ANTENAS

Anteriormente ya hemos hablado algo de lo que son y para qué nos pueden ser útiles las antenas, profundizaremos un poquito en esta sección y describiremos las más comunes.

Dos son los factores que determinan lo importante que puede llegar a ser una antena:

- **La ganancia**
- **La zona de cobertura**

Existen **otros factores** importantes a la hora de utilizar antenas, como es la **polarización, direccionabilidad, montaje,** etc.. poco a poco iremos descubriéndolas.

El fabricante de la antena debería adjuntarnos sus características técnicas y especificaciones junto con un plano o diagrama de la zona de cobertura...porque uno de los principales cometidos de la antena es ser capaz de irradiar las ondas al exterior o de recibirlas.

Pero.. ¿por dónde? ¿hacia a donde?, es decir, las ondas de radio salen de la antena ¿hacia arriba? ¿Hacia abajo? ¿A la izquierda?¿A la derecha? ¿En todas direcciones?

Son preguntas "*tontas*", pero son preguntas que todas nos hacemos alguna vez.... *si mi PC está por encima de la antena será capaz de captar las ondas o de transmitirlas?*

También existen tarjetas *wireless* que incluyen conectores para acoplar una antena... seguro que nos viene otra pregunta a la cabeza... ¿***necesito realmente una antena***?

Y si es así.... mi tarjeta ya tiene una incorporada... o es una *pcmcia o cardbus* de un portátil... *¿realmente necesito otra antena?*

Por otra parte... ***también existe guía ondas***, *¿qué es eso? ¿Es una antena?*

Y por si fuera poco posiblemente hayas oído hablar de ***pigtails***, de ***antenas caseras*** o del tipo brico-antena...

Seguro que te asaltan más preguntas... *¿y si mi antena no es suficiente para enviar o recibir la seña?, ¿necesito otra? ¿Más grande? ¿Más pequeña? ¿Existen amplificadores para las antenas?*

Más preguntas...

¿Por qué existen antenas del "tipo palo" o lineales, parabólicas, otras que parecen banderitas, unas muy altas otras menos...? ¿Cual es la mejor? O mejor dicho, *¿cual de los diferentes tipos de antenas es el que mejor se adapta a mis necesidades?*

Siguen siendo preguntas que parecen simples, y es que ***de esto se trata en este apartado, dar respuestas simples a preguntas sencillas*** sin necesidad de hacer un post-grado en telecomunicaciones, sin necesidad de conocer profundamente leyes físicas, complicadas fórmulas o cálculos matemáticos... queremos cosas claras, sencillas y que las entendamos todos, aunque estas explicaciones adolezcan de cuestiones más técnicas.

Vale pues vamos a ello.

Antenas y Guía ondas

Una antena es un sistema conductor metálico capaz de radiar y recibir ondas electromagnéticas, se utiliza como la interfase entre un transmisor (la tarjeta *wireless* en nuestro caso) y el espacio libre o el receptor (que puede ser otra tarjeta equipada con su respectiva antena, el punto de acceso o cualquier otro dispositivo que permita recoger esas ondas)

Es un dispositivo recíproco pasivo, pasivo porque no puede amplificar la señal aunque **dispone de ganancia** y es recíproco por que **puede emitir y recibir.**

Un guía de ondas es un tubo metálico conductor por medio del cual se propaga energía electromagnética de alta frecuencia y que por lo general se sitúa entre una antena y un transmisor, un receptor, o ambos.

Una guía de onda, se utiliza solo para interconectar eficientemente una antena con el transceptor, que es el que se encarga de transmitir la señal al medio.

La famosa ***"antena construida con una lata de Pringles***" o con latas de refrescos, son en realidad *guía ondas* más que antenas, aunque también se pueden construir *guía ondas* rectangulares que se pueden comportar como antenas *omnidireccinales* o *sectoriales*.

Una antena se tendrá que conectar a un dispositivo capaz de transmitir y deberá radiar el máximo de potencia posible con un mínimo de perdidas y se deberás adaptar la antena al transmisor para una máxima transferencia de potencia, que se suele hacer a través de una línea de transmisión, por lo general un cable.

