Conceptos básicos de comunicaciones inalámbricas

Con este primer avance voy a explicar la terminología usada en comunicaciones inalámbricas, que no es poco y disponen de un maremagno de siglas, especificaciones y peculiaridades.

Aunque esta sea la parte "*mas pesada*" del Taller, es **IMPRESCINDIBLE**, que tengamos estos conocimientos claros y bien afianzados, en esta parte no encontraréis otra cosa que llamar a cada cosa por su nombre y asentar los principios básicos de la comunicación sin cables.

El objetivo de esta parte del Taller es ser capaces de diferenciar los distintos protocolos, hardware disponible o necesario, normativas, factores que determinan la comunicación, problemática y por ondas, etc..

Comencemos.... Las señales inalámbricas son ondas electromagnéticas que viajan a través de un medio concreto: habitualmente el aire, pero también el vacío o cuando "*se tropiezan*" con un obstáculo parte de esa señal lo atraviesa o queda retenida o se "*refracta*"

Pueden cubrir tanto grandes distancias como pequeñas, todo dependerá de factores como la frecuencia, la potencia o como se dijo antes, los medios que atraviesa la señal....

La unidad de medida para distinguir unas señales de otras en las comunicaciones *wireless*, es el **hercio** y cada dispositivo o conjunto de ellos, emiten en diferentes frecuencias, en distintos hercios, para que unas señales no "*estorben*" a otras.

Sin embargo, no todas las comunicaciones inalámbricas transportan datos, las hay de vídeo o de voz, también... el conjunto de todas ellas se les denomina **espectro de radio**, es una parte de un todo llamado **espectro electromagnético**, y utiliza frecuencias desde los 3 Kilo hercios (3KHz) hasta los 300 Giga hercios (300 GHz), todo lo que a continuación se relata, versa sobre la transmisión inalámbrica de datos.

Cada tipo de comunicación inalámbrica tiene sus "*mas y sus menos*", entre los más significativos tenemos:

IR. Infrarrojos: que soporta tasas de datos muy elevadas, costes bajos pero con distancias muy limitadas.

Banda Estrecha: Con tasas de transferencia bajas y costes medios. Alcanza distancias limitadas y requiere una licencia para transmitir

Espectro Diverso: El llamado y conocido por su nombre inglés ***Spread spectrum***, las tasas de datos son altas, coste medio y cubre áreas no muy grandes.

PCS: Personal ***Communications Service*** o Servicio de comunicaciones de banda ancha, las tasas de datos son bajas, coste medio y el objetivo de cubrir un área de una Ciudad

CDPD: ***Cellular Digital Packet Data***, Datos Celulares y Datos Digitales, Tasas bajas, coste elevado y cobertura de un País.

No podemos emitir en cualquier frecuencia... bueno si... pero podemos incurrir en delitos... hay "***bandas de frecuencia***" que se necesita un permiso, una **Licencia**, para transmitir por ella y otras que no.

Las Licencias las entregan los gobiernos u organismos autorizados para ello, obviamente lo que llamamos comunicaciones ***WiFi*** o ***wireless*** utilizan bandas sin licencia, también los ***bluetooth***, las ***PDA's***, etc... ellos también usan bandas sin licencia... y los mandos de la televisión, del aire acondicionado, los coches teledirigidos, juguetes de niños, etc... todos ellos son ejemplos de uso de bandas de radio frecuencia sin licencia.

Independientemente del tipo de comunicación a usar, existen diversos factores, parámetros y problemáticas , como base, apuntaré de momento varias preguntas que debemos hacernos:

¿Cuál es la Tasa de datos que podemos conseguir?

¿ A qué distancia se pueden colocar las estaciones inalámbricas entre ellas? Claro... manteniendo la tasa máxima de datos.

¿Cuántos usuarios pueden existir sin perjuicio de la tasa de datos?

Como ves, el factor determinante es **la tasa de transferencia de datos**, el ancho de banda máximo, como lo quieras llamar.... cuanto mayor sea la tasa de datos mejor.... pero hay que luchar con la distancia, la cantidad de usuarios y la rapidez para lograr una óptima comunicación.

Además, a estos factores "*tangibles*", se le añaden otros que pueden reducir la calidad de la señal, ya lo veremos más adelante.

El caso es que todos esos parámetros y factores persiguen un objetivo: **La capacidad de recibir una señal buena tan lejos como sea posible.**

Algo que no debemos olvidar es que el incremento de la cantidad de datos requiere un uso de un espectro de frecuencia mayor, o por lo menos, un método diferente de colocar en el medio la señal de radio frecuencia.

Es como el cable... para obtener mayores "*velocidades*" sin pérdidas de señal podemos usar medios "*de mayor capacidad*", como la fibra, o podemos usar métodos diferentes para transportarla... como el uso de cables para recibir y emitir al mismo tiempo (*Full Duplex*) en lugar de un mismo cable para las dos cosas (*Half Duplex*)

Si lo prefieres puedes verlo de otro modo... *imagina los bomberos en acción apagando fuegos con sus mangueras ... o imagínatelos usando pajitas de esas que usamos para tomarnos una horchata.... la tasa de trasferencia de agua será mayor con sus mangueras, no sólo porque son "mas anchas", también porque "sale más deprisa", con mayor presión, más cantidad en menos tiempo....* ***algo parecido ocurre cuando combinamos frecuencia, potencia y amplitud en las señales inalámbricas.***

Las comunicaciones inalámbricas se ven afectadas por varios factores:

