Facultad de Ciencias Sociales y de la Comunicación

Diplomatura en Gestión y Administración Pública

Asignatura de:

Redes de datos

Tema XI anexo

Redes inalámbricas

(Transparencias de clase)

DEPARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS

Profesor: Manuel Fernández Barcell

e-mail: manuel.barcell@uca.es

Índice

1 ANEXO sobre WI-FI

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. ;-)

1.1 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.

Símbolos utilizados en *Warchalking*: http://notabug.com/warchalking/card300.png

1.2 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 promíscuo 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.

1.3 Sopa de letras (y números)

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 Contro*l) 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 el cifrado 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.

1.4 Casos de estudio

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.

- Caso de estudio Nº 1: Uso personal
- Caso de estudio Nº 2: Comunidad de vecinos / ISPs pequeños
- Caso de estudio Nº 3: Uso empresarial

1.4.1 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)

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.

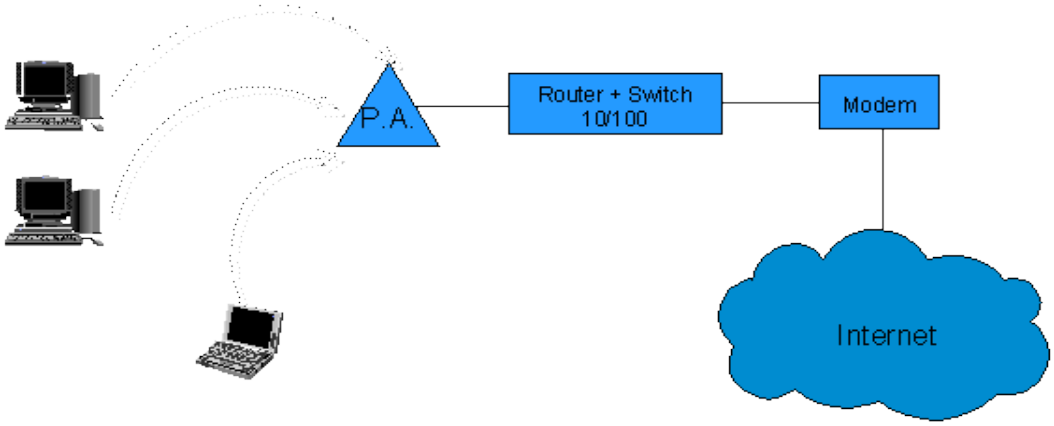
Es necesario hacer notar al lector que en el caso de conectar tarjetas USB WiFi, debemos tener en cuenta que el USB 1.1 sólo permite transferir datos a una velocidad máxima de 12 Mbps por lo que si le conectamos una tarjeta USB WiFi 802.11g con una velocidad máxima de 54 Mbps no conseguiremos aumentar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

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 Euros
- 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.

1.4.2 Caso de estudio Nº 2: Comunidad de vecinos / ISPs pequeños

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 sobre-dimensionamiento 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 10 Mbps, el cual es demasiado caro para una sola persona pero perfectamente asumible pagándolo 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 lo 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.

Vamos ahora a echar 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 Internet en el mejor de los casos.

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

En el tramo que hay entre el TR y el PA, nuestro PA va a ser capaz de repartir sus 54 Mbps entre 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 llegar a los 54 Mbps. J. Realmente el límite razonable va a estar en la mitad de esto, llegando sólo hasta 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.

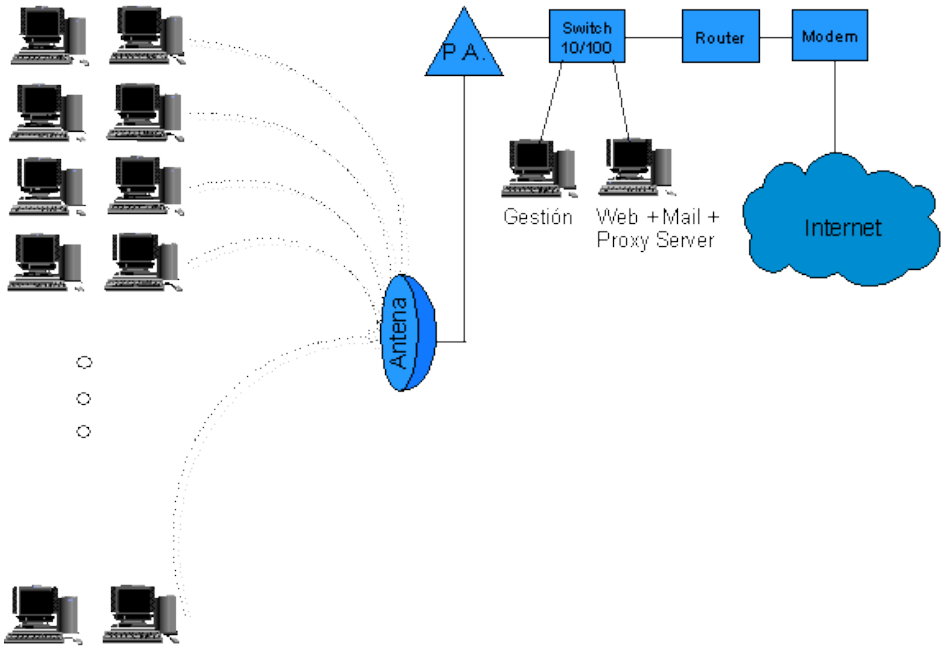
Esto es muy peligroso hoy en día dada la proliferación de las redes Peer to Peer, o redes Punto a Punto de intercambio de ficheros, con ejemplos como el Kazaa, E-donkey y otros que se comerían casi por completo el ancho de banda que les diésemos.