Este cable también influirá en la adaptación, debiéndose considerar su ***impedancia*** características, ***atenuación*** y ***longitud***

Una definición simple:

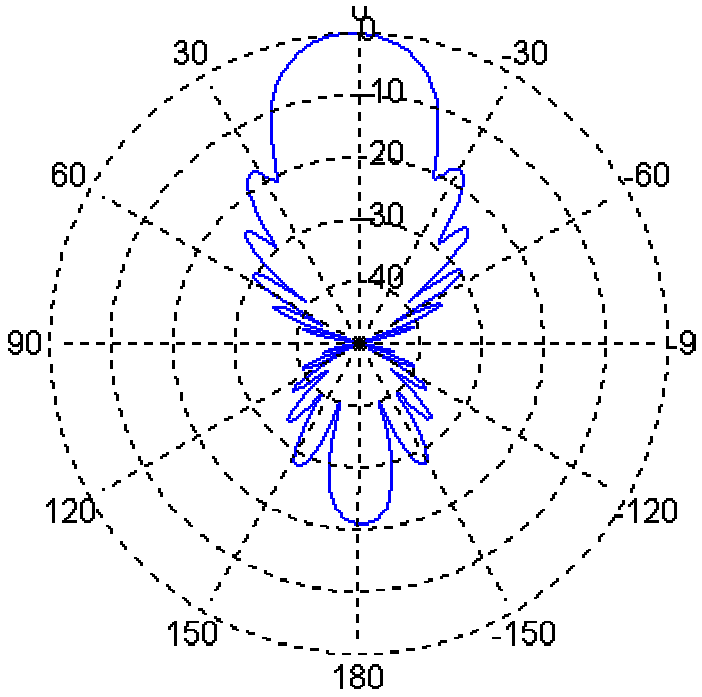
> *No por tener una antena más larga logramos radiar mejor, lo único que conseguimos es variar el diagrama de radiación (la zona que cubre la antena) y la impedancia que presenta, que no es otra cosa que la resistencia ofrecida para enviar la señal.*

Nota: Al ***diagrama de radicación*** se le llama también ***espectograma*** y en otras ocasiones en esta sección me refiero a ***patrón de radiación o de cobertura***, ***alcance***, ***zona iluminada, zona de cobertura, haz de radiación, ancho del haz,*** es la misma cosa con distintos nombres.

Esa relación entre impedancia, transmisor, corriente que pasa a la antena, pérdidas que produce, etc. es lo que se llama ***frecuencia de resonancia***. Aplicar **corrientes excesivas, calor, en una antena provoca grandes pérdidas de señal.**

Por eso **la antena y el equipo que transmite deben guardar una relación con la potencia a lo que lo hace, la longitud de la antena, su montaje, sus conectores**, etc... si rompemos esa relación podemos generar pérdidas de señal, repito de nuevo, ***no por tener una antena más grande seremos capaces de disponer de una mejor señal.***

Las antenas "*cubren*" un ***área de alcance***, lo que hemos llamado **zona de cobertura o ancho del haz,** gráficamente sería algo así:



Este patrón de cobertura pertenece a una antena UHF de irradiación vertical (polarizad), vamos la de "la tele" ;)

Es un ejemplo, cada tipo de antena tiene un patrón diferente y el fabricante nos deberíam proporcionar un gráfico con el patrón de radiación de la antena en concreto.

Como ya se ha dicho **una antena es pasiva**, pero **dispone de cierta ganancia** y esa ganancia se mide en ***dBi (decibelios de un dispositvo radiador isotrópico)***

Ese "*palabro*", *dispositivo radiador isotrópico*, es un dispositivo imaginario que emite sus ondas en todas las direcciones.

Como **las antenas son pasivas**, no añade potencia a la señal, **el aumento de la ganancia se consigue "enfocando" las ondas que se emiten en alguna dirección**, es decir, un haz más estrecho con el objeto de conseguir un mayor alcance... como muestra el dibujo anterior, las zonas azules serían el haz de la antena, no irradia en todas las direcciones por igual.

