UNIVERSIDAD AMAZONICA DE PANDO

DIRECCION DE POSTGRADO E INVESTIGACION

TESIS PARA OPTAR EL GRADO ACADEMICO DE

MAESTRIA EN INGENIERIA INFORMATICA

"VULNERABILIDADES DE LOS PROTOCOLOS DE SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL Y PROTOTIPO DE DETECCIÓN DE INTRUSOS"

POSTULANTE: ING. GROVER MARIO CARLO QUICAÑA

TUTOR: LIC. JUAN RAMIRO VILLA

COBIJA-BOLIVIA

2012

DEDICATORIA Y AGRADECIMIENTO

Esta investigación la dedico a mi hija Lorenita por ser mi motivación en cada momento. Agradezco a mis colegas docentes de la Universidad Privada Domingo Savio por su apoyo y colaboración.

RESUMEN

Las de área local inalámbrica conocida hoy en día como las WLAN (del inglés wireless local areanetwork), muy utilizado como una alternativa a las redes de área local cableada o como extensión a estas, por su facilidad de uso a través de la autenticación de usuarios se han constituido en redes vulnerables, el mismo se constituye en objeto de estudio en la presente investigación, los métodos de vulneración a estas redes, el desarrollo de un modelo de aplicación para control de acceso de usuarios a las mencionadas redes y el planteamiento de una estructura de red de área local inalámbrica sin las debilidades estudiadas. Siendo el objetivo principal, el estudio de los protocolos de seguridad presentes en los accespoint y a base del mismo plantear un modelo de red sin debilidades como también la implementación de un modelo de aplicación unix para control de acceso a redes inalámbricas. Para lograr estos propósitos se ha hecho uso tanto de los métodos teóricos como empíricos, mas propiamente del método experimental. Finalizado el estudio se ha concluido que la única manera eficiente de autenticar usuarios en redes inalámbrica es a través de una aplicación que incorpora base de datos de cada usuario que se incorpora a la red. Habiendo hecho el estudio respectivo de los métodos de intrusión se concluye que no siempre estos ataques tendrán éxito debido a la dependencia de muchos factores técnicos. Como un modelo de aplicación sujeta a futuras mejoras se plantea una aplicación desarrollada en Linux Ubuntu como controlador de usuarios que acceden a una determinada red inalambrica.

Palabras clave:

Wireless, WiFi, Radius, WLAN

CONTENIDO

INTRODUCCIÓN 1

1. PLANTEAMIENTO DEL PROBLEMA 3

2. MARCO TEÓRICO

2.1 Redes de Computadoras 10
2.1.1 Clasificación de las Redes 11
2.1.1.1 Según la Topología de la Red 11
2.1.1.2 Según su Alcance o Extensión 20
2.1.1.3 Según su Tipo de Conexión o Medios de Transmisión 23
2.1.2 Redes de Computadoras Inalámbricas 28
2.1.2.1 Redes Inalámbricas de Área Local 32
2.1.2.2 Tecnología o Estándares de Redes Inlámbricas 33
2.1.2.3 Topología de las Redes Inalámbricas 34

3. MARCO REFERENCIAL

3.1 Seguridad de un Sistema de Red 36
3.1.1 Seguridad en Redes WiFi 37
3.1.1.1 Protocolos de Seguridad en Redes Inalámbricas 39
3.2 Modelo de Referencia OSI 40
3.3 Espacio Electromagnético 48
3.4 Antenas Inalámbricas 56
3.4.1 Tipos de Antenas Inalámbricas 56
3.4.2 Potencias de Transmisión en Antenas Inalámbricas 58
3.5 Punto de Acceso Inalámbrico 66
3.6 Sistema Operativo Ubuntu 68
3.6.1 Shel Script de Linux 69

4. MARCO APLICATIVO Y RESULTADOS

4.1 Introducción 73
2.2 Estándares 802.11 74
4.2.1 Estándar IEEE 802.11 – 1997 77
4.2.2 Capas del Protocolo 78
4.2.3 Método de Acceso al Medio 80
4.2.4 Prioridad de Tramas 83
4.2.5 Fragmentación de Paquetes 84
4.2.6 Proceso de Conexión a la Red Inalámbrica 85
4.2.7 Seguridad 87
4.2.8 Tramas 88
4.3 Mejoras en la Capa Física: 802.11 a/b/g/n 90
4.3.1 Mejoras En Seguridad: 802.11i 92
4.3.2 Seguridad en el Estándar 802.11 93
4.4 Seguridad WEP 95
4.4.1 Bases del Sistema WEP 95
4.4.2 WEP Estático 100
4.4.3 Wep Dinámico 101
4.5 Seguridad WPA 102
4.5.1 Protocolo TKIP 103
4.5.2 EAP 108
4.5.3 LEAP 108
4.5.4 EAP-TLS 109
4.5.5 EAP – TTLS 109
4.6 Estudio de la Seguridad en Redes 802.11 110
4.7 Seguridad Ofrecida al Usuario – Seguridad por los proveedores 111
4.7.1 Fabricantes 112
4.7.2 Proveedores de Acceso a Internet 114
4.8 Seguridad ofrecida por el Estándar 802.11 116
4.8.1 Puntos Débiles en la Seguridad 116
4.8.2 Debilidades de WEB 117

4.8.3 Debilidades de WPA 120
4.9 Ataques a Redes Inalámbricas 120
4.9.1 Términos Básicos 122
4.9.1.1. Wardriving 122
4.9.1.2 Modo Monitor 122
4.9.1.3 Inyección de Paquetes 124
4.9.2 Ataque al Protocolo WEP 124
4.9.2.1 Ataque por Fuerza Bruta 124
4.9.2.2 Ataque Mediante Criptoanálisis Estadístico FMS 125
4.9.2.3 Ataque Mediante Criptoanálisis Estadístico PTW 126
4.9.2.4 Otros Ataques 126
4.9.3 Ataque al Protocolo WPA 128
4.10 Ejemplos Prácticos 129
4.11 Herramientas 130
4.11.1 Hardware 130
4.11.2 Software 132
4.11.3 Casos de Estudio 136
4.11.3.1 Acceso a una Red sin Seguridad 136
4.11.3.2 Acceso a una Red con Seguridad WEP 141
4.12 Desarrollo de la Aplicación 151
4.12.1 Configuración del Daemon 151
4.12.2 Escenario de Ejecución del Programa 151
4.12.3 Elementos 151
4.12.4 Configuración de Red del SO Ubuntu 152

CONCLUSIONES 160
RECOMENDACIONES 162
BIBLIOGRAFIA

INTRODUCCIÓN

Desde la década de los 60’s, fueron años clave para las redes de computadoras, ya que se construyeron las primeras redes de computadoras de la historia. denominada ARPANET, y posteriormente en la década de los 70’s la ARPANET comienza a utilizar para sus comunicaciones un protocolo Host-to-host. Este protocolo se denominaba NCP y es el predecesor del actual TCP/IP que se utiliza en toda la Internet.

Actualmente una red de computadoras, es una de las principales actualizaciones de la tecnología ya que un ejemplo de una red es el Internet, la cual es un conjunto de dispositivos electrónicos inteligentes interconectados entre si, en otras palabras, maquinas que procesan y manipuan informacióncomo por ejemplo una computadora. Existen dos tipos de red que son LAN y WAN.

La red LAN (local área network) es una red que es privada, esto quiere decir, que todos los cables, concentradores, ruteadores, etc. que useesta red es propiedad de una persona, ejemplo de esta red es un cyber café, o una empresa que tenga todas sus máquinas interconectadas entre si.

La red WAN (wide área network) es una red que usa canales de comunicación de uso público, esto quiere decir, que paga un canal de comunicación por el servicio de red, como por ejemplo cuando se quiere conectar a Internet se tiene que marcar un numero para poder acceder al medio y este a su vez depende del proveedor de servicios.

En los últimos años las redes cableadas han sido alternadas con otro tipo de red que son las redes inalámbricas, las cuales cuentan con una tecnología innovadora que apenas está surgiendo como una solución electiva para las implementaciones empresariales, públicas y residencales, estas permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar, como ocurre con las redes cableadas.

Nokia y Symbol Technologies crearon en 1999 una asociación conocida como WECA (Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica). Esta asociación pasó a denominarse Wi-Fi Alliance en el 2003. El objetivo de la misma fue crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

De esta forma en abril de 2000 WECA certifica la interoperatividad de equipos según la norma IEEE 802.11b bajo la marca Wi-Fi. Esto quiere decir que el usuario tiene la garantía de que todos los equipos que tengan el sello Wi-Fi pueden trabajar juntos sin problemas, independientemente del fabricante de cada uno de ellos. Se puede obtener un listado completo de equipos que tienen la certificación Wi-Fi en Alliance – Certified Products.En el año 2002 la asociación WECA estaba formada ya por casi 150 miembros en su totalidad.

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico. Por tanto, una red localinalámbrica802.11 es completamente compatible con todos los servicios de las redes locales (LAN) de cable 802.3 (Ethernet).

Desde su aparición las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas.

Con las WLANs la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA, OBJETIVOS Y ESTRATEGIA METODOLOGICA

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radio eléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instalados sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables a los crackers), sin proteger la información que por ellas circulan.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son:

La utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

Ningún tipo de red es totalmente segura, incluso las redes con cable sufren de distintos tipos de vulnerabilidades. Las redes inalámbricas son aún más vulnerables que las redes con cables, debido a la propagación de la señal en todas direcciones.

No es raro que un usuario doméstico con una computadora con conexión inalámbrica capte una señal de red inalámbrica (a menudo, de forma inadvertida) procedente de un punto de acceso que se encuentre en las inmediaciones.

Aunque quizá no importe mucho compartir la conexión a Internet con un usuario ajeno, pero se debe tener en cuenta que, si lo hace, éste podría tener acceso a computadoras de su red doméstica (es decir, a los archivos almacenados en esos equipos), realizar actividades ilegales en línea o dañar su sistema de algún otro modo.

Lo preocupante de todo esto es que ésta conexión que ha concretado un intruso, se lo ha realizado aun cuando el AP (Access Point) tenía implementado protocolos de seguridad.

Por tanto se puede ver que existe la necesidad de dar respuesta a varios problemas que demanda la sociedad informática vinculadas a esta nueva tecnología de la cual no se puede evadir, mas al contrario se debe encontrar soluciones para garantizar una segura y confiable LAN inalámbrica a partir del siguiente problema de investigación:

De este modo, habiéndose publicado las formas o técnicas de intrusión para vulnerar algunos protocolos de seguridad, en muchos casos se hace insuficiente el contar o aplicar cierto protocolo, en tales casos se debe acudir a otras formas o alternativas para controlar el acceso de usuarios, si no es restringirlos entonces mínimamente monitorear la WLAN. Pero en el actual contexto no es común contar con programas de detección de intrusos, los mismos servirían para tomar ciertas medidas de seguridad de acceso.

El **problema de investigación** asimilado es: ¿Cómo mejorar la seguridad y protección del entorno vulnerable de una WLAN (Red de Área Local Inalámbrica)?

El **objetivo general:** Desarrollar un prototipo de detección de intrusos en redes inalámbricas Wi-Fi de área local para plantear una Estructura de Red Local segura y protegida donde el **objeto de estudio** son la Redes Inalámbricas más propiamente las WLAN (Redes de Área Local Inalámbricas), el **campo de acción** son los Protocolos de Seguridad de las WLAN para Implementar un Entorno Seguro de Red.

Para poder cumplir con el objetivo se plantean **preguntas científicas**:

- ¿Cuáles son los fundamentos teóricos sobre WLAN, vulnerabilidades de los protocolos de seguridad en WLAN?
- ¿Cuál será el estado actual de las vulnerabilidades en WLAN y estructuras de red?
- ¿Cuáles son elementos estructurales del prototipo para redes seguras bajo un estudio de vulnerabilidades en WLAN?
- Qué grado de validez revela el prototipo aplicado en entorno de red local??

Dando respuesta a las preguntas científicas se detallan los siguientes pasos o **tareas científicas:**

- Sistematizar los fundamentos teóricos sobre WLAN y protocolos de seguridad que estos poseen.
- Determinar el estado actual de las vulnerabilidades que presentan los protocolos actuales.
- Estructurar un prototipo en Shell Script Linux basado en un escenario de ataque preparado que revela las vulnerabilidades estudiadas.
- Determinar el grado de validez que se revela en la aplicación del prototipo.

Para llegar a la veracidad de su factibilidad y justificar esta propuesta se considerará involucrar las distintas áreas de estudio las cuales brindan un sustento para la **justificación de la investigación**, en la elaboración de este proyecto, llegando a mencionar estas distintas áreas:

El prototipo implementado será una aplicación de uso en áreas donde se provee el servicio de internet a varios usuarios simultáneamente. Toda institución debe preservar el acceso a su red y sobre todo proteger la información no solo institucional, sino también de los usuarios en general.

Si bien existen alternativas de realizar control de acceso a redes WiFi a través de Hardware especializado, los mismos implican destinar montos económicos adicionas, el prototipo desarrollado tendrá capacidades similares y estará desarrollado en una plataforma de Software Libre que no implican costos por concepto de Licencias.

La mayoría de los sistemas inalámbricos usan radiofrecuencia transmitiendo ondas que pueden salvar paredes y algunos obstáculos. El rango (radio de cobertura) varía desde los 30 hasta los 90 mts. cuadrados. La cobertura puede extenderse y la movilidad es posible a través de la capacidad de Roaming y con el uso de micro celdas.

Una LAN inalámbrica ofrece un rendimiento adecuado para las aplicaciones de oficina más comunes que trabajan en red, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, acceso a bases de datos y aplicaciones multiusuario. El diseño robusto de las LAN inalámbricas y la distancia limitada a la que viajan las señales, dan como resultado conexiones que proveen un desempeño en la integridad de los datos iguales o mejor que en las redes cableadas.

Los beneficios sociales que se pueden obtener son muy amplios para la ciber sociedad el cual es el directo beneficiario, las redes inalámbricas ofrecen flexibilidad de configuración e instalación y la posibilidad de desplazarse dentro de un área sin perder conectividad, al trabajar sin cables, rosetas de teléfono o tarjetas de red local inalámbrica, se puede acceder de forma segura a los archivos desde la red de una empresa, investigar en Internet o colaborar al instante con los miembros de su equipo empresarial desde el despacho osu casa. Y todo esto significa que el tiempo que se pase desplazándose dejará de ser sinónimo de tiempo de inactividad, se puede llevar la portátil a cualquier lugar con acceso a un punto de conexión y conectarse con facilidad a Internet. Hacer consultas y operaciones bancarias o enviar mensajes de correo electrónico sin tener que quedarse encadenado a un equipo de sobremesa.

Las alternativas de seguridad harán casi imposible el acceso no autorizado al tráfico en una red inalámbrica. Específicamente el conjunto de la sociedad que se beneficia con este proyecto son las empresas o instituciones que manejan información confidencial como ser: Instituciones Bancarias, Hoteleras, Empresas Farmacéuticas, Instituciones de Estudios Superiores, Etc.

Sabiendo que los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio -en principio- pueden viajar más allá de las paredes y filtrarse en

habitaciones/casas/oficinas contiguas o llegar hasta la calle, motiva encontrar una solución para este terrible problema más para aquellas empresas que necesitan una seguridad total en sus transacciones, libres de intrusiones, para este motivo primero se necesita saber qué clase de intrusiones son y cómo se realizan las intrusiones a una red inalámbrica.

El estudio delos protocolos de las redes inalámbricas y la necesidad creciente de consolidar una privacidad y seguridad, es de por sí bastante complejo ya que se requiere un estudio de los protocolos de seguridad de la norma b del estándar IEEE 802.11 para implementar una encriptación eficiente y sólida, profundizando la investigación de estos protocolos de seguridad como es el WEP y vulnerándolos para obtener el propósito.

De esta manera se hace un hincapié a la propuesta científica que se realiza tomando de ejemplo una estructura de red para poder implementar esta herramienta, que no solo sirve a una institución o empresa sino a todo un conglomerado de personas o usuarios que necesiten seguridad en su información.

El planteamiento teórico presentado constituirá en un fundamento considerable a tiempo de proponer niveles de seguridad en redes WLAN, los protocolos de de seguridad que se deben aplicar en escenarios Inalámbricos. Se va a plantear el uso de determinado HW especializado para Auditoria en Redes Wireless.

Una vez desarrollado al prototipo en Shell Script de Linux, éste se constituirá en una herramienta fundamental para hacer un seguimiento de quienes se conectan a nuestra red Inalámbrica. Se debe tomar en cuenta que en la actualidad no existen aplicaciones para usuario final que permitan monitorear a los usuarios conectados al Access Point.

Durante el proceso de investigación y desarrollo de este proyecto se aplica una **metodología de la investigación** la cual proporciona muchos métodos utilizados para este propósito, estos se indican a continuación:
Métodos teóricos:

Histórico Lógico: Que permite revelar regularidades sobre las redes inalámbricas en un devenir histórico concreto.

Inducción – deducción: Para determinar las vulnerabilidades más comunes existentes en el campo de acción de la investigación y lograr concretar elementos estructurales que den respuesta a esos hechos.

Análisis – Síntesis: Para determinar las vulnerabilidades existentes y sus relaciones más esenciales.

Modelación: preparar un escenario de ataque Para estructurar los elementos del Prototipo para dar seguridad.

Métodos empíricos:

Estudio Documental: Es para revisar tendencias y corrientes contemporáneos acerca de las WLAN.

Observación Directa: Para explicar el comportamiento de trafico de red ….

Métodos estadísticos matemáticos:

Para cuantificar el grado de validez de la propuestas. (ANEXO) resultados en el capítulo de resultados.

CAPÍTULO II

MARCO TEÓRICO

2.1 Redes de Computadoras

Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI [Wikipedia, 2011].

La definición más clara de una red de computadoras es la de un sistema de comunicaciones, ya que permite comunicarse con otros usuarios y compartir archivos y periféricos. Es decir es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información. Se entiende por red de computadoras al conjunto interconectado de ordenadores autónomos. Se dice que dos ordenadores están interconectados, si éstos son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre , también puede hacerse mediante el uso de láser, microondas y satélites de comunicación [Monografias, 2010].

En conclusión, una red de computadoras es un conjunto de computadoras conectadas o enlazadas utilizando un conjunto de reglas o protocolos que aseguren un servicio confiable, estas comparten recursos y se comunicaran entre si en un área geográficamente determinada utilizando una red cableada o inalámbrica.

2.1.1 Clasificación De Las Redes

Las redes informáticas también llamadas según el lugar, redes de computadoras o redes de ordenadores, son una serie de computadoras o dispositivos o de ambos, que están conectados entre si bien por un medio físico (cable) o de manera inalámbrica. Los elementos de la red pueden compartir la información sus archivos, recursos como por ejemplo las impresoras y los servicios como el correo electrónico, juegos, chats etc.. Los administradores de redes, pueden permitir los accesos a los recursos por categorías o prioridades según las necesidades o cargos de cada usuario o grupo de ellos [Bricopage, 2003].

Las redes de computadoras se clasifican en:

2.1.1.1 Según La Topología De La Red

Una topología no es más que la disposición de una red. La topología puede referirse a la disposición física de la red o a la disposición lógica de la red. La topología lógica establecen las reglas del camino para la transmisión de datos, como ya sabe, en la transmisión de datos, solamente una computadora puede transmitir a través de un segmento de cable en un momento dado. En contraste con la topología físicas, la topología lógica son abstractas en gran medida, la topología física se puede expresar a través de componentes específicos, como tarjetas de red y tipos de cableado; las redes lógicas son esencialmente las reglas del camino [Hayden, 1999].

La configuración de una red, recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se entiende como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando se habla de la configuración lógicase tiene que pensar en como se trata la información dentro de nuestra red, como se dirige de un sitio a otro o como la recoge cada estación [Monografias, 2011].

Es importante mencionar que Topología de Red, se entiende por la parte que define la estructura de la red o la forma de una red. Se divide en dos tipos de topología, que son:

- **Topología Física**: consiste en la configuración o disposición del cableado y equipos de comunicación.
- **Topología Lógica**: define como los datos fluyen a través de la red.

Topología o Nivel Físico:

Cuando se ha determinado realizar una red, lo que se debe tener en cuenta es la estructura que va a hacer utilizada, o sea la distribución física de los equipos conectados. Para ello se utilizan las siguientes topologías: BUS, ESTRELLA Y ANILLO, también existen otras como MALLA, ARBOL, COMPLETA, INTERSECCIÓN DE ANILLOS, MIXTA E IRREGULAR. Las redes Locales que fueron diseñadas como tales usualmente tienen una topología simétrica, en contraste con las redes de área amplia típicamente tienen topologías irregulares [Tanenbaum, 1999].

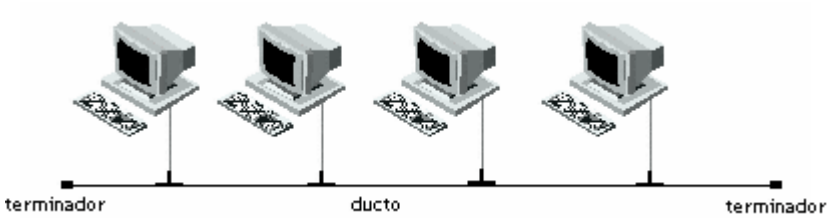
Las topologías más usadas son:

- Topología Horizontal (Bus), Canal O Ducto.

La ventaja de una red con topología en bus es su simplicidad (es la mas sencilla que existe) como se muestra en la fig.2.1. Una ves que las computadoras están físicamente conectadas y con el software de red en cada computadora; generalmente todas las computadoras serán capaces de verse entre si sin dificultad, pero si uno de los enlaces entre cualquiera de las computadoras se rompe, la red deja de funcionar [Hayden, pag.8, 1999].

Su funcionamiento es conectar las computadoras en red en una sola línea con el fin de poder identificar hacia cuál de todas las computadoras se este eligiendo.

Fig.2.1 Estructura Física de una Red en Bus, Canal o Ducto



Fuente: [Martinez, 2004] pag 1.

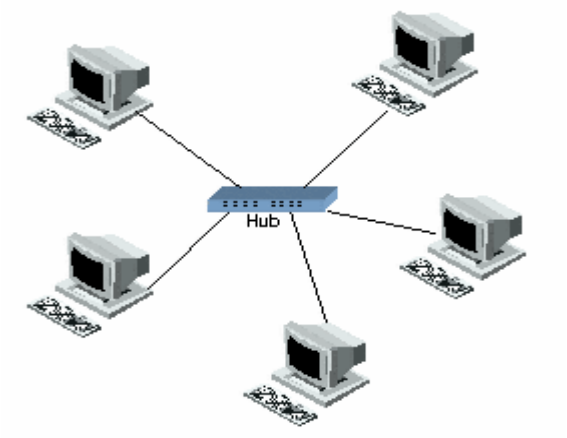
El bus permite que todas las estaciones reciban la transmisión. Es decir que cada estación puede difundir la información a todas las demás. El principal inconveniente de esta topología es que habitualmente solo existe un único canal de comunicaciones al que se conectan todos los dispositivos de la red. En consecuencia si falla dicho canal la red deja de funcionar, la cual le hace vulnerable para una sólida comunicación.

- Topología En Estrella

Existen redes más complejas construidas con topología de estrella. En contraste con la topología de bus en la que el cable corre de una computadora a otra, las redes con topología estrella tienen una caja de conexiones llamada hub o concentrador en el centro de la red, donde todas las computadoras se conectan al concentrador, el cual administra las comunicaciones entre computadoras, como se muestra en la fig.2.2. Una red tipo estrella puede conectar computadoras a pesar de que la red este operando, sin causar fallas en la misma. La topología en estrella a pesar que cuesta un poco mas debido al hardware adicional, pero este costo vale la pena debido al incremento en la confiabilidad inherente a este diseño [Hayden, 1999].

Una computadoratambien puede hacer la función de Servidor y se ubica en el centro de la configuración y todas las otras computadoras o estaciones de trabajo se conectan a ella.

Fig.2.2 Estructura Física de una Red en Estrella



Fuente: [Martínez, 2007]pag 1.

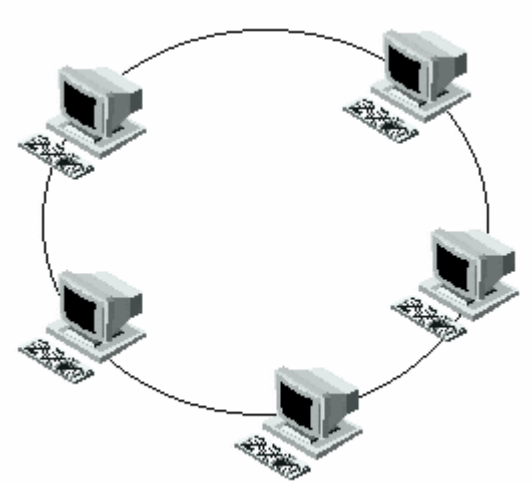
Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, quien se encarga de gestionar las transmisiones de información por toda la estrella. La topología de Estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central. Resulta económico la instalación de un nodo cuando se tiene bien planeado su establecimiento, ya que este requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo.

- Topología En Anillo

En una topología en anillo el cableado y la disposición física son similares a los de una topología en estrella. Sin embargo, en lugar que la red de anillo tenga un concentrador en el centro, tiene un dispositivo llamado MAU (unidad de acceso a multiestaciones) la cual realiza la misma tarea que un concentrador, pero en lugar de trabajar con redes Ethernet lo hace con redes Token Ring y maneja la comunicación entre computadoras de una manera ligeramente distinta, por lo que si una conexión de red falla, la otra puede reanudar automáticamente la tarea [Hayden, pag.10, 1999].

En ésta red, las computadoras se conectan en un circuito cerrado formando un anillo por donde circula la información en una sola dirección, como se muestra en la fig.2.3,con esta característica permite tener un control de recepción de mensajes, pero si el anillo se corta los mensajes se pierden.

Fig.2.3 Estructura Física de una Red en Anillo



Fuente: [Martínez, 2007] pag 1.

En esta red cada estación está conectada a la siguiente y la última está conectada a la primera.

Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando. La topología de anillo esta diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado muestra alguna economía respecto al de estrella. El anillo es fácilmente expandido para conectar más nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo. Así también, el

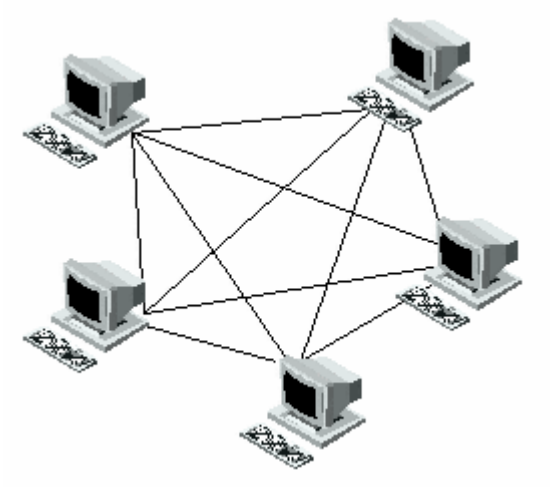
movimiento físico de un nodo requiere de dos pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar [Monografias, 2011].

- Topología De Malla (Mesh)

La topología de malla (mesh) utiliza conexiones redundantes entre los dispositivos de la red aí como una estrategía de tolerancia a fallas. Cada dispositivo en la red está conectado a todos los demás (todos conectados con todos)como se muestra en la fig.2.4. Este tipo de tecnología requiere mucho cable (cuando se utiliza el cable como medio, pero puede ser inalámbrico también). Pero debido a la redundancia, la red puede seguir operando si una conexión se rompe [Martínez, 2007].

Las redes de malla, obviamente, son mas difíciles y caras para instalar que las otras topologías de red debido al gran número de conexiones requeridas.

Fig.2.4 Estructura Física de una Red en Malla



Fuente: [Martínez, 2007] pag 1.

La Red en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes

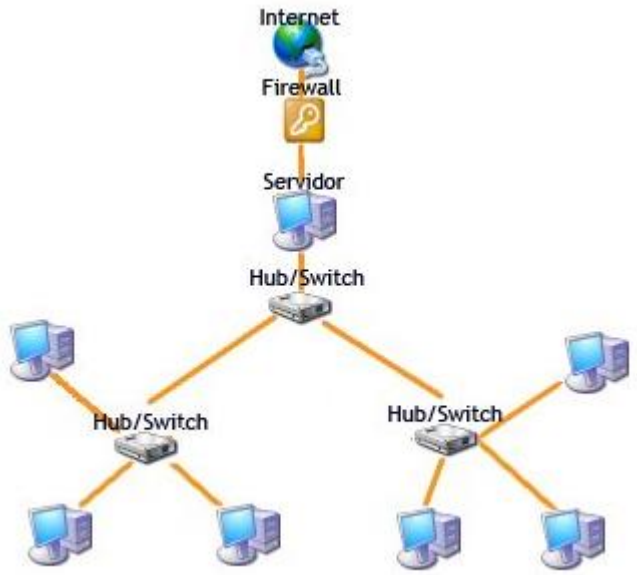
caminos. Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores[Paz, 2009].

- Topología En Árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones. Cuenta con un cable principal (*backbone*) al que hay conectadas redes individuales en bus [Paz, 2009].

La topología de árbol combina características de la topología de estrella con la BUS. Consiste en un conjunto de subredes estrella conectadas a un BUS, como se observa en la fig.2.5. Esta topología facilita el crecimiento de la red.

Fig.2.5 Estructura Física de una Red en Árbol



Fuente:[Aprende, 2009] pag 1

Topología o Configuración a Nivel Lógico:

- Topología Ethernet

Cada host envía sus datos a todos los otros host conectados al medio físico en la red. No hay un orden de transmisión de datos, el primero en acceder al medio es el primero en transmitir [Aprende, 2009].

Norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionada para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps. En sus versiones de hasta 1 Gbps utiliza el protocolo de acceso al medio CSMA/CD (CarrierSenseMultipleAccess / CollisionDetect - Acceso múltiple con detección de portadora y detección de colisiones). Actualmente Ethernet es el estándar más utilizado en redes locales/LANs. Los estándares sucesivos (100 Mbps o Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet) abandonaron los

coaxiales dejando únicamente los cables de par trenzado sin apantallar (UTP - UnshieldedTwistedPair), de categorías 5 y superiores y la Fibra óptica[Paz, 2009].

- Topología Token Ring

Aquí se controla el acceso al medio utilizando un testigo electrónico que se pasa a cada host. Cuando un host recibe el testigo puede transmitir datos si los tiene. Si no, entonces pasa el testigo al siguiente host [Aprende, 2009].

La topología de esta red es un anillo alrededor del cual se distribuyen las estaciones de trabajo.Las computadoras conectadas a la red se comunican todo el tiempo entre sí mediante un paquete de información (token) que está viajando en todo momento a través de la red [Bustillos, 2007].

Esta red posee las siguientes características:

- Monitoreo de Red.
- Acepta múltiples tipos de cables.
- Diseñada para ambientes de oficina en las cuales se requiere una red que tenga amplia capacidad de expansión en el ambiente PC y también hacia otro tipo de ambientes de computadoras, tales como mini-computadoras o macro-computadoras.

Una topología de anillo conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa. Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red. El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token". El token circula alrededor del anillo y cuando una computadora desea enviar datos, espera al token y posiciona de él. La computadora entonces envía los datos sobre el cable. La computadora destino envía un mensaje (a la computadora que envió los datos) que de fueron recibidos correctamente. La computadora que transmitió los datos, crea un nuevo token y los envía a la siguiente

computadora, empezando el ritual de paso de token o estafeta (tokenpassing) nuevamente [Martínez, 2007].

En este acápite se hace mención que el tipo de topología que se utilizaen este respectivo trabajo de investigación, se denomina Topología de Redes Inalámbricas que se verá en un inciso posterior, sin embargo las topologías vistas hasta el momento nos ayudan a comprender el enfoque a cerca de las topologías y en algún momento dado si se utilizaestas topologíasserá de acuerdo a la identificación que una determinada persona tenga por una de ellas, no obstante se puede decir que la topología que encaja para este trabajo de investigación es la Topología en Estrella.

2.1.1.2 Según Su Alcance o Extensión

Un criterio alterno para clasificar las redes es su escala, como se muestra en la fig.2.6, damos una clasificación de los sistemas de múltiples procesadores de acuerdo con su tamaño físico. En la parte superior están las máquinas de flujo de datos, computadoras con alto grado de paralelismo y muchas unidades funcionales, en el mismo programa. A continuación vienen las multicomputadoras, sistemas que se comunican enviando mensajes por buses muy cortos y rápidos. Más allá de las multicomputadoras están las verdaderas redes, computadoras que se comunican intercambiando mensajes por cables largos. Éstas pueden dividirse en redes locales, metropolitanas y de área amplia. Finalmente, la conexión de dos o más redes es una interred. La red Internet, de alcance mundial, es un ejemplo muy conocido de interred. La distancia es muy importante como medio de clasificación porque se usan diferentes técnicas a diferentes escalas [Tanenbaum, 1999].

Fig.2.6 Clasificación de los sistemas de múltiples procesadores

Distancia entre Procesadores	Procesadores ubicados en el (la) mismo(a)	
0.1m	Tarjeta de circuito	Máquina de flujo de datos
1m	Sistema	Multicomputadoras
10m	Cuarto	
100m	Edificio	
1km	Campus	Red de área local
10km	Ciudad	
100km	País	
1,000km	Continente	
10,000km	Planeta	

Fuente: [Tanenbaum, 1999] pag. 8

Una vez que se comprende los conceptos técnicos básicos, es oportuno familiarizar con los conceptos básicos de organización de la conectividad de redes: LAN, MAN y WAN. También existen dos tipos de redes adicionales, CAN y TAN. A parte del hecho de que estos tipos de redes riman, son entidades completamente diferentes, es importante recordar que todas estas redes son redes privadas, esto quiere decir que son utilizadas por un organismo a pesar de que las redes pueden estar ubicadas en más de un sitio [Hayden, pag.11, 1999].

- **Red de área personal (PAN):** es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso.

- **Red de área local (LAN):** es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

- **Red de área de Campus (CAN):** es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar. Puede ser considerado como una red de área metropolitana que se aplica específicamente a un ambiente universitario. Por lo tanto, una red de área de campus es más grande que una red de área local pero más pequeña que una red de área amplia.

- **Red de área metropolitana (MAN):** es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

- **Red de área amplia (WAN)**: es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismoedificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes [Aprende, 2009].

Estas redes hace referencia a las características que cada una de ellas tiene respecto al área geográfica que las rige y de acuerdo a ello cumplen con ciertas limitaciones o en caso contrario ampliaciones que estas puedan proporcionar de acuerdo al tipo que se necesite para una comunicación.

2.1.1.3 Según su Tipo de Conexión o Medios de Transmisión

En los medios de transmisión, el propósito es transportar una corriente de bits en bruto de una máquina a otra. Se puede usar varios medios físicos para la transmisión real; cada uno con su propio nicho en términos de ancho de banda, retardo, costo y facilidad de instalación y mantenimiento. A grandes rasgos, los medios se agrupan en medios guiados, como el cable de cobre y la fibra óptica, y medios no guiados, como la radio y los láser a través del aire [Tanenbaum, 1999].

Una vez que se tienen las estaciones de trabajo, el servidor y las placas de red, requerimos interconectar todo el conjunto. El tipo de cable utilizado depende de muchos factores, que se mencionarán a continuación: Existen dos tipos o medios de cableado de red. **Los medios guiados** que son: par trenzado, cable coaxial y fibra óptica. Y **los medios no guiados**se pueden realizar conexiones a través de radio, infrarrojo y microondas.Cada tipo de cable o método tiene sus ventajas. y desventajas. Algunos son propensos a interferencias, mientras otros no pueden usarse por razones de seguridad.La velocidad y longitud del tendido son otros factores a tener en cuenta el tipo de cable a utilizar[Paz, 2009].

- **Medios Guiados**

- El **cable de par trenzado,**consiste en dos hilos de cobre trenzado, aislados de forma independiente y trenzados entre sí. El par está cubierto por una capa aislante externa. Entre sus principales ventajas se tienen:

- Es una tecnología bien estudiada
- No requiere una habilidad especial para instalación
- La instalación es rápida y fácil
- La emisión de señales al exterior es mínima.
- Ofrece alguna inmunidad frente a interferencias, modulación cruzada y corrosión.

- El **cable coaxial,** se compone de un hilo conductor de cobre envuelto por una malla trenzada plana que hace las funciones de tierra. Entre el hilo conductor y la malla hay

una capa gruesa de material aislante, y todo el conjunto está protegido por una cobertura externa.

El cable está disponible en dos espesores: grueso y fino.

El cable grueso soporta largas distancias, pero es más caro. El cable fino puede ser más práctico para conectar puntos cercanos.

El cable coaxial ofrece las siguientes ventajas:

- Soporta comunicaciones en banda ancha y en banda base.
- Es útil para varias señales, incluyendo voz, video y datos.
- Es una tecnología bien estudiada.

- La **fibra óptica,**esta conexión es cara, pero permite transmitir la información a gran velocidad e impide la intervención de las líneas. Como la señal es transmitida a través de luz, existen muy pocas posibilidades de interferencias eléctricas o emisión de señal. El cable consta de dos núcleos ópticos, uno interno y otro externo, que refractan la luz de forma distinta. La fibra está encapsulada en un cable protector.

Ofrece las siguientes ventajas:

- Alta velocidad de transmisión
- No emite señales eléctricas o magnéticas, lo cual redunda en la seguridad
- Inmunidad frente a interferencias y modulación cruzada.
- Mayor economía que el cable coaxial en algunas instalaciones.
- Soporta mayores distancias.

- **Medios No Guiados**

- **Red por radio**

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significan que viajan en todas direcciones desde la fuente, por lo que el transmisor y el receptor no tienen que alinearse con cuidado físicamente. Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce

drásticamente con distancia ala fuente, aproximadamente en proporción $1/r^3$ en el aire. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia. En todas las frecuencias, las ondas de radio están sujetas a interferencia por los motores y otros equipos eléctricos. Por la capacidad del radio de viajar distancias largas, la interferencia entre usuarios es un problema. Por esta razón, los gobiernos legislan estrictamente el uso de radiotransmisores con algunas excepciones. [Tanenbaum, 1999].

Dentro del capítulo de Redes inalámbricas la Red por radio es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red. Es un tipo de red muy actual, usada en distintas empresas dedicadas al soporte de redes en situaciones difíciles para el establecimiento de cableado, como es el caso de edificios antiguos no pensados para la ubicación de los diversos equipos componentes de una Red de ordenadores. Los dispositivos inalámbricos que permiten la constitución de estas redes utilizan diversos protocolos como el Wi-Fi: El estándar IEEE 802.11. El cual es para las redes inalámbricas, lo que Ethernet para las redes de área local (LAN) cableadas. Además del protocolo 802.11 del IEEE existen otros estándares como el HomeRF, Bluetooth y ZigBee. El término radiofrecuencia, también denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz. El Hertz es la unidad de medida de la frecuencia de las ondas, y corresponde a un ciclo por segundo.[1] Las ondas electromagnéticas de esta región del espectro se pueden transmitir aplicando la corriente alterna originada en un generador a una antena[Wikipedia, 2011].

- **Red por infrarrojos**

Las ondas infrarrojas y milimétricas no guiadas se usan mucho para la comunicación de corto alcance. Todos los controles remotos de los televisores, grabadoras de video y estéreos, utilizan comunicación infrarroja. Estos controles son relativamente direccionales, baratos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos (pruebe a pararse entre su control remoto y su televisor y vea si todavía funciona). En general, conforme pasamos de la radio de onda larga hacia la luz visible, las ondas se comportan cada

vez mas como la luz y cada vez menos como la radio. Por otro lado, el hecho de que las ondas infrarrojas no atraviesen bien las paredes sólidas también es una ventaja, esto significa que un sistema infrarrojo en un cuarto de un edificio no interferirá un sistema similar en cuartos adyacentes. A demás, la seguridad de los sistemas infrarrojos contra el espionaje es mejor que la de los sistemas de radio, precisamente por esta razón. Por lo mismo, no es necesario obtener licencia del gobierno para operar un sistema infrarrojo, en contraste con los sistemas de radio, que deben tener licencia. Estas propiedades han hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores. Por ejemplo, las computadoras y las oficinas de un edificio se pueden equipar con transmisores y receptores infrarrojos relativamente desenfocados (es decir, un tanto omnidireccionales). De esta manera las computadoras portátiles capaces de utilizar infrarrojo pueden esta en la LAN local sin tener que conectarse a ellas físicamente. Cuando varias personas se presentan a una reunión con sus máquinas portátiles, solo tienen que sentarse en la sala de conferencias para estar conectado por completo, sin tener que enchufar. La comunicación con infrarrojo no se puede usar en exteriores porque el sol brilla con igual intensidad en el infrarrojo como en el espectro visible. [Tanenbaum, 1999].

Las redes por infrarrojos permiten la comunicación entre dos nodos, usando una serie de leds infrarrojos para ello. Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación por ello es escasa su utilización a gran escala. Esa es su principal desventaja, a diferencia de otros medios de transmisión inalámbricos (Bluetooth, Wireless, etc.). [Wikipedia, 2011].

- **Red por microondas**

Por encima de los 100 Mhz. Las ondas viajan en línea recta y, por tanto, se pueden enfocar en un haz estrecho. Concentrar toda la energía en un haz pequeño con una antena parabólica (como el tan familiar plato de televisión por satélite) produce una señal mucho mas alta en relación con el ruido, pero las antenas transmisoras y receptoras deben estar muy bien alineadas entre sí. A demás, esta direccionalidad permite a transmisores múltiples alineados en una fila, comunicarse con receptores múltiples en fila, sin interferencia. Antes de la **fibra**

óptica, estas microondas formaron durante décadas el corazón del sistema de transmisión telefónica de larga distancia. De hecho, el nombre de la empresa de telecomunicaciones de larga distancia MCI proviene de MicrowaveCommunications, Inc., porque sus sistema entero se basó originalmente en torres de microondas, desde entonces ha modernizado las principales porciones de su red empleando fibras. A diferencia de las ondas de radio a frecuencias mas bajas las microondas no atraviesan bien los edificios. Además, aun cuando el haz puede estar bien enfocado en el transmisor, hay cierta divergencia en el espacio. Algunas ondas pueden refractarse en las capas atmosféricas más bajas y tardar un poco más en llegar que las ondas directas. Las ondas diferidas pueden llegar fuera de fase con la onda directa y cancelar así la señal. Este efecto se lama desvanecimiento de trayectoria múltiple y con frecuencia es un problema serio que depende del clima y de la frecuencia. En síntesis, la comunicación por microondas se utiliza tanto para la comunicación telefónica de larga distancia, los teléfonos celulares, la distribución de la televisión y otros usos, que el espectro se ha vuelto muy escaso, esta tecnología tiene varias ventajas significativas respecto a la fibra, la principal es que no se necesita derecho de paso [Tanenbaum, 1999].

