Tema 3. *REDES. INTERNET*

1.- Redes de ordenadores

- Concepto de red de ordenadores.
- Hardware de redes locales
- Medios de comunicación
- Ejemplo de red local
- Cómo se comunican los ordenadores: protocolos
- Dirección IP (Ipv4 - IPv6)
- Redes inalámbricas

2.- Internet

- Qué es Internet
- Servidores y hosts
- Qué es un anfitrión (host)
- Nombre de dominio
- Dominios principales
- Servidores DNS
- Proveedores de acceso a Internet
- Servicios de internet: WWW, FTP, Correo electrónico, buscadores….
- La web 2.0: blogs, wikis, redes sociales…

3- World Wide Web

- Documento de hipertexto
- Significado de los términos http y html
- Dirección url
- Web 2.0

4- El navegador Web

- Guardar un documento
- Abrir un fichero del ordenador local
- Guardar una imagen

5- Búsqueda de información

- Buscadores
- Motores de búsqueda e índices temáticos

6- Transferencia de ficheros (FTP)

- ¿Qué es FTP?
- Sesión ftp con un navegador web

7- Correo electrónico

- Qué es el correo electrónico
- Programas de correo
- Qué es la dirección de correo electrónico
- Estructura de un mensaje

8- Seguridad en redes cableadas e inalámbricas. Seguridad en Internet

- Principios de la seguridad
- Seguridad física y lógica.
- Riesgos y amenzas en internet
- Cortafuegos (Firewall)
- Criptografía
- Autenticación
- NAT, DPI y VPN
- WPA2
- Filtrado MAC

1.- REDES DE ORDENADORES

CONCEPTO DE RED DE ORDENADORES

Una red es un conjunto de ordenadores, conectados entre sí que pueden comunicarse compartiendo datos y recursos. A través de una red se pueden realizar, entre otras, las siguientes operaciones:

- Acceder a ficheros de otros ordenadores e, incluso, ejecutar sus programas.
- Enviar mensajes.
- Compartir programas y recursos como bases de datos, impresoras, discos… o la conexión a internet.

Los ordenadores suelen estar conectados entre sí mediante cables o por ondas electromagnéticas Wi-Fi. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas o medios inalámbricos, como ondas electromagnéticas, microondas, fibra óptica, satélites…

HARDWARE DE REDES LOCALES

Para interconectar varios ordenadores necesitamos varios recursos hardware:

- **Adaptador o Interfaz de red** (o tarjeta de red): su función es convertir la información que quiere enviar el ordenador en señales que se puedan transmitir por el medio.
- **Router:** (enrutador o encaminador), su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir interconectar dos redes. Construyen tablas de encaminamiento con **direcciones IP** para saber cuál es la mejor ruta hacia cada destino.
- **Switch: (**conmutador) dispositivo cuya función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta. Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

- **Punto de acceso inalámbrico:** (*Wireless Access Point*, conocido por las siglas WAP o AP) es un dispositivo de red que interconecta equipos de comunicación cableada para formar una red inalámbrica que interconecta dispositivos móviles o con tarjetas de red inalámbricas.

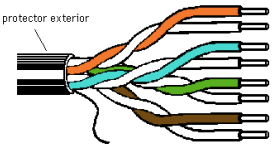
- **Servidor de red:** nodo que ofrece algún servicio: web, ftp, correo electrónico…
- **Medios de comunicación:** es la vía por la que se transmite la información en una red. Pueden ser cableados o inalámbricos.

MEDIOS DE COMUNICACIÓN

Son el cableado y los conectores que enlazan los componentes de la red. Existen diferentes tipos de medios de comunicación, agrupados en dos grandes categorías: medios cableados y medios inalámbricos.

Los **medios físicos (en redes cableadas)** más utilizados son:

- el **cable de par trenzado**, y conectores RJ-45. El cable par trenzado consiste en 8 hilos de cobre aislados entre sí, trenzados de dos en dos que se entrelazan de forma helicoidal. De esta forma el par trenzado constituye un circuito que puede transmitir datos. Un cable de par trenzado está formado por 4 pares trenzados, recubiertos por un material aislante. Cada uno de estos pares se identifica mediante un color.

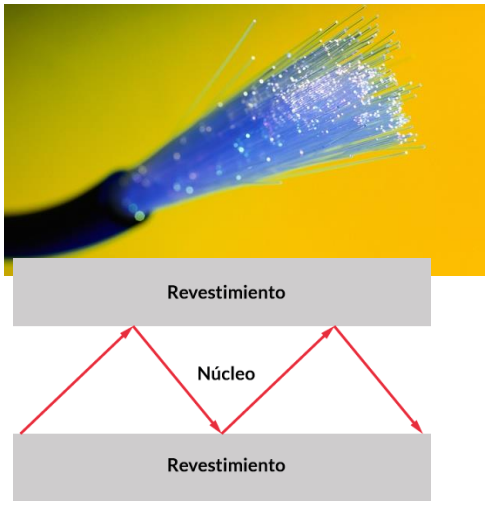


Cable UTP (4 pares)

- el **cable coaxial** : es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado núcleo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla, blindaje o trenza, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante (también denominada chaqueta exterior).El conductor central

  puede estar constituido por un alambre sólido o por varios hilos retorcidos de cobre; mientras que el exterior puede ser una malla trenzada, una lámina enrollada o un tubo corrugado de cobre o aluminio. En este último caso resultará un cable semirrígido.

- la **fibra óptica**: consistente en 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. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión. La fuente de luz puede provenir de un láser o un diodo led.



Propagación de la luz en fibra óptica.