Imagina un Faro de un puerto, una linterna, el haz de luz se "enfoca" en una dirección, no se dispersa como lo haría una bombilla convencional, al enfocar la luz ganamos en alcance y perdemos por los laterales, algo así pasa con las antenas y las ondas... ;)

Esto lo hemos comprobado en numerosas ocasiones en casa, al "mover" la antena de la televisión, conseguimos una mejor o peor recepción, verdad?

Pero ojo!!!, sobre plano parece fácil entender el patrón de radiación... sólo que el mundo real es en tres dimensiones, no se te olvide, no sólo hay ancho y alto... :P

Es por ello, que las antenas se suelen “catalogar” por sus patrones de radiación y por el ancho del haz que emiten o reciben, esta es una de esas clasificaciones:

1.- Antenas omnidireccionales

- Montaje en mástil
- Montaje en Pilar
- Plano de tierra
- Montaje en techo

2.- Antenas Parcialmente direccionables

- Tipo parche
- Panel
- Sectoriales
- Yagi

3.- Antenas totalmente direccionables

- Parabólicas
- Satélite

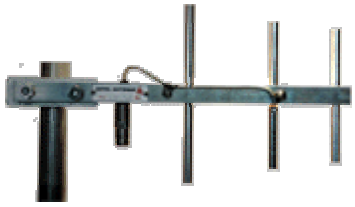
Las antenas omnidirecconables disponen de una zona de cobertura horizontal de 360 grados y consiguen la ganancia limitando el ancho del haz vertical, evitan que la radiación se disperse hacia abajo o hacia arriba.

Imaginate un “palo” grande y alto en el que introducimos un enorme Roscón de Reyes :P. Ese es el aspecto del *patrón de radiación* en antenas *omnidireccionales*, son útiles cuando se quieren abarcar zonas amplias y se desconoce de dónde provienen los clientes, con el inconveniente que también recibe el ruido en todas las direcciones.

Las hay de todos los tamaños, desde postes de varios metros y pequeño grosor hasta de pocos centímetros de altura, para varias, influye el precio.... mayor ganancia más cara.

Las antenas parcialmente direccionables disponen de un *patrón de cobertura* como si fuese una burbuja que se extiende entre los 60 grados y 120, parecida a la ilustración del *espectograma* de la antena UHF que se mostraba antes, se usan para cubrir espacios “rectos”, una calle, un pasillo, etc. Y si colocamos varias antenas de este tipo en círculo tenemos una *omnidireccional* con más ganancia y ancho de banda... solución más cara pero de mayor rendimiento.

La excepción que rompe la regla de las antenas parcialmente direccionables son las ***antenas Yagi,*** es decir, lo dicho en el párrafo anterior lo aplicamos a las antenas de tipo parche, sectoriales y de panel... **las antenas yagi forman una haz de radio más estrecho y por tanto con más ganancia,** se usan para interconectar edificios. Se parecen mucho físicamente a las antiguas antenas de televisión, esas que parecen banderitas, y su ancho de haz oscila entre los 15 y 60 grados



Las antenas de alta direccionalidad emiten un **patrón de radiación en forma de embudo**, bueno, los libros y documentación que leas dirán que son de tipo cónico muy estrecho, pero este es un breve homenaje a ***Wadelbertia*** :P

Son capaces de alcanzar grandes distancias y de gran calidad en su señal, y debido a su alta ganancia son capaces de atravesar objetos sin pérdidas importantes en la relación señal ruido.

Amplificadores de Radiofrecuencia

Las antenas consiguen ganancia pasiva enfocando su energía en patrones de radiación, **los amplificadores consiguen ganancia activa mediante la suma de potencia continua.**

También existen **dos tipos fundamentales de amplificadores**:

- ***Unidireccionales***: sólo aumentan la potencia de transmisión.
- ***Bidireccionales***: que incrementan la potencia de transmisión y sensibilidad de recepción.

Ambos pueden disponer de **ganancias fijas o variables** y se usan para compensar las pérdidas en la señal convencional o para resolver las pérdidas que se sufre en el cable que conecta la antena con el dispositivo transmisor-receptor.

Piensa en la antena de casa... la de la "tele", seguramente hay amplificadores porque la antena está en la azotea de una casa con doce plantas y vives en la primera... el cable que une tu televisión con la antena es muy largo y la señal sufre atenuación y pérdidas de ganancia.