Una red por microondas es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. El protocolo más frecuente es el IEEE 802.11b y transmite a 2.4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo). Otras redes utilizan el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11a. Se denomina microondas a las ondas electromagnéticas definidas en un rango de frecuencias determinado; generalmente de entre 300 MHz y 300 GHz, que supone un período de oscilación de 3 ns (3×10^{-9} s) a 3 ps (3×10^{-12} s) y una longitud de onda en el rango de 1 m a 1 mm. Otras definiciones, por ejemplo las de los estándares IEC 60050 y IEEE 100 sitúan su rango de frecuencias entre 1 GHz y 300 GHz, es decir, longitudes de onda de entre 30 centímetros a 1 milímetro. El rango de las microondas está incluido en las bandas de radiofrecuencia, concretamente en las de UHF (ultra-highfrequency - frecuencia ultra alta) 0,3–3 GHz, SHF (super-highfrequency - frecuencia super alta) 3–30 GHz y EHF (extremely-highfrequency - frecuencia extremadamente alta) 30–300 GHz. Otras bandas de radiofrecuencia incluyen ondas de menor frecuencia y mayor longitud de onda que las microondas. Las microondas de mayor frecuencia y menor longitud de onda —en el orden de milímetros— se denominan ondas milimétricas. La existencia de ondas electromagnéticas, de

las cuales las microondas forman parte del espectro de alta frecuencia, fueron predichas por Maxwell en 1864 a partir de sus famosas Ecuaciones de Maxwell. En 1888, Heinrich Rudolf Hertz fue el primero en demostrar la existencia de ondas electromagnéticas mediante la construcción de un aparato para generar y detectar ondas de radiofrecuencia [Wikipedia, 2011].

2.1.2 Redes De Computadoras Inalámbricas

Tal como su nombre lo indica, las redes inalámbricas son aquéllas que carecen de cables. Gracias a las ondas de radio, se lograron redes de computadoras de este tipo, aunque su creación refirió varios años de búsqueda. Esta tecnología facilita en primer lugar el acceso a recursos en lugares donde se imposibilita la utilización de cables, como zonas rurales poco accesibles. Además, estas redes pueden ampliar una red ya existente y facilitar el acceso a usuarios que se encuentren en un lugar remoto, sin la necesidad de conectar sus computadoras a un hubo a un switchpor intermedio de cables. Estos usuarios podrían acceder a la red de su empresa o a la computadora de su casa en forma inalámbrica, sin configuraciones adicionales [Lectores, 2011].

Una red inalámbrica es aquella que posibilita la conexión de dos o más equipos entre sí, sin que intervengan cables, utilizando la tecnología “Wi-Fi” en inglés significa “WirelessFidelity”. Este tipo de redes nos ofrecen gran ventajas para hogares y empresas, ya que no se necesitan instalar cables. Wi-Fi, fue publicado bajo el estándar IEEE 802.11, el mismo ha sufrido actualizaciones, los cuales trabajan a diferentes velocidades. Las redes de área Local Inalámbricas, permite una gran movilidad a los usuarios, al permitirles minimizar las conexiones de cables, utilizando tecnología de radiofrecuencia. [mweb, 2007]

Las redes inalámbricas de alta velocidad pueden proporcionar beneficios de conectividad en red sin las restricciones de estar ligadas a una ubicación o tejidas por cables. Existen muchos escenarios en donde esta puede ser una alternativa interesante, incluyendo los siguientes:

- Las conexiones inalámbricas pueden ampliar o reemplazar una infraestructura cableada en situaciones en donde es costoso o está prohibido tender cables.
- Las instalaciones temporales son un ejemplo de cuándo una red inalámbrica puede tener sentido o hasta ser requerida. Algunos tipos de edificios o códigos de construcción pueden prohibir el uso de cables, haciendo de las redes inalámbricas una alternativa importante.
- Y por supuesto el fenómeno de "no tener cables nuevos" que se relaciona con una instalación inalámbrica, conjuntamente con la red de líneas telefónicas y hasta la red eléctrica, se ha vuelto un catalizador principal para las redes en el hogar y la experiencia de un hogar conectado.

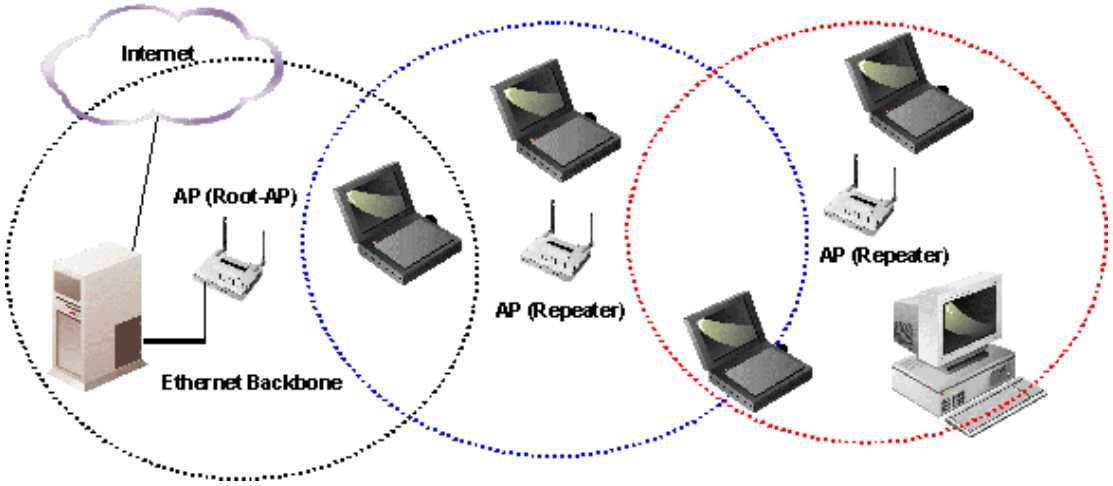
Los usuarios que cada vez son más móviles se vuelven un candidato evidente para una red inalámbrica. El acceso móvil a redes inalámbricas se puede lograr utilizando computadoras portátiles y tarjetas de red inalámbricas. Esto permite al usuario viajar a distintas ubicaciones - salas de reuniones, pasillos, vestíbulos, cafeterías, salas de clases, etc. - y aún tener acceso a los datos en red. Sin un acceso inalámbrico, el usuario tendría que llevar molestos cables y encontrar un punto de red para conectarse. Más allá del campo corporativo, el acceso a Internet y hasta los sitios corporativos podría estar disponible a través de puntos de redes inalámbricas en lugares públicos. Aeropuertos, restaurantes, estaciones de ferrocarril y áreas comunes en una ciudad pueden contar con este servicio. Cuando el profesional que viaja llega a su destino, quizás para reunirse con un cliente en su oficina corporativa, él podría tener acceso limitado a través de una red local inalámbrica. La red puede reconocer al usuario de otra empresa y crear una conexión que quede aislada de la red local corporativa, pero que proporcione acceso a Internet al visitante.

En todos estos escenarios, vale la pena destacar que las redes inalámbricas actuales basadas en estándares operan a altas velocidades; las mismas velocidades que se consideraron de última tecnología para redes cableadas hace tan sólo unos años, con la diferencia que las redes inalámbricas son mucho mas cómodas por su portabilidad.

Las redes inalámbricas son denominadas a aquellas nuevas redes sin cables que hacen posible que se pueda conectar a una red local cualquier dispositivo sin necesidad de instalación de

cables, lo que permite que nos podamos pasear libremente por la oficina con nuestro ordenador portátil conectado a la red o conectar sin cables, cámaras de vigilancia en los lugares más inaccesibles. También se puede instalar en locales públicos y dar el servicio de acceso a Internet sin cables, Como se muestra en la fig.2.7. La norma IEEE 802.11b dio carácter universal a esta tecnología que permite la conexión de cualquier equipo informático a una red de datos Ethernet sin necesidad de cableado, que actualmente se puede integrar también con los equipos de acceso ADSL para Internet[Paz, 2009].

Fig.2.7 Estructura física de una Red Inalámbrica



Fuente:[Paz, 2009]parte.2

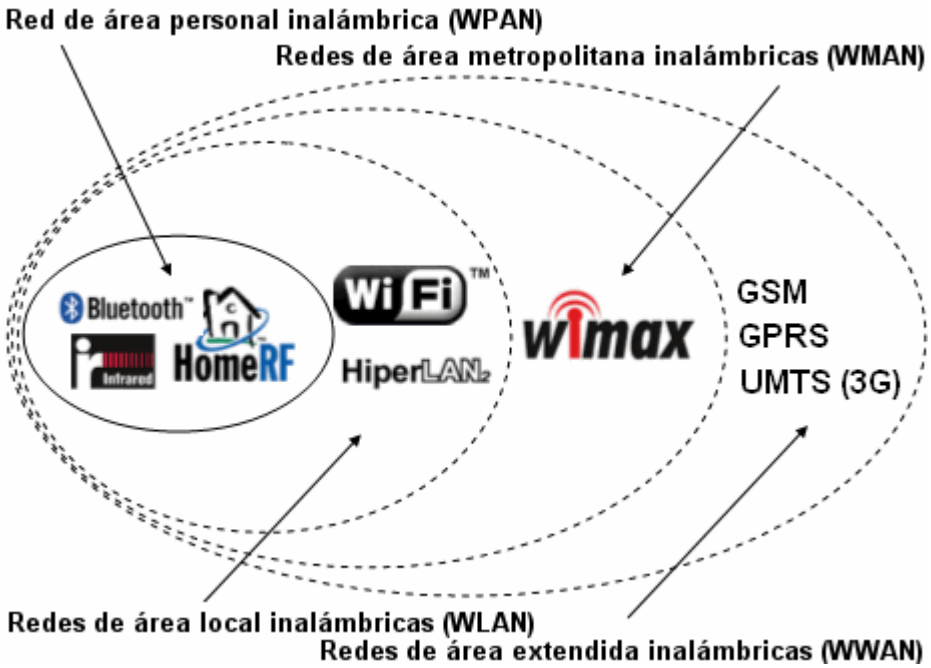
La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran

velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina [Aguirre, 2007].

- **Categorías de las redes inalámbricas**

Por lo general, las redes inalámbricas se clasifican en varias categorías, de acuerdo al área geográfica desde la que el usuario se conecta a la red (denominada área de cobertura) como se muestra en la fig. 2.8:

Fig.2.8Categorías de las redes inalámbricas



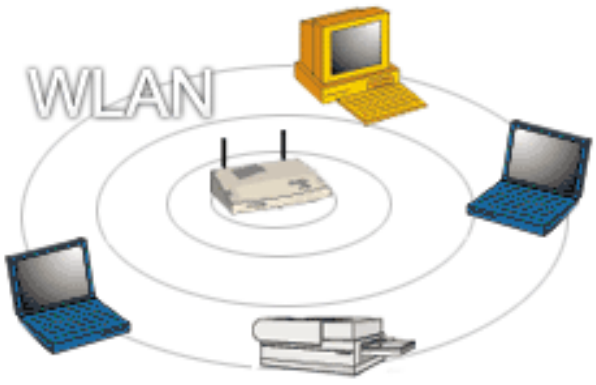
Fuente: [Jeff, 2008] pag.1

2.1.2.1 Redes Inalámbricas De Área Local (Wlan)

Una red inalámbrica de área local (Wireless LAN) es un sistema flexible de transmisión de datos implementados como una extensión, o como alternativa, de una red cableada. Utiliza tecnología de radio frecuencia, transmite y recibe datos utilizando como medio el aire, minimizando la necesidad de una conexión de cable, permitiendo la combinación conectividad y movilidad. Una red de computadoras local inalámbrica es un sistema de comunicación de datos que utiliza tecnología de radiofrecuencia. En esta red se transmite y recibe datos sobre aire, minimizando la necesidad de conexiones alambricas, es decir, combinan la conectividad de datos con la movilidad de usuarios.[CBTIS, 2004]

Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar. Con las WLANs la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada, asi se muestra en la Fig. 2.9. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores [maestrow, 2004].

Fig 2.9. Red Inalámbrica de Área Local



Fuente: [maestrow, 2004] pag.1

La disponibilidad de la tecnología inalámbrica y de las redes (LAN) inalámbricas puede ampliar la libertad del usuario en red, resolver distintos problemas asociados con redes de cableado físico y en algunos casos, hasta reducir los costos de implementar redes. Sin embargo, junto con esta libertad, las redes inalámbricas conllevan también un nuevo conjunto de retos.

2.1.2.2 Tecnología o Estándares De Redes Inalámbricas

Actualmente, existen dos soluciones prevalecientes de redes inalámbricas que se están implementando. Estas soluciones son los estándares IEEE 802.11, principalmente 802.11b, y la solución propuesta por el grupo de trabajo HomeRF. Estas dos soluciones no interfieran entre sí o con otras soluciones de redes inalámbricas. Si bien HomeRF está diseñada exclusivamente para el ambiente del hogar, 802.11b está diseñada y se puede implementar en hogares, pequeñas, medianas y grandes empresas, así como en un número cada vez mayor de lugares públicos con redes inalámbricas. Muchos de los principales fabricantes de PCs portátiles ya incluyen o tienen planes de ofrecer sistemas con tarjetas de red internas 802.11b [CBTIS, 2004].

Existen diversos tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE802.11 aprobado. Son los siguientes:

- Los estándares IEEE 802.11b e IEEE 802.11g disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz está disponible casi universalmente, con una velocidad de hasta 11 Mbps y 54 Mbps, respectivamente.
- En la actualidad ya se maneja también el estándar IEEE 802.11a, conocido como WIFI 5, que opera en la banda de 5 GHz y que disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada y, además no existen otras tecnologías (Bluetooth, microondas, ZigBee, WUSB) que la estén utilizando, por lo tanto existen muy pocas interferencias. Su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance).

- Un primer borrador del estándar IEEE 802.11n que trabaja a 2.4 GHz y a una velocidad de 108 Mbps. Sin embargo, el estándar802.11g es capaz de alcanzar ya transferencias a 108 Mbps, gracias a diversas técnicas de aceleramiento. Actualmente existen ciertos dispositivos que permiten utilizar esta tecnología, denominados Pre-N.

Existen otras tecnologías inalámbricas como Bluetooth que también funcionan a una frecuencia de 2.4 GHz, por lo que puede presentar interferencias con Wi-Fi. Debido a esto, en la versión 1.2 del estándar Bluetooth por ejemplo se actualizó su especificación para que no existieran interferencias con la utilización simultánea de ambas tecnologías, además se necesita tener 40.000 k de velocidad [Wikipedia,2010].

2.1.2.3 Topología De Las Redes Inalámbricas

Las redes inalámbricas se construyen utilizando dos topologías básicas. Estas topologías se llaman de distintas formas, incluyendo administradas y no administradas, "hosted" y de punto a punto ("peer-to-peer"), así como de infraestructura y ad-hoc. En este documento se emplearan los términos "infraestructura" y "ad-hoc". Estos términos se relacionan esencialmente con las mismas funciones básicas de la topología [CBTIS, 2004].

- Una Topología de Infraestructura, es una que amplía una red cableada existente a dispositivos inalámbricos, proporcionando una estación base (llamada punto de acceso). El punto de acceso se une a las redes inalámbricas y cableadas, actuando como un controlador central para la red inalámbrica. El punto de acceso coordina la transmisión y la recepción de múltiples dispositivos inalámbricos dentro de un rango específico. El rango y cantidad de dispositivos dependen del estándar inalámbrico que se utilice y el producto del proveedor. En la infraestructura puede haber varios puntos de acceso para cubrir una gran área o sólo un punto único de acceso para un área pequeña, como por ejemplo una casa o un edificio pequeño.

- Una Topología AD-HOC es una en la cual se crea una red LAN únicamente por los dispositivos inalámbricos mismos, sin controlador central o punto de acceso. Cada dispositivo se comunica directamente con los demás dispositivos en la red, en lugar de que sea a través de

un controlador central. Esto es útil en lugares en donde pequeños grupos de computadoras pueden congregarse y no se necesita acceso a otra red. Por ejemplo, un hogar sin una red cableada o un cuarto de conferencia en donde se reúnen regularmente equipos para intercambiar ideas, son ejemplos en los que puede ser útil una red inalámbrica ad-hoc.

Por ejemplo, cuando se combinan la nueva generación de software y las soluciones inteligentes de punto a punto, estas redes inalámbricas ad-hoc pueden permitir a los usuarios que viajan colaborar, disfrutar de juegos con varios participantes, transferir archivos o comunicarse de alguna otra forma entre sí, utilizando sus PCs o dispositivos inteligentes de manera inalámbrica.

CAPITULO III

MARCO REFERENCIAL

3.1 Seguridad de un Sistema de Red

Tanenbaum asegura que durante las primeras décadas de su existencia, los sistemas de redes de computadoras fueron usadas principalmente por investigadores universitarios para el envió de correo electrónico y por empleados corporativos para compartir impresoras. En estas condiciones, al campo de seguridad no se le prestó mucha atención, pero ahora millones de ciudadanos usan un sistema de red ya sea para una transacción bancaria, compras, declaraciones de impuestos y otras acciones más. La inseguridad de un sistema de red aparece en el horizonte como un problema potencial de grandes proporciones. [Tanenbaum, 1997]

El caso donde la comunicación que fluye en un sistema de red donde millones de datos viajan a diario entre sistemas de redes, la convierten en un medio altamente inseguro y la posibilidad real de interceptar, alterar o introducir datos en estas comunicaciones representa un peligro potencial para cualquier usuario. No obstante, a causa de la introducción de la informática en la amplia escala de la sociedad y el frecuente avance de la tecnología que cada día sorprende más y más, da lugar al surgimiento de personajes más peligrosos que otros, los cuales difunden miedo en un sistema de red ya sea este público como por ejemplo el Internet o una privada como las VPNsa sí como también al cibernauta o comúnmente llamado usuario (VPN En léxico ingles significa virtual Private Network, traducido Redes privadas Virtuales).

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes se han instalado por administradores de sistemas o de redes por su simplicidad de implementación, sin tener en consideración la seguridad y por tanto han convertido sus redes en redes abiertas, sin proteger el acceso a la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes, las más comunes son la utilización de protocolos de encriptación de datos como el

WEP y el WPA, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) y 802.1x, proporcionados por o mediando otros dispositivos de la red de datos [Paz, 2009]. Por otra parte, los dispositivos físicos de seguridad que se desarrollan para una óptima seguridad de un sistema de red o así como también los IDS,quedándose obsoletos debido a que son vulnerados por aquellos personajes conocidos en la cibersociedad los cuales pueden ser los hackers, crackers, lamers o un simple virus.

3.1.1 Seguridad En Redes Wi-Fi Inalámbricas

La seguridad es el punto débil de las redes inalámbricas, pues la señal se propaga por el aire en todas las direcciones y puede ser captada a distancia de centenares de metros, utilizando una notebook con antena. Esto hace que las redes inalámbricas sean vulnerables a ser interceptadas [Wikipedia, 2010].

Si nuestra instalación está abierta, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna o a nuestro equipo -donde podríamos tener carpetas compartidas- o analizar toda la información que viaja por nuestra red -mediante sniffers- y obtener así contraseñas de nuestras cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.
Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando analizamos el entorno corporativo nos damos cuenta de que las redes cerradas son más bien escasas.

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales se pueden destacar:

- Al ser redes de tecnología inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, no así en la tecnología por cable.

- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo se puden utilizar la tecnología Wi-Fi con una compatibilidad total. Esto no ocurre, por ejemplo, en móviles.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema Wi-Fi es una menor velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.

La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente fáciles de conseguir con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos muchas compañías no permiten a sus empleados tener una red inalámbrica. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista (desde fuera de una oficina, desde una vivienda colindante) [Wikipedia, 2010].

La mayoría de los problemas de seguridad en WLAN son debidos al medio de transmisión utilizado, el aire, que es de fácil acceso para los atacantes. Por ello, hay que establecer unos medios para asegurar la privacidad de nuestros datos. - Medios Físicos - Medios Lógicos (SW) . En la Seguridad Lógica principalmente son técnicas de cifrado e integridad de la información y técnicas de Autenticación/ Autorización/ Accounting (AAA) . Estos dos tipos de técnicas pueden complementarse. Los primeros pasos para hacer más segura una WLAN: No emitir públicamente la SSID de la WLAN, para no permitir su conexión al AP.

Los problemas que se puede presentar son:

- Se puede obtener fácilmente escuchando tráfico de la WLAN.
- Definición de un listado de los dispositivos que pueden acceder o no, mediante la dirección MAC del dispositivo.
- Se puede falsear la dirección MAC de un dispositivo .

La Seguridad Cifrado e integridad de la información. Se encargan de mantener la privacidad de nuestros datos, y de evitar posibles suplantaciones de personalidad en la comunicación. El cifrado se basa en claves compartidas previamente (Pre-Shared Key) o que se asignan de forma dinámica. - WEP (WiredEquivalentPrivacy) - WPA (Wi-Fi Protected Access) - WPA2 [Share, 2011].

3.1.1.1 Protocolos De Seguridad En Redes Inalámbricas

Al contar con la aucencia de algun método de seguridad. Esta opción no es recomendable, ya que permite a los usuarios no autorizados a acceder a la WLAN de la red, aunque todavía se puede limitar el acceso de la WLAN mediante la creación de reglas de firewall. Este método es adecuado para la creación de puntos de acceso público.

La utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos [Wikipedia, 2010].

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire. Este tipo de cifrado no esta muy recomendado, debido a las grandes vulnerabilidades que presenta, ya que cualquier cracker puede conseguir sacar la clave.

En el WEP (WiredEquivalentPrivacy) método de cifrado de seguridad, las estaciones inalámbricas deben utilizar una clave pre-compartida para conectarse a la red. Este método no

es recomendable, debido a fallos de seguridad conocidos en el protocolo WEP. Se proporciona para la compatibilidad con las implementaciones inalámbricas

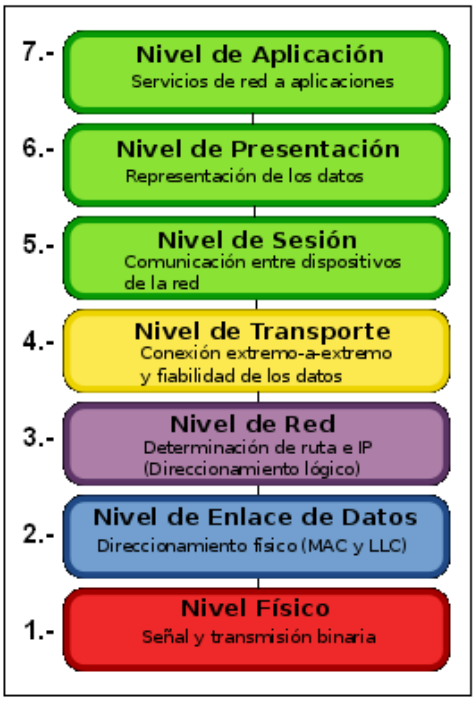
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE802.1X, que permite la autenticación y autorización de usuarios.
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo mas recomendable si solo se va a usar con pocos equipos.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

3.2 Modelo De Referencia OSI

En 1984, la Organización Internacional de Estandarización (ISO) desarrolló un modelo llamado **OSI (Open SystemsInterconectiòn**, Interconexión de sistemas abiertos). El cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red [Puigdemunti, 1999].

Fig.3.1. Capas del Modelo de Referencia OSI



Fuente:[Wikipedia, 2011] Pag.1

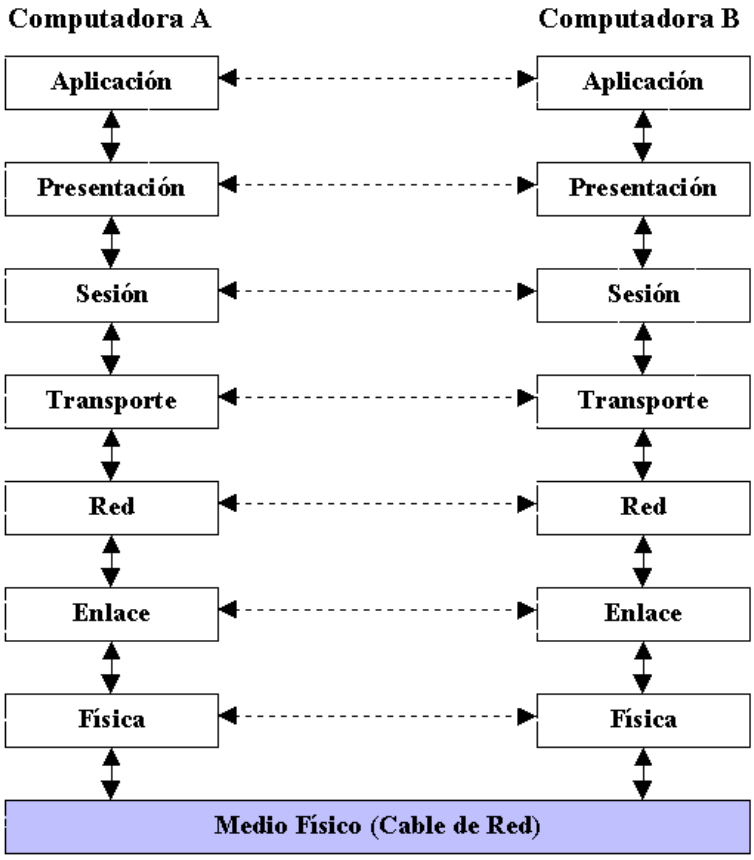
Como se muestra en la figura 3.1, las capas OSI están numeradas de abajo hacia arriba. Las funciones más básicas, como el poner los bits de datos en el cable de la red están en la parte de abajo, mientras las funciones que atienden los detalles de las aplicaciones del usuario están arriba.

En el modelo OSI el propósito de cada capa es proveer los servicios para la siguiente capa superior, resguardando la capa de los detalles de como los servicios son implementados realmente. Las capas son abstraídas de tal manera que cada capa cree que se está comunicando con la capa asociada en la otra computadora, cuando realmente cada capa se comunica sólo con las capas adyacentes de las mismas computadoras.

Como se observa en la figura 3.2, se puede apreciar que a excepción de la capa más baja del modelo OSI, ninguna capa puede pasar información directamente a su contraparte en la otra

computadora. La información que envía una computadora debe de pasar por todas las capas inferiores, La información entonces se mueve a través del cable de red hacia la computadora que recibe y hacia arriba a través de las capas de esta misma computadora hasta que llega al mismo nivel de la capa que envió la información. Por ejemplo, si la capa de red enviainformaciòn desde la computadora A, esta información se mueve hacia abajo a través de las capas de Enlace y Física del lado que envia, pasa por el cable de red, y sube por las capas de Física y Enlace del lado del receptor hasta llegar a la capa de red de la computadora B.

Fig. 3.2 Comunicación de las Capas



Fuente: [Puigdemunti, 1999] Pag.1

La interacción entre las diferentes capas adyacentes se llama interface. La interface define que servicios la capa inferior ofrece a su capa superior y como esos servicios son accesados. Además, cada capa en una computadora actúa como si estuviera comunicándose directamente

con la misma capa de la otra computadora. La serie de las reglas que se usan para la comunicación entre las capas se llama protocolo.

La ISO (International OrganisationforStandarisation) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores. El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca. El modelo OSI describe siete niveles para facilitar los interfaces de conexión entre sistemas abiertos [Jonathan, 2004].

Nivel 1.- **Físico** - Se ocupa de la transmisión del flujo de bits a través del medio. - Cables, tarjetas y repetidores (hub).

RS-232, X.21.

Nivel 2 - **Enlace** - Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos. - Puentes (bridges). HDLC y LLC.

Nivel 3 - **Red** - Establece las comunicaciones y determina el camino que tomarán los datos en la red. - Encaminador(router). IP, IPX.

Nivel 4 - **Transporte** - La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente. - Pasarela (gateway). UDP, TCP, SPX.

Nivel 5 - **Sesión** - Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones). – Pasarela.

Nivel 6 - **Presentación** - Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes. - Pasarela. Compresión, encriptado, VT100.

Nivel 7 - **Aplicación** - Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero). - X400.

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas datos de control como se muestra en la fig. 3.3.

De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. La forma, pues de enviar información en el modelo OSI tiene una cierta similitud con enviar un paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí.

Fig. 3.3 C7-C2: Datos de control específicos de cada nivel.

Emisor	**Paquete**	**Receptor**
Aplicación	C7 Datos	Aplicación
Presentación	C6 C7 Datos	Presentación
Sesión	C5 C6 C7 Datos	Sesión
Transporte	C4 C5 C6 C7 Datos	Transporte
Red	C3 C4 C5 C6 C7 Datos	Red
Enlace	C2 C3 C4 C5 C6 C7 Datos	Enlace
Físico	C2 C3 C4 C5 C6 C7 Datos	Físico

Fuente: [Jonathan, 2004]Pag.1

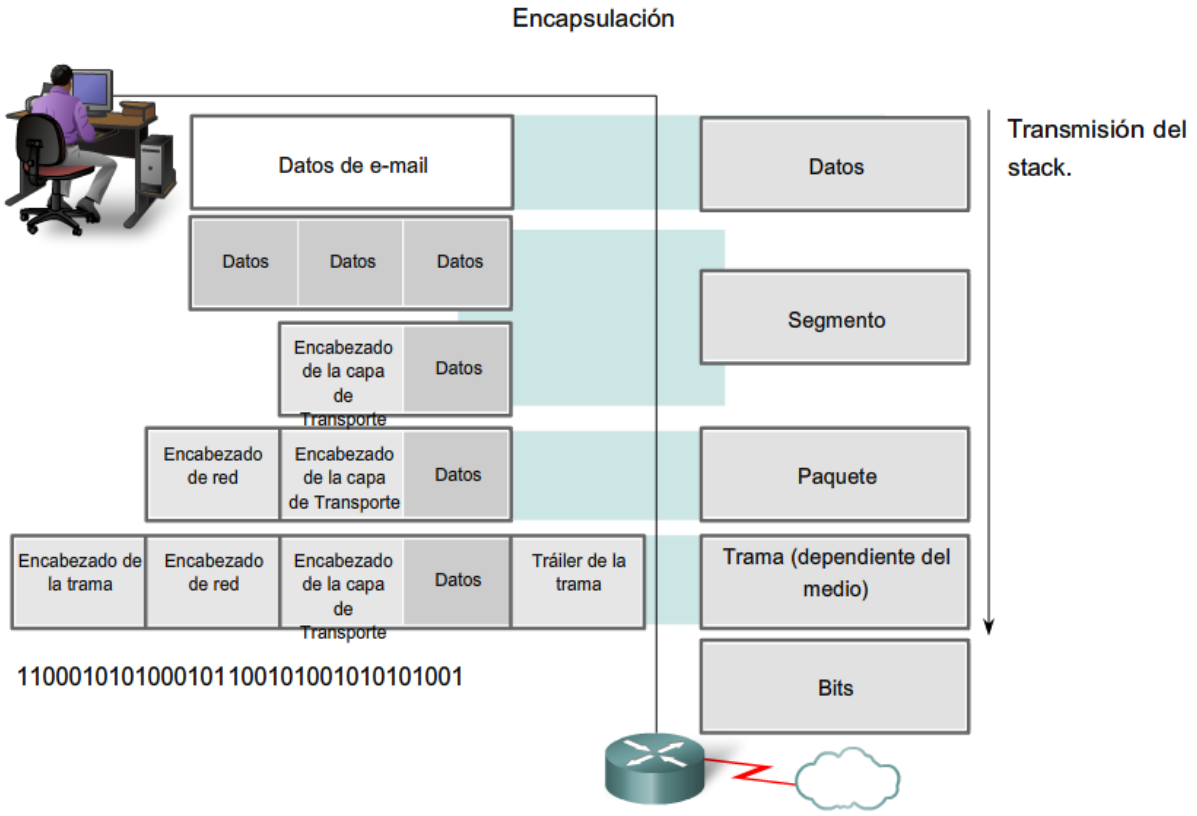
Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que se llaman**protocolos**. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.
En las familias de protocolos más utilizadas en redes de ordenadores (TCP/IP, IPX/SPX, etc.) se encuentra a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

Cabe notar que esta investigación está orientada a un nivel bajo por tanto las operaciones de comunicación se lo realiza o se direcciona al nivel 1 que es la capa física, nivel 2 la capa de enlace y como máximo llega a un nivel 3 la capa de Red.

- **Transmisión de datos en el Modelo OSI.**

En la Fig. 3.4 se muestra de cómo se pueden transmitir datos empleando el modelo OSI:

Fig.3.4 Transferencia de información en el modelo OSI.



Fuente: [Wikipedia, 2011] Pag.1

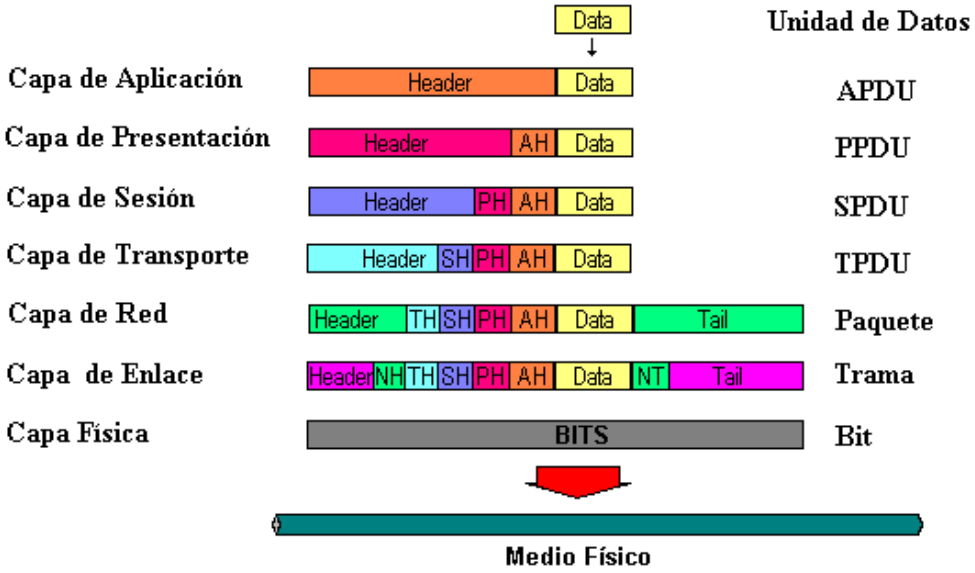
La capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU de la capa de aplicación. La PDU se transfiere a la capa de aplicación del nodo destino, este elimina la cabecera y entrega el mensaje al usuario [Wikipedia, 2011].

Para ello ha sido necesario todo este proceso:

1. Ahora hay que entregar la PDU a la capa de presentación para ello hay que añadirle la correspondiente cabecera ICI y transformarla así en una IDU, la cual se transmite a dicha capa.
2. La capa de presentación recibe la IDU, le quita la cabecera y extrae la información, es decir, la SDU, a esta le añade su propia cabecera (PCI) constituyendo así la PDU de la capa de presentación.
3. Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.
4. Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.
5. Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar la PDU a la capa superior.
6. Finalmente llegará a la capa de aplicación la cual entregará el mensaje al usuario.

Otros datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren, debido a como se describió anteriormente la adhesión de una serie de encabezados e información final. Los formatos de información son los que muestra en la fig.3.5 [Wikipedia, 2011]:

Fig. 3.5 Formato de Datos



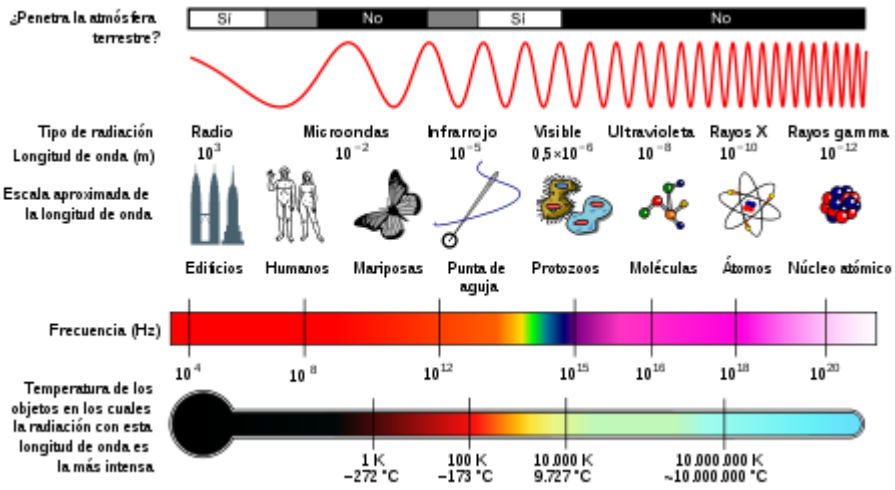
Fuente: [Wikipedia, 2011] Pag.1

APDU ..... Unidad de datos en capa de aplicación(capa 7).
PPDU ..... Unidad de datos en la capa de presentación(capa 6).
SPDU ..... Unidad de datos en la capa de sesión(capa 5).
TPDU (segmento) ..... Unidad de datos en la capa de transporte(capa 4).
Paquete o Datagrama . Unidad de datos en el nivel de red(capa 3).
Trama ..... Unidad de datos en la capa de enlace(capa 2).
Bits ..... Unidad de datos en la capa física(capa 1).

3.3 Espacio Electromagnético

Se denomina espacio o espectro electromagnético a la distribución energética del conjunto de las ondas electromagnéticas. Referido a un objeto se denomina espectro electromagnético o simplemente espectro a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar. Los espectros se pueden observar mediante espectroscopios que, además de permitir observar el espectro, permiten realizar medidas sobre éste, como la longitud de onda, la frecuencia y la intensidad de la radiación como se ejemplifica en la fig.3.6.[Wikipedia, 2011].

Fig3.6. Diagrama del espectro electromagnético, mostrando el tipo, longitud de onda con ejemplos, frecuencia y temperatura de emisión de cuerpo negro



Fuente: [Wikipedia, 2011] pag.1

El espectro electromagnético se extiende desde la radiación de menor longitud de onda, como los rayos gamma y los rayos X, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio. Se cree que el límite para la longitud de onda más pequeña posible es la longitud de Planck mientras que el límite máximo sería el tamaño del Universo, aunque formalmente el espectro electromagnético es infinito y continuo.

- **Rango energético del espectro**

El espectro electromagnético cubre longitudes de onda muy variadas. Existen frecuencias de 30 Hzs y menores que son relevantes en el estudio de ciertas nebulosas.[1] Por otro lado se conocen frecuencias cercanas a $2{,}9\times10^{27}$ Hz, que han sido detectadas provenientes de fuentes astrofísicas.[2]

La energía electromagnética en una particular longitud de ondaλ (en el vacío) tiene una frecuencia f asociada y una energía de fotónE. Por tanto, el espectro electromagnético puede

ser expresado igualmente en cualquiera de esos términos. Se relacionan en las siguientes ecuaciones:

$$C = f\lambda \text{ , o lo que es lo mismo } \lambda = \frac{C}{f}$$

$$E = hf \text{ , o lo que es lo mismo } E = \frac{hC}{\lambda}$$

Donde C = 299.792.458 m/s (velocidad de la luz) y *h* es la constante de Planck, ($h \approx 6{,}626069.10^{-34} J.s \approx 4{,}13567\ \mu eV/GHz$).

Por lo tanto, las ondas electromagnéticas de alta frecuencia tienen una longitud de onda corta y mucha energía mientras que las ondas de baja frecuencia tienen grandes longitudes de onda y poca energía. Por lo general, las radiaciones electromagnéticas se clasifican en base a su longitud de onda en ondas de radio, microondas, infrarrojos, visible – que percibimos como luzvisible – ultravioleta, rayos X y rayos gamma. El comportamiento de las radiaciones electromagnéticas depende de su longitud de onda. Cuando la radiación electromagnética interactúa con átomos y moléculas puntuales, su comportamiento también depende de la cantidad de energía por quantum que lleve. Al igual que las ondas de sonido, la radiación electromagnética puede dividirse en octavas. La espectroscopía puede detectar una región mucho más amplia del espectro electromagnético que el rango visible de 400 a 700 nm. Un espectrómetro de laboratorio común y corriente detecta longitudes de onda de 2 a 2500 nm.

- **Bandas del espectro electromagnético**

Para su estudio, el espectro electromagnético se divide en segmentos o bandas, como se observa en la fig. 3.6, aunque esta división es inexacta. Existen ondas que tienen una frecuencia, pero varios usos, por lo que algunas frecuencias pueden quedar en ocasiones incluidas en dos rangos.