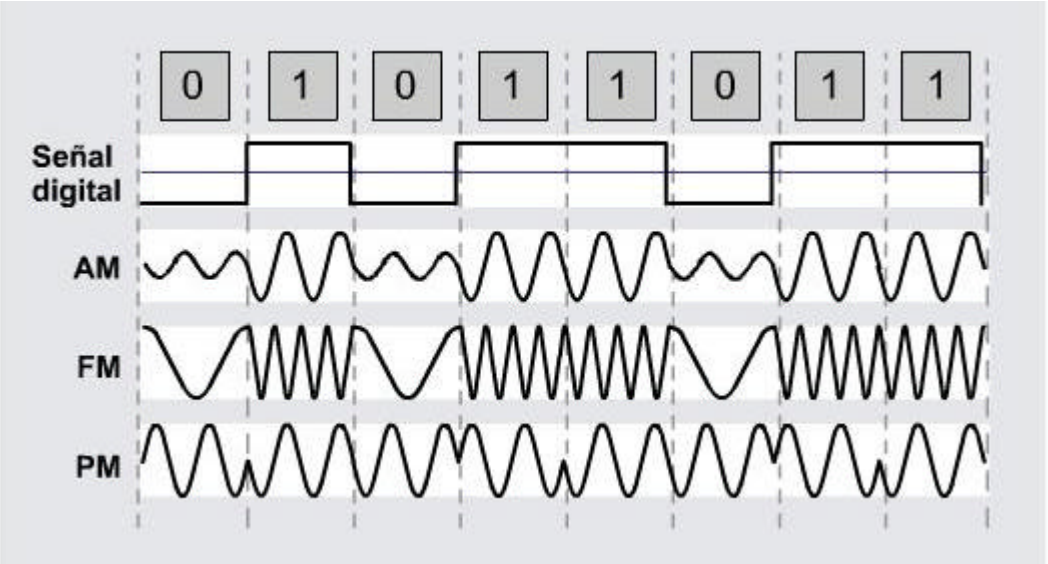
?? **El tipo de modulación usada:** La modulación es el proceso por el que la frecuencia o amplitud es modificado para transmitir datos, seguro que conoces varios métodos de modulación...

AM, lo que llamamos comúnmente onda media... lo que hace la modulación ***AM es alterar la altura de la onda***

FM, nuestra vieja amiga frecuencia modulada... y hace eso... ***alterar la frecuencia***...

PM, lo que se llama modulación de fase... y lo que hace es alterar la polaridad, es decir, si hemos dicho que las ondas forman parte del espectro electromagnético, éste puede tener estados positivos o negativos, la modulación de fase altera los estados electromagnéticos de las ondas.

También tenemos las **ondas digitales**, que "*cambian*" de 0 a 1... lo que se llaman las ondas cuadradas... con un gráfico lo entenderemos mejor:



La señal digital "*sube*" cuando existe un uno y "*baja*" cuando el dato a representar es un cero.

En AM, como lo que se modula es la altura de la onda... si observas, son "*mas altas*" cuando se trata de representar a un uno y "*mas bajas*" cuando el valor representado es un cero.

FM, modula la frecuencia... cuando es un uno el valor, las ondas están "*más pegaditas*" unas de otras que cuando lo que se pretende representar es un cero... en estos casos la onda se "*alarga*"

PM, polariza la señal, cuando representa a un uno es una onda "*invertida*" con respecto a la representación del cero... es como la letra M y la letra W es lo mismo pero al revés.

?? **La distancia** es un factor clave en las comunicaciones inalámbricas... cuanto más lejos estén emisor y receptor más débil será la señal... es obvio... pero no hay que olvidarlo.

Si queremos ser un poco más técnicos, diremos que **cuanto más lejos estén los nodos inalámbricos, la diferencia entre la señal y el ruido será menor**... porque ruido hay... siempre lo hay... cuando un receptor solo capta ruido no se puede comunicar.

Con ruido no sólo me refiero al ruido electrónico, al ruido eléctrico o al ruido de otras señales... en comunicaciones el ruido puede ser una pared que se debe atravesar... no es lo mismo que una onda electromagnética atraviese un fino panel de pladur o un tabique que una puerta acorazada o una ventana o el agua....

?? **La relación señal ruido** es un requisito fundamental en la comunicación, hay que tender a más señal con menos ruido, si hay ruido en el medio, en el canal, la velocidad de transmisión se reduce... o reducirse tanto que no exista comunicación.

Por tanto, **el ruido, la velocidad y la distancia están íntimamente ligados en la transmisión**, recuerda esto también.

Los ordenadores envían señales de datos electrónicas, los radio transmisores son los encargados de convertir esas señales en ondas de radio, por eso se necesitan antenas, **una antena (entre otras cosas) se ocupa de cambiar la corriente eléctrica en ondas**... esas ondas se *"lanzan"* (se irradian) hacia el exterior en línea recta y a medida que *"avanzan"* van perdiendo la fuerza... **se atenúan**... si además deben atravesar obstáculos, árboles, paredes, ventanas, etc... se debilitan aún mas... terminado por desaparecer.... o dicho de otra forma... el ruido es mayor que la señal y se pierde la comunicación.

Para que te hagas una idea, la fuerza de una señal a unos pocos metros de la antena que la transmite es de sólo la centésima parte que la salida inicial... **esto es la atenuación.... pérdida de la señal debido a la distancia entre dos nodos.**

Por si fuese poco, a la atenuación hay que sumarle otros factores negativos en la pérdida de la señal, como son la **absorción, la dispersión, la refractación y otras interferencias**.

Cuando una señal de radio atraviesa un objeto, parte de ella *"se absorbe"*, esa **absorción** puede **refractar** la onda o **dispersarla**... por ejemplo, una pared *"normal"* refracta la onda... "la dobla", pero también el aire hace eso mismo... todo depende del índice de refracción del material por el que pasa... repito, no es lo mismo hacer pasar una onda por el aire o por un cristal que por una pared metálica.

El agua es un factor muy negativo.... y a veces llueve... o hay niebla.... las gotas en el aire hacen que la señal se absorba o disperse perdiendo la comunicación... por ello en días lluviosos, con niebla es probable que nuestras comunicaciones se vean afectadas.

