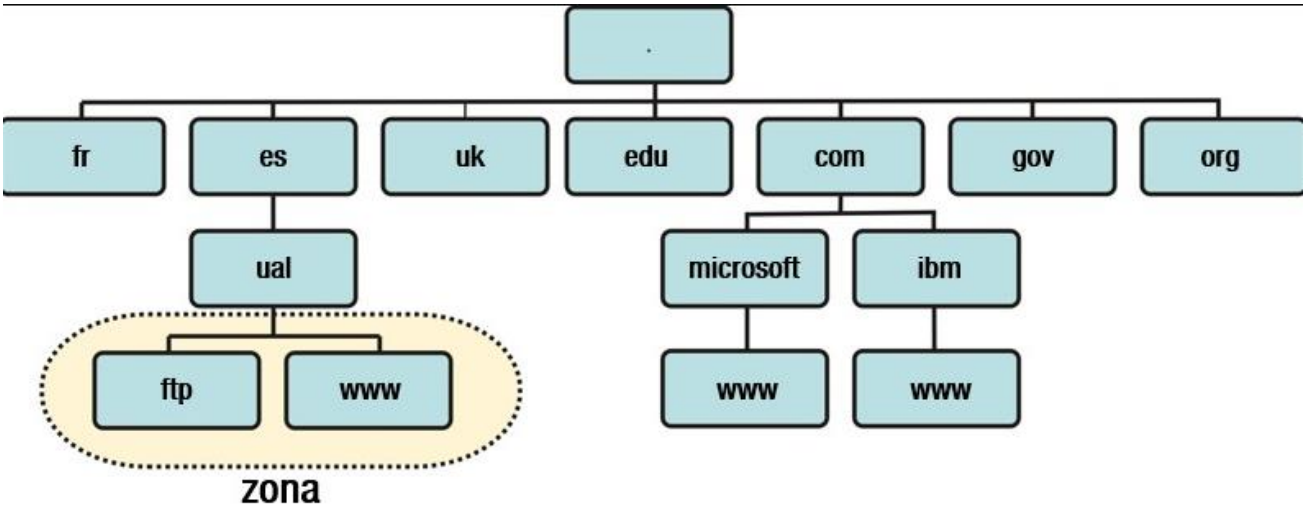


El sistema de nombres de Internet presenta, por tanto, una estructura jerárquica en árbol, en el que cada rama constituye lo que se denomina un dominio de Internet, y dependiendo de la profundidad del árbol, hablaremos de dominios de primer, segundo o tercer nivel, pudiendo existir más, aunque no es habitual.

En el primer nivel del árbol encontramos que los nombres de los nodos ya están establecidos de antemano, existiendo dos tipos de divisiones: geográfica y organizativa. Con la primera se distingue una rama -dominio- por país: **.es** para España; **.uk** para Gran Bretaña; **.de** para Alemania,... Con la segunda se establece una rama por tipo de organización: **.com** para empresas, independientemente del país en el que se encuentren; **.int** para organizaciones establecidas mediante tratados internacionales; **.org** para organizaciones no gubernamentales y, por último, **.edu**, **.gov** y **.mil** para organizaciones educativas, del gobierno y el ejército de EEUU. Posteriormente, se han introducido nuevos dominios de primer nivel como **.name** para nombres de personas; **.info** para proveedores de servicios de información; **.web** para empresas relativas a servicios web; etcétera.

Cada rama del árbol jerárquico en el que se estructura el sistema de nombres de dominio, recibe el nombre de dominio y, para la resolución global de nombres no es determinante quién se encarga de mantener la información asociada a cada dominio. Con esta estructura, la asignación de nombres de una rama del árbol de primer nivel se delega en un responsable, la empresa pública REDES para España, el cual puede decidir, a su vez, delegar la autoridad de resolución de los nombres de las distintas ramas en las que se divide, en otras corporaciones.

Un servidor DNS puede encargarse de gestionar los datos de un dominio completo o parte de un dominio. El conjunto de datos que puede administrar un servidor de nombres recibe el nombre de zona. En la siguiente figura puede verse que el servidor DNS será el encargado de gestionar los datos del dominio **ual.es**



Por otra parte, con la importancia que ha adquirido la resolución de nombres, nadie usa ya las direcciones IP, sino los nombres asociados, una característica crucial es la máxima disponibilidad del servicio. Para ello, una buena solución es que existan varios servidores independientes capaces de realizar el mismo servicio de tal forma que la autoridad de resolución de zona siga recayendo en un servidor, aunque éste puede permitir que otros puedan responder a requerimientos de los clientes. Los servidores que tienen asignada la autoridad de resolución de nombres y que gestionan la base de datos de la zona, reciben el nombre de servidores primarios. Los servidores que pueden resolver requerimientos para una zona, pero que la fuente de información la obtienen de otro servidor, reciben el nombre de servidores secundarios.