Fig. 3.6 Bandas del espectro electromagnético

Banda	Longitud de onda (m)	Frecuencia (Hz)	Energía (J)
Rayos gamma	< 10 pm	> 30,0 EHz	$> 20 \cdot 10^{-15}$ J
Rayos X	< 10 nm	> 30,0 PHz	$> 20 \cdot 10^{-18}$ J
Ultravioleta extremo	< 200 nm	> 1,5 PHz	$> 993 \cdot 10^{-21}$ J
Ultravioleta cercano	< 380 nm	> 789 THz	$> 523 \cdot 10^{-21}$ J
Luz Visible	< 780 nm	> 384 THz	$> 255 \cdot 10^{-21}$ J
Infrarrojo cercano	< 2,5 µm	> 120 THz	$> 79 \cdot 10^{-21}$ J
Infrarrojo medio	< 50 µm	> 6,00 THz	$> 4 \cdot 10^{-21}$ J
Infrarrojo lejano/submilimétrico	< 1 mm	> 300 GHz	$> 200 \cdot 10^{-24}$ J
Microondas	< 30 cm	> 1 GHz	$> 2 \cdot 10^{-24}$ J
Ultra Alta Frecuencia - Radio	< 1 m	> 300 MHz	$> 19.8 \cdot 10^{-26}$ J
Muy Alta Frecuencia - Radio	< 10 m	> 30 MHz	$> 19.8 \cdot 10^{-28}$ J
Onda Corta - Radio	< 180 m	> 1,7 MHz	$> 11.22 \cdot 10^{-28}$ J
Onda Media - Radio	< 650 m	> 650 kHz	$> 42.9 \cdot 10^{-29}$ J
Onda Larga - Radio	< 10 km	> 30 kHz	$> 19.8 \cdot 10^{-30}$ J
Muy Baja Frecuencia - Radio	> 10 km	< 30 kHz	$< 19.8 \cdot 10^{-30}$ J

Fuente: [Wikipedia, 2011] pag.1

- **Radiofrecuencia**

En radiocomunicaciones, los rangos se abrevian con sus siglas en inglés como se muestra en la fig.3.7. Y se pueden observar que los rangos son:

Fig. 3.7 Rangos en radiofrecuencia

Nombre	Abreviatura inglesa	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
Extra baja frecuencia	ELF	1	3-30 Hz	100.000–10.000 km
Super baja frecuencia	SLF	2	30-300 Hz	10.000–1000 km
Ultra baja frecuencia	ULF	3	300–3000 Hz	1000–100 km
Muy baja frecuencia	VLF	4	3–30 kHz	100–10 km
Baja frecuencia	LF	5	30–300 kHz	10–1 km
Media frecuencia	MF	6	300–3000 kHz	1 km – 100 m
Alta frecuencia	HF	7	3–30 MHz	100–10 m
Muy alta frecuencia	VHF	8	30–300 MHz	10–1 m
Ultra alta frecuencia	UHF	9	300–3000 MHz	1 m – 100 mm
Super alta frecuencia	SHF	10	3-30 GHz	100-10 mm
Extra alta frecuencia	EHF	11	30-300 GHz	10–1 mm
			Por encima de los 300 GHz	< 1 mm

Fuente: [Wikipedia, 2011] pag.1

- **Frecuencias extremadamente bajas**: Llamadas ELF (ExtremelyLowFrequencies), son aquellas que se encuentran en el intervalo de 3 a 30 Hz. Este rango es equivalente a aquellas frecuencias del sonido en la parte más baja (grave) del intervalo de percepción del oído humano. Cabe destacar aquí que el oído humano percibe ondas sonoras, no electromagnéticas, sin embargo se establece la analogía para poder hacer una mejor comparación.
- **Frecuencias super bajas**: SLF (SuperLowFrequencies), son aquellas que se encuentran en el intervalo de 30 a 300 Hz. En este rango se incluyen las ondas electromagnéticas de frecuencia equivalente a los sonidos graves que percibe el oído humano típico.
- **Frecuencias ultra bajas**: ULF (Ultra LowFrequencies), son aquellas en el intervalo de 300 a 3000 Hz. Este es el intervalo equivalente a la frecuencia sonora normal para la mayor parte de la voz humana.

- **Frecuencias muy bajas**: VLF, VeryLowFrequencies. Se pueden incluir aquí las frecuencias de 3 a 30 kHz. El intervalo de VLF es usado típicamente en comunicaciones gubernamentales y militares.
- **Frecuencias bajas**: LF, (LowFrequencies), son aquellas en el intervalo de 30 a 300 kHz. Los principales servicios de comunicaciones que trabajan en este rango están la navegación aeronáutica y marina.
- **Frecuencias medias**: MF, Medium Frequencies, están en el intervalo de 300 a 3000 kHz. Las ondas más importantes en este rango son las de radiodifusión de AM (530 a 1605 kHz).
- **Frecuencias altas**: HF, High Frequencies, son aquellas contenidas en el rango de 3 a 30 MHz. A estas se les conoce también como "onda corta". Es en este intervalo que se tiene una amplia gama de tipos de radiocomunicaciones como radiodifusión, comunicaciones gubernamentales y militares. Las comunicaciones en banda de radioaficionados y banda civil también ocurren en esta parte del espectro.
- **Frecuencias muy altas**: VHF, Very High Frequencies, van de 30 a 300 MHz. Es un rango popular usado para muchos servicios, como la radio móvil, comunicaciones marinas y aeronáuticas, transmisión de radio en FM (88 a 108 MHz) y los canales de televisión del 2 al 12 [según norma CCIR (Estándar B+G Europa)]. También hay varias bandas de radioaficionados en este rango.
- **Frecuencias ultra altas**: UHF, Ultra High Frequencies, abarcan de 300 a 3000 MHz, incluye los canales de televisión de UHF, es decir, del 21 al 69 [según norma CCIR (Estándar B+G Europa)] y se usan también en servicios móviles de comunicación en tierra, en servicios de telefonía celular y en comunicaciones militares.
- **Frecuencias super altas**: SHF, Super High Frequencies, son aquellas entre 3 y 30 GHz y son ampliamente utilizadas para comunicaciones vía satélite y radioenlaces terrestres. Además, pretenden utilizarse en comunicaciones de alta tasa de transmisión de datos a muy corto alcance mediante UWB. También son utilizadas con fines militares, por ejemplo en radares basados en UWB.
- **Frecuencias extremadamente altas**: EHF, Extrematedly High Frequencies, se extienden de 30 a 300 GHz. Los equipos usados para transmitir y recibir estas señales son más complejos y costosos, por lo que no están muy difundidos aún.

Existen otras formas de clasificar las ondas de radiofrecuencia:

- **Microondas**

Cabe destacar que las frecuencias entre 1 GHz y 300 GHz, son llamadas microondas. Estas frecuencias abarcan parte del rango de UHF y todo el rango de SHF y EHF. Estas ondas se utilizan en numerosos sistemas, como múltiples dispositivos de transmisión de datos, radares y hornos microondas, se ejemplifica en la fig.3.8.

Fig. 3.8. Bandas de frecuencia de microondas

Banda	P	L	S	C	X	K_u	K	K_a	Q	U	V	E	W	F	D
Inicio (GHZ)	0,2	1	2	4	8	12	18	26,5	30	40	50	60	75	90	110
Final (GHZ)	1	2	4	8	12	18	26,5	40	50	60	75	90	110	140	170

Fuente: [Wikipedia, 2011] pag.1

- **Infrarrojo**

Las ondas infrarrojas están en el rango de 0,7 a 100 micrómetros. La radiación infrarroja se asocia generalmente con el calor. Éstas son producidas por cuerpos que generan calor, aunque a veces pueden ser generadas por algunos diodos emisores de luz y algunos láseres.

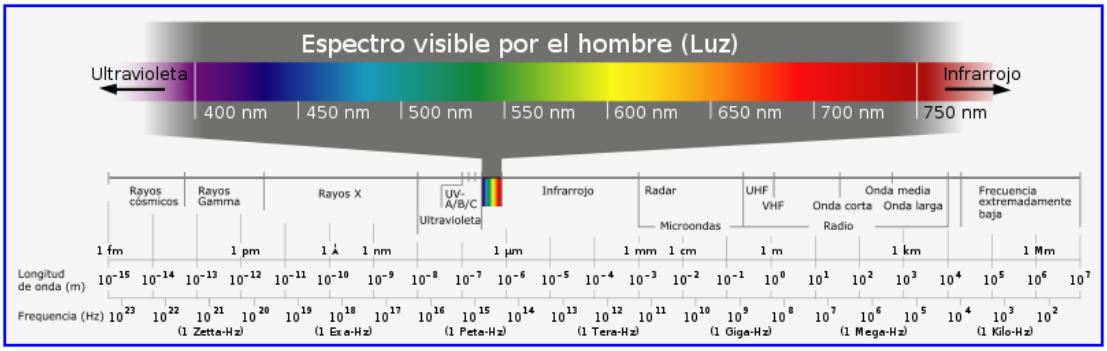
Las señales son usadas para algunos sistemas especiales de comunicaciones, como en astronomía para detectar estrellas y otros cuerpos y para guías en armas, en los que se usan detectores de calor para descubrir cuerpos móviles en la oscuridad. También se usan en los mandos a distancia de los televisores y otros aparatos, en los que un transmisor de estas ondas envía una señal codificada al receptor del televisor. En últimas fechas se ha estado implementando conexiones de área local LAN por medio de dispositivos que trabajan con infrarrojos, pero debido a los nuevos estándares de comunicación estas conexiones han perdido su versatilidad.

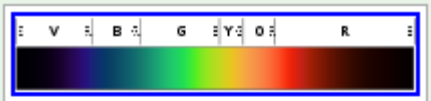
- **Espectro visible**

Por encima de la frecuencia de las radiaciones infrarrojas se encuentra lo que comúnmente es llamado luz, un tipo especial de radiación electromagnética que tiene una longitud de onda en

el intervalo de 0,4 a 0,8 micrómetros. La unidad usual para expresar las longitudes de onda es el Angstrom. Los intervalos van desde los 8.000 Å(rojo) hasta los 4.000 Å (violeta), donde la onda más corta es la del color violeta como se muestra en la fig.3.9.

Fig. 3.9 Espectro electromagnético





Color	Longitud de onda
violeta	380–450 nm
azul	450–495 nm
verde	495–570 nm
amarillo	570–590 nm
naranja	590–620 nm
rojo	620–750 nm

Fuente: [Wikipedia, 2011] pag.1

La luz puede usarse para diferentes tipos de comunicaciones. Las ondas de luz pueden modularse y transmitirse a través de fibras ópticas, lo cual representa una ventaja pues con su alta frecuencia es capaz de llevar más información.

Por otro lado, las ondas de luz pueden transmitirse en el espacio libre, usando un haz visible de láser.

- **Ultravioleta**

La luz ultravioleta cubre el intervalo de 4 a 400 nm. El Sol es una importante fuente emisora de rayos en esta frecuencia, los cuales causan cáncer de piel a exposiciones prolongadas. Este tipo de onda no se usa en las telecomunicaciones, sus aplicaciones son principalmente en el campo de la medicina.

- **Rayos X**

La denominación rayos X designa a una radiación electromagnética, invisible, capaz de atravesar cuerpos opacos y de impresionar las películas fotográficas. La longitud de onda está entre 10 a 0,1 nanómetros, correspondiendo a frecuencias en el rango de 30 a 3.000 PHz (de 50 a 5.000 veces la frecuencia de la luz visible).

- **Rayos gamma**

La radiación gamma es un tipo de radiación electromagnética producida generalmente por elementos radioactivos o procesos subatómicos como la aniquilación de un par positrón-electrón. Este tipo de radiación de tal magnitud también es producida en fenómenos astrofísicos de gran violencia. Debido a las altas energías que poseen, los rayos gamma constituyen un tipo de radiación ionizante capaz de penetrar en la materia más profundamente que la radiación alfa o beta. Dada su alta energía pueden causar grave daño al núcleo de las células, por lo que son usados para esterilizar equipos médicos y alimentos.

3.4 Antenas Inalámbricas

La definición formal de una antena es un dispositivo que sirve para transmitir y recibir ondas de radio. Convierte la onda guiada por la línea de transmisión (el cable o guía de onda) en ondas electromagnéticas que se pueden transmitir por el espacio libre. Así mismo, dependiendo de su forma y orientación, pueden captar diferentes frecuencias, así como niveles de intensidad.

3.4.1 Tipos De Antenas Inalámbricas

Hay distintos tipos de antenas inalámbricas, las mas conocidas son las antenas direccionales y omnidireccionales, las primeras emiten/capturan la señal en una dirección y tienen más alcance, generalmente son utilizadas para conectar puntos muy distantes; las segundas emiten/capturan la señal en todas direcciones y tienen menos alcance, por ejemplo pueden ser utilizadas para darle cobertura a toda una casa [Spam, 2008].

Las antenas de redes inalámbricas se pueden dividir en tres tipos:

- **Antenas direccionales (o directivas)**

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz concreto y estrecho pero de forma intensa (más alcance). Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores. El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

- **Antena omnidireccionales**

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance. Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales. El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

- **Antenas sectoriales**

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal. Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) se deberá instalar o tres antenas sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

3.4.2 Potencias de Transmisión en Antenas Inalámbricas

El ancho de banda de la antena se define como el rango de frecuencias sobre las cuales la operación de la antena es "satisfactoria". Esto, por lo general se toma entre los puntos de media potencia, pero a veces se refiere a las variaciones en la impedancia de entrada de la antena.Cada subconjunto o banda de frecuencias dentro del espectro electromagnético tiene propiedades únicas que son el resultado de cambios en la longitud de onda. Por ejemplo, las frecuencias medias (MF, Medium Frequencies) que van de los 300 kHz a los 3 MHz pueden ser radiadas a lo largo de la superficie de la tierra sobre cientos de kilómetros, perfecto para las estaciones de radio AM (Amplitud Modulada) de la región. Las estaciones de radio internacionales usan las bandas conocidas como ondas cortas (SW, Short Wave) en la banda de HF (High Frequency) que va desde los 3 MHz a los 30 MHz. Este tipo de ondas pueden ser radiadas a miles de kilómetros y son rebotadas de nuevo a la tierra por la ionosfera como si fuera un espejo, por tal motivo las estaciones de onda corta son escuchadas casi en todo el mundo.Los estaciones de FM (Frecuencia Modulada) y TV (televisión) utilizan las bandas conocidas como VHF (Very High Frequency) y UHF (Ultra High Frequency) localizadas de los 30 MHz a los 300 MHz y de los 300 MHz a los 900 MHz, este tipo de señales debido a que no son reflejadas por la ionosfera cubren distancias cortas, una ciudad por ejemplo. La ventaja de usar este tipo de bandas de frecuencias para comunicaciones locales permite que

docenas de estaciones de radio FM y televisoras " en ciudades diferentes " puedan usar frecuencias idénticas sin causar interferencia entre ellas como se muestra en la fig. 3.10.

Fig. 3.10 Espectro Electromagnético de Antenas Inalámbricas

Espectro electromagnético			
Banda	**Significado**	**Rango de Frecuencias**	**Servicios**
VLF	Very Low Frequency	3 kHz - 30 kHz	Conducción de electricidad
LF	Low Frequency	30 kHz - 300 kHz	Conducción de electricidad, navegación marítima, control de tráfico aéreo
MF	Medium Frequency	300 kHz - 3 MHz	Radio AM
HF	High Frequency	3 MHz - 30 MHz	Radio SW
VHF	Very High Frequency	30 MHz - 300 MHz	Radio FM, TV, radio dos vías
UHF	Ultra High Frequency	300 MHz - 3 GHz	TV UHF, telefonía celular, WLL, comunicaciones móviles
SHF	Super High Frequency	3 GHz - 30 GHz	Servicios por Satélite y microondas, MMDS, LMDS
EHF	Extremely High Frequency	30 GHz en adelante	LMDS
Infrarojo		3 x 1012 - 4.3 x 1014 Hz	WPANs
Luz visible		4.3 x 1014 - 7.5 x 1014 Hz	Fibras ópticas
Ultravioleta		7.5 x 1014 - 3 x 1017 Hz	
1 kHz = 1x103 Hz 1 MHz = 1x106 Hz 1 GHz = 1x109 Hz WLL = Wireless Local Loop MMDS = Multichannel Multipoint Distribution Service LMDS= Local Multipoint Distribution Service WPANs = Wireless Personal Area Networks			

Fuente: [Martínez, 2002] Pag.1

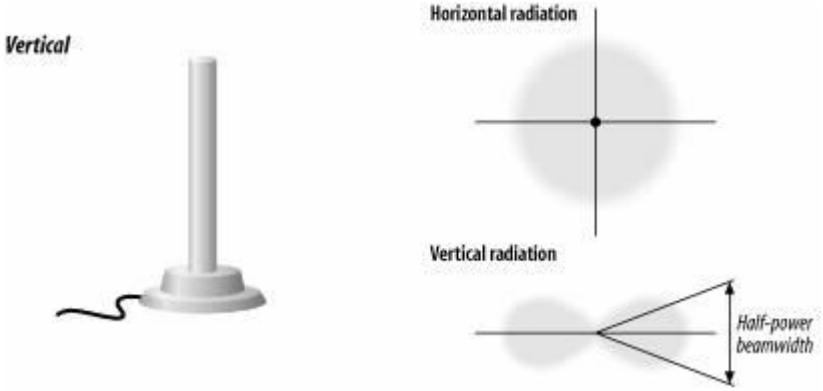
- **Antena Omnidireccional.**

  - **Monopolo Vertical**

Es una antena constituida de un solo brazo rectilíneo irradiante en posición vertical. Se puede ver una antena vertical con Ganancias de 3 dBi hasta 17 dBi.

- El uso en VHF es principalmente para las aplicaciones de radio móvil en vehículos.
- En Monopolos de ¼ de onda: la impedancia de la antena es de 36 ohmios

Fig.3.11 Antena OmnidireccionalMonopolo Vertical

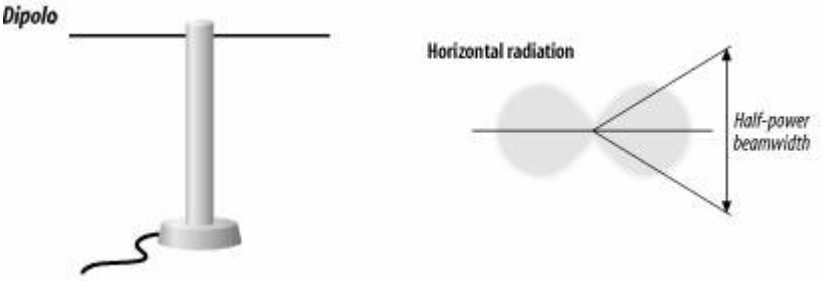


Fuente: [Martínez, 2002] Pag.1

- **Dipolo**

- Usada en frecuencias arriba de 2MHz
- Ganancia baja: 2.2 dBi
- Angulo de radiación ancho
- En el espacio ideal, la impedancia del dipolo simple es de 73 Ohm.

Fig. 3.12Antena Omnidireccional Dipolo



Fuente: [Martínez, 2002] Pag.1

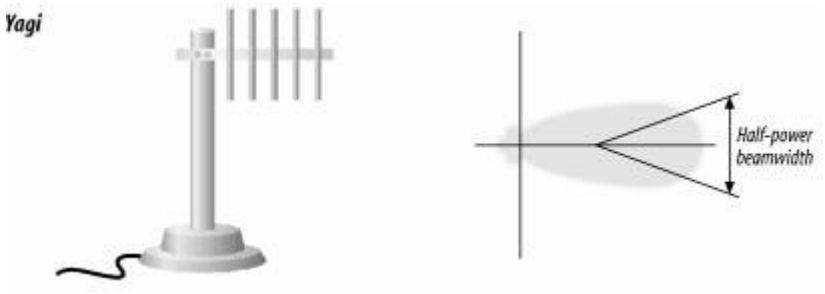
- **Antenas Direccionales**

  - **Yagi**

Antena constituida por varios elementos paralelos y coplanarios, directores, activos y reflectores.

- Utilizada ampliamente en la recepción de señales televisivas, comúnmente en frecuencias de 30Mhz y 3Ghz, (canal 2 al canal 6 de 50MHz a 86 MHz).
- Ganancia elevada: 8-15 dBi
- Para el servicio 802.11 pueden tener ganancias entre el dBi 12 y 18. Manejan una impedancia de 50 a 75 Ohms
- Desventajas: Direccionarlas en la posición correcta no son tan difícil como una antena parabólica, pero aun así puede llegar a ser difícil.

Fig. 3.13Antenas Direccionales Yagi



Fuente: [Martínez, 2002] Pag.1

- **Parabólica**

Antena provista de un reflector metálico, de forma parabólica, esférica o de bocina, que limita las radiaciones a un cierto espacio, concentrando la potencia de las ondas.

- Se utiliza especialmente para la transmisión y recepción vía satélite.
- Ganancia alta: 12-25 dBi
- Directividad alta
- Ángulo de radiación bajo

Fig. 3.14 Antenas Direccionales Parabólica



Fuente: [Martínez, 2002] Pag.1

- **Infrarrojo**

Los enlaces infrarrojos se encuentran limitados por el espacio y los obstáculos. El hecho de que la longitud de onda de los rayos infrarrojos sea tan pequeña (850-900 nm), hace que no pueda propagarse de la misma forma en que lo hacen las señales de radio.

Fig. 3.15Antenas DireccionalesLaser Infrarrojo



Fuente: [Martínez, 2002] Pag.1

- **Panel o 'PatchAntenna'**

- Panel o .parche. metálico radiante sobre un plano de tierra metálico.
- Normalmente planas, en encapsulado de PVC.
- Ganancia media-elevada: 5-20 dBi
- Directividad moderada
- Ángulo de radiación medio

Fig. 3.16Antenas Direccionales Panel

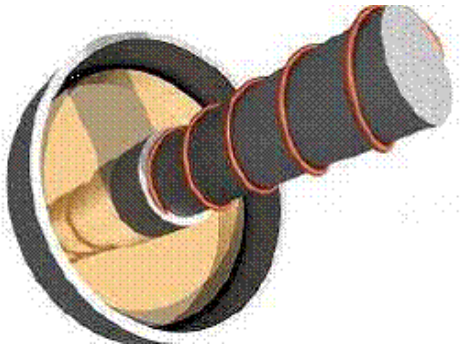


Fuente: [Martínez, 2002] Pag.1

- **Helicoidal (modo axial)**

- Hilo conductor bobinado sobre un soporte rígido. Detrás plano de tierra.
- Ganancia media-elevada: 6-18 dBi
- Directividad moderada
- Ángulo de radiación medio

Fig. 3.17 Antenas Direccionales Helicoidal



Fuente: [Martínez, 2002] Pag.1

- **Microondas terrestres**

- Microondas: rango de frecuencias comprendido entre 2 GHz y 40 GHz
- Son altamente direccionales
    - Requieren antenas parabólicas en la recepción
- Las antenas han de estar muy altas para evitar obstáculos
- Constituyen una alternativa al cable coaxial y a la fibra óptica para comunicaciones a larga distancia
- Otras aplicaciones
    - Transmisión de televisión y voz

Fig. 3.18Antenas Direccionales Microondas



Fuente: [Martínez, 2002] Pag.1

- **Microondas por satélite**

- Se usa un rango de frecuencias entre 1GHz a 50 Ghz
- Los satélites
    - Reciben una señal terrestre
    - La señal es amplificada o repetida
    - Envían la señal a uno o varios receptores terrestres
- Los satélites han de tener órbita geoestacionaria
    - A una distancia de 35,784 km
- Se producen retardos en las comunicaciones
- Aplicaciones
    - Televisión, telefonía a larga distancia, redes privadas

Fig. 3.19 Antenas Direccionales Microondas por Satélite



Fuente: [Martínez, 2002] Pag.1

3.5 Punto De Acceso Inalámbrico (Access Point)

Los puntos de acceso, también llamados APs o wirelessaccesspoint, son equipos hardware configurados en redes Wifi y que hacen de intermediario entre el ordenador y la red externa (local o Internet). El accesspoint o punto de acceso, hace de transmisor central y receptor de las señales de radio en una red Wireless. Los puntos de acceso utilizados en casa o en oficinas, son generalmente de tamaño pequeño, como se muestra en la fig.3.20, componiéndose de un adaptador de red, una antena y un transmisor de radio. Existen redes Wireless pequeñas que pueden funcionar sin puntos de acceso, llamadas redes *"*ad-hoc*"* o modo *peer-to-peer,* las cuales solo utilizan las tarjetas de red para comunicarse. Las redes mas usuales que se verán son en modo estructurado, es decir, los puntos de acceso harán de intermediario o puente entre los equipos wifi y una red Ethernet cableada. También harán la función de escalar a mas usuarios según se necesite y podrá dotar de algunos elementos de seguridad. Los puntos de acceso normalmente van conectados físicamente por medio de un cable de pares a otro elemento de red, en caso de una oficina o directamente a la línea telefónica si es una conexión doméstica. En este último caso, el AP estará haciendo también el papel de Router. Son los llamados WirelessRouters los cuales soportan los estándar 802.11a, 802.11b y 802.11g. Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a el se llama "celda". Usualmente se hace un estudio para que dichas celdas estén lo mas cerca posible, incluso solapándose un poco. De este modo, un usuario con un portátil, podría moverse de un AP a otro sin perder su conexión de red. Los puntos de acceso antiguos, solían soportar solo a 15 a 20 usuarios. Hoy en día los modernos APs pueden tener hasta 255 usuarios con sus respectivos ordenadores conectándose a ellos. Si conectamos muchos Access Pointjuntos, se pueden llegar a crear una enorme red con miles de usuarios conectados, sin apenas cableado y moviéndose libremente de un lugar a otro con total comodidad. A nivel casero y como se ha dicho, los puntos de acceso inalámbricos nos permitirán conectar varias conexiones Ethernet o Fast Ethernet, y a su vez conectar varios clientes sin cable. Cualquier persona con una tarjeta de red inalámbrica y un portátil puede conectarse a nuestra red Wifi y aprovecharse gratuitamente de nuestro ancho de banda. Para

evitar esto, el AP puede hacer filtrados por MAC o dirección física no permitiendo la conexión de clientes desconocidos. Muchos de estos dispositivos llevan ya instalado su propio Firewall con el que proteger la red [Ordenadores, 2011].

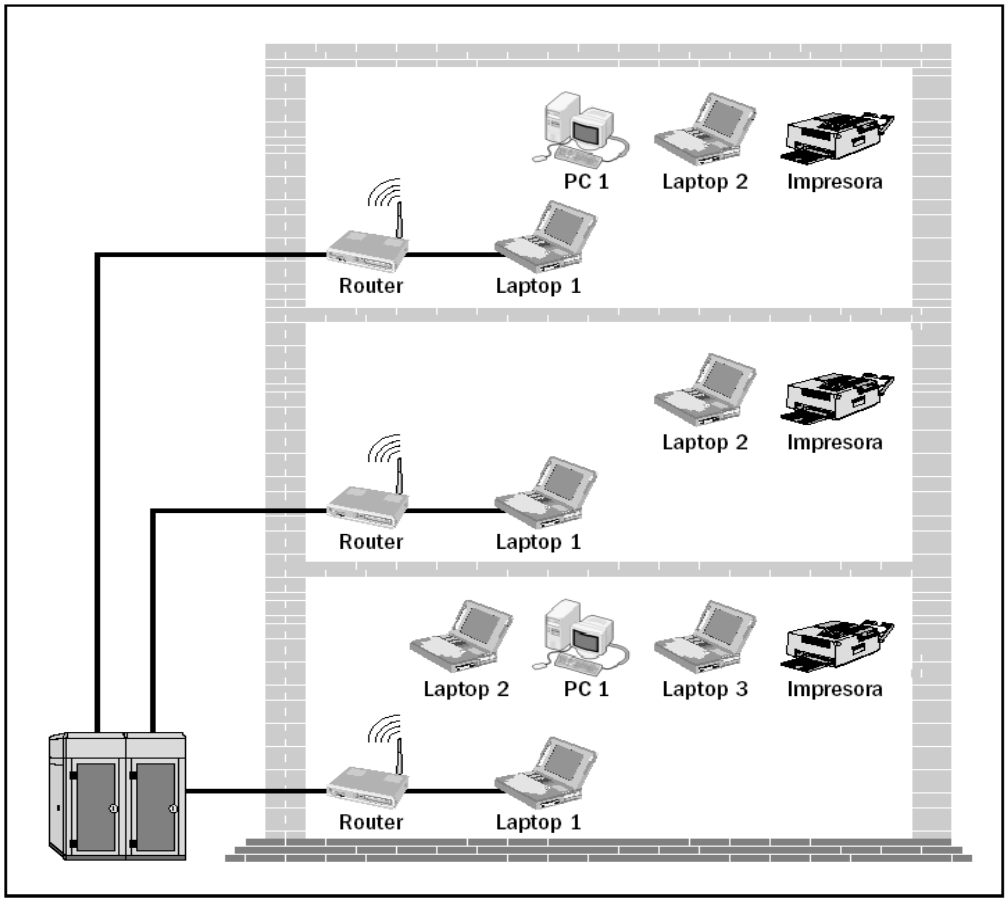
Fig. 3.20 Access Point



Fuente: [Ordenadores, 2011] pag.1

Por medio de la instalación de un Access Point, es posible duplicar la distancia a la cual los dispositivos pueden comunicarse, ya que éstos actúan como repetidores de la señal. Desde que el Access Point se conecta a la red, cualquier cliente tiene acceso a los recursos del servidor y, además, este dispositivo gestiona el tráfico de la red entre las terminales más próximas. Cada Access Point puede servir a varias máquinas, según el tipo y el número de transmisiones que se realicen. Existe un gran número de aplicaciones en el mundo real con un rango de 15 a 50 dispositivos cliente con un solo Access Points. Los Access Point tienen un alcance finito, que generalmente es del orden de los 150 metros en lugares cerrados y de 300 metros en áreas abiertas. En zonas grandes, como por ejemplo un campus universitario o un edificio, es probable que se necesite la instalación de más de uno de éstos (repitiendo la señal). El objetivo es cubrir el área con células que solapen sus áreas así los clientes puedan moverse sin cortes entre los grupos de Access Points. Esto es llamado roaming como ejemplo se muestra en la fig. 3.21 [Lectores, 2011].

Fig.3.21 Ejemplo de roamingentre varios Access Point



Fuente: [Lectores, 2011] pag.27

3.6 Sistema Operativo Ubuntu

Ubuntu es un sistema operativo basado en la distribución Debian GNU / Linuxde distribución y se distribuye como software de código abierto y libre . Es el nombre del África Meridional para la filosofía de Ubuntu ("humanidad hacia otros"). Con un uso global estimada de más de 12 millones de usuarios, Ubuntu está diseñado principalmente para uso de escritorio, aunque netbook y servidor ediciones existen también. Estadísticas web sugieren que la cuota de Ubuntu de Linux de escritorio de uso es del 50%, e indican una tendencia al alza-como el uso de un servidor web. Ubuntu es patrocinado por el Reino Unido con sede en compañía Canonical Ltd. , propiedad de la sudafricana empresario Mark Shuttleworth . Canónica genera ingresos mediante la venta de soporte técnico y servicios ligados a Ubuntu, mientras que el

propio sistema operativo es totalmente gratuito. Ubuntu es un tenedor de la Debian proyecto de código base . El objetivo original del equipo de Ubuntu fue la de crear un fácil de usar (la libertad para los usuarios en lugar de libertad para los programadores) de escritorio Linux con nuevos lanzamientos programados en un período de seis meses de forma previsible, lo que resulta en un sistema más actualizado con frecuencia. La primera versión de Ubuntu fue el 20 de octubre de 2004. Desde entonces, Canonical ha publicado nuevas versiones de Ubuntu cada seis meses con el compromiso de apoyar a cada versión de dieciocho meses, proporcionando soluciones de seguridad, parches para fallos críticos y actualizaciones de menor importancia a los programas. Se decidió que cada cuarto disco, publicado en un período de dos años, recibiría un apoyo a largo plazo (LTS). versiones LTS son apoyados por tres años en el escritorio y cinco años en el servidor. La última versión LTS de Ubuntu es 10.04 (Lucid Lynx), publicado el 29 de abril de 2010, mientras que la última versión normal es Ubuntu 10.10 (MaverickSuricata), publicado el 10 de octubre de 2010 [Wikipedia, 2011].

En primer lugar, Ubuntu es un Sistema Operativo. Al igual que Microsoft ® Windows ® y Apple MacOS, puede usar Ubuntu para navegar por Internet, consultar el correo electrónico, o cualquier cosa que quiera hacer. He aquí un "Top Ten" lista de cosas que usted debe saber acerca de Ubuntu [Dell, 2011].

3.6.1 Shell Script De Linux

El Shell scripts en Linux conforme más se usa la línea de comandos, más se descubre de la enorme potencia que la correcta combinación, concatenación, secuencia de comandos, etc que es capaz de ofrecer. A través de estos scripts se puede aprender muchos secretos de los comandos de Linux y de las técnicas para escribir adecuadamente shell scripts, que permiten sobre todo la automatización de tareas [Gonzales, 2011].

Una **Shell de Unix** o también **Shell**, es el término usado en informática para referirse a un intérprete de comandos, el cual consiste en la interfaz de usuario tradicional de los sistemas operativos basados en Unix y similares como GNU/Linux. Mediante las instrucciones que aporta el intérprete, el usuario puede comunicarse con el núcleo y por extensión, ejecutar

dichas órdenes, así como herramientas que le permiten controlar el funcionamiento de la computadora. Los comandos que aportan los intérpretes, pueden usarse a modo de guion si se escriben en ficheros ejecutables denominados shell-scripts, de este modo, cuando el usuario necesita hacer uso de varios comandos o combinados de comandos con herramientas, escribe en un fichero de texto marcado como ejecutable, las operaciones que posteriormente, línea por línea, el intérprete traducirá al núcleo para que las realice. Sin ser un shell estrictamente un lenguaje de programación, al proceso de crear scripts de shell se le denomina programación shell o en inglés, shellprogramming o shell scripting [Wikipedia, 2011].

En el sentido más genérico del término, shell significa cualquier intérprete que los usuarios usen para escribir comandos. Su etimología proviene del uso natural de consolas en computadores funcionando bajo Unix(antaño), cuando los usuarios conectaban al computador central, lo hacían mediante consolas, (shells) por las cuales a través de un intérprete, hacían inicio de sesión y manejaban la computadora principal. Posteriormente, con la proliferación de los computadores personales y su filosofía monousuario, un computador por usuario (entiéndase lo contrario de la filosofía inicial de Unix, un computador, muchos usuarios conectados por terminales), se desarrolló un software que emulase las características principales de las consolas físicas, a modo de poder seguir usándolas como clientes en un computador o núcleo que comprendiera la convención estándar usada para configurar y llevar a cabo tareas de administración de emergencia con servidores basados en Unix. Los usuarios de Unix y similares, pueden elegir entre distintos shells (programa que se debería ejecutar cuando inician la sesión, como:bash, ash, csh, Zsh, ksh, tcsh, tal como se muestra en la tabla. 1.1). Las interfaces de usuario gráficas para Unix, como son GNOME, KDE y Xfce pueden ser llamadas shells visuales o shells gráficas. Por sí mismo, el término shell es asociado usualmente con la línea de comandos. En Unix, cualquier programa puede ser un shell de usuario. Los usuarios que desean utilizar una sintaxis diferente para redactar comandos, pueden especificar un intérprete diferente como su shell de usuario.

Archivos de configuración para shells

Un shell lee archivos de configuración en múltiples circunstancias bajo diferentes dependencias de la shell. Esta tabla 3.1 muestra los archivos de configuración de las shells más populares:

Tabla 3.1 Archivos de configuración para shells

	sh	Ksh	csh	tcsh	bash	zsh
/etc/.login	no	No	login	login	no	no
/etc/csh.cshrc	no	No	no	yes	no	no
/etc/csh.login	no	No	no	login	no	no
~/.tcshrc	no	No	no	yes	no	no
~/.cshrc	no	No	yes	yes	no	no
~/.login	no	No	login	login	no	no
~/.logout	no	No	login	login	no	no
/etc/profile	login	login	no	no	i.login	no
~/.profile	login	login	no	no	login	no
~/.bash_profile	no	No	no	no	login	no
~/.bash_login	no	No	no	no	login	no
~/.bashrc	no	No	no	no	n/login	no
/etc/zshenv	no	No	no	no	no	yes
/etc/zprofile	no	No	no	no	no	login
/etc/zshrc	no	No	no	no	no	int.
/etc/zlogin	no	No	no	no	no	login
/etc/zlogout	no	No	no	no	no	login
~/.zshenv	no	No	no	no	no	yes
~/.zprofile	no	No	no	no	no	login
~/.zshrc	no	No	no	no	no	int.
~/.zlogin	no	No	no	no	no	login
~/.zlogout	no	No	no	no	no	login

Fuente: [Wikipedia, 2011] Pag.1

Explicación:

- "no" significa que la shell no leerá el archivo en absoluto.
- "yes" significa que el archivo es siempre leído por el shell.
- "login" significa que el archivo es leído si la shell es una shell de sesión (logingshell).
- "n/login" significa que el archivo is leído si la shell no es una shell de sesión.

- "int." significa que un archivo es leído si es un shell interactivo.
- "i.login" significa que un archivo is leído si la shell es de sesión interactiva.

Una de las mayores utilidades que posee una shell es el permitirnos crear funciones para realizar tareas repetitivas fácilmente. El funcionamiento de estas funciones es parecido al que posee cualquier lenguaje de programación, en el cual se agrupan conjunto de comandos y se los llama por un nombre. El formato de las funciones es el siguiente:

```
nombre_funcion(){
primero_a_realizar
segundo_a_realizar
        }
```

Estas funciones pueden ser definidas en cualquier lugar, incluso en la misma línea de comandos. Lo que habrá que recordar que hechas de esta forma se borraran de la memoria una vez que se a salido del shell. Una forma de hacer que queden disponibles en forma permanente es incorporarla en el archivo de inicio del shell, el .bash_profile, en el cual se pondrá la función. De esta forma se puede seguir utilizándola dado que será cargada en memoria cada vez que ejecute el shell. Veamos un ejemplo de una función simple:

```
[shrek@pantano:~]$ que_tal()
> {
> echo "Hola $1, como estás?"
> }
[shrek@pantano:~]$ que_talshrek
Hola shrek, como estás?
```

CAPITULO IV

MARCO APLICATIVO Y RESULTADOS

4.1 Introducción.

Cuando se hace mención al estudio y análisis de la vulnerabilidad del estándar 802.11, quiere decir que el objetivo de este documento es el estudio de la seguridad actual ofrecida por este estándar y la creación de una red inalámbrica segura. Para el mismo se plantean los Objetivos específicos:

- Llevar a cabo la implementación de métodos de Intrusión para descubrir las vulnerabilidades y falencias de los protocolos de seguridad de las WLAN.
- Diseñar e implementar una aplicación o prototipo para la administración y monitoreo de los usuarios conectados a la WLAN y posibles intromisiones.
- Plantear el diseño de una estructura de WLAN protegida.

Para lograr estos propósitos, el presente capítulo se ha dividido en las siguientes partes:

- Estudio del estándar 802.11 haciendo hincapié en la temática de la seguridad en las redes inalámbricas.

- Análisis y comprobación de la seguridad que implementan los productos que actualmente están en el mercado local.

- Análisis para la implementación de una solución que cumpla con determinados requerimientos de seguridad y de facilidad de uso (definidos una vez realizados los dos estudios previos).

La finalidad de la primera parte del proyecto será la de presentar el estándar 802.11, denotando los puntos que se crean interesantes para el desarrollo de este proyecto. El estudio esta centrado en la seguridad que puede ofrecer el estándar, lo cual proporcionará un

conocimiento crítico sobre las soluciones ofrecidas en el mercado, pudiendo analizar su seguridad e incluso, proponer una solución a los distintos problemas.

En la segunda parte se realizará un estudio y análisis sobre la seguridad de diferentes casos de seguridad en redes actuales. Se describirá más profundamente la seguridad en el estándar, incluyendo sus debilidades, las cuales se mostrarán mediante ejemplos de ataques reales. El conocimiento de las posibilidades del estándar, de sus deficiencias y de las diferentes técnicas de ataque, nos proporcionará la información necesaria para poder definir los requerimientos del modelo a desarrollar en la tercera parte.

La tercera y última parte pretende plantear una solución de seguridad en sistemas inalámbricos, o wireless de Área Local, que intente cubrir las deficiencias descritas anteriormente, especificando requerimientos, modelos de topologías lógicas que limiten al acceso no autorizado a la red,

Parte I

4.2 Estándares 802.11

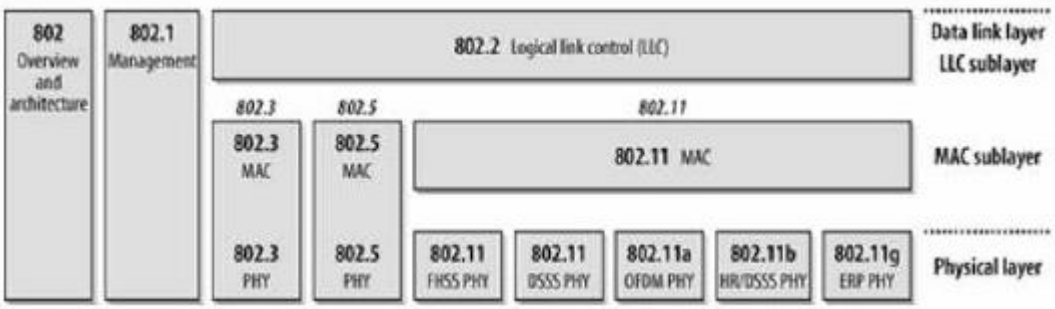
Un estándar es una norma o requerimiento propuesto por una o varias entidades para promover una facilidad de diseño, construcción, homogeneidad y compatibilidad de los dispositivos. Por esto, un estándar ha de ser ampliamente conocido, e incluso público, y estará sometido a un uso continuo y masivo. Debido a ello, es posible que se descubran debilidades de diseño en los estándares, aún disponiendo de sistemas de seguridad. Estas debilidades no suelen ser ni fáciles ni rápidas de solucionar, con lo que los atacantes, poco a poco, perfeccionan sus ataques y los hacen más potentes y certeros.

En el estándar 802.11 existen debilidades introducidas por el diseño del estándar, las cuales ponen en peligro la seguridad de nuestra red como se verá en la PARTE II. Pero antes de exponer estas debilidades, para comprender la problemática de la seguridad en las redes

802.11 y proponer una solución en la PARTE III, primero se expondran los puntos más importantes del estándar 802.11.

En los apartados siguientes serán mostradas varias versiones del estándar 802.11. Todas las versiones activas del 802.11 tienen compatibilidad descendente, pero cada una de ellas añade funcionalidades que versiones anteriores no podrán utilizar. Aún así, las versiones tienen la base común del estándar IEEE 802.11-1997, la mayoría de las cuales afectan a la capa física (Physical Layer).

Fig. 4.1 Estándares 802



Fuente: [CBTIS, 2004] Pag.1

Como se puede ver en la Figura 4.1, el estándar 802.11 es de la familia de estándares 802 del IEEE, que es el que define las especificaciones para las redes LAN. En esta figura también se ven algunas de las versiones del estándar que modifican la capa Física.

Las versiones más relevantes de cara al usuario son las mostradas en la Figura 4.2 siguiente. Las versiones que modifican la capa física suelen estar orientadas a la mejora de la velocidad de transmisión. Las versiones en la capa MAC (Media Access Control o Control de Acceso al Medio) tienen que ver con la seguridad en la transmisión de datos.

Fig. 4.2 Actualizaciones del 802.11

Estado Inicial 802.11 – 1997 Mejoras	
Capa Física 802.11a 802.11b 802.11g 802.11n	**Seguridad** 802.11i

Fuente: Elaboración Propia

En este documento serán citadas las mejoras a nivel de la capa física de manera cualitativa ya que éstas han sido las causantes del uso masivo de esta tecnología.

Además, el conocimiento de algunos aspectos de la capa física ayudara al éxito de los ataques a la seguridad de las redes 802.11.

Por otra parte, la mejora en la seguridad del estándar 802.11i, se tratará posteriormente, dando a conocer la propuesta realizada por el IEEE para evitar el uso de sistemas que proporcionan una seguridad débil, como es el sistema propuesto por el estándar inicial de 1997, WEP (Wired Equivalent Privacy).

Aún así, como ya se ha dicho, el estudio se centra más en el estándar publicado en 1997, ya que la subcapa MAC (parte de la capa Data Link Layer o DLL) que define prevalece intacta en la mayoría de las versiones, y es esta capa MAC la que se encarga de la seguridad en el estándar 802.11.