Vuelvo a repetir algo importante.... **la pérdida de señal no tiene porqué ser una pérdida de comunicación total**.... pero **afectará a la velocidad, a la distancia a recorrer y a la tasa máxima de datos a transferir.**

Cuando hablamos de **interferencias** en una comunicación inalámbrica, nos referimos a *"otras señales"* que pueden interferir negativamente en las mismas, entre ellas están:

Señales de banda estrecha: Afectan a parte de del espectro de radiofrecuencias, es muy difícil diagnosticarlo (*y caro, un analizador de espectros puede costar cerca de los 5.000 euros, eso de los baratos*) sus orígenes pueden ser por muchos factores, desde solapamientos parciales de señal hasta interferencias generadas por malos funcionamientos o fraudulentos.... hay quien se construye *"aparatillos"* con los magnetrones de los microondas de casa para distorsionar las señales en la capa física y provocar un DoS a la red.

Todas las Bandas: El mayor enemigo... los ***bluetooth***, las tecnologías *bluetooth* saltan continuamente y muchas veces por segundo por la banda de los 2,4 Ghz y pueden provocar interferencias, también los microondas, los teléfonos inalámbricos (sobre todo los analógicos)

La Intemperie: niebla, excesiva humedad, relámpagos cargan la atmósfera y alternan (refractan) la señal a transmitir.

Bueno, hasta aquí ya está bien de *"problemas"*... pasemos a explicar eso de las bandas de radiofrecuencia....

Bandas de Radiofrecuencia

Como ya dije, la mayor parte de las bandas suelen estar autorizadas, esto es, son bandas en las que se necesita una licencia para poder emitir.

Las bandas sin licencia son las que nos interesan, estas son:

900 MHz, aunque originalmente se usaron para las transmisiones de datos, hoy en día prácticamente están relegados a algunos teléfonos móviles e inalámbricos, su tasa fiable de transmisión es de 1 Mbps pero permite recorrer distancias mucho mayores que las bandas 2.4 y 5 GHz, realmente las tasas de transferencia oscilan entre los 200 y 800 Kbps....

2.4 GHz, se corresponde con la norma ***802.11b***, que es la más extendida y que entrega una señal con una tasa máxima de 11 Mbps, aunque puede transmitir a ***1, 2, 5.5 u 11 Mbps***

5 GHz, se corresponde con la norma 802.11a, dispone de compatibilidad *"hacia atrás"*, es decir, ***es una tecnología de banda dual*** para dar soporte a dispositivos de 2.4 GHz de la norma 802.11b, su tasa máxima de transmisión es de ***54 Mbps***

Seguro que estás pensando que se me olvida "algo"... seguro que has oído hablar de 802.11g, de 802.11i, de 802.16.... de la banda UNII que transmite a 5,8 GHZ....

Bien.... **802.11g** dispone de un **tasa doblada**, es decir, el método de modulación de onda permite ratios mayores, ***hasta de 108 Mbps***, eso sí.... en detrimento de la distancia... sólo para unos 20 metros en espacios interiores y de unos 800 en espacios abiertos.

En cuanto a 802.11i, 802.16 y nuevas bandas de frecuencia, deberás esperar al final de este "*avance*" para saber más de ello... por el momento ya vamos servidos.

Como estarás intuyendo **hay una relación entre la frecuencia, potencia, distancia y tasa de trasferencia....**

Dejando aparte fórmulas y cálculos complejos (que ya vendrán para los mas frikis) digamos que:

A mayor frecuencia e igual potencia y ganancia, la distancia a cubrir disminuye.

Cuando más alta sea la frecuencia mayor necesidad de que los nodos estén alineados o sean visibles.
La frecuencia digamos que es la banda o conjunto de bandas a usar, la potencia será la fuerza de la señal y la ganancia la capacidad de recepción de la antena, esto es de andar por casa... ya os digo, elegí la forma "*simple*" de expresarlo en lugar de excesivos tecnicismos.

Lo explico.... supongamos una señal de 100mW (***mili watios*** *y no Watios como he leído por algún post... que si fuesen Watios achicharramos a todo bicho viviente*) a 5GHz se obtiene mayor tasa de trasferencia que a 2.8GHz pero "*alcanza*" la mitad de la distancia y mayor será la necesidad de que emisor y receptor estén alineados.

Una señal a 900 MHz, alcanza distancias mayores, es menos susceptible a cambios al atravesar obstáculos.

Claro, lo mejor será cuanto "mas mejor", es decir, tasas muy altas con distancias muy lejanas y velocidades muy rápidas con el mínimo de absorción, dispersión y refracción... pero eso es muy costoso, de mantener, de implementar y de fabricar....

Entonces... ***¿Qué se utiliza en lo que llamamos WiFi o Wireless?***

R: ***El Espectro Diverso. (SS, Spread Stream)***

Al igual que una radio "*convencional*" dispone de distintas bandas (AM, FM, MW….) otras radios utilizan determinadas bandas, frecuencias y tipos de modulación.

SS* es una técnica de modulación** que dispersa una señal por una banda ancha de radiofrecuencias, ahora en cristiano: ***Sacrifica el ancho de banda para ganar rendimiento... para una mejor relación señal-ruido. (mayor señal, menos ruido, tasa de datos mas alta)

En realidad lo que hace ***SS*** es dispersar la señal por una frecuencia mucho más ancha de la que necesitaría, con ello se crean menos interferencias y se ganan señales menos susceptibles al ruido.

Antes hablamos de banda estrecha... lo que hace una banda estrecha es amplificar la señal con la esperanza de que la información recibida sea correcta... es justamente lo contrario de la tecnología de espectro diverso (SS).

