Redes inalámbricas. Wi-fi, el futuro de la comunicación

Autor: Ander Otxoa Gilo

[Ver curso online]

Presentación del curso

Hasta este momento para conectarnos a Internet, a nuestro correo o a cualquier otro tipo de información necesitábamos estar conectados a una red. Estas redes eran físicas, se tenía que estar siempre buscando una toma de red y un cable para conectar nuestro ordenador con esta red.

La necesidad de estar siempre conectados a Internet y sobre todo la movilidad, están haciendo que las redes inalámbricas vayan apareciendo poco a poco en empresas, casas, aeropuertos, hoteles

Estas redes permiten que una persona pueda moverse, si necesidad de una conexión física para estar conectados.

En este curso queremos explicar que es, cómo funciona, la seguridad y muchos aspectos técnicos sobre esta forma de realizar una conexión en red.

Visita más cursos como este en mailxmail:
[http://www.mailxmail.com/cursos-informatica]
[http://www.mailxmail.com/cursos-internet]

¡Tu opinión cuenta! Lee todas las opiniones de este curso y déjanos la tuya:
[http://www.mailxmail.com/curso-redes-inalambricas-wi-fi-futuro-comunicacion/opiniones]

Cursos similares

Cursos	Valoración	Alumnos	Vídeo
Cableado de Red de datos y telefonía Curso orientado a las personas que deben mantener la red de datos de una red de area local (LAN), atendiendo a las tareas más cotidianas.Incluimos la red de voz (... [08/08/06]		8.887	
Internet. Tu negocio Intenet fue un negocio que en algún momento parecía una idea "descabellada". Ahora el internet es una herramienta de uso indispensable en las e... [03/02/09]		1.000	
Impacto de las nuevas tecnologías en la empresa Hablar de nuevas tecnologías es hablar de un amplio abanico de técnicas, herramientas, ámbitos de investigación y desarrollo que abarcan desde el estudio de la vida anima... [29/04/05]		2.091	
Twitter... para quien no usa Twitter (1/2) Twitter... para quien no usa Twitter, con este curso del autor Juan Diego Polo, especialista en el mundo del Internet[19/01/10]		1.080	
Curso de E-Business En la actualidad esta surgiendo una nueva forma de hacer negocios. Esta se basa en la nueva tecnología conocida por muchos como Internet, aunque surgió antes que Internet... [12/01/06]		2.298	

1. Introducción a las redes inalámbricas

[http://www.mailxmail.com/...mbricas-wi-fi-futuro-comunicacion/introduccion-redes-inalambricas]

Desde hace relativamente poco tiempo, se está viviendo lo que puede significar un revolución en el uso de las tecnologías de la información tal y como lo conocemos. Esta revolución puede llegar a tener una importancia similar a la que tuvo la adopción de Internet por el gran público.

De una forma callada, las **redes inalámbricas** o **Wireless Networks** (WN), se están introduciendo en el mercado de consumo gracias a unos precios populares y a un conjunto de entusiastas, mayoritariamente particulares, que han visto las enormes posibilidades de esta tecnología.

Las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, pues ésta estará al alcance de todos a través de Internet en cualquier lugar (en el que haya cobertura).

En un futuro cercano se reunificarán todo aquellos dispositivos con los que hoy contamos para dar paso a unos nuevos que perfectamente podrían llamarse Terminales Internet en los cuales estarían reunidas las funciones de teléfono móvil, agenda, terminal de vídeo, reproductor multimedia, ordenador portátil y un largo etcétera.

Se podría dar lugar a una Internet paralela y gratuita la cual estaría basada en las redes que altruistamente cada uno de nosotros pondríamos a disposición de los demás al incorporarnos a las mismas como destino y origen de la información.

En un futuro también cercano la conjugación de las redes Mesh, con las redes inalámbricas y las redes Grid podría llevar a cabo al nacimiento de nuevas formas de computación que permitan realizar cálculos inimaginables hasta ahora debido a las necesidades HW de las que eran objeto.

En las grandes ciudades por fin se podría llevar a cabo un control definitivo del tráfico con el fin de evitar atascos, limitando la velocidad máxima y/o indicando rutas alternativas en tiempo real.

Las tecnologías que son necesarias para llevar a cabo estos sistemas hoy existen desde ayer, su precio es mínimo o al menos muy asequible y su existencia mañana sólo depende de las estrategias comerciales de las empresas que las poseen.

Antes de echar la imaginación a volar es necesario tener un cierto conocimiento sobre la tecnología que va a ser la base de estas aplicaciones, sobre las redes inalámbricas. Vamos entonces a intentar describir las mismas.

2. Clasificación de las redes inalámbricas - Redes inalámbricas personales

[http://www.mailxmail.com/...on/clasificacion-redes-inalambricas-redes-inalambricas-personales]

Lo primero que tenemos que hacer antes que nada es situarnos dentro del mundo inalámbrico. Para ello vamos a hacer una primera clasificación que nos centre ante las diferentes variantes que podemos encontrarnos:

- Redes inalámbricas personales
- Redes inalámbricas 802.11
- Redes inalámbricas de consumo

Redes inalámbricas personales

Dentro del ámbito de estas redes podemos integrar a dos principales actores:

a- En primer lugar y ya conocido por bastantes usuarios están las redes que se usan actualmente mediante el intercambio de información mediante **infrarrojos**. Estas redes son muy limitadas dado su corto alcance, necesidad de "visión sin obstáculos" entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.

b- En segundo lugar el **Bluetooth**, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún que otro ordenador portátil. Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha ido plagada de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes que ha imposibilitado su rápida adopción. Opera dentro de la banda de los 2'4 Ghz.

Para más información sobre el mismo vea http://www.bluetooth.com.

3. Clasificación de las redes inalámbricas - De consumo v. 802.11

[http://www.mailxmail.com/...uturo-comunicacion/clasificacion-redes-inalambricas-consumo-80211]

Redes inalámbricas de consumo

a- **Redes CDMA** (estándar de telefonía móvil estadounidense) y **GSM** (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes. Vea http://www.gsmworld.com.

b- **802.16** son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (**MAN**) en la banda de entre los 2 y los 11 Ghz. Estas redes no entran dentro del ámbito del presente documento.

4. Redes inalámbricas 802.11 - Primera variante

[http://www.mailxmail.com/...-fi-futuro-comunicacion/redes-inalambricas-80211-primera-variante]

Las **redes inalámbricas** o **WN** básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del IEEE (Organismo de estandarización internacional).

Como suele pasar siempre que un estándar aparece y los grandes fabricantes se interesan por él, aparecen diferentes aproximaciones al mismo lo que genera una incipiente confusión.