Los **medios inalámbricos** emplean medios no guiados, van por el aire. Siguen estándares de la IEEE (Instituto de Ingenieros Electronicos y Electricos). Los más empleados son:

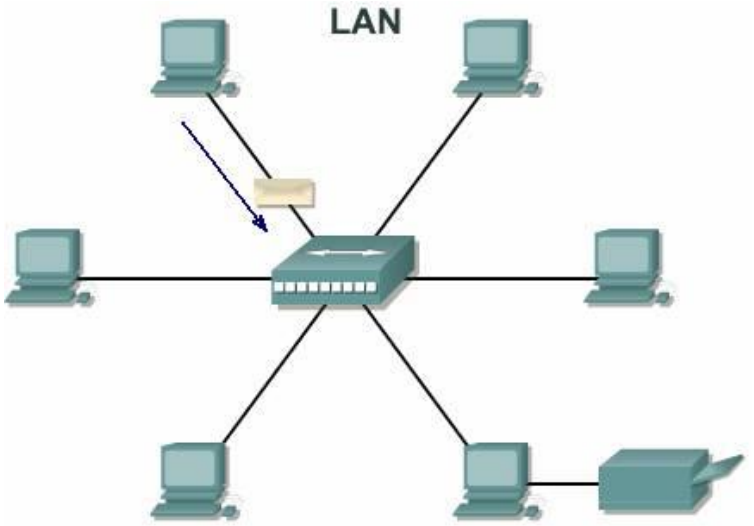
- **Ondas electromagnéticas o WiFi**: invisibles, viajan a la velocidad de la luz. El estándar es el 802.11g. La cobertura es de unos cuantos metros cuadrados. Velocidad hasta 56Mbps.
- **WiMax**: ofrece 48km de radio de cobertura, a velocidades de hasta 70 Mbps.
- **Microondas**: son un tipo de radiofrecuencia que no supera la curvatura de la tierra y requiere de antenas repetidoras para mantener la conexión. Alcance de varios kilómetros cuadrados.

- **Satélite digital**: hace uso de satélites que orbitan en el espacio y dan mayor cobertura.
- **Bluetooth:** para redes de área personal con poca cobertura, unos pocos metros.
- **Láser:** esta tecnología utiliza un diodo emisor de luz o un láser como fuente de transmisión. Para recibir la señal, los haces de luz se centran en un lente de recepción conectada a un receptor de alta sensibilidad a través de un cable de fibra óptica.

EJEMPLO DEMONTAJE DE RED LOCAL CABLEADA (LAN)

Supongamos que vamos a conectar 8 ordenadores en una red local o LAN mediante par trenzado. Necesitamos: un switch de 10 entradas, un router, cable par trenzado con conectores RJ-45.

1. En primer lugar conectamos las tarjetas de red a los ordenadores.
2. En segundo lugar conectamos los conectores RJ-45 de los cables a los ordenadores por un extremo y al switch por el otro extremo.
3. En tercer lugar conectamos el switch al router mediante el par trenzado.
4. Por último configuramos el protocolo TCP/IP en cada equipo. Podemos configurar la dirección IP de cada equipo de dos formas: IP fija en cada ordenador o dinámica. En este caso el router asignará la IP de forma dinámica.



CÓMO SE COMUNICAN LOS ORDENADORES: PROTOCOLO TCP/IP

Sea cual sea el tipo de ordenador que se tenga (PC clónico, DELL, Apple, servidor SUN...) o el sistema operativo que se utilice (UNIX, Windows 95, MS DOS, OS/2, etc.), la comunicación entre dos ordenadores en Internet es posible porque "hablan" el mismo lenguaje: ***protocolo de comunicaciones.*** El protocolo usado en Internet es conocido por sus siglas: **TCP/IP**.

El protocolo establece las normas en la comunicación: la división de mensajes en paquetes y el tamaño de los mismos, los códigos para detectar errores, etc…

DIRECCIÓN IP (192.168.1.73)

Cada ordenador conectado a Internet tiene una **dirección Internet** exclusiva, denominada *dirección IP*, que lo distingue de cualquier otro ordenador en el mundo. Esta dirección está formada por cuatro números separados por puntos, cada uno de los cuales puede tomar valores entre 0 y 255.

Por ejemplo, las siguientes podrían ser dos direcciones IP válidas: 130.238.44.8 y 199.22.125.15.

Actualmente se está migrando desde el protocolo IPv4 a una nueva versión del protocolo llamado IPv6.

IPv4 soporta **4.294.967.296** direcciones de red. Este es un número pequeño cuando se necesita otorgar a cada computadora, teléfono, PDA, etc. una dirección de red.

IPv6 soporta **340.282.366.920.938.463.463.374.607.431.768.211.456** (340 sextillones) direcciones de red; un número notablemente superior al anterior Ipv4.

Características de la IPv6

Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.
- Capacidad de ampliación, calidad del servicio y mayor velocidad.

Direcciones IPv6.

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo Ipv6. Está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits. La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales, como en IPv4, se pueden obviar.

Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 → 2001:123:4:ab:cde:3403:1:63.

- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación sólo se puede hacer una vez.

Ejemplo: 2001:0:0:0:0:0:0:4 → 2001::4.

Ejemplo no válido: 2001:0:0:0:2:0:0:1 → 2001::2::1 (debería ser 2001::2:0:0:1 ó 2001:0:0:0:2::1).

REDES INALÁMBRICAS

En las redes inalámbricas la conexión de nodos que se da por medio de **ondas electromagnéticas**, sin necesidad de una red cableada. Una de sus principales ventajas es notable en los costos, ya que se elimina el cableado Ethernet y conexiones físicas entre nodos, pero también tiene una desventaja considerable ya que para este tipo de red se debe tener una **seguridad** mucho más exigente y robusta para evitar a los intrusos, además de ser **más lentas** que las cableadas.

2- INTERNET

QUÉ ES INTERNET

Internet es una **red mundial de redes** de ordenadores, que permite a estos comunicarse y compartir información. No es una red "típica" de ordenadores, sino una red de redes, donde cada una de ellas es independiente y autónoma.

Año	1989	1992	1995	1996
Redes conectadas en Internet	**800**	**7.000**	**61.000**	**134.365**

Como dato significativo, en el año 2010 se superan los **5.000 millones** de ordenadores conectados a Internet en todo el mundo (*y estamos hablando únicamente de ordenadores; a Internet también se conectan hoy día los teléfonos móviles, video-consolas, tablets, etc*.).

Internet emplea la arquitectura cliente-servidor (la aplicaciones se divide en dos partes: una parte se ejecuta en el servidor y otra parte en el cliente). Hay dos tipos de ordenadores en internet:

- **Servidores**: proveen servicios de internet, como la WWW, de correo, de webhosting, …
- **Clientes**: envían peticiones a los servidores y reciben datos normalmente a través de un navegador web.