Para que no existan problemas de sincronización entre servidores, los secundarios deben conseguir sus datos del servidor primario mediante el proceso llamado “transferencia de zona” que no es más que el traspaso de todas los pares dirección IP-nombre simbólico que gestiona el servidor. Cada vez que se modifique un dato del servidor primario debe transmitirse a todos los secundarios que estén declarados para el correcto funcionamiento del sistema.

De esta forma, no sólo se consigue aumentar la disponibilidad del servicio, sino hacerlo más eficiente ya que la carga de trabajo puede repartirse entre distintos servidores. Si el objetivo es exclusivamente éste, existe otro tipo de servidores llamados caché cuya finalidad es la de responder a peticiones de resolución, consultando, previamente, las peticiones almacenadas en memoria y, si no se corresponde con ninguna de ellas, iniciar el proceso de resolución de nombres recursivo visto anteriormente. Los servidores caché sólo son útiles si el número de usuarios es suficientemente elevado para sacar provecho de la caché de direcciones.

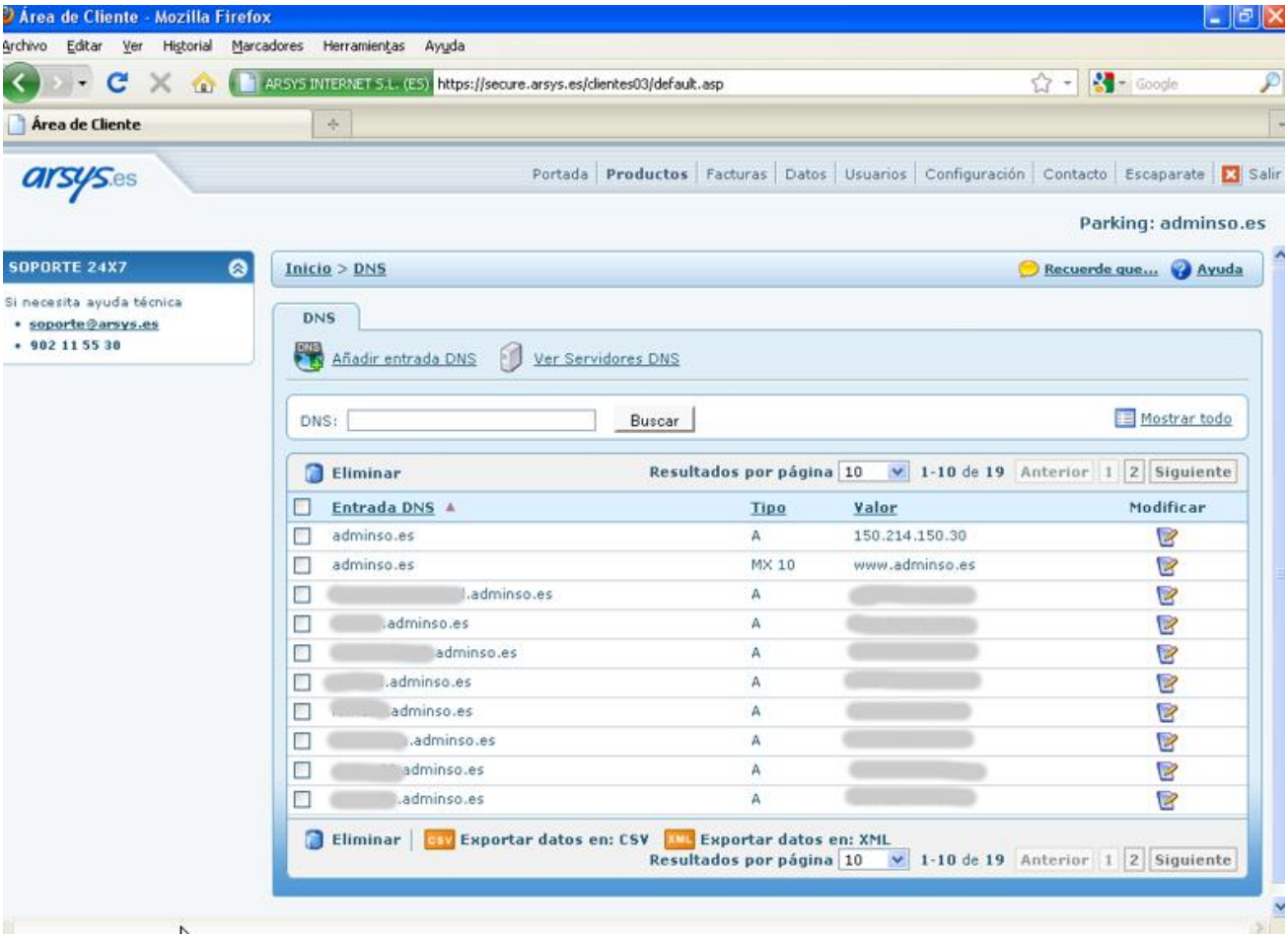
9.2.2. REGISTRAR UN DOMINIO.