Nos encontramos ante tres principales variantes:

1- **802.11a**: fue la primera aproximación a las **WN** y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por Punto de Acceso.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares **802.11b** y **g**, la no incorporación a la misma de **QoS** (posibilidades de aseguro de Calidad de Servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia online), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la **HyperLAN2** (Ver http://www.hiperlan2.com) y la parcial disponibilidad de la misma en Japón.

El hecho de no estar disponible en Europa prácticamente la descarta de nuestras posibilidades de elección para instalaciones en este continente.

5. Redes inalámbricas 802.11 - Segunda y Tercera variante

[http://www.mailxmail.com/...ro-comunicacion/redes-inalambricas-80211-segunda-tercera-variante]

2- **802.11b**: es la segunda aproximación de las **WN**. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE. Opera dentro de la frecuencia de los 2'4 Ghz. Inicialmente se soportan hasta 32 usuarios por PA.

Adolece de varios de los inconvenientes que tiene el **802.11a** como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2'4 Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos Bluetooth..., lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por el IEEE.

3- **802.11g**: Es la tercera aproximación a las **WN**, y se basa en la compatibilidad con los dispositivos **802.11b** y en el ofrecer unas velocidades de hasta 54 Mbps. A 05/03/2003 se encuentra en estado de borrador en el IEEE, se prevee que se estandarice para mediados de 2003. Funciona dentro de la frecuencia de 2'4 Ghz.

Dispone de los mismos inconvenientes que el **802.11b** además de los que pueden aparecer por la aún no estandarización del mismo por parte del IEEE (puede haber incompatibilidades con dispositivos de diferentes fabricantes).

Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

6. Dispositivos Wireless

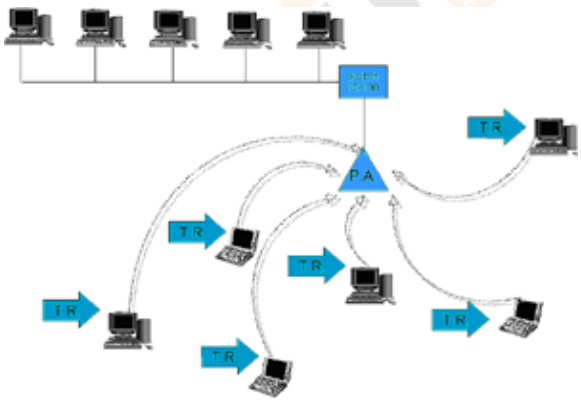
[http://www.mailxmail.com/...edes-inalambricas-wi-fi-futuro-comunicacion/dispositivos-wireless]

Sea cual sea el estándar que elijamos vamos a disponer principalmente de dos tipos de dispositivos:

a- **Dispositivos "Tarjetas de red", o TR**, que serán los que tengamos integrados en nuestro ordenador, o bien conectados mediante un conector **PCMCIA** ó **USB** si estamos en un portátil o en un slot PCI si estamos en un ordenador de sobremesa. SUBSTITUYEN a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

b- **Dispositivos "Puntos de Acceso", ó PA**, los cuales serán los encargados de recibir la información de los diferentes **TR** de los que conste la red bien para su centralización bien para su encaminamiento. COMPLEMENTAN a los Hubs, Switches o Routers, si bien los PAs pueden substituir a los últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

Para una representación gráfica de una red inalámbrica vea el siguiente gráfico.



7. Funcionamiento de los dispositivos

[http://www.mailxmail.com/...lambricas-wi-fi-futuro-comunicacion/funcionamiento-dispositivos-1]

En este documento vamos a referirnos principalmente al **802.11g**, por ser el probable vencedor de la "guerra de estándares" abierta hoy en día, aunque lo explicado será fácilmente extrapolable a los demás teniendo en cuenta las características propias de cada uno.

Todos los estándares aseguran su funcionamiento mediante la utilización de dos factores, cuando estamos conectados a una red mediante un cable, sea del tipo que sea, disponemos de una velocidad fija y constante. Sin embargo cuando estamos hablando de redes inalámbricas aparece un factor añadido que puede afectar a la velocidad de transmisión, que es la distancia entre los interlocutores.

Así pues cuando un **TR** se conecta a un PA se ve afectado principalmente por los siguientes parámetros:

- Velocidad máxima del **PA** (normalmente en 802.11g será de 54Mbps)

- Distancia al **PA** (a mayor distancia menor velocidad)

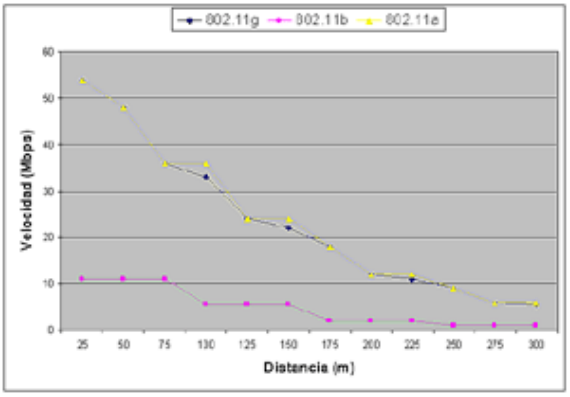
- Elementos intermedios entre el **TR** y el **PA** (las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el PA y el TR modifican la velocidad de transmisión a la baja)

- Saturación del espectro e interferencias (cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias.)

Normalmente los fabricantes de PAs presentan un alcance teórico de los mismos que suele andar alrededor de los 300 metros. Esto obviamente es sólo alcanzable en condiciones de laboratorio, pues realmente en condiciones objetivas el rango de alcance de una conexión varía (y siempre a menos) por la infinidad de condiciones que le afectan.

Cuando ponemos un TR cerca de un PA disponemos de la velocidad máxima teórica del PA, 54 Mbps por ejemplo, y conforme nos vamos alejando del PA, tanto él mismo como el TR van disminuyendo la velocidad de la transmisión/recepción para acomodarse a las condiciones puntuales del momento y la distancia.

Así pues, se podría decir que en condiciones "de laboratorio" y a modo de ejemplo teórico, la transmisión entre dispositivos 802.11 podría ser como sigue:


802.11g
802.11b
802.11a
Velocidad (Mbps)
60
50
40
30
20
10
0
25
50
75
100
125
150
175
200
225
250
275
300
Distancia (m)

8. Funcionamiento de los dispositivos II

[http://www.mailxmail.com/...lambricas-wi-fi-futuro-comunicacion/funcionamiento-dispositivos-2]

Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de **TX/RX** (transmisión y recepción) de los dispositivos wireless.