ANFITRIÓN (HOST)

En Internet, un anfitrión o *host* es cualquier ordenador conectado a la red.

A aquellos a los que se accede en busca de información se les llama **servidores**: servidores Web, servidores FTP, servidores IRC.... dependiendo del servicio utilizado.

A los ordenadores desde los que se solicita la información se les llama **clientes**.

PROVEEDORES DE ACCESO A INTERNET

La mayoría de los usuarios que se conectan a Internet lo hacen a través de un intermediario al que se conoce como proveedor de acceso a Internet. A él hay que abonarle una cuota fija, o variable, por los servicios que ofrece: posibilidad de navegar, cuenta de correo electrónico, espacio para páginas Web, etc. Algunos proveedores de internet son Movistar, Blaveo, Jazztel, Orange, Vodafone….

NOMBRE DE DOMINIO

Además de la dirección IP, existe otra forma de identificar cualquier ordenador en Internet, más fácil de recordar, y que permite saber, generalmente, el país en el que se encuentra. Se trata del **nombre de dominio**.

Este otro nombre está constituido por un conjunto de palabras, separadas igualmente por puntos. Por ejemplo: iesfuente.es, juntadeandalucia.es.

La primera palabra que aparece a la izquierda de un nombre de dominio se refiere habitualmente al nombre del ordenador, mientras que cada una de las palabras que la siguen corresponden a *subdominios* cada vez más amplios.

Por ejemplo, el nombre ficticio: pitagoras.mat.iesfp.es podría corresponder al ordenador **pitagoras** del departamento de matemáticas (subdominio **mat**) del I.E.S. Fuente de la Peña (subdominio **iesfp**) situado en España (dominio principal **es**).

SITIO WEB	NOMBRE DE DOMINIO	DIRECCIÓN IP
ANAYA EDUCACIÓN	www.anaya.es	194.224.88.153
JUNTA DE ANDALUCÍA	www.juntadeandalucia.es	217.12.16.221
PRESIDENCIA DEL GOBIERNO	www.la-moncloa.es	217.140.16.48
WEB OPENOFFICE	es.openoffice.org	204.16.104.2

Tabla de equivalencias *(las IP's pueden ser cambiantes en el tiempo por lo que no tienen porqué coincidir los dominios del ejemplo anterior con las IP's asignadas).*

Ejercicio

¿Qué direcciones IPv4 de las siguientes son correctas y cuáles erróneas?:

122.44.85.11 40.262.28.32 140.23.44 130.206.44.220

¿Qué direcciones IPv6 de las siguientes son correctas y cuáles erróneas?:

11FF:6BC8:34:978:A5F:FF4:9:11D 223A:889:FF811:9:34:FA2:BB4:46:45:D2

Simplifica las siguientes direcciones IPv6

0002:4A0:02:05:0021:FF4E:34:0001

AA4:0:0:0:0:0:54:FFE2

E23:0:0:0:25:0:0:2

Cuando se está conectado a Internet desde Windows o Linux, se puede abrir una ventana de MS DOS, consola o terminal y ejecutar el comando ***ping*** +DirIP para, además de saber si ese servidor está operativo y el tiempo de respuesta, averiguar su dirección IP.

Otro comando es nslookup + dominio: devuelve la dirección IP del servidor. Ej: nslookup www.google.es devuelve la IP de Google.

DOMINIOS PRINCIPALES

Los dominios de primer nivel o dominios principales, constan de dos letras que indican, por regla general, a qué país pertenece el ordenador. En la siguiente tabla pueden verse algunos ejemplos:

Dominio →	País	Dominio →	País
Ar	Argentina	at	Austria
Fr	Francia	be	Bélgica
Au	Australia	gr	Grecia
Bg	Bulgaria	in	India
Ca	Canadá	it	Italia
Ch	Suiza	ip	Japón
Cl	Chile	ki	Kiribati
De	Alemania	mx	México
Dk	Dinamarca	nl	Países Bajos
Es	España	se	Suecia
Fi	Finlandia HT	uk	Reino Unido

Algunos dominios principales.

Ejercicio

- ¿Cuál es la dirección IP del servidor Web de la Biblioteca Nacional?: www.bne.es
- ¿Es posible más de una dirección IP para un mismo dominio?
- ¿A qué países corresponderán los ordenadores con los siguientes nombres de dominio?: honduras.xlh.be, fisica.abc.ar, chirac.eli.fr

Otros dominios principales, utilizados fundamentalmente en Estados Unidos, son los que hacen referencia al tipo de organización. Así, por ejemplo, el dominio **.com** indica que se trata de una empresa comercial; el dominio **.edu** corresponde a una organización educativa, etc.

SERVIDORES DNS

Ya que un ordenador necesita la dirección IP para establecer contacto con otro ordenador, si se utiliza el nombre de dominio para hacer referencia a éste, debe existir un mecanismo que permita determinar cuál es la dirección IP correspondiente. Para resolver este problema se dispone de unos ordenadores, llamados servidores de nombres de dominio (DNS servers), cuya misión es **traducir los nombres de dominio a sus correspondientes direcciones IP**.

Todo ordenador conectado a Internet deberá estar configurado para acceder a uno de estos servidores.

3- WORLD WIDE WEB

WWW

Las siglas WWW, también conocidas como **W3** o **Web**, provienen de las palabras World Wide Web, algo que podría traducirse como trama o telaraña mundial; éste es el sistema más utilizado para

acceder a la información en Internet. Dicho sistema está formado por un conjunto de ordenadores conectados entre sí, denominados **servidores Web**, que presentan las siguientes características:

- Para visitar uno de estos servidores o **sitios Web** (*Web sites*) se debe Utilizar un programa **navegador**, como Netscape Navigator, Opera o Internet Explorer.
- Cuando se accede a un servidor Web, lo que aparece en pantalla es una **página Web** o **documento de hipertexto**.

Las páginas Web pueden pertenecer a una gran variedad de empresas, instituciones y particulares: universidades, centros de investigación, revistas y periódicos, ayuntamientos, organizaciones internacionales, agencias de turismo, museos, empresas comerciales... de todas ellas hay un gran número en distintos servidores Web.

