

TEMA 3

INDICE

1.- Características de las redes de ordenadores.....	3
1.1.- Sistema de comunicación.....	4
1.2.- Redes de ordenadores. Ventajas.....	5
1.3.- Redes de ordenadores. Ventajas.....	6
1.4.- Redes de ordenadores. Ventajas.....	8
2.- La arquitectura de red.....	10
2.1.- Modelo OSI y protocolos TCP/IP.....	11
2.2.- Protocolo de comunicación.....	12
2.3.- Funcionamiento de una arquitectura basada en niveles.....	13
2.4.- TCP/IP.....	14
2.5.- El nivel de acceso a la red.....	15
2.6.- El nivel de internet o de red.....	16
2.7.- El nivel de transporte.....	18
2.8.- El nivel de aplicación.....	19
3.- Topologías de red y modos de conexión.....	21
3.1.- Bus y anillo.....	22
3.2.- Estrella.....	22
3.3.- Modo infraestructura y modo ad-hoc.....	23
4.- Componentes de una red informática.....	25
4.1.- Clasificación de los medios de transmisión.....	26
4.2.- Cableado y conectores.....	26
4.2.1.- Cableado estructurado.....	28
4.3.- Elementos de interconexión.....	29
4.4.- Tarjetas de red y direccionamiento MAC.....	29
4.5.- Conmutadores.....	30
4.6.- Enrutadores.....	31
4.7.- IDS.....	32
5.- Redes inalámbricas 802.11.....	34
5.1.- Tipos de redes 802.11. Características.....	35
5.2.- El canal de una red 802.11.....	36
5.3.- El SSID de una red 802.11.....	37
5.4.- Seguridad en 802.11.....	38

Introducción a los sistemas en red.

Caso práctico

Ada está pensando en María y Antonio para que se encarguen de un proyecto de la empresa, donde tendrán que revisar la infraestructura de red y la seguridad de la red de una pequeña compañía.

Pero antes de empezar con este proyecto, deben repasar algunos conceptos importantes relacionados con las redes, ya que si no, será mucho más difícil hacer un trabajo adecuado.

Por esta razón Ada le ha pedido a María y Antonio que hagan un repaso de las características de las redes, que estudien las diferentes arquitecturas, que vean que componentes son los más adecuados para trabajar en red, y que se pongan al día en las redes inalámbricas, ya que, casi con total seguridad, en el proyecto que van a trabajar van a tener que utilizar o instalar redes inalámbricas.

1.- Características de las redes de ordenadores.

Caso práctico

Para empezar, María y Antonio van a repasar algunos conceptos que creen necesarios para conocer mejor como funcionan las redes de ordenadores.

María aún recuerda lo que estudió en el Ciclo de Administración de Sistemas Informáticos, por tanto va a encargarse de recabar información, y así poder ayudar a Antonio, que no conoce tanto sobre el tema.

Además, María ha recordado que Ana está estudiando el Ciclo de Desarrollo de Aplicaciones Multiplataforma, y seguro que tiene información actualizada sobre estos temas, por lo que le va a pedir que le pase sus apuntes.

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:

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

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.
http://es.wikipedia.org/wiki/Red_de_computadoras

1.1.- Sistema de comunicación.

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

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

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

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

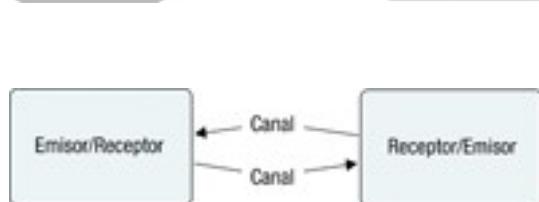
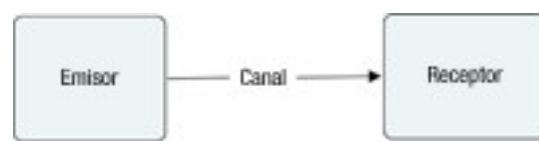
Como podemos deducir, es necesario que emisor y receptor codifiquen la información de forma que ambos se entiendan, por tanto necesitan crear un conjunto de reglas que regulen la comunicación entre ambos, este conjunto de reglas es lo que conocemos por protocolo de comunicación.

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

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

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

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



Si quieres conocer más detalles relacionados con los conceptos de simplex, semidúplex y dúplex, te sugerimos que leas el siguiente artículo de la wikipedia.
http://es.wikipedia.org/wiki/D%C3%BAplex_%28telecomunicaciones%29

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.

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.

<http://www.slideshare.net/mamogetta/sistema-de-comunicacion-redes-de-telecomunicaciones-presentation>

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** 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.