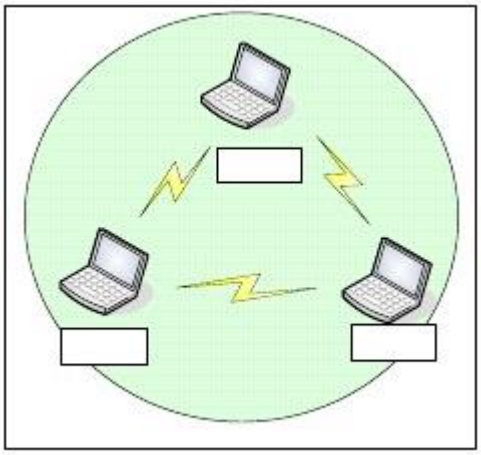
4.2.1 Estándar IEEE 802.11-1997

Arquitectura:

La arquitectura de las redes inalámbricas 802.11 son sistemas divididos en células. Se permiten dos tipos de arquitectura:

Ad-hoc: Los dispositivos se conectan directamente entre ellos, sin necesidad de un punto de acceso o AP (Access Point), como se muestra en la Figura 4.3. Los usuarios han de encontrarse en el mismo rango de direcciones para poder comunicarse. En este proyecto el desarrollo estará basado en redes con infraestructura, con lo que el tipo de red Ad-hoc no serán tratados.

Fig. 4.3 Red Ad-Hoc

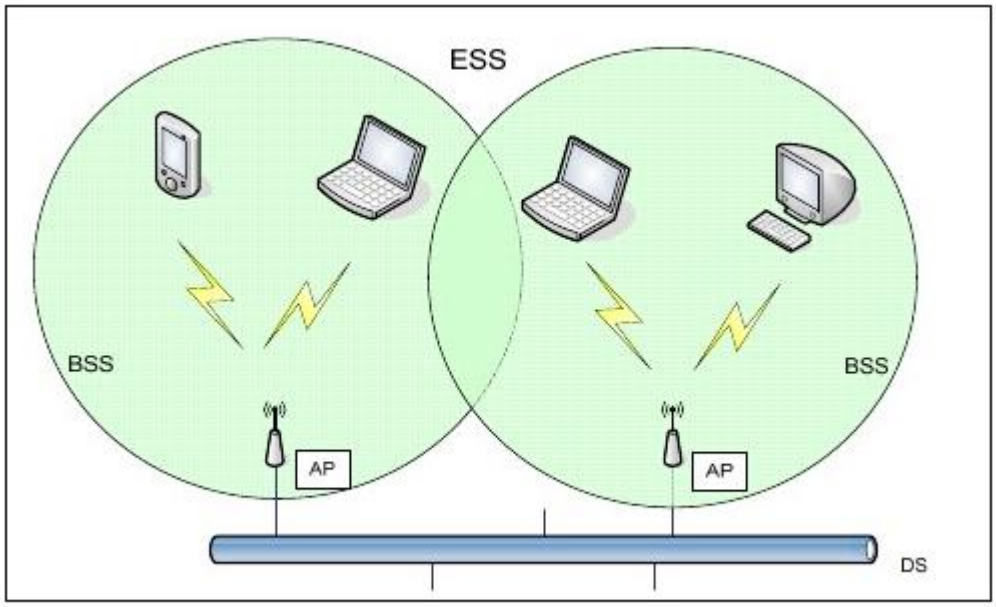


Fuente: [Share, 2011] Pag. 1

Infraestructura: Todos los dispositivos realizan la comunicación inalámbrica a través de un punto de acceso o AP, Figura 4.4. Este punto de acceso recoge todas las comunicaciones y las reparte, ya sea dentro de su área inalámbrica o BBS (Basic Service Set) o a través de la red de distribución o DS (Distribution Service), que suele ser una red Ethernet. El propio AP esta implementado de manera que realiza la función de puente, o bridge, entre la red cableada y la inalámbrica. Cuando agrupamos varias BSS generamos un nuevo conjunto llamado ESS (Extended Service Set). Este último conjunto permite que los clientes puedan pasar de un BSS a otro sin necesidad de perder la conexión (siempre y cuando las áreas de cobertura sean

contiguas).

Fig. 4.4 Red Infraestructura



Fuente: [Share, 2011] Pag. 1

4.2.2 Capas Del Protocolo

El estándar 802.11 sólo cubre las dos primeras capas de la arquitectura OSI. En concreto son la capa física y la subcapa MAC (parte de la capa Data Link Layer o DLL). En el estándar en su edición inicial del 1997, se propone una única capa MAC y tres posibles capas Físicas. Estas posibles capas físicas son:

• IR (Infrarrojos): que nunca ha sido implementado de manera comercial.

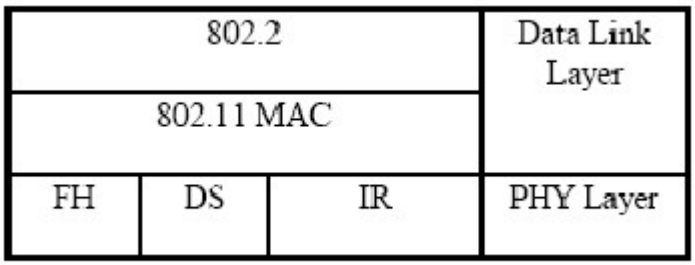
• FHSS (Frequency Hoping Spread Spectrum): Usa la frecuencia de 2,4 GHz.

Esta capa fue en la que se centraron los primeros estudios, ya que la electrónica que usaba era relativamente barata. Además este tipo de modulación permitía la coexistencia de varias redes en un mismo lugar manteniendo niveles relativamente altos de transmisión de datos. Aún así,

en la versión de 1999 se introdujo DSSS, con lo que el desarrollo y producción de dispositivos usando FHSS propuesto en 1997 no fue llevado a término.

• DSSS (Direct Sequence Spread Spectrum): Usa la frecuencia 2,4 GHz. Mediante el uso de DSSS se consiguen velocidades de 1 o 2 Mbps, operando en la misma frecuencia que FHSS. La tecnología basada en DSSS fue mejorando y desplazó definitivamente a la FHSS (como se observa en la mejora 802.11b).

Fig. 4.5 Estructura de las capas MAC y física del estándar de 1997



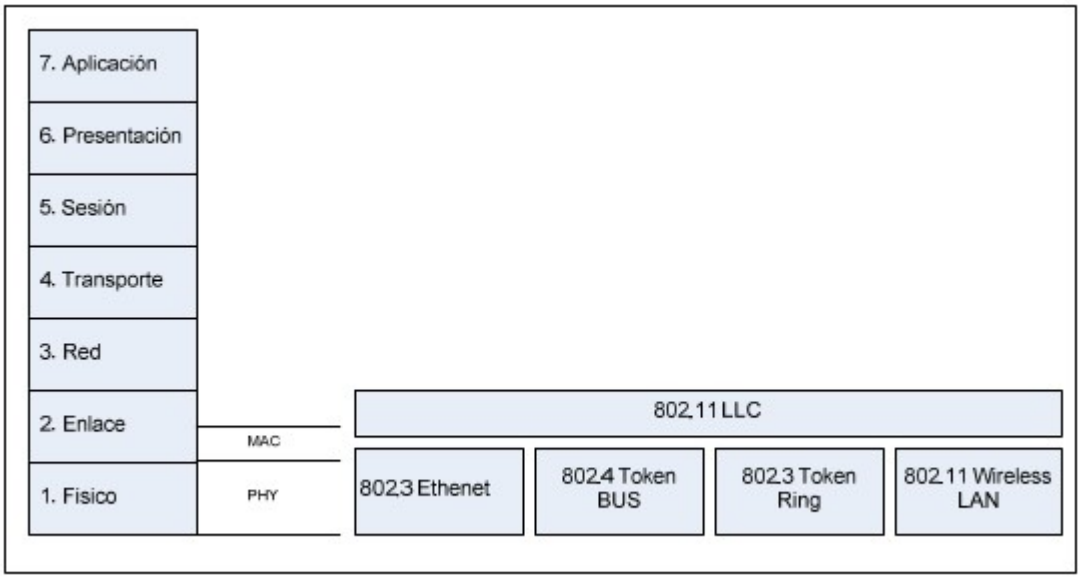
Fuente:

Se puede observar en la Figura 4.5 que por encima del nivel MAC encontramos el LLC (Logical Link Control). A partir del LLC la pila de protocolos utilizada ya no depende del estándar 802.11, sino que depende del estándar 802.2.

La definición de capas MAC y Física específicas por parte del estándar 802.11, no sólo posibilita la implementación de dispositivos sencillos para realizar el encaminamiento o bridging entre redes, sino que también permite a las redes inalámbricas realizar control de errores optimizados para este tipo de comunicación. Se pretende así, que los errores producidos por la transmisión inalámbrica no lleguen a capas superiores del protocolo. De no ser así, deberíamos llegar a niveles superiores del modelo OSI para corregir los errores, con lo que la retransmisión de los paquetes se haría de manera más costosa, tanto en ancho de banda como en tiempo de proceso. Esto podría causar una sobrecarga de retransmisiones influyendo de manera drástica en la eficiencia de estas redes.

Por lo tanto, como se puede ver en la Figura 4.6, el estándar 802.11 y las redes de la familia 802 tienen en común todas las capas del modelo OSI, a excepción de la capa MAC y la capa física, que en el caso de las redes 802.11 están optimizadas para la transmisión inalámbrica.

Fig. 4.6 Diferencias entre protocolos de la familia 802
Según el modelo OSI



Fuente: [Jonathan, 2004] Pag.1

4.2.3 Método de Acceso Al Medio

El método de acceso usado por las redes inalámbricas es conocido como Distributed Coordination Function. Este está basado en el protocolo CSMA/CA (Carrier Sense Multiple Access Collision Avoidance), el cual es similar al CSMA/CD (Carrier Sense Multiple Access Collision Detection) usado por Ethernet.

Con CSMA/CD una estación comprueba el medio antes de transmitir. Si el medio está ocupado la estación no intentará el envío de datos hasta pasado un tiempo definido por el protocolo. Si el medio está libre, la estación podrá transmitir.

El problema en CSMA/CD aparece cuando dos estaciones sondean el medio simultáneamente. Esta casuística es muy común en redes inalámbricas, ya que el medio es compartido por

muchas estaciones. El envío simultáneo provocaría un alto número de retransmisiones haciendo descender la velocidad real de transmisión de datos. Es por ello que no se estima CSMA/CD para el estándar 802.11 y se busca un método de acceso el cual asegura que no se produjeran colisiones por acceso simultáneo al medio.

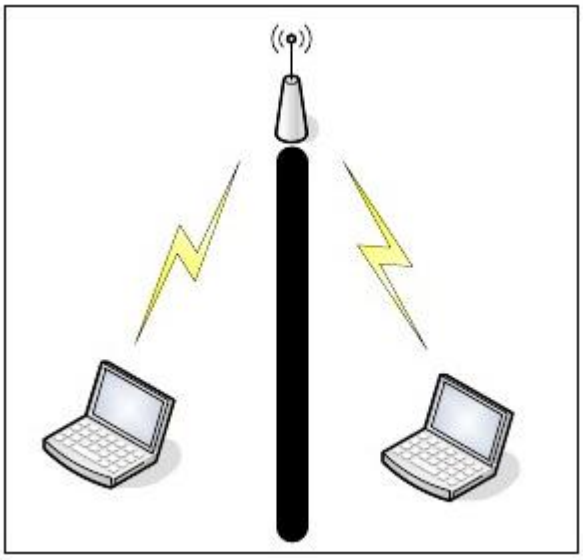
En CSMA/CA una estación que quiere transmitir comprueba si el medio está ocupado. Si está ocupado entonces no transmite. Si el medio está libre la estación esperará un tiempo específico, llamado DIFS (Distributed Inter Frame Space). Si pasado el DIFS sigue libre, entonces la estación podrá transmitir. La estación receptora comprobará el CRC del paquete recibido y enviara un ACK (Acknowledge). Si el emisor del paquete recibe el ACK implicará que no ha habido colisiones durante la petición de acceso y que el medio ha sido reservado para esa estación. Si el emisor no recibe el ACK, el proceso de acceso volverá a empezar hasta que el protocolo anule la petición y descarte el paquete (después de varios intentos).

Además, el protocolo 802.11 en su capa MAC incluye un mecanismo detector de portadora virtual (Virtual Carrier Sense) para evitar colisiones. Este mecanismo trata de evitar colisiones entre estaciones que no se oyen mediante la utilización de paquetes de confirmación de acceso al medio como se muestra en la Fig. 4.7. Para ello la estación que trata de transmitir un paquete primero, transmitirá un RTS (Request to Send). El RTS es un paquete más corto de lo normal (para reducir posibles colisiones con otros paquetes), y sólo indicará información del emisor, del receptor y la duración de la transmisión. Si el medio está libre, la estación receptora contestara enviando un CTS (Clear to Send) que sólo informará de la duración permitida de la comunicación.

Todas las estaciones que reciban tanto el RTS como el CTS pondrán en marcha el contador de tiempo de detección de colisión virtual, NAV (Network Allowance Vector).

El NAV expirará cuando el contador llegue al tiempo marcado en el campo del RTS o del CTS.

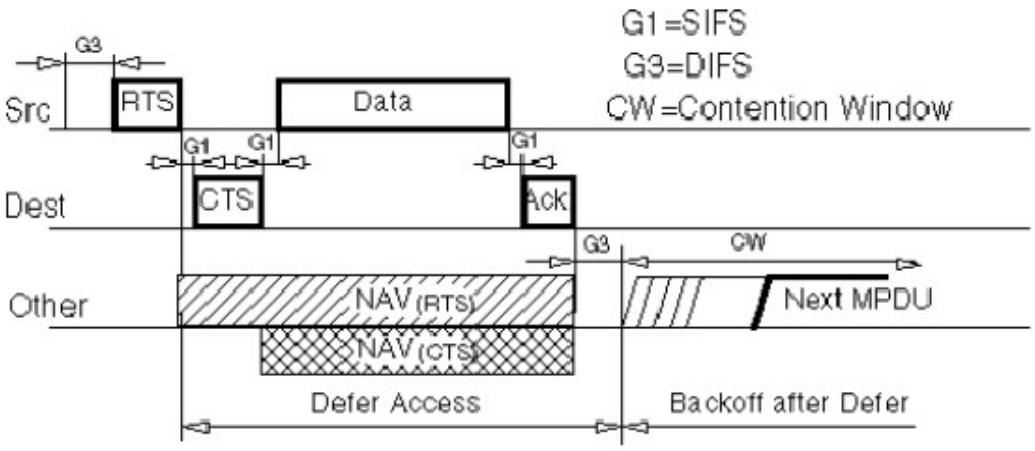
Fig. 4.7 Imagen de dos estaciones ocultas



Fuente: [maestrow, 2004] pag.1

El estándar también permite excepciones. Los paquetes de datos pequeños podrán ser transmitidos sin la necesidad del RTS y CTS, ya que su probabilidad de colisión es baja. Esta excepción provoca una mejora en la eficiencia de la red.

Fig. 2.8 Ejemplo de acceso mediante CSMA/CA



Fuente: [CCNA, 2011], pag. 76

En la Figura 4.8 se puede ver la transacción entre dos estaciones (Src y Dest) y una tercera (Other) que escucha. La estación origen pide el acceso enviando un RTS y la estación destino le confirma que dispone del medio con un CTS . Después de la transmisión de datos el destino confirma la recepción con el ACK. Un tercer dispositivo ha estado escuchando el medio durante toda la transmisión y sabe que no podrá intentar transmitir hasta después de un DIFS.

4.2.4 Prioridad De Tramas

Para establecer la prioridad en las tramas, el estándar definió unos tiempos de espera que han de cumplirse antes de enviar las diferentes tramas. El tiempo de espera cambia dependiendo del tipo de trama que será enviada. Estos tiempos son, de menor a mayor, los siguientes:

SIFS (Short Inter Frame Space): es el tiempo de espera más corto y por lo tanto el más prioritario. Separa dos transmisiones, las cuales pertenezcan al mismo dialogo (por ejemplo antes de enviar un ACK). El valor del SIFS lo determina la capa física, ya que dependerá de la velocidad máxima de transmisión y de cómo se module la señal. El SIFS ha de ser mayor al tiempo que tarda el emisor a poner su tarjeta en modo escucha más decodificar un paquete de entrada. En el caso del primer estándar del 1997, el tiempo es de 28 µs.

PIFS (Point Coordination IFS o Access Point Coordination IFS): es el tiempo que usan los AP's para conseguir el acceso al medio. En el 802.11 de 1997 se definió como un SIFS más un slot de transmisión. Esto equivale a 78 microsegundos.

DIFS (Distributed IFS): es el tiempo que han de esperar las estaciones para conseguir el acceso al medio. Este tiempo es el PIFS más un slot de tiempo que corresponden a 128 microsegundos.

EIFS (Extended IFS): será el tiempo de espera utilizado por una estación cuando esta recibe un paquete que no ha podido entender. Esto evita que se produzcan colisiones entre posibles paquetes que pueden pertenecer al mismo diálogo entre las dos estaciones (ya que al no entender el paquete, tampoco se podrá conocer la duración del NAV).

También existe otro tiempo llamado de Backoff. Este tiempo no tiene un valor determinado ya que está pensado para que sea aleatorio en cada estación. La estación que quiera transmitir esperará un número de slots aleatorios antes de pedir el acceso al medio. Una vez pasado este tiempo de Backoff se comprobará que el medio sigue libre y si es así, definitivamente se realizará la comunicación. Con esta aleatoriedad se consigue que la colisión por acceso simultáneo al medio sea bastante más baja que si el acceso se realizara inmediatamente después del tiempo DIFS.

4.2.5 Fragmentación De Paquetes

En las redes inalámbricas es preferible usar paquetes pequeños dado que la tasa de error del canal es más alta. Dicha tasa de error aumenta la probabilidad de que un paquete esté corrupto cuanto más largo sea. Además, las retransmisiones de paquetes largos provocarían una sobrecarga excesiva en la red.
Para las redes Ethernet, el tamaño de los paquetes es de 1518 bytes, con lo que para poder hacer compatible las redes inalámbricas con las cableadas, y evitar así tener que definir una capa específica para las redes inalámbricas, se decidió añadir a la capa MAC del estándar 802.11, un mecanismo de fragmentación de paquetes. Con este mecanismo se fragmentan los

paquetes Ethernet para que puedan ser enviados mediante los paquetes más pequeños del estándar 802.11.

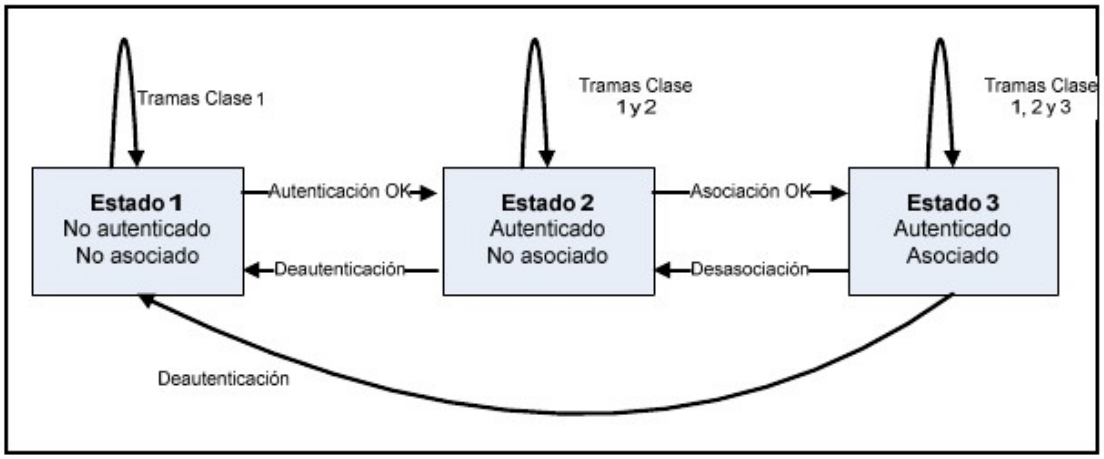
El mecanismo que se implementa para la fragmentación de paquetes es el Send-and-Wait Éste, además de permitirnos trocear una trama Ethernet en fragmentos más pequeños, no permite al emisor enviar otra trama a no ser que reciba el ACK correspondiente, como pudo verse en la Figura 2.8. Para mejorar la fluidez de la comunicación, el estándar permite que aunque para un destinatario que esté esperando el ACK, se pueda transmitir un paquete destinado a otra dirección distinta. Esta excepción es básica para evitar el bloqueo momentáneo de tráfico en los AP.

4.2.6 Proceso de Conexión a la Red Inalámbrica

Para que una estación se asocie a otra (o a un AP) es necesario que se sincronicen. En la sincronización ambas estaciones darán a conocer la configuración que van a usar para la transmisión de datos. Los pasos siguientes a la sincronización serán la autenticación y la asociación.

En la Figura 4.9 se puede ver el proceso de autenticación y asociación. Se incluyen en esta figura la clase de mensajes o Frame, de control del estándar que están permitidos en cada estado. Con detalle.

Fig. 4.9 Diagrama de estado de una conexión 802.11



Fuente: [CCNA, 2011], pag,35

Sincronización:

En el caso de las redes con infraestructura, las estaciones pueden sincronizarse escaneando el medio de dos maneras diferentes:
Escaneo pasivo del medio: la estación escucha el medio y recibe unas tramas llamadas balizas o Beacon desde el AP. Los Beacon se envían periódicamente e incorporan: una marca de tiempo (para la sincronización), el nombre de la red (SSID), si se usa cifrado, las velocidades soportadas, etc.
Escaneo activo del medio: la estación conoce el nombre de la red y es la propia estación la que busca la red determinada transmitiendo una trama llamada Probe Request. El AP contestará con el Probe Response dándole la misma información que da el Beacon. Este sistema se utiliza para evitar que el AP tenga que transmitir continuamente el Beacon y pueda ser ocultado.

La marca de tiempo de los Beacon es básica ya que será la que usarán todas las estaciones cliente de ese AP para sincronizarse.

Autenticación:

El siguiente paso, una vez sincronizadas ambas estaciones, es el de la autenticación. La autenticación 802.11, no tiene nada que ver con la autenticación de usuario que propone el estándar 802.1x en redes inalámbricas. La autenticación 802.11 aplica a la capa MAC del estándar. En el caso de la autenticación mediante 802.1x, los mensajes necesarios para realizarla sólo son posibles una vez la estación ha completado la autenticación 802.11.

El proceso de autenticación se realiza en una sola dirección (sólo el cliente debe autenticarse). El cliente debe demostrar que conoce la contraseña de autenticación, como puede ser mediante el cifrado con esa contraseña de una serie de bits conocidos por ambos extremos de la comunicación.

Asociación:

Finalmente, una vez autenticada la estación cliente, se realiza el proceso de Asociación. Este proceso sirve al AP para tener un registro de clientes que tiene conectados, así, una vez autenticados, el sistema de distribución (DS), sabrá dónde encontrar un cliente que esté conectado a la red inalámbrica. En este proceso se intercambia la IP actualizando la tabla ARP del AP y del cliente.

4.2.7 Seguridad

El estándar incluyó un método de seguridad con el que pretendía obtener el mismo nivel de privacidad que aporta una red cableada. Este método de seguridad tiene como fin:
Permitir sólo el acceso de usuarios legítimos a la red (control de acceso). Evitar que los usuarios ilegítimos sean capaces de leer los datos transmitidos por la red inalámbrica (cifrado de comunicaciones).

El método utilizado es el llamado WEP (Wireless Equivalent Privacy). Este método cifra las transmisiones mediante una clave compartida (que los usuarios y el punto de acceso han de conocer) usando el algoritmo RC4. Además, el uso de estas claves compartidas también puede servir para realizar la autenticación de usuario (método Shared-Key Authentication).

El sistema propuesto por el estándar inicial quedo totalmente obsoleto y desfasado a causa de la aparición de métodos de rotura del algoritmo RC4 y del incremento de la potencia de los procesadores. El IEEE propuso una revisión de seguridad y, en 2004, publicó el 802.11i. Hay que destacar que algunas de las mejoras propuestas por el 802.11i son incompatibles con el hardware anterior, como puede ser, cifrado mediante AES (Advanced Encryption Standard) que necesita de tarjetas inalámbricas con hardware especializado. Esto propicia que aún se use el sistema WEP por motivos de compatibilidad.

4.2.8 Tramas

Los equipos diseñados para las comunicaciones 802.11 deben gestionar y entender tramas de 3 tipos diferentes:

• Data Frames

• Control Frame

• Management Frames

Fig. 4.10 Trama 802.11 a nivel física



Fuente: [CCNA, 2011], pag. 38

En la Figura 4.10 se puede ver una trama a nivel físico. Seguidamente describimos los distintos campos:

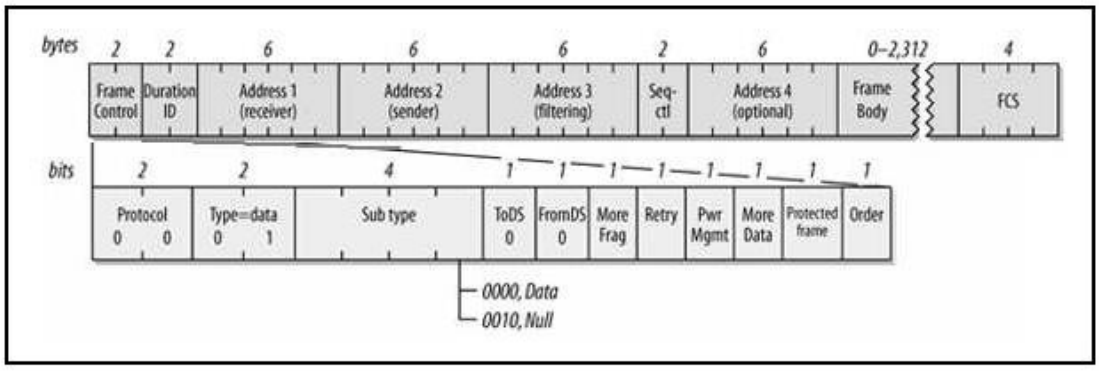
- Preámbulo: esta parte de la trama viene definida por el estándar en su capa física, por lo tanto su contenido variará según sea 802.11a, b, g. El preámbulo incluye:
  - Synch: una secuencia de 80 bits de 1's y 0's para sincronizar los equipos y realizar comprobaciones de canal, de antena (si hay diversidad), etc.
  - SFD (Start Frame Delimiter): es el bit de start que indica a partir de donde empieza la información útil de la trama.

- Cabecera PLCP (Physical Layer Convergence Protocol): se transmite siempre a 1 Mbit/s (proporciona compatibilidad entre estándares y dispositivos diferentes). Contiene información lógica que le servirá a la capa física para comprender la trama.
- Datos MAC: son los datos de la capa MAC los cuales están definidos en la Figura 2.11.
- CRC (Cyclic Redundancy Check): bits de comprobación de la trama.

Para el desarrollo de este documento, las cabeceras introducidas por la capa Física pueden ser obviadas, ya que sólo dan información sobre la transmisión física de la comunicación. Por el contrario, las cabeceras que incluye el nivel MAC serán las que aportaran más información relevante para nuestro interés. El formato básico de las tramas a nivel de la capa MAC es el mostrado en la Figura 4.11.

Como se puede observar, estas tramas incluyen en el Frame Body toda la información recogida por los protocolos superiores al MAC.

Fig. 4.11 Trama 802.11 a nivel MAC



Fuente: [CCNA , 2011], pag.40

A Continuación se describen los campos más relevantes de estas tramas:

Frame Control: los dos bytes del Frame Control están compuesto por otros
campos que dan la siguiente información.
Protocol: versión del 802.11. Tipo y subtipo: indican si la trama es de datos, control o gestión.

ToDS y FromDS: indican si viene del DS (Distribuition System) o si va hacia el DS.
More Frag: indica si hay más fragmentos de esta misma trama.
Retry: indican si el fragmento es una retransmisión.
Power Management: indican si el gestor de energía está establecido
WEP: indica si los datos del campo Frame Body están cifrados mediante el mecanismo WEP.
Order: indica si se puede cambiar el orden de las tramas unicast y multicast.
Duration: se utiliza para el cálculo del tiempo NAV (excepto en los mensajes de Power-Save Poll que no serán aquí tratados).
Campo de direcciones: indica las direcciones del receptor final, emisor final, receptor del siguiente salto y emisor del anterior salto. Pueden variar dependiendo si vienen del AP o si se dirigen a él.
Sequence Control: representa el orden de las tramas que han sido troceadas en diferentes fragmentos.
FCS (Frame Check Sequence): bits extras añadidos para el control de errores de la trama.

4.3 Mejoras En Capa Física: 802.11 a/b/g/n

Dado a las necesidades del mercado y a la evolución constante producida en la técnica para transmitir señales a través del aire, han ido apareciendo mejoras sobre el estándar inicial. Estas mejoras aplican sobre la capa física y son compatibles hacia atrás, esto es que los dispositivos que implementen las mejoras más recientes deben ser compatibles con los anteriores.

En la Tabla 4.1 se puede ver una lista comparativa entre las diferentes mejoras, o subestándares, relacionadas con la capa física que utilizan:

Tabla 4.1 Cuadro comparativo entre las versiones del 802.11

Estándar	Año	Velocidad Max	Frecuencia	Modulación
802.11	1997	1-2 Mbps	2.4 GHz	FH / DS / IR
802.11 b	1999	11 Mbps	2.4 GHz	DSSS
802.11 a	1999	54 Mbps	5 GHz	OFDM
802.11 g	2003	54 Mbps	2.4 GHz	OFDM
802.11 n	Enero - 2010	600 Mbps	2.4 / 5 GHz	OFDM

Fuente: Elaboración Propia

Actualmente el estándar más usado en Europa es el 802.11g, aunque aún se puede encontrar muchos dispositivos antiguos que sólo disponen de 802.11b.

El estándar 802.11a no está muy extendido en Europa ya que la banda ISM (Industrial Scientific Medical) sólo contempla las frecuencias 2,4 GHz ya que la banda de 5 GHz ya está ocupada.

El estándar 802.11n aún no es oficial, aunque ya hay diversos borradores o drafts publicados e incluso fabricantes que han puesto a la venta productos basados en el draft "pre-n". El objetivo de este nuevo estándar es superar la barrera de los 100 Mbps y esto se pretende conseguir incrementando los picos de velocidad y mejorando la capa MAC (mejorando el rendimiento de esta capa eliminando determinados tiempos de espera, bits que de control en las tramas, Acknowledges, etc.). De todas maneras este estándar puede saturar el rango frecuencial, ya que usa toda la banda disponible en 2,4 GHz y su funcionamiento puede ser poco óptimo en zonas donde colisionan varias redes.

4.3.1 Mejoras En Seguridad: 802.11i

Como se ha comentado, el mecanismo WEP, propuesto en el estándar inicial para dar seguridad a las redes inalámbricas, no proporciona la seguridad suficiente (véase la PARTE II). Debido a esto, el IEEE formó el grupo de trabajo I, dentro del grupo de redes inalámbricas 802.11, para desarrollar una mejora de la seguridad de estas redes. De aquí apareció el estándar 802.11i.

Esta nueva mejora del estándar inicial propone una modificación a nivel de capa LLC (Link Layer Control). Concretamente modifica la capa MAC, ya que los datos a cifrar (igual que hace WEP) son los que encontramos a partir de esta capa y hacia niveles superiores de la pila OSI. Al modificar e incluir nuevos apartados en el estándar, corría el peligro de provocar la incompatibilidad con los dispositivos anteriores a esta mejora los cuales sólo "conocían" WEP. Así que el grupo I propuso la mejora incluyendo dos tipos distintos de cifrado:

TKIP (Temporal Key Integrity Protocol): basada en RC4, compatible con los anteriores dispositivos y sólo implica actualización del firmware4 en los dispositivos antiguos.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol): basada en AES, un nuevo algoritmo de cifrado mucho más robusto pero que implica un hardware distinto que el usado para realizar el cifrado RC4. Este sistema es incompatible con los anteriores dispositivos.

Además, el estándar 802.11i incluye la posibilidad de usar un sistema de distribución de claves robusto (WEP no proponía ningún método de distribución). Este método se basa en una autenticación mutua mediante clave compartida (Pre-Shared Key) o mediante algún método EAP (Extensible Authentication Protocol). A partir de esta clave se compone la PMK (Pairwise Master Key) y se derivan diversas claves, las cuales serán claves de cifrado temporales. Sólo estas claves serán las que realicen el cifrado y estén expuestas. Esto separa la autenticación de la encriptación evitando que la PMK se deba transmitir directamente por la red.

En el punto 2 se expondrá con más detalle el proceso de desarrollo de esta mejora incluyendo una descripción del 802.1x, propuesto para la autenticación de usuarios.

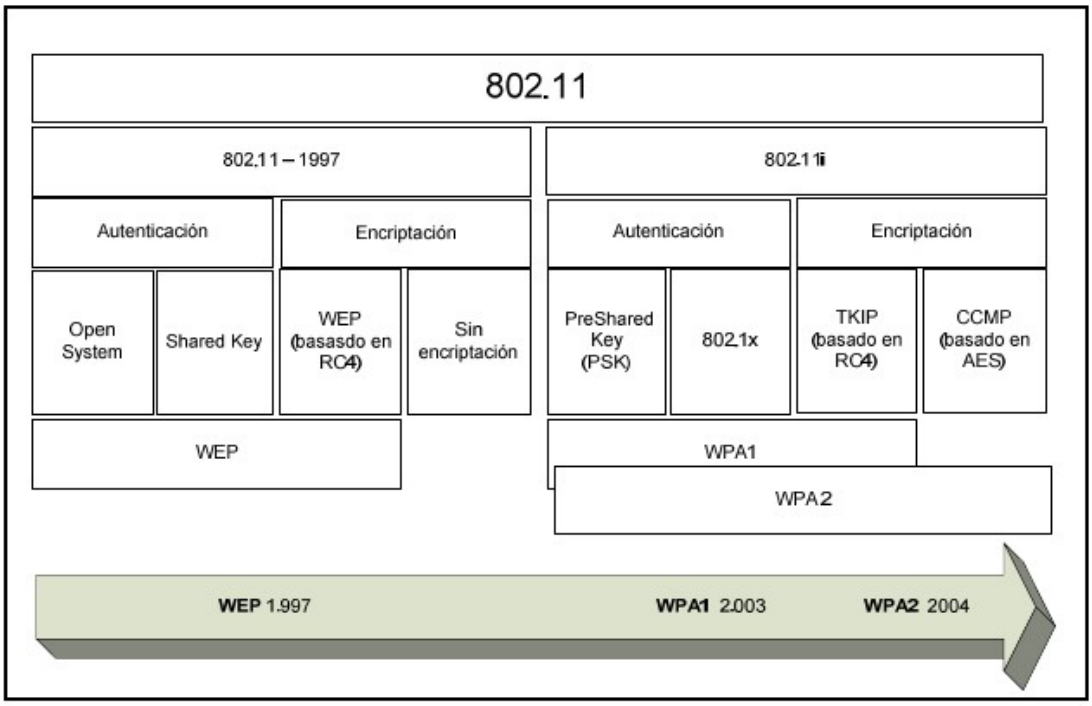
4.3.2 Seguridad en ll Estándar 802.11

Como se ha podido ver al describir el estándar, las mejoras más necesarias y que más han repercutido en el éxito de esta tecnología son las mejoras en la capa física. Éstas garantizan y aumentan la velocidad de las transmisiones haciendo más atractiva esta tecnología.

La importancia de la seguridad ha ido creciendo a medida que estas redes se han ido popularizando. La preocupación por la seguridad en las comunicaciones inalámbricas se puede apreciar especialmente en las redes propiedades de empresas. Para una empresa, tener un punto de acceso con seguridad débil es lo mismo que tener un punto de red Ethernet fuera de los límites de su edificio.

El estándar 802.11 se diseñó con el sistema de seguridad WEP, donde los datos se cifran mediante el algoritmo RC4. Al observar diversas debilidades en dicho algoritmo se propuso la mejora 802.11i. En la Figura 2.12 se puede ver la organización definitiva de los mecanismos de seguridad utilizados por el estándar en la actualidad.

Fig. 4.12 Mecanismos de seguridad de 802.11



Fuente: [CCNA, 2011]

Los mecanismos mostrados en la Figura 4.12 son los aceptados por el estándar, aunque hay soluciones propietarias ampliamente aceptadas. Por ejemplo, al reconocerse la debilidad en WEP por el rehúso masivo de la clave de cifrado, se desarrolló WEP dinámico, el cual cambia la clave WEP periódicamente. Además, WEP dinámico posibilitaba la autenticación mediante 802.1x con lo que permitía separar la parte de la autenticación y la parte del cifrado. Aún así WEP dinámico mantenía el RC4 para el cifrado de los datos.

Como se vio en el apartado 1.3 de la PARTE I, para resolver estos problemas, el IEEE propuso el 802.11i. Pero la aparición de esta mejora se fue aplazando ya que se quería usar el algoritmo de cifrado AES, el cual en ese momento no estaba completamente desarrollado. Por este motivo la organización y por querer que los dispositivos anteriores fueran compatibles, Wi-Fi Alliance decidió la certificación del mecanismo de seguridad llamado WPA (Wi-Fi Protected Access) basado en el tercer draft del 802.11i. WPA proporciona varios métodos de autenticación y mejora el cifrado usando claves temporales o TKIP. Como TKIP utiliza el algoritmo RC4, le permite a WPA ser compatible con la mayoría de dispositivos anteriores simplemente con una actualización del firmware.

Finalmente, en 2004, una vez implementado el nuevo mecanismo llamado CCMP basado en el cifrado AES, apareció el estándar 802.11i. En este estándar se confirmo WPA (que usa el cifrado TKIP basado en RC4) y se incorporó WPA2 (que CCMP basado en AES). Con la inclusión de estos dos mecanismos de cifrado en el estándar final se promueve la compatibilidad (en el caso de CCMP es necesario que todos los dispositivos lo soporten, de no ser así, deberá ser usado TKIP).
En este capítulo se presentan los métodos WEP, el WPA y se introduce el estándar de autenticación 802.1x.

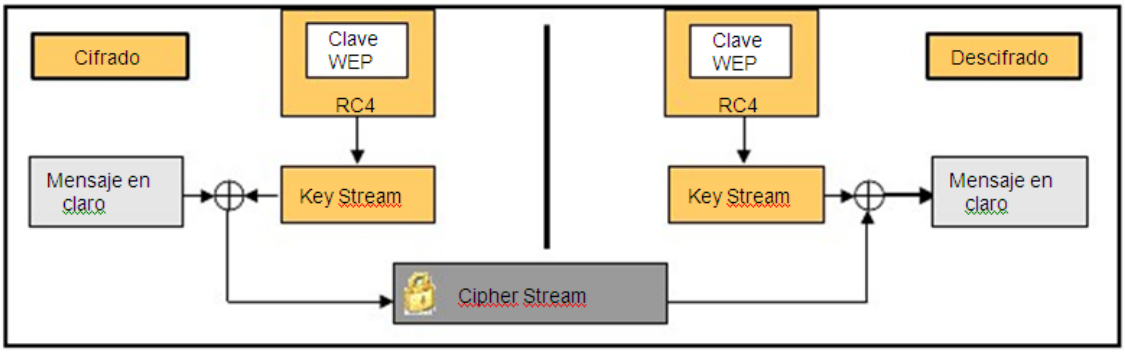
4.4 Seguridad Wep

WEP (Wireless Equivalent Privacy) se diseñó para intentar ofrecer al usuario los servicios de autenticación, integridad y confidencialidad. Pero estos objetivos no se vieron cumplidos debido a fallos tanto en el concepto, como en el mecanismo usado para el cifrado. Aún así, como se verá en el punto 5 de la PARTE II, WEP es actualmente el método de seguridad más extendido, sobre todo debido a que los proveedores de Internet ofrecen routers inalámbricos configurados con este sistema.

4.4.1 Bases del Sistema Wep

Como se comentó en la definición del estándar, WEP usa el algoritmo de clave simétrica RC4. Mediante el algoritmo RC4 se expande la clave compartida (que han de conocer los dos extremos de la comunicación) y se genera un flujo de bits pseudoaleatorios llamados Key Stream. Para cifrar el mensaje se realiza la operación XOR (O-exclusiva) entre el Key Stream y el mensaje a enviar, generándose un flujo de datos cifrados llamado Cipher Stream. Para recuperar el mensaje se vuelve a realizar la operación XOR entre el Cipher Stream recibido y el Key Stream (que ha generado el otro extremo con el RC4 y con la misma clave compartida). Este proceso se puede apreciar en la Figura 4.13.

Fig. 4.13 Proceso de cifrado y descifrado del mecanismo WEP



Fuente: [CCNA, 2011]

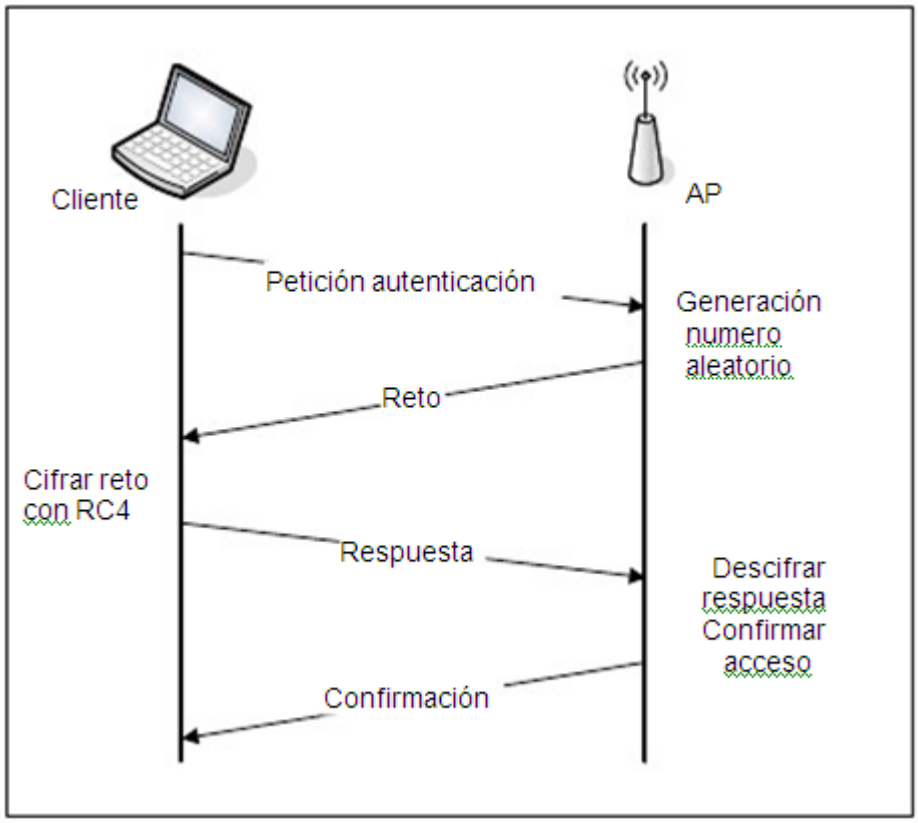
Por lo tanto se puede evidenciar que la seguridad de este Cipher Stream recae en la clave compartida y en el algoritmo RC4.