DOCUMENTO DE HIPERTEXTO

Cada página Web o documento de hipertexto es una combinación de **texto, imágenes, elementos multimedia en general** y, lo más importante, **hiperenlaces** (también llamados **hipervínculos, vínculos o enlaces**).

Características de los hiperenlaces

- Se muestran en pantalla como palabras o frases destacadas en distinto color o subrayadas.
- Apuntan a documentos que pueden estar situados en el mismo ordenador o en otro de cualquier parte del mundo.
- Cuando se hace clic sobre uno de ellos, aparece en pantalla el documento al que hacía referencia.

SIGNIFICADO DE LOS TÉMINOS HTTP Y HTML

Estos acrónimos aparecerán frecuentemente al navegar por la Web.

El primero de ellos, **http**, proviene de ***H**yper**T**ext **T**ransfer **P**rotocol*, y es el protocolo de comunicación usado en WWW para transferir información y ficheros, por ejemplo, los documentos de hipertexto.

Cuando un navegador accede a la información disponible en un servidor WWW, utiliza este protocolo para comunicarse. El prefijo **http** suele aparecer en las **direcciones URL** para indicar que corresponden a servidores WWW.

Por otra parte, **html** es el acrónimo de ***H**yper**T**ext **M**arkup **L**anguage*, que es el lenguaje usado para escribir los documentos de hipertexto. El nombre de los ficheros que contienen documentos de hipertexto suele terminar en **.html** o **.htm**

DIRECCIÓN URL

La dirección URL, acrónimo de ***U**niform **R**esource **L**ocator*, es la forma de escribir las direcciones de los distintos servicios Internet.

La estructura de una dirección URL, en su forma más simple y frecuente, se compone de tres partes:

http://www.anayamultimedia.es/catalogo/index.htm

- La primera parte es el **método de acceso**, indica el tipo de servicio que se va a utilizar, por ejemplo http, ftp, file, etc.
- La segunda parte es la **dirección del ordenador** (dirección IP o nombre de dominio) al que se quiere acceder. El método de acceso debe estar separado de la dirección del *host* por los caracteres **://**
- La última parte es opcional y puede ser el nombre de un directorio, la ruta de acceso hasta un subdirectorio determinado, o el nombre de un fichero con su ruta de acceso completa.

WEB 2.0

La Web 2.0 es la representación de la evolución de las aplicaciones tradicionales hacia aplicaciones web enfocadas al usuario final. **El Web 2.0 es una actitud y no una tecnología**.

La Web 2.0 es la transición que se ha dado de aplicaciones tradicionales hacia aplicaciones que funcionan a través del web enfocadas al usuario final. Se trata de aplicaciones que generen colaboración y de servicios que reemplacen las aplicaciones de escritorio.

Y es que cuando el web inició, nos encontrábamos en un entorno estático, con páginas en HTML que sufrían pocas actualizaciones y no tenían interacción con el usuario.

Entender la evolución que ha llegado con la Web 2.0 puede realizarse con ejemplos, con proyectos. Podemos comparar servicios web que marcan claramente la evolución hacia el Web 2.0 con una nueva forma de hacer las cosas:

Web 1.0	→ ***Web 2.0***
Doubleclick	→ Google AdSense (Servicios Publicidad)
Ofoto	→ Flickr (Comunidades fotográficas)
Akamai	→ BitTorrent (Distribución de contenidos)
mp3.com	→ Goear o Spotify (Compartir música en la nube)
Britannica Online	→ Wikipedia (Enciclopedias)
Sitios personales	→ Blogs (Páginas personales)
Especulación con dominios	→ Optimización en motores de búsqueda SEO

4- EL NAVEGADOR WEB

Un navegador o navegador web (del inglés, *web browser*) es un programa que permite ver la información que contiene una página web (ya se encuentre ésta alojada en un servidor dentro de la World Wide Web o en un servidor local).

El navegador *interpreta* el código, HTML generalmente, en el que está escrita la página web y lo presenta en pantalla permitiendo al usuario interactuar con su contenido y navegar hacia otros lugares de la red mediante enlaces o hipervínculos.

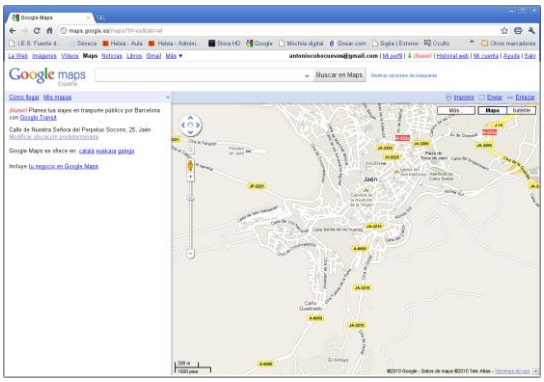
Las páginas Web, que son documentos (archivos) transmitidos por la red o almacenados localmente, poseen hipervínculos que enlazan una porción de texto o una imagen a otro documento, normalmente relacionado con el texto o la imagen.

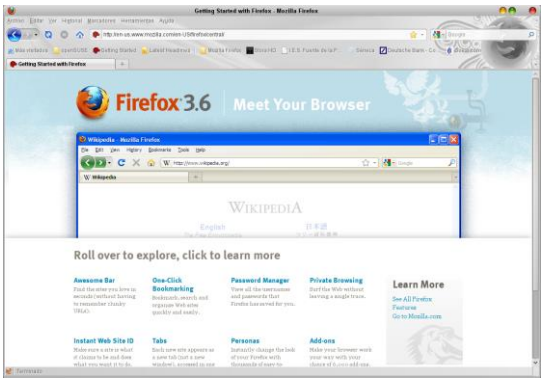
El seguimiento de enlaces de una página a otra, ubicada en cualquier computadora conectada a la Internet, se llama **navegación**, de donde se origina el nombre **navegador**.

La comunicación entre el servidor web y el navegador se realiza mediante el **protocolo HTTP**, aunque la mayoría de los navegadores soportan otros protocolos como **FTP**, **Gopher**, y **HTTPS** (*una versión cifrada de HTTP basada en Secure Socket Layer o Capa de Conexión Segura (SSL)*).