De las siguientes afirmaciones elige las que sean correctas:

- | | |
|-------------------------------------|---|
| <input type="checkbox"/> | Siempre que montemos una red de ordenadores reduciremos costes. |
| <input checked="" type="checkbox"/> | Si tenemos una red de ordenadores tenemos la posibilidad de compartir recursos. |
| <input type="checkbox"/> | Siempre que los ordenadores esten en red podremos hacer una gestión centralizada de los mismos. |
| <input checked="" type="checkbox"/> | Los motivos principales para conectar ordenadores en red suelen ser compartir una conexión a Internet y compartir información. |

1.3.- Redes de ordenadores. Ventajas.

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

Por alcance o extensión tenemos:

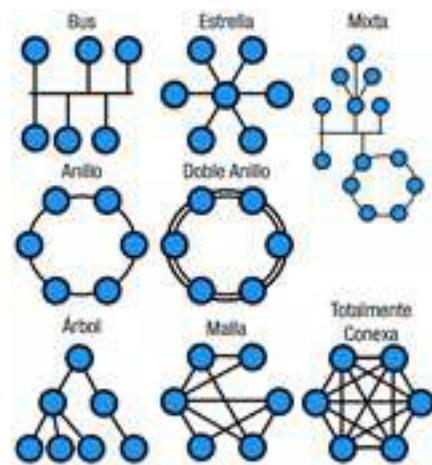
- ✓ **Red de área personal** o PAN (personal area network) es una red de ordenadores usada para la comunicación entre los dispositivos del ordenador cerca de una persona.
- ✓ **Red de área local** o LAN (local area network) es una red que se limita a un área especial, relativamente pequeña, tal como un cuarto, un aula, un solo edificio, una nave, o un avión. Las

redes de área local suelen tener las mayores velocidades, además de considerarse como el componente esencial para la creación de redes más grandes.

- ✓ **Red de área de campus** o CAN (campus area network) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar. Este término se suele utilizar como extensión del de LAN, ya que realmente lo que se tiene son redes locales conectadas entre sí para abarcar 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 entre 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 esta manera, y una de sus características más destacadas es que cada usuario controla su propia seguridad.
- ✓ **Redes cliente-servidor**, se basan en la existencia de uno o varios servidores, que darán servicio al resto de ordenadores que se consideran clientes. Este tipo de redes facilitan la gestión centralizada. Para crear redes de este tipo necesitamos sistemas operativos de tipo servidor, tales como Windows 2008 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.

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

✓ **Intranet** es una red de computadoras que utiliza alguna tecnología de red para usos comerciales, educativos o de otra índole de forma privada, esto es, que no comparte sus recursos o su información con otras redes, a no ser que autentifiquen, o cumplan unas medidas de seguridad determinadas.

✓ **Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Precisamente esta característica, es la que ha hecho que el uso de Internet se generalice y que todas las redes funcionen utilizando protocolos TCP/IP.

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.

<http://es.wikipedia.org/wiki/Internet>

¿Qué tipos de redes pueden considerarse si tenemos en cuenta el lugar en que se instalan o la zona a la que prestan servicios?

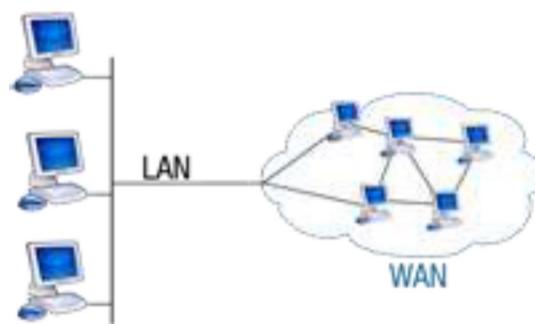
- Intranet e Internet.
- Red de área local, red área metropolitana y red de área amplia.
- Cableadas e inalámbricas.
- Bus, anillo y estrella.



1.4.- Redes de ordenadores. Ventajas.

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

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



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

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

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

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

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

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.

http://es.wikipedia.org/wiki/Conmutaci%C3%B3n_de_paquetes

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

- ✓ La **red telefónica básica** o **red telefónica conmutada** (RTB o RTC) permite que hablemos por teléfono, pero si utilizamos un módem podemos transmitir datos a baja velocidad.
- ✓ El **bucle de abonado digital asimétrico**, más conocido como **ADSL**, las operadoras de telefonía ofrecen la posibilidad de utilizar una línea de datos independiente de la línea de teléfono, aprovechando el ancho de banda disponible por encima del requerido por el servicio telefónico hasta el límite permitido por la propia línea.
- ✓ Telefonía móvil mediante **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.