¿Necesitamos amplificadores y antenas?

Te lo imaginas.. depende :P

Bueno, está claro que si deseo cubrir grandes espacios, comunicar edificios o naves circundantes, incluso una misma nave industrial de techos muy altos y grandes zonas a cubrir, etc.. es muy probable que precise de antenas específicas y de amplificadores de señal.

Pero la pregunta y título de este apartado va más dirigida a que si desde el punto de vista de la seguridad (ataque/defensa) ***¿necesitaremos el uso de antenas y amplificadores para descubrir redes, etc...?***

Tanto unas como otros dan bastante juego, **veamos las dos perspectivas, la del atacante y la del defensor:**

Uso de antenas y amplificadores por el atacante

La primera ventaja es que **ofrecen distancia**, es decir, podemos estar más lejos sin necesidad de "*jugárnosla*" en la puerta de la oficina o en el rellano de la escalera.

Otra ventaja es la **calidad de la señal**, a **mayor ganancia y menores pérdidas, mayor alcance y mejor ancho de banda,** recuerda que las wireless pueden negociar la velocidad y bajar el rendimiento de 54Mbps a 1 ó 2 Mbps si hay excesivo ruido.

En el wardriving, se usan antenas *omnidireccionales* de montaje magnético, este tipo de antenas el plano de tierra es el propio coche ;)

Sin embargo recuerda una cosa, **cuanto mayor sea la ganancia, más delgada será la zona de cobertura**, es decir, que podemos pasar por alto máquinas que se encuentren por encima o por debajo de nuestra antena, es por ello que suelen utilizarse antenas parcialmente direccionables cuando se desea "*barrer*" un área y en caso de querer estar más ocultos, pues amplificadores.

Claro, imaginate el tinglado... el portátil, mejor DOS portátiles, la antena, una batería para alimentar el amplificador, el amplificador, vamos... como los cazafantasmas, por ello es "tan popular" el wardriving, el coche nos suministra espacio, medio de transporte de todos lo necesario y si me apuras... velocidad, velocidad para salir pitando si te detectan :P

Otra cuestión básica por parte del atacante consiste en **identificar las antenas de su objetivo**, observando su montaje y forma es posible hacerse una idea del tipo de antena y hasta de su ganancia y patrón de radiación.

Uso de antenas y amplificadores por el defensor

La colocación correcta de las antenas **delimita el perímetro a cubrir** y por tanto reduce el espacio que le quedará a un alma "*curiosa*" para husmear el tráfico... recuerda... **la primera máxima de seguridad en Wireless es proteger la onda.**

Usando **combinaciones de antenas, se puede triangular la posición del atacante** y descubrirlo, claro... siempre que el atacante transmita algún dato... si sólo escucha, no será posible su localización por triangulación.

También hay que guardar cuidado con la exposición de las antenas, no sólo en mantenerlas lejos de ojos indiscretos, también de la extensión de sus lóbulos laterales... podrían cubrir zonas no deseadas.

Las antenas *omnidireccionales* son útiles para monitorizar un área específica, buscar puntos de acceso piratas o ilícitos, tráfico no autorizado, sospechoso y hasta interferencias.

También podemos usar amplificadores de ganancia variable para ajustar la distancia máxima a la que "*los chicos malos*" se pueden situar, sobre todo para estimar el alcance medio de ataques DoS y distorsiones de señal.

En resumen, **las antenas no proporcionan más señal de la que reciben**, eso lo consiguen los amplificadores, **las antenas dirigen la señal en una dirección**, como lo hace una linterna, en un "haz de luz" llamado patrón de radiación.

Siguiendo con el ejemplo de la linterna, las antenas no aumentan la luz que sale de "la bombilla", sino que enfocan ese haz de luz, cuanto mayor sea la ganancia, mayor será el alcance en la dirección que apuntamos.

Cada tipo de antena tienen su propia aplicación, no hay soluciones "universales" y hay que elegir bien el tipo de antena para que se cubran las necesidades particulares, ni la mejor es la mejor solución, ni es la más cara.