Cualquier persona física con residencia en España, así como empresas constituidas según la legislación española, puede solicitar el registro de dominios a través de la página nic.es o bien, por medio de los agentes registradores acreditados. Los nombres de dominio se deben, según la reglamentación española, corresponder con:

- Nombre (o abreviatura) de una empresa que la identifique de forma inequívoca.
- Nombres comerciales o de marcas.
- Nombre de personas tal y como aparecen en su DNI, con un máximo de 60 caracteres.
- Nombres de profesiones y el apellido o nombre del profesional que se dedica a dicha labor o del nombre del establecimiento.
- Denominaciones de origen, en cuyo caso debe solicitarlo el órgano regulador de dicha denominación.

Una vez registrado el dominio podremos acceder a una web que nos permitirá gestionar los distintos registros del dominio. Por ejemplo, a continuación, se muestra la interfaz de gestión del dominio adminso.es.

Los cambios que realices en un registro estarán visibles en Internet antes de 24 horas.



9.2.3. TIPOS DE REGISTRO.

Tal y como hemos visto anteriormente, un servidor de nombres es el encargado de gestionar un dominio o parte de un dominio. El conjunto de datos que administra el servidor recibe el nombre de zona. Por ejemplo, el servidor de nombres del Ministerio de Educación es el encargado de gestionar la zona **mec.es**.

Para administrar una zona existe un servidor DNS primario y normalmente, además del servidor primario se dispone de uno o más servidores secundarios que únicamente realizan una copia de la zona.

La comunicación entre los servidores DNS se realiza mediante lo que se llama una transferencia de zona. Una zona (por ejemplo, **mec.es**) tiene registros DNS[23] (por ejemplo, www.mec.es) que son los encargados de asociar un nombre a una dirección IP. En la tabla se muestran los diferentes tipos de registros DNS de un servidor de nombres entre los que se destacan:

[23] Registro de un servidor de nombres (DNS) que permite asignar a un nombre una dirección IP (p.e., www.adminso.es apunta a 150.214.150.30).

- Registro tipo A. Es el más utilizado y permite asociar un nombre (por ejemplo, www.mec.es) con una dirección IP (por ejemplo: 193.147.0.29).
- Registro tipo CNAME. Permite establecer un alias entre dos registros. Por ejemplo, www.mec.es es igual que ftp.mec.es.
- Registro MX. Este registro es muy importante ya que permite indicar dónde se encuentra el servidor de correo electrónico (Mail eXchanger). Este tipo de registro se asocia siempre a otro nombre y permite asignar prioridades en los servidores. Así la entrada MX10 indica el primer servidor de nombres, MX20 el segundo, etcétera.

Tipos de registro

Registro	Función
SOA	Inicio de autoridad. Fija los parámetros de la zona.
NS	Servidor de nombre. Nombre de un servidor autorizado para el dominio.
A	Dirección de anfitrión. Asigna a un nombre una dirección.
CNAME	Nombre canónico. Establece un alias para un nombre verdadero.
MX	Intercambio de correo. Especifica qué máquinas intercambian correo.
TXT	Texto arbitrario. Forma de añadir comentarios.
PTR	Puntero. Permite la conversión de una dirección a nombre.
HINFO	Descripción de la computadora. CPU y S.O.
WKS	Servicios públicos disponibles en la computadora.