Para usar bandas de radio sin licencia es obligatorio usar técnicas de espectro diverso y tenemos dos opciones:

- **FHSS**, Que es **espectro diverso por salto de frecuencias**
- **DSSS**, que es **espectro disperso de secuencia directa**

Con ***FHSS*** las transmisiones "*saltan*" de una frecuencia a otra por patrones aleatorios, por ejemplo, de 2.42 a 2,40 a 2,42, a 2,44, a 2,43.... con esta técnica se sortean las interferencias causadas por banda estrecha, se obtiene una señal más clara.

Las tecnologías ***DSSS*** utilizan una secuencia (llamada ***secuencia de chipping***), lo que hace es que cada cero o uno a transmitir se envía como una secuencia de ceros y unos a su vez, por lo que aun cuando se pueda perder la mitad de la señal, el receptor puede reconstruir la cadena original, por tanto permite accesos a mayor distancia y tasas elevadas de datos.

FHSS permite **sólo tasas de 2Mbps** puesto que el receptor y el emisor deben utilizar el mismo patrón aleatorio de salto de frecuencia, por el contrario **DSSS es la tecnología que usa la norma 802.11b**, es decir, el estándar 802.11b proporciona una tasa de datos de tipo *Ethernet* a 11Mbps sobre DSSS.

Aunque los dispositivos basados en DSSS pueden interoperar con dispositivos FHSS hay problemas debido al diseño de los fabricantes, hasta podemos encontrarnos con dificultades si las tarjetas no son de "la misma marca", quizás nos olvidaremos del FHSS y nos centraremos en DSSS.

Normativas de LAN inalámbricas

Para variar el IEEE (Instituto de Ingenieros Electrónicos y Eléctricos) es el emisor de normas para las tecnologías inalámbricas, igual que para Ethernet (IEEE 802.3) o Token (802.5) establece las normas que han de cumplir los fabricantes de dispositivos, sólo que en comunicaciones WLAN (Lan Wireless) el conjunto de protocolos es 802.1x y derivados....

IEEE 802.11

La base de todos ellos lo encontramos en el IEEE 802.11 (digamos que es como "la madre" de todas ellas), los sufijos a, b, g, i, etc... son una especie de revisiones, complementos, mejoras, del protocolo 802.11

Este estándar define tres posibles niveles físicos:

1.- ***FHSS***, el salto de frecuencias
2.- ***DSSS***, Secuencia Directa
3.- ***Infrarrojos***

Encontrar dispositivos que operen únicamente en este estándar es difícil hoy en día, lo normal es encontrar 802.11b u 802.11g, tanto el estándar 802.11 como sus versiones b y g, operan en la frecuencia de los 2,4GHz.

Es un protocolo que opera en DSSS y se aplica a dispositivos que operan a 1 ó 2 Mbps y aunque pueden llegar a los 11 Mbps, no se consideran compatibles

IEEE 802.11b

El sucesor de 802.11 fue 802.11b, también es ***DSSS*** y puede operar a 1,2, 5.5 u 11 Mbps, estos dispositivos son compatibles con el anterior (802.11).

Aunque su tasa puede llegar a los 11Mbps, no te fíes... muchos de ellos dan problemas y terminan funcionando a 1 ó 2 Mbps, sobre todo cuando conectamos la red "sin cables" a la red cableada... ahí es dónde se producen los problemas...

IEEE 802.11a

Los dispositivos que operan en este protocolo lo hacen en **frecuencias de 5 GHz** y no de 2,4GHz como los anteriores, por tanto, no hay compatibilidad entre unos y otros... ten cuidado con ello, si usas dispositivos 802.11 u 802.11b junto con dispositivos 802.11a

Utilizando una tecnología de modulación llamada **OFDM** (***Multiplexión por división de tiempo ortogonal***), en bandas de frecuencia de los 5 GHz

802.11a puede transmitir a 54 Mbps aunque muchos fabricantes ofrecen velocidades de tasa doblada, pudiendo alcanzar los 108 Mbps, pero es tecnología "*de propietario*" y puede no ser compatible con otros estándares o ante dispositivos de distintos fabricantes.

Aunque debiera haber sido el sucesor lógico de 802.11b, no lo es como tal... ambos son incompatibles y la distancia a cubrir por ellos es la mitad que el de los estándar.

IEEE 802.11g

Proporciona el mismo rendimiento que el anterior (54 Mbps).... pero con compatibilidad *"hacia atrás"* utilizando una tecnología de modulación *OFDM* en bandas de frecuencia de los 2.4 GHz por lo demás, lo mismo del anterior.... 54 Mbps y **compatibilidad con el estándar 802.11 y 802.11b**

Seguramente será la tecnología deseada por todos ahora mismo... compatible con el estándar, compatibilidad, mayor rendimiento, mayor distancia.... el problema lo encontraremos en los drivers... sobre todo para LiNUX, ya veremos en sucesivas entregas la problemática de los ***Chipsets*** de los fabricantes... si lo que buscas es una mera conectividad es la mejor opción... pero si quieres "otras cosas" igual hay problemas con tu LiNUX.

IEEE 802.16

Fue aprobado hace unos pocos años nada más... es un protocolo que pretende cubrir un área metropolitana enterita... una ciudad.... **Utiliza frecuencias de 10 a 66 GHz** y como todo evoluciona... el año pasado apareció la revisión 802.16a

Dispone de un **alcance de unos 30 kilómetros** y **velocidades de 70Mbps**, las desventajas... te las imaginas... precio, banda con licencia y muy susceptible al ruido por causas meteorológicas.

IEEE 802.11i

Ciertamente este protocolo es una **variación de los anteriores pero con seguridad añadida**... ya hablaremos de los cifrados, de WEP, de EAP, LEAP, etc... la seguridad en las Wireless se basa en capa 2,

La expectativa de este protocolo es **sustituir a WEP**, pero no todos los fabricantes lo implementan y tampoco están definidas del todo sus funcionalidades... de momento pensaremos que 802.11x es lo que hay.... es más... ***TKIP*** que usa 802.11i ya ha sido vulnerado... todo se andará... tranquilos...