Si quieras conocer más sobre las redes WAN recomendamos el siguiente documento en formato de presentación, donde se hace un exhaustivo repaso a todo lo que tiene que ver con la redes WAN. Se recomiendan especialmente las diapositivas de la 45 a la 81 donde se explican las tecnologías WAN.

<http://es.scribd.com/doc/13257660/Tecnologias-WAN>

X 2.- La arquitectura de red.

Caso práctico

María explica a Antonio algunos conceptos que son útiles para trabajar con las redes. Empieza por explicar el concepto de arquitectura, y le recuerda a Antonio que la arquitectura de una red no sólo tiene que ver con cómo se monta, es un concepto mucho más amplio y está relacionado con el software y con el hardware. Esto a Antonio le sorprende un poco, ya que él relacionaba la arquitectura con construir cosas, y por eso pensaba que la arquitectura de las redes tenía que ver con las conexiones.

María: —No Antonio, ya verás que la arquitectura de una red abarca más conceptos, además es importante conocerla porque más adelante nos ayudará en el diseño, y sobre todo en el mantenimiento de los sistemas con los que trabajamos.

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

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

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

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

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

- ✓ La forma 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, estas reglas serán los **protocolos de comunicación**.

A continuación estudiaremos con más detalle como 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.

¿Cuales son los tres factores principales a tener en cuenta para definir una arquitectura de red?

- El cableado, las conexiones y los ordenadores.



Las aplicaciones, los protocolos que usan estas aplicaciones y las conexiones.

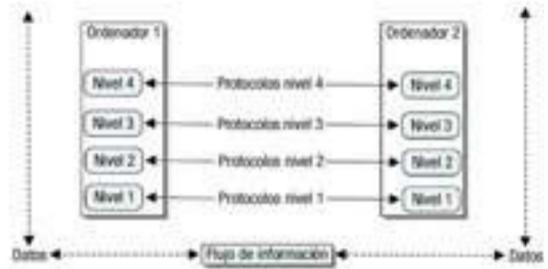
La topología, el método de acceso a la red y los protocolos de comunicaciones.

Si se tienen en cuenta estos tres factores, y se estandarizan, el resto de factores y/o características se pueden implementar más fácilmente.



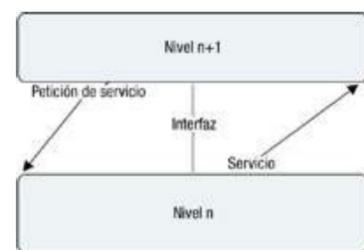
2.1.- Modelo OSI y protocolos TCP/IP.

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 esta manera la información pasará por todas las capas, se pasará al medio de transmisión adecuado y posteriormente sucederá lo mismo, pero en sentido contrario, en el otro ordenador. De esta manera la información llegará a su destino y cada nivel sólo se ocupará de los datos y la información de control que necesite, según el protocolo utilizado, sin preocuparse de lo que hagan o necesiten los otros niveles.



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

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

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

Todo esto implica que para un buen funcionamiento de la red se deben respetar ciertas reglas, como por ejemplo: que los servicios se definan mediante protocolos estándares, que cada nivel sólo se

comunique con el nivel superior o el inferior y que cada nivel inferior proporcione servicios a su nivel superior.

Hay que comentar que este tipo de arquitectura por niveles conlleva que cada nivel genera su propio conjunto de datos, ya que cada capa pasa los datos originales junto con la información que ella genera, para así poder controlar la comunicación por niveles. Esta información para los niveles inferiores se trata como si fueran datos, ya que sólo la utilizará el nivel correspondiente del ordenador de destino. Más adelante veremos los diferentes 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 que nivel se resuelve.
- ✓ **El direccionamiento:** Dado que una red se compone de muchos nodos conectados entre sí, debe haber alguna forma de conocer cual es cual. Para esto necesitamos definir direcciones de red que permitan determinar a que 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 trasnmitir, 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 ha 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.

De los que hemos explicado podemos deducir que las características principales de los protocolos son:

- El emisor, el receptor y el mensaje.
- La identificación del emisor y el receptor.
- El direccionamiento y el enrutamiento.
- Mensaje, codificación, formato, tamaño del mensaje y temporización.

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 un referencia para desarrollar arquitecturas de red, de forma que los protocolos que se desarrolle 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.