Gestión de la autenticación:

Para WEP, el estándar 802.11 proporciona dos maneras distintas de autenticar a los usuarios:
Open Authentication: en este sistema no se usa ninguna clave, sino que todo dispositivo se autenticará enviando una trama de autenticación indicando su dirección física MAC.

Shared Key Autentication (Figura 4.14): en este caso se usa la clave WEP para realizar la autenticación. Después de que el usuario indique la intención de conectarse a la red, el AP's envía un texto plano, o reto, para que el cliente lo cifre mediante WEP. El resultado será enviado al AP, el cual comprobará si el mensaje cifrado es correcto. Si es así se enviará una trama de autenticación.
Como se puede apreciar se trata de un mecanismo de "desafío" usando un mensaje aleatorio generado por el AP. Se ha de destacar que este método es vulnerable a ataques man-in-the-middle.

Fig. 4.14 Flujo de la autenticación Shared Key



Fuente: [Lectores, 2011] pag.27

Se puede incluir un tercer tipo de autenticación el cual, aunque sin estar reflejado en el estándar, implementan la mayoría de puntos de acceso:

MAC authentication: en este caso, una vez el cliente envía su dirección MAC, el AP la compara con una lista de MAC's a las cuales les está permitida la autenticación.

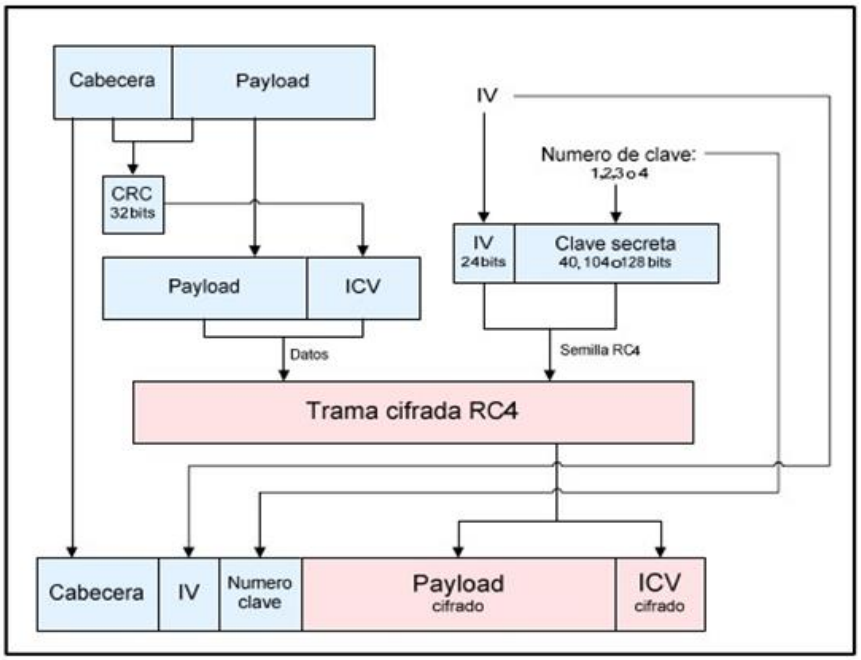
Proceso de cifrado:

En el proceso de cifrado se proporcionan los servicios de confidencialidad (cifrado de datos transmitidos) y los de integridad (mediante ICV o Integrity Check Value). En la Figura 4.15 se puede ver el diagrama de bloques que representa el proceso de cifrado. El mecanismo WEP tiene 3 entadas de datos distintas:

- Trama de entrada: está compuesta por la cabecera del nivel MAC más los datos proporcionados por los protocolos de las capas superiores (MAC payload).

- Clave WEP: es la clave compartida por todos los usuarios de la misma red, la cual se usará, junto a un IV (Initialization Vector), como semilla para generar el Key Stream RC4. Según el estándar, la clave WEP puede tener un tamaño de 40 de 104 bits, aunque hay fabricantes que ofrecen la posibilidad de usar 256 y hasta 512 bits.
- IV: es el vector de inicialización. Es un vector de 24 bits que se añadirán a la clave WEP. El IV será diferente para cada trama que se cifre (representa la parte variable de la clave de cifrado). Sumando estos 24 bits a los proporcionados por la clave WEP se tiene para generar el Key Stream RC4 se usan 64 (40 fijos más 24 variables) o 128 bits (104 fijos más 24 variables).

Fig. 4.15 Diagrama de bloques de la generación de tramas según WEP



Fuente: [Wikipedia, 2010].

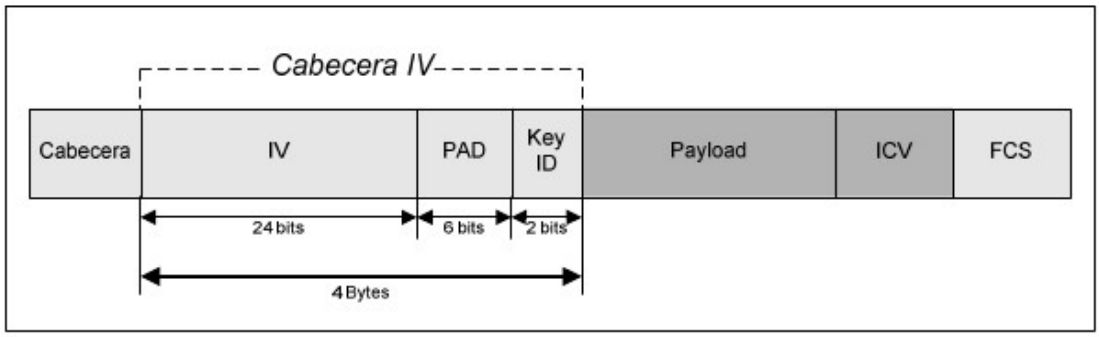
El proceso de cifrado empieza con la trama de entrada de la cual se calcula su CRC tomando la cabecera MAC y el payload de la misma. A este CRC se le llama ICV (Integrity Check Value). El ICV será cifrado junto al payload y permitirá al receptor comprobar la integridad del payload más la cabecera MAC.

El algoritmo RC4 tiene dos entradas: la entrada del payload más el ICV y la entrada de la WEP seed. La entrada WEP seed es la combinación de la clave compartida por los usuarios y un IV único que se genera para cada trama. Como ya se ha dicho, la longitud de esta combinación suele ser de 64 bits (40 clave compartida + 24 IV) o de 128 (104 clave compartida + 24 IV). La introducción del IV tiene la finalidad de conseguir que cada trama tenga un WEP seed diferente y no se cifre siempre con el mismo Key Stream. No obstante, el IV debe ser transmitido al receptor y esta transmisión se hará en claro. Esto implica que un posible atacante también puede ver el IV y, por consiguiente, parte de la clave usada para generar el cifrado de esa trama en concreto.

El proceso de cifrado suele realizarse mediante un módulo hardware (circuito que integra el algoritmo RC4). El módulo dará como resultado a la salida el payload y el ICV cifrados. A esto se le añadirá la cabecera, el IV y el índice de clave compartida usado (puede haber hasta 4 claves WEP distintas definidas con el mismo índice en cada extremo de la comunicación).

En lo que a eficiencia se refiere, en la Figura 2.16, se puede ver que una vez cifrada, la trama enviada crece en 4 bytes (los 4 bytes de la cabecera IV). Esto implica que la velocidad de transmisión de datos útiles para el usuario final sea relativamente más baja en redes con cifrado que sin él.

Fig. 4.16 Trama enviada al receptor codificada con WEP a nivel MAC



Fuente: [CCNA, 2011]

4.4.2 Wep Estático

Como se ha dicho, WEP es el mecanismo original que plantea el estándar 802.11. Pero el estándar no indica ningún método de distribución de claves, por lo tanto el método seguido es el método manual o estático.

En cuanto a la administración de la red, la falta de una distribución de claves plantea las siguientes problemáticas:

- La introducción de la clave se debe realizar manualmente por el administrador o el propio usuario.
- La actualización de la clave ha de realizarse de manera manual en cada dispositivo. Si se usa sólo un índice de clave, este cambio debe ser simultáneo en todas las máquinas y en el AP. Los dispositivos con la clave antigua se quedarán sin conexión.

En cuanto a la seguridad, la falta de un sistema robusto de distribución de claves, también plantea serios problemas:

- Todos los usuarios tienen la misma clave.
- La misma clave es usada para cifrar por todos los usuarios, con lo que se expone constantemente. Puede ser fácil obtener grandes cantidades de datos cifrados con la misma clave.

Puede ponerse en compromiso la clave dado a que esta en todos los dispositivos inalámbricos. Se deja el secreto de la clave en manos de cada fabricante y de cómo implementa la seguridad para almacenar contraseñas, en vez de hacer recaer la seguridad en el estándar.

El cambio de claves no es dinámico, con lo que un cambio de clave tiene un alto coste en trabajo de administración. Esto implica que el cambio de clave se realice con poca frecuencia, posibilitando los ataques por acumulación de datos cifrados, (aunque el tráfico diario en la red sea bajo).
WEP implementa un sistema de almacenamiento de claves e indexado que permite usar 4 claves distintas. Como puede observarse en la Figura 2.16, las tramas incluyen un campo llamado índice de clave (Key_ID) que determina que número de clave se está utilizando.

El almacenamiento de distintas claves se ideó pensando en dar la posibilidad al administrador de la red de realizar un cambio de clave progresivo. Así, durante un tiempo determinado, la red inalámbrica puede usar dos claves de manera simultánea, dejando el tiempo suficiente para cambiar las claves de todos los dispositivos sin necesidad de dejarlos sin acceso a la red.

4.4.3 Wep Dinámico

Dado que muchos fabricantes se dieron cuenta de las debilidades del mecanismo WEP, decidieron lanzar un nuevo mecanismo propietario que fuera más robusto. Este mecanismo no modifica nada del estándar, sino que aprovecha la capacidad de poder definir distintos índices de clave.

Este mecanismo propone tener una clave compartida para todos los usuarios, que se utilizará para cifrar el tráfico común a todas las estaciones, o broadcast, y otra clave particular para cada usuario para cifrar el tráfico unicast. La clave compartida es conocida por todos los usuarios de la red y la clave particular es única para cada usuario y generada en cada conexión (distribuida mediante la clave broadcast). De esta manera se diferencia lo que es la autenticación de cliente y el cifrado (ya no se usa la misma clave). Al usar claves dinámicas

para las transmisiones unicast (las que generan más trafico), reducimos el tiempo de vida de estas claves evitando exponer la misma clave durante un largo periodo de tiempo.

WEP dinámico lo implementan la mayoría de dispositivos inalámbricos, aunque, al no ser estándar no puede ser considerado como una forma de seguridad de una red. Además, el sistema sigue utilizando el algoritmo RC4 con lo que tarde o temprano se darán los mismos problemas que con el mecanismo WEP.

4.5 Seguridad Wpa

Como se expone en la PARTE II, el mecanismo propuesto por el estándar, WEP, tiene debilidades muy importantes en el mecanismo de autenticación y de cifrado. La autenticación puede mejorarse ya que el estándar permite usar métodos robustos de autenticación como EAP. En el caso del cifrado, para mejorarlo sería necesario el rediseño de la capa de enlace (LLC) del estándar.

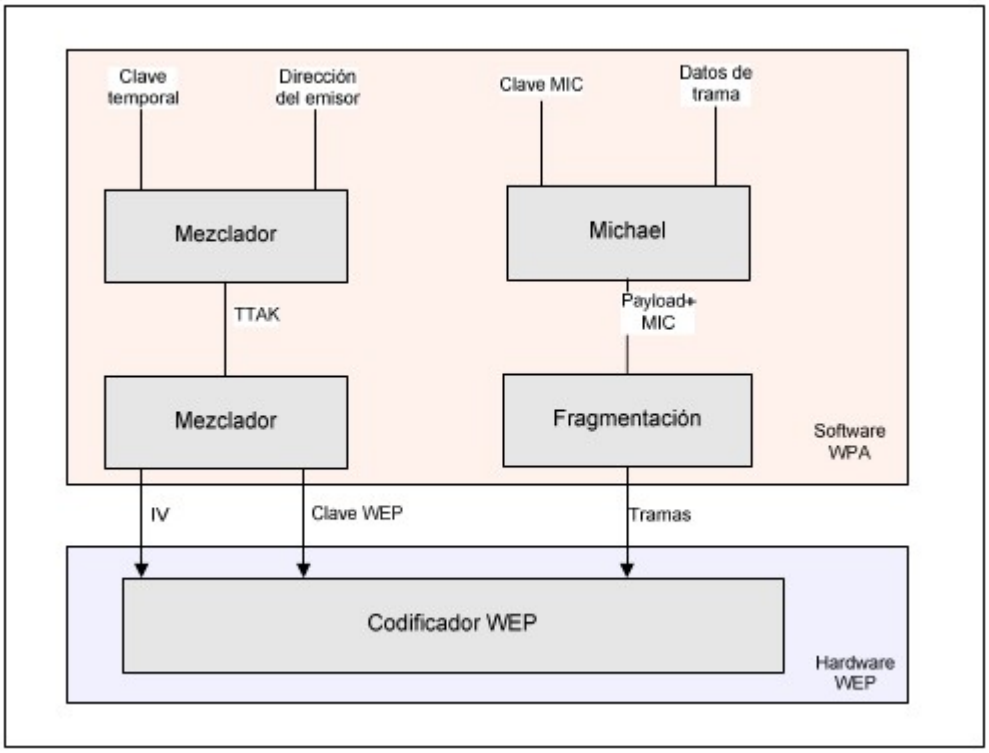
Dado las necesidades del mercado, Wi-Fi Alliance propuso dos nuevas versiones que mejoran la seguridad del estándar basadas en 802.11i: WPA y el WPA2 respectivamente. Recordamos que la diferencia entre estos dos protocolos está en el cifrado que usan:
WPA usa TKIP basado en RC4 (compatible con WEP) y WPA2 utiliza CCMP basado en AES. Como curiosidad y para evitar confusiones, WPA no es el nombre de un estándar oficial, sino que se estableció así para identificar y popularizar las mejoras en la seguridad que basadas en 802.11i. Aún así esta división en pseudo-estándares nos es útil para comprender el funcionamiento y la seguridad ofrecida por cada uno de ellos. En la Figura 4.12 que anteriormente se ha mostrado, podíamos ver la división de estos nuevos mecanismos.

Seguidamente se hará mención los nuevos métodos de cifrado que WPA propone estableciendo las diferencias entre ellos y mostrando cómo mejoran al protocolo WEP. También se introducirá la manera de funcionar de estos métodos y diferentes configuraciones de seguridad posibles usando WPA.

4.5.1 Protocolo Tkip

El protocolo TKIP (Temporal Key Integrity Protocol) fue la primera mejora a nivel de enlace. TKIP mejora la seguridad que ofrece WEP, pero sin necesidad de tener que cambiar el hardware (sólo es necesaria una actualización a nivel de firmware). La compatibilidad es posible ya que el protocolo TKIP utiliza del algoritmo de cifrado usado por WEP, el RC4.

Fig. 4.17 Mecanismo de encriptación TKIP



Fuente: [Wikipedia, 2010].

Manejo y generación de claves

Como ya se comentó, el problema principal del RC4 en WEP es el uso de IV, los cuales se transmiten en claro. Esto posibilita que el atacante pueda conocer parte de la clave que se usa para generar la semilla RC4 para cifrar el mensaje.

Para evitar esto, TKIP usa una clave compartida entre los usuarios (passphrase). De ésta se deriva unas claves principales (Master Keys). A partir de estas Master Keys serán derivadas las claves temporales que servirán de WEP seed. Estas últimas claves, al ser temporales, evitarán el problema de reutilización y, además, se consigue evitar la exposición de las claves principales. TKIP también dobla el tamaño del IV de 24 a 48 bits.

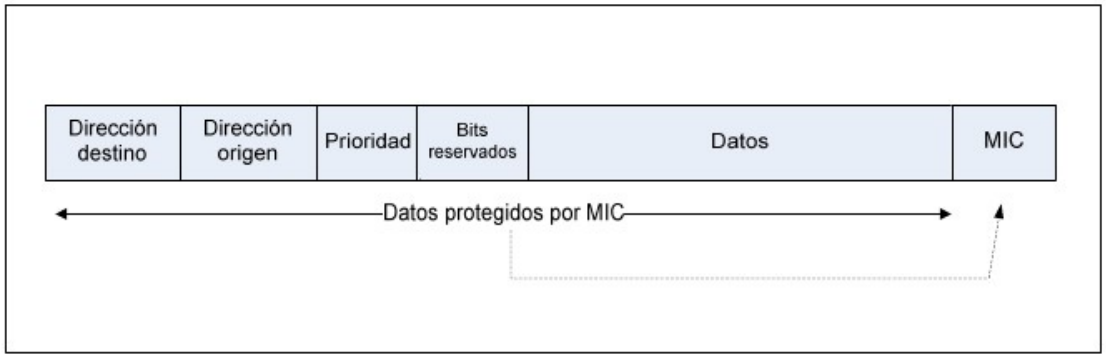
En la Figura 4.17 se puede ver el proceso que se sigue para realizar el cifrado con TKIP. Se muestra como el módulo de cifrado WEP se mantiene igual al definido por el estándar inicial. Las entradas que necesita el módulo WEP son la trama a enviar en claro y el seed WEP (que se compone de un IV y una clave secreta). el módulo software TKIP se encarga de generar los datos necesarios para que el módulo hardware WEP funcione de manera transparente a las mejores planteadas por el WPA .

La generación de la clave WEP y del IV se tuvo que diseñar en dos fases dado a las limitaciones que tenían muchos dispositivos inalámbricos que ya estaban operativos en el mercado. Para generar estos dos valores se utilizan elementos aleatorios o que dependen de cada dispositivo inalámbrico para dar aleatoriedad a las claves.

Control de secuencia de trama MIC

En la Figura 2.17 se puede ver que antes de enviar el mensaje en claro al módulo WEP, TKIP realiza unas manipulaciones sobre la trama. Las modificaciones que se realizan son para introducir el método MIC (Michael Integrity Check). Al contrario del CRC que usa el método WEP, el nuevo método MIC usado por TKIP podrá detectar manipulaciones en el payload del mensaje (la manipulación de CRC de WEP es relativamente sencilla). Aun así, el CRC que introduce WEP no es eliminado, ya que éste es parte del estándar WEP. El MIC será añadido tomando slots que pueden pertenecer a los de datos.

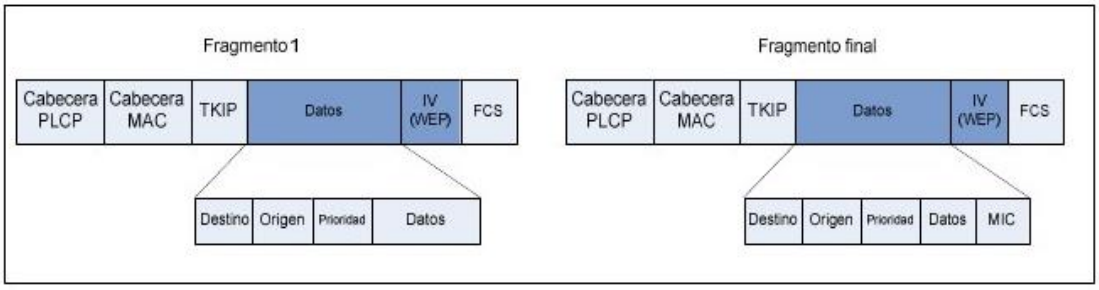
Fig. 4.18 Datos protegidos por MIC



Fuente: [CCNA, 2011]

El MIC no protege cada paquete sino bloques de ellos (un máximo de 32 tramas). Así pues, en la Figura 4.18, se tiene un solo MIC por cada conjunto de fragmentos de trama. El primer paquete, además de los datos, contiene información como las direcciones de los dispositivos. El último paquete, de un máximo de 32 tramas, es el que contiene en si el campo MIC que protege a las tramas anteriores.

Fig. 4.19 Mecanismo MIC



Fuente: [CCNA, 2011]

El proceso de gestión del MIC lo realizará el módulo software TKIP. Se lo puede ver en la rama derecha de la Figura 4.19.

Como se ha dicho, otra ventaja que se introduce con MIC es que, al estar a nivel de la capa MAC, permite que pueda ser implementado mediante hardware o software, con lo que los

nuevos chips inalámbricos puedan incorporar un módulo exclusivo para esta función y de esta forma aumentar el rendimiento de la tarjeta.

Aún así, por si solo no es un método seguro completamente. Es vulnerable a ataques de fuerza bruta y por eso incorpora varios contadores para evitar posibles ataques de Captura de paquetes o de re inyectado.

Modos de funcionamiento

WPA tiene 2 modos de funcionamiento de cara al usuario:
Personal: el usuario debe compartir una contraseña con el AP y con todos los demás usuarios de la red. A diferencia de WEP, donde el shared secret era de tamaño fijo, en WPA la passphrase puede tener entre 8 y 63 caracteres.
Enterprise: en este caso se usa algún método externo (como puede ser alguno de los métodos EAP) para la autenticación. Este modo es más seguro que WPA personal porque este sistema puede autenticar por usuario, no por maquina (cada usuario tiene su identificador no compartido). Este caso necesita un servidor RADIUS de autenticación.

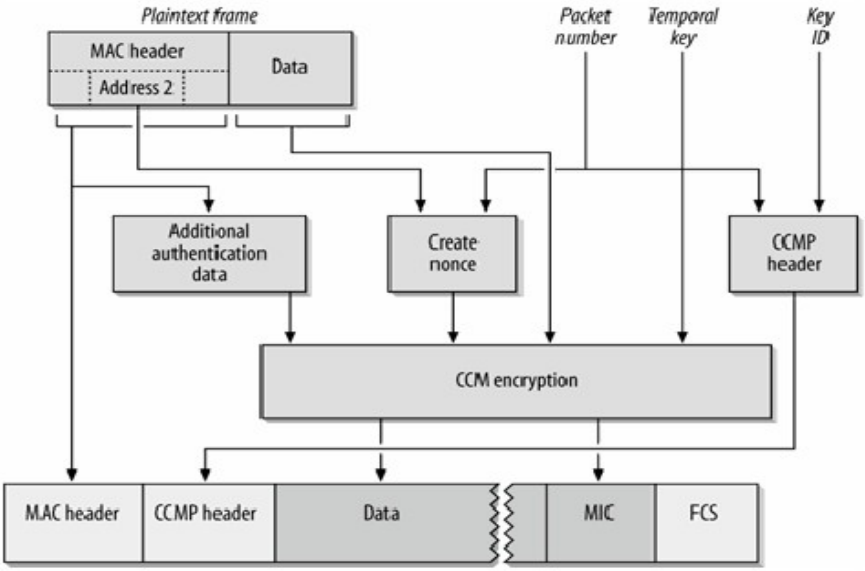
Protocolo CCMP

El protocolo CCMP (Counter Mode with CBC-MAC Protocol) es el protocolo diseñado para utilizar el algoritmo de cifrado AES en 802.11. CCMP usa el CCM (Counter Mode With CBC-MAC) que está definido en el RFC 3610.

Manejo y generación de claves

Como en el caso del TKIP, CCMP integra en un mismo proceso, el cifrado de datos y el mecanismo de comprobación de integridad de los datos transmitidos (Figura 4.20).

Fig. 4.20 Mecanismo CCMP



Fuente: [CCNA, 2011]

El supplicant y el autenticador son los elementos que funcionan mediante el método de puertos, por eso son llamados elementos PAE (Port Authentication Entities). Estas entidades se pueden comunicar mediante mensajes EAPOL (EAP Over LAN) aún cuando el cliente no tenga ni dirección IP ni tenga un puerto autorizado (sólo se permitirán los mensajes de inicio de autenticación). El autenticador y el servidor de autenticación se comunican mediante mensajes RADIUS, ya que RADIUS proporciona una gran variedad de métodos de autenticación, flexibilidad y compatibilidad con muchas de las bases de datos de usuarios.

En definitiva, este sistema de autenticación se incorporó al estándar 802.11 el cual intenta eliminar una de las dos debilidades más importantes de WEP en este campo. El punto fuerte del 802.1x es que evita el paso de cualquier tipo de tráfico hacia la red si el usuario no ha sido previamente autorizado. El usuario no autenticado sólo puede conseguir enviar paquetes del tipo EAPOL al puente para que éste los envíe al servidor de autenticación.

4.5.2 Eap

EAP (Extensible Authentication Protocol) nació de la necesidad de tener un mecanismo de autenticación más robusto para las conexiones PPP (Point-to-Point). El EAP está definido en RFC 3748 y al ser "Extensible" (o tener estatus de framework) se le permite que pueda ser modificado para incluir nuevos métodos de autenticación (como en su momento hizo CISCO Systems con la autenticación LEAP).

En el caso de las transmisiones inalámbricas, el EAP es utilizado por el 802.1x para realizar la comunicación entre los dispositivos que intervienen en la autenticación del cliente.
A continuación se describen los métodos de autenticación más importantes para el desarrollo de este documento. Estos métodos han de cumplir con lo dicho en la introducción del proyecto: han de tener una autenticación veraz y han de proporcionar seguridad sobre sus mensajes. Es por eso que sólo se trataran los métodos de autenticación criptográficos dejando de lado los que usan una criptografía débil como pueden ser el EAP-MSCHAP (versión 1 y 2), EAP-AKA, CHAP, MD-5 entre otros.

4.5.3 Leap

Como ya se ha dicho LEAP (Lightweight Extensible Authentication Protocol) fue diseñado por la compañía CISCO Systems con tal de proveer a sus sistemas de una autenticación robusta con WEP y a la vez sencilla de implementar.

Este sistema, dado a su carácter propietario, sólo puede hacerse servir en dispositivos CISCO y en algunos compatibles con este. Este sistema usa un servidor RADIUS, el cual también ha de ser de CISCO. Con esto se limita la agilidad del sistema dado a la obligación de usar los dispositivos del fabricante.
Con el tiempo el sistema LEAP se ha visto debilitado a causa de que está basado en el sistema de autenticación CHAP (el cual es inseguro). Aprovechando ataques a MS-CHAP se diseñaron diversos ataques de diccionario a los cuales se demostró que LEAP era vulnerable.

LEAP actualmente es desaconsejado por el propio fabricante CISCO y es importante conocerlo debido a que fue el primer paso de los fabricantes para facilitar y mejorar la seguridad de las redes inalámbricas. Cisco desarrollo EAP-Fast que mejoró la seguridad ofrecida por su predecesor, pero sigue siendo propietario y no estándar.

4.5.4 Eap-Tls

Este método es el más robusto de todos los métodos de autenticación que implementa EAP. Este método considera la red inalámbrica totalmente insegura, es decir, como si se tratara de la red de Internet, por lo tanto la autenticación debe ser mutua, tanto el cliente como el servidor deben ser autenticados. La autenticación se realiza mediante certificados digitales, con lo que es necesario disponer una estructura PKI (Public Key Infrastructure).

Con esto se puede ver que este sistema proporciona los requerimientos para poder asegurar que la autenticación es completa y segura. Los certificados proporcionan autenticación entre usuarios y el servidor, con lo que se evitan los ataques de llamados rogue (atacante que usa un AP para suplantar a otro operativo). Además, dado a que los certificados digitales incluyen claves criptográficas, estos proporcionan un método para distribuir claves de cifrado de datos de manera segura.

En este sistema el problema llega en el momento de distribuir los certificados: la clave privada de un certificado digital puede quedar a la vista de un atacante que tenga acceso a los archivos personales de un usuario. No obstante, el mayor inconveniente de este sistema es que implica la necesidad de mantener una estructura PKI y un servidor de autenticación RADIUS. Por lo tanto, la dificultad de implementación de este sistema evita que muchas redes puedan disponer de esta seguridad.

4.5.5 Eap-Ttls

Este sistema es similar al EAP-TLS pero sólo se usa el certificado de servidor. Este método apareció dado a que se prefería mantener la autenticación de red nativa ya implementada,

como puede ser la autenticación contra el Directorio Activo (método usuario y contraseña usado en un dominio Windows), LDAP Directory o autenticación mediante Kerberos. Por lo tanto este método proporciona una mezcla entre el sistema inalámbrico y el sistema que ya funciona en la red cableada.

En un primer paso, se establece un túnel TLS mediante el certificado digital del servidor de autenticación (en el cual confiamos ya que está firmado por una CA). Una vez establecido el túnel seguro, se envía la autenticación de usuario original que ya no depende del método EAP.

Con este método se puede ver que eliminamos parte de la estructura de la PKI (ya no son necesarios los certificados de usuario). Aún así necesitamos disponer de otro método de autenticación el cual puede no estar disponible en redes no empresariales.

Parte Ii

4.6 Estudio de la Seguridad en Redes 802.11

Las redes inalámbricas proporcionan cuatro servicios básicos los cuales determinaran su seguridad:

Autenticación: verificación mutua entre ambos actores en el proceso de la comunicación. Se Ha de asegurar de que con quien se comunica es realmente quien dice ser.

Integridad: asegurar que los mensajes no han sido modificados desde que fueron creados hasta que son recibidos.

Confidencialidad: asegurar que sólo el emisor y el receptor puedan comprender el mensaje transmitido. Para todos los demás este mensaje ha de ser indescifrable.

No repudio: asegurar que sólo el emisor puede firmar digitalmente los certificados, de manera que este no puede negar la emisión de un mensaje con su firma.

Como se pudo ver en la PARTE I el estándar inicial trató de ofrecer estos servicios aunque no logró proporcionarlos correctamente, provocando puntos débiles y lagunas. Aún sin ser cien por cien fiable, actualmente el estándar no es el principal culpable de la debilidad de las redes que se pueden encontrar. Los factores ajenos al estándar introducen mucha más debilidad al sistema.

El factor ajeno que más impacto tiene sobre la seguridad en los sistemas 802.11, como se verá más adelante, son los planificadores, administradores y usuarios de la red.

Actualmente las diferentes posibilidades en cuanto a seguridad del 802.11 no son provechadas ni por los usuarios, por desconocimiento de la tecnología), ni por los proveedores para evitar así problemas de compatibilidad con dispositivos antiguos y problemas de configuración que significarían gastos extras en servicio técnico y la desconfianza del usuario en sus productos. Por lo tanto, en este punto se expondrá las debilidades del estándar y se analizara la seguridad ofrecida por parte de los principales proveedores de acceso a Internet y los fabricantes de hardware. Una vez conocidas las debilidades y posibilidades existentes en el mercado y teniendo en cuenta las más usadas para dar veracidad a los resultados, se mostrara algunos ataques a redes inalámbricas y se realizara algunos ejemplos prácticos de los mismos, se demostrara cuan robusto es cada sistema.

4.7 Seguridad Ofrecida Al Usuario - Seguridad Ofrecida Por Los Proveedores

Como proveedores consideramos a toda aquella entidad que proporciona el hardware para el acceso a Internet, ya sean los fabricantes (3Com, Zyxel, Linksys, Cisco, etc.), como los proveedores de acceso a Internet que ofrecen routers pre-configurados mediante un sistema diseñado o supervisado por ellos (Telefónica, Ono, Orange, Tele2, etc.).

Como se verá en el siguiente apartado, en ambos casos la seguridad que ofrecen inicialmente estos dispositivos es insuficiente y puede comprometer el sistema. Aún así se diferencian los dos casos (fabricantes y proveedores de Internet) ya que en el caso de los fabricantes

normalmente venden sus productos configurados con un nivel de seguridad baja para que sean fácilmente accesibles, indicando y guiando al usuario a soluciones más seguras (con lo que normalmente debería ser el usuario el que tome la decisión). En cambio, los proveedores de Internet, venden una solución completa (Internet y configuración) la cual anuncian como solución totalmente segura. Como vera más adelante, lo único que consiguen con estas facilidades es debilitar aún más la seguridad ofrecida al usuario.

4.7.1 Fabricantes

La mayoría de routers tienen una configuración por defecto de fábrica similar. Para facilitar la conexión del dispositivo al usuario inexperto, el router viene preconfigurado para ser conectado a la red sin ninguna modificación. El servidor de direcciones IP o DHCP (Dynamic Host Configuration Protocol) normalmente está activado para evitar que el usuario deba configurar sus dispositivos (lo que facilitaría a un posible intruso una IP una vez dentro de la red). Además, la tarjeta de red inalámbrica de estos routers también suele venir pre configurada en modo encendido, con broadcast (emisión) del ESSID y sin cifrado. En las Tabla 4.2 y Tabla 4.3 pueden verse los datos sobre la configuración de fábrica de algunos modelos de diversos fabricantes. Estas configuraciones han sido extraídas de los manuales de usuario de los dispositivos que se muestran.

Tabla 4.2 Configuración de fábrica de algunos routers

	3Com 11G	CT 536+	C54BRS4	DSL-604+G	WRT45G	DG834G
Marca	*3Com*	Comtrend	Conceptronic	D-Link	*Linksys*	Netgear
Estándar	*802.11b* y g	*802.11b* y g	*802.11b* y g	*802.11b* y g	802,11 b y g	802,11 b y g
IP	192.168.2.1	192.168.1.1	192.168.2.1	192.168.0.1	192.168.1.1	192.168.0.1
User / pass	/ 1234admin	admin/admin	admin/1234	admin/admin	/ admin	admin / password
Radio	off	on	on	on	on	on
SSID	-	Cometrend	WLAN	default	linksys	NETGEAR
Seguridad WLAN	-	abierto	abierto	abierto	abierto	abierto
DHCP	-	-	-	2 a 33	100 a 150	2 a 254
Manual	no	si	si	si	si	si

Fuente: [Cisco, 2007]

Tabla 4.3 Configuración de fábrica de algunos routers

	7404 WBRA	1500 Fast	WebSTAR 2320	Prestige 660	7768r
Marca	SMC	sagem	Scientific atlantic	*Zyxel*	Xavi
Estándar	802,11 b y g	802,11 b y g	802,11 b y g	802,11 b y g	802,11 b y g
IP	192.168.2.1	192.168.0.1	192.168.0.1	192.168.1.1	192.168.1.1
User/pass	(SIN PASSWORD)	(SIN PASSWORD)	(SIN PASSWORD)	1234 / 1234	admin / admin
Radio	on	off	on	on	on
SSID	Wireless	-	WebSTAR	Wireless	act1
Seguridad WLAN	abierto	-	abierto	abierto	abierto
DHCP	100 a 199	-	10 a 255	33 a 100	deshabilitado
Manual	si	no	si	si	si

Fuente: [Cisco, 2007]

Como se puede observar en las tablas anteriores, todos los routers son configurados por el fabricante con una IP que suele ser 192.168.1.1 (las definidas para redes privadas de 254 direcciones, es decir con una máscara /24). También observamos que la gran mayoría tienen

habilitada la interfaz inalámbrica con un ESSID sin ocultar (broadcast) y sin seguridad, es decir, abiertos. Además, también la mayoría de ellos tiene el servidor DHCP habilitado con lo que servirá una IP automáticamente. Muchas de estas configuraciones provocan que cualquier cliente (deseado o no) que esté en el radio de cobertura del router, pueda conectarse a nuestra red inalámbrica. La mayoría de fabricantes incluyen en sus manuales una advertencia de que la configuración inicial no es segura e indican los pasos a seguir, tanto en el router como en el cliente, de cómo conseguir aumentar la seguridad del sistema pare evitar la mayor parte de intrusos.

Por lo tanto en este caso podríamos exculpar al fabricante y señalar al usuario como el culpable de su mala utilización en las redes domésticas.

4.7.2 Proveedores de Acceso a Internet

Desde hace unos años los proveedores a Internet utilizan la tecnología inalámbrica como una ventaja. Antes de la existencia de esta tecnología, se debía realizar el cableado en el hogar del usuario para darle acceso. En el pasado algunos proveedores, en sus ofertas, ofrecían la gratuidad de esta instalación como un reclamo para captar clientes.

Con la aparición de la tecnología inalámbrica los proveedores vieron una manera de rebajar sus costes y sobretodo de promocionar su producto evitando la molestia de la instalación del cableado. A priori todo parecían ventajas para la operadora y el usuario, que cree recibir un producto de más calidad (eliminando molestias). Pero estos mismos proveedores, ofuscados por todas estas mejoras, no se preocuparon de la seguridad que ofrecían con este tipo de redes inalámbricas.

Aún así, poco a poco fueron cogiendo consciencia del problema que significa introducir este tipo de hardware sin ningún tipo de control e introdujeron algunas mejoras. No obstante los cambios (básicamente uso de cifrado WEP en sus configuraciones) no mejoraron excesivamente la seguridad de la red.

Así pues, los primeros routers instalados por los proveedores ni siquiera tenían configurada su seguridad, estaban abiertos a cualquiera dentro de su radio de cobertura. Esto era normal al principio de esta tecnología dado a su novedad, precio y su poco uso. Entonces había un riesgo mínimo de intrusión. A medida que esta tecnología iba ganando adeptos, el nivel de posibles intrusos creció. La inclusión en los portátiles del chip Centrino (placas madre con una tarjeta inalámbrica embebida) marcó un punto de inflexión ya que a partir de ese momento todo portátil podría conectarse a estas redes desprotegidas.

Como se ha comentado, actualmente, la situación ha mejorado, eliminando posibles intrusos usando cifrado WEP y en algunos casos WPA-PSK. Pero el acceso a la gran mayoría de puntos de acceso sigue siendo relativamente fácil para usuarios expertos o simplemente usuarios curiosos por esta tecnología debido a la debilidad de las configuraciones de estos proveedores En la Tabla 4.4 se puede encontrar una descripción de los principales proveedores actuales y de diferentes características del acceso inalámbrico que ofrecen.

Tabla 4.4 Configuración de proveedores acceso a Internet

Proveedor	*Telefónica*	YA.COM	ORANGE	ONO
Marca y modelo	*Zyxel, Xavi, (otros)*	D-LINK DLS-G624T	SAGEM 1500	Motorola
SSID	WLAN_XX	DLINK-WIRELESS	adslXXXX	P1XXXXXX0000X
Cifrado	WEP 128	WEP 128	WEP 128	WEP 64 o 128
Gateway	192.168.1.1	192.168.1.1	192.168.0.1	192.168.1.1
DCHP	Habilitado	Habilitado	Habilitado	Habilitado
user/password	1234/1234 o teléfono abonado	1234/1234	(deshabilitado)	(en blanco)

Fuente: [Cisco, 2007]

Puede verse que todos los proveedores aquí analizados implementan seguridad WEP. La mayoría de IP's de red son las típicas de redes privadas y las contraseñas de acceso a los routers suelen ser las de configuración de fábrica.

En este caso la responsabilidad recae en primera instancia en el proveedor de Internet. Este debería proporcionar la misma seguridad que en la red de su propiedad (es decir en la red

cableada). Puede excusarse a los usuarios ya que esta configuración muchas veces no es cambiada por los usuarios, no por desconocimiento, sino a veces no les está permitido el acceso al router (la contraseña de acceso al router está en posesión solamente de la operadora y no se comunica al usuario), o porque confían en que el producto adquirido ya es seguro (ya que la operadora no da ninguna recomendación en la modificación de la seguridad).

4.8 Seguridad Ofrecida por El Estándar 802.11

Como se ha visto en la PARTE I de este documento, el estándar proporciona varios niveles de seguridad, así como varios mecanismos de autenticación y algoritmos de cifrado posible. Por parte del estándar, esta gran variedad de posibilidades proporcionan agilidad al sistema y se puede decir que el estándar posee métodos que actualmente pueden considerarse totalmente seguros. Aún así, dentro de estas diferentes opciones que proporciona, hay algunas las cuales su seguridad no es suficientemente robusta, lo que provoca que al ser usadas se ponga en entre dicho la seguridad de estas redes. Así pues, se puede afirmar que el estándar proporciona posibilidades de seguridad suficientemente confiables siempre que sea usado de una manera correcta y se comprenda dónde están sus debilidades.

4.8.1 Puntos Débiles En La Seguridad

Seguidamente se trataran los puntos débiles de la seguridad en las redes 802.11. Se hará referencia a la base teórica introducida anteriormente en la PARTE I dedicada al estándar 802.11.

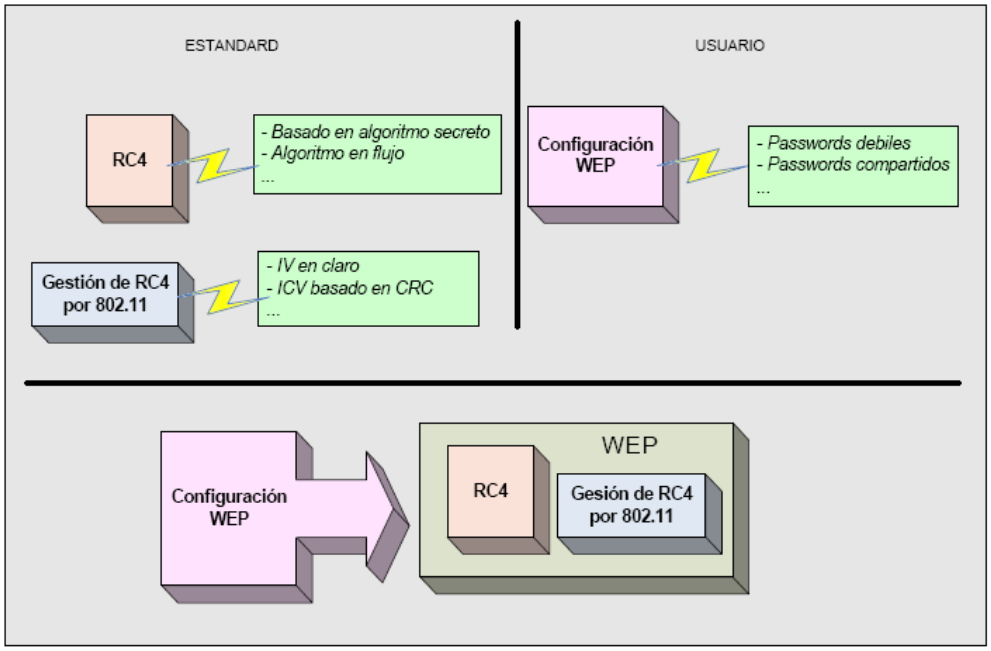
La seguridad más extendida en las redes inalámbricas es WEP. Es por ello que los puntos débiles de la seguridad serán enfocados hacia este mecanismo, aún conociendo que existen otros mecanismos mucho más seguros en la actualidad.