Dispositivos inalámbricos y Topologías

Para comunicar un PC mediante dispositivos sin cables, necesitaremos tarjetas de red con capacidades inalámbricas, las hay de muchos tipos... ***ISA, PCI, Cardbus, Pcmcia, USB***... imagino que todas estos conceptos los conoces... lo más habitual es encontrarnos con tarjetas PCI para equipos de sobremesa y con tarjetas *pcmcia* o *cardbus* para portátiles.

Es importante la diferencia entre *cardbus* y *pcmcia*, en ocasiones hablamos de *pcmcia* y englobamos *cardbus* en ello, su comportamiento, *drivers* y configuración son diferentes, las tarjetas *cardbus* son una especie de PCI en ranuras *pcmcia*... usan 32 bits y son más actuales que sus predecesoras.

Los dispositivos *usb* también llegan con fuerza, pero volvemos a lo de antes... tristemente los fabricantes *"se olvidan"* un poco de que existe LiNUX, proporcionan drivers y controladores para *Microsoft Windows*... hasta para *W98!!!!* Pero es la comunidad de usuarios de *LiNUX* los que en muchas ocasiones se buscan la vida... por eso para configurar muchos dispositivos "*modernos*" tenemos que hacer un auténtico vía crucis para que se soporten en este sistema operativo.

Ya lo desarrollaré mejor, el secreto está en el ***chipset***, en los módulos del ***kernel*** y en una configuración *"artesanal"*, sobre todo con tarjetas muy modernas hasta para alguna de ellas nos tendremos que olvidar de *LiNUX*... bueno, no para comunicarnos... más bien para usarlas

como herramientas de escaneo, ataques o similares, pero casi siempre pasa por "*el trauma*" de compilar el kernel y/o actualizarlo.

Si estás pensando en adquirir una tarjeta *wireless* para trabajar con *LiNUX* ANTES de comprar "*el no va mas*" piensa que igual te has de conformar con tener conexión y nada mas... no obstante explicaré la forma de cómo usar dispositivos en *LiNUX* usando los *drivers* que nos suministran para Windows, eso sí... sólo conseguiremos "hacer funcionar" la tarjeta y lograr conectividad... nos olvidaremos de usarla como herramienta de análisis o de intrusión.

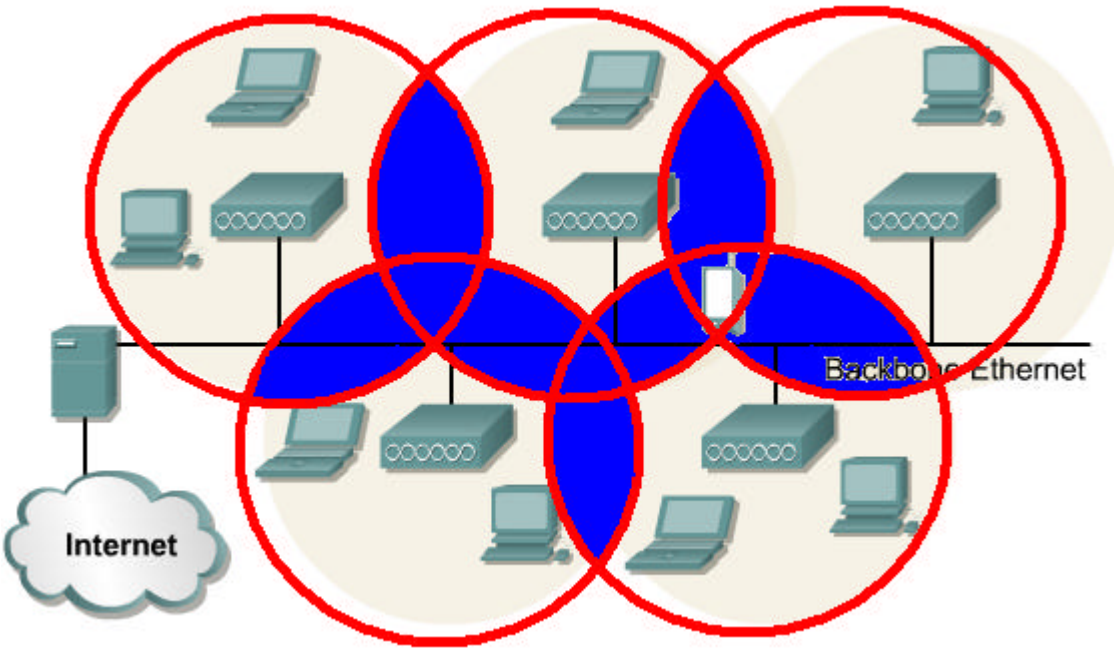
El caso es que para conectar dos Pc's bastará con disponer de una tarjeta inalámbrica en cada uno de ellos... si quieres conectar más de dos hosts, has de recurrir a un ***Access Point***, un ***Punto de Acceso (PA)***, que se comportará como un HUB inalámbrico que también se podrá conectar a la red de cable convencional y unir ambas redes.

Lo normal es disponer de un *PA*, sin embargo también es posible montarse un *PA* "manual" con dos tarjetas WiFi en un PC y ofreciendo capacidades de puente (*bridge*) para ello, de hecho una de nuestras prácticas será construir falsos puntos de acceso y derivar la comunicación hacia ellos... ***una especie de Man in the Middle aplicado a las WLAN.***

Dependiendo de la estructura y localización de los puntos de acceso, de las antenas, del tamaño de la celda y de la ganancia, podemos extender la WLAN desde unos metros hasta cerca de los 40 Kilómetros.