Si quieres obtener más información, puedes ver más información sobre el servicio DNS. DNS (wikipedia)

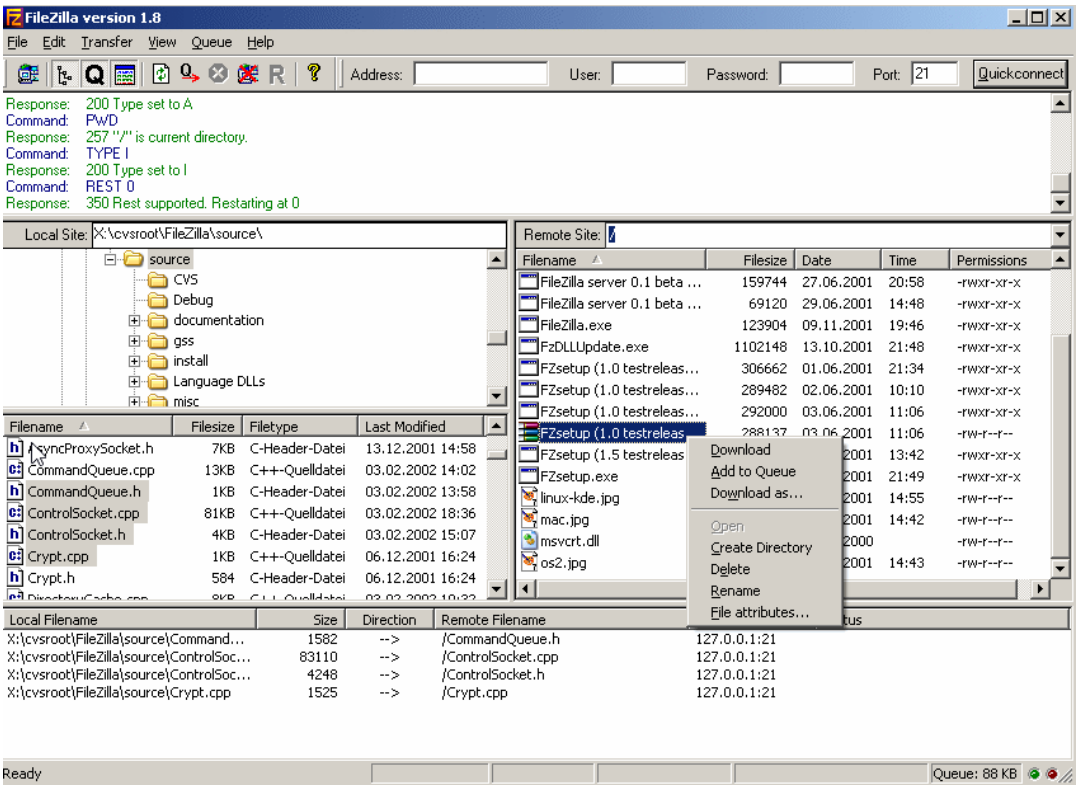
9.3. SERVICIO FTP.

FTP es el protocolo más antiguo de la capa de aplicación TCP/IP que permite la transferencia de ficheros. FTP define un protocolo cliente/servidor que describe la manera en que se establece la comunicación entre los servidores y clientes FTP. Concretamente, permite el envío y la recepción de archivos del servidor.

Aunque pueden contemplarse otras posibilidades, hay dos tipos fundamentales de acceso a través de FTP:

- **Anónimo**. La comunicación se realiza sin ningún tipo de identificación y, por lo tanto, el usuario tendrá muy pocos privilegios en el servidor. En este caso, el usuario estará confinado en un directorio público donde puede descargar los archivos allí ubicados, pero sin posibilidad de escribir o modificar ningún fichero.
- **Acceso autorizado**. El usuario establece la comunicación con una cuenta de usuario. Tras identificarse, se confina al usuario a su directorio predeterminado desde donde puede descargar ficheros y, si la política del sistema lo permite, también escribir. Esta opción es ampliamente utilizada para que los usuarios puedan acceder a sus ficheros o para poder actualizar de forma remota su portal web.

Existen programas que permiten conectarse cómodamente a un servidor FTP (por ejemplo: filezilla, cuteftp, vsftp, Internet Explorer). Sin embargo, la forma más simple de utilizar un servidor FTP es estableciendo una conexión por línea de comandos. Para poder conectarte a un servidor puedes ejecutar ftp servidor en el intérprete de comandos de tu sistema, y utilizado los comandos FTP que aparecen en la tabla de comandos de FTP, sin importar el sistema operativo que utilices, puedes trabajar en el servidor FTP.