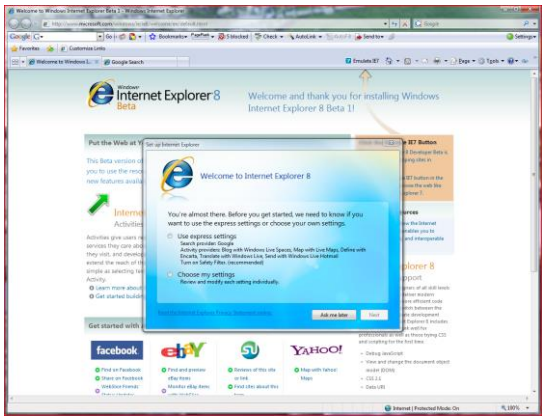
La función principal del navegador es descargar documentos HTML y mostrarlos en pantalla. En la actualidad, no solamente descargan este tipo de documentos sino que muestran con el documento sus imágenes, sonidos e incluso vídeos *streaming* en diferentes formatos y protocolos. Además, permiten almacenar la información en el disco o crear marcadores (*bookmarks*) de las páginas más visitadas.

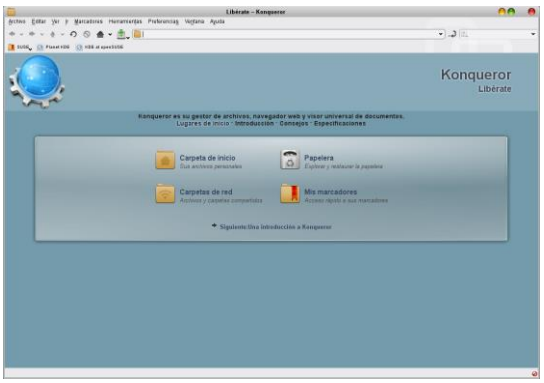
Los navegadores más usuales son: Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Konqueror….





Google Chrome





Microsoft Internet Explorer

Navegadores más usuales

NOTAS:

- Si se desea cambiar el tamaño de los caracteres de la pantalla, se puede abrir el menú **Ver**, seleccionar la opción **Fuentes** o **Tamaño** para cambiar el tamaño del texto de la Web. Además podemos usar el atajo de teclado "Ctrl +" y "Ctrl –" para aumentar o disminuir respectivamente los tamaños.
- Los formatos de imágenes más utilizados en Internet son JPG, GIF y PNG, porque son los que menos espacio ocupan (*excepto PNG que se usa por que tiene calidad fotográfica y admite transparencias*).
- **Teclas rápidas (*atajos de teclado*):**

  <F5> → Actualiza la página.

<Esc> → Interrumpe la carga de la página.

<Control> + <A> → Abre el cuadro de diálogo Abrir.

<F11> → Activa el modo Pantalla completa.

<Control> + <P> → Imprime la página.

5- BÚSQUEDA DE INFORMACIÓN

En Octubre de 2010 la empresa ***netcraft***, dedicada a ofrecer servicios de Internet, realizó un estudio en el que se obtuvo la cifra de **232.839.963 *sitios Web.*** Viendo estas cifras es fácil comprender que se hace necesaria una buena herramienta de búsqueda de información en la red.

BUSCADORES

Para buscar información en internet hay sistemas avanzados de búsqueda, a los que se accede a través de la World Wide Web: son los llamados buscadores.

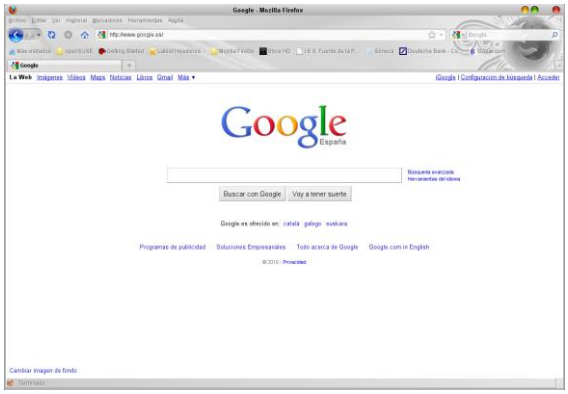
Se pueden clasificar en dos tipos:

- **Índices temáticos:** Son sistemas de búsqueda por temas o categorías jerarquizados (aunque también suelen incluir sistemas de búsqueda por palabras clave). Se trata de bases de datos de direcciones Web elaboradas "*manualmente*", es decir, hay personas que se encargan de asignar cada página web a una categoría o tema determinado.
- **Motores de búsqueda:** Son sistemas de búsqueda por palabras clave. Son bases de datos que incorporan automáticamente páginas web mediante "*robots*" de búsqueda en la red.

Clases de buscadores

Buscadores jerárquicos (Arañas o Spiders). Motor de búsqueda.

- Recorren las páginas recopilando información sobre los contenidos de las páginas. Cuando se busca una información en los motores, ellos consultan su base de datos y presentan resultados clasificados por su relevancia. De las webs, los buscadores pueden almacenar desde la página de entrada, a todas las páginas que residan en el servidor.
- Si se busca una palabra, por ejemplo, "ordenadores". En los resultados que ofrecerá el motor de búsqueda, aparecerán páginas que contengan esta palabra en alguna parte de su texto.



- Si consideran que un sitio web es importante para el usuario, tienden a registrarlas todas. Si no la consideran importante, sólo almacenan una o más páginas.
- Cada cierto tiempo, los motores revisan los sitios, para actualizar los contenidos de su base de datos.
- Los buscadores jerárquicos tienen una colección de programas simples y potentes con diferentes cometidos. Se suelen dividir en tres

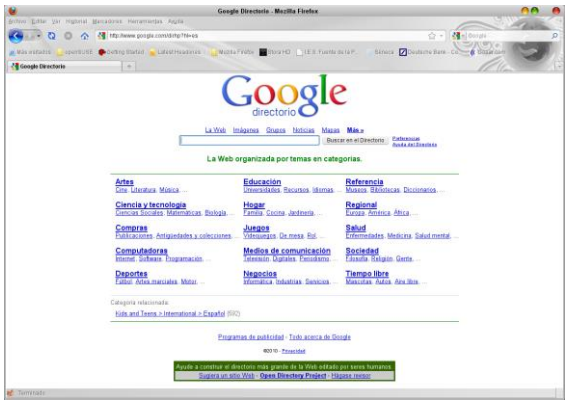
partes. Los programas que exploran la red -*arañas (spiders)*-, los que construyen la base de datos y los que utiliza el usuario (el programa que explota la base de datos).