Dentro de los **PAs** (actualmente ya se puede comenzar a aplicar también a los **TRs**) se puede modificar enormemente la capacidad de **TX/RX** gracias al uso de antenas especiales. Estas antenas se pueden dividir en: direccionales y omnidireccionales.

Las **antenas Direccionales** "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

Las antenas **Omnidireccionales** "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

Muchos particulares se han construido sus propias "antenas caseras" con diferentes resultados. Es bueno darse un paseo por el Google de vez en cuando para ver qué se va inventando. A modo de ejemplo, ciertos usuarios han descubierto que usando el envase cilíndrico de cierta marca de patatas fritas como antena direccional se puede emitir y recibir mucho mejor.

9. Velocidad vs Modulación

[http://www.mailxmail.com/...-inalambricas-wi-fi-futuro-comunicacion/velocidad-vs-modulacion-1]

Cuando transmitimos información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas. Estas tramas son básicamente secuencias de bits. Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que verdaderamente se quieren transmitir.

La cabecera es necesaria por razones de gestión de los datos que se envían. Dependiendo de la forma en la que se module la cabecera (o preámbulo), podemos encontrarnos con diferentes tipos de tramas, como son:

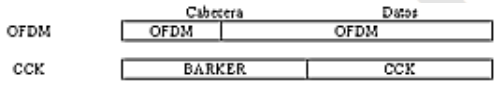
- **Barker**. (RTS / CTS)

?- **CCK**. Complementary Code Keying

?- **PBCC**. Packet Binary Convolutional Coding

?- **OFDM**. Orthogonal Frequency-Division Multiplexing

Una representación gráfica de las tramas más importantes:



Como podemos ver la cabecera en el caso de la codificación **OFDM** es más pequeña. A menor tamaño de cabecera menor "overhead" en la transmisión, es decir, menor tráfico de bits de gestión luego mayor "sitio" para mandar bits de datos. Lo que repercutirá positivamente en el rendimiento de la red.

10. Velocidad vs Modulación (II)

[http://www.mailxmail.com/...-inalambricas-wi-fi-futuro-comunicacion/velocidad-vs-modulacion-2]

Ya a primera vista podemos ver que el estándar **802.11g** es una unión de los estándares **802.11** "**a**" y "**b**". Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que "a" opera en la banda de los 5 Ghz, mientras que los otros dos operan en la del los 2'4 Ghz.

		802.11a		802.11b		802.11g	
Velocidad nominal	Portadora	Obligatorio	Opcional	Obligatorio	Opcional	Obligatorio	Opcional
1	única			Barker		Barker	
2	única			Barker		Barker	
5.5	única			CCK	PBCC	CCK	PBCC
6	múltiple	OFDM				OFDM	CCK-OFDM
9	múltiple		OFDM				OFDM, CCK-OFDM
11	única			CCK	PBCC	CCK	PBCC
12	múltiple	OFDM				OFDM	CCK-OFDM
18	múltiple		OFDM				OFDM, CCK-OFDM
22	única						
24	múltiple	OFDM				OFDM	CCK-OFDM
33	única						
36	múltiple		OFDM				OFDM, CCK-OFDM
48	múltiple		OFDM				OFDM, CCK-OFDM
54	múltiple		OFDM				OFDM, CCK-OFDM

Cuando tenemos una red inalámbrica en la que todos los dispositivos son tipo "a" o todos de tipo "b" no hay problemas en las comunicaciones. Cada AP tipo "a" tendrá sólo TRs tipo "a" y los APs tipo "b" tendrán sólo TRs tipo "b". Se seleccionará la mejor modulación y se transmitirá. Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible.

En el caso de dispositivos AP 802.11g normalmente estaremos usando la modulación OFDM, modulación que es la óptima para este estándar.

Si por un casual un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar "b", cosa que es capaz de hacer. Sin embargo el dispositivo "b" no puede escuchar las transmisiones de los otros dipositivos "g" que hablan con su "partner" pues éstos usan una modulación que él no es capaz de entender. Si un dispositivo "b" comenzase a hablar a la vez que un dispositivo "g" se producirían colisiones que impedirían la transmisión, no por que interfieran ya que usan diferente modulación sino porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez.

Para evitar las colisiones, los equipos "b" usan la modulación **Barker** con **TRS/CTS** (Request To Send / Clear To Send), que básicamente significa que deben pedir permiso al AP para transmitir.

11. Topología y Modos de funcionamiento de los dispositivos

[http://www.mailxmail.com/...i-futuro-comunicacion/topologia-modos-funcionamiento-dispositivos]

Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos **WiFi**. Con topología nos referimos a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

En el mundo Wireless existen dos topologías básicas:

- **Topología Ad-Hoc**. Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red **Peer to Peer** o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si.

- **Topología Infraestructura**, en el cual existe un nodo central (Punto de Acceso WiFi) que sirve de enlace para todos los demás (Tarjetas de Red Wifi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP.

Un caso especial de topología de redes inalámbricas es el caso de las redes Mesh, que se verá más adelante.

Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

- **Modo Managed**, es el modo en el que el TR se conecta al AP para que éste último le sirva de "concentrador". El TR sólo se comunica con el AP.

- **Modo Master**. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra vía firmware o vía SW. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de linux llamada LINUXAP - OPENAP.

Esta afirmación se ve confirmada al descubrir que muchos APs en realidad lo que tienen en su interior es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como TR.

12. Mesh Networks

[http://www.mailxmail.com/...curso-redes-inalambricas-wi-fi-futuro-comunicacion/mesh-networks]

Los inicios de las redes acopladas son, como no, militares. Inicialmente se usaron para comunicarse con aquellas unidades de militares que aún estando lejos de las zonas de cobertura de sus mandos estaban lo suficientemente cerca entre si como para formar una cadena a través de la cual se pudiese ir pasando los mensajes hasta llegar a su destino (los mandos).

Las redes **Mesh**, o redes acopladas, para definirlas de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los PA están dentro del rango de cobertura de algún TR que directamente o indirectamente está dentro del rango de cobertura del PA.

También permiten que los TRs se comuniquen independientemente del PA entre sí. Esto quiere decir que los dispositivos que actúan como TR pueden no mandar directamente sus paquetes al PA sino que pueden pasárselos a otros TRs para que lleguen a su destino.

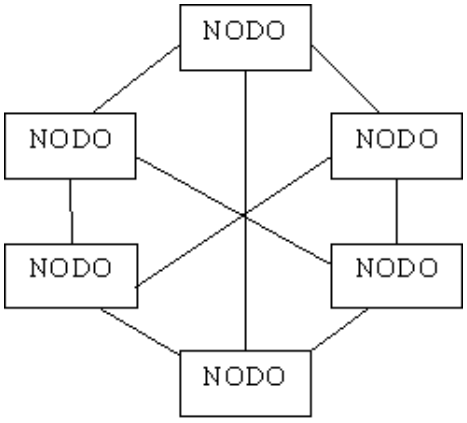
Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (**Hops** en inglés) o con un número que aún no siendo el mínimo sea suficientemente bueno.

Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

Antiguamente no se usaba porque el cableado necesario para establecer la conexión entre todos los nodos era imposible de instalar y de mantener. Hoy en día con la aparición de las redes **wireless** este problema desaparece y nos permite disfrutar de sus grandes posibilidades y beneficios.

Hoy por hoy uno de los principales fabricantes de SW y HW para redes acopladas es **LocustWo LocustWorld** http://www.locustworld.com.

A modo de ejemplo de muestra una red acoplada formada por seis nodos. Se puede ver que cada nodo establece una comunicación con todos los demás nodos. Si este gráfico ya comienza a ser complicado, imagine si el número de nodos fuese de varios cientos.



13. Seguridad en las comunicaciones Wireless - Terminología

[http://www.mailxmail.com/...uturo-comunicacion/seguridad-comunicaciones-wireless-terminologia]

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que nos permitan disponer del grado máximo de seguridad del que seamos capaces de asegurar.

Terminología

Para poder entender la forma de implementar mejor la seguridad en una red wireless, es necesario comprender primero ciertos elementos:

- **WEP**. Significa **Wired Equivalet Privacy**, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Es INSEGURO debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.

- **OSA vs SKA**. **OSA** (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP. **SKA** (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.

- **ACL**. Significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

- **CNAC**. Significa Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

- **SSID**. Significa Service Set IDentifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

14. Pasos para segurar una red inalámibrica

[http://www.mailxmail.com/...ambricas-wi-fi-futuro-comunicacion/pasos-segurar-red-inalamibrica]

En primer lugar hay que situarse dentro de lo que seguridad significa en el mundo informático.

Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99'99%, por ello debemos desechar la idea de que los sistemas informáticos son seguros al 100%. No es cierto.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener.

Una vez situados vamos a ver los pasos que podemos seguir para introducir una seguridad razonablemente alta a nuestra red **wireless**. Debemos tener en cuenta que cuando trabajamos con una red convencional cableada disponemos de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma. En nuestro caso no, de hecho vamos a estar "desperdigando" la información hacia los cuatro vientos con todo lo que esto conlleva.

15. Enumeración pasos para asegurar una red inalámbrica

[http://www.mailxmail.com/...fi-futuro-comunicacion/enumeracion-pasos-asegurar-red-inalambrica]

A continuación comentaremos los pasos necesarios para asegurar nuesta red **Wirelwess**

Paso 1, debemos activar el **WEP**. Parece obvio, pero no lo es, muchas redes inalámbricas, bien por desconocimiento de los encargados o por desidia de los mismos no tienen el WEP activado. Esto viene a ser como si el/la cajero/a de nuestro banco se dedicase a difundir por la radio los datos de nuestras cuentas cuando vamos a hacer una operación en el mismo. WEP no es completamente seguro, pero es mejor que nada.

Paso 2, debemos seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla. No debemos usar fechas de cumpleaños ni números de teléfono, o bien hacerlo cambiando (por ejemplo) los ceros por oes...

Paso 3, uso del **OSA**. Esto es debido a que en la autenticación mediante el **SKA**, se puede comprometer la clave **WEP**, que nos expondría a mayores amenazas. Además el uso del SKA nos obliga a acceder físicamente a los dispositivos para poder introducir en su configuración la clave. Es bastante molesto en instalaciones grandes, pero es mucho mejor que difundir a los cuatro vientos la clave. Algunos dispositivos OSA permiten el cambiar la clave cada cierto tiempo de forma automática, lo cual añade un extra de seguridad pues no da tiempo a los posibles intrusos a recoger la suficiente información de la clave como para exponer la seguridad del sistema.

Paso 4, desactivar el **DHCP** y activar el **ACL**. Debemos asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas. De esta forma no permitiremos que se incluyan nuevos dispositivos a nuestra red. En cualquier caso existen técnicas de sniffing de las direcciones MAC que podrían permitir a alguien el descubrir direcciones MAC válidas si estuviese el suficiente tiempo escuchando las transmisiones.

Paso 5, Cambiar el **SSID** y modificar su intervalo de difusión. Cada casa comercial reconfigura el suyo en sus dispositivos, por ello es muy fácil descubrirlo. Debemos cambiarlo por uno lo suficientemente grande y difícil como para que nadie lo adivine. Así mismo debemos modificar a la baja la frecuencia de broadcast del SSID, deteniendo su difusión a ser posible.

Paso 6, hacer uso de VPNs. Las Redes Privadas Virtuales nos dan un extra de seguridad que nos va a permitir la comunicación entre nuestros dispositivos con una gran seguridad. Si es posible añadir el protocolo IPSec.

Paso 7, aislar el segmento de red formado por los dispositivos inalámbricos de nuestra red convencional. Es aconsejable montar un firewall que filtre el tráfico entre los dos segmentos de red.

Actualmente el **IEEE** está trabajando en la definición del estándar **802.11i** que permita disponer de sistemas de comunicación entre dispositivos wireless realmente seguros.

También, en este sentido hay ciertas compañías que están trabajando para hacer las comunicaciones más seguras. Un ejemplo de éstas es CISCO, la cual ha abierto a otros fabricantes la posibilidad de realizar sistemas con sus mismos métodos de seguridad. Posiblemente algún día estos métodos se conviertan en estándar.

16. Técnicas de búsqueda y marcado de redes Wireless - Warchalking

[http://www.mailxmail.com/...comunicacion/tecnicas-busqueda-marcado-redes-wireless-warchalking]

Dentro del mundo **wireless**, no podemos dejar de lado dos prácticas que se han extendido rápidamente entre algunas comunidades de usuarios de esta tecnología sobre todo son el ánimo de conseguir acceso gratuito a Internet. La adaptación a las nuevas tecnologías en algunos ámbitos es extremadamente rápida. ;-)

Warchalking

Es un lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

La sencillez del lenguaje ha sido uno de los factores que han hecho posible su proliferación por las grandes ciudades. Además otras características como la no perdurabilidad de las marcas durante grandes periodos de tiempo hacen que sea muy dinámico y se vaya adaptando constantemente a las características cambiantes de las redes sobre cuya existencia informa.

Los símbolos más usados son:

Retina *-> SSID*

)(*-> Nodo abierto ,() ?Nodo cerrado, (W) ?Nodo con WEP*

1.5 *-> Ancho de Banda*

1. En primer lugar se identifica el nombre del nodo, o SSID
2. En segundo lugar se identifica el tipo de red, bien sea abierta, cerrada o con WEP.
3. En último lugar se identifica la velocidad del mismo.