4.8.2 Debilidad De Wep

Las debilidades de WEP no sólo se limitan al algoritmo utilizado (RC4), sino que el diseño de WEP introduce otras que provocan que RC4 aún sea más vulnerable a taques estadísticos. Por lo tanto, se puede decir que el protocolo WEP gestiona de una manera incorrecta RC4.

Además, deben ser consideradas la debilidad que pueden introducir los usuarios y proveedores al configurar WEP con una clave débil y compartida por muchos usuarios. Así pues, como se puede apreciar en la Figura 4.21, se pueden agrupar debilidades en debilidades provocadas por deficiencias en el estándar y en debilidades provocadas por una mala configuración por parte del usuario/proveedor.

Fig. 4.21 Causas de las debilidades de WEP



Fuente: [Wikipedia, 2010].

Debilidades provocadas por el estándar

RC4 es un algoritmo de cifrado en flujo y por esta razón ya posee una debilidad intrínseca. Los algoritmos en flujo tienen la propiedad de que si realizamos la función XOR de dos paquetes cifrados con la misma clave, el resultado será el mismo que realizar la misma operación pero con los paquetes en claro. Por tanto, cuando tengamos 2 paquetes cifrados con la misma clave, y conozcamos el texto en claro de uno de ellos, se podrá conocer el otro texto claro. WEP intenta solucionar dicha debilidad de los algoritmos en flujo mediante la introducción de los IV's, pero no lo consigue. Como vimos en el apartado 2.4 de la PARTE I, WEP añade estos IV's como parte variable de la clave compartida para generar el flujo de bits de la clave o Key Stream, que cifra cada trama transmitida. WEP envía estos IV sin cifrar, por lo tanto, se volverán a tener tramas repetidas (los IV proporcionan un máximo de 16.777.216 combinaciones diferentes).

Por lo tanto el transmitir en claro los IV provoca otra debilidad que facilita los ataques de tipo estadístico. Estos ataques fueron presentados en 2001 cuando Itsik Mantin, Scott Fluhrer y Adi Shamir (este último uno de los creadores del RC4 y de otros sistemas criptográficos como el RSA) presentaron sus estudios sobre dicha estadística y las debilidades del RC4 (aplicables a WEP).

Otra de las debilidades es que el estándar inicial sólo daba la posibilidad de usar claves de 40 bits (+ 24 bits de IV) o 104 bits (+40 bits del IV). Esta longitud de clave es insuficiente para cifrar de manera segura con RC4. Además tampoco obliga a que estas claves sean seguras criptográficamente, con lo que un usuario puede dejar la clave WEP por defecto o elegir una clave que sea sencilla de recuperar por el atacante mediante fuerza bruta.

Otro de los errores que dependen de la implementación de WEP es el uso de un CRC para comprobar la integridad (véase el apartado 2.4 de la PARTE I). Los algoritmos CRC no fueron diseñados para la criptografía, ya que un atacante puede determinar el valor que tendrá el CRC si se realiza un cambio en el payload de la trama. Por lo tanto, será sencillo modificar un paquete cifrado con WEP y que este siga siendo válido.

La solución a este último problema hubiese sido la utilización de métodos basados en el hash de la trama, que harían que el resultado de este hash no fuera predecible y modificarlo significara el descarte de la trama. Aún así este método de protección necesitaría de una electrónica más potente, que en el momento del diseño del estándar fue desestimada.

Debilidades provocadas por el usuario

En el caso del usuario, las debilidades no son exclusivamente suyas, sino que son a causa de varias deficiencias del estándar. Estos errores suelen ser los más graves ya que pueden poner en compromiso la seguridad de todo el sistema.

Una de ellas es que el estándar 802.11 no especifica ningún tipo de gestión de claves, con lo que las claves compartidas suelen ser utilizadas durante mucho tiempo y por muchos usuarios al mismo tiempo. El administrador debería realizar cambio de claves de manera periódica, además de mantenerlas secretas y utilizar la posibilidad de usar varias claves WEP en un mismo punto de acceso. El uso de estas prácticas queda a elección del administrador, es por ello que en este caso el estándar no es el principal culpable.

Otra debilidad introducida por el usuario es la elección de claves sencillas y cortas. Mediante ataques estadísticos, las claves sencillas serán rápidamente encontradas. Finalmente se puede decir que muchas veces el usuario no se preocupa por cambiar la configuración de fábrica, lo que implica estar usando una configuración genérica, lo que posibilita el acceso simplemente disponiendo de la configuración de fábrica.

4.8.3 Debilidad De Wpa

Como dijimos al principio de la PARTE II, este documento se centrara en el protocolo WEP debido a que es el más extendido. En la actualidad no tiene sentido querer atacar una red WPA para conseguir acceso a la red, ya que seguramente, alrededor de ella tengamos varias redes con WEP, las cuales serán mucho más sencillas de acceder.

A título informativo, se puede decir que la debilidad en estas redes se encuentra en el método de autenticación. Durante este proceso pueden obtenerse los mensajes del reto de conexión o handshake.

Otra debilidad, la cual comparte con WEP, es el uso de claves compartidas. Como dijimos con WEP, el uso de este tipo de claves posibilita que la clave WPA pueda dejar de ser secreta, poniendo en compromiso a todas las estaciones.

4.9 Ataques A Redes Inalámbricas

El medio que utilizan las transmisiones inalámbricas, el aire, es muy propicio a todo tipo de ataques. En una red cableada, el atacante ha de estar físicamente conectado a un punto de la red, sino es imposible conseguir ningún tipo de acceso. En las redes inalámbricas el acceso a este medio no supone ninguna barrera, con lo que la posibilidad de ataque será más amplia y con un índice más elevado de éxito.

Los siguientes ataques que aquí se muestran han sido particularizados para redes inalámbricas, pero estos ataques pueden llevarse a cabo (con más o menos facilidad) en cualquier red:
- Man-in-the-middle: este ataque es mucho más sencillo en redes inalámbricas que en las redes cableadas dado que el medio de acceso es el aire. En redes cableadas no todos los paquetes han de pasar obligatoriamente por el cable o tramo de red en el cual estamos capturando tráfico. Los ataques Man-in-the-middle consisten en la interceptación de las tramas enviadas por algún usuario. Este ataque puede ser pasivo o activo. En los ataques pasivos el atacante realiza eavesdropping, es decir, simplemente se limita a capturar paquetes sin provocar

ninguna alteración en ellos. En los ataques activos normalmente el atacante captura paquetes y los reenvía modificados según le convenga. Este ataque será el más utilizado en el estudio de ataques a redes inalámbricas que se verán en el apartado 2.11 de la PARTE II (llamado reinyección de tráfico).

- Denegación de servicio (Denial of service, DOS): significa evitar que los clientes consigan acceder a la red, o a un servicio que esta ofrezca. Este ataque puede ser realizado enviando tramas erróneas al medio, degradando tanto el servicio hasta hacer caer al punto de acceso. También existen maneras más rudimentarias en comunicaciones inalámbricas, las cuales provocan un ataque DOS con la utilización de dispositivos que saturen la banda de frecuencias 2’4 GHz. Como se verá en el apartado 2.11 de la PARTE II, serán usado este tipo de ataques para des autenticar algún cliente ya autenticado.

- ARP poisoning: el protocolo ARP (Address Resolution Protocol) permite encontrar la dirección IP a partir de la dirección MAC. Las peticiones ARP se realizan sólo una vez para ser almacenadas en una tabla y así evitar peticiones ARP cada vez que hay que enviar un paquete a una determinada IP. Para realizar un ataque a la red sólo sería necesario introducir un paquete ARP con la dirección IP del atacante pero con la dirección MAC del cliente al que se quiere atacar. Con esto todas las trasmisiones enviadas al cliente serian enviadas realmente al atacante. Este ataque puede verse limitado por la cantidad de saltos que haya por la red (ya que no siempre la dupla ARP-IP corresponderán al destinatario del paquete). En el apartado 2.11 de la PARTE II no será usado este ataque de re direccionamiento, sino que se suplantara la identidad de algún dispositivo usando su dirección MAC.

Una vez descritos los ataques genéricos a cualquier tipo de red, se deberán dar a conocer otros conceptos que son necesarios para llevar a cabo ataques a redes 802.11.

4.9.1 Términos Básicos

4.9.1.1 Wardriving

La captura de tráfico inalámbrico y el ataque a estas redes no es una ciencia exacta debido a que el medio de transmisión es muy variable. Por eso, se necesitara usar algún dispositivo portátil para conocer la ubicación de la red que se quiere atacar. Además se deberá reconocer el terreno para saber desde que lugar se puede obtener una mejor potencia de señal. La necesidad de disponer de una buena relación señal a ruido es debido a que la captura de paquetes, al ser una técnica pasiva donde el atacante no está asociado, no hay posibilidad de retransmisión o de comprobación de errores, por lo tanto, un paquete perdido malinterpretado no podrá ser detectado. Al reconocimiento de redes de manera remota (mediante un portátil o una PDA desplazándonos por una zona) se le llama wardriving.

Para realizar wardriving necesitamos un hardware y software que nos permitan cuantificar la señal que recibimos y darnos los datos básicos de la red (ESSID, BSSID, canal de transmisión, MAC de los clientes, etc.). Siempre es bueno realizar el wardriving con la misma tarjeta que realizamos el ataque, ya que para cada tarjeta inalámbrica se pueden obtener resultados diferentes. Para la composición de este documento se ha realizado una estadística de wardriving, con la que se podrá justificar determinadas acciones tomadas en esta PARTE II.

2.9.1.2 Modo Monitor

En el apartado 4 de la PARTE II se verán diferentes casos de ataque. También en él se incluirán las características del hardware utilizado, remarcado la importancia del fabricante del chip de la tarjeta inalámbrica o chipset (véase apartado 2.11.1 de la PARTE II).

Como avance se puede decir, que esta importancia recae en que para realizar determinadas técnicas de ataque hace falta que la tarjeta se ponga en un modo especial llamado modo monitor. Los chipset que se describen en este documento poseen controladores o drivers de código abierto con lo que es posible acceder de manera directa a esas funciones especiales no

diseñadas para usos comunes. Se ha de destacar que la mayor parte de estos drivers sacan el mayor partido a las tarjetas inalámbricas bajo Linux. Para Windows hay algunos drivers diseñados por algunas compañías como Wildpakets (AiroPeek) o TamoSoft (ComView) y sólo para determinados modelos de chipsets que permiten experimentar con estas funciones. Por lo tanto, la mayor parte de casos de estudios en este proyecto planteados, serán tratados bajo distribuciones Linux.

En cuanto al modo monitor, éste es uno de los cuatro modos en los cuales una tarjeta inalámbrica puede actuar. Los siguientes son los cuatro modos posibles:

- Managed: modo más común, el cual proporciona las funciones para hacer de clientes inalámbricos y conectarnos a un punto de acceso. - Ad-Hoc: modo similar al Managed pero para acceder o crear una red punto a punto.
- Master: usado por el punto de acceso para actuar como tal (varios clientes conectados). Con este modo la tarjeta puede actuar como punto de acceso.
- Monitor: permite captar todos los paquetes de cualquier red que esté a nuestro alcance sin necesidad de estar asociados a la red.

El modo monitor es similar al modo promiscuo de las tarjetas Ethernet, pero como se ha dicho, en el caso del modo monitor, para capturar el tráfico no necesitamos estar asociados con ningún AP. Mediante el modo monitor se recogerán todos los paquetes que seamos capaces de escuchar. A esto se lo llamara esnifar y al programa capaz de recoger estos datos, sniffer.

Tampoco hay que confundir el modo monitor, con el sistema comentado monitorización activa del medio inalámbrica comentado en el apartado 2.2.6 de la PARTE I. En el caso del modo monitor (monitorización pasiva), la tarjeta inalámbrica simplemente capta las señales sin enviar ningún tipo de paquete.

2.9.1.3 Inyección De Tráfico

La inyección consiste en el envío intencionado de paquetes por parte del atacante. Estos paquetes pueden haber sido creados por el atacante o capturados por este. Esta técnica no necesita conocer la clave WEP, debido a que en las retransmisiones de tráfico el payload del mensaje se suele dejar sin modificación, ya que lo que interesa es la cabecera y tal vez el CRC es vulnerable ante las modificaciones como vimos en el apartado 2.8.2 de la PARTE II.

La finalidad de esta técnica en muchos casos es conseguir la generación de tráfico por parte del dispositivo atacado. Un ejemplo podría darse en puntos de acceso que tienen un tráfico de datos muy bajo. Con esta técnica, si se dan determinadas condiciones que podrán verse en el apartado 2.11 de la PARTE II, se puede llegar a generar un seguido de paquetes que, al ser contestados por el punto de acceso, nos proporcionen un IV nuevo cada vez. Con la captura de suficientes IV's se podran aplicar los ataques estadísticos sobre WEP.

Se ha de destacar que algunos drivers y chipsets no nos permitirán inyectar tráfico con la misma tarjeta con la que realizamos el esnifado, por lo tanto según el chipset se necesitara una tarjeta para la inyección y otra para la captura. En el apartado 2.11.1 de la PARTE II se indicaran estos chipsets.

4.9.2 Ataque Al Protocolo Wep

En este proyecto, los ataques a WEP serán los más estudiados debido a que WEP es el sistema que más se utiliza para la seguridad de redes inalámbricas. Por lo tanto, la mayoría de escenarios que se pueden encontrar en la realidad será el de redes inalámbrica con seguridad WEP.

Los ataques a las redes con seguridad WEP se basan en las debilidades comentadas en el apartado 2.8.2 de la PARTE II. Gracias a técnicas estadísticas que se comentaran seguidamente será posible obtener con más facilidad la clave WEP. Dichas técnicas estadísticas se han ido mejorando. En sus versiones iniciales, los ataques FMS, necesitaban del

orden de 5 millones de paquetes que contuvieran IV's para llegar a descifrar una clave WEP de 128 bits. Gracias a una la mejora introducida por un usuario llamado KoreK rebajó esta cifra unos 500.000 IV. Actualmente existen técnicas que sólo necesitan unos 50.000 IV's.

4.9.2.1 Ataque Por Fuerza Bruta

Este es el ataque trivial y se realiza probando todas las claves posibles. Para realizar este ataque es indispensable conocer el texto en claro y el texto cifrado del mensaje. Una vez tengamos estos dos mensajes se aplicara el cifrado sobre el texto claro hasta conseguir la clave WEP. El gran problema es que este proceso es extremadamente lento dependiendo de si la clave usada contiene caracteres poco habituales.

Esta técnica, sola no sería útil de no ser utilizada conjuntamente con el criptoanálisis estadístico, que se verán en los siguientes puntos.

4.9.2.2 Ataque Mediante Criptoanálisis Estadístico Fms Y Korek

El FMS (Fluher, Martin y Shamir) es el primer ataque a WEP que se implementó a partir de la debilidad mostrada en el 2001. Este ataque consiste en recoger entre 5 y 10 millones (dependiendo del software utilizado y de la aleatoriedad de la clave) de IV's para descifrar una clave de 128 (véase apartado 2.8.1 de la PARTE II).

Este ataque necesita de la existencia de abundante tráfico en la red, por lo tanto, necesita de un cliente conectado y transmitiendo información. Además, los paquetes que capturamos han de contener IV's válidos. Los paquetes no siempre contienen IV's ya que los paquetes como los Beacons no están cifrados.
No obstante, mediante las técnicas ya comentadas de reinyección de tráfico, se puede provocar la generación de IV's mediante paquetes falsos que provoquen la emisión de paquetes codificados que contengan IV's. Estas técnicas se presenta en el apartado 2.11 de la PARTE II. Como se ha dicho, este ataque se vio mejorado por KoreK cuando planteó una serie de ataques que permiten descartar algunas claves según unos patrones.

4.9.2.3 Ataque Mediante Criptoanálisis Estadístico Ptw

En 2005 apareció otro ataque sobre RC4 llamado ataque de Klein. Este ataque aprovecha correlaciones entre la clave que usa RC4 y el Key Stream que genera. Erik Tews, Ralf-Philip Weinmann y Andrey Pyskin utilizaron esta nueva debilidad para realizar un ataque sobre WEP (ataque PTW) que permite recuperar la clave con solo 85.000 paquetes que contengan IV's con una probabilidad de éxito del 95%. La condición para el éxito de este ataque es que estos paquetes sean del tipo ARP. Debido a que se conoce parte del mensaje se tiene más información que ayudará a nuestro ataque estadístico.

En puede verse como el software aircrack-ng contempla los ataques anteriormente nombrados y los aplica según dictamine el usuario.

4.9.2.4 Otros Ataques

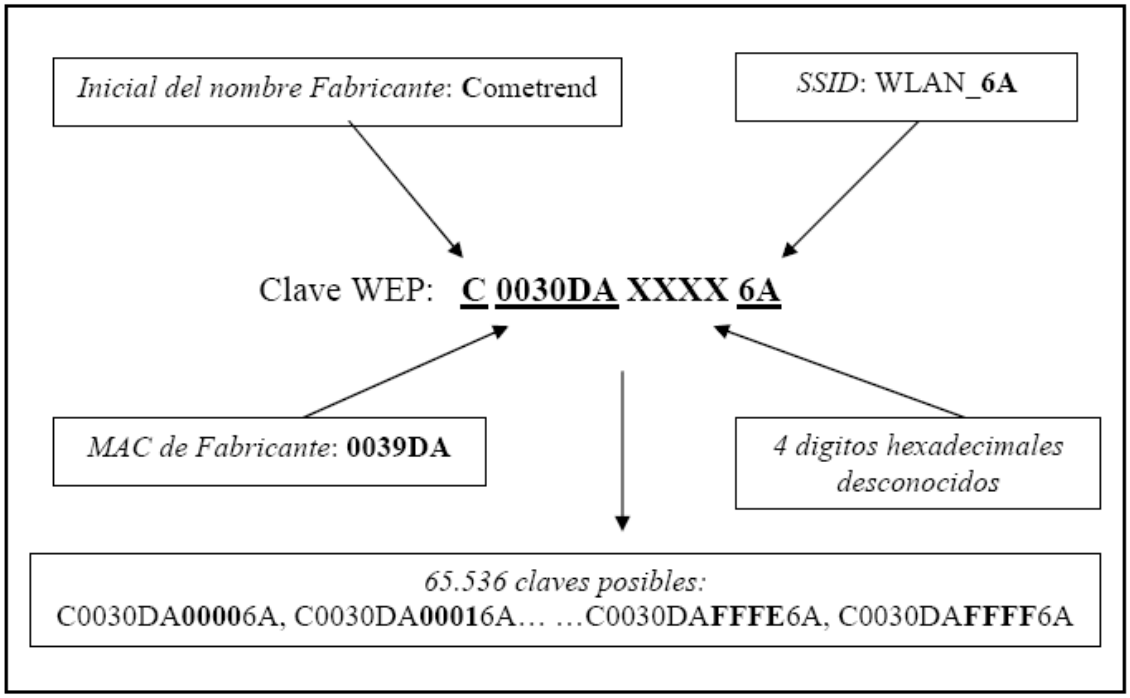
Hay otro tipo de ataques que aprovechan debilidades introducidas por los proveedores. Estos casos son particulares, pero son un caso muy interesante de debilidad introducida por la mala configuración de la red. Muchos de estos proveedores configuran su clave WEP siguiendo un patrón. Ejemplos de esto son el operador Ono, el cual usa como clave WEP el resultado de aplicarle el algoritmo MD5 al SSID de la red; o el de las redes DLINK_WIRELESS, las cuales usan como WEP la dirección MAC modificada según un patrón conocido. De esta manera, conociendo dichos parámetros no es necesario aplicar ningún tipo de ataque.

En otros casos, sólo parte de la clave WEP es conocida, lo que obliga a usar los ataques antes definidos, pero con un número muy reducido de claves a probar. Este es el caso de Orange y de Telefónica.

En caso de las redes WLAN_XX (donde XX serán hexadecimales) de Telefónica, estas utilizan WEP de 128 bits y usan como primeros dígitos de la clave WEP una letra que corresponde al fabricante y los 6 dígitos iniciales de la MAC de su router (los cuales son los

dígitos que identifican a cada fabricante). Los dos últimos dígitos de la clave WEP son los dos últimos caracteres del SSID de la red. Con esto se obtiene 9 de los 13 dígitos de la clave WEP, con lo que la clave desconocida pasa de ser de 104 bits a ser sólo de 32 bits. Teniendo en cuenta que, aún pudiendo usar caracteres especiales para la clave, sólo se usan valores del 0 al 9 y de la A ala F, esto implica que tengamos sólo 65.536 (164) claves posibles (véase Figura 4.22). Sobre un solo paquete capturado se puede probar las 65.536 claves distintas hasta dar con la correcta.

Fig. 4.22 Ejemplo de clave WEP en los routers de Telefónica



Fuente: Elaboración Propia

En el apartado 11.3. de la PARTE II podrá verse el caso de las redes de Telefónica, mostrando cómo mejorarlo para evitar la necesidad de que exista un cliente conectado.

Este caso es muy interesante ya que los otros ataques a WEP necesitaban de la existencia de algún cliente.

4.9.3 Ataque Al Protocolo Wpa

Las redes bajo la norma 802.11i y configuradas con WPA, pueden considerarse relativamente seguras. Aún así, en este caso parte de la seguridad sigue recayendo en como sea configurada, con lo que una clave sencilla puede provocar que la seguridad se vea comprometida (como se verá en un caso de ejemplo práctico).

Los ataques a WPA se basan en la captura del handshake, o secuencia de autenticación, de WPA. Para capturar un handshake se debera esperar a que un cliente se conecte a la red o provocar su desconexión para obligar a este a realizar dicho proceso de handshake.

Sobre el handshake capturado puede realizarse un ataque por fuerza bruta (o mediante un diccionario) con tal de descifrar la clave, con lo que se limita el éxito del ataque al nivel de seguridad que la clave proporciona.

Como se dijo al inicio de la PARTE II, actualmente la cantidad de redes con cifrado WPA son muy bajas y por lo tanto estos ataques aun no están muy depurados ni optimizados como los de WEP.

Se ha de añadir que a finales de 2008 apareció un nuevo ataque que puede ser realizado sobre una red WPA basada en TKIP, con una red con clientes y con una contraseña débil.

4.10 Ejemplos Prácticos

Una vez conocido y comprendido el estándar 802.11, y habiendo planteado los posibles problemas y las técnicas para llegar a romper la seguridad de dichas redes, se aplicara este conocimiento sobre casos reales, mezclando los conceptos comentados en esta PARTE II.

Para decidir los posibles casos que más se asemejen a escenarios reales se ha basado en la estadística del wardriving. Ésta ha sido realizada en diversos lugares de la ciudad y con ellas se puede ver la tendencia sobre la seguridad utilizada en las redes inalámbricas actuales.

Gracias a la estadística de los wardriving se puede asegurar que el estándar de seguridad más utilizado es el WEP con claves de 128 bits, sin autenticación y con el SSID en modo broadcast (difundido mediante la emisión constante de Beacons). Por ello, los casos de estudio en este documento serán enfocados hacia la intrusión en redes cifradas con WEP.

Se añadirán casos que cada vez se dan con menor regularidad (redes abiertas), pero que en un pasado no muy lejano eran más habituales.
Se ha de añadir, que la estadística de los wardriving también nos muestra que una gran mayoría de las redes que encontramos son las nombradas WLAN_XX (donde XX son valores hexadecimales) con lo que deducimos que han sido configuradas por Telefónica y donde se podrá aplicar la técnica comentada en el apartado anterior (apartado 2.9.2.4 de la PARTE II).

Por otra parte, las redes con autenticación 802.1x no serán aquí estudiadas, dado que mediante la técnica de wardriving no han sido encontradas en zonas residenciales. Por lo tanto, después de observar y analizar los datos del wardriving, se decidió considerar los siguientes casos de estudio:

- Acceso a una red sin seguridad
- Acceso a una red con SSID oculto
- Acceso a una red con seguridad WEP
- Acceso a una red con SSID WLAN_XX

4.11 Herramientas

Antes de exponer los casos de estudio se determinaran el hardware y software con el que se debe trabajar.

4.11.1 Hardware

El adaptador inalámbrico:

En ataques a redes inalámbricas el punto más importante es "saber escuchar". Esto significa que se tiene que disponer de herramientas hardware y software que nos permitan captar con la menor tasa de paquetes perdidos, todo lo que es transmitido del AP hacia los clientes y viceversa. Por tanto, lo primero que necesita es determinar es el adaptador inalámbrico o WNIC (Wireless Network Interface Card).

Los adaptadores inalámbricos, conocidos vulgarmente como tarjetas inalámbricas, pueden ser de muchos tipos: los hay USB, PCMCIA, PCI, con antena interna, con conector de antena externa, que soporten solo la norma 802.11b, etc. Aún así, como vimos en el apartado 2.9.1.2 de la PARTE II, estas tarjetas deben, entre otras características, ser capaces de entrar en modo monitor, lo cual nos obliga a elegir entre unos chipset determinados.

Seguidamente se describirán conceptos que se ha de tener en cuenta para conseguir realizar los ataques que se verán a continuación:

Chipset: es el chip que gestiona la interfaz inalámbrica de la tarjeta y el que determinará si la tarjeta puede ponerse en modo monitor. Hay varias marcas de chipset aunque lo más importante es que algunos de ellos tienen drivers de código abierto, con lo que pueden ser utilizadas para acciones no-estándares.

Estos drivers suelen estar sólo disponibles para Linux. Además se ha de elegir una tarjeta que pueda ser usada con las diferentes normas del estándar (a/b/g), para poder sniffar a cualquier velocidad. Los chipsets más conocidos y contrastados que permitirán realizar acciones son Atheros, Prism 2.0 y 2.5, Intel Centrino, Ralink y Orinoco.

- **Sensibilidad:** como se ha dicho antes, captar bien los paquetes enviados por terceros será fundamental. Cuanta más sensibilidad tenga una tarjeta inalámbrica menos señal se necesitara recibir y más lejos se podrá estar para realizar capturas. La sensibilidad también depende de la velocidad de transmisión (a más velocidad menos sensibilidad). Los valores para dispositivos inalámbricos normales son de -85 dBm5 a 11 Mbps y -89 dBm a 1 Mbps La experiencia adquirida nos lleva a ser más exigentes y elegir tarjetas de aproximadamente 90 dBm a 11 Mbps y 95 dBm a 1 Mbps (en estos datos no incluimos 54 Mbps ya que se intentará realizar los ataques a la mínima velocidad posible).

- **Potencia de transmisión:** igual que captar bien la señal, para algunos ataques también será importante poder enviar correctamente. La potencia se verá reducida por la velocidad de transmisión, por eso que los ataques se intenten realizar a velocidades bajas. Aunque la normativa Europea y española limitan la potencia a 100 mW, pueden encontrarse algunas tarjetas que soporten hasta 250 mW (24 dWm) o incluso más si se usan drivers de código abierto. Por lo tanto se escogerá tarjetas con límites superiores a los 20 dWm para asegurar que la inyección de tráfico se realiza correctamente.

- **Tipo de conexión con el PC:** existen varios tipos de conexiones posibles (PCI, PCMCIA, USB). En este caso la conexión no determina si se pueden o no realizar ataques, lo que sí que determinará será la portabilidad del dispositivo, con lo que en el caso de las PCI, los ataques deberán ser realizados en un mismo lugar y con un PC de sobremesa, mientras que con un dispositivo PCMCIA podrá realizarse en cualquier sitio mediante un portátil. Por lo tanto se necesitara disponer de una tarjeta portable para realizar nuestros ataques.

- **Conector antena:** es importante que la antena pueda ser remplazada para conseguir diferentes configuraciones que permitan optimizar nuestro sistema.
Se precisara una tarjeta con conector externo del tipo RP-SMA, MC-Card, Conector UFL o Mini PCI.

- **Antena:** la antena es uno de los puntos clave para realizar con éxito ataques.

Como se ha coment0ado, en según qué situaciones la señal que nos llegará habrá sido atenuada por diversos objetos. Además, no se debe de olvidar que la señal a 2'4 GHz en según qué materiales (como el acero) rebota, con lo que no sólo se tendrá un camino de llegada, sino múltiples o, lo que se conoce como multipath. Así pues, será recomendable utilizar antenas directivas, en vez de las omnidireccionales, las cuales nos proporcionarán una ganancia más alta y evitaran parte del multipath (aunque la mejor forma de evitar el multipath es usar diversidad, es decir, varias antenas para la recepción). Así pues, será bueno disponer de una antena yagi o parabólica para realizar ataques.

Para los casos de estudio se han elegido las tarjetas que pueden ver en la Tabla 4.5, las cuales cumplen con los requisitos antes expuestos.

Tabla 4.5 Tarjetas inalámbricas aptas para ataques

Marca	Modelo	Conexión con PC	Estándares *802.11* Compatibles	Chipset	Antena
Senao	NMP5354	PCI	a / b / g	Atheros	1 Externas
Intel	PRO Wireless 2200 b/g	MiniPCI	b / g	Intel Centrino	2 Interna
Cisco	802.11 a/b/g Cardbus	PCMCIA	a / b / g	Atheros	1 Interna

Fuente: Elaboración Propia

4.11.2 Software

Wifi Slax

WifiSlax es una distribución Linux basada en los LiveCD's6 Slackware (llamados Slax) y BackTrack, otro LiveCD dedicado a la auditoria de la seguridad informática llamado. El LiveCD proporciona la ventaja de poder ser ejecutado en la mayoría de PC's sin necesidad de modificar ningún elemento que esté instalado.

WifiSlax 3.0 será nuestra herramienta prima. Esta distribución ha sido modificada para reunir una gran variedad de herramientas para la auditoria en la seguridad informática, incluyendo la parte de redes inalámbricas.

Además, otro punto fuerte de WifiSlax es que incluye los drivers necesarios compilados e instalados para la inyección de paquetes para los adaptadores inalámbricos. Con esto evitamos la instalación de los drivers Madwifi o IPW2200 que requieren la recompilación del núcleo del sistema operativo Linux o kernel.

Suite Aircrack-ng

Aircrack-ng es una Suite, o conjunto de programas, desarrollados para la auditoria de redes inalámbricas. La Suite Aircrack en su versión 2.4 (conocida como Aircrack-ng) será la utilizada en este documento y está incluida en la compilación WifiSlax.

Aircrack-ng es la evolución de la suite Aircrack, que fue el primer software que implementó el ataque FMS para ser aplicado sobre ficheros de captura de paquetes. Más tarde también incluyó los ataques KoreK que mejoraron el tiempo de ejecución de
Aircrack.

La versión NG incluye otras mejoras sobre sus versiones anteriores, pero la más importante es que implementa también el ataque PTW que sólo necesita unos 80.000 IV's para descifrar la clave WEP.
Aircrack-ng también incluye otros programas que permite capturar e inyectar tráfico, entre otras funcionalidades. Se ha de destacar que Aircrack puede ser ejecutado tanto en Linux como en Windows, pero sus herramientas de captura e inyección necesitan las tarjetas y los drivers comentados en el apartado 2.11.1, que no siempre funcionan en Windows.

Los componentes de Aircrack-ng que se utilizaran de esta suite serán: airodump-ng. Esta herramienta permitirá la captura de paquetes tipo 802.11. Se pueden usar filtros para capturar

en un solo canal o de un solo punto de acceso. Tanto en Windows como en Linux necesitará usar el modo monitor para la captura y, por lo tanto, los drivers adecuados.

aircrack-ng

Ésta es la herramienta estrella del paquete ya que es la que se encargará de realizar el ataque FMS y KoreK tomando los IV's de un fichero de captura de tramas. El programa analiza el fichero y muestra por pantalla las diferentes redes y cifrados permitiéndonos seleccionar cómodamente la red a atacar. Además se podrá deshabilitar algunas de las mejoras introducidas por KoreK, dado que a veces no son efectivas.

aireplay-ng

Este programa nos permitirá crear, modificar e inyectar tramas inalámbricas. Tiene varios ataques pre configurados los cuales enviaran distintos tipos de trama. Una descripción somera de estos ataques se tiene a continuación:

- **Ataque 0:** Ataque de des autenticación de clientes mediante el envío de paquetes modificados para llevar al cliente a la confusión de que el AP le ha des autenticado.

- **Ataque 1:** Autenticación en un AP, que permite crear un usuario falso en el AP cuando no hay ninguno conectado. Este ataque a veces no es efectivo ya que algunos AP ya no guardan en la tabla ARP la MAC de los clientes autenticados pero no asociados y por lo tanto una pregunta ARP no será contestada por el AP.

- **Ataque 2:** Reinyección de paquetes interactiva, permitiendo elegir manualmente, mientras se capturan paquetes, los que se quieren inyectar.

- **Ataque 3:** Reinyección de paquetes ARP. Similar al ataque 2, pero en este caso los paquetes que se capturan para reinyectar serán del tipo ARP. Este ataque es el más efectivo para provocar que el AP genere paquetes que contengan nuevos IV's.

- **Ataque 4:** Ataque de Korek. Este ataque no nos proporciona IV's sino que nos da la posibilidad de descifrar el contenido de un paquete (o lo que es lo mismo, el Key Stream de cifrado). No todos los puntos de acceso son vulnerables a este ataque ya que este ataque necesita paquetes más cortos de 42 bytes y algunos AP rechazan paquetes menores a 60 bytes.

- **Ataque 5:** Ataque de fragmentación. Este ataque no proporciona la clave WEP, sino que nos proporciona 1500 bytes de los cuales se pueden extraer la función de PRGA (Pseud-Random Generation Algorithm), y por tanto parte del Key Stream de cifrado. Estos bytes nos servirán para generar paquetes válidos que pueden ser reinyectados para obtener IV's.

- **Ataque 6:** Este ataque realmente es un test del enlace. Comprueba mediante el envío de paquetes, la calidad del enlace y si sera capaces de inyectar.

airemon-ng

Es un script que nos servirá para gestionar las interfaces inalámbricas, permitiéndonos ponerlas en modo monitor. En el caso de las tarjetas con chipset Atheros, este script permite crear varias interfaces virtuales con una sola tarjeta.
airdecap-ng

Esta utilidad descifrará los ficheros de captura (.cap) usando la clave que nosotros le introduzcamos. Con esto se lograra ver en claro las capturas que se ha realizado.7

Wireshark

Wireshark es la nueva versión del analizador de protocolos Ethereal. Éste nos permitirá capturar y leer ficheros de captura de tramas. En este proyecto será usado como visualizador de capturas ya que ofrece una facilidad de uso y un conjunto de filtros muy útiles para el análisis.

4.11.3 Casos De Estudio

Con la descripción de estos casos de estudio se pretende mostrar la facilidad actual para acceder a una red ajena. También se quiere mostrar como la mayoría de operadores desprecian la seguridad de la red y como pueden llegar a diseñar sistemas que aún empeoran el nivel de seguridad.
Se podrá encontrar en formato .cap las capturas mostradas en los 4 distintos casos de estudio (puede utilizarse Wireshark para visualizarlas).

4.11.3.1 Acceso a Una Red Sin Seguridad

En este caso se considerara una red sin seguridad inalámbrica, es decir, abierta. Aún que parece un caso trivial, no se conocen los datos de configuración de la red IP, cosa que dificultará la intrusión. Aquí se muestra cómo conseguir estos parámetros.

Este caso es necesario tenerlo en cuenta ya que, para casos más elaborados (con seguridad), una vez que conozcamos la clave de la red inalámbrica, la siguiente barrera será la obtención de los parámetros de red. Además, aprovechamos este caso para mostrar las herramientas que en Windows también permitirán capturar tráfico y el su análisis, ya que la mayoría del software utilizado en los demás casos será bajo sistema operativo Linux.

I- Escenario
SSID: desconocido0
Seguridad: sin seguridad

Autenticación: sin autenticación
DHCP: desactivado
MAC AP: 00:16:C0:E7:10:C3
MAC Cliente: 00:60:B3:0E:A8:85
Hardware
PC: Sobremesa pentium IV,
Adaptador inalámbrico: Senao NMP5354
Chipset: Atheros
Software
OS: Windows
Sniffer: airodump 2.38
Drivers: drivers Wildpackets9 Atheros en Windows

II- Ejecución

Paso 1: Wardriving

Como en cualquiera de los ataques lo primero será realizar una exploración del área o wardriving para obtener los datos del escenario en el cual nos encontramos. Es importante conseguir mantener el nivel de señal recibida constante y al nivel más alto posible. Si el SSID está oculto se necesitaran otras herramientas y otro proceder el cual será explicado en el siguiente apartado.

Del wardriving con Netstumbler se obtiene:
SSID: Linksys
MAC AP: 00:16:C0:E7:10:C3
Canal de emisión: 11

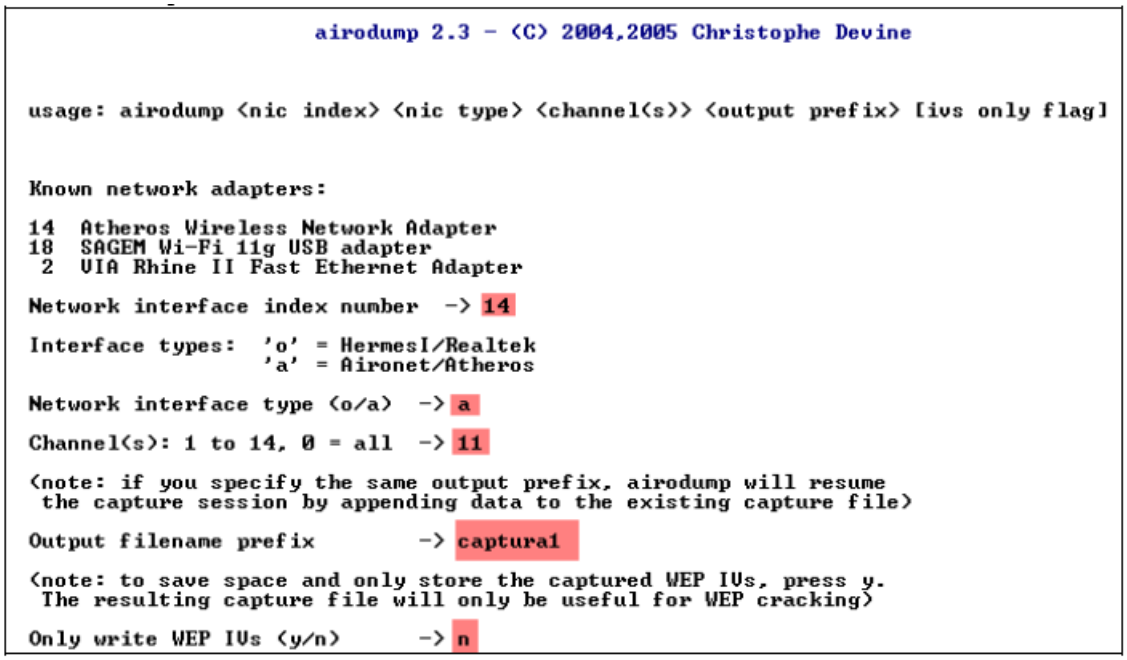
Con esta información sólo se podrá realizar la conexión con la red (la cual no tiene ningún tipo de autenticación y cifrado). Aún así, el acceso a cualquier servicio de la red aún no será posible, dado que el DHCP está desactivado y no se puede obtener la configuración de red.

Para obtener esta configuración de red se necesitara leer los paquetes transmitidos por algún cliente de la red.

Paso 2: Captura de tramas

Para capturar las tramas de un cliente inalámbrico se utilizara airodump. Se hará la configuración como muestra la Figura 4.24 (marcado en rojo) para que sólo capture los datos del AP que se está analizando.

Fig. 4.24 Configuración de airodump en Windows



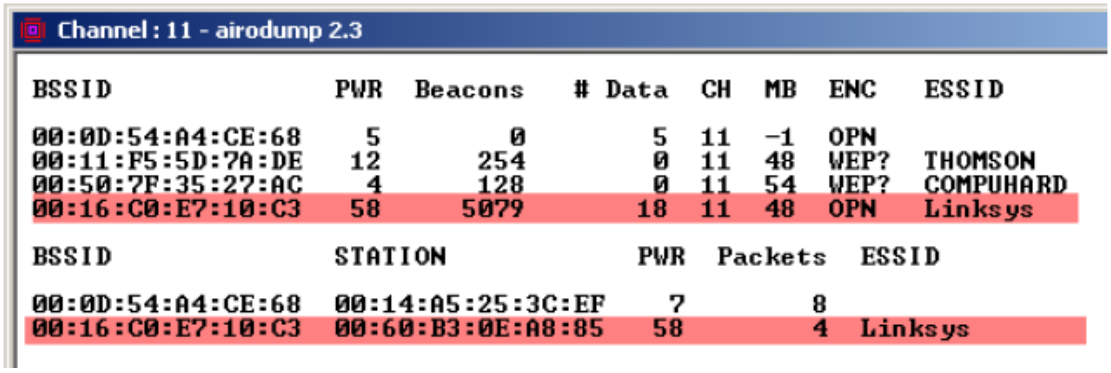
Fuente: Elaboración Propia

Es importante seleccionar como no la opción Only Write WEP IVs. Si no se hace así los datos almacenados sólo será una colección de IV's sin la cabecera ni el payload de los paquetes capturados, información que necesitamos.

En la Figura 2.25 se puede ver la captura de paquetes en Windows. La columna DATA indica las tramas capturadas con contenido en el nivel de red (nivel 3 de la capa OSI). Estas tramas

con información de red serán las que posiblemente contengan IP's. Durante la captura, airodump, también mostrará los clientes que tiene este AP (en el caso de la Figura 4.25 el cliente es 00:60:B3:0E:A8:85). Los datos almacenados serán guardados en un fichero para su posterior análisis.

Fig. 4.25 Ventana de captura de airodump en Windows



Fuente: Elaboración Propia

En las diferentes pruebas que se han realizado, se ha podido ver que airodump no siempre es fiable al cien por cien. La posibilidad de realizar una buena captura, depende de la velocidad de trasmisión que soporte la tarjeta que captura. Por ejemplo, en cuanto a los clientes se refiere, si estos transmiten a una velocidad a la cual nuestra tarjeta no puede trabajar, estos clientes no podrán ser detectados de manera correcta, ya que, aunque la cabecera del paquete, que corresponde a nivel enlace y nivel físico, se envía a velocidad fija (1 Mbps), la parte superior al nivel de enlace (en nuestro caso todo lo que hay LLC en la capa OSI) viajará a la velocidad negociada entre AP y dispositivo inalámbrico. Con lo cual, no será posible leer lo que hay en el interior de ese paquete si la velocidad de transmisión no es soportada.