- Si se paga, se puede aparecer en las primeras páginas de resultados, aunque los principales buscadores delimitan estos resultados e indican al usuario que se trata de resultados esponsorizados o patrocinados. Hasta el momento, aparentemente, esta forma de publicidad, es indicada explícitamente. Los buscadores jerárquicos se han visto obligados a este tipo de publicidad para poder seguir ofreciendo a los usuarios el servicio de forma gratuita.

Ejemplos de arañas: **Google, Bing, Hotbot.**

Directorios

Una tecnología barata, ampliamente utilizada por gran cantidad de scripts en el mercado. No se requieren muchos recursos de informática. En cambio, se requiere más soporte humano y mantenimiento.



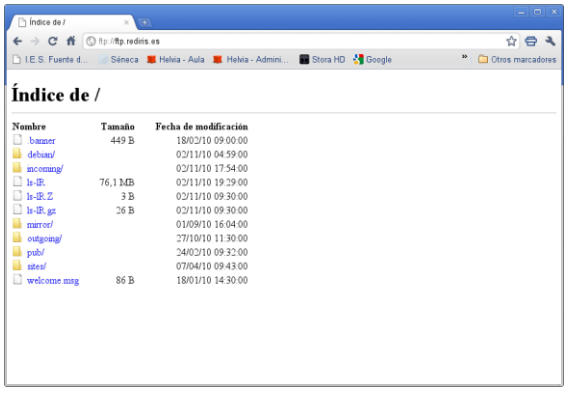
- Los algoritmos son mucho más sencillos, presentando la información sobre los sitios registrados como una colección de directorios. No recorren los sitios web ni almacenan sus contenidos. Solo registran algunos de los datos de nuestra página, como el título y la descripción que se introduzcan al momento de registrar el sitio en el directorio.
- Los resultados de la búsqueda, estarán determinados por la información que se haya suministrado al directorio cuando se registra el sitio. En cambio, a diferencia de los motores, son revisadas por operadores humanos, y clasificadas según categorías, de forma que es más fácil encontrar páginas del tema de nuestro interés.
- Más que buscar información sobre contenidos de la página, los resultados serán presentados haciendo referencia a los contenidos y temática del sitio.
- Su tecnología es muy barata y sencilla.

Ejemplos de directorios: Antiguos directorios, Open Directory Project, Yahoo!, Terra (antiguo Olé). Ahora, ambos utilizan tecnología de búsqueda jerárquica, y Yahoo! conserva su directorio. Buscar Portal, es un directorio, y la mayoría de motores hispanos son directorios.

6- TRANSFERENCIA DE FICHEROS (ftp)

¿QUÉ ES FTP?

FTP, acrónimo de *File Tansfer Protocol*, es el servicio de Internet mediante el cual se transfieren ficheros entre dos ordenadores. Estos ficheros pueden ser documentos, imágenes, sonidos, programas, etc.

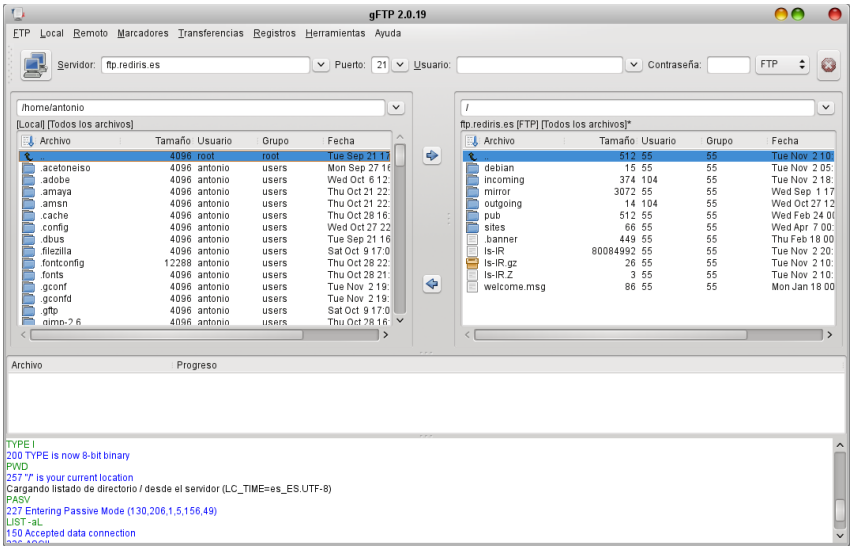


Sesión ftp con Google Chrome

Existen multitud de servidores en Internet, **servidores FTP**, que están repletos de archivos. Algunos de ellos son públicos, por lo que cualquier usuario puede acceder a ellos, mientras que otros son privados y exigen disponer de autorización para poder realizar la transferencia de fiche-

ros.

La transferencia se puede realizar bien utilizando el navegador, bien mediante un programa especial, que se denomina **cliente FTP**, como **WS_FTP, gftp**.



Acceso a ftp mediante un programa específico (gftp).

SESIÓN FTP CON UN NAVEGADOR WEB

Los navegadores Web son capaces de utilizar el protocolo FTP, y acceder de este modo a cualquier servidor de ficheros.

Para abrir una conexión FTP en un navegador se debe:

- Abrir el navegador.
- Escribir la dirección URL del servidor FTP que incluirá, como modo de acceso, el prefijo **ftp**, como en **ftp://ftp.rediris.es**

Ejercicio

Copiar a nuestro equipo el archivo ***README*** de la siguiente ruta ftp:

ftp.rediris.es → pub → mozilla .org → firefox → releases

7- CORREO ELECTRÓNICO

QUÉ ES EL CORREO ELECTRÓNICO

El correo electrónico (**e-mail**) es una de las herramientas más utilizadas de Internet. Las ventajas de este servicio son innumerables, constituyendo, hoy en día, uno de los mejores sistemas de comunicación.

Si se utiliza el correo electrónico, es posible enviar y recibir mensajes que contengan texto, programas, ficheros multimedia y todo tipo de información que pueda ser digitalizada.