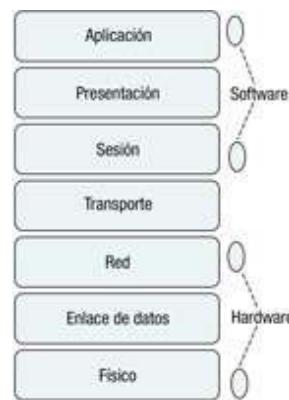
Los niveles OSI son:

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.	Empaque 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 tomarán los datos y define el direccionamiento.
4	Capa o nivel de transporte.	Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores.
5	Capa o nivel de sesión.	Mantiene y controla el enlace entre los dos extremos de la comunicación.
6	Capa o nivel de presentación.	Determina el formato de las comunicaciones así como adaptar la información al protocolo que se esté usando.
7	Capa o nivel de aplicación.	Define los protocolos que utilizan cada una de las aplicaciones para poder

aplicación. 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.



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

http://es.wikipedia.org/wiki/Modelo_OSI

Es especialmente recomendable que dediques un tiempo al siguiente video donde encontraras un explicación bastante completa de todo el modelo OSI.

http://www.youtube.com/watch?v=J4fyelWeq-Q&feature=player_embedded#!

2.4.- TCP/IP.

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

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

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

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

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 esta arquitectura está pensada para conectar ordenadores diferentes en redes diferentes, por lo que las cuestiones de nivel físico no se tratan, y se dejan lo suficientemente abiertas para que se pueda utilizar 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 tomarán los paquetes y define el direccionamiento. En esta arquitectura los paquetes pueden viajar hasta el destino de forma independiente, pudiendo atravesar redes diferentes y llegar

		desordenados, sin que la ordenación de los paquetes sea responsabilidad de esta capa, por tanto tampoco se encarga de los errores. El protocolo más significativo de esta capa es el protocolo IP, y entre sus funciones está la de dar una dirección lógica a todos los nodos de la red.
3	Capa o nivel de transporte.	Es igual al nivel de transporte del modelo OSI. Se encarga de que los paquetes de datos tengan una secuencia adecuada y de controlar los errores. Los protocolos más importantes de esta capa son: TCP y UDP. El protocolo TCP es un protocolo orientado a conexión y fiable, y el protocolo UDP es un protocolo no orientado a conexión y no fiable.
4	Capa o nivel de Aplicación.	Esta capa englobaría conceptos de las capas de sesión, presentación y aplicación del modelo OSI. Incluye todos los protocolos de alto nivel relacionados con las aplicaciones que se utilizan en Internet.

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

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 leer el artículo del Modelo TCP/IP de la wikipedia, y prestar especial atención al 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.
http://es.wikipedia.org/wiki/Modelo_TCP/IP

2.5.- El nivel de acceso a la red.

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

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

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

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

En este nivel se deben tener en cuenta las cuestiones relacionadas con las conexiones físicas, que en las redes locales vienen definidas por el estándar Ethernet. Este estándar define las características de

cableado y señalización de nivel físico, y los formatos de las tramas de datos del nivel de enlace de datos. Ethernet es la base para el estándar IEEE 802.3, que es un estándar internacional que tiene posibilidades de uso tanto en redes locales como en redes de área amplia.

Artículo sobre Ethernet y su evolución al estándar IEEE 802.3.

<http://es.wikipedia.org/wiki/Ethernet>

Otro aspecto importante de este nivel es lo relacionado con el **direcccionamiento 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.

Las 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.



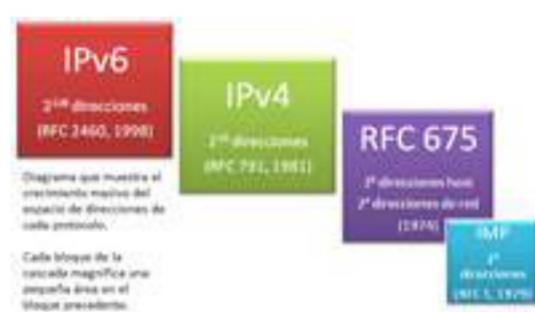
Sólo destacaremos que en la trama tenemos los datos que recibimos de las capas superiores, y que la capa de enlace le agrega una cabecera, con las direcciones MAC origen y destino, junto con el tipo de trama Ethernet que se utiliza, y una cola donde se agrega información para el control de errores.

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

http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC

2.6.- El nivel de internet o de red.

El nivel de red del modelo TCP/IP se considera el nivel de la arquitectura más importante, ya que permite que las estaciones envíen información a la red en forma de



paquetes. Estos paquetes viajan por la red de forma independiente, pudiendo atravesar diferentes redes y sin un orden establecido. Esta es una de las principales ventajas de esta arquitectura y por eso es la base de Internet.