Lo más frecuente es que el alcance ronde los 150 metros, para distancias mayores hay que instalar varios PA con solapamiento y tránsito entre celdas, igual que hacen los operadores de telefonía... es como "*alumbrar*" una zona usando varios puntos de acceso, varias "*antenas*".

La celda es la conectividad de un área específica en las comunicaciones inalámbricas y el solapamiento es la intersección de la zona que "*alumbra*" con la celda de otro punto de acceso, mejor un gráfico....



Las zonas azules representan el solapamiento de áreas de cada Punto de Acceso.

El solapamiento óptimo es debe ser entre un 20% y 30%, porcentajes mayores provocarían que los hosts que "*pertenecen*" a un punto de acceso entren en estados de conexión/desconexión frecuentemente y se asocien a los puntos de acceso no deseados o que se queden "aislados" de la red.

Con porcentajes de solapamientos de 20-30 conseguiremos estados de conexión y desconexión transparentes al usuario (sin intervención del mismo) y sin interrupción del servicio.

BSS, IBSS y ESS

IEEE 802.11b dispone de dos modos de radio posibles: **BSS e IBSS**, **INCOMPATIBLES** entre sí ¡!!

BSS es el modo de operación en el que un punto de acceso actúa como puerta de enlace entre una red inalámbrica y una red cableada, los nodos que pertenecen a la red inalámbrica, los clientes de *BSS*, establecen la comunicación con el punto de acceso y éste, actúa como un puente entre las dos tecnologías de red.

ESS es un conjunto extendido de *BSS*, es decir, los servicios que se ofrecen cuando existen más de un punto de acceso de tal forma que los clientes pueden unirse a cada punto de acceso permitiendo la movilidad.

IBSS es un servicio básico entre iguales, en este modo dos clientes se pueden comunicar entre sí sin necesidad de que exista un punto de acceso, basta que ambos dispongan de tarjetas de red compatibles para lograr la comunicación, sería el equivalente a conectar dos *pc's* con tarjetas de red *Ethernet* mediante un cable cruzado, no se necesitan, *hubs, switches* ni otros dispositivos.

Además si uno de los clientes que operan en *IBSS* dispone de conexiones con otras redes, puede proporcionar acceso a las mismas actuando como reenviador o puente de conexión.

Es necesario configurar el protocolo *802.11b* para trabajas en *BSS ó IBSS*, pero no se puede trabajar en los dos modos de forma simultánea... o uno o el otro, pero no los dos a la vez.

Tanto *BSS* como *IBSS* admiten el cifrado y codificación **WEP** de clave compartida.

Lo más habitual es disponer de topologías con uno o varios *BSS* que brindan conectividad a sus respectivos clientes.

Una limitación de las comunicaciones *IBSS*, a parte de que sólo pueden comunicarse dos nodos entre sí, es que si usamos tarjetas de diferentes fabricantes, pueden existir incompatibilidades, si bien, con la expansión de las redes *802.11b*, cada fabricante han contribuido en la compatibilidad con el protocolo y podemos decir que hoy en día se certifica la conectividad de tarjetas que operan en *802.11b*.

Podrás encontrar también el modo *IBSS* como modo ***Ad-Hoc o Ad-Hoc Demo***, son otras formas de llamar al modo de operación *IBSS*.

Localización de Dispositivos

Al fin!!!! Bueno... tras este "*peazo*" de rollo, de siglas, de normativas, etc... vamos a empezar a entender DE VERDAD como se produce la conexión *wireless*... todo lo que vienen a continuación es muy, **MUY IMPORTANTE** que lo comprendas bien, además es muy sencillo.

No es que todo lo anterior no haya sido importante, pero no deja de ser "*culturilla*" y aclaraciones, sin embargo a partir de aquí.... **FUNDAMENTAL**.

Proceso de conexión

Cuando un cliente es activado en una WLAN, éste empieza escuchando para localizar un dispositivo compatible al conjunto de protocolos que implementa su tarjeta.

Este proceso de escucha se denomina ***escaneo*** y puede ser de dos tipos:

- **Activo:** El cliente envía una solicitud de prueba que contiene un ***SSID/ESSID*** (**Servicio de Identificación**) de la red a la que pretende unirse. Si existe un Punto de Acceso con el mismo *SSID*, le reenvía una respuesta a su prueba y el cliente se asocia y se autentica en la red.

- **Pasivo:** El cliente sólo escucha y busca unas tramas de datos especiales llamadas **becons o tramas de administración de balizas**, esas ***beacons*** son emitidas por el Punto de Acceso y contienen el *SSID*, entonces el cliente intenta unirse a la red usando el *SSID* proporcionado en la baliza y si el proceso se completa, el cliente es asociado y autenticado.

Como ves... seguridad poca... porque "*aparentemente*" cualquiera que llegue con su portátil cerca de un punto de acceso y lo configure en modo pasivo terminará por "*entrar*" en la red.

Por otra parte, *si los chicos malos se vuelven peores...* pueden lograr que equipos lícitamente asociados y autenticados se disocien utilizando señales mal intencionadas o intentando que la el punto de acceso cambie la fuerza de sus señales.

También, si los clientes de la red ya están asociados y "*entramos*" con un nuevo punto de acceso, esos clientes se asociarán al nuestro... vamos que hay para mucho juego....

Claro... no vayas a pensar que para todo esto se necesita acudir a la oficina con un hub, un punto de acceso, una antena, baterías, etc... nos basta con un portátil y dos tarjetas pcmcia o cardbus.

Aclaremos más sobre los estados posibles.

Primero hay que recordar que **la autenticación WLAN tiene lugar en la Capa 2 del modelo OSI**, aunque parezca mentira, el conjunto de protocolos 802.1x no es realmente un protocolo inalámbrico, sencillamente describe un método de autenticación de puertos que se puede aplicar a cualquier red, pero bueno... esto no es lo que interesa en estos momentos.