PROGRAMAS DE CORREO

Para poder hacer uso de este servicio podemos acceder a nuestro correo a través de una ***interfaz Web*** (como es habitual hoy en día con *gmail*, *hotmail*, *yahoo*, etc.), o podemos recurrir a un **programa cliente** que permita gestionar los mensajes recibos y enviados en modo local. Algunos de ellos son: Out1ook Express, Kmail (*KDE*), Evolution (*Gnome*), Thunderbird (Mozilla), ...

QUÉ ES LA DIRECCIÓN DE CORREO ELECTRÓNICO

Para enviar un mensaje de correo es necesario conocer la dirección electrónica del destinatario. Una dirección de correo suele tener el siguiente aspecto:

* Nombre o clave de usuario — Nombre de dominio del servidor de correo

mlopez@jupiter.es

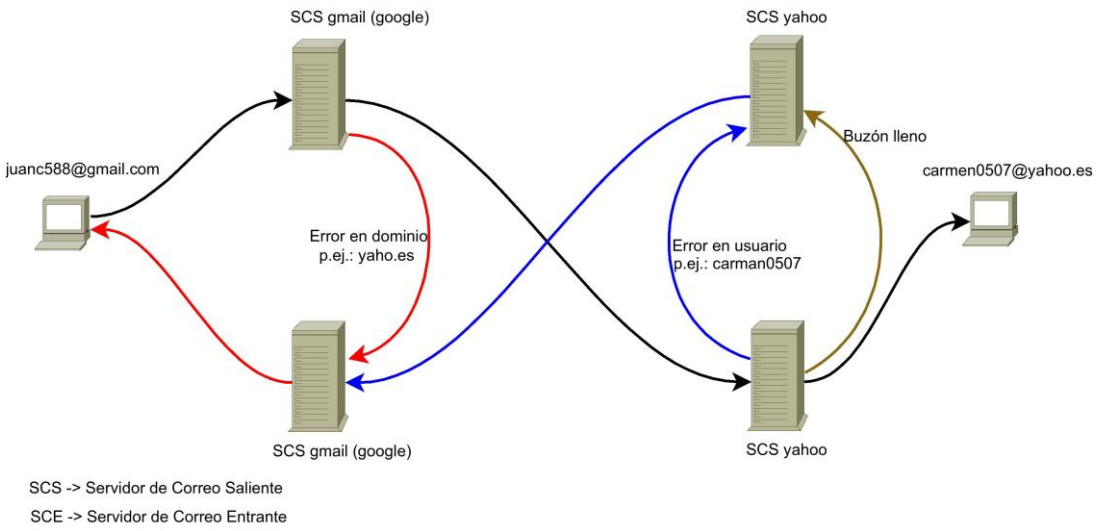
Por ejemplo: **jgómez360@gmail.com**, **pperez2@yahoo.es,** etc.

ESTRUCTURA DE UN MENSAJE

Un mensaje de correo consta de las siguientes partes:

- **Cabecera**. Es una parte importante del mensaje, pues informa de a quién se envía, del asunto del mensaje y de las personas a las que se ha enviado una copia de él.
- **Cuerpo del mensaje**. Éste es el mensaje propiamente dicho; en él se debe escribir el texto y, como se verá más adelante, se podrán incluir los ficheros que se deseen enviar.
- **Firma**: Es un texto opcional, que suele incluir datos de identificación del usuario que envía el mensaje.
- **Firma**. mensaje.

Ejemplo de funcionamiento del correo electrónico



8. SEGURIDAD EN REDES CABLEADAS E INALÁMBRICAS

PRINCIPIOS DE SEGURIDAD

Para poder garantizar la seguridad de la información de una empresa hace falta que se cumplan los principios de Confidencialidad, Integridad y Disponibilidad de la información que almacena y gestiona (también conocidos como "triada CID"):

- **Confidencialidad**: es la propiedad que impide que la información sea divulgada a personas, entidades o sistemas no autorizados, de manera que sólo puede acceder a ella aquellas personas que cuenten con la debida autorización y de forma controlada.

- **Integridad**: es la propiedad que busca proteger la exactitud de la información, evitar que sufra modificaciones no autorizadas.

- **Disponibilidad**: garantiza que la información sea accesible y usable bajo demanda de un usuario autorizado, que esté disponible en todo momento, evitando interrupciones del servicio por cortes de electricidad, fallos de hardware, etc

SEGURIDAD FÍSICA Y LÓGICA

SEGURIDAD FÍSICA: todos aquellos mecanismos -generalmente de prevención y detección- destinados a proteger físicamente cualquier recurso hardware del sistema; equipos, cableado, servidores…Son medidas frente a intrusos (control de acceso: tarjetas, biometría, videocámaras, vigilante jurado…), desastres naturales como incendios (extntores), inundaciones, apagones…(sistemas alimentación ininterrumpida) o acondicionamiento, temperaturas extremas (refrigeración), copias de seguridad (backup).

SEGURIDAD LÓGICA: consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información, que sólo se permita acceder a ellos a las personas autorizadas para hacerlo. La seguridad lógica se basa, en gran medida, en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de los accesos (contraseñas). También son medidas de seguridad lógica los antivirus, firewall, actualización del sistema y aplicaciones.

SEGURIDAD EN INTERNET: RIESGOS Y AMENAZAS.

Las amenazas externas son las amenazas principales a las que se enfrenta un sistema de seguridad de redes. En este caso, las más habituales son los ataques hacker o las infecciones basadas en distintos tipos de virus, aunque hay muchas otras. Cuando se sufre uno de estos ataques, se debe a que el sistema de seguridad que está establecido en una empresa no cumple con los requisitos adecuados o simplemente se ha vuelto más vulnerable. En la mayor parte de los casos es habitual hacer un buen trabajo, pero hay que entender que los ciberdelincuentes siempre están desarrollando nuevas formas de adentrarse en los sistemas de las organizaciones. Las principales amenazas son:

- **Malware**: todo tipo de software intrusivo que afecta de manera negativa a la víctima (virus, spyware...)
- **Ataques a sitios web** y a aplicaciones web. ...
- **Ataque de denegación de servicio DDoS** (*Distributed Denial of Service):* saturar al servidor de peticiones entrantes. Un ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un servidor, con el fin de bloquear el servicio para el que está destinado. Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso

puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

- **Botnets**: redes zombi. Una botnet, o mejor dicho, una red de bots (también conocida como ejército zombi) es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición de un hacker. Al tomar el control de cientos o miles de equipos, las botnets se suelen utilizar para enviar spam o virus, para robar información personal o para realizar ataques de denegación de servicio distribuido (DDoS). A día de hoy, se consideran una de las mayores amenazas en Internet.
- **Phishing**: uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.
- **Spam**: publicidad no deseada por correo electrónico, que te llenan la bandeja del correo y te hacen perder tiempo.
- **Ransomware**: cuando alguien es víctima de un ataque de ransomware, toda la información de su computadora o dispositivo queda 'atrapada' o cifrada, y la víctima tiene que pagar una suma de dinero al hacker para recuperarla.