En el siguiente enlace encontraras la tabla de comandos de FTP, que citamos anteriormente, y que te servirá para poder utilizar el protocolo FTP. Tabla de comandos de FTP.

9.4. SERVICIO WEB.

Conocido con el nombre de World Wide Web, o más concretamente, por sus siglas WWW que, además, aparecen en el nombre de prácticamente todos los servidores web, el servicio web es, posiblemente, el servicio más extendido y utilizado de los que se ofrecen en Internet, con el permiso del sistema de correo electrónico.

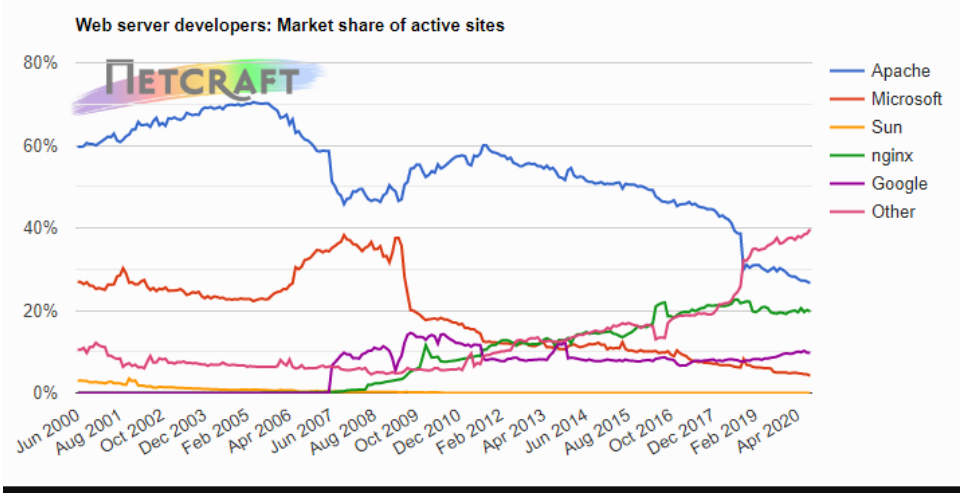
El servidor web se encarga del almacenaje y la difusión de información mediante la distribución de páginas HTML. Su arquitectura se basa en la archiconocida cliente-servidor, típica de los servicios basados en TCP/IP, en la que se distinguen: el proceso servidor, como, por ejemplo, Apache, Internet Information Server e Iplanet y el proceso cliente (también llamado navegador), como Mozilla Firefox, Google Chrome, Internet Explorer, etcétera.

El servidor es el que almacena y sirve las páginas HTML. Los navegadores se encargan, además de realizar la petición de la página deseada, de interpretarla y mostrar el resultado al usuario. Para que el cliente y el servicio se entiendan, se comunican mediante el protocolo HTTP. Este es un protocolo orientado a conexión y del tipo de solicitud-respuesta, es decir, no se guarda información de estado, sino que toda interacción entre el cliente y el servidor se fundamenta en pedir y servir.

Para identificar qué página desea un cliente, éste realiza una petición con la que especifica toda la información necesaria para que tanto el navegador como el servidor web interpreten correctamente qué recurso desea el cliente y dónde se encuentra. La petición se realiza mediante el llamado localizador universal de recursos (URL).

Para solicitar páginas y visualizarlas, los clientes web (navegadores) presentan un entorno gráfico y amigable que facilita la navegación por la WWW. Existen multitud de navegadores con la misma funcionalidad y, prácticamente, con las mismas características. Las principales diferencias entre los clientes web residen en el número e importancia de vulnerabilidades que presentan, así como en diferentes matizaciones que existen en cuanto a la interpretación del código HTML y que puede impedir la correcta visualización de algunas páginas en determinados clientes. En las siguientes figuras puede ver dos navegadores diferentes: a la izquierda Google Chrome y a la derecha Internet Explorer.