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 comunicaciones 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 el 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 puede no ser necesario o puede no ser un módem.



1.4.3 Caso de estudio Nº 3: Uso empresarial

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.

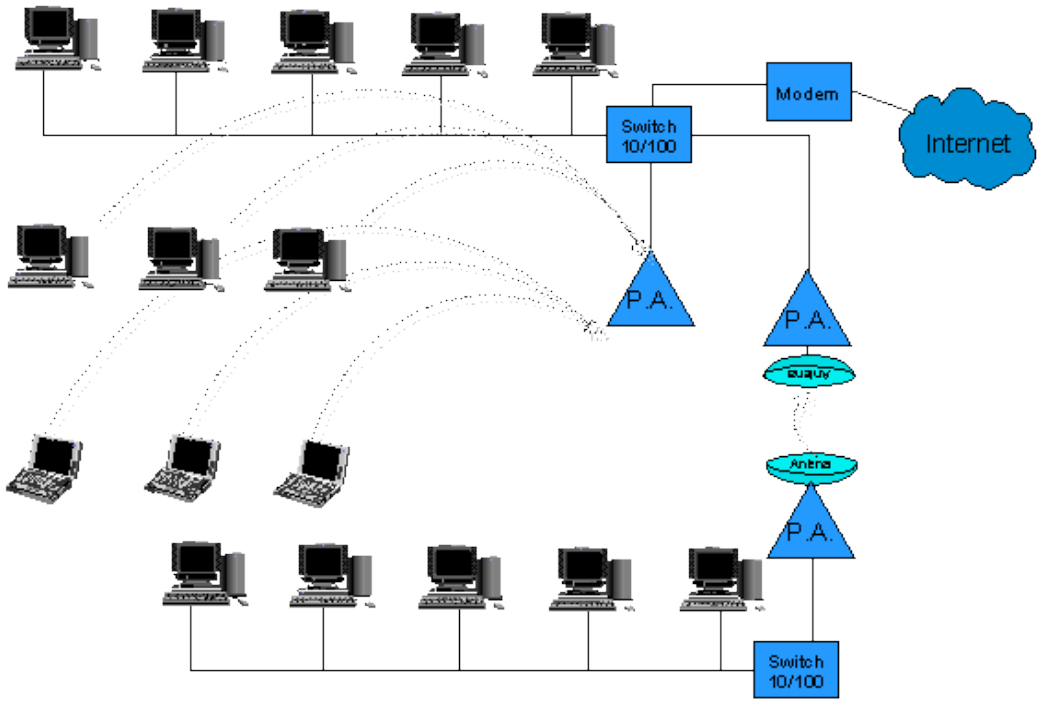
Vamos a suponer una empresa en la que disponemos de por ejemplo 50 ordenadores repartidos por diferentes plantas y con un área física a cubrir mayor que en los casos anteriores. La seguridad dentro de las comunicaciones será un aspecto crítico. Se aconsejará el uso de VPNs (Redes Privadas Virtuales).

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.

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.



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.

1.4.4 Estándares SI - Estándares NO ¿Qué 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.

Fabricantes de productos Wifi

- Belkin www.belkin.com
- Linksys www.linksys.com
- D-Link www.d-link.com
- Buffalo www.buffalotech.com
- Benq www.benq.com
- SMC www.smc.com
- CISCO www.cisco.com
- Atheros www.atheros.com/

Sitios donde comprar dispositivos Wireless

- http://www.ibm.es
- http://www.batchpc.com
- http://www.pecenet.com

- http://www.areapc.com
- http://www.instantbyte.com

Puntos de información relacionada

IEEE http://grouper.ieee.org/groups/802/11

Web de Seattle Wireless http://www.seattlewireless.com

Web de Madrid Wireless http://madridwireless.net

Información sobre WiFi http://www.newswireless.net/

Información sobre WiFi http://www.communitywireless.org

Alianza WiFi http://www.wi-fi.com/

Redes Mesh http://www.meshnetworks.com/

Standards IEEE "Get IEEE 802": Wireless (IEEE 802.11) http://standards.ieee.org/getieee802/802.11.html

Best Practices for Deploying Wireless LANs http://www.ebcvg.com/download.php?id=1160

Warchalking http://www.warchalking.com

Símbolos utilizados en Warchalking http://notabug.com/warchalking/card300.png

Wireless Security: Thoughts on Risks and Solutions

http://www.ebcvg.com/download.php?id=1371

Documentos varios sobre seguridad en redes inalámbricas

http://www.ebcvg.com/category.php?cat=11&p=1

Una-al-día (21-03-02): Acceso a Internet gracias a los tubos de galletas Pringles

http://www.hispasec.com/unaaldia.asp?id=1243

Por Ander Otxoa Guilo

Artículo original en: http://el202.homeip.net/schedule.htm