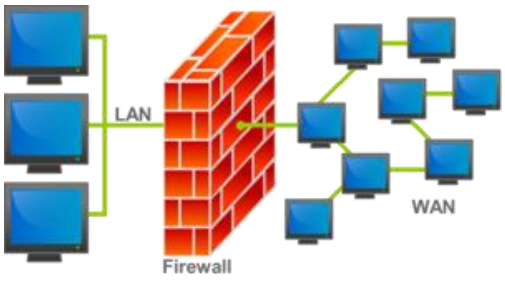
SEGURIDAD EN REDES CABLEADAS

Algunos mecanismos de seguridad en redes cableadas son:

Cortafuegos (Firewall)

Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuegos a una tercera red, llamada *zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.



Criptografía

La criptografía se encarga del estudio de los algoritmos, protocolos (protocolos criptográficos), y sistemas que se utilizan para cifrar (enmascarar) la información y así protegerla y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
Para ello los criptógrafos investigan, desarrollan y aprovechan técnicas matemáticas que les sirven como herramientas para conseguir sus objetivos. Por ejemplo, aplicando funciones matemáticas a las secuencias de bits, se consigue encriptar mensajes. Ejemplos de métodos criptográficos son: la firma digital, mensajes de correo encriptados, protocolos seguros como TransportLayer Security (TLS), HTTPS, WPA2…

SEGURIDAD EN REDES INALÁMBRICAS

Las redes inalámbricas, al funcionar con ondas electromagnéticas, tienen el inconveniente de que cualquier intruso con un dispositivo móvil puede intentar acceder a la red. Debemos por tanto configurarla de forma que sólo puedan acceder a ella los usuarios acreditados. A continuación figuran algunas opciones de seguridad de redes inalámbricas:

Acceso protegido WiFi (WPA y WPA2)

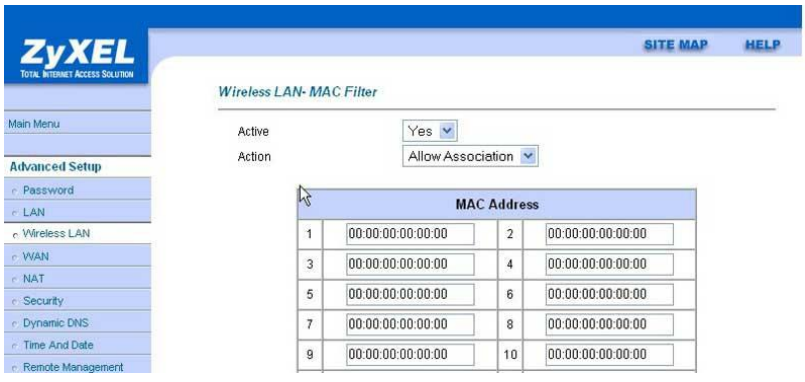
WPA, Wi-Fi Protected Access, en español «*Acceso Wi-Fi protegido*», es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo, *Wired Equivalent Privacy* (WEP). **WPA** adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante una **clave** precompartida, que de un modo similar al WEP, **requiere introducir la misma clave en todos los equipos de la red.**

WPA2, creado para corregir las deficiencias del sistema previo (WPA), utiliza el algoritmo de cifrado AES (Advanced Encryption Standard), que es más seguro que el de WPA.

Filtrado MAC

Una **dirección MAC** es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particulalar. Una dirección MAC consiste en seis grupos de dos caracteres, cada uno de ellos separadoS por dos puntos. 00:1B:44:11:3A:B7 es un ejemplo de dirección MAC.

El filtrado MAC consiste en dar instrucciones al router para que permita conectarse a los dispositivos cuyo MAC aparezca en un listado. Cualquier otro terminal cuyo identificador de red no se encuentre en esta lista no podrá acceder. Esto tiene sus desventajas, ya que limita radicalmente el acceso hasta el punto que si un amigo visita nuestra casa y quiere conectarse al WiFi habrá que **modificar la lista introduciendo el MAC de su dispositivo** para que pueda hacerlo.



Otra manera de usar el filtrado MAC es en forma de lista negra, **escribiendo los identificadores de aquellos dispositivos que no queremos que se conecten a la red**. Parece algo rebuscado pero lo cierto es que en algunas ocasiones puede resultar útil. Si vemos que el equipo del vecino se está conectando al WiFi cuando no debería es posible evitarlo obteniendo su identificador (con uno de los programas que existen para vigilar nuestra red WiFi, como Wireless Network Watcher) y vetándolo.

Para activar el filtrado MAC hay que entrar en la configuración del router desde un navegador, pinchar en la sección "*MAC Filter"* y a continuación añadir los identificadores a los que queramos dar o quitar permiso.

ENLACES EN LA WEB:

- www.incibe.es
- www.osi.es
- www.**red**.**es**/
- www.**internet**society.org
- http://www.iana.org/
- http://www.rediris.es/
- ftp://ftp.rediris.es/
- http://www.adslzone.com
- http://www.internautas.org
- http://www.internetsociety.org/es/breve-historia-de-internet
- https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#Redes_cableadas
- http://platea.pntic.mec.es/jdelucas/redes.htm
- http://www2.infotelecom.es/~ecampins/Departament/Internet/La%20red%20Internet.htm
- http://www.ecured.cu/index.php/Red_de_computadoras
- https://lordratita.wordpress.com/2012/07/16/unidad-9-protocolos-criptograficos-2/