Tampoco te dejes engañar por "*sus formas*" las hay que se asemejan más a una alarma que a una antena como tal, las hay planas pegadas al techo o en una pared, o un simple "*palo*" que baja del techo unos centímetros...

Aunque este enlace no hace referencia exclusiva para wifi y las antenas que estamos hablando, al menos podrás comprobar los distintos patrones de radiación según diferentes antenas de televisión, wi-fi, etc..

http://www.upv.es/antenas/catalogos/antenas_televes.pdf

Ahora nos asalta otra pregunta... ***¿dónde conectamos la antena?***

Conectores, Cables y Adaptadores Pigtails

Los cables son una de las fuentes de mayor pérdida en redes inalámbricas, *recuerda el ejemplo de la antena en el tejado de una casa de muchos pisos y la televisión del vecino de la primera planta.*

Si hay que tender cable entre el receptor y la antena**, usa cables con el menor nivel de atenuación, los cables de antena suelen indicar el número de decibelios de pérdida por cada 100 metros.**

Los conectores también son otra fuente de pérdida de señal, un conector mal hecho o defectuoso puede dar al traste con las comunicaciones, tanto los defectos en el cable, como en los conectores, son difíciles de medir y de descubrir, es por ello que siempre y cuando sea posible, usaremos conectores y cables industriales ya "*montados*".

Otro problema derivado es la impedancia, el cable debe tener la misma impedancia que el resto de componentes, en especial con la antena, el más habitual es de ***50 ohmios***.

Lo natural es que tanto los conectores como el cable como la antena dispongan de unos conectores determinados, no obstante, puede darse el caso de tener que **usar adaptadores**, es decir, una especie de roscas que unen los dispositivos con su antena y/o cableado, **cuando se usan adaptadores suelen existir pérdidas entre 2 y 3 decbelios**, eso supone una reducción de la mitad de la potencia y sensibilidad en la recepción.

Los pigtails son adaptadores de los fabricantes de dispositivos *wireless* para que puedan conectarse a antenas comunes, como si fuese un adaptador de clavijas o enchufes, y además de costar un pico, se rompen fácilmente.

Así tenemos conectores *pigtail* de CISCO compatibles con tarjetas *aironet*, *LUCENT* compatibles con tarjetas *ORiNOCO* y *Hermes*, etc... y por otra parte, **no todas las tarjetas wireless disponen de conectores para antenas**, en PCI es habitual, pero las *pcmcia* y/o *cardbus* que se conectan a los portátiles es menos frecuente.

Luego si quieres usar una antena con un portátil equipado con *una pcmcia wi-fi*, tendrás que comprar una tarjeta con su conector y en su caso, con el *pigtail*... son más caras, como no... ya hablaremos de ellas en el apartado de los *chipset*, pero para que te hagas una idea, una *pcmcia* "*normal*" puede constar una media de 40 euros, *una Aironet de CISCO, Xircom o 3Com* con conector, *pigtail*, etc... más de 250 euros.

El Chipset. El factor clave de la elección.

Es de todos conocido que en el mundo *LiNUX* los *drivers* para que nos funcionen nuestros dispositivos suelen obtenerse por el tipo de componente o ***chipset*** principal del dispositivo más que por el fabricante del mismo.

Hay que dar un *pequeño tirón de orejas a los fabricantes*, se olvidan de otros Sistemas Operativos que no son Microsoft y no sólo hablo de *LiNUX*, también de *Novell*, de *MAC-OS*, etc.. si os aventuráis en ir a la tienda y comprar la primera tarjeta que os parezca "*buena*" os podréis encontrar con una auténtica peregrinación por la Web buscando cómo configurar la dichosa tarjeta en vuestro *LiNUX*.

Con *Windows*, no hay muchos problemas, prácticamente todos los fabricantes suministran *drivers* para sus tarjetas y los sistemas operativos de *Microsoft*, no es el caso de *LiNUX*, y no es que haya que usar *LiNUX* para "*atacar*" o monitorizar una red inalámbrica, es que muchos controladores de Windows no ofrecen las posibilidades que nos brinda *LiNUX*.