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

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

Entre las funciones de la capa de red se encuentra:

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

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

- ✓ **IP:** Internet Protocol, o Protocolo de Internet proporciona un enrutamiento de paquetes no orientado a conexión y es usado tanto por el origen como por el destino para la comunicación de datos.
- ✓ **ARP y RARP:** También se utilizan en la capa de enlace de datos y sirven para relacionar direcciones IP con direcciones MAC y viceversa.
- ✓ **ICMP:** Protocolo de mensajes de control en Internet, suministra capacidades de control y envío de mensajes. También se considera protocolo del nivel de transporte, y herramientas tales como ping y tracert lo utilizan para poder funcionar.
- ✓ **OSPF:** Es un protocolo de enrutamiento que busca el camino más corto entre dos nodos de la red.
- ✓ **RIP:** Protocolo de enrutamiento de información, al igual que OSPF, también busca el camino más corto, pero utilizando otras técnicas de enrutamiento.

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

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.

http://es.wikipedia.org/wiki/Protocolo_IP

<http://es.wikipedia.org/wiki/IPv4>

<http://es.wikipedia.org/wiki/IPv6>

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 las redes físicas.

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 un 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.

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

http://es.wikipedia.org/wiki/Transmission_Control_Protocol

http://es.wikipedia.org/wiki/User_Datagram_Protocol

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 término puerto se utiliza en Internet, el término 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).

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

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

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**) 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**

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

<http://es.wikipedia.org/wiki/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.

El modelo TCP/IP permite definir una arquitectura de red, que se utiliza en el diseño e implementación de dispositivos de red y software de red, tales como los sistemas operativos, que nos permiten utilizar las redes de ordenador y conectarnos a internet. TCP/IP tiene cuatro niveles, que son: nivel de acceso a la red o de subred, nivel de internet o red, nivel de transporte y nivel de aplicación. Los protocolos principales de este modelo son: TCP e IP. Además uno de los protocolos más utilizados en el nivel de aplicación es el protocolo HTTP, que se utiliza para dar servicio de páginas web.

3.- Topologías de red y modos de conexión.

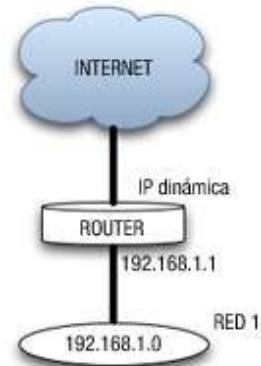
Caso práctico

Maria y Antonio ya han repasado todo lo que tiene que ver con la arquitectura de ordenadores. Ahora se van centrar en las topologías y los modos de conexión. María conoce la diferencia, pero Antonio aún no tiene muy claro qué es lo que diferencia un concepto de otro.

Vamos a ayudarle a entenderlo.

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 un 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 como 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 como 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.

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.

Relaciona cada concepto con su definición:

Relacionar topologías y modos de conexión.

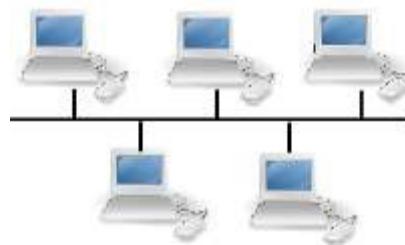
Concepto	Relación	Definición
Topología física	3	1. Esquema de conexión que muestra algunas características de la conexión.
Topología lógica	1	2. Modo de conexión inalámbrico, especialmente pensado para un propósito específico.
Modo infraestructura	4	3. Forma de conectar los ordenadores de una red.
Modo ad-hoc	2	4. Modo de conexión para ordenadores inalámbricos, que utiliza punto de acceso.

Es conveniente que sepas diferenciar las topologías y los modos de conexión, las primera están más relacionadas con las conexiones físicas y el diseño, y las otras tienen relación con el diseño de redes inalámbricas.

3.1.- Bus y anillo.

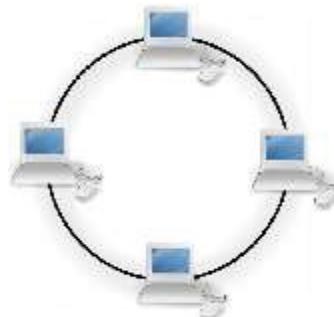
La topología en bus utiliza un único cable troncal con terminaciones en los extremos, de tal forma que los ordenadores de la red se conectan directamente a la red troncal. La primeras redes Ethernet utilizaban esta topología usando cable coaxial.

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



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 el pasan todos los paquetes de usuarios, este nodo central realizará funciones de distribución, conmutación y control. Es importante que este nodo siempre esté activo, ya que si falla toda la red queda sin servicio.