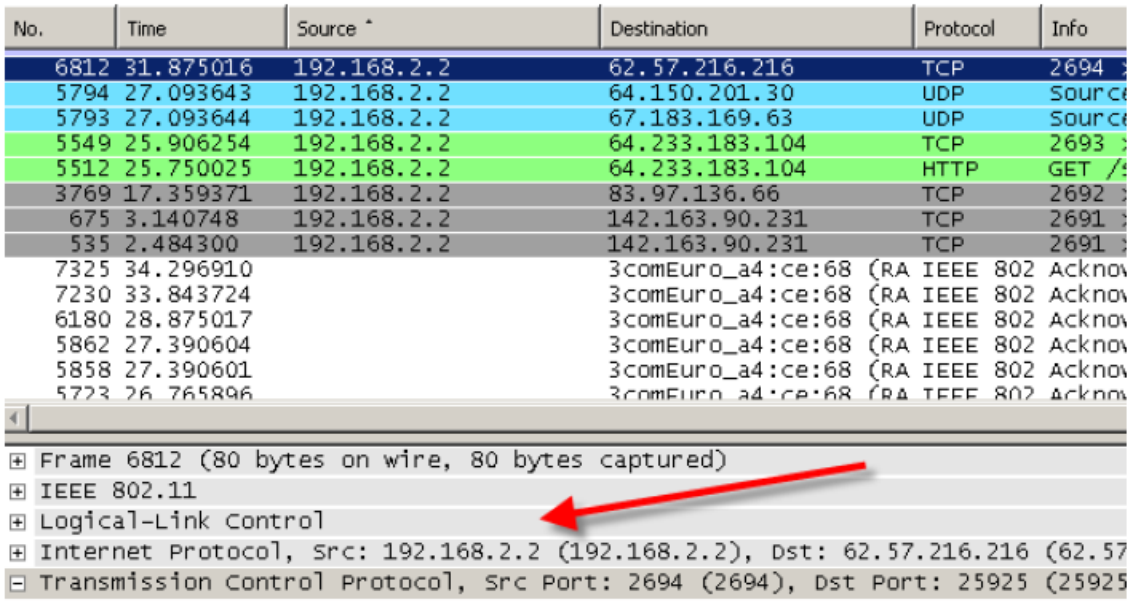
Paso 3: Análisis de datos de la captura

Para obtener las direcciones IP de la red, necesitamos obligatoriamente que esté conectado algún usuario y que transmita algún paquete IP. Esto es porque si no hay clientes conectados, las tramas enviadas sólo contendrán información básica (SSID, MAC, rates permitidos, potencia, etc.) ya que solo trabajarán hasta el nivel LLC. Para que haya información de niveles superiores al LLC (a nosotros nos interesa TCP/IP, por lo tanto nivel de red y de transporte) será necesario el cliente.

Una opción que evitaría realizar capturas y su posterior análisis sería probar las configuraciones que se consideren más probables. Un buen principio podría ser comprobar las configuraciones descritas en el apartado 2.7 de la PARTE II. Las configuraciones ahí descritas suelen ser las utilizadas en la mayoría de routers, con lo cual, si el router mantiene sus parámetros por defecto, seguramente este tendrá su IP original y nos permitirán configurar nuestra tarjeta para conseguir el acceso aun sin clientes ni capturas.

En la Figura 2.25 se pude ver que en la captura se dispone de un cliente (00:60:B3:0E:A8:85). Para extraer la información de las tramas enviadas por estos, se deberá abrir el archivo de capturas mediante Wireshark y filtrar la captura por la MAC del AP atacado, obteniendo lo mostrado en la Figura 4.26.

Fig. 4.26 Captura de Paquetes Filtrados



Fuente: Elaboración Propia [Wireshark]

En esta captura se puede ver que, una vez filtrados los paquetes, las direcciones IP se mueven dentro del rango 192.168.2.x. Se deduce por las demás direcciones de la captura que la máscara será 255.255.255.0.

4.11.3.2 Acceso a una Red con Seguridad Wep

La situación que frecuentemente se encuentra al analizar casos reales es el caso de las redes con seguridad WEP. Para realizar este ataque es fundamental que exista un cliente asociado al punto de acceso, ya que el punto de acceso sin clientes sólo transmitirá tramas beacon, las cuales no contienen ninguna información útil sobre la clave WEP.

En este caso, para aumentar la velocidad del ataque se realizara inyección de tráfico. Si no se realiza esta inyección el atacante debería esperar a que hubiese suficiente tráfico inalámbrico que le proporcionara la cantidad de IV's necesaria. Así pues, para conseguir tráfico en la red se deberá capturar un paquete ARP cifrado, ya que los paquetes ARP serán retransmitidos por el AP por todas sus interfaces. Además debe tener habilitado el flag ToDs (véase apartado

1.1.8 de la PARTE I), es decir, que se dirija desde la red inalámbrica hacia la cableada. Este paquete será manipulado para que incluya la dirección de broadcast (FF:FF:FF:FF:FF) y será reinyectado, provocando que el AP responda con otro paquete ARP el cual contendrá, cada vez, un nuevo IV. De esta manera se independizara el ataque de la cantidad de tráfico existente entre el AP y el cliente.

Las ventajas de utilizar el ataque con inyección no acaban ahí. Dado que la mayoría de paquetes capturados serán tramas ARP con diferentes IV, se podra utilizar el nuevo ataque PTW de Aircrack. Como vimos en el apartado 3.2.3 de la PARTE II, este ataque aprovecha que las tramas ARP siempre empiezan de la misma manera para incrementar la eficacia del ataque estadístico, rebajando la cantidad de IV's necesario para obtener la clave.

Así pues, siguiendo la Figura 2.23, este ataque comienza en el estado de captura de datos de usuario, para luego ser reinyectados. Seguidamente se realiza el snifado de las respuestas a nuestra reinyección, el ataque a WEP y el análisis de los parámetros de red.

Finalmente, también se introducirá la posibilidad de crear paquetes ARP por si no es posible conseguirlos de manera pasiva. Para ello se utilizara el ataque Chop-Chop o el ataque de fragmentación, los cuales consiguen hasta los primeros 1024 bytes del Key Stream (dependiendo del tamaño del paquete). Mediante este Key Stream se pueden crear paquetes ARP cifrados para ser inyectados.

I- Escenario

SSID: ROC
Seguridad: WEP 128 bits
Autenticación: sin autenticación
DHCP: habilitado
MAC AP: 00:11:E6:6D:A5:44
MAC Cliente: 00:02:6F:21:35:D7

Hardware

PC:	Sobremesa Pentium IV
Adaptador inalámbrico:	Senao
Chipset:	Atheros

Software

OS:	WifiSlax (Linux)
Sniffer:	airodump-ng
Descifrador de clave:	aircrack-ng
Inyección de trafico:	aireplay-ng
Creación de paquetes:	packetforge-ng
Cambio de MAC:	macchanger
Drivers:	madwifi

II- Ejecución

Paso 1: Wardriving

Se realizara wardriving para encontrar el punto de acceso y el cliente a atacar. En nuestro caso el AP a atacar tendrá como SSID el nombre de ROC y como MAC 00:11:E6:6D:A5:44, y la MAC del cliente será 00:02:6F:21:35:D7. El canal usado será el 2.

Paso 2: Captura de tráfico

Fijar airodump para que capture las tramas de este punto de acceso.

Airodump-ng –channel 2 –bssid 00:11:E6:6D:A5:44 –w captura – i aht1

Fig. 4.27 Captura de IV's



Fuente: Elaboración Propia

En la Figura 4.27 se puede observar el tráfico en la red. El campo Data nos indica los paquetes con IV's capturados. Este indicador se irá incrementando poco a poco dependiendo de la cantidad de tráfico con IV's entre el punto de acceso y el cliente.

Como en el caso anterior, se deberá configurar la tarjeta inalámbrica para que actúe como dos interfaces (el ataque se hará desde ath0 mientras que la captura de datos se hará desde ath1). Airodump deberá capturar tráfico en la interfaz ath0 hasta finalizar la inyección de tráfico.

Paso 3: Inyección de tráfico

Para que el campo Data incremente, se deberá realizar la inyección de paquetes ARP, suplantando al punto de acceso, y engañando al cliente para que genere respuestas ARP las cuales contendrán nuevos IVs.

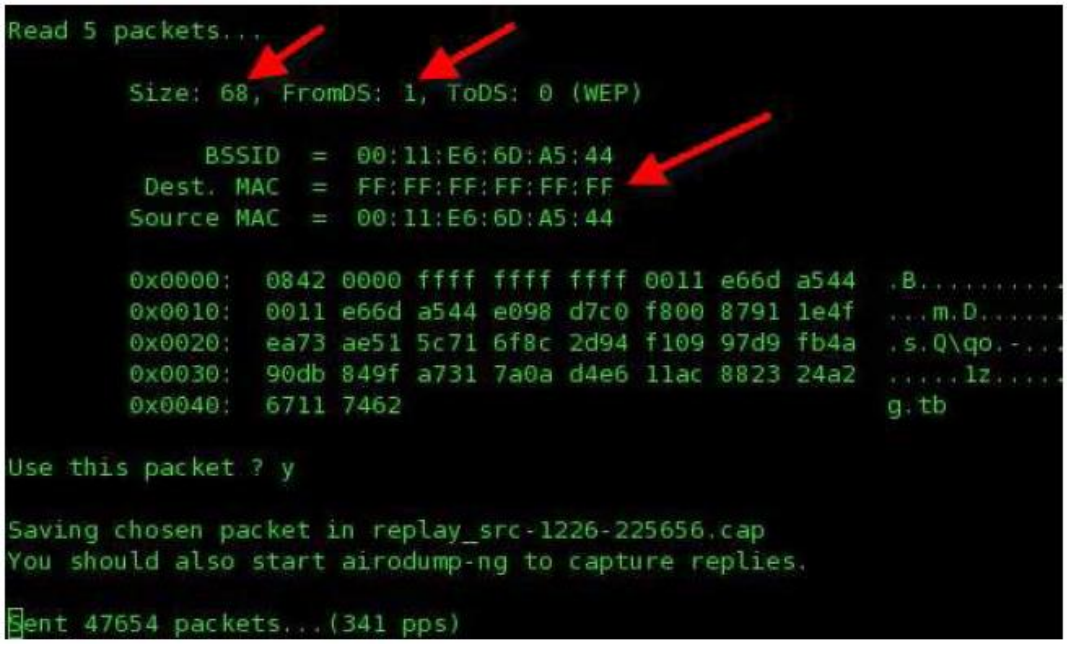
Para realizar este ataque se utilizara el ataque de inyección de tráfico o ataque 2 de aireplay. Este ataque capturará un paquete ARP y lo reenviará. El comando utilizado será el siguiente:

Aireplay-ng -2 –b 00:11:E6:6D:A5:44 –d FF:FF:FF:FF:FF –f 1 –m 68 –n86 ath0

Con este comando se indicara el tipo de ataque y los filtros para realizar la captura del paquete ARP. Los paquetes ARP se filtraran por la MAC del punto de acceso (00:11:E6:6D:A5:44) y por la MAC del destino (FF:FF:FF:FF:FF, broadcast para asegurarnos retransmisión). Se

Indicara que éste ha de ser un paquete que venga del sistema de distribución, es decir desde la parte Ethernet de la red (fromDS) hacia la red inalámbrica (sino no será contestado al reinyectarlo). También se fijara el tamaño mínimo y máximo del paquete a capturar (para el caso de los paquetes ARP suele estar entre 68 y 86, aunque preferiblemente se escogerá los de tamaño 68 bytes).

Fig. 4.28 Captura de paquetes ARP mediante aireplay



Fuente: Elaboración Propia

Como se puede ver en la Figura 4.28, aireplay irá capturando paquetes que concuerden con lo especificado en el filtro y lo mostrará para que se determine si se quiere usarlo para la inyección. Como el contenido del paquete estará cifrado sólo se conocerá su tamaño y se deberá realizar la prueba hasta encontrar un paquete ARP. Cuando se dé con el paquete correcto (en nuestro caso es el paquete que aparece en la Figura 2.28) y se lo inyecte, se verá en la ventana de airodump como el indicador Data se incrementa de manera rápida.

Fig. 4.29 Captura de tráfico después del re inyectado



Fuente: Elaboración Propia

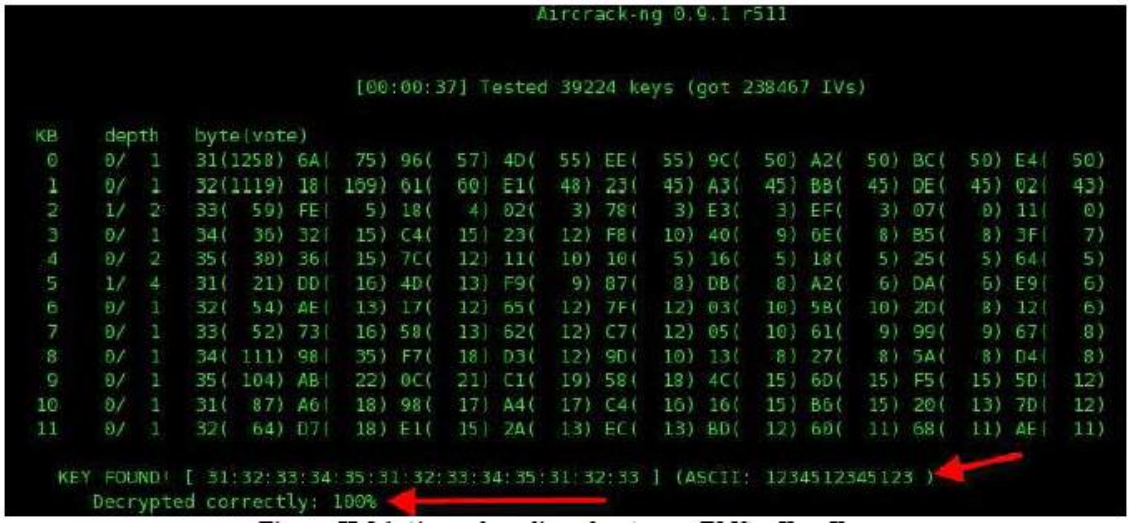
Como detalle, en la Figura 4.29, también se puede ver el incremento rápido en el indicador Packets, que serán las respuestas por parte del cliente a los paquetes falsos que se van inyectando. Recordar que el cliente ha de estar asociado durante el ataque, ya que si no los paquetes que se inyectan serán desechados.

Paso 4: Obtención de la clave con ataque FMS y KoreK

Para obtener la clave se deberá usar aircrack-ng sobre el fichero de captura. El comando será el siguiente:

Aircrack-ng captura.cap

Fig. 4.30 Aircrack realizando ataque FMS y KoreK



Fuente: Elaboración Propia

Se verá que aircrack muestra los diferente SSID's que ha encontrado en el fichero de captura, permitiendo seleccionar sobre cual realizar el ataque. Si sólo hay un SSID, éste será seleccionado automáticamente empezando el ataque seguidamente.

En la Figura 4.30 se ve que aircrack, al analizar el fichero de capturas, encuentra 238467 IV's los cuales serán sometidos a las pruebas estadísticas. Se probarán las claves hasta hallar la correcta o acabar con todas las posibilidades. En este caso la clave será encontrada al pasar 37 segundos habiendo probado 39224 claves diferentes.

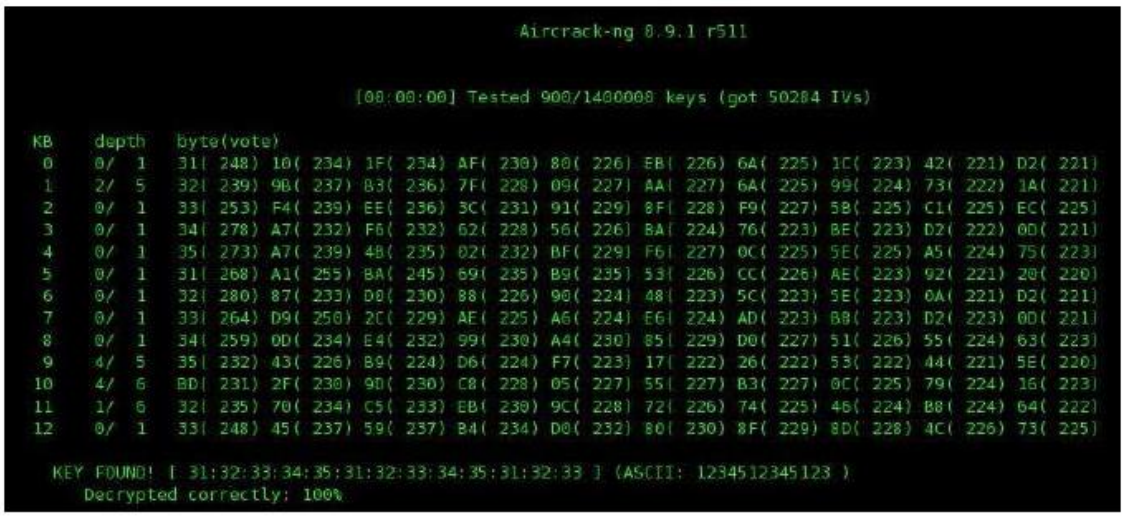
Puede verse que aircrack nos muestra la clave en formato hexadecimal y su traducción a formato ASCII.

Paso 5: Obtención de la clave con ataque PTW

Como se ha dicho, para acelerar este proceso se puede aplicar el ataque PTW ya que la mayoría de paquetes con IV son peticiones ARP (véase el apartado 2.9.2.3 de la PARTE II). Para realizar este ataque se usara el siguiente comando:

Aircrack-ng –z captura.cap

Fig. 2.31 Aircrack realizando ataque FMS y KoreK



Fuente: Elaboración Propia

En la Figura 4.31 se puede ver que en PTW se usa un proceso muy similar al anterior pero acortando el espacio de claves a 1.400.000 claves diferentes. En nuestro caso se evidencia que la clave, al ser sencilla y con caracteres comunes, es obtenida después de haber probado 900 claves.

Después de diversas pruebas realizadas pudimos obtener que eran necesarios sólo 50000 IV's diferentes del tipo ARP para que el ataque PTW funcionase correctamente.

Paso extra: Creación de paquetes ARP.

Es posible encontrar redes donde el tráfico de peticiones ARP sea nulo. En este caso será necesario conseguir un paquete cifrado de cualquier tipo para extraer el Key Stream. Con el Key Stream se podra generar un paquete ARP válido.
Para obtener los primeros bytes del Key Stream se puede realizar el ataque de fragmentación o el ataque Chop-Chop. En nuestro caso se ha usado el ataque Chop-Chop. Este ataque requiere que la tarjeta esté asociada al punto de acceso. Para ello, primero se usara una MAC falsa para

ocultar la identidad y luego se lo asociara (esto se lo puede hacer en cualquier otro ataque para evitar ser trazados mediante una MAC falsa).

El cambio de MAC se lo realizara mediante el macchanger con el comando:
Macchanger –m 00:11:22:33:44:55 ath0, como se muestra en la Fig.4.32.

Fig. 4.32 Cambio de MAC con macchanger



Fuente: Elaboración Propia

Luego se asocia esta MAC al punto de acceso mediante el ataque de autenticación falsa de aireplay con el siguiente comando:

Aireplay-ng -1 0 –e Roc –a 00:11:E6:6D:A5:44 –h 00:11:22:33:44:55 ath0

Seguidamente se realiza el ataque Chop-Chop, el cual capturará una trama cifrada cualquiera y lanzará el ataque mediante la MAC falsa, obteniendo así los primeros bytes del Key Stream. Cuanto más grande sea el paquete capturado más bytes del Key Stream se obtendra. Interesan obtener paquetes superiores a 86 bytes, que es la cantidad máxima de bytes que tienen los paquetes ARP. El comando a usar para el ataque Chop- Chop es el siguiente:

Aireplay-ng -4 –h 00:11:22:33:44:55 ath0

Este ataque proporcionara un fichero con extensión .xor, el cual contendrá el Key Stream.

Seguidamente se fabricara el nuevo paquete ARP, el cual ha de contener la MAC origen (ha de ser real), la MAC destino (ha de ser real), la MAC por la que la petición ARP pregunta, la IP origen y la IP destino. Para ello se usara el siguiente comando

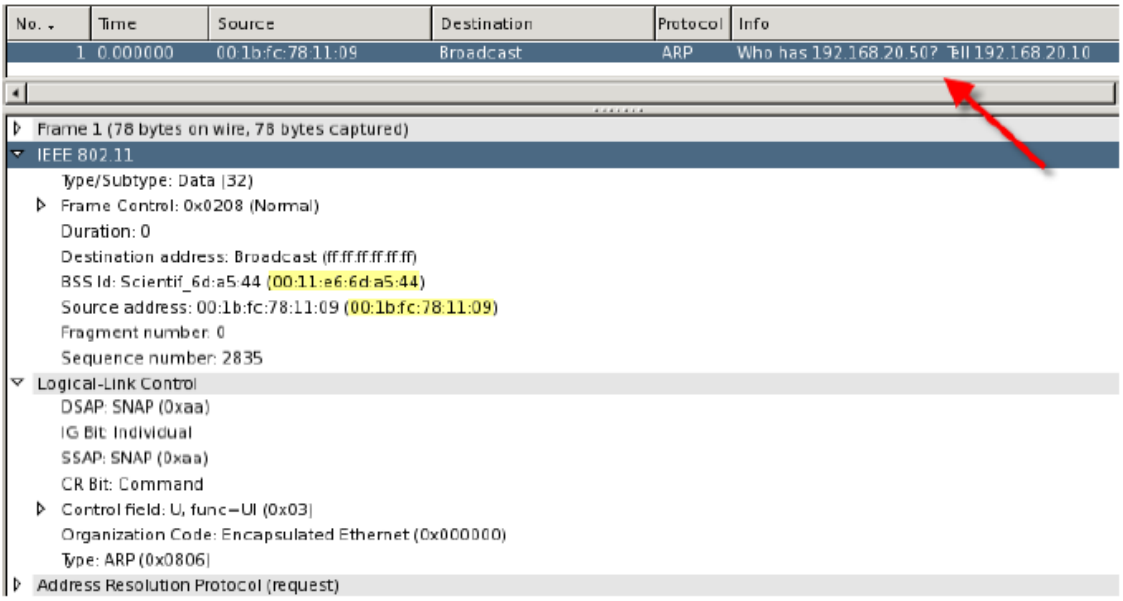
Packetforge-ng –arp –a 00:11:E6:6D:A5:44 –c 00:02:6F:21:35:D7

-h 00:04:AC:C5:37:C9 –j –o –l 192.168.20.50 – k 192.168.20.10
–y keystream.xor –w paquete.cap

En este caso se ha de usar las MAC's auténticas del cliente y del AP, con lo que en el momento de realizar el ataque el cliente real ha de estar asociado. Además necesitamos conocer las IP's del cliente y del destino, las cuales pueden ser obtenidas observando los paquetes capturados. Aún así es posible usar las IP's de broadcast (255.255.255.255) ya que algunos AP's transmitirán este tipo de petición y los clientes responderán a ellas.

Finalmente se establecen mediante –j y –o los flags que indican que el paquete viene del sistema de distribución hacia la red inalámbrica (FromDS 1, ToDS 0)

Fig. 4.33 Paquete creado mediante Wireshark



Fuente: Elaboración Propia

En la Figura 4.33 se puede ver el paquete creado antes de ser cifrado mediante el Key Stream. Este paquete será una petición ARP para que un determinado cliente responda mediante una respuesta ARP.
Finalmente se inyectara de la siguiente manera el paquete creado y se obtendrá el mismo resultado que en el procedimiento anterior al inyectar un paquete ARP original.

Aireplay-ng -2 –r paquete.cap ath0

Parte III

Antes del desarrollo de la aplicación se instaló el Sistema Operativo Linux Ubuntu como se muestra en el Anexo 1.

4.12 Desarrollo De La Aplicación (Script Shell Linux)

EL programa que tiene la finalidad de detectar equipos desconocidos en una determinada WLAN ha sido desarrollado en Shell Script de Linux partiendo de un algoritmo para detección de intrusos (Ver Anexo 2). Este programa a través de Bash es interpretado en línea de comandos Unix.
La implementación del Script se sitúa en el Anexo3.

4.12.1 Configuración Del Daemon

Un proceso (Configurado para actuar en un intervalo de tiempo) es implementado para que el programa envíe notificaciones al panel del mismo Sistema Operativo y visualizar una alerta de intrusión como se detalla en el Anexo 4.

4.12.2 Escenario De Ejecución Del Programa

Se implementa la detección de un equipo que está comprendido fuera del segmento de la red conocida.

El Demon configurado para ejecutar el programa de detección de intrusos WIFI en un intervalo de tres minutos en caso de verificar la presencia de un equipo ajeno a la WLAN visualizará este a través del panel de notificaciones del S.O. como se muestra en la Fig. 2.42.

4.12.3 Elementos

- **Access Point TP-LINK**
  Firmware Versiòn: 3.11.1 Build 100312 Rel 42991n
  Hardwae Versión: WR471N v1

- **Laptop HP con S.O. Linux Ubuntu versión 10.04** (Equipo Detector de Intrusos Wifi implementado en Máquina Virtual)

  Interfaz de Red: 802.11g Broadcom

- **Laptop DELL con S.O. Windows 7** (Equipo desconocido a ser detectado)
  Interfaz de Red WLAN 1397 DELL

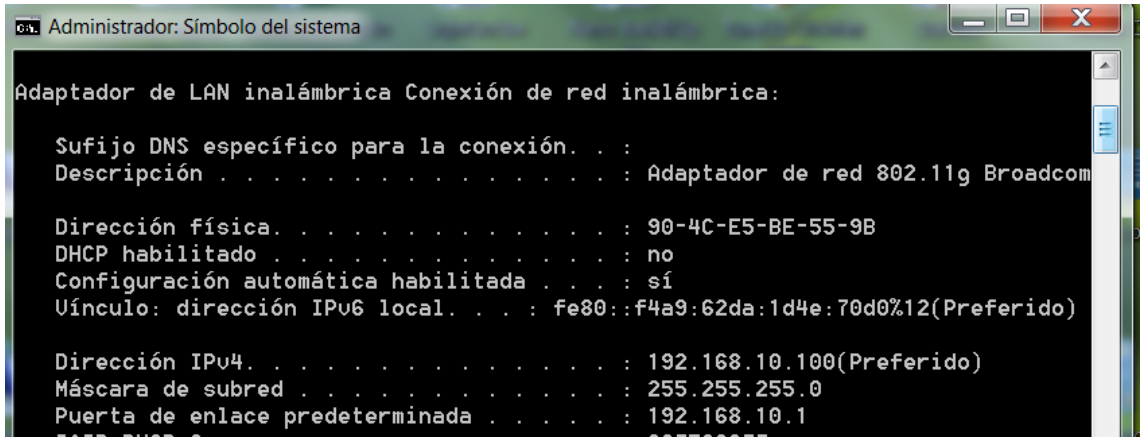
4.12.4 Configuración De Red Del So Linux UBUNTU (Equipo portador de la Aplicación)

- **Direccionamiento Lógico** (Estático)

Segmento de Direccionamiento IP: 192.168.10.0 /24
Puerta de Enlace: 192.168.10.1

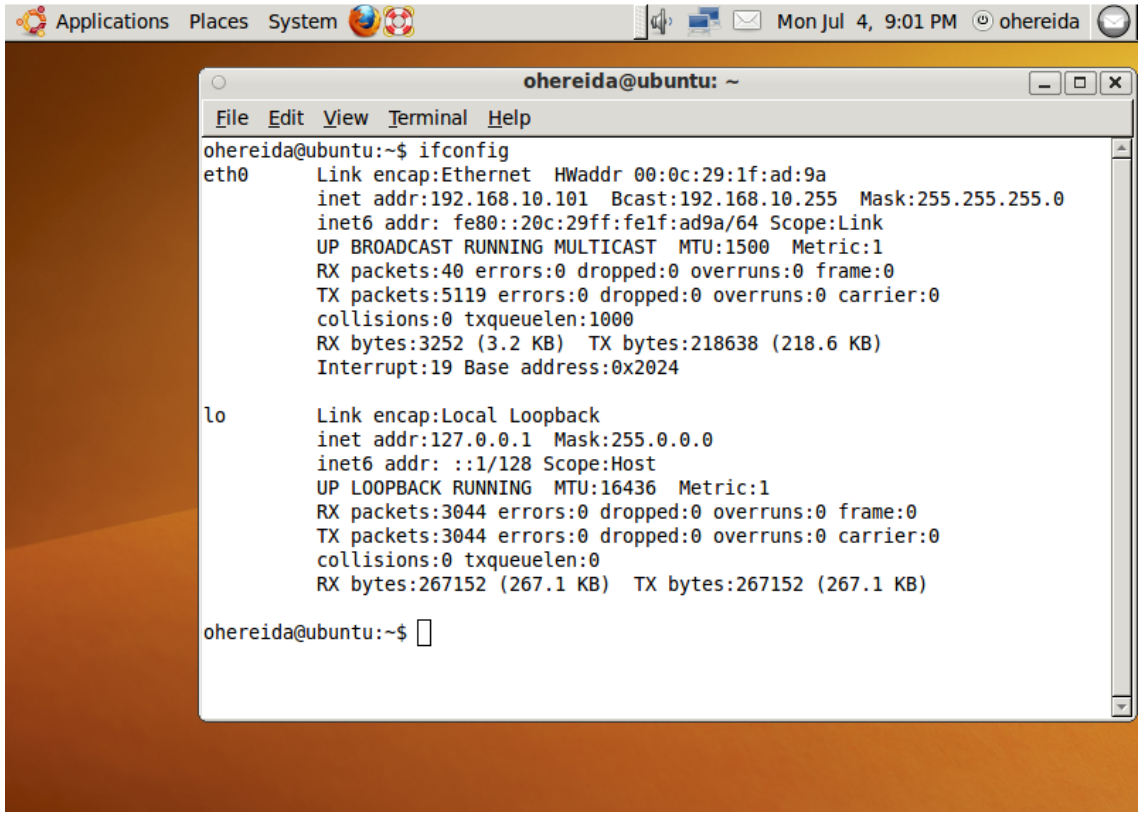
- **Direccionamiento Físico**
  WHAddr: 00:0c:29:1f:ad:9ª

Fig. 4.34 Direccionamiento Lógico y Físico



Fuente: Elaboración Propia

Fig. 4.35 Configuración del SO Ubuntu en VMWare



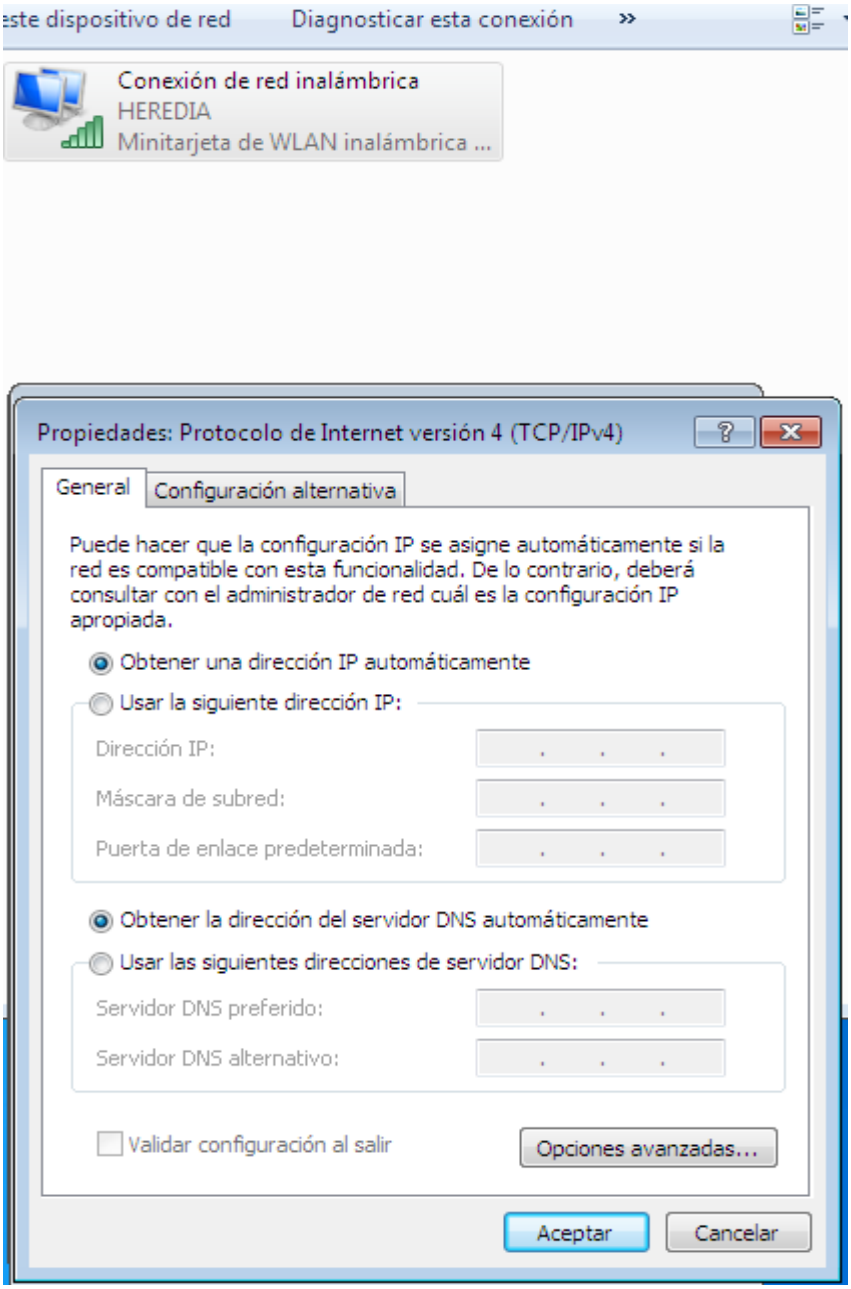
Fuente: Elaboración Propia

4.12.5 Configuración de Red del Equipo Cliente con S.O. Windows 7 (Equipo Desconocido)

- Direccionamiento Lógico (Dinámico)

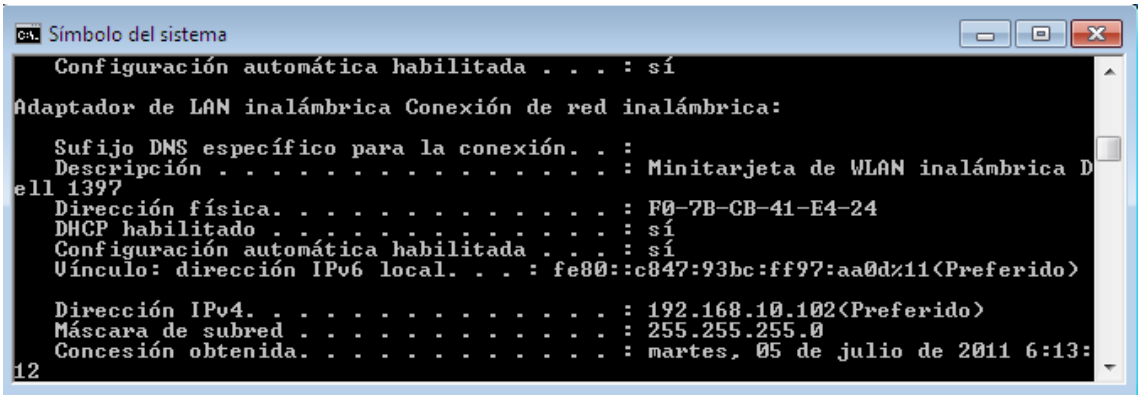
- Direccionamiento Físico: f0:7b:cb:41:e4:24

Fig. 4.36 Configuración de la Red Equipo Desconocido



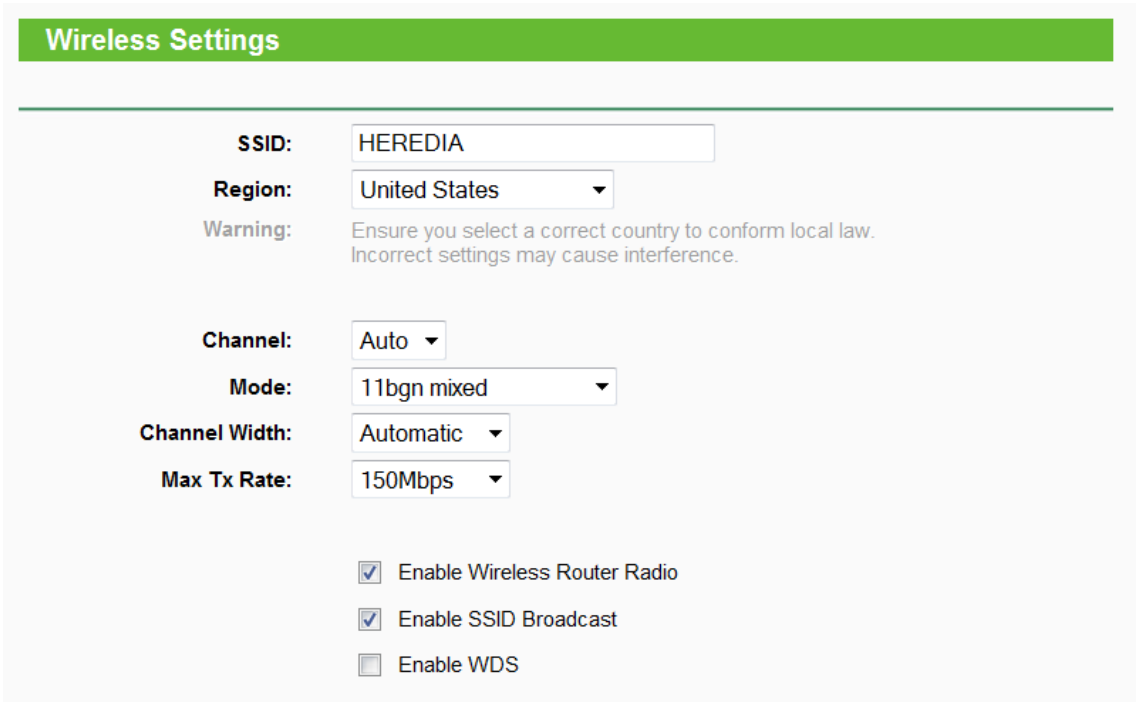
Fuente: Elaboración Propia

Fig. 4.37 Visualización del equipo desconocido por consola



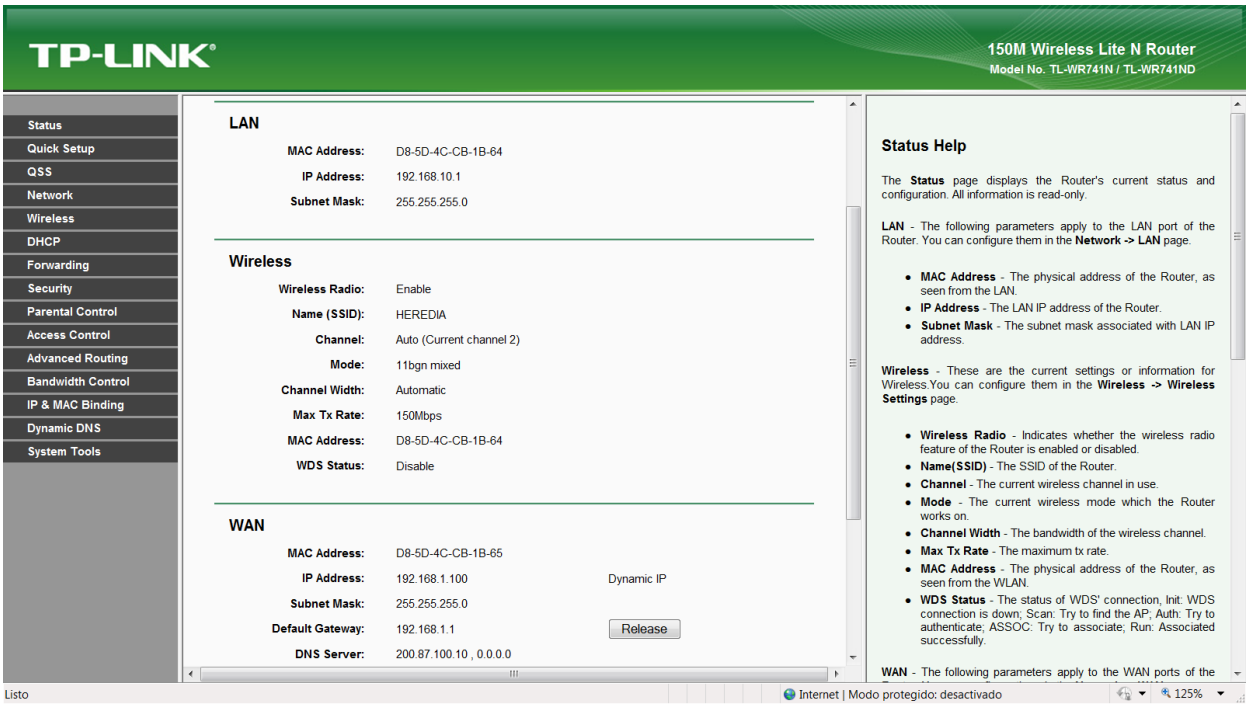
Fuente: Elaboración Propia

Fig. 4.38 Configuración del AP



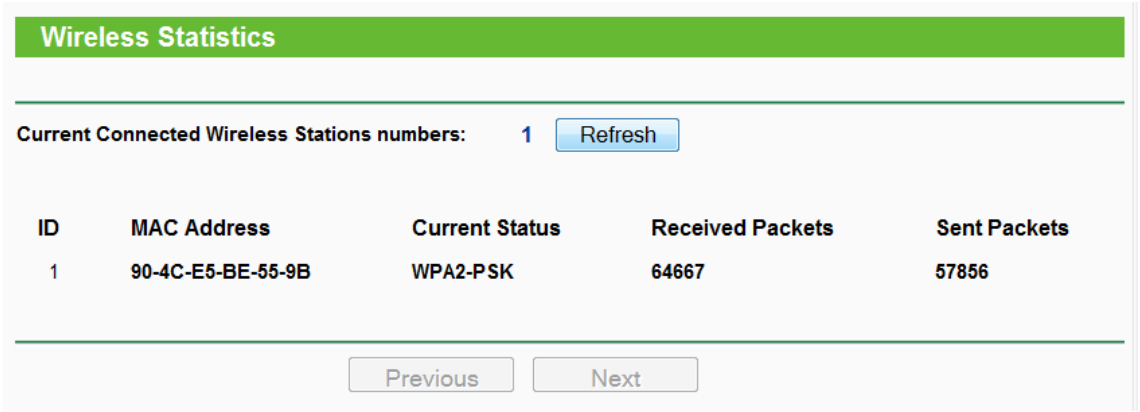
Fuente: Elaboración Propia

Fig. 4.39 Visualización de la pantalla principal del AP



Fuente: Elaboración Propia

Fig. 4.40 Estado Inicial y equipos conectados en AP



Fuente: Elaboración Propia

Inicialmente solo se tiene Conectado un equipo, que es el Computador portador de la Aplicación. Se puede evidenciar la MAC del equipo contendor del detector de intrusos wifi.