En la actualidad existen varios servidores Web tanto para sistemas GNU/Linux como para sistemas Windows. Como se observa en la siguiente gráfica, a finales de 2020 Apache sigue siendo el servidor Web más utilizado en Internet, por encima del resto de competidores, aunque en los últimos años otros servidores web como nginx han ido ganando fuerza y se prevé que eventualmente acaben superando a Apache:



9.5. SERVICIOS DE CORREO ELECTRÓNICO.

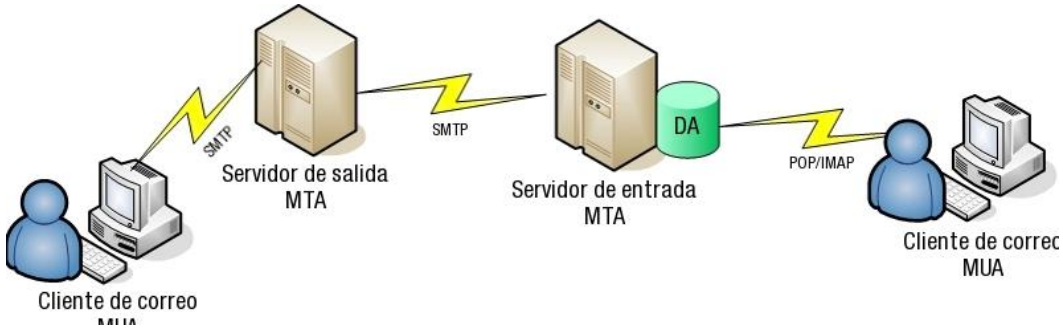
El sistema de correo electrónico es, junto al WWW, el servicio proporcionado en Internet que más importancia y auge ha presentado, al menos en cuanto al número de usuarios se refiere. De hecho, se considera como uno de los principales factores que ha popularizado el uso de Internet.

Este servicio es un sistema para la transferencia de mensajes, rápido y eficiente, ideado bajo la arquitectura cliente-servidor típica de Internet. No es simplemente un programa cliente que se comunica con un servidor mediante un protocolo de aplicación, sino que está compuesto por varios subsistemas, cada uno con una funcionalidad determinada que interaccionan entre sí mediante distintos protocolos de aplicación. La funcionalidad que todo usuario espera de este sistema es:

- Composición del mensaje.
- Transferencia desde el origen al destino sin intervención del usuario.
- Generación de un informe de la transmisión del mensaje.
- Visualización de los correos recibidos.
- Gestión de los correos: lectura, borrado, almacenaje...

Otras características que puede aportar un sistema de correo electrónico a un usuario son, por ejemplo, la redirección de correos de unas cuentas a otras, listas de correo, correo de alta prioridad o cifrado... El sistema de correo electrónico lo constituyen cuatro componentes:

- Agente de acceso (AA)[24]. Se encarga de conectar un agente de usuario al mensaje almacenado mediante protocolos de aplicación como POP e IMAP.
- Cliente de correo electrónico (MUA). [25] Ofrece los mecanismos necesarios para la lectura y composición de los mensajes de correo.
- Servidor de correo saliente (MTA)[26]. Recibe el correo electrónico y lo envía al servidor de entrada del dominio del receptor. Normalmente utiliza los protocolos SMTP o IMAP.
- Servidor de correo entrante (MTA).[27] Almacena los correos electrónicos enviados a los buzones que gestiona y cuando un cliente consulta su cuenta le envía los correos electrónicos que ha recibido. Normalmente utiliza los protocolos POP o IMAP.



[24] Se encarga de conectar un agente de usuario al mensaje almacenado mediante protocolos de aplicación como POP e IMAP.
[25] Programa que permite gestionar el correo electrónico de una cuenta de usuario.
[26] Recibe el correo electrónico y lo envía al servidor de entrada del dominio receptor. Normalmente utiliza los protocolos SMTP o IMAP.
[27] Almacena los correos electrónico enviados a los buzones que gestiona y cuando un cliente consulta su cuenta le envía los correos electrónicos que ha recibido. Normalmente utiliza los protocolos POP o IMAP.

Para comunicar los distintos subsistemas que componen la arquitectura del servicio de correo, se dispone de los protocolos:

- Simple Mail Transport Protocol (SMTP) encargado del transporte de los mensajes de correo.
- Postal Office Protocol (POP) e Internet Message Access Protocol (IMAP) encargados, ambos, de comunicar a los agentes de usuario (MUA) con los agentes de entrega de correo (MDA). Además, permiten la gestión, por parte de los usuarios, de sus buzones de correo.

El cliente de correo electrónico es una aplicación que proporciona al usuario una interfaz -más o menos amigable- con los mecanismos necesarios para escribir, recibir y contestar a mensajes. A continuación se muestra el cliente de correo Evolution.