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

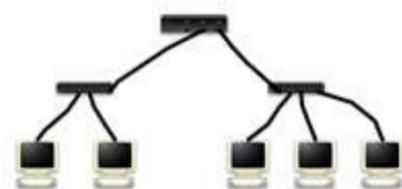


Un ampliación de la topología en estrella es la estrella extendida o árbol donde las redes en estrella se conectan entre sí.



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.

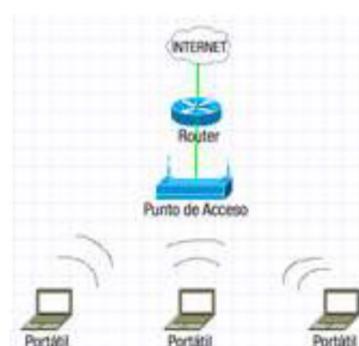
Este tipo de topologías es muy típica en redes de área local donde el principio de la jerarquía será el router que conecta a Internet, usualmente el que nos pone la compañía de telecomunicaciones, y el resto son los switch que dan servicio a diferentes aulas, salas de ordenadores, despachos, etc.



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

3.3.- Modo infraestructura y modo ad-hoc.

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



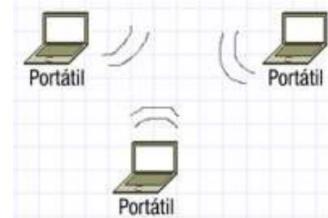
En las redes inalámbricas con estándar IEEE 802.11, también llamadas redes Wi-Fi se especifican dos modos de conexión, que son el modo infraestructura y el modo ad-hoc. Cabe mencionar, que algunas veces oiréis hablar de modo de conexión o topología de conexión en referencia a la forma de conectar los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

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

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

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

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



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

Lo que caracteriza al modo infraestructura es:

- Que todos los ordenadores se pueden conectar a Internet.
- Que todos los ordenadores pueden compartir información de forma inalámbrica.
- Que todos los dispositivos inalámbricos se conectan a través de un punto de acceso.

4.- Componentes de una red informática.

Caso práctico

Antonio está acostumbrado a montar y desmontar el ordenador, pero no sabe muy bien como montar redes que sean eficaces y que puedan trabajar con distintas tecnologías a la vez.

Con María están repasando todo lo que tiene que ver con las redes de ordenadores, y ahora van a dar un repaso a un buen número de componentes que se usan para montar las redes.

Como existen muchos componentes distintos se van a centrar en aquellos más utilizados.

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 este 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.

Relaciona los conceptos con sus definiciones:

Ejercicio de relacionar.

Concepto	Relación	Definición
Nodo de red	2	1. Permite conectar redes diferentes.
Estación de trabajo	4	2. Cualquier dispositivo o periférico que pueda conectarse a la red o utilizarse a través de la red.
Router	1	3. Permite conectar segmentos de red diferentes.
Switch	3	4. Ordenador que trabaja en red.

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 hablamos 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 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:

http://es.wikipedia.org/wiki/Medio_de_transmisión

4.2.- Cableado y conectores.

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

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

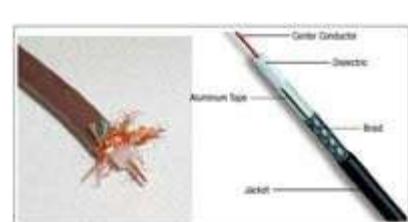
Los colores son: blanco-naranja, naranja, blanco-verde, verde, blanco-azul, azul, blanco-marrón y marrón. La distribución de estos colores cuando se conectan en el conector viene estandarizada, para que las conexiones de red sean fácilmente reconocibles.

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

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.

http://es.wikipedia.org/wiki/Cable_de_par_trenzado

<http://es.wikipedia.org/wiki/RJ-45>



También se utiliza en las redes de ordenador, el **cable coaxial**.

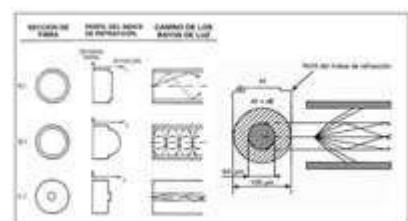
Este cable está compuesto de un hilo conductor, llamado núcleo, y un mallazo externo separados por un dieléctrico o aislante.