Lo que importa y sí que es importante es que recuerdes que **la autenticación es del dispositivo, no del usuario....** es física y de enlace a datos.... capas superiores no intervienen, por tanto con dispositivos configurados a tal efecto y ante una red "*desprotegida*" las travesuras pueden ser de máximo riesgo para el pobre administrador despreocupado o que se fía de sus conexiones....

La autenticación puede ser un proceso nulo, este es el caso de puntos de acceso y tarjetas de red sin configurar (nada mas salir del embalaje), sencillamente se envía la trama *beacon* y se produce la autenticación.

La asociación llega después de la autenticación... de la autenticación positiva, claro... y en ese estado el cliente puede usar los servicios que brinde la red.

Por tanto tenemos **tres estados** de autenticación/asociación:

- **Desautenticado y disociado:** El cliente está desconectado de la red y no se asoció con el Punto de Acceso

- **Autenticado y disociado:** El cliente ha sido autenticado pero todavía no se asoció al punto de acceso.

- **Autenticado y asociado:** El cliente puede transmitir y recibir datos por la red.

En cuanto a **los métodos de autenticación**, IEEE 802.11 define dos formas posibles:

- **Autenticación abierta:** Bastará con que coincidan los *SSID* del cliente y punto de acceso para que sea un nodo autenticado y asociado.

- **Clave compartida:** Requiere el **uso de WEP** que es un protocolo de cifrado con claves de 40 a 128 bits, cada dispositivo (incluido el punto de acceso) dispone de una contraseña estática que se envía o recibe, se compara y si coincide se autentica y se asocia.

  Proporciona mayor seguridad... pero *WEP* es vulnerable... y mucho.... aunque se precisa de cierta cantidad de tráfico *esnifado* para hallar la clave y craquearla... te adelanto... usaremos herramientas que provocarán que el punto de acceso emita mas balizas de la cuenta.... extraeremos la clave cifrada y la craqueamos... o mejor... la pasamos *"con audacia*" y ZAS!!! En la red... *nos ahorraremos el incordio del crack... que siempre es lento....*

También hay que hablar de canales... los canales son "*pequeñas*" variaciones de la frecuencia, los dispositivos inalámbricos pueden configurarse para que hagan un barrido de los canales disponibles o forzarles a usar uno en concreto.

Si hacemos esto último, TODOS los dispositivos deberían usar el mismo canal, de otro modo nos quedamos sin conexión... el *roaming* es la capacidad que tienen los dispositivos *wireless* para *escanear* señales por todos los canales disponibles de su banda de frecuencia.

Canales comunes:

Canal 1	2.412 GHz
Canal 2	2.417 GHz
Canal 4	2.427 GHz
Canal 5	2.432 GHz
Canal 6	2.437 GHz
Canal 7	2.442 GHz
Canal 8	2.447 GHz
Canal 9	2.452 GHz
Canal 10	2.457 GHz
Canal 11	2.462 GHz
Canal 12	2.467 GHz
Canal 13	2.472 GHz
Canal 14	2.484 GHz

Formato de Tramas

Como ya sabemos... al menos así me esforcé en el Taller de TCP/IP, ***sin conexión física no hay conexión lógica...*** *sagrada frase....*

Las tramas *Ethernet 802.3* utilizan un formato específico... las tramas 802.1x utilizan otro... sin embargo para poder conectar la red inalámbrica a la red de cable, se mantienen ciertas coincidencias para que ambas redes sean compatibles sin necesidad de encapsular unas tramas en otras... es por ello que muchos autores llaman al conjunto de protocolos 802.11 *Ethernet inalámbrica*... pero eso es una falacia... no es verdad.

En 802.11 existen tres tipos de tramas:

- Tramas de Administración, que contienen:
  - Solicitud/respuesta de asociación
  - Solicitud/respuesta de pruebas
  - Beacons
  - Autenticación
- Tramas de control
  - Solicitud para enviar RTS (Request to Send)
  - Listo para enviar (CTS, Clear to Send)
  - Acuses de recibos
- Tramas de datos que contienen eso... los datos a enviar.

De todas ellas **SOLO la trama de datos es similar a las tramas Ethernet** de cable (802.3) y es eso.... similar... no igual.

Las tramas inalámbricas pueden transportar 2346 bytes (es el *MTU*, la unidad máxima de transmisión) mientras que las tramas Ethernet 802.3 el MTU está limitado a 1518 bytes, si bien, sólo se usan 1500

Es por ello que las tramas *WiFi* están limitadas a 1500 bytes, así se consigue una compatibilidad con *ethernet* si necesidad de otros dispositivos como *routers*.

Cuando expuse en el apartado las Normativas IEEE, me repetía constantemente algo fundamental...esas velocidades, esas tasas de transmisión son.... son cuanto menos engañosas, en este apartado encontraremos los motivos.

La Radiofrecuencia es un medio compartido y **los puntos de acceso actúan como un HUB**...

ya ... y???

Pues que las señales de unos y otros "*chocan*" **colisionan** constantemente... *y qué ocurría en Ethernet cuando se producía una colisión???*

Pues que las tramas (los datos a transmitir) se destruyen, se envía una señal para que todo *quisqui* se calle o deje de transmitir y se espera un tiempo aleatorio antes de poder volver a hacerlo, en esto se basa el algoritmo ***CSMA/CD que usa Ethernet***.

Esto significa que **si hay muchos nodos, habrá muchas colisiones** y si los paquetes colisionan se han de retransmitir por que lo que colisionaron se descartan... por tanto la velocidad no es la que nos pintan.... *si para enviar 50 megas tengo que repetirlo 2500 veces, tardaré mas que si lo repito una sola vez... es de cajón... y mientras yo envío (me apropio del*

medio) y los otros no pueden hacerlo, esto son microsegundos... pero muchos microsegundos hacen minutos, horas, días....