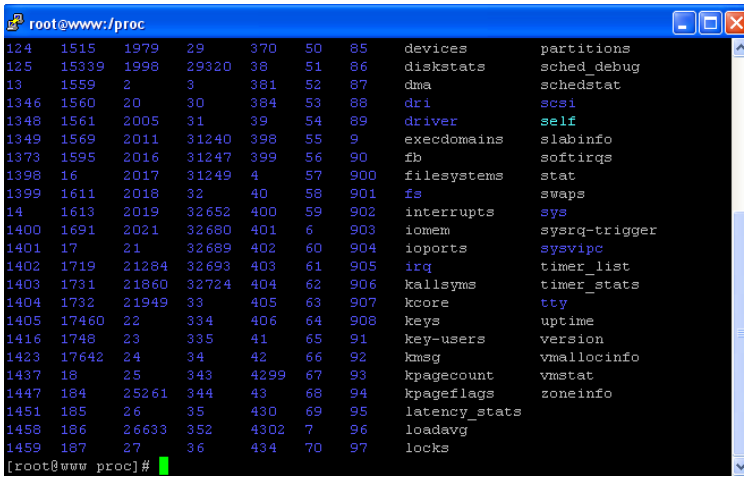
Existen clientes de correo electrónico basados en diferentes interfaces, de texto o gráfica, que introducen más o menos familiaridad y coste de aprendizaje para el usuario, pero todos presentan las mismas funciones: recepción, composición y ordenación mediante carpetas y subcarpetas del correo electrónico.

Si desea gestionar el correo electrónico en un terminal GNU/Linux puede ejecutar el comando mail.

9.6. SERVICIO DE ACCESO REMOTO.

Los servicios que permiten acceder de forma remota a un equipo a través de la red se conocen como servicios de acceso remoto y se clasifican en dos categorías:

- **Acceso remoto en modo terminal.** Para acceder a un servidor GNU/Linux en modo terminal es posible utilizar los servicios Telnet (Telecommunication NETwork) y SSH (Secure SHell). Actualmente el servicio SSH es el más utilizado ya que garantiza la seguridad de las comunicaciones mientras que el servicio Telnet no se utiliza por ser inseguro.



- **Acceso remoto en modo gráfico.** Para acceder en modo gráfico a un servidor puede utilizar el servicio VNC (Windows y GNU/Linux) o el servicio de Escritorio remoto (o Terminal Server) en sistemas Windows.

10. DISEÑO LÓGICO Y FÍSICO DE UNA RED.

Vamos trabajar con la herramienta **Cisco Packet Tracer versión estudiante**, que nos la podemos descargar en el siguiente enlace de forma gratuita, apuntándonos en el curso.

Aunque esta herramienta tiene copyright de Cisco, esta versión permite su uso a profesores y estudiantes.

Esta herramienta es muy sencilla de manejar en los aspectos básicos de cada uno de los componentes que forman nuestra red, y nos permitirá configurarlos, prácticamente como si tuviésemos el dispositivo físicamente.

Para aprender a utilizarla nos vamos a apoyar en una serie de video tutoriales, que podemos encontrar en los siguientes enlaces: Curso Packet Tracer. Ejercicios de Todo Packet Tracer.

Para obtener más información sobre la herramienta, puedes consultar su página oficial. Página oficial de Cisco Paket Tracer.

ANEXO I. EJEMPLOS DE REDES SIMPLES.

En los siguientes vídeos se muestran ejemplos de redes sencillas que van aumentando en complejidad, utilizando para su diseño el software Cisco Packet Tracer. En dichos ejemplos se aplican conceptos de direccionamiento IP como la asignación de direcciones IP, máscaras de subred y puertas de enlace por defecto.

Dos equipos conectados entre sí en la misma red:
https://www.youtube.com/watch?v=i2SzTnh9xuI&t=1s

Tres equipos conectados con un switch en la misma red:
https://www.youtube.com/watch?v=op6GIdV2eYw

Cuatro equipos conectados con dos switches en la misma red:
https://www.youtube.com/watch?v=5_a0m9Koaa0

Cuatro equipos en dos redes distintas, usando dos switches y un router:
https://www.youtube.com/watch?v=qfASIkQYz38

Red doméstica típica usando un router casero multifunción:
https://www.youtube.com/watch?v=TJ_Az8N1PmY

Equivalencia a la red anterior usando elementos simples:
https://www.youtube.com/watch?v=WuhKorLcflk