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 quieras saber algo más sobre el cable coaxial te recomendamos el siguiente enlace.

http://es.wikipedia.org/wiki/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, en las redes de ordenadores se suele utilizar el láser. Permite transmitir gran cantidad de datos a una gran distancia, a una velocidad adecuada, y al ser inmune a las interferencias electromagnéticas es muy fiable. Es utilizado en la distribución de señales de telecomunicaciones a largas distancias y en las redes locales, constituye la infraestructura de distribución de la señal que permite conectar redes entre sí, por ejemplo en un mismo edificio. Esto último es conocido como **backbone**.

Tenemos dos tipos de fibra óptica, la 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.

http://es.wikipedia.org/wiki/Fibra_%C3%B3ptica

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.



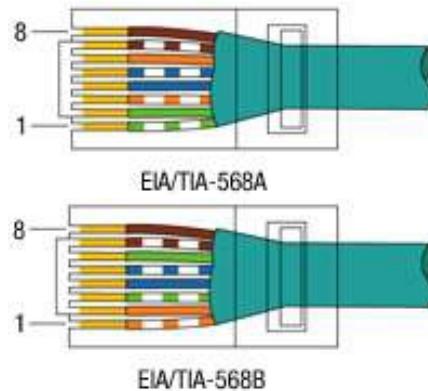
El cableado estructurado define algunos subsistemas para organizar la instalación del cableado. Los subsistemas de cableado estructurado son:

- ✓ 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.

http://es.wikipedia.org/wiki/Cableado_estructurado

4.3.- Elementos de interconexión.

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

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



- ✓ En el **nivel físico** tenemos:
 - ➔ Tarjetas de red: pueden ser cableadas o inalámbricas. Las tarjetas de red permiten conectar los equipos a la red.
 - ➔ Concentradores también conocidos como hubs: permiten distribuir la señal a diferentes ordenadores sin discriminar entre ello.
 - ➔ Repetidores: pueden ser locales o remotos, y su función es repetir la señal para regenerarla y/o amplificarla.
- ✓ En el **nivel de enlace de datos** tenemos:
 - ➔ Conmutadores o switch: se encargan de conectar segmentos de red, y ordenadores entre sí pero de forma más eficaz que un concentrador, ya que sólo envía la información al ordenador que la necesita.
 - ➔ Puentes o bridges: conectan subredes, transmitiendo de una a otra el tráfico generado no local.
 - ➔ Puntos de acceso: pueden considerarse como elementos de nivel de enlace de datos, se encargan de conectar elementos inalámbricos entre sí, y de permitir el acceso de dispositivos inalámbricos a redes cableadas.
- ✓ En el **nivel de red**:
 - ➔ Encaminador o router: se encarga de conectar redes diferentes. Su principal uso está en la conexión a Internet, ya que permite que redes de área local puedan conectarse a Internet. Se basa en el uso del protocolo IP, por lo que necesita tener asignadas al menos dos dirección IP, una para Internet y otra para la red local. También maneja protocolos de enrutamiento y de control de red. Puede dar servicio inalámbrico y por tanto dar servicio de punto de acceso.
- ✓ En los **niveles superiores**:
 - ➔ Pasarelas: suele denominarse pasarelas a los equipos de interconexión que trabajan en los niveles superiores del modelo OSI. Existen diferentes tipos de pasarelas, podemos tener las que se encargan de conectar redes con tecnologías diferentes, las que facilitan el control de acceso a una red, las 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, qué protocolos utilizar, y todo 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.

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

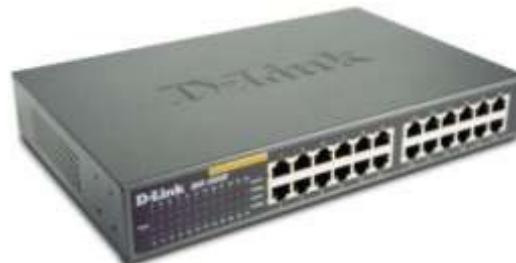
<http://es.kioskea.net/contents/pc/carte-reseau.php3>

Gracias a la relación que se establece entre la dirección **MAC** de la tarjeta, y la dirección **IP** que se le asigna se puede identificar a un ordenador en la red.

4.5.- Comutadores.

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.

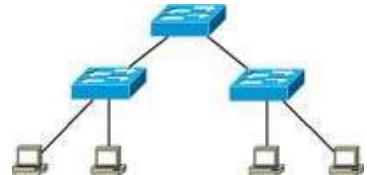


Esta característica es la que le hace ser el elemento central de conexiones en las redes de área local con topología en estrella.

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.

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



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

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

http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29

<http://es.wikipedia.org/wiki/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 la 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, qué 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 qué 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.

<http://es.wikipedia.org/wiki/Router>

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.

<http://es.kioskea.net/contents/detection/ids.php3>

5.- Redes inalámbricas 802.11.