17. Técnicas de búsqueda y marcado de redes Wireless - WarDriving

[http://www.mailxmail.com/...-comunicacion/tecnicas-busqueda-marcado-redes-wireless-wardriving]

El **WarDriving** es un método usado para la detección de redes inalámbricas.

Se realiza bien desde dentro de un vehículo o bien simplemente caminando a pie por diferentes zonas, habitualmente del centro, de una ciudad, con un dispositivo como un**PDA** o un ordenador portátil con los que se pueden detectar estas redes.

Para la identificación de las redes es necesario usar una **TR WiFi** en modo promiscuo junto con un **SW** especial, modo en el cual va a detectar todas las redes de los alrededores que estén configuradas mediante un PA.

Una vez detectada la red, se analiza y bien se "marca" mediante el **warchalking** bien se apunta para su posterior explotación.

Adicionalmente se puede dotar al sistema de un **GPS** con el cual marcar exactamente en un mapa la posición de la red. Ya existe SW apropiado para estos casos como es el AirSnort para Linux, el BSD-AriTools para BSD y el NetStumbler para Windows.

18. Sopa de letras (y números)

[http://www.mailxmail.com/...-redes-inalambricas-wi-fi-futuro-comunicacion/sopa-letras-numeros]

Existen multitud de estándares definidos o en proceso de definición que es necesario conocer para una correcta interpretación de las redes **wireless**:

- **802.11a** Estándar de comunicación en la banda de los 5 Ghz, ya descrito

- **802.11b** Estándar de comunicación en la banda de los 2'4 Ghz, ya descrito.

- **802.11c** Estándar que define las características que necesitan los APs para actuar como puentes (bridges). Ya está aprobado y se implementa en algunos productos.

- **802.11d** Estándar que permite el uso de la comunicación mediante el protocolo

- **802.11** en países que tienen restricciones sobre el uso de las frecuencias que éste es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.

- **802.11e** Estándar sobre la introducción del QoS en la comunicación entre PAs y TRs. Actua como árbitro de la comunicación. Esto permitirá el envío de vídeo y de voz sobre IP.

- **802.11f** Estándar que define una práctica recomendada de uso sobre el intercambio de información entre el AP y el TR en el momento del registro a la red y la información que intercambian los APs para permitir la interportabilidad. La adopción de esta práctica permitirá el Roamming entre diferentes redes.

- **802.11g** Estándar que permite la comunicación en la banda de los 2'4 Ghz, ya descrito.

- **802.11h** Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además define el TPC (Transmit Power Control) según el cual la potencia de transmisión se adecúa a la distancia a la que se encuentra el destinatario de la comunicación.

- **802.11i** Estándar que define la encriptación y la autentificación para complementar completar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).

- **802.11j** Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.

- **802.11m** Estándar propuesto para el mantenimiento de las redes inalámbricas.

19. Casos de estudio - Uso personal (I)

[http://www.mailxmail.com/...alambricas-wi-fi-futuro-comunicacion/casos-estudio-uso-personal-1]

Dentro de la puesta en práctica de las redes inalámbricas se han incluido tres casos de estudio que pueden representar un alto número de los escenarios de uso de esta tecnología.

- Uso personal
- Comunidad de vecinos / ISPs "pequeños"
- Uso empresarial

Caso de estudio Nº 1: Uso personal

Este viene siendo y es hoy por hoy uno de los escenarios más comunes de esta tecnología.

Hasta hace bien poco los usuarios "caseros" de ordenadores, bien por uso particular bien por uso profesional del ordenador y por ende de Internet, estaban "atados" a las zonas de la casa/local donde tenían las tomas telefónicas o bien los módems**ADSL/DSL/CABLE**. El mover los ordenadores a otra localización dentro de la casa / pequeño negocio era prácticamente imposible o muy costoso.

Además con el continuo avance de la tecnología y el rápido desfase de los ordenadores nos podemos encontrar en una casa normal con varios ordenadores unidos mediante una**LAN** (red de área local) y eso significaba que tanto el módem como los ordenadores debían estar en un espacio muy reducido, normalmente poco idóneo para su uso y/o ubicación.

Este hecho, unido con la "habilidad" de ciertos constructores que se han dedicado a poner las toma telefónicas y/o las tomas de ADSL/DSL/CABLE en los lugares más originales pero menos aprovechables de las casas podía llegar a presentar un serio inconveniente para implantar una pequeña red.

Gracias a la tecnología inalámbrica actual, esto es posible solucionarlo de una manera muy fácil y nos va a permitir disponer de los ordenadores en la situación que queramos dentro de la casa (a no ser que vivamos en el Palacio de Buckingham).

20. Casos de estudio - Uso personal (II)

[http://www.mailxmail.com/...alambricas-wi-fi-futuro-comunicacion/casos-estudio-uso-personal-2]

Vamos a tomar como ejemplo una casa con tres ordenadores, dos de ellos de sobremesa y uno portátil. Esta configuración es una configuración estándar que representa bastante bien un amplio espectro de los hogares medios, en los cuales uno de los ordenadores se ha quedado tecnológicamente desfasado pero aún se quiere aprovechar, se ha comprado un segundo ordenador de sobremesa más potente y se tiene uno portátil bien por necesidades particulares o bien porque el trabajo de uno de los integrantes de la familia lo provee.

Suponemos que disponemos bien de una conexión telefónica o bien un ADSL/DSL/CABLE para conectarnos a Internet.

La lista de elementos que vamos a necesitar para implantar la red es muy corta.

- Ordenador 1 (ya disponible)
- Ordenador 2 (ya disponible)
- Ordenador portátil (ya disponible)
- 1 tarjeta PCI WiFi 802.11b (a adquirir)
- 1 tarjeta USB WiFi 802.11b (a adquirir)
- 1 tarjeta PCMCIA WiFi 802.11b (a adquirir)
- 1 PA Router Wifi 802.11b (a adquirir)

La configuración más normal será la de configurar el ordenador más tecnológicamente atrasado con la tarjeta **Wifi PCI**, poniendo la **USB WiFi** al ordenador más moderno y dejando la **PCMCIA WiFi** para el ordenador portátil.

Lo preferible sería ponerle a los dos ordenadores de sobremesa **TR USB WiFi**, pero si no disponemos de puerto **USB** o no tenemos ninguno libre en el ordenador antiguo habrá que ponerle tarjeta **PCI WiFi**.

Es necesario hacer notar al lector que en el caso de conectar tarjetas USB WiFi, debemos tener en cuenta que el USB 1.1 sólo permite transferir datos a una velocidad máxima de 12 Mbps por lo que si le conectamos una tarjeta USB WiFi 802.11g con una velocidad máxima de 54 Mbps no conseguiremos aumentar la velocidad. Para conectar este tipo de tarjetas es necesario disponer de conectores USB 2.0.