Es más, el mismo fabricante puede ofrecer modelos de tarjeta con diferente ***chipset***, lo cual implica usar distintos *drivers*, y un problema añadido, es cuando queremos usar tarjetas *pcmcia* wi-fi en portátiles, la mayor parte de las que hay en la actualidad no incluyen compatibilidad con *LiNUX*, ni tan siquiera usando la última revisión del *kernel*.

Es por ello, que si piensas usar *LiNUX* y *Wi-Fi*, presta especial atención a todo lo que aquí voy a decir, te ahorrarás dinero y mucho tiempo.

Además, no se te olvide comprobar el estándar que usa, **IEEE 802.11a es incompatible con el resto** a menos que el fabricante implemente en sus ***chipset*** la denominada banda dual, de todo esto y de muchas otras cosas más hablaremos en esta sección.

Los chipsets más comunes son:

- Prism
- Cisco Aironet
- Hermes/Orinoco
- Atheros
- Symbol
- Broadcom
- Atmel
- Realtek
- ADM
- TI

Y otos más "*peculiares*" como son los que incorporan muchos portátiles, **chipset toshiba, intel, Ralinktech** y seguro muchos otros que existirán.

Es importante reconocer el chipset que incorpora la tarjeta como ya se dijo antes y no sólo por la funcionalidad en *LiNUX* u otros Sistemas Operativos, si no también porque muchas de las herramientas que usaremos se diseñaron para usarse con ***chipsets*** específicos, hasta incluso una misma herramienta se distribuye para usarse "*en versiones*" dependiendo del ***chipset*** que se disponga.

Como podréis entender no puedo (y tampoco se necesita para lo que nos ocupa) describir uno por uno cada ***chipset***, sus especificaciones, sus características técnicas, sus compatibilidades, etc.. no serviría de mucho esquemas electrónicos ni nada de eso, simplemente con averiguar el modelo que usa la tarjeta elegida será suficiente.

Desgraciadamente cuando nos acercamos a la tienda y curioseamos por entre las cajas y características de la tarjeta que guarda dentro, no encontramos el ***chipset***... *al menos yo no he visto absolutamente ninguna que lo indique, por tanto necesitaremos "una chuleta" de los principales fabricantes, el soporte que ofrece y el chipset que incorpora la misma*.

Este enlace es un ejemplo de ello:

http://www.linux-wlan.org/docs/wlan_adapters.html.gz

En la próxima sección hablaremos largo y tendido de los que es ***linux-wlan***, ahora nos servirá como base de identificación.

Por el momento vamos a enumerar las **cuestiones básicas a la hora de elegir una tarjeta:**

- El chipset
- Potencia de salida
- Sensibilidad de recepción
- Posibilidad de ajustar la potencia y/o sensibilidad
- Conectores, pigtails, etc..
- Soporte IEEE

Del ***chipset*** es de lo que estamos hablando... *¿cuál es el mejor? ¿cuál elijo?*

Pues son preguntas difíciles, sin duda ***Prism*** y sus derivados (***Prism I, II, III, GT, Indigo, Duette, Nitro, Worldradio...***) son los que mayor soporte y con los que casi al 100% tendremos éxito en *LiNUX*.

- ***Prism I, II, III*** son compatibles con IEEE 802.11b
- ***Prism Indigo*** es exclusivo para IEEE 802.11a
- ***Prism GT*** para IEEE 802.11b y 802.11g
- ***Prism Duette*** para IEEE 802.11a y 802.11b
- ***Prism Nitro*** para IEEE 802.11g
- ***Prism WorldRadio*** para IEEE 802.11a, b, d, g, h, i, j

Cielos!!!! TAMBIÉN EXISTE d, h, y j???? Si de esos no hemos hablado!!!!!!

Pues sí... luego te contaré algo de esos otros estándares ;) (En la Ampliación V)

Prism es el chipset más indicado para muchas de nuestras prácticas, está muy documentado y se ofrecen recursos gratuitos por todas partes y los desarrolladores ofrecen informes y notas técnicas constantemente.

¿Cual usas tú?