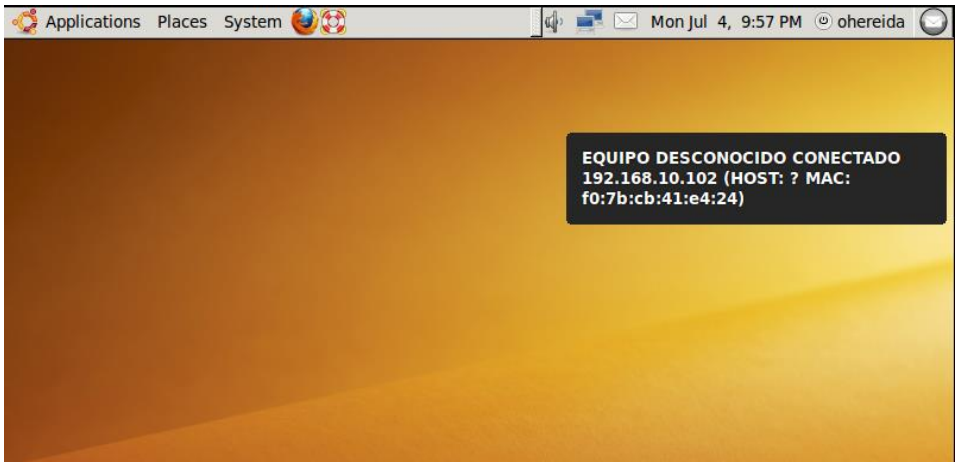
Fig. 4.41 Acceso del Equipo Desconocido



Fuente: Elaboración Propia

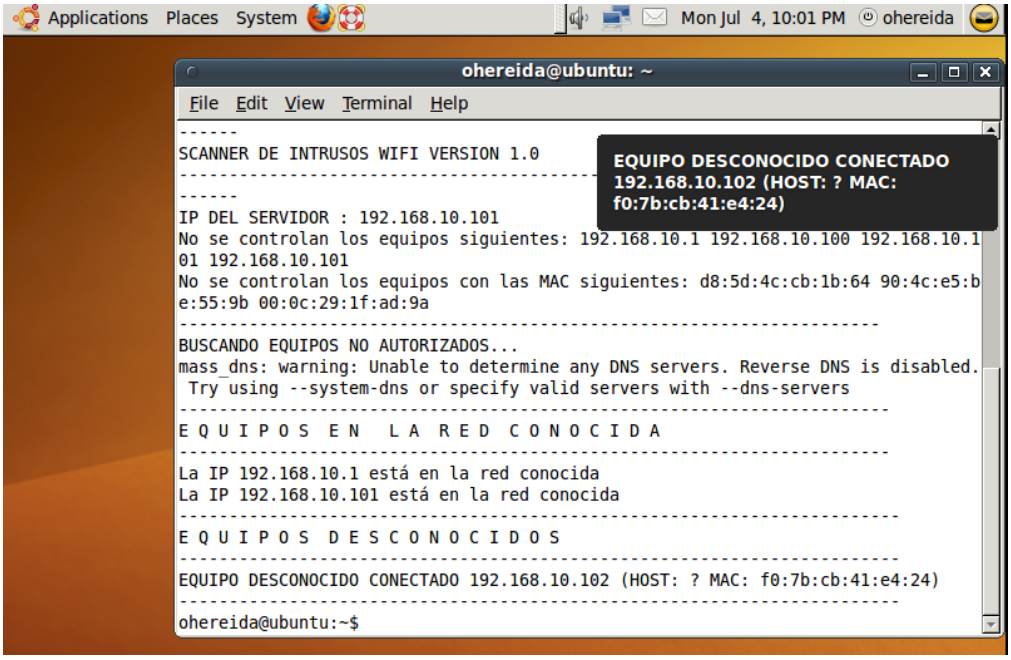
Acción del programa Detector: Scanner__Wifi (Daemon configurado envía mensaje de intrusión al panel de notificaciones de Ubuntu)

Fig. 4.42 Mensaje de Intrusión al panel de notificaciones de Ubuntu



Fuente: Elaboración Propia

Fig. 4.43 Acción del Programa por consola Unix:

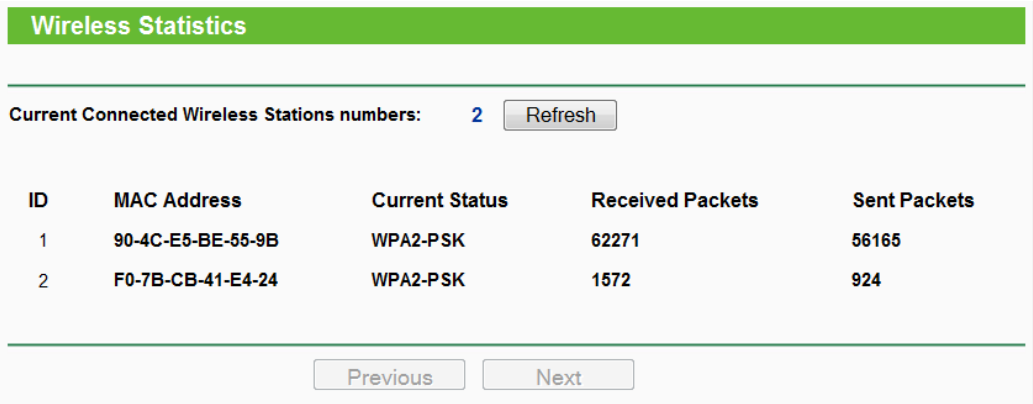


Fuente: Elaboración Propia

El equipo desconocido que recientemente se conectó se ha detectado a través del programa: scanner__wifi, el mismo esta programado su ejecución en un intervalo de tres minutos.

Este hecho es afirmado si se accede al AP y se verifica en Wireless Statistics :

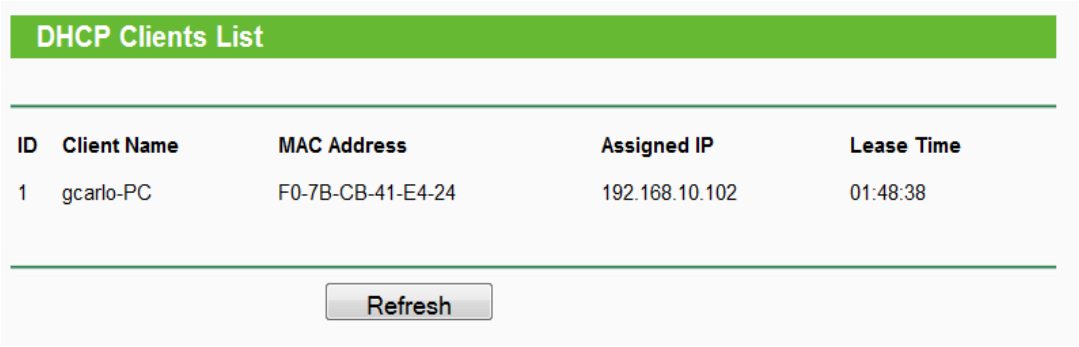
Fig. 4.44 Verificación del equipo Desconocido



Fuente: Elaboración Propia

A través de DHCP Client List, se logra constatar que el Servidor DHCP del AP asignó una dirección IP a un equipo con las características de direccionamiento que el programa scanner__wifi visualizó y categorizó como equipo desconocido.

Fig. 4.45 Asignación de una dirección IP a un equipo desconocido



Fuente: Elaboración Propia

La MAC que muestra conectada en la lista en la figura, es la dirección física del equipo desconocido que se conectó recientemente.

CONCLUSIONES

Al término de este trabajo de investigación se puede llegar a las siguientes conclusiones:

- Se ha realizado el estudio referente a las redes inalámbricas, limitándonos a las redes de alcance local WLAN, propiamente el estándar 802.11 y a la vulnerabilidad que estos presentan, de manera particular se ha hecho el estudio de los protocolos WEP y WEPA implementados en los Acces Point.

- Se ha hecho un análisis del comportamiento que poseen los adaptadores inalámbricos PCI y USB de las marcas más conocidas en el mercado local, de los mismos se concluyó que no todo chip inalámbrico soporta el modo monitor, configuración imprescindible que un adaptador debe poseer para realizar captura e inyección de paquetes wifi. El modo monitor es un requisito para obtener una clave WEP o WPA por métodos de intrusión.

- El proceso de obtención de clave wifi de un AP no siempre será exitoso, esto debido a que el tráfico de red de un AP es variante conforme a los clientes que éste tenga conectados. Mientras mas tráfico genere el AP mayor será la posibilidad de obtención de una clave wifi. Y el tiempo de obtención de una clave wifi por métodos de intrusión también es variante, esto de acuerdo a la cantidad de paquetes que se logre capturar con la herramienta sniffer.

- Se ha desarrollado un programa de control de intrusos wifi en Shell Script de Linux, más propiamente en S.O. Ubuntu versión 10.04. Este programa realiza la detección de equipos no comprendidos en la red local conocida y da información del equipo desconocido. Los parámetros de información son: dirección IP y Dirección MAC. Dependiendo a la versión del SO intruso se podrá o no obtener también el nombre del HOST.

- Para la ejecución de la aplicación se ha implementado un Demon (Demonio) como tarea parte del S.O. para que este se ejecute consecutivamente cada determinado tiempo.

- El programa desarrollado es escalable en cuanto a la cantidad de intrusos que puede detectar.

- La existencia de equipos intrusos en una red wifi, pueden ser no visibles dependiendo de la versión de Firewall que estos poseen, pero su presencia no autorizada podrá ser determinada por el programa desarrollado.

- Se plantea una estructura de red para evitar intrusiones o ataques que hacen uso de programas sniffer.

RECOMENDACIONES

Las recomendaciones que se pueden dar a la culminación de este trabajo de investigación son las siguientes:

- En futuros trabajos de investigación relacionados al presente área se recomienda ampliar el tema de los Métodos de encriptación mencionados en la actual investigación.

- Una infraestructura corporativa de WLAN hoy en dia deberá necesariamente implementar un sistema de autenticación de usuarios como el planteado en la presente investigación.

- Por considerarse la captura de paquetes en nivel de Enlace de Datos es importante comprender que las unidades o PDU que generan tráfico son tramas propiamente y no así paquetes IP.

- El flujo de datos que genera un AP es vigente hasta el segundo nivel del modelo de referencia OSI y siempre que se haga referencia a transmisión inalámbrica en las WLAN debe ser contemplado con las características que poseen estas dos capas únicamente.

- Por las debilidades que poseen algunos protocolos de seguridad y que se han dado a conocer en el presente trabajo, se recomienda configurar los dispositivos con niveles de seguridad actuales.

- Se recomienda diferenciar los adaptadores inalámbricos USB y PCI, aún estos sean idénticos en seria, aspecto muy importante a tiempo de elegir cierta serie de adaptador para captura de paquetes wifi.

REFERENCIAS BIBLIOGRÁFICAS

[Wikipedia, 2011]

Wikipedia, Wiki. – 2011. Redes de Computadoras.

http://es.wikipedia.org/wiki/Red_de_computadoras

Esta página fue modificada por última vez el 2 abr. 2011, a las 18:56. pag.1

Wikipedia, Wiki. – 2011. Cliente Servidor.

http://es.wikipedia.org/wiki/Red_de_computadoras/Cliente Servidor

Esta página fue modificada por última vez el 15 abr. 2011, a las 15:25. pág. 1

Wikipedia, Wiki. – 2011. Peer-To-Peer.

http://es.wikipedia.org/wiki/Red_de_computadoras/Peer-To-Peer

Esta página fue modificada por última vez el 13 abr. 2011, a las 16:10 pág. 1

Wikipedia, Wiki. – 2011. Redes por Radio

http://es.wikipedia.org/wiki/Red_por_radio

Wikipedia, Wiki. – 2011. Redes por Infrarrojos

http://es.wikipedia.org/wiki/Red_por_infrarrojos

Wikipedia, Wiki. – 2011. Rede por Microondas

http://es.wikipedia.org/wiki/Red_por_microondas

Wikipedia, Wiki. – 2011. Espectro Electromagnético.

http://es.wikipedia.org/wiki/Espectro_electromagn%C3%A9tico

29 mar 2011, a las 04:29. Pág. 1

Wikipedia, Wiki. – 2011. GNU/Linux

http://es.wikipedia.org/wiki/GNU/Linux

Esta página fue modificada por última vez el 4 abr 2011, a las 10:59. Pag. 1

Wikipedia, Wiki. – 2011. Ubuntu (sistema operativo)
http://en.wikipedia.org/wiki/Ubuntu_(operating_system)

This page was last modified on 26 April 2011 at 20:40

Wikipedia, Wiki. – 2011. IEEE 802.11

http://es.wikipedia.org/wiki/IEEE_802.11

Esta página fue modificada por última vez el 2 mar 2011, a las 21:48.

Wikipedia, De Wikipedia, la enciclopedia libre. Modelo OSI

http://es.wikipedia.org/wiki/Modelo_OSI#Capa_de_transporte

Esta página fue modificada por última vez el 27 jun 2011, a las 19:30.

Wikipedia, De Wikipedia, la enciclopedia libre. Shell de UNIX

http://es.wikipedia.org/wiki/Shell_de_Unix

Esta página fue modificada por última vez el 20 may 2011, a las 05:39.

Wikipedia, De Wikipedia, la enciclopedia libre. Diagrama de Flujo

http://es.wikipedia.org/wiki/Diagrama_de_flujo

Esta página fue modificada por última vez el 14 jun 2011, a las 06:50.

[Monografias, 2010].

Monografías, 2010. Redes de Computadoras

Monografias.com

Lunes, 29 de Noviembre de 2010 a las 13:46. © Monografias.com S.A. 2010.pag 1-1

[Aprende, 2009]

Aprende, Facil - 2009. 2011 The House of Blogs. Clasificación de las Redes
http://www.thehouseofblogs.com/articulo/clasificaci%C3%B3n_de_redes-475.html
Miecoles, 2 de Septiembre de 2009. pag. 1

[Tanenbaum, 1999]

Tanenbaum, Andrew S. - 1999 Redes de Computadoras, 3a. Ed. Prentice Hall Hispanoamericana, S.A., México, 1999. pag.8,12,13,82,97,98,100,

[Monografias, 2011]

Monografías, - 2011. Clasificación de las Redes

http://www.monografias.com/trabajos15/redes-clasif/redes-clasif.shtml

Miercoles, 2 de Marzo de 2011 a las 16:08 © Monografias.com S.A. 2011. pag. 1

[Hayden, 1999]

Hayden, Matt. – 1999. Aprendiendo Redes en 24 Horas 1ª Ed., Ed. Prentice Hall Hispanoamericana, S.A., México, 1999. pag. 7,8,9,11

[Paz, 2009]
Paz,Ariel e Silva – 2009. Topología de Red
http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml
Jueves, 22 de Octubre de 2009 a las 15:24. © Monografias.com S.A. partes 1, 2

[Martínez, 2007]
Martínez, Evelio – 2007. Topologías de Red
http://www.eveliux.com/mx/topologias-de-red.php
Sábado 21 de Julio de 2007 00:08. © 2011 eveliux.com

[Martínez, 2002]
Martínez, Evelio Martínez – 2002. Tipos de Antena
Publicado en la Revista RED en la edición especial
"El ABC de las Telecomunicaciones", Diciembre del 2002
http://www.eveliux.com/index.php?option=content&task=view&id=21
Tambien disponible en:
http://www.ensenadamexico.net/hector/it/reporte_antenas.php

[Bustillos, 2007]

Bustillos, Alí Alberto Safe. Las Redes
http://www.monografias.com/trabajos15/redes-clasif/redes-clasif.shtml
© Monografias.com S.A. pag. 1

[Bricopage, 2003]
Bricopage. Redes Informáticas
Bricopage e iniciada en Marzo de 2003. Copyright (c) 2003 Bricopage.com. Pag. 1

[Ciberhábitat, 2011]

Ciberhábitat, Museo. Ciudad de la Informática. Fundamentos de Redes

http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/fundamentos/04.htm . Pag.1

[Jimmyok, 2009]
Jimmyok - 2009. Por la Relación Funcional
http://jimmystalin.blogspot.com/2009/07/por-la-relacion-funcional.html
Publicado el 6 de Julio de 2009 a hrs. 07:53 pag.1
[Aguirre, 2007]

Aguirre, José Eduardo – 2007. Redes Inalámbricas

http://www.slideshare.net/alandk/topologias-inalambricas-presentation

Martes, 20 de Febrero de 2007 a las 18:09. Pag 1

[mweb, 2007]

mweb, maestrosdelweb - 2007**.** Configuración de una red inalámbrica en 13 pasos
http://www.maestrosdelweb.com/principiantes/configurar-una-red-inalambrica-en-13-pasos/
- Publicado el 10 de Mayo, 2007 – pag.1

[Barba, 2010]

Barba, Sandra Elena Jiménez – 2010. Redes Inalámbrica.

http://redesinalambricas.galeon.com/topologia.htm

Universidad de Guadalajara - Centro Universitario de Ciencias Exactas e Ingeniería - División de Computación - Teoría de la Computación. Galeon – Hispa Vista, pag.1

[CBTIS, 2004]

CBTIS, Centro de Bachillerato Tecnológico Industrial y de Servicios no. 103 cd. Madero, Tamaulipas. "Redes Inalámbrica", a 11 de marzo del 2004.

[maestrow, 2004].

maestrow, maestrosdelweb - 2004. Redes Inalámbricas

Publicado el 5 de Julio, 2004.

[Wikipedia, 2010]

Wikipedia, Wikipedia la enciclopedia libre.mht. Wi-Fi

http://es.wikipedia.org/wiki/wi-fi

Esta página fue modificada por última vez el 15:03, 17 ene 2010.

[Share, 2011]

Share, Slide – 2011.TopologíasInalámbricas

http://www.slideshare.net/alandk/topologias-inalambricas-presentation

© 2011 SlideShare Inc. All rights reserved. Pag 1

[Lectores, 2011]

Lectores, Servicio de Atención. Wireless - RedesInalámbricas

http://www.redsinfronteras.org/pdf/redes_wireless.pdf

lectores@mpediciones.com. Pag 20

[Jeff, 2008]

Jeff, Kioskea – 2008. Redes inalámbricas – Sistemas Operativos

http://es.kioskea.net/contents/wireless/wlintro.php3

jueves, 16 de octubre de 2008, 15:43:35. es.kioskea.netpag. 1

[Spam, 2008]

Spam, Loco SpamLoco. **AntenaWiFicasera**
http://spamloco.net/2008/03/antena-wifi-casera.html

16 marzo, 2008. SpamLoco 2006 - 2011

http://www.ensenadamexico.net/hector/it/reporte_antenas.php

[Masadelante, 2011]
Masadelante, Diseño Web España. Sistema operativo
http://www.masadelante.com/faqs/sistema-operativo
Copyright 1999 - 2011 Masadelante.com pag.1

[**Funes**, 2000]
Funes, Alejandro – 2000. Sistema operativo
http://www.euram.com.ni/pverdes/verdes_informatica/informatica_al_dia/que_es_un_so_144.htm
Copyright © 2000. Derechos Reservados **Euroamericana S,A**. pag. 1

[Ciberaula,2010]
Ciberaula, online – 2010. ¿Qué es Linux?
http://linux.ciberaula.com/articulo/que_es_linux/
© 2010 - Todos los derechos reservados Ciberaula. Pag.1

[Dell, 2011]
Dell, Diseño Web - 2011. Ubuntu
http://www.dell.com/content/topics/segtopic.aspx/ubuntu?c=us&l=en&cs=19

pag.1

[Ordenadores, 2011]
Ordenaores ,Portatiles – 2011. Punto de Acceso
http://www.ordenadores-y-portatiles.com/punto-de-acceso.html

Ordenadores-y- portátiles.com Pag.1

[Puigdemunti, 1999]

Puigdemunti, EduardGelabert&Harlam José Alvarado Sediles - © 1999. El Modelo OSI. Usuario online

http://www.pchardware.org/redes/redes_osi.php

[**Jonathan, 2004]**

Jonathan, 2004. Que son las Redes? – Capítulo 5 El modelo OSI

mail x mail.com (Cursos para compartir lo que sabes)

http://www.mailxmail.com/curso-que-son-redes/modelo-osi

Fecha publicación: 25/11/2004. Pag. 1

[**Gonzales, 2011]**

Gonzales, Sergio Duran – 2011. Shell Scripts en Linux

LinuxTotal.com.mx · Información y servicios en Linux y Open Source · info@linuxtotal.com.mx sergio.gonzalez.duran@gmail.com

http://www.linuxtotal.com.mx/index.php?cont=info_shell

[Becerra, 2011]

Becerra, Leonardo – 2011. Flujograma

© Monografias.com S.A.
http://www.monografias.com/trabajos14/flujograma/flujograma.shtml

[CCNA, 2011]

CCNA, CCNA CISCO – 2011. Redes

Curso de Certificación CCNA CISCO.

[Cisco, 2007]

Cisco,NationwideValueComputer- 2007. Routers

http://www.nvcsales.com/cisco/newcisco.asp?gclid=CN_Ct42X6KkCFcV_5QodmzAxYw

BIBLIOGRAFÍA

Tanenbaum, Andrew 5. (1997), Redes de Computadoras, Modelos de Referencia tercera edición, 1997, Prentice may Hispanoamericana S.A.

http://www.maestrosdelweb.com/editorial/redeswlan/

http://es.wikipedia.org/wiki/Red_de_ordenadores

http://www.alegsa.com.ar/Dic/sistema%20de%20deteccion%20de%20intrusos.php

http://www.maestrosdelweb.com/principiantes/configurar-una-red-inalambrica-en-13-pasos/

http://es.wikipedia.org/wiki/Eavesdropping

http://imstrangeandilikeit.blogspot.com/2007/12/mac-spoofing.html

http://www.javamexico.org/blogs/ezamudio/ejemplo_de_ataque_de_negacion_de_servicio

http://es.wikipedia.org/wiki/Red_de_ordenadores

http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

http://es.wikipedia.org/wiki/Hacker

http://es.wikipedia.org/wiki/Script_Kiddies

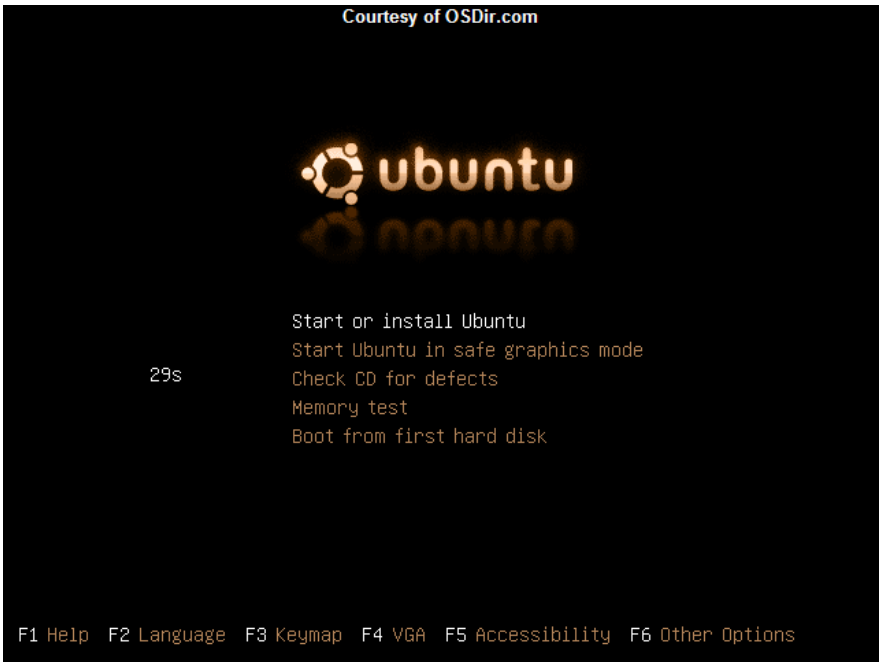
http://es.wikipedia.org/wiki/Cracker

ANEXO 1

INSTALACIÓN DE UBUNTU

Iniciar desde CD

Menú de inicio donde “startorinstall Ubuntu” está iluminado por defecto. Antes de empezar, presionar **F2** y escoger el **idioma** con el que se quiere iniciar ubuntu. Tras escoger idioma, presionar enter para seleccionar la opción de "iniciar o instalar Ubuntu".



La primera pantalla es la de selección de idioma, en la cual se puede escoger el idioma por defecto en la instalación. Cuando se haya seleccionado, hacer click en el botón “Adelante”



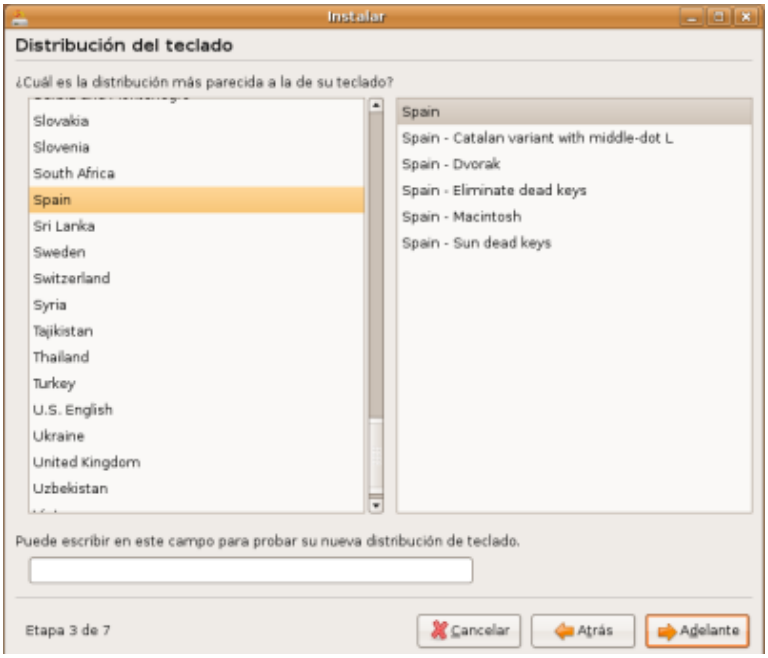
Zona horaria

Haciendo click en el mapa seleccionar más fácilmente la localización.. Cuando la hora sea correcta, haz clic en “Adelante”.



Distribución de Teclado

Selecciona tu distribución de teclado, escribir algo en la caja de texto de abajo para comprobar que funciona correctamente si se no está seguro de la distribución.



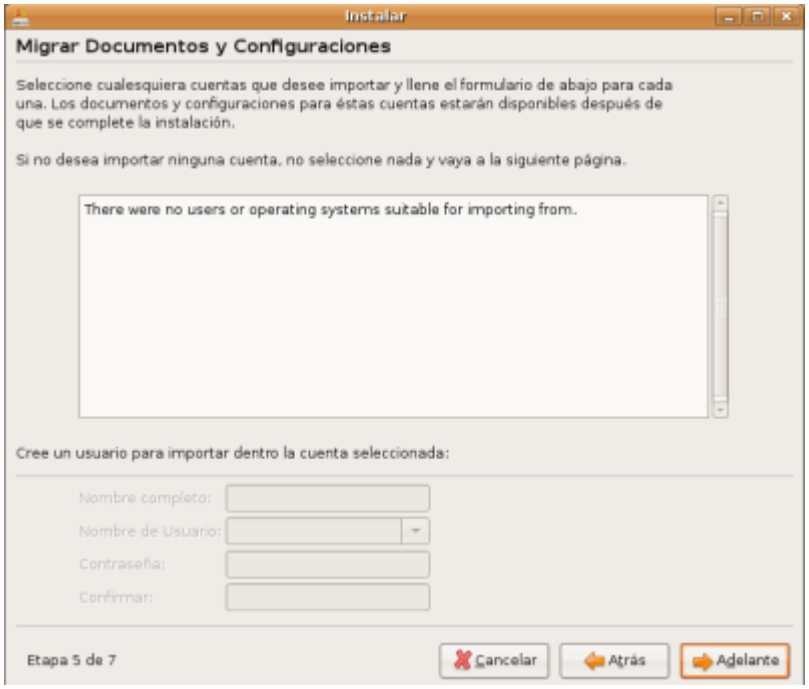
Usuario

Introducir nombre de usuario, contraseña y el nombre del equipo. (nota: no utilice espacios, mayúsculas o caracteres extraños en el nombre de usuario.)



Migración de datos

(Se ha de completar ya que la guía inicial no era de Feisty y esta característica es nueva)



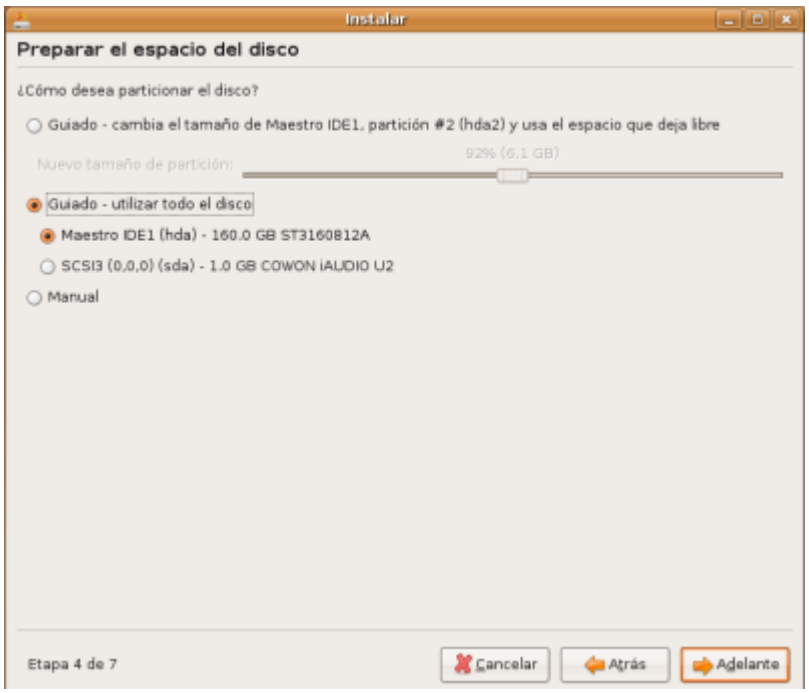
Seleccionar un disco

La primera parte de estas opciones es una lista de los discos duros que Ubuntu ha detectado. Para usar la partición guiada (guided) seleccionar uno de ellos y click en siguiente.

La segunda parte de la lista contiene una opción para utilizar automáticamente el área más grande de espacio libre en disco y una opción para editar manualmente la tabla de particiones (con una herramienta gráfica). El espacio libre al que se refiere es un área de disco sin ninguna partición en él. Nótese que no es lo mismo un espacio que no contiene ningún archivo que un espacio que no contiene ninguna partición (es decir, está sin formatear). Esta opción es por si se ha dejado espacio libre en el disco duro antes de empezar a instalar, o si se está instalando en un disco sin formatear (sin particiones aún).



Si se ha seleccionado un disco en la primera parte de las opciones disponibles, la siguiente pantalla le preguntará qué quieres hacer con el disco para hacer espacio a Ubuntu.



La acción por defecto es redimensionar una partición existente. La barra deslizante le permite seleccionar un nuevo tamaño para la partición existente. Puede también escoger el eliminar una partición existente para liberar espacio (esto lógicamente borrará todos los archivos que existan en esa partición).

Confirmación

Este es el momento de comprobar que todo está bien antes de que el instalador empiece a hacer cambios en el sistema.

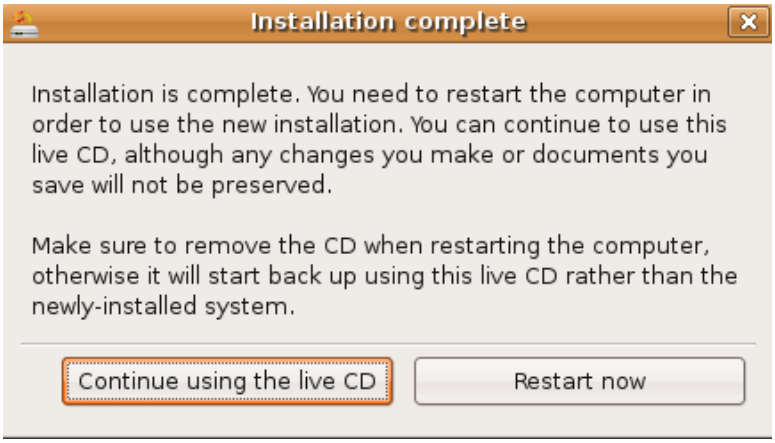


Instalación

El instalador hará los cambios en las particiones e instalará Ubuntu. Esto puede durar algún tiempo, especialmente el redimensionado de particiones ya que todos los datos han de ser movidos a la parte de la partición que va a mantenerse.

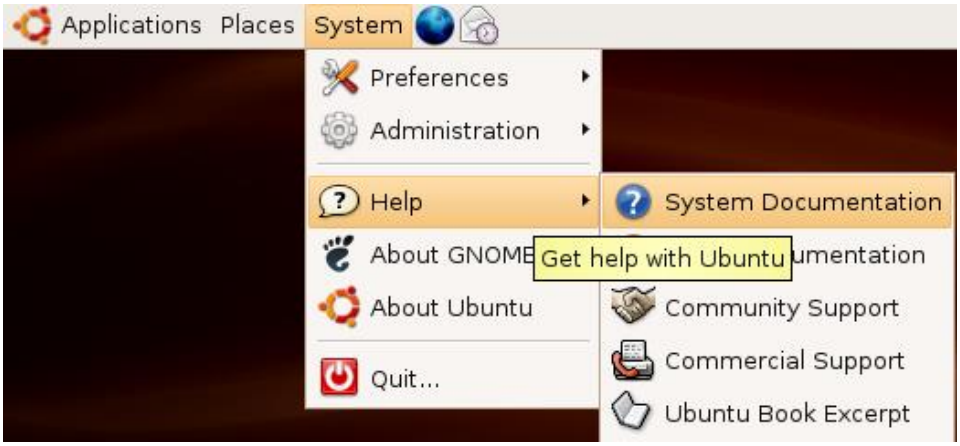
Finalización

Cuando el instalador acabe, se tendrá la opción de continuar en el CD o reiniciar tu ordenador.



Cuando reinicie el ordenador, este cargará Ubuntu si es el único sistema operativo instalado en el ordenador. Si se tiene más de un sistema operativo, le permitirá elegir con cual de ellos se quiere iniciar sesión.

Ahora ya se puede ingresar con el usuario y contraseña que se eligió durante la instalación. Se tiene documentación sobre el uso de Ubuntu instalada en su equipo, accesible desde **Sistema->Ayuda->Documentación** del sistema u online en:


Applications
Places
System
Preferences
Administration
Help
About GNOME
About Ubuntu
Quit...
System Documentation
Get help with Ubuntu
Community Support
Commercial Support
Ubuntu Book Excerpt

ANEXO 2

SECUENCIA DE EJECUCIÓN DEL ALGORITMO PARA DETECCIÓN DE INTRUSOS WIFI

1. Creación de Vector contenedor de direcciones IPs de equipos en la red conocida
2. Creación de Vector contenedor de direcciones MAC de equipos en la red conocida
3. Inicialización de Interfaz de red del Servidor (eth0, eth1, etc)
4. Establecimiento de Segmento IP en el cual trabaja la WLAN.
5. Especificación de Gateway del Router AP
6. Registro de Direcciones IP de equipos existentes en la WLAN autorizados.
7. Inicio de sesión del programa en AP
8. Operación Selectiva: Direcciones Autorizadas / Direcciones Desconocidas
9. Verificación de existencia de direcciones distintas a los contenidos de los vectores inicializados.
10. Obtención de Direccionamiento Físico y Lógico.
11. Publicación de datos de equipos en la Red Local y Desconocida.

ANEXO 3

CODIGO FUENTE - PROGRAMA DE DETECCIÒN DE INTRUSOS WIFI

```
#!/bin/bash

#declaracion de arrays
declare -a IPS_CONOCIDAS
declare -a MACS_CONOCIDAS

####################
#Configuracion:
####################

#Array de ip's conocidas,

IPS_CONOCIDAS=( "192.168.10.1" "192.168.10.100" )

#Array de MAC's conocidas

MACS_CONOCIDAS=( "00:11:22:33:44:55" "00:12:13:14:15:16" )

#Interfaz de red
DEVICE="eth0"

#Mascara de red (24=255.255.255.0, 16=255.255.0.0)
MASK=24

#####################
#Menu de opciones
foropt in $@; do
if [ "$opt" = "-h" ]; then
echo "PROGRAMA DE DETECCIÒN DE INTRUSOS WIFI"
echo "MENU DE OPCIONES:"
echo " -h Muestra esta ayuda"
echo " intruso con la fecha primero, no escribe ninguna otra información"
echo " -n No hace uso del programa notify-send que informa al escritorio de los
resultados"
echo " -m No hace uso del programa arp y no resuelve las MAC de los
resultados"
echo " -a Devuelve todos los hosts encontrados independientemente de las"
```

```
echo " variables internas IPS_CONOCIDAS y MACS_CONOCIDAS"
exit
fi
if [ "$opt" == "-l" ]; then
LOG=1
fi
if [ "$opt" == "-n" ]; then
NONOTIFY=1
fi
if [ "$opt" == "-m" ]; then
NOMAC=1
fi
if [ "$opt" == "-a" ]; then
IPS_CONOCIDAS=( )
MACS_CONOCIDAS=( )
fi
done

#aqui se obtiene la ip local
ip=$(/sbin/ifconfig "$DEVICE" | grep "inet" | awk '{print $2}' | cut -c 6-)
if [ ! $LOG ]; then
echo "Mi ip: $ip"
fi

IPS_CONOCIDAS[${#IPS_CONOCIDAS[*]}]=$ip
if [ ! $LOG ]; then
echo "No se controlan los equipos siguientes: "${IPS_CONOCIDAS[*]}
if [ "${MACS_CONOCIDAS[*]}" != "" ] && [ ! $NOMAC ]; then
echo "No se controlan los equipos con las MAC siguientes:
"${MACS_CONOCIDAS[*]}
fi
fi

#Comproción de los programas que se usan en la notificación
if [ ! -x /usr/bin/nmap ]; then
echo "El programa nmap no está instalado!"
exit
fi
if [ ! $NONOTIFY ]&& [ ! -x /usr/bin/notify-send ]; then
echo "El programa notify-send no está instalado!"
echo "Puedes llamar al programa con la opcion -n para no usar notify-send"
```

```
exit
fi
if [ ! $NOMAC ]&& [ ! -x /usr/sbin/arp ]; then
echo "El programa arp no está instalado!"
echo "Puedes llamar al programa con la opcion -m para no usar arp"
exit
fi

if [ ! $LOG ]; then
echo "Buscando equipos..."
fi
HOST_IPS=$(/usr/bin/nmap -sP ${IPS_CONOCIDAS[0]}/$MASK -oG -)

#aqui cortamos el formato obtenido anteriormente de archivo para solo obtener
las ip's
IPS=$(echo "$HOST_IPS" | grep Host | cut -c 7-20 | tr -d "()"

#aqui se captura el numero de lineas que tiene el archivo
#la cantidad de ip's que hay en el archivo "-" (entrada standard)
contador=$(echo "$IPS" | wc -l - | cut -c 1-2)
total=$(expr $contador - 1)

export DISPLAY=:0
export XAUTHORITY="$HOME/.Xauthority"

#Bucle de búsqueda entre las ip's encontradas
var=0
while [ $var -le $total ]; do
SALTA_BUCLE=0
letvar=$var+1
#captura de ip por linea
linea=$(echo "$IPS" | sed -n "$var p"
linea=${linea/ /}
for i in ${IPS_CONOCIDAS[*]}
do
if [ "$i" == "$linea" ]; then
if [ ! $LOG ]; then
echo "La IP $linea está en la red conocida"
fi
SALTA_BUCLE=1
break
```

```
fi
done
if [ "$SALTA_BUCLE" == "1" ]; then
continue
fi
#obtención de informacion de la ip
if [ ! $NOMAC ]; then
ARP=$(/usr/sbin/arp -a $linea)
else
ARP=""
fi
#infor de mac
MAC=$(echo "$ARP" | awk '{print $4}')

MAC=${MAC/ /}
NAME=$(echo "$ARP" | awk '{print $1}')
for i in ${MACS_CONOCIDAS[*]}
do
if [ "$i" == "$MAC" ]; then
if [ ! $LOG ]; then
echo "La IP $linea (HOST: $NAME MAC: $MAC) está en la red conocida"
fi
SALTA_BUCLE=1
break
fi
done
if [ "$SALTA_BUCLE" == "1" ]; then
continue
fi

if [ ! $NOMAC ]; then
AVISO="Conectado $linea (HOST: $NAME MAC: $MAC)"
else
AVISO="Conectado $linea"
fi

if [ ! $NONOTIFY ]; then
#aviso al sistema de notificaciones de escritorio
/usr/bin/notify-send "$AVISO"
fi
```

```
if [ $LOG ]; then
if [ ! $NOMAC ]; then
echo `/bin/date --rfc-3339=seconds`" HOST $linea ARP $ARP"
else
echo `/bin/date --rfc-3339=seconds`" HOST $linea"
fi
else
echo "$AVISO"
fi

done
```

ANEXO 4

COMANDOS DE INSTALACIÓN Y CONFIGURACIÓN DE APLICACIONES NECESARIAS PARA EJECUCIÓN DEL PROGRAMA DETECTOR DE INTRUSOS WIFI

CREACIÓN DEL PROGRAMA BASH

Guardar el scritp (código fuente del programa) scanner__wifi en el directorio:

/home/nombre_usuario/scanner__wifi

comando:

sudogeditalertared

ASIGNACIÓN DE PERMISOS DE EJECUCIÒN

comando:

sudochmod +x sacanner__wifi

CREACIÓN DE DAEMON:

comando:

crontab -e

editar linea:

*/3 * * * * /home/nombre_usuario/scanner__wifi

Con esta especificación el sistema ejecutara cada 3 minutos el script , en caso de detectar la presencia de equipos desconocidos, a través del notificador del SO se visualizará los datos de

equipos intrusos.

INSTALACIÓN DE PANEL DE NOTIFICACIONES DE UBUNTU

comando:

```
sudo apt-get install libnotify-bin nmap net-tools
```