El PA Router será el encargado de conectarnos a Internet. Hay algunas unidades que llevan un MODEM 56K V90 integrado por lo que no es necesario comprar un MODEM adicional. En cualquier caso usar un MODEM para conectarse a Internet debería de ser la última de nuestras opciones, pues es muy recomendable el contratar las ya baratas soluciones ADSL / DSL / CABLE de cualquier proveedor que nos la ofrezca. Es caso del ADSL, por ejemplo y del DSL y CABLE por extensión, los routers disponen de una entrada WAN a la cual enchufar el MODEM sea del tipo que sea, por lo que el configurarlo será muy sencillo. Para este caso, supongamos una salida a internet mediante ADSL 256/128 Kbps.

Es muy interesante que disponga de Servicio DHCP (asignación dinámica de direcciones IP) y de NAT (traducción/asignación de direcciones IP mediante el uso de direcciones privadas del tipo 198.162.x.x ó 10.x.x.x) lo que nos permitirá permanecer protegidos de las

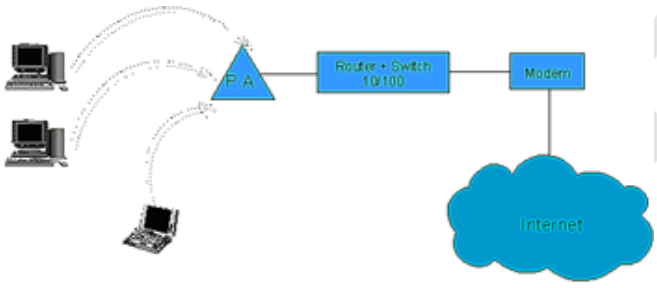
"inclemencias" de internet.

21. Casos de estudio - Uso personal (III)

[http://www.mailxmail.com/...alambricas-wi-fi-futuro-comunicacion/casos-estudio-uso-personal-3]

El PA Router distribuirá la señal entre los tres ordenadores, que ahora podremos poner en cualquier sitio. La configuración normal será que el niño / joven de la casa disponga del más potente para jugar en su habitación, el / los padres del tecnológicamente desfasado pero seguro para almacenar su documentación y navegar por internet en su despacho y el ordenador portátil se reservaría para hacer en casa (sigh!!) cosas del trabajo y poco más.

Dado que tenemos tres adaptadores "recibiendo" información desde internet, y dada la conexión ADSL con 256 Kbps de bajada, en el peor momento punta tendremos 256 Kbps/3 = 85'32 Kbps para cada uno, el cual parece un ancho de banda razonable, es más, dadas las características de los tres aparatos es altamente improbable que los tres estén conectados al mismo tiempo, y en ese caso de los tres conectados, es poco probable que estén los tres recibiendo información al máximo de su velocidad al mismo tiempo.



Para realizar este tipo de red es deseable usar un tipo de conexión 802.11b que nos va a permitir conectarnos a Internet sin ningún problema además de transferir archivos entre las máquinas y compartir recursos sin ningún problema de velocidad.

La configuración recomendada es la de más alta seguridad, tal y como se ha detallado en el apartado correspondiente a seguridad. El único paso que podemos obviar sería el uso de redes VPNs, aunque de todas formas sea recomendable su uso.

Tomando como ejemplo de marca a seleccionar a D-link, los precios (sin IVA) pueden ser los que siguen (sólo válidos como guía para este estudio):

- D-Link DWL-520+ PCI 61'12"
- D-Link DWL-650+ PCMCIA 50"
- D-Link DWL-120 USB 60'43"
- D-Link DWL-900AP+ AP 122'22"

Lo cual hace un total de 293'34", cantidad perfectamente asumible por una familia media o pequeño negocio. Si lo comparamos con el equivalente necesario (sin contar con el tiempo para realizar la instalación y los conocimientos que son necesarios) para instalar una red Ethernet típica a 10/100 Mbps, podemos llegar a la conclusión de que la red inalámbrica es MAS BARATA y más fácil de configurar, sin contar que nos permite conectar los ordenadores independientemente de dónde los hayamos colocado, evitando la instalación de incómodas canaletas por suelo y paredes.

22. Casos de estudio Nº 2: Comunidad de vecinos / ISPs "pequeños"

[http://www.mailxmail.com/...-comunicacion/casos-estudio-n-2-comunidad-vecinos-isps-pequenos-

Este escenario en el que nos vamos a mover difiere en ciertos aspectos del que acabamos de describir. Contrariamente a lo que se puede pensar en un primer momento no nos encontramos ante un sobredimensionamiento del caso anterior.

Para describir este escenario vamos a suponer que una comunidad de propietarios de un edificio, desea conectarse a Internet, a la vez que quiere disponer de una página Web que muestre información a los vecinos sobre reuniones, pagos de comunidad...

Partamos de un edificio en el centro de una gran ciudad que dispone de 15 vecinos. Todos se han puesto de acuerdo y quieren alquilar a un proveedor de Internet por cable un acceso de 1(Mbps, el cual es demasiado caro para una sola persona pero perfectamente asumible pagándo entre toda la comunidad.

Cada vecino va a disponer de un ordenador en su casa (máximo dos) desde los cuales se les dará servicio de conexión a Internet. Esto hace un total de en el peor de los casos 30 ordenadores conectados simultáneamente a Internet.

Para empezar vamos a describir la infraestructura necesaria.

- Vamos a necesitar bien de un **router** estándar con un punto de acceso o bien de un PA Router. En cualquier caso debería poder disponer de una toma a la que conectar una antena adicional o bien que la antena del mismo sea desmontable. El protocolo seleccionado para el PA será el 802.11g.

- Sea cual sea la elección, conectaremos al router un **ordenador** que será el encargado de realizar la gestión de todo el sistema. No es necesario que sea muy potente, pero si al menos l suficiente como para poder instalar el SW de servidor Web + Correo electrónico, Sw de gestión de las comunicaciones y poco más.

- Si fuese necesario, necesitaríamos una **antena** con un pigtail (cable) que sea capaz de ubicar a la misma en el centro del edificio o en la parte más alta del mismo. Debemos tener en cuenta que cuanto más largo sea el cable de conexión a la antena mas atenuación de la señal emitida recibida tendremos.

- Cada vecino ya dispone al menos de un ordenador, al cual conectará una TR 802.11g. No es conveniente hoy por hoy el mezclar tarjetas 802.11b con PA 802.11g pues provoca que éstos bajen su rendimiento de forma apreciable.