Bueno, yo tengo varias tarjetas y con diferentes chipset, una USRobotics con chipset Texas Instrument, Tarjetas Xircom y media docena de CISCO con chipset airones, cuatro tarjetas 3Com Prism II, una Sitecom con ADM, una SMC con Prism 54 GT y una Toshiba.

De ellas, 4 son pcmcia y el resto son PCI para equipos de sobremesa... bueno y tengo "un cacharro" también que es un adaptador PCI a pcmcia, así puedo pinchar una tarjeta del portátil en un PC de sobremesa :P

Y claro, también varios puntos de acceso, ahí sólo tengo dos modelos un 3COM y los CISCO... pero eso no me preocupa de momento.

Me falta para completar "el lote" alguna LUCENT con chipset Hermes y algún USB o bluetooth con el chipset que le venga en gana :P

¿He de tener todos esos?

NO, estaría bien disponer de más de un modelo, pero si te sirve de consejo, **busca una tarjeta de cualquier fabricante con chipset Prism.**

Las CISCO aironet son excelentes para barridos y escaneos por su gran potencia y su capacidad de saltar por las diferentes bandas de frecuencia, también por su sensibilidad en la recepción y la posibilidad de acoplarles antenas externas, pero es un chipset de propietario y aunque se basan en chipset Prism mejorados **algunas de nuestras herramientas y controladores para crear puntos de acceso ilícitos no funcionarán en esas tarjetas**. Como ventaja añadida, CISCO incluye los drivers, parches y controladores necesarios para todos los sistemas operativos más populares, incluido *LiNUX, BSD* y por supuesto *Microsoft*, *Novell*, *MacOS*, etc... pero son muy caras...

Las tarjetas de LUCENT y chipset Hermes precisan de parches específicos para funcionar con algunas herramientas y **costará más trabajo el configurarlas en LiNUX**, son una buena opción para el rastreo, existe un proyecto llamado *HemesAP* pero **no es compatible con HostAP que será uno de nuestros controladores favoritos para muchas herramientas.**

Los chipset Symbol son realmente **chipsets Prism con una controladora de capa MAC diferente**, ocurre lo mismo, hay que parchear las aplicaciones para poderlos usar en modo monitor.

Atheros son chipset para IEEE 802.11a, por tanto **nos quedamos sin compatibilidad con otros protocolos** y aunque también puedes encontrar tarjetas con **chipset atheros para 802.11b y g, para usarlos baj LiNUX tendremos que usar controladores madwifi** para obtener compatibilidad con otras tarjetas.

Chipsets más modernos como los ***TI (Texas Instrument, ADM, Bradcom, etc..)*** son peligrosillos... **para algunos no hay soporte en LiNUX** y es posible que se tarde bastante en obtenerlo, sin embargo podemos hacer funcionar esas tarjetas en *LiNUX* usando **Wrappers o los propios controladores de Windows!!!!!**

Pero no pienses que podrás usar esas tarjetas para monitorizar, descubrir y penetrar por redes inalámbricas usando los controladores de *Win32* bajo *LiNUX*, s**olamente te proporcionarán conectividad**, que ya es bastante si lo que buscamos es que simplemente funcione.

En resumen, **huye de chipsets novedosos** y que no estén ampliamente documentados, cuidado con los fabricantes y protocolos IEEE a los que dan soporte, **atento por si necesitas parches** en determinadas herramientas de análisis, ataque o defensa, **compilar el kernel** de *LiNUX* para dar soporte a esas tarjetas/chipsets... **y si todo falla, nos quedará el consuelo de usar esos Wrappers o controladores de Windows bajo LiNUX** para al menos lograr conectividad con la red... eso sí, olvidándonos de todo lo demás.

Una Buena elección: PRISM ;)

Prism es una buena elección para usar tarjetas *WLAN* si demasiados problemas en plataformas *LiNUX y BSD... sí estoy dejando aparte BSD, y es que aunque parecidas las herramientas y dirvers, en la mayor parte de los casos son diferentes en uno y otro*.