Caso práctico

María y Antonio ya han repasado muchos de los conceptos que les hacían falta. Pero todavía falta repasar algunas cosas de las redes inalámbricas, ya que en muchos casos se encontrarán con redes Wi-Fi y tendrán que saber cuales son sus características y sus posibilidades de uso.

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 tecnología 3G, 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.

http://es.wikipedia.org/wiki/Red_inal%C3%A1mbrica

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

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

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

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

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

- ✓ Algunas **ventajas** de las redes Wi-Fi son:
 - ➔ Movilidad: se pueden conectar dispositivos estáticos y móviles.
 - ➔ Escalabilidad: son relativamente fáciles de ampliar, tanto en usuarios como en cobertura.
 - ➔ Flexibilidad: se puede conseguir un alto grado de conectividad.
 - ➔ Menor tiempo de instalación: instalando un punto de acceso se puede conseguir rápidamente conectividad.
- ✓ Las mayores **desventajas** son:
 - ➔ La seguridad: es difícil conseguir un alto grado de seguridad.
 - ➔ Interferencias: al trabajar en rangos de frecuencias compartidos por otros dispositivos se pueden tener muchas interferencias.

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

<http://www.microsoft.com/spain/technet/recursos/articulos/wifisocho.mspx>

5.1.- Tipos de redes 802.11. Características.

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

Dentro del estándar se definen los conceptos de:

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

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

- ✓ **IEEE 802.11a:** 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, 8 para redes inalámbricas y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b.
- ✓ **IEEE 802.11b:** opera en la banda de 2,4 Ghz tiene una velocidad máxima de 11 Mbps, con velocidades reales de entre 2 y 4 Mbps, tiene 14 canales, y pueden usarse 3 sin solapamiento en redes inalámbricas. Esta versión tiene una ventaja con respecto a la anterior y es el alcance, puede llegar a dar cobertura a 120 metros en exterior y 60 metros en interior con velocidades adecuadas.
- ✓ **IEEE 802.11g:** 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 pudiendo usarse hasta 11, teniendo en cuenta que deben ir de 3 en 3 para impedir el solapamiento, para esto hay que cuidar el diseño de la red. 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.
- ✓ **IEEE 802.11n:** 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. Además es útil que trabaje en la banda de 5 Ghz ya que está menos congestionada y sufre menos interferencias de otros dispositivos. Tiene una velocidad máxima de 600 Mbps con velocidades medias de operación de entre 100 y 200 Mbps. 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, esto permite usar múltiples antenas transmisoras y receptoras para mejorar la eficiencia del sistema, permitiendo manejar más información que si utilizáramos una sola antena.

En que se diferencian las versiones del estándar IEEE 802.11:

- Qué ninguna puede trabajar con las otras versiones.
- En las velocidades y coberturas.
- En la certificación Wi-Fi.
- En los canales.

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 subdivididas en canales. Estos canales pueden variar según las leyes de cada país, por lo que el número de canales que se pueden utilizar puede variar de un país a otro.

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

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

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

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

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

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

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

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

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

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

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

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

http://es.wikipedia.org/wiki/IEEE_802.11n

<http://www.intel.com/support/sp/wireless/sb/cs-025344.htm>

5.3.- El SSID de una red 802.11.

Una vez que ya sabemos como funcionan los canales vamos a explicar el término SSID de una red inalámbrica. Cuando se instala una red inalámbrica es conveniente asegurarnos de que los ordenadores se conectan con la red apropiada, esto se hace utilizando un SSID, que son las siglas en inglés 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.

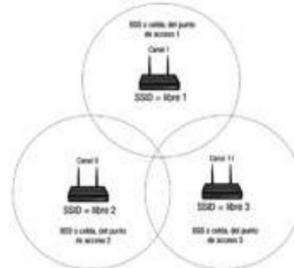
Cuando hablamos de redes ad-hoc, el área cubierta por la red se le llama conjunto de servicios básicos independientes cuyas siglas en inglés son **IBSS**. En el caso de una red en modo infraestructura el área cubierta por un punto de acceso se le llama conjunto de servicios básicos,

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 del estándar IEEE 802.11b/g, implicará utilizar canales con una diferencia de 5.

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

Tres puntos de acceso configurados para no interferirse, y para formar tres redes diferentes.



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.

Hemos visto muchos términos parecidos, pero cuáles son las siglas que se utilizan para definir el nombre de la red inalámbrica y que los usuarios puedan conectarse.

- ESS
- BSS
- 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, esta 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 autenticado 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. Esta 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.

<http://www.intel.com/support/sp/wireless/wlan/sb/cs-025323.htm>