Hagamos cuentas:

10 Mbps/30 ordenadores = 350 Kbps velocidad que es bastante buena para una conexión a Internet en el peor de los casos.

10 Mbps/15 ordenadores = 700 Kbps velocidad que es muy buena para una conexión a Intern en el mejor de los casos.

10 Mbps/1 ordenador = 10 Mbps velocidad que es bastante buena para una conexión (idílica) Internet.

Dado el número de usuarios/ordenadores, vamos a olvidarnos de el 802.11b con sus 11/22 Mbps y nos vamos a ir al 802.11g con sus 54 Mbps.

23. Casos de estudio Nº 2: Comunidad de vecinos / ISPs "pequeños" (II)

[http://www.mailxmail.com/...-comunicacion/casos-estudio-n-2-comunidad-vecinos-isps-pequenos-

En el tramo que hay entre el TR y el PA, nuestro PA va a ser capaz de repartir sus 54 Mbps entr los 30 ordenadores de los vecinos, lo cual hace un total de 1'8 Mbps disponibles en el peor caso para cada ordenador.

- Dado que en el peor de los casos cada ordenador dispone sólo de 350 Kbps para acceder a Internet, 1'8 Mbps son más que suficientes. De hecho, esta infraestructura nos permitiría teóricamente aumentar el ancho de banda de nuestra conexión por cable a internet hasta llega a los 54 Mbps. Realmente el límite razonable va a estar en la mitad de esto, llegando sólo hast alrededor de 26 Mbps.

- Desde el punto de vista de los usuarios y manteniendo un mínimo de 128 Kbps de velocidad de acceso a Internet para cada uno, y dada la conexión de 10 Mbps, teóricamente podríamos dar servicio a alrededor de 80 ordenadores/usuarios simultáneos como máximo, pero en el tramo de comunicación entre el TR y el PA, la velocidad sería de 691 Kbps con 80 usuarios. Dado que esta velocidad no está soportada, tendríamos que subir hasta 1 Mbps lo que nos llevaría a su vez a dar servicio a 56 usuarios simultáneos como máximo.

- Estas dos aproximaciones han sido hechas, tomando que cada usuario tiene un 100% del ancho de banda de su conexión en el peor caso como CIR. Si suponemos un CIR más bajo para cada usuario, entonces podríamos aumentar el número de usuarios, pero teniendo en cuenta que en momentos de acceso "masivo" podemos tener picos que hagan que las comunicaciones se vean apreciablemente ralentizadas.

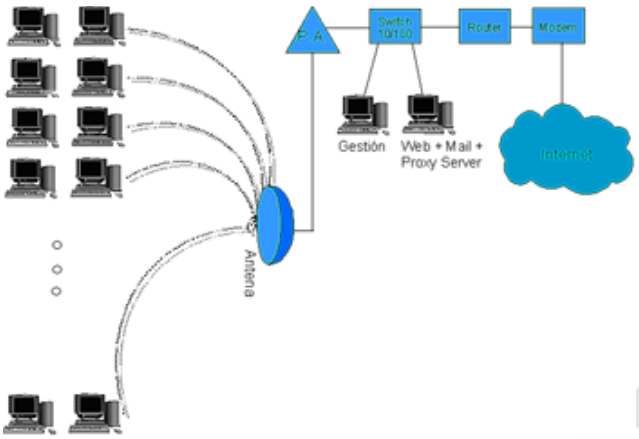
Ya hemos visto que cada vecino puede conectarse a Internet a una velocidad razonable, pero esto sólo es teoría pues dado que el estándar 802.11g de momento no dispone de **QoS** (posibilidad de garantizar un ancho de banda determinado) no podemos asegurar que un solo vecino no se "coma" todo el ancho de banda, dejando al resto "parado".

Esto es muy peligroso hoy en día dada la proliferación de las redes Peer to Peer, o redes Punto Punto de intercambio de ficheros, con ejemplos como el Kazaa, E-donkey y otros que "se comerían" casi por completo el ancho de banda que les diésemos.

Normalmente, dentro de los ISPs / comunidades, el 10% de los usuarios tenderían a usar el 90% del ancho de banda.

Para resolver este problema vamos a tener que recurrir algún SW de gestión de comunicacione y más concretamente del ancho de banda que o bien venga con el mismo PA o bien lo instalemos en la máquina de gestión del sistema. Puede ser necesario el tener que instalar en e servidor el SW de servidor **RADIUS** (Remote Authentication Dial-In User Service), el cual nos administrará la red como si de un pequeño ISP se tratase.

Respecto a la seguridad, es la misma que siempre, prestando especial atención al tema de que cada vecino sólo debe tener dos máquinas dadas de alta en la lista de direcciones MAC del PA.



Aunque en el gráfico se ha incluido un MODEM entre Internet y el Router, se ha hecho sólo con la intención de indicar que en ese lugar ha de ir un elemento de comunicaciones, aunque pued no ser necesario o puede no ser un módem.

24. Caso de estudio Nº 3: Uso empresarial

[http://www.mailxmail.com/...icas-wi-fi-futuro-comunicacion/caso-estudio-n-3-uso-empresarial-1]

Este tercer caso vamos a enfocarlo desde un punto de vista diferente.

?- El primer caso estudiado estaba enfocado al intercambio de archivos y a compartir recursos entre un conjunto muy limitado de ordenadores/usuarios con un acceso a Internet restringido a entre 56 y 256 Kbps.

?- En el segundo nos basamos casi exclusivamente en el acceso a Internet y la gestión del ancho de banda del mismo, teniendo muy pocos recursos o ninguno compartidos entre los participantes de la red.

?- Este tercer caso vamos a enfocarlo como un escenario en el que vamos a compartir recursos, impresoras, servidores, espacios de almacenamiento..., y además vamos a tener un acceso a Internet. Este acceso no va a ser para todos los ordenadores y aunque el ancho de banda va a ser mayor que en el primer caso no va a llegar a ser tan grande como en el segundo.

Tendremos una infraestructura de sistemas internos muy grande, a la cual se dirigirá la mayoría de las comunicaciones. El acceso a Internet no será muy amplio, basándose sobre todo en el uso del correo electrónico.

Vamos a suponer una empresa en la que disponemos de por ejemplo 50 ordenadores repartidos por diferentes plantas y con un área física a cubrir mayor que en los casos anteriores. La seguridad dentro de las comunicaciones será un aspecto crítico. Se aconsejará el uso de **VPNs** (Redes Privadas Virtuales).

Dispondremos de una infraestructura básica de comunicaciones "tradicional" mediante el uso de una red Ethernet 100, a la que conectaremos PA Routers 802.11g.