Con *Prism* (o ***Intersil Prism*** que era el proyecto inicial o como lo puedes encontrar por muchos sitios) **tendrás menos problemas y más ayuda.**

Antes hablé de compilar el kernel, y en la mayor parte de los casos así será, aunque a partir de 2.4.18 ya se incluyen controladores incorporados al núcleo "*por defecto*" puede ser que nuestra tarjeta en cuestión precise de parches específicos u opciones de núcleo que no estaban habilitadas, eso también será importante, sobre todo si usamos portátiles con *pcmcia, cardbus, usb, etc...* en la mayor parte de estas ocasiones necesitaremos habilitar o parchear módulos, *hotplugs*, etc... todo llegará en su momento.

Si tuviésemos que planear el hardware necesario para salir "por ahí" ha husmear redes o para auditarlas... una configuración amplia sería:

- **Uno o varios portátiles** con varias *pcmcia*, equipados con *LiNUX, BSD* o ambos
- **Tarjetas CISCO** para barrer el tráfico de forma eficiente
- **Tarjetas Prism** para usarlas como falsos puntos de acceso, ruptura de *WEP, DoS, o ataque de hombre en medio*
- **Tarjetas con chipset atheros** para protocolos IEEE 802.11a o en su defecto cualquier otra que permita banda dual
- **Antenas externas**, al menos una **omnidireccional** y otra **direccional**, con ganancia suficiente y/o amplificadores si llega el caso.
- **Nuestro "maletín" de herramientas**, esto es, las aplicaciones que luego describiremos, preparadas y a punto, entre ellas, *escaneo, modo monitor o RFMON, decodificadores, craqueadotes, inyectores de datos y de tramas y alguna tarjeta/aplicación configurada como un falso punto de acceso*.

Claro, que si queremos "*salirnos*" del molde... **podemos añadir a todo esto:**

- **Un receptor GPS** conectado al portátil
- **PDA's**
- **Baterías**
- **Amplificadores**

Y para transportar todo eso, **un coche, mapas, prismáticos, etc**... hasta se me ocurre otra historia... si disponemos de acceso físico a la red/empresa/oficina.... podemos "*pinchar*" un ***usb wireless*** y **usarlo como un troyano, es lo que se llama backchannel**, un mecanismo que actuaría de forma oculta en la red a nuestro servicio... *aunque esto es ya historias del FBI ;)*

Como pocos de nosotros tenemos esto, **nos conformaremos con ser víctimas y atacantes**, **con un par de pc's y sus correspondientes tarjetas, más un access point**, si entra dentro de nuestras posibilidades dos tarjetas WLAN en el equipo atacante y las herramientas que comenzaremos a estudiar más adelante.

Si no disponemos de muchos Pc's o sólo de uno... ***siempre nos queda vmWare***, con algún límite, ***vmWare*** se comporta de forma *"no muy habitual*" cuando parcheamos el núcleo de *LiNUX*, pero sobre todo ***es un quebradero de cabeza cuando montamos una máquina virutal sobre portátiles equipados con tarjetas pcmcia, usb o cardbus.***

Teóricamente VmWare da soporte a todo ello, pero cuando hablamos de wireless la cosa cambia, yo no lo he conseguido, posiblemente si usamos la versión 5 de vmware (que aún no probé) puede que se solucione esta situación, el problema viene por la MAC y por el uso de vmware en modo NAT y/o Bridge.

Para usar una máquina virtual con tarjetas wi-fi, tendremos que configurar la máquina huésped en modo host-only, eso significa que se trata de un equipo "*aislado*" sin conexión con la máquina anfitrión, por tanto no lo podremos usar simultáneamente y si sólo disponemos de un PC, pues ya me diréis....

Lo mejor, dos físicamente, un punto de acceso, todas las tarjetas que podamos y las herramientas, con eso será suficiente, de no ser que cuando prueba más afondo la última versión de *vmware* me encuentre con la sorpresa de que sí se puede, con la 4.x NO, al menos no con el portátil y tarjetas *pcmcia/cardbus.*

Hasta aquí la teoría IMPRESCINDIBLE con lo que ya hemos visto y las ampliaciones que se adjuntan a este documento, no creo que tengas problemas en comprender la terminología, las necesidades hardware, el equipamiento y la filosofía de trabajo en *Wireless*, a partir de este momento empezaremos con la práctica, con "*la chicha*" del Taller.

Hasta otra :P