Las Wireless usan un protocolo llamado CSMA/CA (parecido al de Ethernet) por lo que si le añadimos, el protocolo, las veces que se han de repetir los datos tras las colisiones, el uso de un medio compartido, el cifrado, las balizas, las tramas de control y administración, los acuses de recibo, las interferencias, el ruido, los obstáculos y toda la problemática vista hasta ahora.... nos quedamos que en una red sin cables ***la eficiencia no llega al 50% del ancho de banda***...

Dicho de otro modo... *si usamos 802.11b (11Mbps) nos daremos con un canto en los dientes si la tasa de trasferencia real llega a los 5Mbps.*

Además... **cuando la señal pierde potencia, se invoca a una señal llamada *ASR*** (*Selección de Tasa Adaptativa*) **que obliga a disminuir la tasa de transferencia**.... por lo que en muchos casos, aunque dispongamos de conexiones de 54Mbps, podemos llegar a disponer tan sólo 1Mbps.... tasas menores suponen la pérdida de conexión.

Introducción a la Seguridad o inseguridad Wireless

Ya he contado lo frágil que puede llegar a ser un WLAN mal administrada... también puede comprometerse aunque esté bien diseñada o protegida... nada es seguro al 100%.

Este apartado es sólo otro avance más de lo que vendrá.... una aperitivo y una serie de consejos útiles para los que ya tengáis en marcha alguna WLAN.

El primer nivel de seguridad de una Wireless radica en **proteger la propia onda**.

Con una red de cable esto es más sencillo, para que un intruso "*esnife*" nuestros datos tendría que acceder a nuestras dependencias y conectarse a una boca libre del switch o hub... pero en una wireless no necesita ni eso... basta con estar cerca del punto de acceso para empezar a escuchar el tráfico.

Por tanto **una de las primeras medidas es restringir el alcance de nuestras ondas**... si en nuestra red los nodos están a tan sólo 15-20 metros del punto de acceso para qué usar alcances superiores.... a menos que deseemos que toda la finca y los de la de enfrente participen de nuestra red, para nada...

Pero cuando se han de cubrir distancias mayores, por ejemplo mediante el uso de antenas de ganancia para interconectar puntos lejanos, entre edificios, etc... no estaremos a salvo de que un "*husmeador*" desde la esquina de nuestra oficina lo intente....

Para ello **podemos usar varias alternativas:**

La primera es WEP, que no es la panacea pero algo dificultará el proceso, *WEP* usa **algoritmos RC4 de cifrado simétrico** (la misma clave se usa para cifrar y descifrar) pero como ya dije antes... WEP hace tiempo que está reventado, lo haremos.

Otras opciones consisten en **usar servidores de autenticación como Radius o AAA** mediante el uso de **protocolos EAP o LEAP** (es un EAP de Cisco). Tampoco es del todo seguro, *si es que.... esto es una guerra*

También debemos **asegurarnos que la red esté cerrada**, vamos **que no se permitan las autenticaciones abiertas** que vimos antes... es decir, que todos aquellos que quieran comunicarse usen SSID.

Muchos Puntos de acceso proporcionan mecanismos de **filtrado de MAC's**, recuerda que la MAC es la dirección física de la tarjeta, la que nos suministra el fabricante y aunque se puede cambiar a voluntad en la mayor parte de las tarjetas de red, es otro obstáculo mas... de alguna manera le explicaremos a nuestro punto de acceso que sólo determinadas direcciones MAC, con SSID válidos y WEP habilitado puedan comunicarse... si además le añadimos que la autenticación la efectúa un servidor RADIUS en lugar del propio punto de acceso, pues mejor.

Pero.... **si te fijas en los contenidos del Taller en la sección de ataques**.. hay cosas como estas:

- Ruptura de cifrados: WEP, LEAP y EAP
- Saltarse los ESSID, Filtrados de MAC y protocolos
- Fuerza bruta contra los cifrados. Cracker WEP

Vamos que cuando *"toque"* esas medidas comentadas serán insuficientes....

Lo mejor para asegurar una Wireless si lo que prima es la seguridad y la confiabilidad... es tunelizar las comunicaciones mediante **una VPN** porque además de todo lo anterior, las VPN permiten la autenticación de usuarios (no de dispositivos), cifran el tráfico (todo el tráfico) no sólo las claves y autentican los datos garantizando la integridad de los mismos... además mediante una VPN también conseguiremos una autenticación mutua de dispositivos origen y destino.

Pero no te confíes.... recuerda otro punto de este Taller:

- Pruebas de seguridad contra VPN y PtPP

Por lo menos lo intentaremos... asaltar una VPN.... eso es bueno, sin duda....

Otro peligro que hay que cuidar con esmero es cuando usamos Puntos de acceso con **servicios NAT y DHCP habilitados**... si no los aseguramos bien, será una fuente de problemas... y una fuente de información para los intrusos, vamos que asegurar una *Wireless* no es tarea fácil.

También deberíamos usar herramientas para monitorizar el tráfico, IDS especializados, etc... con ello no conseguiremos parar el ataque, pero al menos lo detectaremos y si somos minuciosos y meticulosos, sabremos tanto del atacante como él sabe de nosotros mismos...

Bien pues todo esto y más es lo que desarrollaré... con vuestra ayuda y con vuestras propias experiencias, mi/nuestra idea es que este sea un Taller VIVO, en el que todos podáis participar, que expreséis dudas, eso sí, oor favor.... que no sean del tipo ¿qué puedo usar para ver el correo del vecino de abajo que tiene un router WiFi? Porque si después de todo lo que está por venir no sois capaces de hacer eso mismo sin preguntar.... mejor me dedico a la cosmética o a vender repollos....

Hasta el próximo,