Aunque aún no está estandarizada por el IEEE, la especificación 802.11g parece que va a ser el futuro de este tipo de redes. En este caso el coste de los PAs y TRs no va a ser un punto crítico, por lo que se recomienda fuertemente la compra de los mismos a marcas de reconocido prestigio como por ejemplo CISCO.

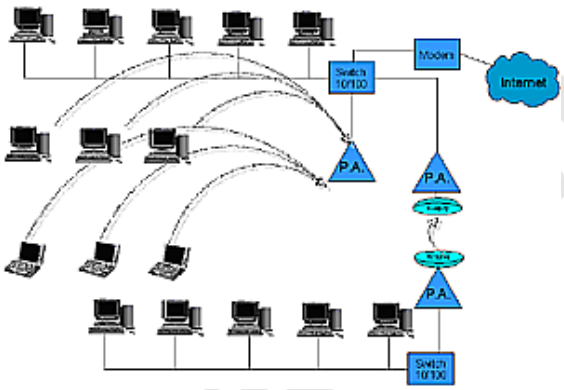
25. Caso de estudio Nº 3: Uso empresarial (II)

[http://www.mailxmail.com/...icas-wi-fi-futuro-comunicacion/caso-estudio-n-3-uso-empresarial-2]

Hay que tener en cuenta que tratándose de una empresa, podríamos llegar a tener puntos con una gran demanda de ancho de banda y otros con muy poca.

Hay que investigar cuáles pueden ser los puntos donde haya más concentración de máquinas, como pueden ser las zonas de reuniones, zonas de gran concentración de trabajadores... De esta forma después de hacer esta investigación decidiremos cuáles son las mejores zonas para montar el PA.

Desde el punto de vista de la seguridad y después de comentar el punto anterior, hay que pensar también que las antenas es mejor colocarlas en lugares "centrales" del edificio, donde el radio de alcance de la señal no exceda demasiado del edificio físico en el que se encuentre. En cualquier caso, siempre o casi siempre tendremos cobertura inalámbrica fuera de nuestro edificio. Por ello hay que seguir las normas de seguridad escrupulosamente.



Desde el punto de vista de la seguridad y después de comentar el punto anterior, hay que pensar también que las antenas es mejor colocarlas en lugares "centrales" del edificio, donde el radio de alcance de la señal no exceda demasiado del edificio físico en el que se encuentre. En cualquier caso, siempre o casi siempre tendremos cobertura inalámbrica fuera de nuestro edificio. Por ello hay que seguir las normas de seguridad escrupulosamente.

Según estudios prácticos hechos en la ciudad de Londres en noviembre de 2002, en hora y media se pueden localizar más de 60 redes inalámbricas simplemente paseando por una calle del centro, y de estas el 75% no tenían ningún tipo de seguridad.

Normalmente los **wardrivers** solamente van a intentar acceder a nuestra red para usar Internet de una forma gratuita, pero podemos descartar las intromisiones de crackers que intenten sabotear nuestras instalaciones o a la competencia intentando llevarse nuestros secretos empresariales...

Otro uso bastante práctico puede ser el unir dos redes empresariales lejanas entre si. Para ello se puede disponer de dos antenas direccionales especialmente preparadas para tal evento y dos puntos de acceso normales.

Se configuran los puntos de acceso para que sólo sea posible la comunicación entre ellos (además de todas las características de seguridad vistas) y se enfocan las antenas entre si. Experiencias anteriores han demostrado que es posible establecimiento de comunicaciones

de hasta 70Km. Normalmente es difícil que tengamos que llegar a tales extremos, pero muestra un valor máximo útil que nos puede dar idea de si son posibles nuestros propósitos.

Para que esta comunicación sea posible es necesario que el **PA WiFi** cumpla el estándar 802.11c (bridge) o bien simularlo mediante un SW dedicado a tal propósito.

26. Anexos - Estándares SI - Estándares NO ¿Qué hacer?

[http://www.mailxmail.com/...-futuro-comunicacion/anexos-estandares-si-estandares-no-que-hacer]

Los estándares son tan buenos que cada fabricante tiene el suyo. Esta broma no puede ser más cierta en el caso que nos incumbe. La proliferación de diferentes estándares viene dada únicamente por la prisa que tienen algunas compañías en introducirse en los mercados emergentes para alcanzar una posición de fuerza y poder manejar de la forma que sea más beneficioso para sus intereses las decisiones de los comités estandarizadores del IEEE.

Idealmente todas las empresas deberían seguir los estándares del IEEE para de esa forma asegurar la interoperabilidad de los dispositivos vendidos con los dispositivos de otros fabricantes, pero lamentablemente eso no ocurre así y diferentes fabricantes ofrecen diferentes soluciones que terminan por no funcionar entre sí.

Esta situación se vivió en los principios de la venta masiva de dispositivos SCSI en los que era mejor adquirir todos los dispositivos SCSI de un mismo fabricante pues si por un lado adquiríamos la tarjeta y por otro los dispositivos podíamos tener incompatibilidades que nos obligaban a tener que tirar uno de ellos a la basura. Bueno pues esa misma situación es en la que nos encontramos hoy en día.

Aunque muchos fabricantes prometen en sus folletos de venta que sus dispositivos no estandarizados cumplirán con las especificaciones del IEEE cuando éste publique el estándar correspondiente, bien sin modificaciones bien mediante una actualización de su Firmware, esto es algo de lo que no podemos estar totalmente seguros.

Hoy por hoy lo mejor es comprar dispositivos estandarizados por el IEEE y si no es así es preferible que sean de una marca reconocida a la cual le pueda hacer daño la mala imagen que pueda causar si no actualiza los dispositivos vendidos no cumplidores del estándar correspondiente por unos que si lo cumplan.

Es la única forma que tenemos de que los dispositivos que compramos hoy funcionen mañana.

Copia de imágenes para la restauración de equipos

Este procedimiento se ha implementado con el fin de poder minimizar los riesgos de daño en los equipos, además de mejorar y agilizar la preparación o restauración de est...
[04/03/05]

3.023

Impacto de las nuevas tecnologías en la empresa

Hablar de nuevas tecnologías es hablar de un amplio abanico de técnicas, herramientas, ámbitos de investigación y desarrollo que abarcan desde el estudio de la vida anima...
[29/04/05]

2.091

Jerarquía Digital Síncrona (SDH)

SDH es el estandar internacional de comunicaciones aceptado por la UIT para redes de transmisión de alta capacidad. Tecnologías como ATM, IP/MPLS o ADSL se apoyan en SDH ...
[07/05/04]

13.117

Internet. Tu negocio

Intenet fue un negocio que en algún momento parecía una idea "descabellada". Ahora el internet es una herramienta de uso indispensable en las e...
[03/02/09]

1.000